UNIVERSITÀ DEGLI STUDI DI TORINO

DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN

DIRITTO, PERSONA E MERCATO

XXIX CICLO

BITCOIN: ANALISI DI UN NUOVO SISTEMA MONETARIO

Tesi presentata da: Dott. Pietro Antonio Messina

Tutor: Prof. Michele Graziadei

Coordinatore del dottorato: Prof. Roberto Caranta

A.A.: 2016-2017

S.S.D.: Ius/05 Diritto dell'economia

Abstract

La tesi concerne la definizione dei bitcoin e la questione se essi siano una moneta.

Per rispondere a tale domanda si elabora la nozione di sistema monetario: un sistema che disciplina (i) il riferimento ad un'unità numerica, divisibile e astratta, e (ii) la produzione e uso di mezzi di pagamento, strumenti attraverso i quali si concretizzano le unità astratte nella realtà dei rapporti tra consociati. Il sistema monetario persegue inoltre lo scopo di sostenere l'aspettativa diffusa di poter utilizzare in futuro (e di vedere utilizzata da altri) l'unità di conto e i mezzi di pagamento, in breve sostiene la fiducia dei consociati nel sistema, e contiene i rischi di comportamenti opportunistici estrattivi di coloro che hanno il potere di emettere nuovi mezzi di pagamento. La moneta è quindi intesa come un'istituzione sociale, prima ancora che economica, regolata dal diritto.

Al termine della ricerca si giunge alla conclusione che i bitcoin sono ideati secondo il modello del sistema monetario e, pur differenziandosi molto dai modelli tradizionali di sistema monetario, per questo aspetto possono essere associati all'idea di moneta.

In particolare, nei bitcoin l'aspettativa dei "consociati" di poter utilizzare in futuro l'unità di conto, e che altri utilizzino a loro volta l'unità di conto, non si fonda su un rapporto di soggezione ed appartenenza ad un sistema giuridico – come nel caso delle monete statali –, bensì sui vantaggi legati all'adozione dei bitcoin e sulla resilienza del sistema. La resilienza del sistema è connessa alla tecnologia implementata, che permette la gestione collettiva di un'attività comune (la tenuta del registro su cui sono allocati i titoli di "proprietà" dei bitcoin tra gli utenti del sistema) mediante una rete peer to peer senza alcuna controparte centrale, mentre i vantaggi legati all'adozione dei bitcoin discendono, in modo particolare, dalla scelta di fissare nell'algoritmo un limite fisso di unità producibili e dalla dinamica deflazionistica implicita a tale scelta.

Mentre nel contesto delle monete tradizionali l'autorità *impone* l'accettazione della moneta avente corso legale, nel contesto dei bitcoin l'algoritmo *persuade* gli utilizzatori a partecipare al progetto. Gli strumenti attraverso cui tale risultato è perseguito, però, in particolare la previsione di un'offerta rigida e limitata, se da un lato proteggono il sistema da comportamenti opportunistici dell'emittente, dall'altro lato provocano instabilità nel valore dei bitcoin e inducono nel pubblico aspettative deflazionistiche che incentivano gli attori economici a tesaurizzare la moneta e non a utilizzarla per gli scambi, rischiando di comprometterne il funzionamento come unità di misura del valore economico di beni e servizi e come mezzo di scambio, specie con riferimento ai rapporti di durata.

Ne consegue che il successo dei bitcoin è più ragionevolmente riconducibile a ragioni speculative e al loro uso come bene rifugio piuttosto che all'adozione diffusa come moneta da utilizzare per i pagamenti. Essi quindi rappresentano un modello nuovo di sistema monetario che offre importanti spunti di riflessione sul funzionamento della moneta e sulle possibili evoluzioni di questo istituto, anche alla luce di questa nuova tecnologia implementata per la prima volta nei bitcoin, ma tale nuovo modello presenta forti limitazioni di tipo strutturale riconducibili alla scelta di non fare affidamento sull'ordinamento giuridico e di non avere controparti centrali responsabili della stabilità del valore della moneta.

BITCOIN:

ANALISI DI UN NUOVO SISTEMA MONETARIO

1. Introduzione

1.1. Incipit

Si narra che il 22 maggio 2010, il programmatore Laszlo Hanyecz comprò due pizze "papa Giovanni" in cambio di 10.000 bitcoin. Sono passati ormai sette anni. Durante il mese di giugno 2017[1], il valore di un bitcoin oscillava tra i 2.400 e i 2.900 dollari. Assumendo un valore medio di 2.500 dollari, al valore di cambio bitcoin/dollaro attuale, le due pizze sono state pagate 25 milioni di dollari. Il giorno 22 maggio è ora celebrato sulla rete come il "*Bitcoin pizza day*": la ricorrenza della prima e probabilmente più famosa vendita conosciuta di un bene contro bitcoin.

Cosa è successo in questi anni? Cosa spiega il successo di questo nuovo fenomeno monetario e come mai oggi un bitcoin vale così tanto? I bitcoin sono davvero una moneta? Se sì, che tipo di moneta sono? Possono essere considerati moneta dal punto di vista giuridico?

La materia oggetto di studio è affascinante: ci si trova di fronte ad una nuova tecnologia che ha permesso di realizzare uno strumento monetario completamente indipendente dallo Stato e dal sistema giuridico tradizionale, le cui peculiarità ne rendono difficile l'inquadramento entro le tradizionali categorie giuridiche. Contestualmente, viviamo in un mondo in cui ritenere che siano moneta in senso giuridico solo le monete e le banconote emesse dallo Stato è completamente anacronistico: tutti facciamo esperienza diretta di pagamenti in formato elettronico e presto ci abitueremo a pagare non solo con bancomat e carte di credito, ma con anche con il telefono cellulare.

I primi bitcoin sono stati creati nel 2009, pochi mesi dopo l'inizio della grande crisi finanziaria che ha colpito il sistema economico globale travolgendo alcune importanti multinazionali finanziarie private e costringendo gli Stati a immettere enormi quantità di denaro pubblico nel circuito bancario per sostenere la liquidità ed evitare il collasso. In questo contesto di crisi del sistema tradizionale, la proposta di una moneta

[1] Nota di redazione: la tesi non prende in considerazione eventi accaduti dopo il 20 giugno 2017.

completamente diversa presentata in antitesi alle monete tradizionali usate nel sistema bancario appare ancora più interessante.

I bitcoin aspirano ad essere una vera e propria moneta, direttamente utilizzabile per comprare o vendere beni senza che occorra intrattenere relazioni contrattuali con soggetti terzi che forniscono servizi di pagamento o che gestiscono conti correnti. L'obbiettivo del progetto è disintermediare i rapporti di scambio monetario sul web: creare un contante digitale gestito direttamente dagli utilizzatori stessi del sistema, uno strumento di pagamento alternativo alle monete statali tradizionali[2]. Essi non dipendono da uno specifico ambiente virtuale, né sono inseriti in un contesto giuridico: sono utilizzabili senza vincoli geografici dappertutto nel mondo e possono essere scambiati liberamente, fatta salva la presenza di leggi in senso contrario all'interno degli ordinamenti giuridici nazionali, contro le valute tradizionali.

La caratteristica che contraddistingue sotto il profilo tecnologico queste valute virtuali[3] da altri esperimenti di registrazione virtuale di valori è l'utilizzo della crittografia per realizzare tre funzioni: (*i*) permettere ad un insieme di persone di riconoscere in modo collettivo in capo ad un soggetto il controllo esclusivo su un bene digitale; (*ii*) sintetizzare in modo univoco un determinato insieme di informazioni in stringhe alfanumeriche che permettono di verificare e garantire la consistenza dei dati nel tempo; e (*iii*) creare una competizione matematica tra i partecipanti di una rete la cui soluzione richiede tempo e nella quale è improbabile che due o più soggetti vincano simultaneamente. Attraverso la

---

[2] DODD N., *The Social Life of Money*, Princeton University Press, 2014, p. 9: "*the debates that have sprung up around the Bitcoin phenomenon are revealing because most of them are focused on the possibility of developing a serious rival to state currency"*.

[3] Il termine valute virtuali è stato utilizzato in uno dei primi studi comprensivi sul tema con un significato molto ampio che comprendeva qualsiasi meccanismo digitale di rappresentazione e gestione di valori, utilizzato all'interno di una comunità virtuale come moneta per consentire scambi tra gli utenti o consentire l'acquisto di servizi ulteriori. In questa ampia categoria venivano inclusi tutti i sistemi di "crediti" che si collezionano in giochi elettronici al fine di acquisire, all'interno del gioco stesso, potenziamenti o vantaggi; ovvero i crediti connessi a programmi di fedeltà; o ancora le valute utilizzate all'interno di Facebook o di Second Life. In tutti questi casi si tratta di sistemi creati e gestiti da entità ben definite, con una regolamentazione generalmente contrattuale delle modalità di acquisizione e uso di tali valori, che nella grande maggioranza dei casi è limitato all'interno del servizio o software offerto all'utente. BANCA CENTRALE EUROPEA, *Virtual Currency Schemes*, 2012, disponibile sul sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (ultima visita 20 giugno 2017).

combinazione di queste funzioni è stato possibile creare dei registri digitali condivisi e decentrati, estremamente affidabili, su cui è possibile annotare in modo sicuro e non modificabile informazioni relative al controllo esclusivo di un soggetto su un valore memorizzato in forma digitale. Ulteriore caratteristica molto importante di questi registri è che l'aggiornamento degli stessi può essere affidato ad un gruppo indeterminato di utenti senza la necessità di individuare un soggetto *super partes* che coordini e gestisca la tenuta del registro, cosicché il registro può essere conservato e aggiornato in modo decentrato su una rete di computer.

L'implementazione di questa nuova tecnologia, chiamata *blockchain*, o *distributed ledger technology*, all'interno di una rete aperta, ha permesso la creazione di sistemi di scambio di valori virtuali che per la prima volta sono gestiti in modo collettivo direttamente dai partecipanti alla rete stessa, senza che occorra un soggetto centrale garante dell'esecuzione delle transazioni e della corretta allocazione delle risorse.

La materia è, evidentemente, molto complessa: le caratteristiche e il funzionamento di questi sistemi sin qui succintamente descritti saranno illustrate con maggiore ampiezza e dettaglio nel corso della tesi. Ciò che preme sottolineare ora è che una nuova tecnologia, strutturata a grandi linee secondo quanto sopra descritto, ha permesso la creazione di un sistema di scambio di valori decentrato. Questa è la caratteristica più importante e significativa, sotto il profilo strutturale, dei bitcoin e di tutte le criptovalute – monete basate sulla crittografia – che ne seguono il modello.

Questa nuova tecnologia, lo si è accennato, è stata inventata con l'obbiettivo di creare una nuova moneta virtuale, alternativa alle monete statali oggi in circolazione. I valori digitali la cui allocazione è riportata nel registro condiviso non rappresentano beni materiali o crediti, bensì sono multipli o sottomultipli di un'unità di conto creata contestualmente al registro e specificamente connessa al software che regola la gestione del registro stesso. Le unità attribuite agli utilizzatori sono, in altri termini, create dal nulla a seguito dell'annotazione sul registro: a differenza di quanto avviene in ambito bancario tali scritture non rappresentano, però, un credito verso un emittente, ma sono mere rappresentazioni numeriche di un'unità di conto astratta.

La produzione di queste unità è disciplinata dall'insieme di regole che organizzano la tenuta del registro, in particolare da quel sotto insieme di regole relativo

alla creazione di nuove unità di conto all'interno del registro. L'insieme di tutte le regole che disciplinano l'organizzazione del registro di una criptovaluta coincidono essenzialmente con le istruzioni contenute nel software su cui si basa la criptovaluta. Ad esse ci si riferisce con il termine "protocollo".

Al di là dei tecnicismi relativi alle modalità con cui è gestita l'attribuzione di unità all'interno del protocollo, i bitcoin sono presentati al pubblico come un bene scarso, suscettibile di appropriazione, durevole ed utilizzabile come mezzo di scambio per ottenere altri beni. Essi sono concepiti, quindi, come bene scarso e prezioso: oro digitale che, in quanto scarso e prezioso, può essere usato come moneta.

I bitcoin, però, non esistono in natura, sono invece il prodotto di un articolato sistema gestito da un software eseguito da una collettività di utenti connessi in rete. Il fatto che la tenuta del registro sia affidata ad una collettività indeterminata di utenti e che le regole di funzionamento del sistema, ivi comprese quelle relative al trasferimento della proprietà dei bitcoin, siano scritte nel software che gestisce il registro collettivo, rende questo schema completamente autonomo rispetto alla regolamentazione esterna quale può essere la legge di fonte statale. Le criptovalute organizzate secondo il modello 'bitcoin' offrono, cioè, un servizio di registrazione e di scambio di valori 'contabili' che non richiede un supporto legislativo da parte di alcuno Stato e che quindi può funzionare in modo sicuro trasversalmente in diverse giurisdizioni, indipendentemente dal luogo in cui l'utente si connette alla rete. In questa prospettiva i bitcoin sono presentati come una moneta sovranazionale, incontrollabile da parte degli stati e quindi libera da quelli che sono considerati i nefasti effetti connessi al monopolio pubblico della moneta: primi fra tutti il signoraggio e l'inflazione. In questa prospettiva il modello è proposto in antitesi alla valuta statale moderna, il cui funzionamento fa affidamento su una banca centrale indipendente e un sistema bancario regolato e garantito che adatta l'offerta di liquidità sul mercato attraverso l'erogazione di crediti, e più in generale in antitesi rispetto a qualsiasi forma monetaria il cui valore sia controllato, anche indirettamente, dallo Stato e quindi sia suscettibile di variare in ragione di interventi che non dipendono direttamente dal comportamento dei mercati.

A differenza, quindi, di altre valute virtuali che afferiscono normalmente al rapporto tra un utente o un gruppo di utenti e il fornitore di un determinato software o

servizio online, le criptovalute aspirano invece ad acquisire rilevanza in uno spazio pubblico non previamente delimitato da accordi tra utenti e controparti centrali.

Dopo questi primi paragrafi introduttivi, densi di concetti che saranno ripresi nel corso della tesi, è possibile intuire che l'analisi giuridica di questo fenomeno non sia affatto semplice, né scontata: che un giurista si proponga di studiare una moneta progettata per essere indipendente dall'ordinamento giuridico ed estranea alla legge può apparire, al contrario, quasi un paradosso. Eppure proprio le particolari caratteristiche delle criptovalute le rendono estremamente interessanti per un giurista, di fronte al quale si manifestano numerosi profili di interesse suscettibili di approfondimento, sia connessi al tema della autoregolamentazione dei sistemi informatici e della *regulation by design*, sia connessi al tema della definizione e regolamentazione del fenomeno monetario.

La presente tesi si interessa allo studio dei bitcoin con particolare attenzione a questo secondo aspetto e si propone, in particolare, di problematizzare: (*i*) la tesi secondo cui i bitcoin sono una nuova forma di moneta che sostituirà la moneta oggi in circolazione; e (*ii*) la concezione stessa di moneta adottata in questo contesto, secondo cui la moneta è, alla base, un bene scarso che viene utilizzato spontaneamente dai consociati per l'intermediazione degli scambi.

Cercare di capire cosa implichi e cosa voglia dire la semplice affermazione secondo cui «*il bitcoin è una moneta*» è un'impresa tutt'altro che semplice ed è bene chiarire sin da subito che a tale domanda non potrà darsi una risposta conclusiva. Si cercherà, invece di offrire una chiave di lettura che permetta di comprendere meglio il fenomeno mettendo in luce alcuni aspetti strutturati che caratterizzano i bitcoin.

Per raggiungere questo obbiettivo occorrerà acquisire una buona familiarità con il funzionamento di queste nuove criptovalute ed in particolare con il protocollo Bitcoin e occorrerà, in secondo luogo, svolgere alcune riflessioni sulla definizione stessa di moneta. Il fenomeno monetario è al tempo stesso sociale, economico, giuridico e politico. Il diritto vi interviene sia per effetto dell'esercizio della sovranità monetaria da parte del sovrano, che nella sua più tipica espressione si risolve innanzitutto nel riconoscimento di una moneta ufficiale all'interno dello Stato, sia in rapporto al riconoscimento e alla regolamentazione dei comportamenti concretamente tenuti dai soggetti privati nel mercato. Affrontata da un giurista, la questione circa la definizione della moneta acquista

quindi uno spessore specifico legato alla regolamentazione e al supporto che il diritto presta a questo istituto particolarmente complesso.

Lo studio dei bitcoin presenta, inoltre, l'ulteriore difficoltà connessa al fatto che i bitcoin nascono e sono concepiti in aperta antitesi con lo Stato e il diritto di fonte statale e prendono forma in un contesto di relazioni economiche e sociali non regolato o solo marginalmente regolato dalla legge. Inoltre, a tutt'oggi il fenomeno delle criptovalute non è stato regolamentato in maniera comprensiva dal legislatore.

Ci si trova, dunque, di fronte ad un fenomeno nuovo, di straordinaria complessità che ha caratteristiche peculiari ed innovative rese possibili dal progresso tecnologico in campo informatico. In questo particolare ambito non ci si trova a commentare particolari aspetti di regolamentazioni esistenti, ma la questione centrale è, invece, come rapportarsi ad un nuovo modello di sistema monetario. Chiedersi se i bitcoin sono moneta e, antecedentemente, cosa è moneta per un giurista, non è un vezzo intellettuale, ma il presupposto necessario per svolgere successivamente delle riflessioni circa l'eventuale regolamentazione di questo fenomeno. È vero che il dato concreto della vita con cui deve confrontarsi la ricerca è che oggi giorno esiste una moneta virtuale chiamata bitcoin a cui è attribuito un valore economico – peraltro considerevole –, che viene venduta e acquistata contro altre valute e che viene utilizzata per effettuare donazioni o pagamenti tra privati. Come deve reagire il diritto di fronte a questo fenomeno? Esistono regolamentazioni esistenti suscettibili di applicazione ai bitcoin? Occorre crearne di nuove *ad hoc*? Per rispondere a queste domande è necessario capire innanzitutto di cosa stiamo parlando e da qui l'esigenza di provare a rispondere in modo critico e di caratterizzare con maggiore spessore l'ipotesi secondo cui i bitcoin sono una moneta.

Lo sviluppo della tecnologia *blockchain* apre nuove possibilità di riforma e riorganizzazione del rapporto tra Stato e moneta[4]. In questo contesto, il primo e importante contributo di una ricerca giuridica sui bitcoin può essere quello di offrire una descrizione del fenomeno con le lenti del giurista, attenta cioè alla dimensione della regolamentazione ed istituzionalizzazione dei rapporti sociali entro norme sorrette dalla minaccia di sanzioni che incentivano determinati comportamenti, cercando di evidenziare

[4] DODD, op. cit., p. 5.

analogie e divergenze tra gli elementi costitutivi del fenomeno oggetto di studio – i bitcoin – e il contesto della moneta statale. Per questi motivi la presente ricerca si pone il duplice obbiettivo di descrivere in ottica giuridica il mondo delle criptomonete e dei bitcoin e di sviluppare alcune riflessioni sulla moneta e sul ruolo che gioca il diritto nella definizione della stessa, per eventualmente comprendere se ai bitcoin corrisponde un nuovo modello di sistema monetario e in che termini questo si differenzi dal modello statale.

1.2. Struttura della tesi

Negli ultimi anni sono stati pubblicati numerosi interventi della dottrina che si sono posti la questione di come possano essere definiti e classificati i bitcoin[5]. Circa la specifica questione se i bitcoin possano essere considerati una moneta, è frequente riscontrare in dottrina un approccio basato sulla definizione funzionale di moneta, secondo cui occorre valutare se essi possano essere utilizzati come mezzo di scambio, riserva di valore e unità di conto. In questa tesi non si condivide tale approccio perché si ritiene che esponga al rischio di trarre conclusioni arbitrarie basate su analisi fattuali che

[5] Tra i recenti contributi della dottrina italiana si segnalano: GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di problema?*, in *Il diritto dell'informazione e dell'informatica*, 2015, p. 415; LEMME G. e PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Rivista di Diritto Bancario*, dirittobancario.it, 2016, p. 43; MANCINI M., *Valute virtuali e Bitcoin*, in *Analisi Giuridica dell'Economia*, 2015, pp. 117 ss.; VARDI N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Il Diritto dell'informatica e dell'informazione*, 2015, p. 448; AMATO M. e FANTACCI L., *Per un pugno di Bitcoin*, Università Bocconi Editore, 2016; e v. anche: AMENTA V., *'Fourth generation' payment sistems: Bitcoins*, in *Ciberspazio e diritto*, vol. 15, 2014, p. 11; ARANGÜENA G., *Bitcoin: una sfida per policymakers e regolatori*, in *Quaderni di Diritto Mercato Tecnologia*, 2014, p. 19; BERTARINI B., *Valute virtuali: problematiche giuridiche e prospettive*, in *Innovazione e Diritto*, vol. 5, 2015, p. 40; SCALCIONE R., *Gli interventi delle autorità di vigilanza in materia di schemi di valute virtuali*, in *Analisi Giuridica dell'Economia*, 2015, 1, p. 139. Tra i contributi della dottrina straniera: GRINBERG R., *Bitcoin: An Innovative Alternative Digital Currency*, in *Hastings Science & Technology Law Journal*, Vol. 4, 2012, p. 160; KAPLANOV N.M., *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, in *Loyola Consumer Law Review*, 2015, vol. 25, pp. 111 ss.; KIEN M. e MENG L., *Coining Bitcoin's «Legal-Bits»: Examining The Regulatory Framework For Bitcoin And Virtual Currencies*, in *Harvard Journal of Law & Technology*, vol. 27, 2014, p. 587; TURPIN J. B., *Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework*, in *Indiana Journal of Global Legal Studies*, 2014, vol. 21, p. 335; JEANS E.D., *Funny money or the fall of fiat: bitcoin and forward-facing virtual currency regulation*, in *Journal on Telecommunication & High Technology Law*, vol. 13, 2015, p. 99.

possono rivelarsi effimere o comunque suscettibili di modificarsi nel tempo e non sufficientemente oggettive.

Si cercherà invece di fare chiarezza sulle diverse teorie inerenti la definizione del fenomeno monetario, concentrando l'attenzione sul contesto istituzionale che circonda la moneta e ne permette l'esistenza: attenzione che difficilmente può essere perseguita allorché ci si concentri sulle funzioni che la moneta svolge e non già su cosa permetta alla moneta di svolgere tali funzioni e come essa sia organizzata.

Ci si chiederà, quindi, *in primis*, cosa è la moneta e, in particolare, come funziona la moneta intesa come istituzione sociale, economica e giuridica. Cercando di rispondere a questa domanda si proverà a ricondurre la nozione di moneta a tre elementi costitutivi: (*i*) un'unità numerica, divisibile e astratta; (*ii*) dei mezzi che ne permettono la rappresentazione nei rapporti tra i consociati; e (*iii*) l'aspettativa diffusa tra un certo numero di persone di poter utilizzare in futuro (e di vedere utilizzata da altri) tale unità numerica e tali mezzi di pagamento per misurare, rappresentare e, quindi, trasferire, valori economici. Tale aspettativa si fonda, a sua volta, su una convenzione più o meno esplicita tra i consociati (la 'convenzione monetaria') che regola le modalità con cui tale unità di conto è rappresentata e scambiata nel mondo reale e che vede come parti, generalmente, i soggetti che fanno uso di tale moneta, il potere costituito che su di essi esercita la propria sovranità e, se diverso, l'emittente dello strumento. Invero, nella storia occidentale lo Stato ha sempre assunto un ruolo preminente nella definizione dei termini della convenzione: perché il sovrano ha interesse a poter riscuotere le tasse (per le quali occorre un sistema di misurazione del valore omogeneo); perché al potere di definire i termini di questa convenzione monetaria possono corrispondere grandi vantaggi economici; e perché garantire la presenza di una moneta è una funzione pubblica di interesse generale. Il corso legale è lo strumento cardine che sorregge l'aspettativa di cui si è parlato nel contesto di sistemi monetari organizzati secondo il modello dell'imposizione da parte dello Stato attraverso la legge e l'accettazione della convenzione da parte dei cittadini mediante l'uso quotidiano della moneta statale.

Ponendo l'accento sulla convenzione tra consociati che regola la moneta si evidenzierà, dunque, che la moneta è sempre innanzitutto un'istituzione sociale regolata dal diritto, prima ancora che economica, e che essa è molto più articolata rispetto alla

narrativa dominante che la descrive essenzialmente come un semplice mezzo di scambio nella (naturale) disposizione degli agenti economici. Per rispecchiare questo passaggio teorico, si proporrà di passare dalla parola "moneta", che implicitamente spesso si ricollega alla nozione di "moneta–mezzo di scambio", ad un discorso sviluppato intorno alla nozione di "sistema monetario". Tale seconda espressione è meno ambigua della parola 'moneta': essa richiama l'aspetto giuridico sotteso al fenomeno monetario ed evita la confusione tra la moneta intesa come istituzione e la moneta intesa come concreta estrinsecazione nella vita reale dell'unità di conto, resa possibile dalla convenzione pocanzi richiamata. Si volgerà infine l'attenzione alle complesse dinamiche che caratterizzano qualsiasi sistema monetario, alle strutture istituzionali che sorreggono la fiducia dei consociati e al ruolo dello Stato e del diritto nella gestione del sistema monetario.

A queste riflessioni sarà dedicato il primo capitolo della tesi.

Così chiarito il quadro di riferimento entro cui si vuole collocare il fenomeno dei bitcoin, nel corso della tesi si cercherà di mostrare che l'aspetto cruciale dei bitcoin è la pretesa di costituire una nuova convenzione monetaria alternativa a quella cui lo Stato partecipa, dove i rapporti tra consociati sono gestiti non in dialogo con un'autorità centrale che "impone" un sistema monetario, bensì dall'utilizzo di un algoritmo uguale per tutti e (apparentemente) immodificabile.

Poiché le ragioni di questa scelta hanno un'origine prevalentemente ideologica, la prima parte del secondo capitolo della tesi sarà dedicata alla descrizione del contesto culturale da cui hanno origine i bitcoin.

La seconda parte del secondo capitolo sarà invece dedicata alla descrizione del protocollo bitcoin. Si darà evidenza, in particolare, dei meccanismi che consentono di fare affidamento sul sistema e di come il codice del software svolga una funzione normativa all'interno del sistema. Da ultimo, si accennerà ai meccanismi attraverso cui sono gestiti gli aggiornamenti del software, e si darà evidenza del fatto che il protocollo non è affatto immutabile.

Nel terzo capitolo si offrirà una sintesi dei tratti essenziali che caratterizzano il protocollo bitcoin e, alla luce della descrizione del funzionamento del sistema offerta nel precedente capitolo, si proveranno ad elaborare alcune considerazioni inerenti

l'importanza delle regole che disciplinano e organizzano il sistema, partendo dalla domanda 'cosa sono i bitcoin?'. Si cercherà quindi di dimostrare che il sistema bitcoin è articolato sulla falsa riga di un sistema monetario.

La seconda parte del capitolo sarà invece dedicata ad una disamina dei tentativi di qualificazione giuridica dei bitcoin, dalla quale si evince la difficoltà di iscrivere i bitcoin all'interno delle categorie conosciute del diritto: essi non sono moneta avente corso legale, non sono moneta scritturale, non sono moneta elettronica e non sono un sistema di pagamento. In tale contesto si renderà conto anche della categoria "valuta virtuale" coniata dalla Banca Centrale Europea e ripresa in altri contesti.

Nell'ultimo capitolo si svilupperanno le riflessioni conclusive sul sistema monetario 'bitcoin'.

Al termine della tesi si vorrà dimostrare che i bitcoin sono un sistema monetario nel quale l'aspettativa dei "consociati" di poter utilizzare in futuro l'unità di conto, e che altri utilizzino a loro volta l'unità di conto, non si fonda su un rapporto di soggezione ed appartenenza ad un sistema giuridico – come nel caso delle monete statali –, bensì sui vantaggi legati all'adozione dei bitcoin e sulla resilienza del sistema. Quest'ulima è connessa alla tecnologia implementata, che permette la gestione collettiva di un'attività comune (la tenuta del registro su cui sono allocati i titoli di "proprietà" dei bitcoin tra gli utenti del sistema) mediante una rete *peer to peer* senza alcuna controparte centrale. I vantaggi legati all'adozione dei bitcoin discendono, in modo particolare, dalla scelta di fissare nell'algoritmo un limite fisso di unità producibili e dalla dinamica deflazionistica implicita a tale scelta, oltre che dalla maggiore privacy che tale sistema offre rispetto alla moneta tradizionale e dalla possibilità di effettuare scambi transfrontalieri.

Mentre nel contesto delle monete tradizionali la convenzione monetaria è un fatto politico-giuridico dove l'autorità *impone* il sistema monetario, nel contesto dei bitcoin l'algoritmo *persuade* gli utilizzatori a partecipare al progetto.

Da questa riflessione scaturiscono una serie di considerazioni.

In primo luogo entrambi i sistemi sono "sistemi monetari", nel senso che in entrambi i casi si ha a che fare con unità di conto ideali, con regole che disciplinano la

creazione e l'uso di mezzi di pagamento e con meccanismi istituzionali che sorreggono la fiducia dei partecipanti nel possibile uso futuro della moneta.

In secondo luogo, a differenza del sistema monetario statale, i bitcoin non fanno affidamento sull'istituto del corso legale, ma sulla scelta di predeterminare il numero massimo di unità. La scarsità artificiale dei bitcoin così creata è il loro punto di forza, ma al tempo stesso anche il loro punto debole, perché l'offerta rigida di moneta rende strutturalmente instabile il valore della moneta e perché l'aspettativa deflazionista indotta dalla scarsità programmata alimenta circoli speculativi pro–ciclici che disincentivano l'uso dei bitcoin come mezzo di scambio e incrementano, ancor di più, la fluttuazione di valore della moneta.

Il contributo teorico più significativo che si intende offrire alla dottrina che si sta sviluppando circa le valute virtuali e i bitcoin consiste nell'avvicinare la nozione di moneta a quella di "sistema monetario", evidenziare che l'aspetto più importante del sistema bitcoin è costituito dalla centralità dell'algoritmo, e sottolineare che a tale aspetto è intrinsecamente collegato il limite più significativo di detto sistema, costituito dalla volatilità del potere d'acquisto dei bitcoin.

Parallelamente a queste considerazioni nella tesi si sviluppano alcune critiche verso la narrativa che dipinge i bitcoin come una moneta completamente "*trust-less*" e si evidenzieranno alcuni vantaggi connessi a tale sistema monetario, tra i quali la riduzione del rischio di comportamenti opportunistici estrattivi da parte del gestore del sistema monetario.

Capitolo I

Moneta e sistemi monetari

1. Prime considerazioni sulla nozione di moneta nelle scienze sociali

La moneta è un istituto particolarmente complesso, a tratti misterioso: tutti sanno intuitivamente di cosa si parla, ma al tempo stesso è assai difficile coglierne l'essenza, invero: "*the social relationships in which money is involved are by far the most abstract and obscure, and the knowledge generated through them is the most vast, complex, and difficult to grasp*"[6]. Di origine antichissima, la presenza della moneta è riscontrabile in società assai differenti tra loro, nello spazio e nel tempo: elemento indispensabile per qualsiasi mercato, essa si è manifestata in una pluralità di modi e forme nel corso della storia acquisendo una rilevanza via via crescente nella civiltà occidentale, al punto che è per noi difficile immaginare un vivere sociale che possa fare a meno di questo istituto[7]. È usuale che le prime pagine degli scritti sulla moneta sottolineino la difficoltà di sintetizzare in un'unica definizione la complessità di questo fenomeno, che può peraltro essere studiato attraverso le lenti di molteplici discipline e che pare quasi richiedere, proprio per la sua natura, un approccio multidisciplinare. Molteplicità e complessità sono, quindi, due concetti che caratterizzano l'istituto oggetto di studio e che si scontrano con

[6] DE SOTO JESÚS HUERTA, *Money, bank credit, and economic cycles*, Ludwig von Mises Institute, 3 ed., 2012, p. 806. INGHAM G., *The Nature of Money*, Polity, 2004, p. 5, ricorda che Schumpeter non è riuscito a finire il suo trattato sulla moneta (pubblicato postumo) perché non riuscì a chiarirsi sufficientemente le idee in merito.

[7] Per un approccio antropologico e sociologico v. DODD, op. cit.; Graeber D., *Debito: i primi 5000 anni*, Il saggiatore, 2012; Gregory C. A., *Savage Money: The Anthropology and Politics of Commodity Exchange*, Harwood Academic, 1997; Hart K., *Money in an Unequal World: Keith Hart and His Memory Bank*, Textere, 2001. Sulla storia della moneta v. anche FANTACCI L., *La moneta: storia di un'istituzione mancata*, Marsilio, 2005.

la semplicità con cui essa si presenta nell'uso quotidiano di qualsiasi consociato. È sorprendente il confronto tra la semplicità e l'intuitività con cui utilizziamo ogni giorno degli strumenti monetari e la difficoltà che ci si porrebbe davanti laddove ci fosse chiesto di definire in modo analitico cosa è moneta, come è prodotta, da dove viene, in cosa consiste o ancora da dove trae il suo valore.

L'idea di moneta utilizzata all'interno del sistema bitcoin riflette, in buona sostanza, la concettualizzazione dominante della moneta la descrive come un bene che svolge la funzione di mezzo di scambio all'interno di un mercato. Tale concettualizzazione si ispira alla visione economica classica della moneta intesa come un bene scarso che assume la funzione di intermediario degli scambi e diventa, essenzialmente, un mezzo di scambio universalmente accettato per i pagamenti. Così, i bitcoin sono concepiti, in primo luogo, come un bene digitale scarso che può essere usato come mezzo di scambio.

Si avrà modo di illustrare in seguito che i bitcoin sono, in realtà, un'istituzione complessa e che la stessa nozione di mezzo di scambio sottende più di quanto a prima vista appaia evidente. Orientandosi verso un'analisi giuridica dei bitcoin, occorre allora problematizzare questa semplificazione e ricontestualizzare la nozione di moneta all'interno di un quadro astratto più ampio e più solido.

Nei numerosi scritti sin qui prodotti sui bitcoin che hanno provato a rispondere alla domanda se essi siano, o non siano, "moneta", si è fatto riferimento alla definizione di moneta che si ricava da un approccio funzionale di stampo economico, secondo cui la moneta è mezzo di scambio, riserva di valore e unità di conto. Questo approccio ha il vantaggio di evidenziare e richiamare la funzione del mezzo di scambio, assai cara all'interno del paradigma dei bitcoin, ma non è sufficientemente descrittiva per un giurista perché, come si avrà modo di chiarire, non rende giustizia alla dimensione giuridica che circonda questo istituto. Studiare la moneta partendo da cosa essa "faccia" in termini economici e non invece chiedendosi cosa una moneta "sia" comporta, infatti, due rischi: il primo è di non evidenziare l'apparato normativo-regolamentare che è sotteso a qualsiasi moneta, fatto assai rilevante, specialmente per un giurista; il secondo è di trarre conclusioni arbitrarie e applicare determinate regole a fenomeni che appaiono essere qualcosa solo perché in un certo momento storico si comportano o non si comportano

secondo dinamiche tipiche del fenomeno astrattamente regolato, invece che applicare le regole a ciò che è strutturalmente configurato secondo la definizione che caratterizza la regola stessa, con il rischio di travisare la *ratio* delle norme o di non essere in grado di proporre nuove regolamentazioni efficaci laddove nuovi fenomeni le richiedano.

Nel corso del successivo capitolo si proverà, dunque, a sviluppare un approccio originale alla descrizione del fenomeno monetario, che evidenzi la dimensione giuridica che caratterizza questo istituto senza con ciò ridurre la questione ad una contrapposizione tra diritto statale e forze del mercato, e che permetta, nel prosieguo della tesi, di affrontare la questione dell'ascrivibilità dei bitcoin al *genus* monetario con maggiore cognizione di causa o, quantomeno, con un minor grado di semplificazione e correndo meno rischi di arbitrarietà.

Considerata la complessità della materia sarebbe oltremodo ambizioso tradurre questo sforzo in un tentativo di proporre una nuova dottrina monetaria *tout court*. Si è accennato a quanto sia difficile questa materia e si ribadisce che innumerevoli pensatori di ben più alta erudizione appartenenti a svariate discipline si sono cimentati, faticosamente, nel tentativo di sviluppare una teoria della moneta o nello sforzo di contribuire ad evidenziare alcuni aspetti del fenomeno monetario. È bene, allora, ribadire che qui si proverà a compiere una operazione di sintesi, in parte originale, delle teorie sviluppate, al fine di evidenziare alcuni aspetti della moneta utili ad una maggiore comprensione dei bitcoin e del loro rapporto con il diritto vigente, in particolare: il passaggio dalla nozione di moneta alla nozione di sistema monetario e di accordo monetario; il tema della "fiducia" all'interno del sistema monetario e l'importanza degli apparati istituzionali implementati per la costruzione di sistemi monetari e per il sostegno di tale fiducia, rispetto ai quali è spesso stato decisivo il contributo dello Stato e del diritto.

In primo luogo si tratterà quindi la definizione funzionale della moneta, cui si è già accennato. Si proporrà, dunque, una concettualizzazione della moneta che sposti l'attenzione dalla dimensione dell'uso della moneta nello scambio sinallagmatico verso la dimensione interpersonale – o meglio istituzionale – del fenomeno monetario e sulla scorta di questa proposta saranno riviste le dottrine sviluppate in ambito giuridico sulla moneta e l'attuale organizzazione della moneta nel contesto economico e normativo contemporaneo.

1.1. L'approccio funzionale: i bitcoin come mezzo di scambio, unità di conto e riserva di valore

1.1.1. *La definizione funzionale della moneta*

È comune riscontrare in opere appartenenti a diverse scienze sociali il riferimento ad una definizione funzionale della moneta, presa a prestito dalla teoria economica contemporanea. In economia si è infatti raggiunto generalmente un consenso circa il fatto che la moneta svolga essenzialmente tre funzioni[8]: (*i*) mezzo di scambio; (*ii*) unità di conto e (*iii*) riserva di valore. Definire la moneta secondo le funzioni che esegue, o dovrebbe eseguire, all'interno di un sistema economico è, però, un approccio riduttivo che nasconde una semplificazione del fenomeno oggetto di studio. La teoria economica dominante non cerca di rispondere alla domanda «cosa sia 'la moneta'», ma propone invece una sintesi delle teorie elaborate nei secoli che permetta di rispondere alla più concreta domanda «cosa sia 'moneta'» e a tale secondo interrogativo risponde che è moneta tutto ciò che è usato come moneta, cioè tutto ciò che svolge le tre funzioni sopra descritte. Tale approccio offre un utile criterio di semplificazione della realtà e permette di creare modelli di comportamento di agenti economici razionali, ma non esaurisce la complessità del fenomeno monetario[9] e, soprattutto, non spiega cosa renda possibile creare e sostenere nel tempo una moneta. Il ricorso a tale approccio nasconde, infatti, l'assunto che non si possa definire in modo universale la moneta, e che sia invece preferibile studiare le varie manifestazioni concrete del fenomeno monetario, limitandosi ad affermare, sul piano generale, le funzioni da esso svolte. L'approccio «economico-funzionale» offre, quindi, una chiave di lettura molto flessibile applicabile in vari contesti che aiuta a comprendere alcuni aspetti del fenomeno monetario, circoscrivendo ed evidenziandone le funzioni salienti sotto il profilo economico.

Per converso, l'astrattezza e la flessibilità di tale definizione non permette di evincere indicazioni sulle infrastrutture sociali, politiche e, soprattutto, giuridiche che sorreggono e regolano la moneta: l'approccio economico-funzionale è, infatti,

---

8 V., per tutti, MANKIW N.G., *Macroeconomics*, Worth Publishers, 6 ed., 2007.

9 Come si evince facilmente volgendo l'attenzione alla storia del pensiero economico e alla irriducibile diversità di opinioni che si sono manifestate circa la natura della moneta e la ragione del suo valore.

impermeabile al contesto in cui deve essere applicato, nel senso che non dipende da esso ed è anzi adattabile a qualsiasi conformazione sociale.

Il punto di partenza da cui si sviluppa l'analisi economico–funzionale è la constatazione che la moneta è utilizzata all'interno del mercato quale strumento che facilita gli scambi tra gli operatori economici[10]. La presenza della moneta all'interno della società è, quindi, data per scontata, o meglio assunta alla base del modello, mentre l'attenzione è concentrata sulle attività degli agenti economici che la moneta permette di realizzare, che sono riassunte nelle tre seguenti funzioni: (*i*) mezzo di scambio, (*ii*) unità di conto e (*iii*) riserva di valore[11].

La funzione di «*mezzo di scambio*» è comunemente ritenuta la più significativa e centrale ed è certamente la funzione più facilmente ricollegabile all'esperienza pratica comune a tutti: in qualsiasi economia di mercato, infatti, l'agente economico utilizza la moneta per cedere o acquistare beni e servizi. Si è soliti evidenziare l'importanza di questa funzione paragonando un sistema di scambi basato sul baratto e un sistema dove i partecipanti al mercato utilizzino un bene che sia accettato universalmente come mezzo di scambio. Nel primo caso i bisogni dei partecipanti potranno essere soddisfatti soltanto laddove l'agente economico trovi una controparte con bisogni simmetricamente opposti ai suoi. Nella seconda ipotesi la scissione del rapporto di scambio merce contro merce, in un duplice rapporto merce contro moneta e moneta contro merce, amplia lo spettro di possibilità di scambi permettendo la realizzazione di un maggior numero di scambi, riduce i costi informativi necessari per ciascuno scambio, valorizza la divisione del lavoro e conduce, quindi, ad una migliore efficienza allocativa nella produzione e nel consumo[12].

---

[10] In questa prospettiva è evidente il collegamento tra la teoria funzionale e la visione catallattica circa le origini della moneta, su cui *infra*, che pone al centro del modello l'uso della moneta per lo scambio di merci.

[11] Cfr. STAMMATI G., *Moneta*, in *Enc. del Dir.*, Giuffré, XXVI, 1976, p. 747, secondo cui è ravvisabile pure una quarta funzione di "*strumento per i pagamenti differiti*".

[12] È appena il caso di sottolineare che tale confronto non ha alcuna pretesa storica né deve essere letto in termini normativi quale giudizio di valore sulla superiorità di un sistema di scambio basato sulla moneta rispetto ad altri modelli di organizzazione sociale in cui alcuni rapporti prevedono l'uso del baratto. Sono esistite società organizzate secondo meccanismi diversi dal mercato in cui le iterazioni sociali sono dominate da logiche diverse dallo scambio e in cui la moneta non trova motivo di esistere: l'eventuale confronto tra queste e il modello occidentale capitalista richiederebbe, evidentemente, di sviluppare anche altri temi, diversi dall'efficienza dello scambio. Ciò che invece si evidenzia con

La seconda funzione è parimenti riconducibile all'esperienza concreta dell'economia di mercato e consiste nella capacità della moneta di offrire una misura del valore dei beni prodotti e offerti nel mercato. Proprio perché bene utilizzato universalmente nel mercato quale mezzo di scambio per qualsiasi altro bene, la moneta permette di misurare il valore degli altri beni con un'unica misura: permette di dare un prezzo alle cose. La moneta è quindi anche "*unità di conto*" del valore dei beni scambiati in un mercato.

La realizzazione del duplice passaggio sopra descritto, merce-moneta e moneta-merce perderebbe di qualsiasi significato se la moneta non potesse acquisire e conservare nel tempo un determinato potere d'acquisto. Perché essa funzioni come lubrificante degli scambi all'interno della società occorre cioè che essa sia in grado di acquisire e mantenere un determinato valore economico nel tempo e nello spazio. A ciò si aggiunge, qui solo con un accenno, che l'incertezza del futuro spinge l'agente economico a trattenere una certa quantità di risorse a riserva: stante l'universale accettabilità della moneta una parte di queste riserve sarà detenuta in moneta. Anche sotto questo profilo, quindi, occorre che la moneta adempia alla terza funzione: essere «*riserva di valore*».

1.1.2. *L'applicazione del modello astratto delle funzioni monetarie ai bitcoin*

La definizione delle funzioni astrattamente svolte dalla moneta in un'economia di mercato ha condotto taluni ad immaginare di poter rispondere alla questione della definizione dei bitcoin ed in particolare alla questione se i bitcoin siano una moneta, sulla base di tali funzioni. Così, nel contesto della giovane letteratura giuridica prodotta in tema di bitcoin, è comune il riferimento a tali funzioni come criterio per sancire se i bitcoin debbano essere considerati moneta oppure no. Il ragionamento svolto è il seguente: posto che la moneta svolge determinate funzioni all'interno di un sistema economico, se i bitcoin svolgono tali funzioni allora i bitcoin sono una moneta. Sulla scorta di questa impostazione i contributi svolgono dunque un'analisi delle *performance* dei bitcoin in ciascuna di queste tre funzioni, giungendo, nella maggior parte dei casi, a ritenere che i

questo esempio è che la moneta svolge un ruolo di intermediazione degli scambi che permette l'esistenza di un modello sociale basato sulla divisione del lavoro, la produzione di surplus e lo scambio economicamente razionale tra consociati.

bitcoin non possano essere considerati moneta[13]. Frequentemente si riconosce ai bitcoin la capacità di svolgere la funzione di mezzo di scambio, mentre si ritiene che i "test" relativi alla funzione di unità di conto e di riserva di valore non siano soddisfatti sostanzialmente in ragione dell'instabilità di valore, la quale induce gli operatori del mercato a definire i prezzi in unità di conto diverse (euro o dollari).

In questa sede si ritiene di non aderire a tale schema di ragionamento. Limitare il fenomeno monetario all'esercizio delle funzioni evidenziate dalla teoria economica non permette di coglierne con sufficiente ampiezza la complessità e induce ad affrettate conclusioni troppo approssimative ed arbitrarie.

Il problema che si rileva con questo approccio è, come è già stato anticipato, che l'analisi economico–funzionale descrive cosa la moneta fa all'interno di un'economia di mercato, non cosa la moneta sia. Se ne deduce che più uno strumento riesce a svolgere efficacemente tali funzioni, più esso può essere considerato "moneta". Il problema che si pone, però, riguarda le conclusioni che si debbono trarre di fronte a uno strumento che adempia solo in parte o in maniera imperfetta a tali funzioni: deve essere considerato come una moneta non efficiente o incompleta, ovvero se ne deve trarre la conclusione che non sia una moneta *tout court*? Ebbene la definizione funzionale non permette di tracciare una linea di distinzione chiara: a seconda dei criteri che di volta in volta si adottano per verificare l'esercizio delle suddette funzioni la risposta varierà[14]. Se ne deduce, che tale definizione di moneta mal si presta ad essere utilizzata per discernere cosa sia moneta da cosa non sia moneta, e quindi mal si presta ad essere applicata per definire la natura di questo nuovo fenomeno digitale. Al più, l'analisi circa l'esercizio delle tre funzioni può essere utile per capire se una moneta è una buona moneta o se è una cattiva moneta.

---

13 V. GASPARRI, op. cit., p. 415; LEMME e PELUSO, op. cit., p. 43; KANCS D'A., CIAIAN P. e RAJCANIOVA M., *The Digital Agenda of Virtual Currencies: Can BitCoin Become a Global Currency?*, European Commission Joint Research Centre - Institute for Prospective Technological Studies, Publications of the European Union, 2015 (Report EUR 27397 EN); LEE D.K.C. (a cura di), *Handbook of digital currency*. *Bitcoin, innovation, financial instruments and big data*, Elsevier, 2015.

14 Cfr. invece PROCTOR C., *Mann on the Legal Aspect of Money*, Oxford University Press, 7 ed., 2012, pp. 32-36, il quale prova a definire in modo puntuale le tre funzioni.

Un esempio può chiarire quanto si sta evidenziando: il valore dei bitcoin espresso in termini di valute tradizionali è molto volatile, con una tendenza di medio–lungo periodo al rialzo. Possiamo dedurre dalla volatilità del valore dei bitcoin che essi non svolgono la funzione di unità di conto o di riserva di valore? Certamente la volatilità del valore comporta un elevato rischio di cambio e in un'economia in cui più monete sono utilizzate simultaneamente ciò si traduce nell'uso di listini dinamici ancorati al valore della moneta più stabile: i prezzi saranno quindi espressi sia in euro (o dollari), sia in bitocin, e il valore del prezzo in bitcoin sarà continuamente aggiornato secondo il tasso di conversione. Questo implica che i bitcoin non siano un'unità di conto? Secondo alcuni economisti sì: essi assumono che la stabilità del valore sia un criterio determinante per verificare l'esercizio delle funzioni di unità di conto e a fronte dell'instabilità del valore dei bitcoin deducono che essi non possono ancora essere considerati una moneta a tutti gli effetti. Secondo un altro approccio potrebbe dirsi che essendoci contratti denominati in bitcoin deve ritenersi che i bitcoin siano usati come unità di conto e che l'alta variabilità del loro valore implica soltanto che essi non siano una buona moneta. In particolare, è sufficiente vi sia un mercato in cui i beni sono espressi in bitcoin – si pensi, ad esempio, al mercato della droga nel *dark web* – ovvero occorre che tutti i beni scambiati in una certa società siano espressi in bitcoin per poter concludere che i bitcoin svolgono la funzione di unità di conto?

Lo stesso può dirsi circa la funzione di riserva di valore: il valore dei bitcoin rispetto alle altre valute è aumentato significativamente nel corso del tempo, ma essendo soggetto a forti oscillazioni a seconda del periodo di tempo considerato dall'analisi possono emergere oscillazioni positive, così come negative. Se per la funzione di "riserva di valore" si considera la capacità della moneta di conservare lo stesso valore nel tempo, allora si deve concludere che il bitcoin non sia una riserva di valore. Se, invece, per riserva di valore si intende che la moneta non perda valore rispetto ad altri beni o altre monete, allora i bitcoin sembrano rispondere a questo requisito. Da ultimo, se si crede invece che per soddisfare il criterio della riserva di valore occorra che esistano meccanismi di salvaguardia tali per cui sia sempre possibile convertire la moneta in beni o in altra moneta, se non nel contesto del mercato, quantomeno per effetto della legge, allora

nuovamente occorre concludere che i bitcoin non sono moneta: il loro valore dipende, infatti, esclusivamente dal mercato[15].

Con questi esempi si vuole sottolineare che il ricorso all'approccio funzionale nasconde un enorme rischio di arbitrarietà e di opacità: a seconda dei criteri che si adottano per valutare l'esercizio o il mancato esercizio delle tre funzioni si può giungere, infatti, a conclusioni diametralmente opposte[16]. La scelta di tali criteri dipende, anche, dalla concezione di moneta che si assume implicitamente quale punto di partenza del discorso, che laddove non sia esplicitata rischia di rimanere un crittotipo di cui non ci si rende conto[17]. Il rischio che si corre nel definire la moneta solo sulla base di queste tre funzioni e nel provare a rispondere alla questione se i bitcoin siano moneta sulla base di queste funzioni è, quindi, di mascherare i veri criteri applicati nell'analisi come semplici o ovvie esternazioni delle tre funzioni e ricorrere così ad una o ad un'altra concezione della moneta senza nemmeno rendersene conto. Le tre funzioni saranno, dunque, richiamate quali utili punti di riferimento per l'elaborazione di una sintesi della moneta, che proverà, però, a descrivere come funziona e cosa sostiene la moneta: cosa permette l'esercizio di queste tre funzioni.

Quali sono, allora, le teorie che provano a cogliere l'essenza della moneta e a definire il fenomeno monetario in modo più puntuale? Le scienze sociali che si occupano della questione, economia, sociologia, antropologia e diritto, hanno sviluppato approcci diversi e definizioni diverse tra loro: persino all'interno delle scienze economiche si riscontrano scuole di pensiero opposte[18]. Ve n'è una, però, che risulta essere la visione

---

15 V. *supra* n. 12 e Cfr. KRAWISZ D., *Bitcoin as a Store of Value, Unit of Account, and Medium of Exchange*, 12 gennaio 2015, pubblicato on line e disponibile sul sito: http://nakamotoinstitute.org/mempool/bitcoin-as-a-store-of-value-unit-of-account-and-medium-of-exchange/ (ultima visita 20 giugno 2017); e Ib., *Bitcoin is the Best Unit of Account*, 10 maggio 2014, pubblicato on line e disponibile sul sito http://nakamotoinstitute.org/mempool/bitcoin-is-the-best-unit-of-account/ (ultima visita 20 giugno 2017).

16 Cfr. INGHAM, *The Nature of Money*, cit., p. 5.

17 Cfr. PROCTOR, op. cit., p. 15, il quale qualifica espressamente l'approccio funzionale aggiungendovi il requisito della copertura legale da parte dello stato: "*With these considerations in mind, it becomes attractive to adopt a functional approach—money is that which serves as a means of exchange—subject to the crucial proviso that its functions must have the formal and mandatory backing of the domestic legal system in the State or area in which it circulates*", ma v. anche *ibidem*, pp. 32-36.

18 Cfr. GOODHART C., *The Two Concepts of Money: Implications for Optimal Currency Areas*, in *European Journal of political economy*, 14, 1998, 407-432.

dominante in ambito economico e che viene pertanto assunta implicitamente a modello anche in altri contesti[19]: essa riflette l'ortodossia economica e descrive la moneta essenzialmente come il bene utilizzato universalmente come intermediario degli scambi, che come gli altri beni è a sua volta oggetto di una domanda ed un'offerta che ne determinano il valore.

A questa dottrina dominante si contrappone un insieme di teorie "eterodosse" che riconducono la nozione di moneta entro una dimensione di tipo istituzionale. La più importante articolazione di questo diverso approccio al fenomeno monetario è la teoria statalista, secondo cui la moneta è essenzialmente espressione del potere sovrano e da esso riceve direttamente la sua legittimazione.

Queste due opposte visioni si riflettono in due diverse spiegazioni di come la moneta sia originariamente creata all'interno di una società: la prima è la visione catallattica, o mengeriana, secondo cui la moneta ha origine dall'acuirsi degli scambi e dal ricorso ad un unico mezzo di scambio universale; la seconda è la teoria cartalista, che assume invece che la moneta origini dall'atto di un sovrano che nell'esercizio della sua sovranità (monetaria) impone un certo strumento per il pagamento delle tasse e per l'esecuzione degli scambi. Tra le visioni "eterodosse" circa la natura della moneta sono incluse anche la teoria societaria della moneta, secondo cui il valore della moneta dipende dal riconoscimento sociale che essa riceve nel contesto in cui è usata, e la teoria istituzionalista, che prova a conciliare la teoria statalista, tradizionalmente predominante in ambito giuridico, con il fatto che nell'economia moderna la maggior parte degli scambi sia conclusa attraverso la circolazione di crediti bancari.

Ciascuna di queste teorie si è sviluppata nel tempo in dialogo con le realtà concrete del contesto storico, in parte per rispondere al desiderio di comprendere e definire questo istituto così centrale al vivere sociale e pertanto così complesso e sfaccettato, in parte per rispondere ad esigenze e problemi concreti ed in particolare allo scollamento tra le teorie monetarie esistenti e quanto accadeva nella società in quel dato momento storico. Qui non si avrà modo di esplorare nel dettaglio ciascuna di queste teorie e le relative implicazioni: il lavoro sarebbe enorme e sproporzionato rispetto all'esigenza di elaborare un quadro

[19] Sulla predominanza di questa visione della moneta in economia e nelle altre scienze sociali v. *ibidem*, p. 408

concettuale rispetto al quale confrontare l'esperienza dei bitcoin. Si proverà quindi a offrire in primo luogo una panoramica delle varie teorie e, in secondo luogo, si proverà ad offrire una sintesi dei vari contributi, funzionale alle esigenze di comprensione e commento dei bitcoin. Tale sintesi sarà espressa nei termini del passaggio dallo studio della moneta, parola che implicitamente nel comune sentire richiama il bene fisico utilizzato come mezzo di scambio, alla considerazione del fenomeno nei termini di sistema monetario. Le conclusioni cui si giungerà non sono così distanti rispetto agli ultimi contributi che la dottrina ha offerto nel tentativo di svolgere una sintesi tra teoria statalista e societaria, secondo cui la moneta è descritta come un accordo tra sovrano e cittadini imposto dallo stato e sorretto dall'uso da parte dei consociati[20]. A differenza di tali descrizioni, però, nel corso dello sviluppo del capitolo si proverà ad evidenziare la dinamica di accordo sociale sottesa alla moneta senza dare per scontata la centralità dello Stato, il cui ruolo sarà invece ripreso ed analizzato al termine del capitolo.

1.2. La visione dell'ortodossia economica

Il focus della teoria economica ortodossa è che la moneta è essenzialmente un mezzo di scambio[21]. Tale principio viene declinato in tre accezioni non sempre accuratamente distinte, secondo cui la moneta (in quanto essenzialmente mezzo di scambio) può essere alternativamente un bene (per esempio l'oro o un'altra moneta preziosa), un simbolo diretto di un tale bene (una banconote convertibile) ovvero la rappresentazione simbolica (*numéraire*) di un bene standard o di un paniere di beni assunto come standard di riferimento[22].

Sempre secondo l'approccio dell'ortodossia economica, dunque, la funzione di mezzo di scambio è la funzione principale della moneta e da essa derivano la funzione di unità di conto e di riserva di valore. Tale rapporto di consequenzialità è ben rappresentato

---

[20] INZITARI B., *Obbligazioni Pecuniarie*, in *Commentario al Codice Civile Scialoja-Branca*, Zanichelli, 2011; DI MAJO A., Obbligazioni pecuniarie, in Enc. Dir., XXIX, Giuffré, 1979, (226); DI MAJO A., *Le obbligazioni pecuniarie*, Giappichelli, 1996.

[21] I due saggi di riferimento del pensiero della scuola economica ortodossa possono essere considerati: VON MISES L., *The Theory of Money and Credit*, Jonathan Cape, 1912; MENGER C., *Principles of Economics*, Ludwig von Mises Institute, 2007 (prima ed. 1871).

[22] INGHAM, *The Nature of Money*, cit., p. 6.

nella ricostruzione catallattica delle origini della moneta, una tesi già parzialmente anticipata da Aristotele e successivamente sviluppata nel tempo sino alla formalizzazione di Menger, il quale integrerà il discorso con riferimenti alla teoria delle scelte razionali, che ancora oggi è posta alla base delle spiegazioni neoclassiche della moneta[23].

Origini della moneta: la teoria Catallattica

Secondo questa scuola di pensiero, la nascita della moneta deve essere ricondotta all'esigenza di superare i limiti intrinseci imposti dai costi transattivi presenti in un sistema di scambi basato sul baratto. La teoria assume che in origine gli scambi siano realizzati, in assenza di alternative, mediante il baratto, che presenta però il problema della necessaria coincidenza di opposti interessi. Per ovviare a questo problema ed ampliare la rete di scambi, gli uomini iniziano ad utilizzare alcune merci che sono gradite a molti come strumento di intermediazione degli scambi. Tra queste, certi metalli si dimostrano particolarmente efficienti in ragione di alcune loro caratteristiche (duttilità, divisibilità, scarsità e resistenza nel tempo) e via via vengono quindi utilizzati da sempre più persone sino a diventare il mezzo di scambio universalmente accettato all'interno di un mercato, dando origine alla moneta[24]. Secondo questo approccio, quindi, la moneta nasce per effetto dell'uso reiterato nel tempo di una particolare merce come strumento di scambio: da qui la definizione di «catallattica», dal verbo greco καταλλάττειν, 'scambiare', attribuita alla teoria da Von Mises[25].

---

23 GOODHART, op. cit., p. 410.

24 A questa teoria si rifà il *refression theorem* di L. von Mises, secondo il quale il valore della moneta può essere rapportato indietro nel tempo sino al valore d'uso del bene che per primo ha iniziato a svolgere la funzione di mezzo di scambio universale.

25 V. GIANNINI C., *L'età delle banche centrali: forme e governo della moneta fiduciaria in una prospettiva istituzionalista*, Il Mulino, 2004, p. 48, il quale subito ricorda, però, che lo stesso Aristotele affronta la questione della nascita della moneta anche con un approccio "cartalista": sul punto v. *infra*.

La moneta come mezzo di scambio universale

Nella visione *de qua*, la moneta è, quindi, ricollegata all'espressione della naturale propensione dell'uomo verso lo scambio[26] ed è definita e concettualizzata come il mezzo di scambio universale o, più precisamente, come la merce universale scambiabile con ogni altro bene presente sul mercato[27]

A tale definizione consegue, in primo luogo, che la moneta stessa sia, almeno in origine[28], concettualizzata come una merce il cui valore dipende dai suoi specifici attributi, in particolare dalle caratteristiche e dalla quantità dei metalli preziosi usati come mezzo di scambio, secondo quanto sostenuto dalle teorie metalliste, per le quali il vero valore della moneta corrisponde al suo valore intrinseco. Inoltre, per quanto la moneta assuma una funzione speciale in quanto merce universale di scambio, ciò non esclude l'applicazione delle leggi economiche della domanda e dell'offerta, da cui si evince che, affinché una moneta abbia valore occorre che sia scarsa e che, al contrario, una produzione eccessiva di moneta causa la perdita di valore della stessa, cioè l'inflazione, secondo quanto ipotizzato dalle teorie quantitative della moneta.

---

[26] Cfr. sul punto i richiami (in senso critico) a Locke in DESAN C., *Money as a legal institution*, in Fox. D. e Enrst W. (a cura di), *Money in the Western Legal Tradition*, Ofxord University Press, 2016, pp. 19-20.

[27] Il richiamo ai metalli preziosi e al rapporto tra moneta e merci non implica, come illustra in modo chiaro e conciso Wray, che l'ortodossia economica predichi il ritorno all'uso di mezzi di scambio fisici, ma piuttosto illustra la chiave di lettura attraverso cui la moneta è concepita; v. WRAY L. R., *From the State Theory of Money to Modern Money Theory: An Alternative to Economic Orthodoxy*, Levy Economics Institute Working Paper n. 792, 2014, p. 2: "*The first* [la visione ortodossa della moneta] *focuses on money as a medium of exchange, which in the past derived its value through a link to precious metal. This is not meant to imply orthodoxy excludes the other functions of money, or to claim that modern orthodox economists would want to return to a gold standard. Rather, the* focus on money's metallic origins as a cost-minimizing medium of exchange *frames thinking about the nature of money"* (enfasi aggiunta).

[28] Secondo Carl Menger la moneta nasce come istituzione sociale, ma con il sopravvento dello Stato ha cessato di esistere secondo tale forma, v. MENGER C., *On the Origin of Money*, in *The Economic Journal*, 2, 1892, pp. 239-255; e GIANNINI, op. cit., p. 69.

In secondo luogo, da tale definizione si deduce che il carattere che distingue la moneta da ogni altra merce è il fatto che essa sia accettata da tutti, sicché l'essenza della moneta è essenzialmente equiparabile al concetto di liquidità[29].

Alla definizione di moneta come mezzo di scambio universale consegue, inoltre, che la moneta è utilizzata non per il suo valore d'uso, ma per la capacità di procurare altri beni, con l'effetto che lo schema tipico dello scambio monetario può essere allora concettualizzato nei termini di un duplice passaggio bene contro moneta e moneta contro (altro) bene, o secondo la sintesi di Marx, come uno scambio «merce–denaro–merce».

Dalla strumentalità della moneta rispetto alla soddisfazione dei bisogni degli agenti economici è dedotta, infine, la sua neutralità rispetto ai valori che concernono la produzione e il consumo di beni reali, cioè rispetto all'economia reale, ai rapporti tra merci e tra merci e agenti[30].

Elementi importanti della teoria

La teoria economica ortodossa offre il quadro di riferimento con cui qualsiasi discorso relativo alla natura o alle funzioni della moneta deve confrontarsi. Nel contesto dei bitcoin essa è molto rilevante perché essa descrive l'ideal tipo di moneta assunto, più o meno esplicitamente, come modello per la realizzazione dei bitcoin: un bene scarso, facilmente trasferibile, che i consociati possono utilizzare per intermediare gli scambi. A

---

29 Nei termini di MENGER (*op. ult.* cit.), la «*saleableness*» o «*Absatzfähigkeit*», su cui v. *infra*. Sulla nozione di liquidità, anche, v. *infra*.

30 V. SCHUMPETER J., *A history of economic analysis*, Routledge, 1994, p. 277 (citato in INGHAM, *The Nature of Money*, cit., p. 17): "*Real analysis proceeds from the principle that all the essential phenomena of economic life are capable of being described in terms of goods and services, of decisions about them, and of relations between them. Money enters the picture only in the modest role of a technical device that has been adopted in order to facilitate transactions ... so long as it functions normally, it does not affect the economic process, which behaves in the same way as it would in a barter economy: this is essentially what the concept of Neutral Money implies. Thus, money has been called a 'garb' or 'veil' of the things that really matter ... Not only can it be discarded whenever we are analyzing the fundamental . features of the economic process but it must be discarded just as a veil must be drawn aside if we are to see the face behind it. Accordingly, money prices must give way to the exchange ratios between the commodities that are the really important thing 'behind' money prices*". Sulla nozione di moneta come velo neutral v. PIGOU, A.C., *The veil of Money*, Macmillan, 1949. Proprio in ragione della neutralità attribuita dagli economisti classici alla moneta, la teoria dell'equilibrio generale walrasiano sostanzialmente ignora il fenomeno monetario.

differenza del modello ortodosso tradizionale, i bitcoin però non nascono come un bene che ha valore d'uso che via via acquista valore come mezzo di scambio[31] e sono invece supportati sin dal principio da un apparato istituzionale iscritto nel software che ne regola la creazione e il trasferimento, sul quale la teoria economica ortodossa ha ben poco da dire, posto che essa considera in maniera molto marginale il contesto istituzionale in cui è creata e riprodotta la moneta, a favore di un approccio atomistico che si concentra sulle funzioni esercitate dalla moneta nel singolo scambio (o meglio nella sequenza di scambi merce–moneta–merce).

Di questa teoria si riprenderà l'importanza della nozione di liquidità e dello scambio, anche sotto il profilo della determinazione del valore della moneta (concetto sviluppato in parte anche dalla teoria societaria della moneta, su cui *infra*).

1.3. La visione eterodossa: la teoria Statalista (o Cartalista) della moneta

In contrapposizione a quanto sopra esposto, secondo la visione eterodossa, la funzione principale della moneta è essere unità di conto[32]. Tale approccio è generalmente associata all'idea che la moneta, nella sua essenza è sostanzialmente un credito nei confronti della società, sicché mentre secondo l'approccio ortodosso la moneta è sostanzialmente una *commodity*, nella visione eterodossa essa incorpora sostanzialmente una pretesa futura ('*claim*')[33].

Secondo questa scuola di pensiero la presenza di un'unità astratta di misura del valore dei beni è logicamente anteriore alle altre funzioni della moneta ed anzi è proprio l'elemento dell'astrazione di un'unità di conto che garantisce i vantaggi connessi all'uso

---

31 Cfr. GRAF K.S., *On The Origins Of Bitcoin. Stages Of Monetary Evolution*, 3 novembre 2013, disponibile online all'indirizzo https://konrad-graf.squarespace.com/s/On-the-Origins-of-Bitcoin-Graf-031113.pdf (ultima visita 20 giugno 2017); DAVIDSON L. e BLOCK W.E., *Bitcoin, the Regression theorem, and the emergence of a new medium of exchange*, in *The Quarterly Journal of Austrian Economics*, n. 3, 2015, p. 18; XC, *Bitcoin does NOT violate Mises' Regression Theorem*, post pubblicato il 27 luglio 2010, 02:09:27 AM, sul sito https://bitcointalk.org/index.php?topic=583.0 (ultima visita 20 giugno 2017) e SATOSHI NAKAMOTO, *Re: Bitcoin does NOT violate Mises' Regression Theorem*, commento pubblicato il 27 Agosto *2010, 05:32:07 PM*, *ivi*.

32 INGHAM, *The Nature of Money*, cit., p. 6 e pp. 38 ss. Sulle posizioni della scuola cartalista v WRAY, *From the State Theory of Money*, cit., e GOODHART, *op. cit.*.

33 Cfr. MITCHELL INNES A., *What Is Money?*, in *Banking Law Journal*, 1913, 30(5), 377–408; e ID., *The Credit Theory of Money* in *Banking Law Journal*, 1914, 31(2), 151–168.

della moneta come mezzo di scambio e tale astrazione già permette la conclusione di contratti di debito e credito, di per sé sufficienti per la realizzazione di scambi multilaterali su larga scala[34]. In altre parole, secondo la scuola eterodossa l'unità di conto precede il mercato, non ne è una diretta conseguenza[35].

L'origine della moneta, dunque, non deve essere ricercata nell'innata propensione ad appropriarsi e a scambiare beni, quanto nel rapporto tra la sovranità politica e l'autorità fiscale, da un lato, e la creazione della moneta, la zecca e la banca centrale, dall'altro[36]. Il punto centrale della critica eterodossa è che la moneta si afferma come misura comune a tutti i consociati del valore grazie all'intervento del Sovrano che impone con l'esercizio della propria sovranità le regole secondo cui le tasse devono essere pagate con un certo bene che ha il potere di liberare *ex lege* dalle obbligazioni private. Così, per la teoria statale, la "*moneta è semplicemente ciò che lo Stato, in qualsiasi momento, dichiara avere il potere legale di liberare dai debiti pecuniari*"[37].

Anche questa teoria, paradossalmente, può essere ricondotta indietro nel tempo sino ad Aristotele[38], ma la sua origine si fa coincidere generalmente agli studi di Knapp, il quale per primo ne offre una formulazione articolata esplicitamente antitetica alla

---

34 INGHAM, *The Nature of Money*, cit., p. 6.

35 Sulle origini della moneta nella prospettiva cartalista v. il recente lavoro di DESAN C., *Making Money: Coin, Currency, and the Coming of Capitalism*, Oxford University Press, 2014, nel quale si cerca di fare emergere, attraverso un articolato studio di storia della moneta, la dimensione istituzionale e politica della moneta in contrapposizione alla visione economica ortodossa di strumento 'naturale' e 'neutrale'.

36 GOODHART, op. cit., p. 409.

37 KEYNES J.M., *La riforma monetaria*, Feltrinelli, 1975, p. 14. Cfr. anche US Uniformal Commercial Code, dove 'money' è definite come "*a medium of exchange authorised or adopted by a domestic or foreign government as part of its currency*". Sulla distinzione tra denaro e valuta v. *infra*.

38 In *Etica Nicomachea* Aristotele afferma che il nome greco della moneta νόμισμα (*nomisma*) derivi dalla parola νόμος (*nomos*), legge, e ciò è dovuto al fatto che essa non esiste in natura, ma solo per effetto di una convenzione o per legge; v. GIANNINI, op. cit., p. 49. Aristotele colloca questa discussione nel contesto della discussione sulla giustizia (Libro V, sezione V), e descrive la moneta in questi termini per sottolinearne la capacità di introdurre ordine all'interno del caos delle relazioni umane (v. DESAN C., *Making Money*, *cit*., p. 217). Schumpeter (*History of economic analysis*, Oxford University Press, 1954, vol. I, p. 63; trad. it. *Storia dell'analisi economica*, Torino, Boringhieri, 1960, vol I, p. 79), è critico circa questa lettura dell'autore greco e nega vi sia una contraddizione tra i due diversi brani di Aristotele affermando che la visione dominante nel pensiero del filosofo è quella secondo cui la moneta è innanzitutto una merce. V. *contra*, CRAWFORD M.H., *La moneta in Grecia e a Roma*, Roma–Bari, Laterza, 1982, pp. 12–14 (citato in GIANNINI, op. cit., p. 49, nota 5).

tradizione metallista[39]. Il giurista tedesco elabora la teoria statale (o cartalista) della moneta in antitesi alla teoria catallattica, che egli trova del tutto irragionevole. Per Knapp non è possibile concepire una teoria della moneta che non prenda in considerazione il ruolo dello Stato: per il tedesco la moneta è, infatti, essenzialmente uno strumento con cui si registrano e si misurano i debiti e i crediti e attraverso il quale possono essere adempiute le obbligazioni pecuniarie, la più importante delle quali è il pagamento delle tasse[40]. Al centro della teoria vi è, quindi, la nozione secondo cui la moneta è l'unità di conto in cui sono espressi i debiti pecuniari (*unit of account*) e che lo Stato provvede ad attribuire *ex lege* ad alcuni beni la capacità di liberare dalle obbligazioni pecuniarie grazie alla rappresentazione simbolica-giuridica dell'unità di conto in un mezzo di pagamento, definita come "*movable thing which has the legal property of being the bearer of units of value*"[41]. Il valore della moneta non dipende, quindi, dal valore intrinseco dei metalli impiegati nello scambio – come sostenuto dai metallisti –, ma dalla accettazione da parte dello Stato di tali strumenti per il pagamento delle tasse. Per Knapp, dunque, l'importanza della moneta dipende dalla creazione di un'unità nominale astratta cui lo Stato conferisce concretezza attribuendo ad alcuni beni un particolare valore simbolico: alla base la moneta è dunque un misuratore, non un bene misurato[42]. La dimensione di *abstract value* implicita nella teoria è però mitigata, in origine, dal fatto che l'obbligazione pecuniaria è comunque ancora iscritta in una logica di corporeità che ne permette l'assimilazione all'obbligazione di dare cose generiche[43]: l'elemento cruciale della teoria statalista di Knapp è che l'identificazione di tali cose e il valore che ad esse è riconosciuto dipendono direttamente dall'esercizio della sovranità monetaria dello Stato.

---

39 KNAPP G.F., *The State Theory of Money*, Macmillan & Company Limited, 1924.

40 Knapp elabora altresì un'interpretazione storica dell'evoluzione della moneta secondo diverse fasi (per una sintesi v. INZITARI, op. cit., p. 6). Secondo l'autore tedesco, il mezzo di pagamento si presenta in origine come «pesatore», cioè uno strumento il cui valore dipende dal peso (cioè dalla quantità di metallo prezioso), prima senza essere dotato di una particolare forma (nel lessico di Knapp: «amorfo»), poi come moneta coniata («morfica»), che però viene sempre pesata all'atto del pagamento. A queste modalità segue una modalità detta ortopica, di circolazione di moneta cartacea convertibile. Si noti che le teorie di Knapp sono elaborate in un contesto in cui il confronto riguardava le posizioni dei metallisti e i nominalisti, v. KNAPP, op. cit., p. 8.

41 *Ibidem*, p. 7.

42 INGHAM, *The Nature of Money*, cit., p. 48.

43 INZITARI, op. cit., p. 6.

Il pregio di questa teoria è quindi di evidenziare l'importanza del principio nominalista e del corso forzoso, e di riuscire a spiegare le ragioni per cui i biglietti emessi dalle banche, private o pubbliche, possano diventare a tutti gli effetti moneta, in termini giuridici, qualora lo Stato inizi ad accettarli come mezzo di pagamento delle tasse. Una volta affermato il principio secondo cui la moneta è sostanzialmente un valore astratto cui lo Stato conferisce concretezza attraverso l'esercizio della propria sovranità si apre, cioè, la strada alla possibilità di creare moneta oltre i limiti delle disponibilità delle riserve di metallo prezioso: in altre parole, diventa concettualmente possibile creare meccanismi di pagamento di natura astratta, tra i quali assume particolare importanza il credito tra privati. In particolare, l'idea che lo Stato possa arbitrariamente creare una certa moneta semplicemente stabilendo l'obbligo di pagare le tasse con un certo strumento emesso e fatto circolare dallo Stato stesso, comporta che si possa descrivere quel dato strumento nei termini di una relazione di credito tra lo Stato e i cittadini: la moneta può essere quindi descritta come un debito trasferibile dello Stato nei confronti dei cittadini ovvero come un credito che i cittadini vantano nei confronti dello stato e che gli stessi possono utilizzare per adempiere agli obblighi fiscali.

Lo sviluppo della teoria cartalista in ambito dell'economia e della sociologia nella direzione anzidetta ha portato alla teorizzazione della moneta come credito nei confronti della società e alla descrizione di qualsiasi relazione monetaria come una relazione che, alla base, può essere descritta in termini di debito e credito[44]. Anche in questo contesto, resta centrale la nozione di unità di conto utilizzata per definire le obbligazioni pecuniarie e il riconoscimento legale di certe specifiche modalità attraverso cui è possibile adempiere a tali obbligazioni.

Mann sintetizza quindi la teoria cartalista nei seguenti termini:

"in law, the quality of money is to be attributed to all chattels that are:

(a) issued under the authority of the law in force within the State of issue;

(b) under the terms of that law, denominated by reference to a unit of account; and

[44] V. WRAY, *From the State Theory of Money*, cit. e INGHAM, *The Nature of Money*, cit., *passim* ed in particolare p. 72 e pp. 74–75.

(c) under the terms of that law, to serve as the universal means of exchange in the State of issue'"[45].

Ai fini della presente ricerca, della teoria cartalista occorre sottolineare, innanzitutto, che essa porta lo studio della moneta verso una dimensione di analisi delle istituzioni che la regolano. In secondo luogo, è fondamentale l'apporto di tale teoria relativo alla concettualizzazione della moneta come unità di conto. Meno rilevante, almeno in un primo momento, è invece la definizione della moneta in termini di credito-debito e la riduzione della categoria dei mezzi di pagamento agli strumenti cui è riconosciuto valore direttamente dalla legge.

1.4. La teoria societaria

La teoria societaria della moneta riprende diversi principi elaborati dalla teoria statalista, in particolare la nozione di unità di conto, ma da essa si differenzia proprio in ragione di un diverso approccio al tema dell'adempimento delle obbligazioni pecuniarie e, conseguentemente, alla definizione stessa di unità di conto.

Nella teoria statale la definizione dell'unità di conto astratta e dei mezzi di pagamento da parte dello Stato sono due risvolti di un unico processo che globalmente definisce la moneta: allo stato compete quindi la definizione di cosa è moneta e del suo valore. Secondo la teoria societaria della moneta, invece, l'uso negli scambi commerciali e la fiducia della gente hanno il potere di creare o riconoscere un certo bene (o un'istituzione) come moneta ed è quindi il comportamento dei consociati l'elemento che determina l'esistenza e il valore di una moneta, non la mera affermazione autoritaria di un certo mezzo di scambio e di una particolare unità di conto da parte dello Stato[46]. Altrimenti detto, nella visione della teoria sociale, quindi, "*i singoli pezzi monetari sono dunque meri strumenti rappresentativi di una data «unità ideale» il cui valore discende, non tanto da un'imposizione dell'autorità statuale, bensì dalla considerazione che gli*

[45] PROCTOR, op. cit., p. 15.

[46] *Ibidem*, p. 17.

viene attribuita dal contesto sociale nell'ambito del quale funge da strumento monetario"[47].

Gli autori più rappresentativi di questa teoria, in ambito giuridico, sono stati Nussbaum[48] e Ascarelli[49], le cui teorie differiscono parzialmente circa la portata dell'astrazione riconosciuta all'unità di conto e alla conseguente definizione dell'obbligazione pecuniaria in termini di obbligo a mettere la controparte nella disponibilità di un certo numero di unità ideali di conto (Nussbaum) ovvero di consegna di una certa quantità di beni fungibili determinati in base al numero di unità di conto che ci si è impegnati a trasferire (Ascarelli)[50].

Nella teoria di Ascarelli, la nozione di moneta è quindi scissa in due elementi: da un lato l'unità di misura che permette di comparare il valore di cose e servizi, dall'altro lo strumento di scambio, cioè una cosa tipicamente ricevuta o promessa in cambio di cose o servizi[51]. Da questa si distingue, invece, la valuta, che corrisponde alla moneta legale dello Stato, cioè al bene al quale il sovrano fa capo come misuratore dei valori ed al quale attribuisce il valore di corso legale[52]. L'orizzonte della definizione di moneta è quindi

---

47 FARENGA L., *La moneta bancaria*, Giappichelli, 1997, p. 23.

48 V. NUSSBAUM A., *Das Geld in Theorie und Praxis des deutschen und auslandischen Rechts*, J. C. B. Mohr, 1925 (dove, a p. 6, per la prima volta si offre una definizione di moneta completamente avulsa da qualsiasi riferimento fisico-materiale; sul punto v. INZITARI, op. cit., p. 14); e NUSSBAUM A., *Money in the Law, National and International. A comparative study in the borderline of law and economics*, The Foundation Press Inc., 1950 (seconda edizione riveduta e ampliata di *Money in the Law*).

49 ASCARELLI T., *La moneta, considerazioni di diritto privato*, Cedam, 1928; ID., *Obbligazioni Pecuniarie*, in *Commentario al Codice Civile Scialoja-Branca*, Zanichelli, 1968 (ristampa della 1 ed. del 1956).

50 Per una sintesi delle teorie di Nussbaum e di Ascarelli e della critica che quest'ultimo volge al primo v. INZITARI, op. cit., p p. 14-22; DI MAJO, *Le obbligazioni pecuniarie*, cit., e FARENGA, op. cit., pp. 23 ss..

51 ASCARELLI, *Obbligazioni pecuniarie, cit*., p. 12.

52 *Ibidem*, pp. 31 ss. e 39 ss. e, in sintesi, p. 41: "*terminologicamente ricorreremo ai termini danaro o moneta per comprendere qualunque misura di valore adottata e qualunque oggetto corrente (in un determinato ambito) tipicamente come strumento di scambio; ai termini valuta e poi unità valutaria e pezzi valutari per indicare l'unità di misura monetaria legale di ogni ordinamento e i pezzi monetari aventi corso legale nel territorio corrispondente a un determinato ordinamento, unità di misura e pezzi ai quali, nell'ambito di ogni ordinamento, si farà riferimento in mancanza di diversa lecita determinazione; al termine ordinamento monetario o valutario, per indicare qualunque ordinamento giuridico determini una unità valutaria*"; nonché, *ibidem*, p. 120 e p. 131, dove l'autore chiarisce che il pagamento in denaro di un'obbligazione pecuniaria costituisce *datio in solutum*.

ampliato, nella teoria sociale, per ricomprendere tutti i beni che sono utilizzati per l'intermediazione degli scambi in una data società[53].

Il pregio di questa teoria è sottolineare l'importanza del comportamento dei consociati in ambito monetario, che sarà ripreso nel prosieguo del discorso, nonché di ricollegare l'origine della moneta all'ipotesi di una convergenza di interessi e di comportamenti conformi da parte dei consociati, senza però concludere che tale convergenza sia del tutto spontanea e guidata da meri interessi economici (come fa la teoria economica ortodossa) o che essa sia frutto dell'imposizione di un obbligo da parte del sovrano[54].

Sebbene, allora, la definizione di moneta come qualsiasi cosa utilizzata come mezzo di scambio possa apparire troppo lassa per trarne conseguenze giuridiche, l'intuizione secondo cui la moneta è sorretta non solo dalla legge, ma anche da convenzioni sociali è invece utile a meglio comprendere il fenomeno e correggere alcune rigidità della teoria statalista, generalmente considerata il punto di riferimento in materia sotto il profilo giuridico per la stretta connessione con il diritto.

Così, per esempio, la teoria di Mann, esponente importante della scuola statale, nei contributi più recenti, a fronte dell'uso sempre maggiore della moneta scritturale – la quale, forse erroneamente, era ritenuta esclusa dalla definizione di moneta secondo la teoria statalista – è stata aggiornata per includervi forme di moneta astratte utilizzate dai consociati all'interno di circuiti regolati dallo Stato[55]. Così, secondo tale teoria la moneta continua ad esistere all'interno di un *framework* legale, e sotto questo profilo la teoria statale della moneta continua a essere valida, ma la sua creazione e circolazione non

---

53 Cfr., in proposito, la critica di Ascarelli sulla eccessiva ristrettezza dell'approccio di Knapp: *Ibidem*, pp. 28–29, nota 2.

54 *Ibidem*, p. 29, nota 2: "*il problema si ricollega con quello c.d. dell'origine della moneta nella quale, pur negata la teoria statalista, si vuole d'altra parte rinvenire il frutto di una cosciente convenzione sociale, anziché un risultato spontaneo sviluppatosi naturalmente «quasi senza che si conoscesse che ella (la moneta) si usava e senza comprenderne l'utilità» come ben scriveva l'abate Galiani*".

55 V. PROCTOR, op. cit., pp. 40 ss. e cfr. *Infra* la teoria istituzionale della moneta, che sviluppa ulteriormente questo approccio sino a formulare una nuova teoria monetaria *tout court*.

dipendono solo dall'emissione fisica di beni che la rappresentano da parte o per conto dello Stato, ma è regolata altresì dagli usi della società riconosciuti dallo Stato[56].

Anche la dottrina italiana successiva all'Ascarelli, confrontandosi con il sempre maggiore utilizzo della moneta scritturale, ha elaborato ulteriormente le intuizioni dell'autorevole maestro sviluppando la nozione di moneta nei termini di una convenzione che vede coinvolti lo Stato da una parte e i cittadini dall'altra[57]:

> *"la forma giuridica del debito pecuniario di astratte unità ideali monetarie costituisce la rappresentazione, in termini di disciplina giuridica, estremamente raffinata ed evoluta, di una convenzione, creata imposta dall'autorità dello Stato resa efficace dal consenso sempre rinnovato di tutti cittadini, di oggettivare, in termini di astratte unità di conto, l'entità delle pretese che si accompagnano allo scambio e alla circolazione dei beni dei servizi. I termini della convenzione si possono, in prima approssimazione, identificare l'attribuzione o meglio nell'imposizione della qualità di mezzo di pagamento e di misura di altri valori. Il riferimento all'unità monetaria nel rapporto di credito debito rappresenta più generalizzate rilevante forma di utilizzazione e di applicazione dell'accennata convenzione al fine di regolare misurare in modo più efficace, almeno in relazione a livello fin qui realizzato della nostra civiltà nello sviluppo della circolazione produzione della ricchezza, la forma di soggezione conseguente allo scambio di beni e/o servizi"* [58].

1.5. Teoria Istituzionale della moneta

La teoria istituzionale della moneta è una teoria piuttosto recente, formulata nel saggio di Antonio Sáinz de Vicuña "*An institutional theory of money*" che ha avuto una certa eco a livello internazionale secondo cui oggi la moneta è sostanzialmente un credito

---

[56] *Ibidem*, p. 32.

[57] INZITARI, op. cit., pp. 36 ss., nonché DI MAJO, *Le obbligazioni pecuniarie*, cit., e FARENGA, op. cit., p. 31 e *passim.*

[58] INZITARI, op. cit., p. 38.

trasferibile all'interno di un framework istituzionale[59]. Tale teoria si discosta leggermente dalle teorie precedenti, pur restando nell'alveo della tradizione che riconosce allo Stato un ruolo centrale nella definizione della moneta, nella misura in cui prova specificatamente a rendere conto del sistema attuale di creazione privata della moneta attraverso un sistema bancario soggetto alle politiche monetarie della banca centrale e alla vigilanza prudenziale dell'autorità pubblica[60].

La teoria istituzionale trae origine dalla considerazione secondo cui la teoria statale e la teoria societaria furono sviluppate in un tempo in cui lo scambio delle valute nazionali era controllato e il loro valore era legato al valore dell'oro: una situazione in cui, quindi, si poteva dire legittimamente che il valore della moneta fosse fissato o determinato dallo Stato. Nel contesto attuale in cui si è affermata la libera circolazione dei capitali e il valore dei cambi oscilla liberamente, ciò non è più vero, perché il valore della moneta oggi dipende principalmente dalle politiche monetarie della banca centrale e dalle forze del mercato[61]. Da qui la necessità di sviluppare una nuova dottrina che permettesse di rendere conto al tempo stesso della centralità e dell'indipendenza del sistema bancario e del rapporto di soggezione e contestuale supporto che intercorre tra il sistema bancario e lo Stato. Il focus della teoria istituzionalista è quindi sull'inclusione della moneta scritturale nella definizione giuridica di moneta, che viene giustificata dall'esistenza di un apparato istituzionale atto a regolare e supervisionare l'emissione privata di moneta da parte delle banche.

---

59 SÁINZ DE VICUÑA A., *An institutional theory of money*, in Giovanoli M. e Devos D. (a cura di), *International monetary and financial law*, Oxford University Press, 2010, pp 517 ss.. La tesi è ripresa, per esempio, in PROCTOR, op. cit., p. 25.

60 Alla teoria statale si contesta, in particolare, che al giorno d'oggi la maggior parte degli scambi sia svolta senza il ricorso a supporti fisici e che anzi molti Stati vietano il pagamento di somme cospicue di denaro in contanti, per cui non è pare più accurato sostenere che i biglietti emessi dallo Stato siano la moneta e che il credito bancaria sia solo un sostituto di essi accettato su base volontaria (SÁINZ DE VICUÑA, op. cit., pp. 520 e 522). Mentre alla teoria sociale si contesta che l'uso della moneta scritturale sia meramente un uso sociale, in ragione dell'apparato regolamentare appositamente predisposto dallo Stato e dall'assunzione in capo allo stesso della responsabilità, attraverso l'istituzione di una banca centrale, di garantire il funzionamento dei sistemi di pagamento e l'approvvigionamento di sufficiente liquidità sul mercato.

61 SÁINZ DE VICUÑA, op. cit., pp. 518 e 520 "*the value of the euro since its launch is the result of the monetary policy of the Eurosystem. Neither the member states nor the Community may establish the value of money*". V. anche PROCTOR, op. cit., p. 25.

Proctor ne offre la seguente sintesi:

"Considerations of this kind lead to the conclusion that 'money' is defined as:

(a) a direct or indirect claim against a central bank;

(b) a claim which can be used by the public as both a means of exchange and a store of value; and

(c) a claim which is originated and managed by a central bank in a manner that preserves its availability, functionality, and purchasing power" [62].

Nel contesto di questa teoria si riconosce dunque ancora allo Stato un ruolo nella determinazione dell'unità di conto e nella creazione e supervisione di un sistema bancario soggetto al controllo di una banca centrale che risponda a certe specifiche caratteristiche e a cui è delegata, entro un certo grado di autonomia, la responsabilità della gestione delle politiche monetarie che, quindi, per converso, è sottratta al diretto esercizio da parte dello Stato[63]. La teoria altresì riconosce che la moneta non ha alcun valore intrinseco e che il valore dipende invece dalla fiducia che il mercato dimostra nei confronti della banca centrale e del sistema bancario in generale[64].

Per questo, come riportato da Proctor, "*money is defined as a direct or indirect credit claim against a central bank which can be used by the public as a general means of exchange and as a store of value, which is originated and managed by central banks in a manner that preserves its avilability, functionality, and purchasing value*"[65], e più specificatamente ancora: " *money is no more than a credit claim that creditors are ready to accept because it is generally transferable as a means of exchange […]* thanks to a legal and regulatory framework organizing*: (1) its creation in a manner that preserves over the course of time its purchasing power; (2) its availability (even in time of crisis); and (3) its functionality for daily use by all economic agents*"[66].

---

62 *Ibidem*, p. 27

63 SÁINZ DE VICUÑA, op. cit.; PROCTOR, op. cit., p. 28.

64 *Ibidem*, p. 29.

65 SAINZ DE VICUÑA, op. cit., p. 525.

66 *Ibidem*, p. 531 (corsivo aggiunto).

Il pregio di questa teoria è che essa pone in evidenza lo stretto rapporto che intercorre tra sistema bancario e Stato ed evidenzia il fatto che la produzione di moneta privata da parte delle banche sia perseguita e permessa grazie a, e per effetto di, disposizioni dello Stato sovrano che attraverso la costituzione di un particolare assetto istituzionale ha delegato a tali organismi la funzione di produzione e di distribuzione della liquidità. Tale risultato è reso possibile, a livello teorico, grazie al ricorso alla nozione di «istituzione» sviluppata nel contesto della scuola di pensiero della *institutional economics*, detta anche '*new institutionalism*', secondo la quale il concetto di istituzione include "*structures, organizations, rules and customs, shaping economic behaviour with a high degree or resilience and permanence*"[67]. Questa nozione risulta particolarmente efficace nel contesto dell'analisi del fenomeno monetario, dove occorre considerare non solo il diritto formale, ma anche gli usi sociali e incentivi economici che concorrono a determinare il comportamento degli agenti: ad essa si farà riferimento, in modo più o meno esplicito, per rapportare la nozione di moneta al mondo dei bitcoin, estraneo, per gran parte, a fenomeni di regolamentazione tradizionali.

Per contro, la teoria istituzionale della moneta risulta troppo specifica rispetto alla realtà attuale dell'organizzazione economica per poter assumere il ruolo di di "*concept of money for the start of the twenty–first century*"[68] che l'autore si prefigge di formulare: così come formulata, la teoria non reggerebbe più al solo cambiare di uno dei criteri di gestione che determinano l'operato della banca centrale (si immagini, per esempio il passaggio dall'obbiettivo dell'inflazione controllata all'obbiettivo della piena occupazione). La teoria descrive efficacemente il sistema monetario vigente nella maggior parte degli Stati del mondo, ma non è sufficientemente astratto per essere adottato come quadro di riferimento. Inoltre, il modello è scevro di qualsivoglia approccio critico allo *status quo* oggetto di descrizione e non ne evidenzia gli effetti distributivi e politici[69].

---

67 *Ibidem*, p. 524. Cfr. anche GIANNINI, op. cit., pp. 50-51 e LANGLOIS R.N., *The new institutional economics: an introductory essay*, in Langois R.N. (a cura di), *Economics as process*: *essays in the new institutional economics*, Cambridge University Press, 1990; WILLIAMSON O.E., *The new institutional economics: taking stock, looking ahead*, in *Journal of Economic Literature*, 2000, p. 599.

68 SAINZ DE VICUÑA, op. cit., p. 517.

69 Sulla dimensione politica e distributiva del modello di sistema monetario, v. *infra.*

1.6. Dalla nozione di «moneta» all'idea di «Sistema Monetario»

1.6.1. *Il singolo scambio monetario presuppone uno scambio futuro, quindi un contesto istituzionale*

Si ritorni, ora, alla differenza tra il baratto e lo scambio monetario, ed in particolare alla semplice ipotesi di uno scambio tra Tizio e Caio in cui Tizio cede a Caio una torta e Caio trasferisce a Tizio mille lire. Analizzato nella sua estemporaneità questo scambio ha ben poco senso da un punto di vista economico: mentre è facile immaginare che Caio possa trarre un'utilità dalla torta, per esempio mangiandola, a nulla servono le mille lire a Tizio se non a condizione che Tizio abbia a sua volta la possibilità di utilizzare quelle lire in un altro scambio. Preme qui sottolineare, cioè, una cosa ovvia: l'uso della moneta non può prescindere dall'esistenza di un mercato. Occorre che lo scambio di un bene contro prezzo sia inserito in un più ampio sistema di scambi. Con riferimento all'esempio concreto è intuitivo che Caio offra e Tizio accetti mille lire perché entrambi ritengono e confidano che quelle mille lire possano essere utilizzate successivamente da Tizio in occasione di altri scambi. Per comprendere l'istituto utilizzato nell'operazione di compravendita occorre dunque soffermarsi non sulle mille lire, ma sul sistema di scambi all'interno del quale l'operazione è inserita. Tale sistema di scambi è caratterizzato da una convenzione, più o meno esplicita, che disciplina l'uso delle lire quale strumento simbolico rappresentativo di un'aspettativa creditoria. Per comprendere meglio questo enunciato occorre, ora, procedere per gradi.

L'esempio svolto si differenzia dall'ipotesi del baratto perché nel caso del baratto si assume che entrambi i beni scambiati abbiano valore d'uso, mentre nel caso di specie un bene con un valore d'uso – la torta – è scambiato contro un bene che non ha un valore d'uso, bensì un valore che si è voluto definire "simbolico" – le lire –. All'interno del sistema di scambi Tizio potrà tradurre il valore simbolico iscritto nel bene ricevuto in un vantaggio concreto scambiando a sua volta il bene ricevuto – le mille lire – con un bene di consumo il cui valore d'uso soddisfi un suo bisogno, ad esempio una birra. Sino a che questa seconda operazione non sarà compiuta, Tizio conserva un'aspettativa di realizzazione futura dei propri bisogni che assomiglia ad una posizione creditoria nei

confronti della società[70]. Le mille lire ricevute da Caio rappresentano simbolicamente questa aspettativa di realizzazione futura dei propri bisogni e affinché tale aspettativa possa realizzarsi occorre, si è detto, che esista un sistema di scambi e che tale sistema di scambi perduri nel tempo sino al momento in cui Tizio cederà le mille lire. Se ne deduce, prima di proseguire con il ragionamento, che non è possibile parlare di moneta se non prendendo in considerazione, almeno implicitamente, una pluralità di rapporti iscritti all'interno di un "sistema" di relazioni.

Non è, però, sufficiente che esista un qualsiasi sistema di scambi, occorre che il sistema di scambi al quale Tizio partecipa preveda e consenta l'utilizzo di quelle mille lire ricevute da Caio e riconosca a quello strumento la capacità di essere nuovamente scambiato per un altro bene. Anche questa considerazione è, a prima vista, ovvia. Immaginiamo che Tizio abbia ricevuto le mille lire in Italia, se si sposta in Francia non potrà utilizzare le lire per comprare la birra perché in Francia utilizzano i franchi: il sistema che gestisce la rappresentazione simbolica di posizioni para-creditizie è diverso dal sistema utilizzato in Italia. Da quanto detto si deduce, tornando al piano dell'astrazione, che l'elemento indispensabile perché sussista uno scambio monetario è la vigenza di una convenzione che attribuisce alle mille lire la capacità di simboleggiare l'aspettativa di soddisfazione futura dei bisogni di Tizio[71].

Si può, ora, rendere più preciso l'enunciato con cui si era precedentemente concluso il paragrafo dicendo che l'istituto centrale all'operazione di compravendita non è la presenza di un sistema di scambi, bensì l'insieme di regole per effetto delle quali si attribuisce a determinati beni la capacità di rappresentare e, quindi, "immagazzinare" e "trasferire" ad un terzo l'aspettativa genericamente "creditoria" di cui Tizio è divenuto titolare con la vendita. Solo l'esistenza di quell'insieme di regole permette la realizzazione di un sistema di scambi "monetari" di merce contro prezzo, all'interno del quale la torta di Tizio può essere venduta in cambio delle mille lire di Caio.

---

70 V. DODD, op. cit., p. 8, ove ulteriori riferimenti a Schumpeter.

71 Cfr. la nozione di "corso fiduciario o volontario" come funzione liberatoria riconosciuta da un atto negoziale (anche stipulato per *facta concludentia*) efficace nella cerchia di determinati soggetti in ALLARA M., *Le nozioni fondamentali del diritto civile*, I (unico), 5° ed., Giappichelli, 1958, p. 318; v. CUFFARO VINCENZO (a cura di), *Delle obbligazioni*. Art. 1277-1320, *Comm. Gabrielli*, tomo 3, UTET, 2013, p. 16.

Ricapitolando quanto evidenziato sin qui, può concludersi che a differenza di quanto accade nell'ipotesi del baratto, lo scambio di tipo monetario sottende sempre un contesto istituzionale all'interno del quale esso acquista significato. La moneta è, dunque, il prodotto di un processo di ingegneria sociale ed al tempo stesso l'insieme di regole che permette l'attribuzione di valori simbolici: la moneta è, nella sua essenza più profonda, un linguaggio condiviso, una convenzione che disciplina rappresentazioni simboliche di valore economico.

Riferirsi a tutto ciò genericamente con la parola "moneta" è decisamente fuorviante perché con questo termine si intende in maniera indistinta sia l'assetto istituzionale che permette di attribuire un determinato significato ad un determinato bene, sia il bene stesso che incorpora tale valore simbolico. Lo stesso problema si presenta nel contesto dei bitcoin, dove con la stessa parola si è soliti riferirsi sia al sistema che regola la creazione e distribuzione dei bitcoin, sia ai bitcoin in quanto unità monetaria immagazzinata e trasferita tra i partecipanti al sistema. Nel caso dei bitcoin si è ritenuto di evitare equivoci utilizzando l'iniziale maiuscola o minuscola. Nel caso della moneta si vuole invece proporre l'uso della nozione di "sistema monetario" per contrapporsi a ogni rischio di semplificazione e approssimazione e per evidenziare che non è dato parlare di moneta senza fare implicito riferimento ad un sistema di regole che disciplini la "traduzione" di valori d'uso in valori simbolici. Con il termine "moneta" ci si riferirà, invece, all'estrinsecazione concreta di un rapporto simbolico disciplinato da un sistema monetario.

1.6.2. *«Sistema monetario», «convenzione monetaria» e «fiducia monetaria»*

Nei paragrafi precedenti si è proposta una rilettura della semplice dinamica di scambio di un bene contro moneta per evidenziare che l'utilizzo della moneta come mezzo di scambio è sempre logicamente preceduto dalla definizione di un quadro di riferimento e si fonda su una convenzione che disciplina il rapporto simbolico tra il quadro di riferimento astratto e l'atto concreto della dazione di quella moneta alla controparte. Se dovessimo esprimere questo concetto facendo riferimento alle funzioni economiche svolte dalla moneta potrebbe dirsi che l'uso della moneta come unità di conto precede sempre logicamente l'uso della moneta come mezzo di scambio: è necessario,

innanzitutto, che il valore economico dei beni sia espresso secondo l'unità di misura condivisa nella forma di un prezzo perché possa sussistere un pagamento del prezzo stesso mediante la dazione di pezzi monetari che rappresentano quel valore[72].

Altro elemento fondamentale che si è evidenziato, è la sussistenza di un'aspettativa, quantomeno in capo al soggetto che riceve la moneta, di poter utilizzare in futuro quella moneta in modo simile, nel contesto di un diverso rapporto di scambio. Una tale aspettativa è configurabile soltanto laddove si possa immaginare la sussistenza di un accordo più o meno esplicito tra un determinato numero di soggetti per effetto del quale essi riconoscono la validità della moneta utilizzata, cioè riconosco il valore simbolico iscritto in quella moneta.

Ogni operazione monetaria si inserisce, quindi, all'interno di un sistema monetario attraverso il quale una certa comunità condivide un sistema di misurazione del valore economico dei beni e un meccanismo di estrinsecazione di tale valore nella realtà.

A sua volta, il sistema monetario altro non è che il frutto di una convenzione, più o meno esplicita, che definisce l'unità di conto ideale e ne disciplina la rappresentazione simbolica nel mondo reale.

Perché una «convenzione monetaria» dia luce ad un «sistema monetario» occorre, che essa sia effettivamente utilizzata da parte dei consociati: occorre, cioè, che sussista quel rapporto di fiducia nella convenzione da cui scaturisce la ragionevole aspettativa in capo ai consociati di poter utilizzare in futuro il valore simbolico iscritto nella moneta ricevuta. Si chiamerà questa particolare aspettativa che l'agente economico ripone nel sistema monetario «fiducia monetaria».

Con le nozioni di sistema monetario e fiducia monetaria si completa il quadro teorico attraverso il quale si intende descrivere il fenomeno monetario, che sarà ora sviluppato con maggiore completezza e dettaglio.

---

72 Cfr. FANTACCI, *La moneta*, op. cit., pp. 18 e 37.

2. Dalla moneta al sistema monetario: sviluppo di una sintesi delle teorie sulla moneta utile allo studio dei bitcoin.

2.1. Mappatura dei concetti fondamentali e sintesi del modello

2.1.1. *L'importanza della moneta oltre i limiti angusti dello scambio*

Per elaborare il tema del rapporto tra moneta e diritto[73], occorre innanzitutto ampliare l'immaginario delle funzioni che la moneta svolge all'interno della società e l'utilità che ne deriva rispetto alla tradizionale narrazione economica della questione. Il tema è spesso trattato in termini economici con particolare attenzione alla dimensione dello scambio, sicché la definizione comunemente adottata nei libri di economia è che la moneta è "*qualsiasi cosa generalmente accettata come pagamento per beni o servizi o per il pagamento di debiti*"[74]. Di essa sono poi comunemente descritte le tre funzioni che si ritiene eserciti da un punto di vista: mezzo di scambio, unità di conto e riserva di valore, spesso sottolineando, però, la prevalenza della funzione di mezzo di scambio, che nella teoria economica ortodossa precede logicamente e per importanza le altre due[75].

---

[73] Sulla moneta v. CAPRIGLIONE F., *Moneta*, in *Enc. del Dir.*, Giuffré, Agg. III, 1999 e BOFFITO C., *Moneta*, in *Enciclopedia*, Einaudi, 1980; STAMMATI, op. cit.; ASCARELLI, *Obbligazioni pecuniarie*, *cit*.; ASCARELLI T., *La moneta*, cit.; INZITARI, op. cit.; MARCHETTA D., *La moneta*, in *Diritto amministrativo speciale*, t. 3, *I servizi pubblici finanza pubblica e privata*, in Trattato di Diritto Amministrativo, a cura di Sabino Cassese, Giuffré, 2003, pp. 3035 ss.; FERRO-LUZZI P., *Lezioni di diritto bancario*, vol. 1, *Parte Generale*, 3° ed., Giappichelli, 2012, pp. 249 ss.; SEMERARO M., *Pagamento e forme di circolazione della moneta*, Edizioni Scientifiche Italiane, 2008.

[74] MISHKIN F.S., GIULIODORI M. e MATTHEWS K., *The Economics of Money, Banking, and Financial markets (European Edition)*, Pearson Education Limited, 7 ed., 2013, p. 46: "*Economists define money (also referred to as the money supply) as anything that is generally accepted in payment for goods or services or in the repayment of debts*".

[75] In questo senso anche STAMMATI, op. cit., p. 747, secondo il quale la funzione principale che definisce la moneta è quella di intermediazione degli scambi, mentre la funzione di misurazione dei prezzi deriva da questa e ad essa non sempre è collegata. Sostiene, infatti, l'a. che tale seconda funzione può essere assolta da uno strumento diverso [sic!] che non circoli sul mercato. "questo «strumento» viene detto allora «unità di conto»". Si vedrà a breve come tale scissione tra la nozione di moneta e l'unità di conto sia frutto di un approccio errato alla questione monetaria, basato sua una visione atomistica dello scambio e sulla forzata assimilazione tra moneta e merce, che non permette di cogliere l'aspetto istituzionale di questo fenomeno e la sua rilevanza sistemica.

La definizione di moneta come qualsiasi cosa accettata in pagamento di beni e servizi è stata ripresa nell'ambito delle dottrine giuridiche dalla teoria societaria della moneta. In questo contesto si ha interesse, però, ad evidenziare che la moneta assolve dei compiti di grande rilevanza pubblica e di interesse giuridico all'interno della società oltre a quello di facilitare gli scambi economici di tipo sinallagmatico, e partendo da questa considerazione si vuole mostrare che la moneta è molto più di un mezzo di scambio: essa corrisponde, piuttosto, ad un complesso assetto istituzionale, rispetto al quale il diritto gioca un ruolo molto importante.

Si proverà ad adottare uno sguardo più ampio, attento ad evidenziare il ruolo dello Stato o più genericamente, del potere costituito. Per incominciare, si evidenziano allora quattro aree in cui la presenza di un sistema monetario – sulla cui definizione torneremo a breve e di nuovo al termine di queste considerazioni di carattere generale – risulta di grande utilità ai consociati e al potere costituito stesso:

- la fiscalità e la raccolta dei tributi,
- il ricorso a sanzioni per la repressione di comportamenti penalmente rilevanti, sostitutive delle pene corporali e della restrizione della libertà,
- la previsione di meccanismi compensativi di danni causati a diverso titolo tra i consociati, e
- la previsione di strumenti che facilitino la produzione e lo scambio di beni e servizi tra i consociati, sia per quanto attiene la dimensione dello scambio, sia per quanto attiene la concessione di crediti e l'assunzione di debiti.

Per comprendere l'importanza dell'uso della moneta in tutte queste aree, può essere utile iniziare questa riflessione sul rapporto tra diritto e moneta e sulla definizione della moneta provando a immaginare in un esercizio mentale cosa comporta l'assenza di quest'ultima in questi ambiti, riservandoci successivamente di chiarire come mai nel trattare il tema della definizione della moneta si insiste con particolare attenzione sulla funzione di mezzo di scambio che essa svolge.

In questa ipotetica società senza moneta, si assume, ovviamente, quale prima condizione essenziale del discorso, che vi siano comunque delle regole che definiscono la proprietà dei beni e disciplinano le modalità di esercizio della facoltà, ovvero di adempimento dell'obbligo, di trasferire la proprietà di certi beni tra consociati e tra

consociati e potere costituito[76]. Ciò posto, escludendo vi sia la possibilità di ricorrere a strumenti monetari e cioè non vi sia un'unità di misura del valore economico dei beni, né un bene che si distingua dagli altri in ragione di un'universale accettabilità, in tutti questi ambiti l'adempimento di obblighi giuridici inerenti il trasferimento di patrimonio comporterebbe la cessione di beni specificamente individuati. A ciò conseguono grossi limiti strutturali inerenti sia l'esercizio dei poteri sovrani, sia l'ambito dello scambio economico e della produzione di beni e servizi, riconducibili alla difficoltà di misurare il valore patrimoniale delle prestazioni imposte od offerte e alla inefficienza connessa alla rigidità che conseguirebbe alla necessità di strutturare tali prestazioni in termini di beni di consumo[77]. Non è difficile svolgere qualche esempio in proposito. La raccolta di tasse in beni di consumo limita la capacità fiscale del potere costituito secondo la effettiva presenza fisica di tali beni e la possibilità di aggregarli e poi consumarli. Ciò comporta l'aggravio dei costi di trasporto e immagazzinamento, nonché, laddove sussistano difficoltà nella conservazione e nel trasporto, la costrizione a dover richiederne la consegna soltanto in quei periodi dell'anno e in quei luoghi dove tali beni siano disponibili[78]. L'assenza di un denominatore comune rende, inoltre, difficile la gradazione dell'imposizione fiscale e ad entrambi questi elementi consegue inevitabilmente una minore capacità fiscale e un maggior rischio di diseguaglianze irrazionali. Nel contesto del risarcimento del danno o delle sanzioni pecuniarie, l'assenza di un'unità di misura rende difficile e costosa, in termini di efficienza, la gradazione del risarcimento rispetto al danno subito, ciò che aumenta il grado di incertezza e di potenziale illogicità del rimedio[79]. Si è dunque costretti a predisporre lunghi e dettagliati codici che prevedano

---

[76] Ciò che avviene nel sistema Bitcoin attraverso la connessione dei bitcoin registrati in un *unspent output* con una determinata chiave privata e il riconoscimento al possessore di detta chiave della facoltà di trasferire ad altrui tali bitcoin attraverso la trasmissione sulla rete di una comunicazione strutturata secondo un certo modo.

[77] Sotto il profilo dell'analisi economica del diritto può dirsi in via generale e astratta che l'assenza di un numeratore comune e di un bene di scambio universale non può che comportare una minore capacità di modulazione della volontà delle parti che partecipano ad una transazione, ciò che allontana dal punto ottimale di incontro a cui le parti convergerebbero laddove avessero maggiore libertà operativa.

[78] Sono interessanti, in proposito, le considerazioni espresse da DESAN C., *Making Money, cit.*, circa le dinamiche fiscali che interessavano le corti inglesi nel medioevo, dove, in un contesto di economia sostanzialmente demonetizzata, il Re e la corte si spostavano di feudo in feudo per consumare *in loco* i proventi della tassazione.

[79] Cfr. GOODHART, op. cit., p. 413 e WRAY, *From the State Theory of Money*, cit., p. 9.

per ciascun tipo di reato o danno civile la qualità e lo specifico ammontare dei beni che devono essere consegnati. Ciò è costoso in termini organizzativi, risolve la questione solo parzialmente e, anzi, ne evidenzia la complessità e l'incidenza: resta, infatti, molto difficile commisurare la compensazione al grado di responsabilità o di danno effettivamente cagionato senza significative approssimazioni e con un forte rischio di esercizio arbitrario del potere giurisdizionale.

Da ultimo, sono ben noti i limiti che presenta il baratto rispetto alla vendita nel contesto dello scambio di merci: la presenza di una merce universale di scambio utilizzata come contropartita negli scambi economici rende più facile la convergenza di interessi, allorché, per converso, la necessità di trovare una controparte specificamente interessata al bene d'uso che si è disposti a cedere e, al tempo stesso, in possesso di un bene di proprio interesse che è disposta a cedere, presenta costi transattivi così alti da rendere inimmaginabile, in concreto, un'economia di scambio basata sul baratto[80].

2.1.2. *Importanza dell'unità di conto*

Per converso in tutti i contesti sopracitati i consociati individualmente così come la collettività nel suo insieme ed il potere politico, traggono vantaggio dalla presenza di un'unità di misura che permetta di esprimere il valore economico delle prestazioni e dei beni in termini numerici: ciò consente di introdurre criteri di razionalità all'interno del sistema, di espandere l'orizzonte delle possibilità in ambito economico e di modulare i meccanismi di repressione dei comportamenti socialmente riprovevoli e di compensazione dei danni secondo criteri caratterizzati da maggiore equità e da un più elevato grado di giustizia.

Nel contesto della fiscalità, la definizione di unità di misura permette di valutare in modo certo e preciso il patrimonio e il reddito di ciascun consociato e di introdurre criteri di contribuzione ispirati a principi di proporzionalità e adeguatezza. La definizione in termini numerici delle sanzioni pecuniarie e il risarcimento del danno permette di

[80] Vero è, altresì, che l'istituzione di meccanismi che permettano di posticipare nel tempo l'esecuzione della controprestazione permette di ovviare, almeno, parzialmente agli alti costi transattivi del baratto: si pensi, per esempio, all'istituzionalizzazione dei rapporti di debito e credito che permetta di aggregare e successivamente compensare rapporti opposti anche non omogenei.

gradare l'esercizio della funzione giurisdizionale, con simili risultati in termini di efficienza e di maggiore giustizia. Da ultimo, nel contesto degli scambi, la misurazione del valore in termini numerici permette di introdurre criteri di razionalità nell'allocazione delle risorse produttive negli scambi[81]. In sintesi, l'unità di misura del valore economico dei beni permette di astrarre in forma numerica il valore dei beni, delle prestazioni e delle sanzioni delle condotte illecite, e di creare, quindi, obbligazioni giuridiche consistenti nella corresponsione di un certo numero di tali unità: le obbligazioni pecuniarie.

2.1.3. *Importanza dei mezzi di pagamento*

Perché l'unità di misura esplichi tali funzioni e conferisca i benefici sociali ed economici sopra descritti, è necessario che i consociati possano dare esecuzione alle obbligazioni assunte mediante il ricorso a dei mezzi di pagamento, cioè a delle procedure che permettono di trasferire la titolarità di un adeguato numero di unità di conto ed estingue l'obbligazione pecuniaria[82]. Il mezzo di pagamento più semplice consiste nella dazione di un bene che ha la caratteristica di incorporare una certa quantità di unità di conto secondo un rapporto definito. In questa ipotesi, la consegna del bene realizza in

---

81 Cfr. BARCELLONA E., *Ius monetarium. Diritto e moneta alle origini della modernità*, Il Mulino, 2012, pp. 52 ss..

82 Cfr. la descrizione di 'pezzo monetario' di INZITARI, op. cit., p. 21: "*I pezzi monetari appaiono dunque come mera manifestazione fenomenica di tale uguaglianza* [riferendosi al valore dei beni espresso in termini matematici dall'unità di conto]" e ancora, a p. 22: "*Il pezzo monetario è, al contrario, solamente la forma di manifestazione materialmente e praticamente necessaria (almeno ad un certo livello dello sviluppo del fenomeno monetario) della unità di misura*". Cfr. la definizione di pagamento offerta nel quadro del diritto dell'Unione Europea dalla Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE, (GU L 319 del 5.12.2007, pag. 1): a mente del combinato disposto delle definizioni di "operazione di pagamento" e "fondi", di cui all'art. 4, comma I, n. 5 e 14, *ivi* per pagamento si intende "*l'atto, disposto dal pagatore o dal beneficiario, di collocare, trasferire o ritirare banconote e monete, moneta scritturale e moneta elettronica, indipendentemente da eventuali obblighi sottostanti tra il pagatore o il beneficiario*". Cfr., altresì, OLIVECRONA K., *La struttura dell'ordinamento giuridico*, Etas Kompass, 1972, p. 315: "*Dove si trovino queste entità è una domanda alla quale è stata data ogni sorta di concepibile risposta senza successo. La ricerca delle entità chiamate unità monetarie è stata, e doveva essere, vana, perché tali unità non esistono: la parola «unità monetaria» non ha nessun referente semantico […] Le unità ideali apparentemente designate dalla parola «sterlina» sono puramente fittizie; la parola è «vuota» non denota nulla, ma quando viene usata in certi contesti, conformemente a certe norme, ne seguono conseguenze pratiche di grande importanza*"; sull'importanza del diritto e del contesto istituzionale entro cui è impiegato il concetto di unità monetaria, v. *infra*.

termini materiali ciò che astrattamente è definito nei termini di trasferimento di unità di conto.

2.1.4. *Rapporto unità di conto – mezzo di pagamento*

Unità di conto e mezzo di pagamento costituiscono quindi due facce della «moneta»[83], entrambe necessarie e compresenti in qualsiasi sistema monetario: per unità di conto si intende il riferimento all'unità astratta, per mezzo di pagamento la concretizzazione nei rapporti sociali ed economici di tali unità. La definizione del rapporto tra l'una e l'altro è condizione imprescindibile per l'esistenza del sistema monetario. Nell'ipotesi più semplice tale rapporto potrebbe consistere sostanzialmente in una perfetta sovrapposizione: è questo il caso ipotetico di un'unità di conto espressa nei termini del bene fisico utilizzato per incorporarla e rappresentarla nella vita materiale. Si pensi, ad esempio, al caso astratto di un'economia dove l'unità di conto è espressa in conchiglie e in cui un succo di frutta vale due conchiglie e un caffè vale quattro conchiglie. Per pagare un caffè si dovranno concretamente consegnare alla controparte quattro *conchiglie* (mezzo di pagamento), mentre per descriverne il prezzo – come poc'anzi fatto – si farà riferimento alla nozione astratta di *quattro* conchiglie (unità di conto). Altrimenti detto, l'espressione quattro conchiglie fa riferimento sia alle conchiglie materialmente esistenti che si intende consegnare in cambio di un caffé, sia ad un numero di unità con cui si misura il valore di scambio bei beni il cui valore corrisponde ad un caffè o due succhi. In questo contesto c'è perfetta corrispondenza tra unità di conto e mezzo di pagamento.

In società caratterizzate da un più alto grado di complessità economica e istituzionale, tale rapporto è disciplinato da una norma giuridica. Per esempio, oggi in Italia si può consumare un cappuccino al bar al prezzo di un euro e venti centesimi. L'unità di conto con cui è espresso il prezzo del bene è l'euro, il quale è un referente astratto computato in numeri interi e centesimi. Il mezzo di pagamento utilizzato per adempiere all'obbligazione consiste nella dazione di due dischi di metallo di un certa specifica fattura: uno bimetallico con l'interno realizzato in una lega di rame-nichel e

[83] Talvolta la distinzione in termini giuridici è espressa facendo riferimento alla nozione di *moneta di conto* e di *moneta di pagamento*, v. OLIVECRONA, op. cit., p. 311.

l'esterno in una lega di nichel-ottone, con massa di 7,5 g, diametro di 23,25 mm e spessore di 2,33 mm, che rappresenta ed incorpora il valore di un euro, ed uno realizzato in lega oro nordico, con massa 5,74 g, diametro 22,25 mm e spessore 2,14 mm, che rappresenta ed incorpora il valore 20 centesimi di euro. Il rapporto tra unità di conto e mezzo di pagamento è definito dal Regolamento (CE) N. 975-98 del Consiglio del 3 maggio 1998, riguardante i valori unitari e le specificazioni tecniche delle monete metalliche in euro destinate alla circolazione, che ha forza vigente in Italia, ed è un rapporto accettato e riconosciuto da tutti i consociati nella prassi. Emerge, quindi, già in queste prime considerazioni introduttive una funzione espletata dal diritto nel contesto della gestione dei sistemi monetari: cioè la definizione di mezzi di pagamento e del loro rapporto con l'unità ideale.

Al variare della complessità istituzionale del sistema monetario in analisi variano le modalità attraverso cui sono creati mezzi di pagamento che permettono di estrinsecare nella realtà un determinato numero di unità di conto. Nel contesto della civiltà occidentale i regnanti sono più volte incorsi nell'esigenza di aumentare la provvista di risorse monetarie a disposizione del potere pubblico e del mercato in generale, sia per ragioni fiscali legate al finanziamento della spesa pubblica, sia per far fronte all'esigenza di regolare un più alto numero di scambi all'interno del mercato. Nel tempo si è venuto a creare un particolare mezzo di pagamento che consiste nel trasferimento di rapporti giuridici, in particolare crediti, che sorgono e perdurano nel tempo con la finalità di essere utilizzati come mezzo di pagamento e non già per effetto di una dilazione dell'esecuzione della prestazione del debitore: crediti, altrimenti detto, costituiti all'intero di un sistema finalizzato alla produzione di un mezzo di pagamento astratto, la cui quantità non sia limitata dalla disponibilità di un certo bene fisico[84].

Come è già stato anticipato, la disponibilità di mezzi di pagamento e la determinazione di un rapporto tra mezzo di pagamento e unità di conto è essenziale affinché possano essere assunte obbligazioni giuridiche definite in termini "monetari" e l'unità di conto possa trovare concreto utilizzo nel mondo reale. La realizzazione – nel senso etimologico di rendere reale un concetto astratto – dell'unità di conto in termini

[84] Sul punto *amplius infra*.

concreti all'interno dei rapporti sociali è inoltre essenziale ai fini della distribuzione di tale risorsa tra i consociati, permettendone l'appropriazione e l'accumulo, oltre che il trasferimento.

2.1.5. *L'uso della moneta tra* mensura *e* mensuratum

L'insieme di unità di conto, mezzi di pagamento e disciplina del rapporto tra essi non è, però, da solo sufficiente a determinare il valore economico di tali unità. Qui sta uno dei paradossi e delle grandi difficoltà teoriche connesse con lo studio dei sistemi monetari che la dottrina giuridica, in particolare con Nussbaum e Ascarelli, ha saputo evidenziare nel contesto del dibattito sulla nozione di moneta: l'unità di conto considerata in sé e per sé non ha alcun valore economico se non quello che le è attribuito dall'uso che di essa fanno i consociati[85]. Prima di chiarire meglio il concetto giova anticipare sin da ora che a ciascun bene suscettibile di valutazione economica possono essere associati due valori: il valore economico, inteso come l'interesse concreto che un gruppo di soggetti attribuisce all'uso di quel bene in quanto idoneo a soddisfare un bisogno della vita e quindi assimilabile all'idoneità del bene stesso di soddisfare un bisogno economico, ovvero il valore monetario, o "prezzo", cioè l'espressione in termini monetari del valore economico attribuito a quel bene, rapportato, evidentemente, ad una scala espressa nei termini dell'unità di conto. Il rapporto tra i due valori è tale per cui il secondo aspira ad essere la misura del primo, allorché il valore reale del bene cui è associato un prezzo è 'misurato' dalla moneta[86].

---

[85] PINI R., *Il denaro pubblico*, vol. I, *Problemi generali*, Cedam, 1984, p. 75: "*Il denaro è uno strumento di relazione tra valori soggettivi; è l'espressione di una analisi dinamica, a base soggettiva, delle scelte individuali*".

[86] È obbligo, qui, fare riferimento, al contributo di ASCARELLI, *Obbligazioni pecuniarie*, *cit*., *passim*, ed in particolare pp. 46 ss., che sviluppa le nozioni di "*mensura*" e "*mensuratum*" nel contesto del dibattito circa la definizione della natura dei pezzi monetari che concretamente vengono consegnati in pagamento di un bene. Qui la distinzione è ripresa, invece, per evidenziare che il processo di misurazione di applica a tutti i beni della società cui è dato un prezzo. Sul punto cfr. STAMMATI, op. cit., p. 750, "*un'altra importante distinzione che viene fatta è quella tra la moneta cosidetta «reale» e la moneta «nominale»: la prima nozione guarda al potere d'acquisto della moneta, cioè la quantità di beni o di servigi che l'unità di moneta può acquistare. La moneta «nominale» indica semplicemente 'l'unità monetaria', il cui valore, come si dirà, varia, grossomodo, in misura inversa al variare del livello generale dei prezzi*".

A differenza di altre unità di misura che definiscono aspetti fisici della materia (il peso, la lunghezza, l'intensità del rumore), la moneta misura un valore che non esiste in natura, ma è costantemente rinnovato dall'apprezzamento e dalle scelte personali dei consociati, cioè dall'attività tipicamente umana di comparare due o più beni o servizi tra loro in relazione all'interesse atteso che si ritiene di poter soddisfare o di non poter più soddisfare attraverso l'acquisizione o la cessione del bene[87]. Si tratta, quindi, di un valore arbitrario connesso all'aspettativa di godimento che si crede di poter ricevere da un certo bene, che può essere espresso solo in relazione all'aspettativa di godimento collegata ad un altro bene. Il problema centrale, dunque, è che non esistendo in natura un esemplare concreto di "valore economico" cui rapportare l'unità di conto, il rapporto tra unità di conto e valore economico è soggetto a variazione[88]. Si immagini, per converso, l'esempio del metro. Il metro è un'unità di misura della lunghezza, di per sé la parola "metro" non significa niente a meno che non la si rapporti con una certa specifica lunghezza del mondo reale cui essa corrisponde. Il rapporto tra tale unità di misura e la sua estrinsecazione reale è definito da una convenzione che esiste tra tutti i soggetti che utilizzano tale unità di misura secondo cui un metro corrisponde alla lunghezza di una specifica barra di platino-iridio conservata a Parigi presso il *Bureau international des poids et mesures*. Esiste, quindi, un bene concreto che rende reale e tangibile la misura espressa dall'unità astratta ed un accordo che sancisce in modo certo tale rapporto.

Nel contesto della moneta questo non accade perché ciò che si misura non è una grandezza fissa, ma una relazione tra il valore di più beni, che viene espressa, appunto, attraverso l'unità di conto[89]. Ciò significa che essa rappresenta una sintesi dei rapporti tra

---

87 Cfr. FELIX M., *Money. The unauthorized biography*, Alfred A. Knopf, 2013, pp. 50-53, che conclude evidenziando che nel contesto della moneta la definizione dei meccanismi che permettono la misurazione del valore economico è un'attività politica e non solo tecnica.

88 *Contra* la visione dei metallisti secondo cui il valore del denaro deriva dal valore intrinseco del bene che lo rappresenta; cfr. David Ricardo: "*There can be no unerring measure of either length, of weight, of time or of value unless there be some object in nature to which the standard itself can be referred*" cit. in SRAFFA P., *The works and Correspondence of David Ricardo*, vol. 1, Cambridge University Press, 1951, p. 401

89 FARENGA, op. cit., p. 32, evidenzia che la funzione di "misurazione dei valori" della moneta è "estremamente difficile da definire giuridicamente" proprio in ragione del fatto che il valore della moneta (intesa come unità di misura) non è costante ed immutabile come nel caso dei sistemi di misurazione (grammo, metro, litro…), "*bensì risente di complessi e numerosi fenomeni economici che determinano continue variazioni nel rapporto tra la moneta e gli altri beni*".

i vari beni e servizi e che il valore dell'unità stessa non rimanda in astratto ad un bene o valore concreto tangibile, ma all'insieme di tutti i beni il cui valore è misurato in termini di unità di conto, secondo il rapporto che in un certo momento storico esiste tra ciascun bene e l'unità astratta. In estrema sintesi, il valore reale della moneta dipende dall'indice generale dei prezzi[90]. L'apparente paradosso consiste nel fatto che si vuole misurare il valore di un bene con un'unità di misura il cui valore, in ultima analisi, dipende dalla misurazione stessa. Ciò in parte è vero, ma si spiega in ragione del fatto che la moneta non misura il valore in sé e per sé del bene, ma unicamente il suo valore in relazione ad altri beni. L'apparente paradosso può quindi essere reso in questi termini: l'unità di conto permette di misurare il valore di un bene nei termini di un valore astratto che rimanda al valore di ogni altro bene presente nell'economia. Il valore dell'unità di conto con cui si intende misurare un bene dipende, quindi, dall'attività di misurazione stessa, ma non dalla misurazione di quello specifico bene, ma dalla misurazione di ogni bene, quello incluso. Da qui la considerazione secondo cui il valore dell'unità di conto dipende dall'uso, cioè dall'impiego di tale unità in accordi o imposizioni giuridiche dalle quali è possibile evincere un'equiparazione tra un bene della vita e una certa quantità di unità di conto. Sotto questo profilo, l'unità di conto assomiglia ad una scala numerica a cui tutti possono fare riferimento per determinare il contenuto delle obbligazioni giuridiche[91]: il sovrano per determinare gli obblighi contributivi dei sudditi o il valore delle pene pecuniarie[92] e i consociati per determinare il prezzo dei beni e dei servizi scambiati nel mercato.

Il più frequente e significativo degli usi che permettono la definizione di questo rapporto tra unità di conto e valori reali è proprio lo scambio economico di tipo sinallagmatico, dove due soggetti liberamente si accordano per scambiare un bene o un servizio contro un prezzo, cioè contro un certo numero di unità di conto. Attraverso la ripetizione di questa operazione il mercato dà un prezzo ai beni e, per converso,

---

90 Cfr. ASCARELLI, *Obbligazioni pecuniarie*, *cit*., p. 14: "*il valore della moneta, il suo potere d'acquisto, costituirà allora necessariamente un'espressione reciproca di quella del livello generale dei prezzi*".

91 Cfr. definizione di BLACKSTONE, i, 276, [citato in PROCTOR, op. cit., p. 12] "*the medium of commerce … a universal medium, or common standard, by comparison with which the value of all merchandise may be ascertained, or it is a sign which represents the respective values of all commodities*".

92 Sull'importanza della definizione di alcune pene e risarcimenti in termini monetari per l'affermazione della moneta come standard di misurazione/unità di conto, v. GOODHART, op. cit., p. 413 e l'estratto di GRIERSON, *The origins of money*, 1977, riprodotto in Goddhart1998, 426.

attribuisce un valore reale all'unità di conto. In ragione dell'importanza degli scambi sotto il profilo appena evidenziato si giustifica il riferimento predominante a tale contesto ai fini della definizione di cosa sia la moneta.

2.2. La moneta e l'intermediazione degli scambi: liquidità, scambio e pagamento

2.2.1. *La liquidità e la definizione di moneta come bene massimamente liquido*

Si torni, per prima cosa, alla nozione diffusa in ambito economico secondo cui la moneta è il bene utilizzato per scambiare altri beni e alla conseguente definizione della moneta nei termini di qualsiasi bene che sia utilizzato per scambiare beni e servizi. Questa sintesi del fenomeno monetario, comunemente adottata dall'ortodossia economica, pone al centro della questione la funzione di mezzo di scambio, che si avrà modo di vedere riveste un'importanza molto significativa all'interno del sistema monetario, e si sviluppa in continuità con la tradizione dell'economia classica, secondo cui vi è perfetta coincidenza tra la nozione di moneta e le merci di volta in volta utilizzate come mezzo di pagamento, e la tradizione metallista, che predicava l'identità tra metalli preziosi utilizzati come mezzo di scambio, in particolare oro e argento, e la moneta. Con riferimento alla questione dell'origine della moneta e di come una certa moneta – *rectius* mezzo di pagamento – inizi ad essere utilizzata in una comunità, l'approccio che considera il fenomeno monetario principalmente quale strumento per l'esecuzione degli scambi è riconducibile alla teoria catallattica.

Il pregio più significativo di queste teorie è di aver evidenziato la particolare logica che è sottesa allo scambio monetario *vis à vis* il baratto e di avere conseguentemente contribuito ad evidenziare alcune caratteristiche che devono assumere i mezzi di pagamento all'interno di un'economia, in particolare l'attributo della liquidità. Queste considerazioni saranno l'oggetto delle seguenti riflessioni.

Il discorso può incominciare con la classica assunzione di un contesto economico in cui vi sia una sovrapproduzione di beni e i consociati abbiano interesse a scambiare il surplus di produzione per ottimizzare il loro benessere[93]. Nell'economia di scambio che

[93] Una delle più significative critiche alla teoria catallattica consiste nell'evidenziare che in assenza di moneta non si ha ragione di avere produzione di surplus, ma è al contrario ragionevole pensare che la

ne consegue ciascun bene può essere caratterizzato nei termini di una maggiore o minore capacità di essere scambiato, per ciò intendendosi il grado di difficoltà che un agente economico incontra nel trovare una controparte interessata ad acquisire il bene offerto sul mercato. Un bene estremamente liquido è, quindi, un bene la cui cessione sul mercato non comporta particolari costi di transazione connessi alla ricerca di una controparte disposta ad acquistare il bene, così come per converso un bene illiquido è un bene rispetto al quale è difficile trovare un compratore. Tale difficoltà, ovviamente, in termini reali incide e dipende anche dal prezzo a cui si è disposti a cedere il bene: è una nozione basilare dell'economia che la domanda di un bene sia inversamente correlata al prezzo, sicché per riuscire a vendere un bene è teoricamente sufficiente alzare o diminuire il prezzo. Proprio in ragione di questa considerazione, la liquidità di un bene si misura nella capacità (astratta) di essere utilizzato come mezzo di scambio[94], cioè con la differenza di valore che intercorre tra lo scambio con cui si acquisisce il bene al fine di una futura cessione e lo scambio con cui lo si cede, con ciò volendo isolare i costi di transazione connessi allo scambio del bene dal valore di mercato del bene stesso, che si presume costante in entrambi gli scambi. Per comprendere questo concetto si parta dall'assunto che qualsiasi bene disponibile può essere scambiato, sia per soddisfare un bisogno diretto, sia al fine di essere conservato e successivamente scambiato con altra merce. Nella seconda ipotesi, tale bene acquista la funzione di medium dello scambio. È interesse dell'agente economico, in questo caso, che il bene utilizzato conservi il proprio valore tra il primo e il secondo scambio. Tale capacità dipende da diversi fattori: oltre ai costi di conservazione del bene, i costi più significativi che l'agente dovrà incorrere sono quelli relativi alla ricerca di una controparte interessata ad ottenere quel bene. Più un bene è

produzione sia orientata al sostentamento e gli scambi siano estremamente limitati. Per tale ragione, non è credibile che in un'economia non monetaria ci sia un numero di scambi tale da permettere di indentificare un bene come mezzo di scambio universale. Al contrario, è invece plausibile l'effetto opposto, cioè che l'introduzione da parte di un soggetto in grado di imporre o proporre efficacemente a tutti consociati un bene che permettesse di rappresentare il valore nel tempo e, quindi, di realizzare scambi di tipo monetario, abbia permesso una maggiore specializzazione nell'economia, la produzione di surplus e la nascita del commercio. Sul punto v. DESAN C., *Making Money*, *cit*., *passim*, e *infra*.

94 V. CECCHETTI S.G. e SCHOENHOLTZ K.L., *Money, Banking, and Financial Markets*, McGraw-Hill Education, 4 ed., 2015, p. 36: "*Liquidity is the ease with which you can turn an asset into a means of payment without loss of value*".

richiesto sul mercato, minori saranno i costi connessi alla ricerca di una controparte e, maggiore, quindi, sarà la liquidità del bene.

La moneta, intesa come merce di scambio universalmente accettata all'interno di una data società è, per definizione, un bene massimamente liquido: la liquidità è quindi un attributo tipico della moneta merce–mezzo di scambio ed anzi può dirsi che la nozione stessa di liquidità, poc'anzi illustrata proprio nei termini di consonanza di un bene ad essere utilizzato come mezzo di scambio, possa riassumere in sé l'elemento centrale della definizione di moneta adottata dagli economisti *mainstream*.

2.2.2. *Il rapporto tra liquidità ed origine della moneta*

La nozione di liquidità è poi ancora collegata alla moneta intesa come mezzo di scambio universale sotto un ulteriore profilo. Si è detto che la liquidità è positivamente correlata con la domanda per quel bene, ora si può aggiungere che la domanda di un bene utilizzato come mezzo di scambio è positivamente correlata con la liquidità dello stesso.

I motivi per cui più persone condividano interesse per una stessa merce possono essere i più vari: è possibile che più soggetti condividano il bisogno di consumare quel bene – si pensi ai generi alimentari, necessari per la vita –, o è possibile che il possesso del bene conferisca un certo status sociale. Tra le ragioni che sostengono la domanda di un bene liquido acquista particolare importanza l'aspettativa di poter utilizzare in futuro il bene come mezzo di scambio, cioè la proiezione della domanda futura del bene da parte degli altri consociati. Tale proiezione, effettuata da un numero consistente di soggetti, ha una portata circolare di autogiustificazione: l'agente acquisisce il bene in virtù della sua (supposta) liquidità, immaginando che tale bene sarà accettato in futuro da altri soggetti che a loro volta penseranno di poter riutilizzare il bene come mezzo di scambio, e il suo comportamento concorrerà a confermare e a far scaturire negli altri soggetti tale aspettativa di potere a loro volta cedere quel bene[95]. In questa prospettiva, dunque, la

[95] V. STAMMATI, op. cit., p. 748: "*La moneta, cioè, deve essere circondata dalla generale fiducia che essa è, e verrà generalmente accettata. «Tale generale accettabilità (continua il Newlyn) può costituire la risultante di molti fattori diversi operanti singolarmente o in combinazione tra loro; e rientra in quel discutibile e fascinoso gruppo di fenomeni che sono soggetti all'influenza di opinioni autogiustificantesi. Se i membri di una collettività pensano che la moneta sarà generalmente accettata, essa lo sarà; altrimenti non lo sarà». È quindi la collettività a decidere quale debba essere lo strumento*

liquidità non è solo un attributo tipico del bene utilizzato come mezzo di scambio universale da tutti i consociati, ma è una caratteristica che suscita e sostiene l'utilizzo di tale mezzo di scambio nel tempo.

Tale ultima considerazione è alla base della teoria catallattica sulle origini della moneta, secondo cui il bene utilizzato come mezzo di scambio è in origine semplicemente un bene liquido, la cui liquidità aumenta in ragione dell'uso da parte di alcuni come mezzo di scambio sino a farne assumere le caratteristiche di mezzo di scambio universale. Secondo tale narrativa, di cui offre una chiarissima illustrazione il famoso saggio di Carl Menger *"On the origins of money*", la nascita della moneta è quindi riconducibile alla trasformazione di un bene liquido in bene universalmente accettato che, per l'effetto, avoca a sé la funzione di misuratore del valore di ogni altro bene. La riflessione del noto economista si pone l'obbiettivo di spiegare, in termini economici, il fatto che certi beni siano utilizzati come mezzi di scambio universalmente accettati da tutti i membri di una certa società[96]. Per rispondere a tale interrogativo Menger illustra innanzitutto il concetto di *saleableness* (o *Absatzfähigkeit*)[97], sostanzialmente paragonabile alla nozione moderna di liquidità, cioè la misura della *vendibilità* di un bene sul mercato. Per l'autore, allora, la moneta non è altro che il bene con il grado più alto di *saleableness*, la *unlimited saleableness*, e si differenzia dagli altri beni unicamente per questa caratteristica[98]. Quanto alle origini di tale moneta, Menger assume che gli attori economici abbiano

prescelto come moneta, il quale non necessariamente si identifica con un bene reale, anzi generalmente, nel mondo moderno, se ne svincola completamente".

96 MENGER, *On the Origin of Money*, cit., p. 239, il punto di partenza della riflessione è l'esistenza di tali mezzi: "*There is a phenomenon which has from of old and ill a peculiar degree attracted the attention of social philosophers and practical economists, the fact of certain commodities (these being in advanced civilizations coined pieces of gold and silver, together subsequently with documents representing those coins) becoming universally acceptable media of exchange*"; e più specificatamente ancora l'a. si interroga sulle ragioni che sorreggono il comportamento degli agenti: "*we have to explain why it is that the economic man is ready to accept a certain kind of commodity, even if he does not need it, or if his need of it is already supplied, in exchange for all the goods he has brought to market*".

97 *Ibidem*, p. 242, "*the different degrees of saleableness (Absatzfähigkeit) of commodities*", e sugli attributi che determinano il grado di liquidità–*saleableness* di un bene, *ibidem*, pp. 246-247.

98 *Ibidem*, p. 243, "*the theory of money necessarily presupposes a theory of the saleableness of goods. If we grasp this, we shall be able to understand how the almost unlimited saleableness of money is only a special case, - presenting only a difference of degree - of a generic phenomenon of economic life - namely, the difference in the saleableness of commodities in general*".

spontaneamente e gradualmente emulato i primi che hanno iniziato ad usare un determinato bene come strumento di intermediazione degli scambi al fine di ampliare il loro orizzonte economico e che per l'effetto di tale emulazione il bene sia diventato un mezzo di scambio universalmente accettato.

Indipendentemente dall'accuratezza storica della tesi secondo cui la moneta sia stata creata attraverso una serie ripetuta di scambi (su cui si tornerà *infra*), emerge in modo evidente da quanto si è detto la stretta connessione tra liquidità e moneta intesa quale mezzo di scambio universale. La portata euristica di questo assunto nel contesto dell'economia e delle scienze sociali può difficilmente essere sottostimata ed è tuttora patrimonio dell'ortodossia economica. In particolare, tale relazione ha suggerito nel tempo la definizione di moneta quale mezzo di scambio universale e, a sua volta, la sovrapposizione inversa della definizione di mezzo di scambio universale nei termini della merce caratterizzata dal più alto grado di liquidità all'interno di una società. Questa duplice sovrapposizione di concetti nasconde, però, il rischio di perdere di vista la particolare l'importanza dell'*unità di conto astratta* e della relazione che viene a crearsi tra essa e il mezzo di pagamento utilizzato negli scambi economici. Per evidenziare questo importante passaggio nei prossimi paragrafi faremo riferimento alla differenza che sussiste tra un «*mezzo di scambio*», pure universalmente riconosciuto e accettato come tale, e un «*mezzo di pagamento*», concetto che per noi implica una differenza qualitativa che non si risolve esclusivamente in una maggiore o assoluta liquidità, ma rimanda al rapporto tra il mezzo di pagamento e l'unità di conto ideale utilizzata per denominare gli scambi monetari.

Oltre a essere direttamente connessa alla moneta in relazione all'intermediazione degli scambi, la nozione di liquidità assume una certa importanza anche sotto il profilo dello studio del risparmio e dell'accumulazione della moneta: essa, cioè, può acquistare rilevanza indipendentemente dal fatto che l'agente al momento dell'acquisto di un bene abbia già maturato il desiderio di cederlo in cambio di altri beni. Si tocca qui un aspetto ineludibile della vita di qualsiasi uomo che è il senso di incertezza verso il futuro: nessuno sa cosa succederà domani. Tale strutturale incertezza suggerisce all'uomo medio una certa prudenza nell'allocazione delle risorse che ha a disposizione oggi, cui consegue un diretto interesse a convertire e conservare una parte del proprio patrimonio in risorse

liquide, suscettibili di essere convertite in beni o servizi atti a soddisfare bisogni che possono sorgere in futuro, per effetto di imprevisti o per il mutamento delle circostanze o delle preferenze dell'agente (cd. "*propensione al risparmio*")[99]. A fronte dell'impossibilità di conoscere il futuro, l'agente economico razionale ha, quindi, interesse a diversificare il suo patrimonio includendovi dei beni liquidi, la cui pronta realizzazione permette di adattarsi efficacemente ai mutamenti. In questo caso, l'agente rinuncia a trarre benefici d'uso da parte del proprio patrimonio accollandosi il rischio della possibile perdita di valore del bene liquido nel tempo per fare fronte al rischio di perdite connesse all'esigenza di fare fronte a bisogni futuri con beni non altrettanto liquidi[100]. In termini finanziari lo stesso concetto è utilizzato in termini diametralmente opposti per giustificare la differente struttura del tasso di interesse sul breve e lungo periodo. Secondo la teoria del *liquidity premium*, i tassi di lungo periodo sono più alti per compensare il maggiore sacrificio di liquidità che sopporta il sottoscrittore del prestito[101].

2.2.3. *Il mezzo di scambio*

Si è presentato il caso, poc'anzi, di una merce che sia scambiata non già per il suo valore d'uso, ma per il suo valore di scambio (futuro), in ragione, cioè, della possibilità attesa e concreta di utilizzare tale particolare merce in un ulteriore scambio futuro. In sintesi, si riprende la descrizione dello scambio monetari nei termini di una intermediazione tra due diversi scambi che si susseguono nel tempo, secondo lo schema merce–denaro–merce.

Qualsiasi bene, si è detto, è suscettibile di essere utilizzato come contropartita di uno scambio sinallagmatico e le ragioni che inducono un agente economico ad acquistare un determinato bene possono essere le più svariate, ivi inclusa l'aspettativa di poter rivendere quel particolare bene ad un valore maggiore su una piazza diversa. Questo

---

99 L'economista che più di ogni altro ha dato un contributo essenziale sullo studio della propensione al risparmio e sulla relazione tra risparmi, investimenti e il valore della moneta è Keynes, sul punto v., in particolare, KEYNES, op. cit. e cfr. MISHKIN, GIULIODORI e MATTHEWS, op. cit., pp. 499 ss.

100 Per l'applicazione di questo concetto in materia finanziaria *Ibidem*, p. 114 e in particolare p. 122.

101 SIMPSON T.D., *Financial Markets, Banking and Monetary Policy*, Wiley, 2014, p. 81; MISHKIN, GIULIODORI e MATTHEWS, op. cit., p. 122, e NORRBIN S. e MELVIN M., *International Money and Finance*, Elsevier, 8 ed., 2013, p. 121.

elemento, solo, non fa del bene un mezzo di scambio, né un mezzo di pagamento. Per poter definire un bene come mezzo di scambio non rileva, infatti, la volontà e il disegno economico del singolo operatore, ma occorre che il bene eserciti oggettivamente la funzione di intermediazione degli scambi all'interno di una certa società o economia. La differenza tra uno scambio di due beni qualsiasi e uno scambio che coinvolge un bene che si può definire «*mezzo di scambio*» è che tale bene è offerto ed accettato in ragione della sua idoneità (al momento dello scambio attesa) a poter essere successivamente ceduto in cambio di altre merci: aspettativa che non appartiene in modo esclusivo alla dimensione della coscienza interna dell'agente economico, ma che è condivisa da entrambe le parti ed origina ed è riflessa e concretizzata, quindi, in una serie di elementi di fatto che caratterizzano il contesto entro cui lo scambio si iscrive. Il primo e più importante di questi elementi di fatto, dai quali è possibile inferire che un certo bene è scambiato non già (o non unicamente) per il suo valore d'uso, ma in ragione del suo valore di scambio, è l'uso reiterato nel tempo da parte di numerosi soggetti di quel bene in una molteplicità di scambi, nonché l'apprezzamento sociale di tale bene quale strumento idoneo a intermediare scambi tra soggetti diversi ed in tempi diversi. Agli occhi del giurista, l'aspetto istituzionale della nozione di mezzo di scambio è in qualche modo riconducibile alla dimensione sociale e non solo puramene economica dell'agente economico. Adottando, *mutatis mutandis*, i criteri tipici della definizione delle consuetudini, può dirsi che una merce diviene un «mezzo di scambio» (nel senso che si vuole utilizzare qui del termine) all'occorrere della *diuturnitas*, che nel caso di specie consiste nell'uso su ampia scala reiterato nel tempo, e della *opinio permutationis*, cioè dalla convergente e diffusa consapevolezza di stare scambiando una merce non già (o non solo) in ragione del suo valore d'uso, ma con l'aspettativa di poterla riutilizzare in futuro come contropartita di ulteriori scambi. A questi termini può essere riconosciuta ad un particolare bene la qualità di «*mezzo di scambio*».

La definizione offerta di mezzo di scambio suggerisce tre ulteriori riflessioni inerenti: (*i*) la dimensione sociale dello scambio; (*ii*) il differimento temporale tra la coppia di scambi che completano il ciclo di utilizzo del mezzo di scambio; e (*iii*) gli effetti dell'uso diffuso di una medesima merce come mezzo di scambio per tutti gli scambi di un'economia.

La dimensione sociale dello scambio

Posto che alla base dell'adozione di un mezzo di scambio utilizzato trasversalmente in una certa economia c'è l'idea che lo stesso bene sia utilizzato da più soggetti in scambi diversi, ciò presuppone l'esistenza di una comunità di soggetti tra i quali tale bene è riconosciuto come mezzo di scambio universale[102]. La stessa nozione di liquidità cara alle teorie dell'ortodossia economica, d'altronde, presuppone essa stessa una socialità alla quale fa riferimento la domanda diffusa del bene, nonché un sistema di scambi regolati, anche se frequentemente l'analisi della funzione di intermediazione degli scambi della moneta è ricondotta ad una dimensione atomistica che prende in considerazione un unico ciclo di scambio merce contro prezzo e prezzo contro merce, contrapponendolo alla difficile realizzazione di scambi merce contro merce.

Proprio per rimarcare l'esistenza di una dimensione sociale insita nella costituzione di strumenti di scambio che superano la dimensione dell'accordo sinallagmatico tra due parti per acquisire rilevanza per più soggetti, si è voluta descrivere la costituzione del più semplice dei mezzi di scambio – nella forma di merce connotata dalla massima liquidità – in termini che sono appena stati connotati come *para–consuetudinari*. Quanto appena detto a proposito del «*mezzo di scambio*» vale, come è logico che sia, anche per l'istituzione di sistemi monetari più complessi. Se ne deduce che qualsiasi moneta o mezzo di scambio è rapportabile ad una data comunità di soggetti che segna il confine, più o meno variabile, entro cui tale istituzione esercita le sue funzioni: non può esistere, da un punto di vista logico, una moneta, un mezzo di pagamento o un semplice mezzo di scambio che non abbia alcun riferimento rispetto ad un corpo sociale, seppure vagamente definito, nel quale tale strumento possa essere utilizzato.

[102] Circa la dimensione sociale dello scambio monetario e quindi, *mutatis mutandis*, della costituzione di un mezzo di scambio universale secondo l'accezione qui proposta, v. GIANNINI, op. cit., *passim* e in particolare p. 53: "*se esistono tra individui o più, e la cessione di moneta effettivamente disobbliga in maniera definitiva il cedente, vuol dire che esiste un accordo a tal fine, tacito o esplicito, fra tutti i componenti del circuito in cui la tecnologia di pagamento e operante, e che quindi travalica le parti direttamente coinvolte in determinato atto di scambio. La moneta, ne consegue, non è un bene come gli altri, bensì un'*istituzione sociale" (corsivo nell'originale).

Il differimento temporale delle controprestazioni "reali" e l'incompletezza informativa tipica dell'intermediazione degli scambi

L'uso di un «mezzo di scambio» che viene acquistato nell'ottica di una cessione futura, presuppone che lo stesso sia capace di incorporare e di conservare un certo valore nel tempo e permette, per l'effetto, di superare, nel contesto degli scambi così come nel contesto della riscossione della fiscalità, i limiti che sarebbero altrimenti imposti dalla necessaria coincidenza temporale di domanda e offerta. In altre parole, a condizione che lo strumento utilizzato riesca a conservare il proprio valore nel tempo, si rende possibile l'intermediazione degli scambi e dei trasferimenti di ricchezza nel tempo.

Ciò è vero in una certa misura, si noti bene, in qualsiasi caso, cioè anche quando il mezzo di scambio non sia *ab origine* strutturato nell'ottica di un utilizzo "intertemporale" di lunga durata: il semplice fatto che il bene sia scambiato non in ragione del suo valore di utilizzo immediato, ma perché suscettibile di essere *successivamente* scambiato, implica un differimento temporale tra il momento in cui si acquista la disponibilità di questo bene "*strumentale*" e il momento in cui il mezzo di scambio è "utilizzato" per ottenere un bene che soddisferà un bisogno della vita[103]. Evidenziando la componente di mera intermediazione tra la controprestazione offerta in cambio del mezzo di scambio e la controprestazione successivamente ricevuta in cambio della cessione del mezzo di scambio, si nota, quindi, un differimento temporale tra le due prestazioni che interessano direttamente beni in grado di soddisfare direttamente i bisogni della vita[104].

Ciò implica sempre, lo si può notare sin da ora, un certo grado di incompletezza informativa al momento della conclusione dello scambio – *rectius*, del contratto –, giacché il valore del *mezzo di scambio* è commisurato in funzione di un'aspettativa che

[103] Sulla base di questa generale osservazione si sviluppa la teoria della moneta come "credito", v. INGHAM, *The Nature of Money*, cit., *passim*, il quale a p. 6 riporta una citazione di Schumpeter secondo cui vi sarebbero solo due teorie sulla moneta degne di questo nome: la *commodity theory* e la *claim theory*, peraltro incompatibili tra loro.

[104] Cfr. STAMMATI, op. cit., p. 747, che descrive la funzione di accumulazione di potere d'acquisto della moneta in diretta connessione con la funzione di intermediazione degli scambi ed osserva: "*poiché generalmente le operazioni di compra e vendita di moneta non sono contemporanee, sorge spontaneamente la tendenza a custodire una certa quantità di moneta in vista di future necessità od opportunità*".

concerne un tempo futuro e quindi, per definizione, è incerta[105]. In altre parole, la proiezione del valore di scambio futuro atteso al momento della conclusione del contratto fa sorgere il problema, ineludibile in un contesto di intermediazione tra scambi non simultanei, dell'intertemporalità tra la rinuncia al godimento o alla disponibilità di un bene della vita che si patisce nel momento in cui si acquisisce il mezzo di scambio e la soddisfazione del bisogno della vita che si ottiene al momento della differita cessione del messo di scambio. Tale differimento comporta un rischio relativo al perimento o alla modificazione di valore del mezzo di scambio che non è possibile prevedere perfettamente, a fronte del quale ci si trova, quindi, sempre, strutturalmente, in una posizione di incompletezza informativa. Specificatamente, ogni qualvolta si accetta un mezzo di scambio si accetta il rischio che nel tempo che intercorre tra tale accettazione e l'utilizzo in un rapporto futuro il valore di scambio dello stesso possa variare: in altre parole, si manifesta sempre la questione di come sia possibile sapere se la comunità continuerà ad accettare tale strumento come mezzo di scambio anche nel futuro.

Quanto appena detto, vale, in egual misura, in qualsiasi scambio di tipo monetario, in cui il sinallagma è definito con riferimento ad un bene che è valutato oggi in funzione del valore di scambio futuro atteso. Nel contesto di merci utilizzate come mezzi di scambio, *ivi* inclusi i sistemi monetari in cui i mezzi di pagamento sono costituiti da merci – c.d. "moneta–merce" –, il rischio appena descritto è mitigato dal fatto che lo stesso bene esercita due funzioni: di scambio e d'uso; sicché, anche qualora non sia più possibile utilizzare il bene come mezzo di scambio, rimane comunque il suo valore d'uso[106]. Ciò non toglie, tuttavia, che permane anche nel contesto della moneta–merce un regime di incompletezza informativa relativamente alla valutazione del valore di scambio atteso del mezzo di pagamento.

---

[105] Il punto sarà ripresto in più momenti nel corso dei prossimi paragrafi. Sulla determinazione della quantità di moneta in funzione del suo valore futuro e sull'importanza del mantenimento del valore cfr. GIANNINI, op. cit., p. 55 "*la qualità di un'unità nominale di moneta dipende dal suo prezzo di vendita al momento in cui verrà spesa*".

[106] Un esempio chiarissimo di commistione tra funzione di scambio e utilizzo secondo il valore d'uso proprio è del bene è dato dal racconto di RADFORD R.A., *The economic organization of a POW camp*, in *Economica*, 1945, 189, in cui si descrive l'utilizzo di sigarette come moneta–merce.

Ancora sul tema in esame, si noti che l'uso del mezzo di scambio secondo lo schema appena descritto rende possibile l'effetto del differimento temporale delle prestazioni che nel diritto civile è reso possibile dalla previsione di un termine, con la differenza che nel caso del diritto civile il rapporto è interamente definito a monte, mentre nel contesto dell'intermediazione degli scambi è possibile che il secondo momento – cessione del mezzo di scambio in cambio di un bene della vita – sia definito in un tempo diverso e con una controparte diversa. La similitudine tra i due meccanismi è, quindi, molto limitata, eppure è utile sin da ora apprezzare che il differimento tra le due prestazioni "reali" reso possibile dal mezzo di scambio (e più in generale dalla moneta) sia paragonabile alla nozione civilistica di credito, inteso non nell'accezione finanziaria di mutuo di una somma fungibile di denaro, bensì come componente attiva di un rapporto obbligatorio che viene in essere tra il momento dell'assunzione dell'obbligo e il momento dell'adempimento dello stesso. Prendendo spunto da tale similitudine taluni autori hanno immaginato e provato a definire la moneta come un credito nei confronti della comunità nel suo insieme[107]. Sul punto si tornerà in seguito, quando si tratterà per brevi cenni il rapporto tra credito e moneta.

La diffusione dell'uso del mezzo di scambio e la conseguente misurazione del valore dei beni scambiati nel mercato

In sintesi, nei paragrafi precedenti soso state svolte alcune riflessioni inerenti la definizione della moneta come mezzo di scambio universale che svolge una funzione di intermediazione di scambi secondo lo schema: merce–denaro–merce. In particolare, si è evidenziato che l'acquisizione di un bene in ragione della possibilità di utilizzare lo stesso come merce di scambio in rapporti futuri evidenzia il fatto che l'uso di un mezzo di scambio (e ancor più della moneta, come si vedrà) è sempre legato ad un contesto sociale all'interno del quale tale strumento conserva un certo valore (di scambio). Inoltre, si è osservato che tale attributo di *riserva di valore* può essere declinato secondo due prospettive: una prospettiva diacronica (di conservazione del valore nel tempo), e una

[107] Per tutti, INGHAM, *The Nature of Money*, cit., p. 47 e 72.

prospettiva di tipo geografico–sociale (ambito della collettività entro cui si riconosce a tale strumento un certo valore di scambio).

A quanto anzi detto si aggiunge ora che l'uso diffuso di un mezzo di scambio permette non solo di ampliare l'orizzonte economico in virtù dell'abbattimento dei costi transattivi, ma anche di comparare tra loro i vari beni scambiati nel circuito economico.

Si torni a concentrarsi sul fatto che il contesto del mezzo di scambio è caratterizzato da una dinamica in cui due parti trasferiscono una parte del loro patrimonio non in ragione del valore d'uso che deriva immediatamente all'*accipiens*, bensì perché essi riconoscono al bene scambiato l'attributo di poter essere utilizzato di nuovo in futuro come contropartita per un ulteriore scambio. Nel sinallagma si riconosce quindi un valore economico che per quanto sia ancora atteso (giacché l'interesse della vita sarà realizzato solo quando tale bene sarà scambiato con altro bene avente valore d'uso) è già misurato e corrisponde al valore economico della controprestazione. Si è detto, altresì, che il bene scambiato in ragione del suo valore di scambio sarà adoperato in ulteriori operazioni: non si potrebbe, altrimenti, parlare di valore di scambio. In ciascuna di queste operazioni, sino ad ora prese in considerazione atomisticamente, si ripete un giudizio sulla equivalenza tra la prestazione adempiuta con la consegna del bene cui è riconosciuto valore di scambio e la controprestazione. Lasciando allora il livello atomistico del duplice scambio merce–moneta–merce per volgere lo sguardo al fenomeno d'insieme comprendendo tutti gli scambi svolti all'interno del gruppo sociale rilevante ai fini dell'analisi, si coglie che l'uso di un unico mezzo di scambio in più rapporti ha un duplice simultaneo effetto: (*i*) di definizione del rapporto tra ciascun bene scambiato e il mezzo di scambio, così concorrendo alla definizione nei termini di un'unica unità di misura del valore economico di dei beni scambiati nel mercato, nonché, simultaneamente, (*ii*) di definizione, questa volta in termini reali, del valore di scambio del bene utilizzato come mezzo di scambio, valore che, in astratto, può differire, dal suo valore d'uso (sul punto *infra*). La diffusione estrema di un mezzo di scambio nel mercato a la sua inclusione a livello universale in qualsiasi scambio comporta, altrimenti detto, che ad ogni bene scambiato sia associato un valore economico espresso nei termini del mezzo di scambio: il mercato adotta, in questo modo, un'unità di conto e il mezzo di scambio diviene mezzo di pagamento.

Il passaggio chiave in questo processo è la trasformazione del mezzo di scambio da mero strumento di intermediazione degli scambi a strumento che permette di comparare il valore delle merci tra loro. Per effetto di questa trasformazione, il mezzo di scambio acquista la capacità di rappresentare il valore di un numero svariato di altre merci secondo il particolare rapporto di equivalenza che viene a crearsi tra i due termini dello scambio sinallagmatico: *id est*, il mercato inizia a dare un prezzo a ciascun bene. In questo contesto, la nozione di valore di scambio del bene utilizzato come mezzo di scambio universale – *rectius*, mezzo di pagamento – acquista maggiore pregnanza: l'agente è sempre confrontato con una la necessità di proiettare nel futuro della capacità di acquisto di tale strumento, ma poiché si diffondono all'interno dell'economia informazioni circa il valore dei vari beni espressi nei termini di tale mezzo di scambio/pagamento, la predizione che l'agente potrà fare potrà essere significativamente più accurata, il costo transattivo inferiore e lo scambio potrà essere più razionale. Resta, dunque, un regime di incompletezza informativa, ma esso è grandemente mitigato dal diverso grado di flussi informativi che conseguono all'utilizzo di un denominatore comune per la definizione dei trasferimenti di ricchezza.

Quanto al mezzo di scambio, esso non è più soltanto un mero strumento di intermediazione, ma acquista la particolare caratteristica di essere in relazione con il metro con cui si misura e compara il valore di tutti i beni sul mercato. Nel caso ipotizzato si verifica la coincidenza di due nozioni in capo allo stesso fenomeno, che in coerenza con l'approccio teorico anticipato nei primi paragrafi introduttivi del capitolo, si vogliono, però, tenere distinte dal punto di vista della teoria monetaria: la funzione di misurazione del valore dei beni, riconducibile alla nozione di «unità di conto» e la nozione di strumento di intermediazione degli scambi, che in questo contesto si ricollega alla nozione di «mezzo di pagamento». Riguardo questa seconda funzione v'è da chiedersi se davvero vi sia una differenza sostanziale tra il «mezzo di pagamento» e il «mezzo di scambio»: in entrambi i casi pare infatti possibile descrivere la dinamica di intermediazione nei termini di un duplice scambio merce–mezzo di scambio – merce, nel quale la merce utilizzata come mezzo di scambio è caratterizzata da un grado altissimo di liquidità. Al più, si potrebbe osservare che il fatto che il valore delle altre merci sia espresso nei termini di tale merce è garanzia del più alto grado di liquidità cui si è fatto

riferimento, per concludere che l'unica differenza tra il mezzo di scambio e le altre merci attenga proprio al grado di liquidità. Questo ordine di risposte è, però, solo parzialmente corretto. È vero, infatti, che anche nel contesto del mezzo di pagamento la funzione di intermediazione degli scambi può essere descritta nei termini di un duplice rapporto merce–mezzo di pagamento–merce ed è altresì vero che il bene utilizzato come mezzo di pagamento è altissimamente liquido, ma tale rassomiglianza non è strutturale e dipende dalla particolare circostanza per la quale nell'esempio sinora sviluppato v'è sostanziale coincidenza tra *unità di conto* e *mezzo di pagamento*, proprio perché si è assunto, *ab origine*, che il mezzo di pagamento utilizzato universalmente abbia acquisito *anche* la funzione di *unità di conto*. In un contesto economico in cui i valori patrimoniali sono espressi nei termini di un'unità di conto, sarebbe più corretto, dal punto di vista analitico, riproporre lo schema dell'intermediazione in termini del seguente schema merce–apprezzamento–mezzo di pagamento–apprezzamento–merce, che rispecchia il seguente processo: produzione di un bene, definizione del suo valore nei termini dell'unità di conto, cessione del bene contro un mezzo di pagamento che rappresenta quel determinato numero di unità di conto – definizione del valore di un altro bene in termini dell'unità di conto (che equivale a dire definizione del valore reale dell'unità di conto nei termini di un altro bene) – acquisto del bene contro un mezzo di pagamento di pari valore. Al momento dell'apprezzamento del bene coincide, dal punto di vista giuridico, l'assunzione dell'obbligazione di dare un certo numero di unità di conto, che viene estinta con la dazione del mezzo di pagamento. Ora, se il prezzo del bene è espresso direttamente nei termini di un certo numero di unità del mezzo di pagamento, allora v'è contestualità tra valutazione e pagamento e sostanziale coincidenza nei termini con cui è espressa l'obbligazione e le modalità del suo adempimento. Resta, però, una differenza nel grado di consapevolezza del valore di scambio del bene acquistato, in ragione dell'espressione del valore di tutti gli altri beni del mercato nei termini di quel bene, che permette in questo caso di assumere scelte razionali che riflettono un calcolo economico (v. *amplius infra* nei paragrafi dedicati all'unità di conto): la differenza, cioè, è che il mezzo di pagamento è in rapporto con l'unità di conto.

In altre parole, nel contesto di una società organizzata in modo semplice è plausibile immaginare che l'unità di conto coincida con il bene fisicamente utilizzato

nella maggior parte degli scambi, giacché ad esso è più facile, in virtù dell'uso diffuso, parametrare il valore di ogni altro bene. In tale ipotesi, il riferimento ad una determinata quantità del bene universalmente utilizzato negli scambi acquista un significato ulteriore e diverso rispetto al bene stesso che rimanda al valore economico corrispondente ai beni ottenibili mediante la sua cessione, giacché in virtù della perfetta corrispondenza tra unità di conto e bene utilizzato negli scambi, il riferimento linguistico a quel bene non rappresenta più soltanto il bene stesso, ma lo trascende e acquista significato a livello sistemico quale rappresentazione e misura del valore economico di ogni altro bene.

2.2.4. *Il mezzo di pagamento*

Alla luce delle considerazioni appena espresse, si definisce allora mezzo di pagamento lo strumento di intermediazione degli scambi rispetto al quale sussiste un rapporto tra il bene scambiato «*mezzo di pagamento*» e l''unità astratta utilizzata per comparare il valore dei beni sul mercato, «*unità di conto*».

Lo scambio monetario in cui un bene è ceduto contro un prezzo ha, dunque, una duplice dimensione: concernente l'appropriazione e il trasferimento di una specifica risorsa (moneta) e di attribuzione e riconoscimento del valore del bene in termini dell'unità di conto e dell'unità di conto in termini del bene reale. In entrambi i casi lo scambio monetario è sempre contestualizzato all'interno di un sistema più ampio nel quale è inserito e con il quale si trova in constante e reciproco dialogo. Si è già evidenziata la dimensione sociale del fenomeno di intermediazione degli scambi; nel contesto di un'economia monetaria che adotta un'unità di misura comune si può connotare con maggior dettaglio tale dialogo, chiarendo che ogni scambio monetario comporta un duplice flusso informativo: da un lato gli agenti economici definiscono il prezzo sulla base delle informazioni che ricevono dal mercato fornite dalle precedenti esperienze di scambio proprie e dei consociati e dalle offerte di scambio disponibili, dall'altro lato attraverso la propria definizione del prezzo al momento della conclusione di un contratto o in occasione di un offerta al pubblico o alla controparte, l'agente economico trasmette a sua volta al mercato un segnale riguardante il suo apprezzamento circa il rapporto tra valore monetario e valore economico del bene reale.

Questo "dialogo" che viene a crearsi tra agenti e collettività si realizza sostanzialmente attraverso la denominazione in unità di conto degli obblighi giuridici assunti (nel caso di scambi tra privati) o imposti (nel caso di obblighi imposti dallo Stato, in particolare sotto il profilo della raccolta delle tasse). Il fatto che i consociati possano dialogare tra loro utilizzando un unico linguaggio ci induce ad un ulteriore riflessione e a sottolineare che il ricorso ad un'unica unità di misura dei valori patrimoniali delle prestazioni è indice di un accordo, esplicito o fattuale, circa tale strumento di misurazione. Posto, inoltre, che tale unità di misura necessita di un'estrinsecazione nel mondo reale, può intuirsi facilmente che il consenso appena richiamato deve interessare anche le modalità attraverso le quali è possibile rappresentare e trasferire l'unità di conto. Nell'ipotesi di sostanziale coincidenza tra unità di conto e mezzo di pagamento è evidente che tale sarà il contenuto dell'accordo sotto questo particolare profilo: un accordo, quindi, piuttosto semplice, che coinvolge necessariamente una pluralità di soggetti, che non necessariamente acquista valore giuridico, ma che è pur sempre presente in qualsiasi scambio monetario e che per questo può essere definito come «*convenzione monetaria*».

Quanto alle modalità con le quali tale accordo è stipulato esse possono essere le più varie, per il momento si osservi che l'uso della moneta, intesa come mezzo di pagamento ed unità di conto, per comparare il valore economico dei beni e intermediarie gli scambi ne dà concreta attuazione: può quindi immaginarsi che nella forma più semplice, quella ipotizzata dall'ortodossia economica in cui gli uomini spontaneamente e senza l'intervento di istituzioni esterne iniziano ad utilizzare un particolare bene prima come mezzo di scambio universale e poi come moneta, l'accordo monetario assumerà quantomeno la forma della consuetudine sociale. Riprendendo il parallelismo prima svolto con la fonte consuetudinaria in senso giuridico, la convenzione sociale relativa all'uso di un mezzo di pagamento (e quindi di un'unità di conto) comporterà l'elemento della *diuturnitas*, ossia l'uso diffuso, non già quale mero intermediario degli scambi, ma anche come metro di misura dei diversi valori e di espressione delle obbligazioni giuridiche, e dell'*opinio pecuniae*, ovvero della *opinio permutationis et mensurae*: la convinzione e consapevolezza diffusa di scambiare un particolare bene in virtù del valore di scambio che riflette il potere d'acquisto atteso esprimibile nei termini di altri beni reali secondo il rapporto definito dal loro prezzo.

In questo contesto, l'uso del mezzo di pagamento per trasferire ricchezza concorre a consolidare e confermare la validità e l'importanza economica concreta dell'unità di conto e del consenso che si viene a creare intorno all'uso di tale unità per esprimere il valore delle prestazioni patrimoniali e determinarne giuridicamente il contenuto[108].

Incompletezza informativa nel contesto dello scambio monetario

Come nel caso dell'utilizzo del mezzo di scambio, anche con il mezzo di pagamento si assiste ad una dilazione temporale tra i due scambi oggetto di intermediazione monetaria. Si è evidenziato che in questo contesto il regime di incompletezza informativa è mitigato dall'esistenza di un meccanismo che permette di conoscere il prezzo degli altri beni. Si è ora inoltre notato che tale meccanismo di apprezzamento del valore dei beni sul mercato consegue ad un accordo che viene in essere tra i consociati circa l'uso di un metro di riferimento comune. Il problema dell'incompletezza informativa può dunque essere espresso sia con riferimento alla moneta in quanto mezzo di pagamento concretamente utilizzato per l'intermediazione degli scambi sia con riferimento alla moneta in quanto unità di conto, sia da ultimo, con riferimento al contenuto dell'accordo monetario circa le modalità di rappresentazione dell'unità di conto da parte del mezzo di pagamento. In ciascuno di questi casi il problema è riconducibile al rischio che la moneta, cioè lo strumento utilizzato per la misurazione e l'intermediazione degli scambi, perda il potere d'acquisto che si era immaginato avrebbe conservato, ma nel contesto di un'economia monetaria tale rischio può dipendere non solo dall'eventualità che il mezzo di pagamento deperisca o che vi sia un mutamento o un'errata valutazione delle preferenze dei consociati, ma anche che vi siano cambiamenti non previsti che interessano il rapporto tra unità astratta e mezzi di pagamento o relativi all'utilizzo dell'unità di conto stessa.

---

[108] PINI, op. cit., p. 64: "*posto che il denaro e uno strumento di scambio e che presenta una utilità meramente eminentemente circolatoria, ho affermato sopra che normalmente la norma statale riconosce la qualità di denaro al bene che convenzionalmente svolge la funzione di scambio all'interno di una comunità, accettando la determinazione di denaro che nella realtà dei fatti è riscontrata, limitandosi a porre le regole applicabili al denaro. Il mezzo di scambio convenzionale (denaro) in forza dell'intervento pubblico in forme di prescrizione normativa assume così la qualità di mezzo di scambio ufficiale di un certo stato (moneta legale o valuta)*".

Se ci si limita a riflettere su queste considerazioni con riferimento al caso teorico in cui i consociati spontaneamente convergano verso l'utilizzo di un certo bene come unità di misura e mezzo di pagamento e definiscano in modo stabile e difficilmente modificabile il rapporto tra questi, la specificazione anzidetta può apparire tediosa ed inconferente. È però vero che l'esistenza di una convenzione per un verso diminuisce l'asimmetria informativa offrendo un unico denominatore, ma per un altro verso offre l'opportunità di incidere sull'intero sistema di scambi a chi abbia sufficiente potere per imporre una modifica dei termini che definiscono tale denominatore comune e il suo uso concreto negli scambi. Si rifletta, cioè, sul caso in cui la convenzione monetaria sia determinata e decisa da un soggetto sovrano capace di imporre arbitrariamente l'uso di un certo mezzo di pagamento o di variare il rapporto tra l'unità di conto in cui sono espresse le obbligazioni giuridiche che gravano sulle parti e i mezzi di pagamento attraverso i quali tali obbligazioni possono essere adempiute. La storia della moneta medievale, in cui per un lungo periodo la separazione tra unità di conto e mezzi di pagamento è stata netta ed ufficiale, offre molti spunti per evidenziare come l'espressione di un comportamento sociale all'interno di paradigma codificato da un lato agevoli i rapporti tra i consociati riducendo i costi transattivi dello scambio, dall'altro esponga al rischio di comportamenti opportunistici da parte di chi è in grado di incidere sulla determinazione del contenuto delle modalità di esecuzione della convenzione monetaria (siano essi i principi o i banchieri che con essi hanno rapporti). Il problema appena descritto acquista ancora più rilevanza nel contesto di un'economia monetaria in cui si faccia ricorso a mezzi di pagamento astratti e la cui produzione non sia limitata dalla contingenza delle scorte fisiche di un certo materiale ed è proprio sul tema dell'uso opportunistico da parte dei governi del potere di determinare il contenuto della convenzione monetaria che si concentrano le critiche della scuola dell'economia monetaria neo–classica austriaca.

Si noti, da ultimo, che l'incompletezza informativa di cui si è appena trattato partendo dall'analisi dell'uso della moneta nel contesto degli scambi, in particolare sotto il profilo dell'intermediazione degli scambi, finisce con l'essere ricollegata direttamente alla dimensione del rapporto tra unità di conto e valori reali e alla capacità del sistema di conservare valore nel tempo ed investe, così, il fenomeno monetario nella sua interezza.

2.3. Il lato astratto della moneta: unità di conto, mezzi di pagamento astratti e credito

2.3.1. *L'Unità di conto e i vantaggi dell'astrazione numerica*

Al centro delle considerazioni sopra esposte c'è, quindi, la nozione di "unità di conto": l'unità astratta, espressa in termini numerici, utilizzata all'interno di un corpo sociale come referente per la misurazione del valore economico dei beni del mercato, ovvero, in termini più generali, per misurare il valore patrimoniale delle prestazioni assunte o imposte dalla legge[109].

L'attributo più importante dell'unità di conto è proprio il fatto che essa sia una "unità", cioè sia espressa in numeri. Ciò permette sia la riduzione della complessità ed eterogeneità del mondo ad una dimensione di perfetta astratta omogeneità e comparabilità in cui si ha un solo grado di differenziazione quantitativa e non qualitativa, sia la gestione di tali valori attraverso calcoli matematici, cioè attraverso procedimenti astratti e logici[110]. La combinazione di questi due elementi consente l'introduzione di criteri di gestione delle risorse di tipo razionale, nell'accezione weberiana del termine «razionalità», cioè opposta alla qualificazione dei rapporti tra soggetti secondo logiche non economiche, ad un livello altrimenti inimmaginabile[111]. È il calcolo monetario, cioè il calcolo su basi matematiche reso possibile dalla misurazione dei valori dei beni, delle prestazioni e più in generale degli obblighi giuridici, che rende possibile l'organizzazione della società e dei modi di produzione e distribuzione delle risorse secondo logiche che non sono più dettate dall'appartenenza ad un certo gruppo sociale, ma concernono uomini liberi e uguali che orientano le proprie scelte secondo criteri di ottimizzazione della soddisfazione delle

---

[109] V. INZITARI, op. cit., p. 20: "*L'unità di misura dei valori non è altro, dunque, che un indice di rapporto matematico che consente di confrontare tra loro vari patrimoni reali (espressi in beni o prestazioni più diverse)*".

[110] Le potenzialità dell'uso di numeri astratti nella finanza acquista poi un significato ancora più pregnante con l'avvento della informatizzazione e l'aumento esponenziale delle capacità di calcolo degli operatori finanziari: sul punto, in relazione anche alla produzione di strumenti para–monetari, v. GALLINO L., *Finanzcapitalismo, la civiltà del denaro in crisi*, Einaudi, 2011.

[111] Sul concetto di razionalità weberiana nei termini di *calcolabilità monetaria* e in generale sull'applicazione di tale nozione allo studio del fenomeno monetario v. BARCELLONA E., op. cit., pp. 10 e 27 ss.

proprie preferenze e, quindi, dell'efficienza[112]. Ciò significia che l'*homo aequalis* occidentale può diventare *homo oeconomicus* perché ha acquisito uno strumento che permette di confrontare diverse possibilità di azione tra loro e scegliere, razionalmente, cioè secondo criteri matematici, quella che permette di conseguire il maggior profitto e di massimizzare la propria utilità. Ciò non solo nel contesto del consumo e cioè della scelta tra prodotti diversi, ma anche nel quadro dell'organizzazione della produzione secondo criteri di sostenibilità economica: si pensi, a questo proposito, all'invenzione del bilancio e all'importanza di esso nello sviluppo del diritto commerciale e nell'organizzazione delle attività produttive. L'invenzione dell'unità di conto è, dunque, essenziale alla nascita e allo sviluppo del mercato e del capitalismo e, più in generale, per la gestione razionale secondo criteri economici delle risorse[113].

Secondo attributo dell'unità di conto, implicitamente connesso e direttamente rapportabile al primo appena evidenziato, è quello dell'astrattezza, senza la quale non sarebbe, ovviamente, possibile parlare di calcolo monetario nei termini sopradescritti: essa permette, infatti, di fare ricorso all'unità monetaria ben oltre i limiti naturali connessi alla presenza di referenti fisici che la rappresentano e incorporano nella vita reale. Tale strumento, così, può essere utilizzato in qualsiasi situazione indipendentemente dalla concreta presenza fisica dei corrispettivi mezzi di pagamento: due parti possono trasmettersi informazioni riguardanti il valore di un bene esprimendolo in un euro senza che occorra la presenza fisica di una o più monete da un euro. L'astrazione dell'unità di conto permette, in particolare, di utilizzare tale unità per definire il contenuto prescrittivo di relazioni di soggezione giuridica tra consociati, sia per il lato attivo, i crediti, sia per quanto riguarda il lato passivo, i debiti.

A proposito delle relazioni di credito e debito protette dal diritto, si è prima evidenziato che l'apposizione di clausole di termine insieme al collegamento tra negozi

---

[112] In senso critico, FELIX, op. cit., p. 157: "*It is a social technology which depends on other people. Yet it is a social technology which isolates us from other people, by transforming the rich and varied ecology of human relationships into the mechanical and monotonous clockwork of financial relationships*".

[113] Cfr. OLIVECRONA, op. cit., p. 317, il quale sottolinea altresì l'importante connessione tra diritto e unità di conto (su cui v. *infra*): "*La fittizia unità monetaria è una meravigliosa invenzione, comparabile al simbolo che indica lo zero nel sistema dei numeri arabi: senza di essa non sarebbe possibile l'economia dell'età industriale; il suo uso, d'altra parte, presuppone il sistema giuridico altamente sviluppato dello Stato industriale e la sua vasta rete di organizzazione bancaria*".

giuridici diversi permette, seppur con alti costi transattivi, astrattamente, di facilitare l'intermediazione degli scambi superando il limite della contestuale compresenza di interessi opposti. Con l'introduzione dell'unità di conto e la denominazione dei rapporti di credito e debito nei termini di tale unità, accade che una molteplicità di rapporti sono ora espressi nei termini di un'unica unità, o comunque in termini direttamente rapportabili a tale unità[114], e per effetto dell'omogeneità che ne deriva possono essere compensati tra loro. Attraverso l'istituto della compensazione del credito, applicato in contesti di iterazioni plurisoggettive mediante l'istituzione di apposite camere di compensazione, è possibile ampliare il volume degli scambi oltre il limite fisico che sarebbe altrimenti imposto nell'ipotesi in cui a ciascuno scambio monetario dovesse corrispondere la concreta dazione del mezzo di pagamento corrispondente. È questo il meccanismo applicato nel contesto delle fiere medievali, durante le quali si concludevano contratti nei quali l'esecuzione delle obbligazioni pecuniarie restava sospesa sino al termine della fiera, quando i commercianti eseguivano le opportune compensazioni[115].

Da quanto appena esposto osserviamo che con l'aumentare del grado di astrazione del sistema monetario, aumenta la possibilità di uso dello stesso e quindi il volume complessivo massimo degli scambi. In questo contesto il diritto gioca un ruolo importantissimo: in primo luogo, perché la compensazione è uno strumento giuridico che opera solo laddove esista un sistema giuridico che ne permetta l'utilizzo[116]; in secondo

---

[114] Non ci si vuole qui soffermare sul problema della qualificazione delle obbligazioni pecuniarie, è sufficiente quindi evidenziare che l'obbligazione assunta nei termini di dazione di un mezzo di pagamento secondo una certa quantità è direttamente rapportabile all'unità di conto e quindi compensabile con obbligazioni di segno opposto. In proposito può invece osservarsi che il meccanismo di compensazione può astrattamente operare anche in un contesto in cui si fa ricorso a mezzi di scambio: la differenza è, però, che solo se tale mezzo è utilizzato in modo diffuso al punto da divenire misura (cioè espressione numerica) degli scambi è possibile organizzare camere di compensazione, e in quest'ultimo caso si avrebbe a che fare con un mezzo di pagamento, non di scambio.

[115] Cfr. BARCELLONA E., op. cit..

[116] Cfr. i commenti di OLIVECRONA, op. cit., p. 316 sull'importanza del diritto nel contesto degli scambi moderni dove circolano soprattutto crediti bancari: "*l'assumere debiti attraverso promesse e il pagarli sono azioni che, secondo le nostre idee e con riguardo ai loro pratici effetti, sono correlate: stando a quanto pensiamo e diciamo, si promette che un certo giorno si trasferirà una somma di unità ideali, e si adempie la promessa cedendo i simboli delle unità o facendo eseguire ad una banca il diretto trasferimento della somma di unità al creditore. L'effetto pratico della promessa è di instaurare uno stato di soggezione per il promittente; l'effetto del pagamento è liberarlo*". Sull'utilizzo di crediti come mezzo di pagamento v. *infra*.

luogo, perché dalla certezza ed effettività del diritto, in particolare delle obbligazioni, dipende la fiducia dei consociati nel sistema di compensazione e, per l'effetto, nell'uso di un mezzo di misurazione del valore che acquisisce connotati sempre più astratti, non solo per quanto riguarda la misura e l'assunzione di obbligazioni, ma anche per quanto riguarda il loro adempimento. Si noti, cioè, che in questo contesto il diritto esplica una funzione importante, non già nella definizione dell'unità di conto, quanto nel sostenere in piedi il sistema che permette di utilizzare quell'unità di conto oltre i limiti strutturali fisici imposti dalla (probabile) scarsità del bene utilizzato come per rappresentare nel mondo reale l'unità di conto.

Laddove vi siano soggetti particolarmente affidabili dal punto di vista dello *standing* finanziario, cioè meritevoli di fiducia nel tempo, il credito denominato in moneta (*unità di conto*) nei loro confronti può essere usato a sua volta come quasi–moneta (*rectius*, come quasi–mezzo di pagamento). Nell'ipotesi in cui non siano riscossi, tali crediti possono infatti circolare tra gli agenti economici ed essere accettati come adempimento di obbligazioni pecuniarie. Questo è il modello teorico intorno al quale sono creati i mezzi di pagamento caratterizzati da un più alto grado di astrazione (come per esempio la cartamoneta o i crediti bancari), che permettono di estrinsecare e rappresentare nel mondo reale nei rapporti tra consociati il possesso (e la dazione) di un certo numero di unità di conto senza che vi sia corrispondenza tra l'unità di conto e il bene fisico o addirittura senza alcun bene fisico, operando squisitamente sul piano dei rapporti giuridici. Sul punto si tornerà a breve.

2.3.2. *Il limite dell'astrazione: il valore reale dell'unità di conto*

Contraltare dell'astrazione che caratterizza l'unità di conto è il fatto che, proprio perché astratta, essa non ha alcun valore intrinseco. In tema di valore economico della moneta si potrebbero scrivere enciclopedie, in questo contesto, preme soltanto ritornare sulla contraddizione strutturale di fondo che segna l'uso di un misuratore dei valori degli altri beni, che si manifesta sia nel contesto della moneta–merce, sia nelle forme monetarie più astratte, ogni qualvolta la moneta eserciti la funzione di misurazione del valore economico degli altri beni e a questi sia attribuito un prezzo: l'unità di conto misura il valore di scambio degli altri beni, ma cosa determina il valore di scambio del

"misuratore"? L'unità di conto astratta non ha alcun valore in sé, l'unico valore economico che le può essere riconosciuto è quello attribuitole nel contesto degli scambi[117].

Il tema è stato già anticipato nel corso dell'introduzione, dove si è evidenziato il rapporto circolare tra *mensura* e *mensuratum* (in senso più ampio di quanto tradizionalmente discusso) per concludere che se è vero, come anzidetto, che la presenza dell'astrazione e l'esercizio della funzione monetaria dell'unità di conto è essenziale per lo sviluppo del mercato, è altrettanto vero che l'unità di conto non può svolgere tali importanti funzioni se non nella misura in cui essa trovi al contempo concretizzazione nel mondo reale attraverso uno o più mezzi di pagamento, che ne permettano la rappresentazione in termini patrimoniali e quindi l'appropriazione e il trasferimento il termini giuridicamente validi.

Ciò rende ancor più difficile la distinzione tra unità di conto e mezzo di pagamento nel contesto della moneta–merce, in cui una merce altamente liquida è al tempo stesso mezzo di pagamento e referente diretto dell'unità di conto ed è quindi difficile giustificare la differenza tra quello che è stato chiamato il valore estrinseco, anche detto valore nominale, cioè le unità di conto rappresentate da un certo pezzo monetario, e il valore intrinseco, cioè il valore sul mercato della quantità di metallo utilizzata per realizzare tale pezzo. A tale difficoltà di distinzione possono essere quindi ricondotte le ragioni della scuola metallista, secondo la quale v'è coincidenza tra moneta è il metallo prezioso con il quale essa è coniata e tra i due valori, estrinseco ed intrinseco, prevale sempre il secondo[118].

Opposte conclusioni invece sono raggiunte dagli economisti classici i quali proprio in virtù della funzione di intermediazione della moneta e della relatività del valore

---

117 ASCARELLI, *Obbligazioni pecuniarie*, *cit*..

118 Sul punto, PINI, op. cit., p. 28: "*contestualmente, il denaro veniva tuttavia concepito dagli studiosi anche* ***come una merce*** *in relazione al metallo contenuto, e da qui partirà la reazione alla dottrina feudale della moneta […] Con Bartolo [sec. XIII-XIV] viene affermata l'identificazione del denaro col metallo; il valore del denaro è quello del metallo con cui è coniato: infatti, se il denaro è uno strumento di scambio e, come sostenevano gli aristotelici, nello scambio deve essere assicurata l'equivalenza delle prestazioni, è necessario che la moneta abbia un valore, che è appunto quello del metallo con cui è coniata. Ne consegue* ***la prevalenza del valore intrinseco del denaro sul valore estrinseco****, del valore metallico su quella nominale*".

dell'unità di conto deducono la neutralità della moneta rispetto ai valori reali di tutti i beni. A tale conclusione si può opporre, però, che se è vero che l'unità di conto non ha di per sé alcun valore, la rappresentazione della stessa nei mezzi di pagamento ne permette l'accumulazione e ne regola la distribuzione ed alterazioni della distribuzione o quantità di mezzi di pagamento disponibili, così come la previsione di simili variazioni, possono provocare modifiche del valore di scambio dell'unità di conto. L'esempio più semplice attiene proprio alla definizione della quantità di mezzi di pagamento in circolazione nell'economia, cioè al tema della produzione della moneta. Il punto è che mentre l'unità di conto acquista valore reale sono in termini relazionali, il mezzo di pagamento esercita una funzione concreta di incorporazione di valore economico e per questo acquista, in modo molto particolare, un proprio valore "d'uso". L'agente economico avrà, infatti, interesse ad acquistare la proprietà di mezzi di pagamento, vuoi per poter mantenerne una scorta a disposizione per far fronte all'incertezza del futuro (si rimanda sul punto agli studi di Keynes e a quanto già anticipato in tema di liquidità), vuoi perché ne ha bisogno per definire degli scambi con altri agenti. In entrambi i casi viene a crearsi una domanda dei mezzi di pagamento.

A tale domanda corrisponde un'offerta, le cui forme dipendono dai termini della convenzione monetaria. Applicando le teorie macro economiche alla moneta (per noi intesa come mezzi di pagamento, cioè alla moneta estrinsecata nella realtà e distribuita tra i consociati) e ritenendo che la moneta, come tutte le altre merci, sia soggetta alle leggi della domanda e dell'offerta, la scuola di pensiero che si rifà agli economisti classici e neo–classici e alla scuola austriaca ha elaborato la teoria quantitativa della moneta, da cui si evince che una variazione della domanda o nell'offerta può causare una modifica del "prezzo" della moneta (mezzo di pagamento) stessa. Essendo l'unità di conto in rapporto diretto con i mezzi di pagamento, tale modifica del "prezzo", cioè del valore di scambio dei mezzi di pagamento, o si ripercuote sul rapporto tra unità di conto e mezzo di pagamento (è il caso della svalutazione o rivalutazione legale della moneta), o si ripercuote direttamente sul valore dell'unità di conto concretizzandosi in una modifica, in termini reali, del valore sia del mezzo di pagamento, sia dell'unità di conto (è questo, invece, il caso dell'inflazione e della deflazione).

Si noti, peraltro, come non sia concepibile la creazione di un mezzo di pagamento che non abbia caratteristiche di scarsità, se non a costo di rendere del tutto incerta, e quindi insignificante, la nozione di unità di conto. Si rammenti, in proposito, che al momento dello scambio monetario la definizione del rapporto tra mezzo di pagamento/unità di conto e merce, ciò che viene in rilievo è il valore di scambio futuro atteso dell'unità di conto. Per tale ragione è essenziale che la quantità del mezzo di pagamento disponibile sul mercato sia limitata, cioè scarsa, cioè non sia possibile per il *quisque de populo* appropriarsi di nuove unità monetarie, se non al costo di compromettere la fiducia nel valore futuro del bene. In altri termini, la scarsità dei mezzi di pagamento è un attributo che contribuisce a sostenere la fiducia.

Posto, allora che lo stock di moneta (cioè la quantità di mezzi di pagamento) in circolazione in un dato momento storico abbia una certa dimensione, da quanto appena detto si deduce che al variare dell'offerta in termini accrescitivi, cioè per esempio nel caso in cui vi sia un'iniezione di liquidità nel sistema (la scoperta di nuovi giacimenti o la produzione di nuovi certificati cui sia riconosciuto il valore di mezzi di pagamento), assumendo il rapporto tra unità di conto e mezzo di pagamento costante, il valore del mezzo di pagamento in termini reali dovrebbe diminuire, cioè dovrebbe verificarsi l'inflazione, con l'effetto che tutti i possessori di mezzi di pagamento si troverebbero ad essere più poveri in termini reali. Similmente, potrebbe darsi il caso in cui non sia l'offerta di moneta a cambiare, bensì la domanda. Si immagini, per esempio, una situazione di crescita degli scambi economici all'interno di un dato paese: con l'aumentare degli scambi cresce, inevitabilmente, anche la domanda di moneta. Qualora non sia possibile aumentare l'offerta di moneta (mezzi di pagamento), per esempio perché vincolata alla quantità disponibile di un certo metallo prezioso, l'effetto che si ha è di tipo deflazionistico. Il frequente verificarsi di situazioni di questo tipo, in cui la quantità di moneta in circolazione risultava inferiore rispetto alla domanda, ha spinto verso la creazione di sistemi compensativi alternativi all'utilizzo di mezzi di pagamento (quali i circuiti di compensazione che operavano nelle fiere medievali cui si è fatto prima riferimento) e di mezzi di pagamento caratterizzati da un più alto livello di astrazione, sui quali si tornerà a breve.

Il problema del valore dell'unità di conto calato nel contesto dell'incompletezza informativa dello scambio monetario

Si è detto che un cambiamento della domanda o nell'offerta dei mezzi di pagamento può comportare una modifica del valore: lo studio delle dinamiche connesse alla gestione dell'offerta di moneta è chiamato economia monetaria. In questo settore gli studi hanno sviluppato ulteriori considerazioni relative alle aspettative di azioni future. In estrema sintesi, occorre fare riferimento alla circostanza per cui il valore della moneta scambiata corrisponde, come si è detto, alla proiezione presente della sua capacità di acquisto futura. Sulla base di questa considerazione, dalla quale dipende la strutturale incompletezza informativa che contraddistingue lo scambio monetario, si è evidenziato che non occorre vi sia un effettivo mutamento dell'offerta o della domanda di moneta perché si verifichi un mutamento di valore, ma è sufficiente che tale cambiamento sia atteso da parte del pubblico. Secondo la teoria delle *rational expectations*, in altri termini, il comportamento degli agenti tiene conto delle variazioni macroeconomiche attese ed in particolare della previsione di modifiche nell'offerta di moneta: ciò rende ancora più complessa la gestione della politica monetaria.

Variazioni del valore e razionalità degli scambi

Come può conciliarsi il rischio che il valore reale dell'unità di misura cambi con la pretesa di organizzare la produzione e lo scambio di merci in modo razionale attraverso l'uso dell'unità di conto? Le due cose sono, invero, in tensione tra loro: l'inflazione o la deflazione di una moneta provocano spostamenti di ricchezza che non sono giustificabili dal punto di vista dell'allocazione ottimale delle risorse, con effetti distributivi che è difficile controllare e prevedere. La questione è che non può farsi altrimenti: il rischio di modifiche "irrazionali" del valore, che riflette la stessa questione sin qui proposta dal punto di vista dell'incompletezza informativa che caratterizza ogni scambio monetario, dipende ad un livello più generale, da quanto detto sul difficile equilibrio circolare tra

mensura e *mensuratum* e dal fatto che l'unità di conto non può, per definizione, data l'astrattezza, avere un valore intrinseco[119].

L'unità di conto offre, dunque, una razionalità economica limitata. Da un lato essa permette di comparare le grandezze tra loro e organizzare la produzione e l'allocazione delle risorse secondo criteri coerenti con l'obbiettivo della massimizzazione delle utilità personali. Dall'altro, vincolano l'attività economica all'uso di uno strumento il cui valore reale dipende da un meccanismo circolare di produzione e assunzione di prezzi, sul quale inoltre incidono le scelte inerenti l'organizzazione dei meccanismi di concreta estrinsecazione dell'unità di conto nella vita reale, cioè il sistema molto complesso di produzione e distribuzione dei mezzi di pagamento, che a sua volta interagisce con le aspettative future degli utilizzatori circa la capacità della moneta di conservare il proprio potere d'acquisto.

2.4. L'evoluzione del sistema di pagamento: il mezzo di pagamento astratto e le sfide che comporta

2.4.1. *Il mezzo di pagamento astratto*

Al quadro, già complesso, che si sta delineando, può essere ancora aggiunta qualche considerazione in merito alla creazione di mezzi di pagamento alternativi all'uso di merci scarse, che definiremo genericamente come mezzi di pagamento astratti, per evidenziare che alla creazione di tali strumenti corrisponde un più alto grado di astrazione del fenomeno monetario[120].

Inizialmente, lo si è detto, nella tradizione occidentale sono stati usati come mezzi di pagamento particolari metalli, rispetto ai quali la corrispondenza tra il valore del bene e il valore nominale attribuitogli era tale da far ritenere che il metallo fosse la moneta e viceversa. Questi mezzi di pagamento appartengono alla categoria della moneta–merce:

---

[119] Keynes mette in guardia molto chiaramente sul fatto che non si possa avere una moneta completamente isolata da qualsiasi fluttuazione, sicché per il grande economista la scelta concreta è tra meccanismi che più facilmente stimolano l'inflazione contro meccanismi che più facilmente stimolano deflazione; v. KEYNES, op. cit., p. 53.

[120] Ne sono esempio i mezzi di pagamento il cui valore è principalmente simbolico, come la cartamoneta convertibile e la cartamoneta non convertibile, e i mezzi di pagamento non materiali, quali la moneta elettronica e la moneta scritturale, che consiste in partite contabili su conti correnti bancari.

sistemi monetari in cui per l'intermediazione degli scambi e il trasferimento della ricchezza sono utilizzati merci cui è riconosciuto un valore d'uso o di consumo diverso dal valore di scambio. Un problema che però si è evidenziato nel contesto di questi sistemi è la ricorsiva mancanza di sufficiente metallo rispetto alla domanda di moneta: nelle parole di Giannini: "*l'innovazione monetaria nasce cioè dall'esigenza di contrastare la «deriva deflazionistica» insita in tecnologie di pagamento caratterizzate da un'offerta di moneta rigida, perlomeno nel breve–medio periodo*"[121]. Attraverso l'invenzione e poi l'impiego di mezzi di pagamento astratti è stato possibile incrementare in modo significativo l'offerta di moneta, da un lato rispondendo ai bisogni del mercato, dall'altro garantendo e consentendo l'espansione costante del ciclo produttivo capitalista attraverso l'offerta di crediti di lungo periodo per investimenti in produttività da parte delle banche[122].

Il grado di astrazione del mezzo di pagamento dipende dalla differenza che viene a crearsi tra valore intrinseco del bene utilizzato per rappresentare nella vita reale le unità di conto e il valore nominale delle stesse espresso in termini reali di potere d'acquisto, cioè il valore di scambio atteso delle unità di conto. Tale secondo valore dipende dalla convinzione diffusa di poter usare in futuro le unità incorporate in tale mezzo di scambio, cioè dalla fiducia che in qualsiasi sistema monetario i consociati devono riporre nello strumento utilizzato come mezzo di pagamento e nel valore futuro dell'unità di conto: la *opinio pecuniae, permutationis et mensurae*, cui si è fatto riferimento *supra*. Ne consegue che all'aumentare del grado di astrazione aumenta l'importanza della convenzione monetaria e della fiducia dei consociati nel sistema, e con esse l'importanza del diritto, quale fonte capace di regolare in modo autorevole ed affidabile il sistema monetario, sia

---

[121] GIANNINI, op. cit., p. 33. Tale carenza di mezzi di pagamento è peraltro spesso riconducibile con maggior precisione alla mancanza di disponibilità di moneta nelle casse del sovrano e al problema del finanziamento delle opere collettive e della ridistribuzione della ricchezza all'interno della società; cfr. DODD, op. cit., *passim*.

[122] Cfr. INGHAM G., *Schumpeter and Weber on the Institutions of Capitalism*, in *Journal of Classical Sociology*, 2003, pp. 297 e 302, che in merito all'interpretazione di Weber e Shumpeter da parte della sociologia contemporanea osserva: "*the sociological tradition […] completely ignore[s] the institutional source of dynamism that is central to Schumpeter's Theory of Economic Development and figures in Weber's General Economic History. Both saw that a* differentia specifica *of capitalism is the production of an elastic supply of credit-money by banks and states, without which entrepreneurial activity could not take place*".

sotto il profilo della costituzione e gestione di mezzi di pagamento astratti, sia per quanto concerne il sostegno di tale fiducia[123].

All'aumentare dell'astrazione del mezzo di pagamento, quindi, aumenta l'investimento istituzionale nel sistema di produzione e gestione della risorsa. Il che vale a dire che al vantaggio della maggiore flessibilità offerta dal sistema corrisponde quindi un maggior costo connesso alla necessità di mantenere la fiducia dei consociati nella capacità di acquisto dell'unità di conto, cioè nel valore nominale della moneta.

Entro tali costi devono essere compresi anche quelli connessi alla gestione del rischio di comportamenti opportunistici da parte di chi controlla l'emissione della moneta astratta.

Non più limitata dai limiti fisici della presenza in natura di un certo bene, l'emissione di mezzi di pagamento astrattati è ora soggetta soltanto alla convenzione che gestisce il sistema monetario o, ove applicabile alla legge e, in ultima analisi, dal rischio che i consociati cessino di riconoscere il valore astratto di scambio di tali strumenti. Il rischio assunto dai consociati in caso di fallimento del sistema è qui molto alto: nella moneta–merce questi rischi sono mitigati dalla presenza fisica del bene e dal fatto che esso ha un valore di scambio intrinseco; valore che non dipende dal sistema monetario e che quindi permane anche nell'ipotesi crisi sistemica della fiducia. Il valore del mezzo di pagamento astratto dipende completamente, invece, dal corretto e regolare funzionamento del sistema monetario e quindi, in ultima analisi, dal comportamento del soggetto che definisce ed è in grado di modificare i termini che regolano tale sistema, che nella maggior parte dei casi è lo Stato[124].

---

123 Importanza resa ancora più cogente dal fatto che il meccanismo istituzionale attraverso il quale sono stati creati mezzi di pagamento astratti è modellato sul rapporto di credito (v. *infra*). Sul punto, v. OLIVECRONA, op. cit., pp. 316–317. Sul punto cfr. anche GOODHART, op. cit., p. 417, il quale sottolinea che la teoria catallattica nella sua forma più pura non riesce a spiegare il passaggio dalle monete metalliche alla moneta astratta, cioè alla carta moneta privata o pubblica garantita da metalli preziosi e poi alla cartamoneta non garantita e conclude evidenziando il ruolo dello Stato in questi termini: "*Instead those notes were, and are, backed by the power of government (e.g. legal tender laws) and its ability to impose taxes payable (and often only payable in that fiat currency (as well as legal tender for the discharge of all other payments within the country)*".

124 GIANNINI, op. cit., p. 63 "*al crescere del grado di astrattezza del mezzo di pagamento, quindi del grado di specificità dell'investimento in scorte monetarie, i costi di produzione della fiducia inevitabilmente tenderanno ad aumentare, perché la moneta si trasforma da* un insieme di oggetti [corsivo originale]

2.4.2. *Astrazione e incompletezza informativa nello scambio monetario: il* trade off *tra flessibilità e stabilità*

La creazione di mezzi di pagamento astratti e la conseguente possibilità di espandere l'offerta e la presenza di moneta all'interno di una società con maggiore flessibilità necessità dell'intervento del diritto e per questo espone i consociati al rischio di comportamenti opportunistici da parte dello Stato. Ci si può chiedere, dunque, qual è l'effetto di tale dinamica di astrazione (o giuridificazione) dei mezzi di pagamento rispetto al regime di incompletezza informativo che si è visto caratterizzare qualsiasi scambio monetario.

Da un certo punto di vista, la maggiore astrazione comporta un aumento del rischio perché non v'è più valore intrinseco del bene, né vi è un limite fisico che possa contenere la produzione di nuovi mezzi di pagamento, la cui produzione è ora limitata solo dal diritto e dai termini della convenzione monetaria. L'importanza della definizione (ed eventuale modifica) di tali termini si acuisce e al contempo, a fronte dell'importanza che assume la regola organizzativa del sistema rispetto alla realtà materiale dei beni che esplicano la funzione di mezzo di pagamento, aumenta il potere di chi definisce tali regole e di chi gestisce l'emissione dei mezzi di pagamento astratti. Nel contesto dell'incompletezza informativa caratteristica dello scambio monetario assume così sempre maggiore importanza il rapporto *principle–agent* che si instaura tra l'emittente e l'utilizzatore della moneta, e la corrispondente asimmetria informativa riguardante i criteri di gestione del sistema monetario, le sue eventuali modifiche future e – nel caso di

---

in un insieme di diritti [corsivo originale], *che per essere fatti valere dovranno essere socialmente riconosciuti e protetti. Nel caso di una moneta intrinsecamente inutile ma convertibile, il vincolo è di natura giuridica, perché al crescere dell'offerta di moneta data domanda risulterà più arduo per il produttore onorare i propri doveri di convertibilità. Nel caso della moneta-segno, è di natura politica, perché l'unico vincolo è il controllo sul potere esecutivo, nelle varie forme più o meno democratiche che esso può assumere*"; e ancora più esplicito OLIVECRONA, op. cit., p. 317: "*Tra le norme sulle quali si fonda il sistema ve ne sono certe, giuridiche e di prudenza, concernenti la «creazione» del denaro da parte della banca centrale, il che avviene ampliando il credito allo Stato e alle Banche. Questo è il punto debole del sistema. La possibilità di creare denaro sufficiente per l'espansione dell'economia è un'inestimabile vantaggio, che* ***ha però il suo rovescio nella facilità con la quale troppo denaro viene creato****, con la conseguenza dell'inflazione, e da ultimo, la possibilità che l'intero sistema venga distrutto*".

mezzi di pagamento strutturati nella forma del credito – circa la affidabilità creditizia dell'emittente.

Al contempo, è vero altresì che il potere di influire sui termini della convenzione monetaria permette di ridurre l'incertezza circa i termini dell'accordo stesso e di adeguarla a contesti sociali ed economici in mutamento e di perseguire politiche ridistributive tra i consociati[125]. L'impiego di strumenti di politica monetaria al fine di preservare il valore della moneta nel tempo è un fattore di sostegno e correzione del regime di incompletezza informativa cui si è ripetutamente fatto riferimento e può concorrere a mitigare il rischio di fluttuazioni della moneta tutelando l'affidamento sul valore futuro della stessa.

Si presenta, quindi, una realtà duplice e contraddittoria, ben sintetizzata nelle parole di Giannini:

> *"alla radice della «questione monetaria» vi è una tensione logicamente irrisolvibile. Da un lato, sarebbe socialmente desiderabile che l'offerta di moneta fosse perfettamente adattabile, per azzerare i costi dell'inflessibilità. Dall'altro, non c'è presidio migliore contro il rischio di esproprio monetario della scelta di un bene moneta dall'offerta altamente rigida, dell'imposizione di vincoli legali alla creazione di moneta siamo in presenza di un tipico trade–off: tanto più è adattabile l'offerta di moneta, tanto maggiore è il rischio di comportamenti opportunistici da parte dei produttori di moneta, ma anche tanto maggiori spazi per una politica monetaria consapevole mirata all'interesse collettivo"*[126].

---

125 Cfr. HAYEK F.A., *Denationalisation of money. The argument refined : an analysis of the theory and practice of concurrent currencies*, The Institute of Economic Affairs, 2 ed. , 1978, pp. 23–24, il quale nel comparare l'ipotesi dell'offerta di più monete in concorrenza con quella del monopolio Statale della produzione di moneta riconosce quale vantaggio maggiore di questa seconda opzione l'effetto di ridurre i costi informativi che si dovrebbero altrimenti sopportare con una pluralità di monete, pur tuttavia ritenendo che il costo dell'inflazione dovuto al comportamento opportunistico dello Stato sia comunque superiore rispetto a tale beneficio.

126 GIANNINI, op. cit., p. 65.

2.4.3. *L'uso del credito come mezzo di pagamento astratto*

Con l'innovazione monetaria si è quindi cercato di creare dei mezzi di pagamento che permettessero maggiore flessibilità, in un crescendo di dematerializzazione che ha visto prima l'emissione di buoni convertibili in moneta metallica e poi biglietti di carta raffiguranti una certa quantità di unità di conto la cui produzione è gestita, sia per quanto concerne la concreta manifattura, sia per quanto concerne la quantità dei biglietti in circolazione, direttamente dal potere costituito, direttamente o, più spesso, attraverso gli uffici della banca centrale.

Il processo di progressiva astrazione è stato tale per cui oggi la moneta è sostanzialmente dematerializzata e circola principalmente nella forma del credito privato bancario[127].

Il principio teorico che fonda la creazione di mezzi di pagamento astrattati è quello già anticipato che sta alla base del rapporto di credito: l'assunzione di un debito denominato in unità di conto da parte di un soggetto verso un altro, instaura una posizione di soggezione che, a certe condizioni, può essere trasferita a accettata in luogo del trasferimento di un mezzo di pagamento reale. Il trasferimento del credito, dove consentito dal diritto, presenta però un inconveniente: il prenditore si deve accollare il rischio che il debitore non dia pronta esecuzione all'obbligazione nel momento in cui essa sia richiesta e l'eventuale esecuzione forzosa del credito comporta dei costi aggiuntivi e potrebbe non essere soddisfacente ove il patrimonio del debitore ceduto risulti incapiente. La mera cessione di un credito non può, quindi, essere equiparata *tout court* alla creazione di un nuovo mezzo di pagamento: da un punto di vista giuridico perché si tratta comunque di un rapporto giuridico instaurato nei confronti di un particolare emittente[128]; da un punto di vista economico perché a tali crediti è applicato un *discount* proporzionale al grado di rischio assunto e tale differenza tra valore di scambio e valore nominale del credito è indice del fatto che essi siano beni astratti prima che mere rappresentazioni dell'unità di

[127] Cfr. INZITARI, op. cit., pp. 22 ss., sulla dematerializzazione del denaro e la conseguente difficoltà di collocare la moneta nel sistema dei diritti reali.

[128] Sulla base di questa considerazione la dottrina per lungo tempo ha ritenuto il pagamento tramite bonifico bancario come un *aliud pro alio* dell'obbligazione di pagamento in pezzi monetari emessi dallo Stato. Cfr. FARENGA, op. cit..

conto. A simili conclusioni può giungersi quando qualora il rapporto di credito sorga non con l'obbiettivo tipico di regolare un rapporto bilaterale, eventualmente con effetti dilazionati nel tempo, ma con la consapevolezza che tale rapporto sarà oggetto di vicende transattive che coinvolgeranno soggetti terzi tra i quali il credito circolerà come strumento che incorpora un certo valore economico espresso in termini di unità di conto. È evidente, in questa seconda ipotesi, la somiglianza funzionale con la definizione data di mezzo di pagamento, eppure non v'è ancora perfetta coincidenza fintantoché si possa arrivare ad un momento in cui il debito sarà riscosso, lo strumento incorpori dunque un rischio di default e sia perciò possibile distinguere tra il valore nominale del debito/credito e il valore di scambio.

Un credito/debito può essere costituito al fine di creare uno strumento di intermediazione degli scambi solo se inserito all'interno di un circuito istituzionale in grado di offrire sufficiente affidabilità nel tempo: a tale strumento sarà riconosciuta la capacità di rappresentare un certo numero di unità di conto e sarà, quindi, accettato, in tanto in quanto si riterrà l'emittente affidabile da un punto di vista creditizio. Le banche e gli istituti di pegno hanno saputo convogliare nel pubblico un sufficiente grado di stabilità che ha permesso nel tempo l'emissione di note di credito, le prime banconote, liberamente trasferibili per l'esecuzione di pagamenti tra consociati.

L'istituzionalizzazione dei rapporti di credito e debito entro un circuito regolato da un certo *set* di regole è ciò che ha permesso la trasformazione di tali strumenti giuridici in mezzi di pagamento: l'effetto è che la fiducia personale relazionale tra emittente e prenditore di un certo strumento di debito viene sostituita da una fiducia impersonale che i partecipanti ripongono nel sistema[129].

Questo è il risultato che si è perseguito e raggiunto con la graduale costituzione di un sistema bancario regolato e garantito dallo Stato, le cui origini sono rinvenibili nel *great monetary settlment*[130] raggiunto tra la Banca d'Inghilterra e la corona inglese nel

[129] Cfr. INGHAM, *The Nature of Money*, cit., p. 187, secondo cui la creazione della fiducia impersonale e legittimità necessaria per l'estensione delle relazioni monetarie nel tempo e nello spazio è un compito che storicamente è sempre stato affidato allo Stato.

[130] Sul punto v. GIANNINI, op. cit., pp. 171 ss. e INGHAM, *The Nature of Money*, cit., pp. 128 ss. Non è questa la sede per dilungarsi sugli effetti distributivi e politici dell'accordo tra sistema bancario e Stato, sul quale, specie dopo la crisi del 2008, sono state scritte molte pagine critiche. Sul punto, per tutti,

tardo seicento e la cui organizzazione oggi si fonda sulla istituzione di una banca centrale indipendente cui sono affidati compiti di gestione della politica monetaria dello Stato, secondo lo schema efficacemente sintetizzato nella teoria istituzionale della moneta[131].

2.5. Il sistema monetario

Nell'analisi sin qui proposta, la funzione di intermediazione degli scambi tipicamente associata alla moneta, normalmente posta al centro delle letture del fenomeno monetario nelle scienze sociali, è stata riletta in modo critico al fine di evidenziare la dimensione sociale e istituzionale del fenomeno.

Si è provato, dunque, a proporre una distinzione tra l'ipotesi in cui un «mezzo di scambio» viene utilizzato per intermediare gli scambi in ragione della sua liquidità, e l'ipotesi in cui il valore dei beni scambiati sul mercato è generalmente espresso nei termini del bene utilizzato come intermediario degli scambi o di un'unità di misura direttamente rappresentata o estrinsecata da quel bene secondo un rapporto predefinito. Solo questa seconda ipotesi, che presuppone quindi l'emergere simultaneo di un'unità di conto e di uno o più mezzi di pagamento ad essa connessi, è stata riconosciuta come un sistema di scambi di tipo monetario.

Si è voluto così definire la presenza di una moneta nei termini di un'istituzione complessa composta, quantomeno, da un'unità di conto, un mezzo di pagamento e dalla definizione di una relazione tra essi, giungendo a conclusioni simili all'analisi proposta da Giannini di economia monetaria:

> *"perché si possa parlare di un'economia monetaria, occorre che siano soddisfatte tre condizioni. In primo luogo, ci deve essere un metro comune per valutare le merci, cioè un'unità di conto. In secondo luogo, devono esistere merci o procedure che consentono di estinguere qualunque*

GALLINO L., *Il denaro, il debito e la doppia crisi*, Einaudi, 2015. Da ultimo, cfr. l'efficace annotazione di FELIX, op. cit., p. 230: "*Fortunately, however, modern banks have friends in high places. Under the terms of the Great Monetary Settlement, a bank's liabilities, unlike the liabilities of normal companies, are an officially endorsed component of the national money supply. And since money is the central co-ordinating institution of the economy, any impairment of its transferability would impose grave costs on the whole of society—not just on the particular bank that issued it*".

131 Su cui v. *supra*. Cfr. anche STAMMATI, op. cit., p. 750 sulla differenza tra circolazione fiduciaria (credito bancario) e circolazione legale (moneta statale).

obbligazione derivi dallo scambio di merci, cioè uno o più mezzi di pagamento. […] Tra l'unità di conto è il mezzo (o i mezzi) di pagamento si dovrà poi stabilire una qualche relazione aritmetica, magari non rigidamente fissa ma quantomeno prevedibile. L'insieme delle merci, procedure e convenzioni che consentono di soddisfare queste tre condizioni è ciò che chiameremo una «tecnologia di pagamento»"[132].

La divisione concettuale della moneta in due componenti, riconosciuta già dalla dottrina statalista ed ulteriormente elaborata dalla teoria societaria della moneta, riflette due attributi del sistema monetario che si ritengono centrali nella comprensione e nella definizione della moneta e che sono:

(i) la capacità di misurare i patrimoni dei consociati secondo stime di valore che permettano di ragguagliare beni di tipo diverso tra loro e

(ii) la possibilità di rappresentare concretamente nella realtà l'appropriazione di unità di conto da parte dei consociati, il che a sua volta permette il trasferimento e l'immagazzinamento della risorsa.

In questo contesto teorico, si è evidenziato che l'esistenza di una moneta presuppone vi sia un insieme di regole, di natura giuridica o sociale, in base alle quali i consociati adottano una certa unità di conto come metro di misura delle prestazioni patrimoniali e riconoscono a determinati mezzi di pagamento la capacità di rappresentare tali unità nei rapporti tra loro: occorre cioè una convenzione monetaria che regoli l'istituzione 'moneta'[133].

Da questo primo insieme di considerazioni si trae la conclusione che nel parlare di moneta si fa sempre, in realtà, riferimento ad una istituzione complessa, che si articola in una serie di relazioni e di comportamenti regolati secondo la convenzione monetaria. La dimensione istituzionale del fenomeno suggerisce di concludere, dunque, che sarebbe più corretto e meno fuorviante parlare di "sistemi monetari" invece che di moneta[134].

---

132 GIANNINI, op. cit., p. 52.

133 FARENGA, op. cit., p. 31; INZITARI, op. cit., pp. 36 ss.; DI MAJO, *Le obbligazioni pecuniarie*, cit.; e cfr. OLIVECRONA, op. cit., p. 315.

134 Cfr. in proposito la nozione di "ordinamento valutario" in ASCARELLI, *Obbligazioni pecuniarie, cit*., p. 25, la quale però presuppone l'intervento dello Stato; e la nozione di "*sistema dei pagamenti*" proposta

La definizione di sistema monetario e di convenzione monetaria qui proposta richiama elementi teorici elaborati nel contesto delle teorie eterodosse della moneta, in particolare lo sviluppo in senso istituzionalista delle teorie societarie proposto da alcuni esponenti della dottrina italiana[135]. Da tale teoria il modello qui proposto si discosta, però, perché qui si è cercato di sottolineare ed estrapolare i complessi bilanciamenti sottesi all'organizzazione e alla gestione del fenomeno monetario senza dare per scontata e senza attribuire un ruolo centrale alla presenza dello Stato.

Si è evidenziato, inoltre, che in qualsiasi scambio monetario e in generale ogni qualvolta si stabilisce il controvalore monetario di una prestazione, di un bene o del risarcimento per un fatto illecito, si instaura una particolare relazione circolare inerente la definizione del valore reale dell'unità di conto nella quale le parti ricevono e a loro volta inviano informazioni al mercato circa il rapporto tra l'unità di conto e i beni reali. Si instaura, cioè, un dialogo tra i consociati che permette di attribuire ad ogni bene un prezzo e all'unità di conto un valore reale. Da questa particolare relazione discende l'importanza dell'uso di una moneta da parte dei consociati, la quale è, per converso, limite al potere di affermazione dispotico da parte di un sovrano di un certo mezzo monetario[136].

---

in CECCHETTI e SCHOENHOLTZ, op. cit., p. 26: "*The payments system is the web of arrangements that allow for the exchange of goods and services, as well as assets, among different people. Because the efficient operation of our economy depends on the payments system, a critical public policy concern is that it function well. As we will see in Part IV, that is why central banks are directly involved*". Si noti in proposito che nel nostro ordinamento la nozione di "Sistema di pagamento" ha un significato giuridico particolare ben più specifico che concerne l'organizzazione dell'attività di intermediazione dei pagamenti da parte di soggetti abilitati: v. art. 1, lett. d), D.Lgs. 27 gennaio 2010 , n. 11, *Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE*.

135 INZITARI, op. cit., pp. 36 ss.

136 Cfr. STAMMATI, op. cit., p. 748: "*La moneta, cioè, deve essere circondata dalla generale fiducia che essa è, e verrà generalmente accettata. «Tale generale accettabilità (continua il Newlyn) può costituire la risultante di molti fattori diversi operanti singolarmente o in combinazione tra loro; e rientra in quel discutibile e fascinoso gruppo di fenomeni che sono soggetti all'influenza di opinioni autogiustificantesi. Se i membri di una collettività pensano che la moneta sarà generalmente accettata, essa lo sarà; altrimenti non lo sarà». È quindi la collettività a decidere quale debba essere lo strumento prescelto come moneta, il quale non necessariamente si identifica con un bene reale, anzi generalmente, nel mondo moderno, se ne svincola completamente*".

In accordo con la teoria societaria della moneta si è concluso che l'uso dei mezzi di pagamento da parte dei consociati è essenziale per la definizione del valore reale dell'unità di conto e per mantenere e sostenere la fiducia dei consociati nel sistema monetario. Tale uso dipende da numerosi fattori, tra essi è importante la concreta disponibilità di mezzi di pagamento (c.d. presenza di liquidità all'interno del mercato), l'eventuale presenza di obblighi o sanzioni relativi al mancato uso (i.e. la minaccia del potere) e, ancor di più, la fiducia dei consociati nel funzionamento del sistema monetario ed in particolare nel valore futuro della moneta. Tale fiducia, infatti, è al tempo stesso sostenuta e rinforzata dall'uso, nonché presupposto dell'uso da parte dei consociati della moneta.

Il problema della fiducia è stato affrontato anche nell'ottica del problema di incompletezza informativa che discende dalla dimensione strutturalmente intertemporale dello scambio. La moneta, infatti, è uno strumento per il raggiungimento di fini ulteriori il cui perseguimento non può che essere successivo e conseguente all'appropriazione della moneta. Non è possibile, però, sapere con assoluta certezza al momento dell'appropriazione di risorse monetarie se e in che misura sarà possibile utilizzarle: la risposta a questo quesito dipende dalla capacità del sistema monetario di preservare il valore d'acquisto in termini reali corrispondente alle unità di conto acquisite. Da qui la strutturale incompletezza informativa che caratterizza l'uso di qualsiasi strumento monetario.

Poiché il valore e l'uso della moneta dipendono dalla aspettativa diffusa di poter utilizzare in futuro tale moneta per acquistare altri beni e servizi o comunque adempiere ad obbligazioni pecuniarie di qualsivoglia natura, cioè dipendono dalla anticipazione del valore d'acquisto futuro della moneta, e poiché è strutturalmente impossibile prevedere il valore futuro di una moneta, ne consegue che qualsiasi sistema monetario deve comprendere non solo uno standard di definizione dell'unità di conto, dei mezzi di pagamenti e del loro rapporto, ma altresì meccanismi istituzionali volti a garantire nel tempo il valore della moneta, cioè che sostengano nel tempo la fiducia dei consociati nella tenuta del sistema monetario stesso[137].

[137] Sul punto magistralmente GIANNINI, op. cit., p. 56 : "*È in questo senso che la moneta è un'istituzione, non una mera convenzione: perché la fiducia nella sua qualità deve essere continuamente sostenuta,*

Tra tali meccanismi, deve considerarsi anche la capacità di gestire le variazioni della domanda e dell'offerta di moneta, che possono influenzare il valore della moneta e quindi le valutazioni e la fiducia dei consociati: sia sotto il profilo di un aumento o di una diminuzione della domanda di moneta da parte dei consociati, sia sotto il profilo di una corretta – e non per questo rigida o immutabile, bensì ragionevolmente flessibile – offerta di moneta[138].

Ne consegue che lo studio della moneta nei termini di sistema monetario qui proposto comporta l'adozione di un approccio che tenga conto dei risvolti regolamentari ed istituzionali connessi alla necessità non solo di definire i termini della convenzione monetaria, ma anche di sostenere la fiducia nella moneta nel tempo:

> *"Per ciascuna forma monetaria, gli aspetti salienti sono la tecnologia di pagamento in sé (le caratteristiche di mezzo di pagamento, mezzo di scambio, e unità di conto) e l'insieme dei meccanismi generatori di fiducia ad essa associati (il sistema di tutela dei diritti associati all'uso di una particolare moneta e le istituzioni volte a proteggere il potere di acquisto).*

pena la degenerazione della tecnologia di pagamento di cui essa è al centro. In relazione ad ogni tecnologia di pagamento deve dunque sussistere un corpo di norme, convenzioni meccanismi istituzionali volto a sostenere la fiducia di chi quella tecnologia utilizza. Rudolf Richter dà a questo concetto il nome di «ordine volto alla protezione del potere d'acquisto» [v. Rudolf Richter, *The new institutional economics applied to monetary economics*, in *Journal of Institutional and Theoretical Economics*, febbraio 1988]. *Più semplicemente, nel seguito parleremo di «meccanismi generatori di fiducia». Lo scopo di una teoria della moneta in quanto si scissione è proprio quello di studiare i meccanismi generatori di fiducia evolutisi per sostenere l'accettabilità della moneta come* quid pro quo *in un mondo di informazione imperfetta, o se si vuole di agenti potenzialmente fraudolenti*". Cfr. altresì DESAN, *Money as a legal institution*, cit., p. 29: "*money persists over time because, or insofar as, it is institutionalized. The relationships described above are matters of governance. They are carried out in law, understood expansively to include the wide variety of formal and informal practices of decision, interpretation, and enforcement that communities adopt to channel human interaction*".

[138] Cfr. ancora sulle ragioni per cui la fiducia debba essere preservata e non possa essere data per acquisita: *Ibidem*, 54, "*Una convenzione sociale, una volta prodottasi, è in grado di sorreggersi da sola, perché sarà nell'interesse di tutti i componenti della comunità conformarsi ad essa. Non è così per la moneta. Lo stock di moneta può essere assimilato ad un bene durevole che produce un flusso di servizi per chi ne faccia uso, chiamiamolo il consumatore. Ma, come argomentato da Benjamin Klein in un importante articolo del 1974, la differenza tra la moneta e un qualunque altro bene durevole sta nel fatto che la qualità della moneta, cioè i servizi che essa è in grado di rendere in termini reali, sono una funzione dell'offerta di moneta futura, nonché della domanda espressa dagli altri consumatori* [rif. a Benjamin Klein, *The competitive supply of money*, in *Journal of Money, Credit and Banking*, dicembre 1974]" le quali possono variare nel tempo.

È solo tenendo presente l'insieme di queste componenti che le varie tecnologie di pagamento possono essere analizzate e confrontate. È così, ad esempio, che la moneta-segno, benché non abbia alcun uso alternativo, può comportare, in funzione dell'ambiente istituzionale che fa da sfondo al circuito economico, costi di produzione della fiducia tali da eccedere i costi, di produzione e opportunità, associati a una merce come l'oro. L'efficienza di una data tecnologia di pagamento, in altri termini, non può essere giudicata se non avendo presente l'ambiente istituzionale in cui il circuito economico è inserito"[139].

Soltanto attraverso l'affidamento della gestione e del governo del sistema monetario (i.e. la convenzione monetaria) ad un soggetto politico o ad un suo delegato è possibile adattare l'offerta di moneta alle oscillazioni della domanda ed eventualmente perseguire politiche ridistributive o compensative che preservino l'accettabilità della convenzione monetaria per tutti i consociati e la pace sociale. L'attribuzione (o l'acquisizione) di tale potere espone però, al tempo stesso, i consociati al rischio di comportamenti opportunistici di tipo espropriativo da parte dei gestori del sistema[140].

Storicamente, la capacità di espandere, *in primis*, e adattare, *in secundis*, in modo flessibile l'offerta di strumenti monetari ricorrendo alla produzione di mezzi di pagamento astratti è stata determinante per lo sviluppo del capitalismo e delle relazioni di produzione industriali[141]. In proposito può dirsi, però, altresì, che con l'aumentare dell'astrazione dei mezzi di pagamento che la convenzione monetaria permette di creare e gestire aumentano le chance di flessibilità dell'offerta, la capacità ridistributiva dell'istituzione e i vantaggi connessi a tali caratteristiche, così come aumentano, però, anche i rischi connessi a comportamenti opportunistici dell'emittente e dei soggetti che hanno materialmente il compito di eseguire la convenzione monetaria, così come i costi

---

139 GIANNINI, op. cit., p. 65.

140 Cfr. *ivi*, p. 63: "*La cosa più importante in regime di incompletezza contrattuale e di informazione imperfetta è quella di limitare la libertà di azione della parte forte del contratto, la parte cioè che può dar luogo a comportamenti opportunistici, o, nel linguaggio della teoria dei contratti, «espropriativi»*".

141 Cfr. INGHAM, *Schumpeter and Weber*, cit., p. 304, nonché ARRIGHI G., *The Long Twentieth Century: Money, Power, and the Origins of Our Times*, Verso, 2010.

connessi alla gestione del sistema sia in termini di investimento istituzionale, sia in termini di controllo dei soggetti cui è conferito potere.

La convenzione monetaria concerne, quindi, la definizione dell'unità di conto, dei mezzi di pagamento e del rapporto tra l'una e gli altri, nonché la definizione dei meccanismi istituzionali volti a salvaguardare e sostenere la fiducia nella moneta, *ivi* inclusi i meccanismi connessi alla gestione delle oscillazioni nella domanda e nell'offerta di moneta e quelli relativi al controllo dell'emittente e dei gestori da parte degli utilizzatori. La definizione dei mezzi di pagamento concerne, altresì, il problema assai complesso della distribuzione iniziale delle risorse e comporta, evidentemente, l'attribuzione di un enorme potere politico.

3. Sistemi monetari e convenzione monetaria tra Stato e diritto

3.1. Stato sovrano e convenzione monetaria

In appendice a questo capitolo sui sistemi monetari, prima di passare allo studio dei bitcoin, merita svolgere ancora un paio di osservazioni sul ruolo dello Stato e del diritto nel contesto del modello proposto.

Storicamente, è un dato incontrovertibile che lo Stato abbia sempre avuto a che fare con la moneta. Indipendentemente dall'adesione alla scuola catallattica o alla scuola statalista, è un dato dell'esperienza che lo Stato, o più genericamente il Sovrano, si sia sempre interessato alla questione monetaria, in primo luogo perché, come si è visto nel corso del capitolo, lo Stato utilizza esso stesso la moneta per l'esercizio di funzioni eminentemente pubbliche: raccogliere le tasse, finanziare la spesa pubblica, amministrare la giustizia penale e civile. Già solo il fatto che lo Stato utilizzi un certo sistema monetario è di per sé molto significativo: nel corso della storia, il Sovrano è stato, infatti, il soggetto con la più alta capacità di spesa all'interno della società, cioè il primo utilizzatore, anche in termini quantitativi, della moneta[142].

A ciò si aggiunge che per effetto del particolare potere impositivo di cui dispone, l'uso da parte dello Stato assume un carattere diverso rispetto all'uso che ne fanno tutti gli altri componenti della società: esso corrisponde a scelte di politica pubblica che hanno un effetto diretto, spesso anche in termini giuridici, sui consociati. Così, per esempio, la determinazione dei mezzi di pagamento con i quali i consociati dovranno pagare le tasse[143].

Lo Stato, quindi, in quanto uno tra gli attori economicamente più significativi all'intero di una comunità, in primo luogo utilizza la moneta e utilizzandola contribuisce

[142] Si pensi per esempio al contesto dell'impero romano e alle spese militari che storicamente hanno sempre costituito una grossa fetta del prodotto interno lordo di una comunità e che sono amministrate, nella normalità, direttamente dal Sovrano. Cfr. anche DESAN C., *Making Money*, *cit*..

[143] Secondo Knapp è proprio l'elemento dell'accettazione di un certo bene per l'adempimento degli obblighi fiscali che lo rende 'moneta' in senso giuridico. Non occorre però aderire alla teoria statalista per rendersi conto che una tale determinazione non può che avere l'effetto di sostenere la fiducia nei consociati nel valore futuro di tale bene, che essi sapranno di poter utilizzare, quantomeno, per il pagamento delle tasse.

a definire il funzionamento del sistema monetario. Nell'utilizzare la moneta lo Stato impone altresì delle regole sulla collettività: quando l'imposizione di regole concerne direttamente il funzionamento del sistema monetario, allora può dirsi che lo Stato sta esercitando la propria sovranità monetaria, cioè sta determinando, in quanto soggetto cui è conferito il massimo potere all'interno di una società, i termini della convenzione monetaria[144].

Al riconoscimento di questo potere in capo allo Stato oggi si fa corrispondere una responsabilità tale per cui si pretende dallo Stato che istituisca un sistema monetario funzionante e funzionale e ne curi la stabilità[145]. Per lungo tempo l'esercizio di questo potere ha coinciso con il tentativo di estrarre opportunisticamente risorse per finanziare la spesa pubblica, che si è provato a contrastare attraverso l'affermazione delle dottrine che riconoscevano valore al bene fisico piuttosto che a quanto stabilito ed imposto dal Sovrano[146]. Con l'affermazione dell'economia industriale e il passaggio a mezzi di pagamento astratto la cui convertibilità, prima, e il cui valore nominale, poi, sono fissati direttamente dalla legge, l'importanza dell'organizzazione del sistema monetario e della sua gestione è però aumentata sensibilmente, e il Sovrano ha lasciato il ruolo di antagonista del corretto funzionamento del sistema monetario per assumere invece quello di emittente e garante dello stesso[147]. Nello Stato democratico borghese l'esercizio della sovranità monetaria è divenuto quindi uno dei compiti che il popolo attribuisce e delega allo Stato e per converso può dirsi che con l'avvento del *fiat money*, cioè della moneta

144 Cfr. per tutti, BLACKSTONE, i, 277 (cit. in PROCTOR, op. cit., p. 12) la moneta è esenzialmente un atto del potere sovrano ("*Sovereign Power*") e sulla definizione di sovranità monetaria cfr. BLANC J., *Beyond the quantity theory: a reappraisal of Jean Bodin's monetary ideas*, in Giacomin A. e Marcuzzo M.C. (a cura di), *Money and Markets. A doctrinal approach*, Routledge, 2007**,** pp. 135 ss.

145 v. CECCHETTI e SCHOENHOLTZ, op. cit., p. 26 e cfr. INGHAM, *The Nature of Money*, cit., 187, secondo cui la creazione della fiducia impersonale e legittimità necessaria per l'estensione delle relazioni monetarie nel tempo e nello spazio è un compito che storicamente è sempre stato affidato allo Stato.

146 Cfr. FELIX, op. cit., pp. 99–107 e BARCELLONA E., op. cit., *passim*. Sull'evoluzione nel tempo delle modalità di esercizio della sovranità monetaria da parte dello Stato e la centralità dell'intervento statale v. PINI, op. cit., *passim* e, in particolare, pp. 39-40 e pp. 51-53.

147 V. GIANNINI, op. cit., p. 229, "*La moneta è «legale» nel senso che lo Stato fa direttamente produttore di garante. Il cambiamento di prospettiva rispetto ai secoli precedenti, in cui lo Stato veniva spesso indicato come il principale nemico della stabilità monetaria, è strabiliante*".

legale inconvertibile, il sistema monetario viene interamente a dipendere dallo Stato e dal diritto[148].

Nella prima metà del novecento, a fronte della grande crisi e dei contributi alla scienza economia di Keynes, la sovranità monetaria inizia a essere esercitata non solo al fine di garantire l'esistenza e la fruibilità di una moneta all'interno della società, ma anche per esercitare politiche monetarie pro–attive volte al perseguimento della piena occupazione. Negli anni settanta l'equilibrio tra inflazione, spesa pubblica e occupazione risulta compromesso e lo Stato democratico reagisce sottraendo alla competenza del sovrano parte del suo potere: si stabilisce, così, un regime internazionale di libera circolazione dei capitali e di tassi di scambio variabili e al contempo inizia un processo di trasformazione delle istituzioni monetarie volto a rendere le banche centrali indipendenti dai governi e ad affidare a queste ultime la determinazione e gestione delle politiche monetarie. Si persegue così un modello di sistema monetario in cui: lo Stato continua a garantire ed affermare attraverso il diritto il valore della valuta; la produzione di mezzi di pagamento è gestita privatamente dal sistema bancario secondo criteri di efficienza e profitto, sotto la supervisione della Banca Centrale; e a quest'ultima è affidata, entro i limiti di un mandato 'tecnico', cioè che deve essere espletato avendo cura esclusivamente dell'obbiettivo di preservare il valore della moneta, la determinazione dei tassi di interesse da applicare alle banche e la determinazione (almeno in principio) della quantità di moneta in circolazione[149].

Nel corso di questa lunga evoluzione l'intervento dello Stato ha sempre avuto effetti sul funzionamento del sistema monetario.

Nel contesto di un sistema monetario basato su mezzi di pagamento reali, realizzati con l'impiego di metalli preziosi, è lecito pensare che talune delle caratteristiche stesse di questi metalli abbiano facilitato l'adozione e l'uso del mezzo di pagamento e

---

148 Cfr. OLIVECRONA, op. cit., pp. 311 e 351; e STAMMATI, op. cit., p. 749.

149 Cfr. *supra* la teoria istituzionalista della moneta. Estremamente esemplificativo del modello è l'ordinamento dell'Unione Europea ed in particolare la disciplina che regola le competenze della Banca Centrale Europea circa l'emissione dell'euro. Sull'esercizio delle politiche monetarie da parte di una banca centrale v. BAGLIONI A., *il mercato monetario e la banca centrale. Liquidità bancaria, politica monetaria, sistemi di pagamento*, Bologna, Il Mulino, 2004. Per una rilettura critica del sistema attuale, per tutti, GALLINO L., *Il colpo di Stato di banche e governi: l'attacco alla democrazia in Europa*, Einaudi, 2013.

abbiano contribuito in modo determinante a sostenere la fiducia nel valore della moneta e nel sistema: si pensi, in particolare, alla facile trasferibilità e alla scarsità naturale dei metalli preziosi. Ma anche in tale contesto l'intervento dello Stato pare, nel complesso, determinante.

In primo luogo sotto il profilo della coniazione, la quale, da un lato, permette sì l'estrazione di risorse da parte del sovrano, ma al tempo stesso comporta una significativa riduzione dei costi transattivi connessi alla valutazione del peso e della qualità dei metalli preziosi[150] e permette altresì la creazione di un referente comune espresso in termini numerici, altrimenti non semplice nel contesto di un mezzo di pagamento pesatore amorfico[151]. E se la coniazione può essere intesa per un verso come un servizio di pesatura e certificazione della quantità di metallo prezioso contenuta in un certo pezzo monetario[152] è altresì vero che ad essa contestualmente consegue la definizione di un certo valore nominale del pezzo monetario, cioè, di uno specifico rapporto determinato dal diritto e non dalla natura del bene tra unità di conto astratta e mezzo di pagamento (pezzo monetario metallico)[153]. Anche nel contesto dei mezzi di pagamento con valore intrinseco, cari alla teoria economica ortodossa, è evidente, quindi, l'importanza dello Stato nel determinare l'unità ideale di conto e il rapporto tra essa e i mezzi di pagamento[154].

Nel contesto dei mezzi di pagamento astratti l'importanza del diritto e dell'intervento pubblico si manifesta, invece, in tutta la sua rilevanza: in regime di convertibilità è la legge che garantendo la convertibilità del biglietto di banca sostiene la fiducia nel meccanismo; nel contesto della moneta che circola in regime di corso forzoso la fiducia è sostenuta dalla disposizione di legge che ne sancisce l'idoneità di tale strumento a liberare dall'obbligazione pecuniaria:

---

150 V. GOODHART, op. cit., p. 412.

151 V. KNAPP, op. cit..

152 Questa è la lettura di GOODHART, op. cit..

153 Cfr. PINI, op. cit., p. 30.

154 Sul ruolo del Principe nel contesto della moneta medievale cfr. BARCELLONA E., op. cit., ove ampi riferimenti a ulteriore dottrina.

"*Il sistema si fonda sull'osservanza di norme, e ciò ha reso possibile rinunciare ai metalli preziosi come mezzo di scambio: in loro luogo abbiamo svariati modi di assumere obblighi artificiali, espressi in termini di unità monetaria, modi di liberarcene e determinate conseguenze se non ce ne liberiamo. Tutto è regolato da norme; senza riferimento alle norme, promesse e pagamenti sarebbero suoni e gesti privi di senso. Le norme non sono solo quelle che vengono dette giuridiche; ad esse si aggiungono quelle sociali e, in determinate circostanze, soltanto quelle sociali sono rilevanti. Ma vi debbono essere delle norme.*

La fittizia unità monetaria è una meravigliosa invenzione, comparabile al simbolo che indica lo zero nel sistema dei numeri arabi: senza di essa non sarebbe possibile l'economia dell'età industriale; il suo uso, d'altra parte, presuppone il sistema giuridico altamente sviluppato dello Stato industriale e la sua vasta rete di organizzazione bancaria."[155]

In conclusione, lo Stato ha sempre preso parte alla definizione della convenzione monetaria, il cui contenuto e la cui struttura si è modificata nel tempo secondo le esigenze sociali ed economiche, i rapporti di forza tra cittadini e sovrano e le tecnologie disponibili.

3.2. Diritto ed esercizio della sovranità monetaria

Nel quadro dell'esercizio della sovranità monetaria e della determinazione del sistema monetario il diritto svolge, quindi, un ruolo centrale, nella definizione della convenzione monetaria e quindi della moneta intesa come istituzione. Per quanto riguarda l'Italia e i paesi della eurozona, l'articolo 3, paragrafo 4, del Trattato sull'Unione Europea afferma che: "*L'Unione istituisce un'unione economica e monetaria la cui moneta è l'euro*", sancendo così l'unità di conto giuridicamente riconosciuta dall'ordinamento. Vi sono poi una serie di mezzi di pagamento istituiti direttamente dalla legge (v. per esempio i pezzi metallici e le banconote emesse dalle zecche nazionali sotto la supervisione della BCE) o dei quali la legge permette l'emissione a determinate condizioni (così la moneta elettronica e, in senso più lato, la moneta scritturale bancaria).

[155] OLIVECRONA, op. cit., pp. 316–317.

Quanto all'esigenza di sostenere la fiducia nel sistema, tale obbiettivo è perseguito contestualmente attraverso la predisposizione di un sistema monetario la cui architettura sia funzionale alla conservazione di fiducia da parte degli utilizzatori e rispondente alle loro esigenze, nonché attraverso la predisposizione di particolari regole generali che disciplinano l'uso dei mezzi di pagamento predisposti dal sistema monetario.

L'organizzazione della produzione e distribuzione di mezzi di pagamento deve dunque seguire criteri di giustizia formale e di funzionalità e affidabilità economica. Sotto il profilo specifico dell'offerta di liquidità, cioè di mezzi di pagamento, il sistema dovrebbe inoltre permettere facilità d'uso e accesso a tutti, nonché garantire la flessibilità nell'offerta di moneta necessaria al mantenimento del valore della stessa e adeguati meccanismi di contenimento e gestione dei rischi di comportamenti opportunistici espropriativi a danno della collettività.

Ulteriore sostegno alla fiducia dei privati è poi offerta dallo Stato mediante la regolamentazione dell'uso della moneta nei rapporti tra privati. In questo ultimo ambito, hanno particolare rilevanza: (*i*) l'imposizione del potere liberatorio della valuta; (*ii*) il principio nominalistico; e (*iii*) il c.d. *recurrent link*, espressi nell'ordinamento italiano nell'art. 1277 cod. civ., '*Debito di somma di danaro*', a mente del quale:

> *"1. I debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale.*
>
> *2. Se la somma dovuta era determinata in una moneta che non ha più corso legale al tempo del pagamento, questo deve farsi in moneta legale ragguagliata per valore alla prima".*

Questi tre principi insieme, operano non solo quali strumenti che ordinano e disciplinano il regolare svolgimento dei rapporti economici monetari, ma anche quali strumenti che sostengono la fiducia nei consociati nel sistema monetario riducendo il tasso di incertezza e di asimmetria informativa connessi alla proiezione nel futuro del valore d'acquisto della moneta.

Il principio del corso legale, cioè l'obbligo di accettare in pagamento la moneta ufficiale dello Stato e l'effetto liberatorio dell'obbligazione che consegue a tale dazione, conferisce certezza circa l'accettabilità futuro del mezzo di pagamento, che viene sorretta

e garantita in maniera diretta ed esplicita dal potere statale. Inoltre, l'applicazione di tale principio si estende a tutti i pagamenti che coinvolgono lo Stato, il che contribuisce a sostenere la liquidità (e l'utilità) della valuta.

Corollario del corso legale è il principio nominalistico, che garantisce l'efficacia del riferimento all'unità di conto nel corso del tempo e conferisce così maggiore affidabilità ai mezzi di pagamento che incorporano un certo numero di unità di conto. Con l'applicazione del principio nominalistico diventa cioè possibile, per i consociati, accantonare una certa quantità di mezzi di pagamento in previsione di un pagamento futuro sapendo che indipendentemente dal valore reale che l'unità di conto potrà acquistare o perdere essi potranno, attraverso la corresponsione di tali mezzi di pagamento, saldare il proprio debito.

Da ultimo, il principio del *recurrent link* consiste nella regola in forza della quale nella straordinaria ipotesi di modificazione radicale della convenzione monetaria che comporti la sostituzione di una moneta (i.e. una certa combinazione di unità di conto e mezzi di pagamenti) con un'altra, verrà stabilito un rapporto, con efficacia giuridica, tra l'unità di conto precedentemente in vigore e quella successiva, sicché il riferimento all'unità di conto da parte dei consociati per la determinazione di obbligazioni di natura privata resterà comunque tutelato e agli stessi sarà riconosciuta la possibilità di scambiare i mezzi di pagamento obsoleti con corrispondenti mezzi di pagamento nuovi[156].

Fermo restando, dunque, che il valore reale di una moneta dipende in ultima analisi sempre dalla fiducia e dall'uso che i consociati fanno di questa moneta, i tre principi giuridici del corso legale, nominalistico e del *recurrent link* concorrono nella definizione del sistema monetario statale contribuendo al sostegno della fiducia dei consociati nella moneta, realizzando un contributo diretto e molto importante del sistema giuridico.

[156] Sulla nozione e definizione di *recurrent link*, v. LUMINI C., *La continuità dei contratti alla prova dell'euro*, in *Riv. Notariato*, 1998, pp. 27-54; v. PROCTOR, op. cit..

3.3. Sistemi monetari, esercizio del potere ed effetti distributivi

La rilettura del fenomeno monetario nei termini di un'istituzione definita da una convenzione monetaria permette di evidenziare ancor meglio quanto già è stato messo in luce dai più recenti contributi della scuola eterodossa, cioè che la definizione dell'unità di conto e del mezzo di pagamento è, almeno in parte, frutto di una scelta che ha effetti distributivi della ricchezza di enorme portata, giacché la determinazione dei modi di produzione dei mezzi di pagamento e l'implementazione di meccanismi collettivi volti a tutelarne il valore comportano necessariamente l'allocazione di costi e vantaggi all'interno della società:

> *In Mann's terminology, money is not only 'infrastructural' power, it is also 'despotic' power. In other words, money expands human society's capacity to get things done, but this power can be appropriated by particular interests. This is not simply a question of the possession and/or control of quantities of money – the power of wealth. Rather, as we shall see, the actual process of the production of money in its different forms is inherently a source of power. For example, modern capitalist money is bank credit-money that is produced on the basis of credit ratings that reinforce and increase existing levels of inequality by imposing differential interest rates. In the most general terms, as Weber contended, money is a weapon in the struggle for economic existence.*[157]

A stesse conclusioni giunge il recente contributo di Christine Desan, nel quale si propone una rilettura della storia della moneta sotto un profilo giuridico che evidenzia che la costituzione della moneta dipende da scelte e soluzioni politiche e giuridiche che lungi dall'essere neutrali rispondono ad un progetto di *governance*[158].

---

[157] INGHAM, *The Nature of Money*, cit., p. 4.

[158] DESAN C., *Making Money*, *cit*., *passim* ed in particolare: p. 24 e pp. 432–434. Cfr. anche FELIX, op. cit., p. 53: "*The choice of standard for the measurement of economic value—the choice of the standard for the monetary unit, in other words—affects […] how wealth and income are distributed and who bears economic risks. It is, therefore, not just a technical, but also an ethical question; and the criterion for choosing it is not only which standard unit is efficient, but which is fair. Of course, the determination of what is fair is nothing but politics*". Cfr. Anche KREITNER R., *The Jurisprudence of Global Money*, in *Theoretical Inquiries in Law*, vol. 11, 2010, p. 177.

Tali effetti distributivi, o semplicemente 'politici', della moneta afferiscono in primo luogo alle modalità con cui si ha accesso al sistema monetario, le quali, appunto, possono avvantaggiare o svantaggiare certi gruppi sociali od economici, e alla distribuzione del potere di creazione di nuovi mezzi di pagamento (cioè di nuova liquidità) e dei vantaggi che derivano dall'esercizio di tale potere. In secondo luogo, la definizione del funzionamento del sistema monetario ha effetto sul valore delle risorse già distribuite ed incide, quindi, sui rapporti tra debitori e creditori e sulla ricchezza accumulata in termini monetari dai consociati. In questa prospettiva, la definizione della convenzione monetaria riflette le tensioni sociali e politiche che vengono a crearsi per effetto della corrente allocazione di costi e vantaggi ed è frutto, quindi, di lotte sociali e politiche[159]. Da tale considerazione si deduce un ulteriore differenza tra la moneta come istituzione e altre convenzioni sociali, cioè che la convenzione monetaria è continuamente soggetta a tensioni che originano dall'uso della moneta stessa, e in particolare dalla sua accumulazione, a causa dei riflessi politici connessi alla movimentazione di risorse e alla distribuzione della ricchezza[160].

In questa prospettiva, il rischio connesso al rapporto di *agency* che si instaura in modo particolare tra cittadini e sovrani nel contesto di sistemi monetari che fanno ricorso a mezzi di pagamento astratti, che è precedentemente illustrato nei termini di una "*tensione logicamente irrisolvibile*"[161] tra flessibilità e rischio di comportamenti opportunistici estrattivi del sovrano, è il riflesso del fatto che qualsiasi sistema monetario comporta effetti distributivi (che evidentemente possono anche essere appropriati dal sovrano, specie laddove la produzione di nuove unità non sia limitata dalla disponibilità di un certo bene fisico).

---

159 V. INGHAM, *Schumpeter and Weber*, cit., nota 12, e *ivi* il rif. a Weber; GIANNINI, op. cit., p. 52; e cfr. HAYEK, op. cit., p. 29, secondo cui lo Stato sistematicamente utilizza la sua prerogativa sovrana di monetazione per defraudare la gente tale generando inflazione nell'interesse delle finanze pubbliche.

160 v. in particolare la nozione di *facies obscura* della moneta in BARCELLONA E., op. cit., ove è illustrata magistralmente la tensione tra la dimensione egualitaria e parificatrice della moneta e la sua dimensione violenta connessa alla appropriazione della ricchezza e alla concentrazione di potere. v. anche DODD, op. cit., *passim*.

161 GIANNINI, op. cit., p. 65 e v. anche 63 circa il vincolo di tipo giuridico o politico nel contesto di mezzi di pagamento astratti.

Poiché l'articolazione di un sistema monetario ha sempre effetti allocativi di costi e benefici, la questione che dovrebbe essere posta non è tanto se e in che termini il sovrano possa estrarre benefici, ma invece dove e a chi sono allocati i benefici che derivano dalla gestione del sistema monetario. Per concludere, allora, la sovranità monetaria, cui corrisponde sempre una dimensione politica oltre che tecnica–economica, può essere esercitata nell'interesse secondo forme democratiche nell'interesse di tutti o può essere controllata da gruppi di interesse che si appropriano dei benefici corrispondenti: non pare, però, esservi una soluzione intermedia di 'neutralità'. Se ne deduce, allora, che nel contesto del fenomeno monetario il diritto non solo è importante perché è lo strumento che permette concretamente dare forma alla convenzione monetaria permettendo l'uso di mezzi di pagamento astratti e sostenendo la fiducia nel sistema monetario attraverso il raccordo tra quest'ultimo e il diritto generale delle obbligazioni, ma è altresì lo strumento attraverso cui, a livello costituzionale, sono definiti i rapporti tra sovranità popolare e attori coinvolti nella gestione della convenzione monetaria ed è quindi lo strumento attraverso il quale il rischio di comportamenti espropriativi, da parte di qualsiasi soggetto coinvolto, non solo dello Stato, può essere fronteggiato[162].

Il bitcoin si pone in antitesi rispetto a questo discorso, proponendosi, invece, come un sistema neutrale, accessibile a chiunque e non soggetto al rischio di comportamenti espropriativi da parte dello Stato.

[162] Cfr. FELIX, op. cit., pp. 186-187, che sintetizza la questione nei seguenti semplici termini: «*The original standard of economic value—the standard that had allowed money to serve, not only as a device for organising one line of trade or one part of the bureaucracy, but the entire economy and the whole of society—expressed a political ideal: the equal social value of the individual member of the tribe. But by its nature, money permits social mobility and the accumulation of wealth and power over others. Any fixed standard of monetary value will therefore necessarily become obsolete—and that obsolescence spells mortal danger, for it is the root of civil strife. Instead, the state must be always vigilant to ensure that the architecture of financial obligations reflects what society believes to be fair.* ***Only politics—democratic politics, in constant activity—can furnish such an evolving standard. And only law—its debate, codification, and rule—can enact it***» (sottolineatura aggiunta).

Capitolo II

Bitcoin: origini e funzionamento

Cosa sono i bitcoin? Questo nuovo fenomeno può essere presentato da due angolature molto diverse. Un approccio è quello di analizzare i profili economici connessi alla nascita e all'affermazione dei bitcoin sino alla loro graduale affermazione come mezzo di pagamento o come "moneta". Altro tipo di analisi rivolge l'attenzione alla tecnologia e agli aspetti tecnici da cui dipende il funzionamento del sistema. In questa tesi riteniamo che questi due profili di (i) analisi economico-giuridica circa il significato dell'attribuzione della qualità di «moneta» ai bitcoin e (ii) analisi tecnica del funzionamento del protocollo non siano scindibili. Si ritiene, inoltre, che sia utile cercare di ricostruire una genealogia dei bitcoin, studiando le origini del protocollo/moneta e il contesto culturale in cui matura e nasce questo progetto, al fine di comprendere quali fossero le domande e le esigenze a cui i creatori di questo sistema stavano provavano a rispondere.

Nella prima parte del capitolo si affronterà, quindi, il tema delle origini "culturali" dei bitcoin: si cercherà di contestualizzare questa invenzione all'interno del movimento *cypherpunk* cripto-anarchico e di rinvenire i precursori che hanno contribuito a sviluppare le basi su cui si fonda la tecnologia implementata in questa nuova moneta. Si darà evidenzia, in particolare, del fatto che il desiderio di creare una moneta che tuteli l'anonimato e sia indipendentemente dagli ordinamenti nazionali sia nato in un contesto culturale marcatamente libertario, che si oppone allo Stato e al controllo che può essere esercitato via web, nonché al sistema delle banche e della moneta fiduciaria moderna.

Nella seconda parte, l'attenzione sarà volta all'analisi del funzionamento del protocollo Bitcoin, sia sotto il profilo dei trasferimenti di bitcoin tra utilizzatori, sia sotto il profilo, più interessante, della regolamentazione del sistema nel suo complesso, ivi

compresa la questione di come sono creati nuovi bitcoin e come avviene la gestione decentrata del registro comune distribuito su cui si fonda l'intero progetto. L'aspetto del funzionamento della tecnologia utilizzata nei bitcoin sarà approfondito non solo perché prima di formulare qualsiasi ipotesi di interpretazione del fenomeno è necessario comprendere bene l'oggetto di studio, ma anche perché il software che gestisce l'intero sistema Bitcoin ambisce a svolgere un ruolo che potremmo facilmente definire come para-giuridico. Le regole volte a disciplinare il comportamento dei membri appartenenti alla comunità degli utenti del bitcoin sono definite, infatti, all'interno del software stesso.

1. Le Origini dei bitcoin

"*the foundational motivations for Bitcoin appear to have been largely ideological*"[163]

1.1. Le origini culturali dei bitcoin: capitalismo, anarchia e crittografia

I bitcoin sono un fenomeno digitale le cui origini possono essere ricondotte ad un movimento politico–culturale chiamato «*critto-anarchismo*», o con maggior precisione «*critto-anarco-capitalismo*», in cui una visione del mondo marcatamente liberale è coniugata con una grande fiducia nello sviluppo delle tecnologie crittografiche informatiche.

Nella seconda metà degli anni ottanta, un gruppo di programmatori americani si dimostrano particolarmente sensibili a due innovazioni tecnologiche che si stavano affermando in quel periodo: l'evoluzione delle reti di comunicazione e la scoperta di nuove funzioni matematiche per la crittazione delle informazioni. Alla previsione di un'esponenziale aumento dell'uso delle reti informatiche per lo scambio di informazioni essi associavano la preoccupazione dell'esercizio di un sempre maggiore e più pervasivo controllo da parte dell'autorità pubblica e, potenzialmente, delle multinazionali. Parallelamente, però, essi ritenevano che lo sviluppo dell'informatica avrebbe presto permesso a chiunque di cifrare informazioni digitali con codici estremamente resistenti ai tentativi di decifrazione, senza la necessità di particolari infrastrutture tecnologiche. In questi nuovi meccanismi crittografici essi riconoscevano, allora, uno straordinario strumento di resistenza, che non solo avrebbe permesso ai cittadini di difendersi contro l'ingerenza del potere costituito nella privacy e nella libertà individuale, ma avrebbe persino permesso di realizzare un nuovo modello di società nella quale i soggetti

[163] ALI R., BARRDEAR J., CLEWS R. e SOUTHGATE J., *Innovations in payment technologies and the emergence of digital currencies*, in *Bank of England Quarterly Bulletin*, Vol. 54, 2014, No. 3, p. 267.

avrebbero potuto interagire tra loro sulla base di pseudonimi senza alcun rapporto con il potere costituito.

Il progetto critto–anarchico nasce, quindi, come politico e tecnologico insieme: i crittoanarchici si propongono di fondare una società dove la crittografia delle informazioni digitali permetta l'affrancamento dell'individuo dalla coercizione e dal potere sovrano, garantisca a ciascun individuo una privacy piena e incondizionata e un'esistenza caratterizzata da iterazioni sociali frutto di scelte realmente e pienamente "libere" perché immuni dalla paura dell'esercizio della violenza[164], e per raggiungere questo obbiettivo si impegnano a creare il codice informatico necessario allo scopo.

La visione politica di stampo anarchico viene coniugata, per quanto concerne la politica economica, con un'area di pensiero marcatamente liberista. Non vi sono elaborazioni esplicite sul punto, eppure è agevole dedurre dai documenti che saranno a breve presentati, che alla base del ragionamento anarcocapitalista l'avversione profonda contro lo Stato e i meccanismi di controllo è accompagnata da un'altrettanto considerevole fiducia nel mercato che si riflette nell'assunto secondo cui per soddisfare i bisogni di un individuo è necessario e sufficiente offrire meccanismi che permettano scambi economici volontari. L'individuo posto al centro di tale riflessione rispecchia il modello di agente economico razionale che fonda la teoria economica classica e neoclassica: è un soggetto che essenzialmente ha delle risorse e dei bisogni che saranno naturalmente soddisfatti se sarà lasciato libero di scambiare le proprie risorse con quelle degli altri soggetti. Nell'esercizio di tale libertà economica si esaurisce, essenzialmente, il bisogno di socialità dell'individuo, o almeno si esaurisce il compito di gestione della socialità di un individuo che la "comunità politica" deve avere a cuore. In questa prospettiva libertaria, lo Stato e il potere costituito sono ostacoli alla realizzazione piena della libertà dell'individuo, non certo strumenti imprescindibili che la tutelano contro

[164] Cfr. MAY T., *Crypto anarchy and virtual communities*, 1994, disponibile all'indirizzo http://nakamotoinstitute.org/virtual-communities/ (ultima visita 20 giugno 2017): "*The combination of strong, unbreakable public key cryptography and virtual network communities in cyberspace will produce interesting and profound changes in the nature of economic and social systems. Crypto anarchy is the cyberspatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to make the economic arrangements they wish to make consensually*", e ancora: "*Technology has let the genie out of the bottle. Crypto anarchy is liberating individuals from coercion by their physical neighbors—who cannot know who they are on the Net—and from governments*".

eventuali abusi da parte dei consociati e ne permettono, quindi, in ultima analisi, il godimento. «Anarchia», quindi, connessa al libertarismo e al disprezzo per lo Stato, e «capitalismo», inteso non come sistema economico di gestione delle risorse regolato da un determinato complesso di strutture economico-giuridico-politiche, bensì inteso come pura e semplice affermazione del "libero" scambio, sono quindi i due ingredienti fondamentali dell'«anarcocapitalismo» (che un giurista forse dovrebbe più propriamente riqualificare «anarco-scambismo», ma non è questa la sede per lo sviluppo di tale riflessione). Questo, in sintesi, è l'orizzonte culturale cui fa riferimento il movimento crittoanarchico, per il quale la crittografia rappresenta una promessa di realizzazione del modello politico-sociale agognato.

Le prospettive sopradescritte sono presentate negli scritti di due autori ritenuti genericamente rappresentativi del movimento[165]: Timothy May e Eric Hughes. Il primo dei due è sicuramente uno tra i più entusiasti e ferventi crittoanarchici della prima ora e scrive nel 1988 "*The Crypto Anarchist Manifesto*", un manifesto politico che esordisce affermando con tono minaccioso ed altisonante che "*lo spettro della crittoanarchia sta infestando il mondo*"[166].

Secondo tale autore la tecnologia dei computer avrebbe presto permesso a gruppi di individui di comunicare in forma completamente anonima e ciò avrebbe portato una radicale trasformazione delle nozioni di *fiducia* e *reputazione* e all'impossibilità, per lo Stato, di raccogliere un gettito fiscale e regolare gli scambi economici, e, quindi, ad una ridefinizione della natura stessa del potere politico (ragione per cui, secondo l'autore, lo

---

[165] La rappresentatività o meno dell'intero movimento *cypherpunk* sarebbe certamente oggetto di discussione da parte di questi autori stessi: è lo stesso Timothy May che dichiara in alcuni suoi scritti che scrive quello che egli ritiene essere vero e che alcuni appartenenti a questa linea di pensiero potrebbero non essere d'accordo (v. MAY T., *The Cyphernomicon*, 1994, disponibile all'indirizzo http://nakamotoinstitute.org/static/docs/cyphernomicon.txt (ultima visita 20 giugno 2017)). Il concetto stesso di rappresentatività in capo ad un singolo individuo intesa come attribuzione del potere di rappresentare all'esterno la comunità è estremamente distante dalla visione politica di stampo anarchico del movimento. Resta il fatto che questi due autori sono considerati tra i fondatori del movimento *cypherpunk* e hanno scritto e firmato documenti che aspiravano a sintetizzare le posizioni di questo gruppo e da cui discende la loro, voluta o meno, capacità di rappresentare le visioni di questo gruppo. Parimenti discutibile sarebbe pretendere un collegamento diretto tra questi e i bitcoin, sul punto si veda *infra*.

[166] MAY T., *The Crypto Anarchist Manifesto*, 1988, disponibile all'indirizzo http://nakamotoinstitute.org/crypto-anarchist-manifesto/ (ultima visita 20 giugno 2017).

Stato avrebbe fatto di tutto per impedire lo sviluppo di queste tecnologie)[167]. Ancora in questo documento, l'autore immagina che lo sviluppo della crittografia avrebbe potuto portare anche numerosi effetti negativi, quali la disgregazione sociale, lo sviluppo di reti criminali e la nascita e lo sviluppo di nuovi mercati illeciti[168]. Tuttavia, nella visione critto–anarchica questi sarebbero stati dettagli di contorno a cui non dare troppo peso a fronte del potenziale della imminente rivoluzione culturale e politica permessa dalla crittografia, paragonata da May all'invenzione della stampa ai tempi di Lutero e all'invenzione del filo spinato nel contesto della conquista dei territori del nord America da parte dei coloni europei:

> *"Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a*

---

[167] MAY T., *The Crypto Anarchist Manifesto*, op. cit., "*Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other … These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation*".

[168] Sotto questo profilo le previsioni di May sono state, purtroppo, corrette: ai numerosi siti del Dark Web dove è possibile acquistare droga, documenti falsi, e addirittura commissionare omicidi, che pur non dipendendo direttamente dalla crittografia, utilizzano e fanno affidamento sui bitcoin bitcoin, si è aggiunto recentemente il fenomeno dei *cryptoware*, programmi malevoli simili al tristemente noto *cryptolocker*, che utilizzano la crittografia a fini estorsivi sia per esercitare violenza sulla vittima e commettere il reato (crittando tutti i file del soggetto colpito con algoritmi indecifrabili senza la chiave di decodifica), sia per ottenere profitto dal reato (richiedendo un pagamento in bitcoin in cambio della trasmissione della chiave di decodifica); *malware* che è possibile comprare sul mercato nero, anche in questo caso pagando in bitcoin. Sul fenomeno si veda l'interessante reportage di CAROLA FREDIANI, *Ho comprato un virus che infetta e ricatta i vostri pc. Vi spiego come funziona*, pubblicato il 30 marzo 2016 sulla versione on-line de La Stampa all'indirizzo http://www.lastampa.it/2016/03/30/italia/cronache/ho-comprato-un-virus-che-infetta-e-ricatta-i-vostri-pc-vi-spiego-come-funziona-4M7Po8sYe9X1cnuOLmvtCJ/pagina.html (ultima visita 20 giugno 2017) ; o ancora l'articolo di FEDERICO GENTA, *Con il virus "Cryptolocker" estorcevano denaro on line ad aziende e privati*, La Stampa, 9 luglio 2015, http://www.lastampa.it/2015/07/09/italia/cronache/con-il-virus-cryptolocker-estorcevano-denaro-on-line-ad-aziende-e-privati-07KemCX4Ug0cDWZEf4wvRI/pagina.html (ultima visita 20 giugno 2017).

seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property"[169].

Bisogna riconoscere che il gruppo di programmatori e pensatori che afferiscono a questa corrente di pensiero furono certo lungimiranti nell'intravedere gli sviluppi che, di lì a breve, avrebbero permesso l'accesso a chiunque di usare meccanismi crittografici molto forti[170], così come a intravedere l'importanza dello sviluppo delle reti informatiche e il rischio di programmi di sorveglianza di massa che si sarebbero potuti realizzare negli anni successivi, come del resto è emerso nel contesto delle rilevazioni di Snowden circa le attività della National Security Agency negli Stati Uniti. Quanto invece agli effetti dello sviluppo della crittografia sul piano sociale, politico ed economico, il discorso crittoanarchico è evidentemente troppo semplificato e pretenzioso. Le posizioni più estreme, quali quelle di May, sono invero caratterizzate da toni eclatanti e visionari che tradiscono una fede così cieca nello strumento tecnologico da apparire indice di religiosità o fanatismo, del tutto fuori luogo rispetto all'ambizione di proporre un manifesto politico credibile.

È interessante notare, altresì, come sin dal principio sia presa in considerazione la possibilità che questi strumenti siano utilizzati per perseguire scopi illegali. In un altro documento intitolato *The Cyphernomicon: Cypherpunks Faq And More*, significativamente più corposo del primo[171], May torna sul tema dell'utilizzo di queste tecnologie *contra ius* e rispondendo alla domanda se la crittografia potrebbe aiutare i razzisti risponde riconoscendo che aiuterà chiunque, quindi anche i razzisti, anche ad infrangere la legge, giacché "*strong crypto will enable and empower groups who have different beliefs than the local majority, and will allow them to bypass regional laws*"[172].

---

169 MAY, *The Crypto Anarchist Manifesto*, op. cit..

170 Il software Pretty Good Privacy, "PGP", fu sviluppato da Phil Zimmermann nel 1991 e permise da allora all'utente privato di usare un livello di crittografia paragonabile a standard militari in uso in quel periodo.

171 Si tratta di un documento di circa trecento pagine, contro la singola pagina del manifesto.

172 MAY, *The Cyphernomicon*, punto 2.5.17.

Il discorso poi prosegue sino a riconoscere apertamente che queste tecnologie non solo saranno usate per compiere reali comuni, ma anche con fini esplicitamente anti-democratici e per sovvertire gli ordini costituzionali democratici costituiti nel mondo[173]. Anche in questo caso, pur riconoscendo il disvalore di certi usi (affermazione del razzismo, criminalità ecc..), l'autore pare quasi compiacersi della supposta ineluttabilità della rivoluzione crittoanarchica, limitandosi ad evidenziare che la tecnologia non sia buona o cattiva in sé e ripetendo il mantra secondo cui il rischio di possibili usi "*moralmente riprovevoli*" sarebbe comunque giustificato e compensato dagli opposti (e supposti) straordinari benefici[174].

Condizione essenziale per realizzare il cambiamento sociale ed economico desiderato è, per May, lo sviluppo di una moneta digitale anonima che permetta gli scambi nella nuova società crittoanarchica[175]. Si legge, infatti, ancora nella parte iniziale introduttiva di questo lungo documento scritto nella forma di domande e risposte:

> *"What is Crypto Anarchy? Some of us believe various forms of strong cryptography will cause the power of the state to decline, perhaps even collapse fairly abruptly. We believe the expansion into cyberspace, with secure communications, **digital money**, anonymity and pseudonymity, and other crypto-mediated interactions, will profoundly change the nature of economies and social interactions".*[176]

---

173 *Ibidem*, punto 2.13.6.

174 In un altro paragrafo una simile riflessione è svolta con specifico riferimento all'idea di denaro virtuale che permetta pagamenti anonimi, v. Ibidem, punto 10.8.5.

175 È interessante notare il forte collegamento tra organizzazione della moneta e organizzazione sociale. Cfr., sul punto, la consonanza con le posizioni di un altro pensatore liberale (di ben alto spessore) circa la sua proposta di adottare un sistema monetario basato sulla competizione tra monete private e la relazione tra questa proposta e l'organizzazione generale della società: HAYEK, op. cit., p. 80 : "*I will admit that my radical proposal concerning money would probably be practicable only as part of a much more far-reaching change in our political institutions, but an essential part of such a reform which I am proposing in the economic and the political order are indeed complementary: the sort of monetary system I propose may be possible only under a limited government such as we do not have, and a limitation of government may require that it be deprived of the monopoly of issuing money. Indeed, the latter should necessarily follow the former*".

176 MAY, *The Cyphernomicon*, punto 2.13.1, sottolineatura aggiunta. Il *digital cash* è inoltre evidenziato come uno dei tre "*main Cypherpunks projects*" al punto 2.4.26. Nel documento vi è un intero capitolo dedicato al *digital money*.

Lo sviluppo di una moneta digitale adeguata al nuovo modello di società è parte centrale del più ampio progetto di rivoluzione culturale, sociale e politica, per il quale occorre uno strumento che consenta di realizzare scambi tra soggetti che restano sconosciuti e irrintracciabili gli uni agli altri e che, per questa ragione, sarebbero finalmente liberi di realizzare scambi pienamente 'volontari', frutto dell'esercizio di una nuova piena (e irresponsabile) libertà[177].

Meno estremo e più puntuale è, invece, il *Cypherpunk's Manifesto* di Eric Hughes[178], che offre una visione del movimento con ambizioni più limitate rispetto alle riflessioni proposte da May. In questo documento, sintetico, logico e consequenziale, l'autore si concentra, infatti, esclusivamente sul concetto di privacy, definita come la possibilità di rivelare selettivamente se stessi al mondo e ritenuta un bene indispensabile nella società aperta dell'era elettronica. Assumendo che la privacy sarà sempre più a rischio con l'aumentare dell'informatizzazione, e assumendo, altresì, la privacy come valore (o diritto) irrinunciabile e fondamentale della persona umana, l'attenzione di Hughes si concentra sulla necessità impellente di garantire sistemi di scambio elettronici che salvaguardino l'anonimità delle persone, perché queste possano fruire dei servizi legati all'informatica in modo discreto, senza essere spiati e senza dover rivelare la propria identità.

La riflessione origina dalla semplice considerazione secondo cui nel mondo reale l'uso del denaro contante consente di acquistare beni e servizi senza rivelare la propria

---

177 *Ibidem*, punto 2.3 e ss.: "*2.3. "What's the 'Big Picture'? 2.3.1. Strong crypto is here. It is widely available. 2.3.2. It implies many changes in the way the world works. Private channels between parties who have never met and who never will meet are possible. Totally anonymous, unlinkable, untraceable communications and exchanges are possible. 2.3.3. Transactions can only be *voluntary*, since the parties are untraceable and unknown and can withdraw at any time. This has profound implications for the conventional approach of using the threat of force, directed against parties by governments or by others. In particular, threats of force will fail. 2.3.4. What emerges from this is unclear, but I think it will be a form of anarcho-capitalist market system I call «crypto anarchy». (Voluntary communications only, with no third parties butting in.)*". Si noti che in questo lungo document un intero capitolo è dedicato al *digital cash*. Si tratta però, per lo più, della descrizione dei tentativi allora realizzati o in corso, o di speculazioni sulla possibile ricezione o compatibilità di questa moneta con i sistemi tradizionali sviluppate senza sapere con quali modalità si sarebbe potuta concretamente sviluppare questa parte del progetto crittoanarchico.

178 HUGHES E., *A Cypherpunk's Manifesto*, 1993, disponibile all'indirizzo: http://nakamotoinstitute.org/cypherpunk-manifesto/ (ultima visita 20 giugno 2017).

identità. Proprio come quando si compra un giornale in un'edicola non occorre dichiarare il proprio nome e cognome, così l'autore ritiene che anche nell'ambito digitale debba essere possibile realizzare scambi senza dover comunicare informazioni che non si vogliono condividere[179].

Nella visione di Hughes, nell'era digitale la salvaguardia della privacy dipende dalla creazione di un sistema di scambi anonimo e dal ricorso alla crittografia. Il movimento *cypherpunk* viene quindi definito come il movimento di coloro che si rendono conto di questa esigenza e che, sapendo che la privacy non sarà loro concessa "*benevolmente*" dallo Stato o dalle *corporation*, si attrezzano per scrivere programmi informatici a difesa della privacy delle persone. Da qui il motto che diventerà una delle frasi più rappresentative del movimento: "*Cypherpunks write code*".

Seppur sia meno presente l'aspirazione al fondamento di una società nuova, traspare comunque una visione del mondo e della società nella quale il libero scambio economico monetario ha un ruolo centrale e dirimente. Per questo la rivendicazione della *privacy* è declinata con particolare riferimento all'esigenza di un sistema di scambi che permetta di mantenere l'anonimato, piuttosto che nel contesto della libertà di espressione e di comunicazione o della partecipazione associativa e politica.

Per favorire il confronto su questi temi e la scrittura di programmi di crittografia, Eric Hughes e Timothy May crearono insieme a John Gilmore, nel 1992, la *Cypherpunk Mailing List*, che diventa punto di riferimento e principale forum di discussione e confronto del movimento *cypherpunk*. Negli anni a venire l'opinione pubblica viene gradualmente sensibilizzata sul tema della privacy digitale, sempre più persone sono coinvolte nelle discussioni e nascono nuove mailing list e gruppi di discussione dedicati al fenomeno. Nel 2001 la *Cypherpunk Mailing List* viene in parte riorganizzata perché considerata ormai troppo dispersiva e non più uno strumento efficace di confronto e

[179] È facile immaginare, sebbene non ci siano riferimenti diretti sul punto, come sullo sfondo di queste riflessioni vi sia una contrapposizione netta di due diverse esperienze molto concrete di denaro: da un lato l'uso del contante come mezzo di scambio che garantisce l'anonimità e, dall'altro lato, i circuiti del credito bancario, in particolare negli Stati Uniti quello legato alle carte di credito, che hanno contribuito alla nascita delle banche dati con le *credit history* dei titolari, con tutto quello che ne è seguito in termini di accessibilità ai servizi finanziari e di segmentazione sociale della popolazione.

informazione tanto che taluni la considerano ormai morta e obsoleta[180]. Nel contempo, era già attiva un'altra mailing list dedicata alla crittografia più specificatamente orientata alla discussione degli aspetti tecnologici e alla ricerca e sviluppo di soluzioni tecniche che permettessero avanzamenti nel campo della crittografia e nell'applicazione della crittografia a bisogni della vita reale[181]. Su questa *mailing list* Satoshi Nakamoto pubblica per la prima volta informazioni sul suo progetto di moneta digitale anonima basata sulla crittografia: i bitcoin[182].

Prima di lui altri programmatori provarono a raccogliere la sfida originariamente lanciata dal movimento crittoanarchico, cioè creare sistemi di pagamento digitali che permettessero di regolare scambi nel mondo digitale proteggendo l'anonimato dei contraenti, aprendo la strada al contributo cruciale portato da Satoshi.

1.2. I problemi teorici connessi alla creazione di una moneta virtuale

Il movimento crittoanarchico si propone, quindi, di creare un sistema di pagamento virtuale che preservi l'anonimato. La moneta che si immagina di utilizzare a questo scopo è essenzialmente la trasposizione di un ideale astratto di moneta merce all'interno del mondo digitale: una «moneta-merce digitale», che possa essere trasferita da computer a computer sulla rete in cambio della prestazione di servizi o della consegna

---

[180] V. WILL RODGER, *R.I.P. Cypherpunks*, in *SecurityFocus*, 2001-11-29, disponibile all'indirizzo http://www.securityfocus.com/news/294 (ultima visita 20 giugno 2017)

[181] Non è questa la sede per dare conto del vivace dibattito che si sviluppa in questa mailing list, ma è opportuno osservare che non risulta vi fosse una frattura esplicita o implicita tra questa nuova mailing list e la tra questa nuova mailing list e la Cypherpunk Mailing List o in generale con i lmovimento Cypherpunk. Al contrario, v'è evidenza di continuità culturale e prossimità tra le due esperienze. Ne sono esempio i messaggi con cui si dà notizia di riunioni ed incontri del movimento cypherpunk (v. per tutti il messaggio *SF Bay Area Cypherpunks 5/12/01 Meeting – Stanford*, del 10-5-2001. http://www.metzdowd.com/pipermail/cryptography/2001-May/000080.html, ultima visita 20 giugno 2017), nonché gli aggiornamenti sulle modifiche che hanno interessato la *Cypherpunk Mailing List* nel 2001 (*R.I.P. Cypherpunks*, del 29-11-2001, http://www.metzdowd.com/pipermail/cryptography/2001-November/001332.html, ultima visita 20 giugno 2017, e *Cypherpunks List Info*, del 31-12-2001, http://www.metzdowd.com/pipermail/cryptography/2001-December/001492.html, ultima visita 20 giugno 2017). L'archivio dei messaggi pubblicati sulla mailing list è disponibile al sito: http://www.metzdowd.com/pipermail/cryptography/ (ultima visita 20 giugno 2017).

[182] v. NAKAMOTO S., *Bitcoin P2P e-cash paper*, messaggio del 31–10–2008, disponibile al sito http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html (ultima visita 20 giugno 2017).

di beni. A questa specifica accezione si farà, quindi, riferimento nel corso di queste prime riflessioni con il termine «moneta digitale»: un mezzo di pagamento utilizzabile su internet con la stessa semplicità con cui nella vita reale si utilizza il contante[183].

Prima di concentrare l'attenzione sui tentativi che hanno preceduto i bitcoin, è utile evidenziare due problemi connessi alla creazione di una moneta virtuale: il primo è il problema della replicabilità dei beni digitali e della conseguente necessità di un emittente o garante della genuinità del bene digitale/moneta, il secondo, collegato al primo, è il problema del cd. "double spending".

1.2.1. *La replicabilità dei beni digitali e il problema della contraffazione della moneta digitale*

Com'è noto, qualsiasi documento memorizzato in modo digitale altro non è che una particolare sequenza di informazioni scritte secondo il linguaggio binario: una serie di 0 e di 1 memorizzata su un supporto digitale, di per sé sempre replicabile. Inoltre, trattandosi di informazioni, i beni digitali non sono, in senso stretto, beni rivali: la lettura di un file non ne preclude la simultanea copia, così come l'uso di una "copia" non ha di per sé alcun effetto sul file "originale": la stessa nozione di originale e copia è di per sé sindacabile, essa ha senso solo per quanto attiene l'ordine temporale della registrazione delle informazioni sul supporto, posto che la copia e l'originale sono, in questo frangente, perfettamente identici.

Per replicare gli effetti economici del regime di proprietà privata tipico dei beni materiali nel mondo digitale occorre, quindi, creare artificiosamente rivalità ed escludibilità, operando, o sul piano delle regole giuridiche che disciplinano il comportamento degli agenti, o sul piano degli applicativi mediante i quali si usano le informazioni memorizzate. Centrale in entrambi i casi è il riferimento alle licenze:

[183] Il punto di vista adottato da questi programmatori è riconducibile ad una narrativa dominante nell'economia ortodossa che non considera la moneta come istituzione sociale e giuridica, bensì la descrive in primo luogo come una merce, soggetta alle dinamiche dell'offerta e della domanda. Tale approccio è estremamente riduttivo se portato al di fuori della stretta analisi economica (cfr. *supra*) e risulta quasi paradossale nel contesto digitale dove è evidente (v. *infra*) che i beni digitali non sono beni reali. Nella trattazione seguiremo comunque la *démarche* intellettuale seguita dai programmatori che si sono interessati al problema domandandosi come fosse possibile riprodurre nel mondo digitale un bene che funzioni come mezzo di scambio universale in ragione della sua scarsità.

autorizzazioni all'uso di un certo set di informazioni. Dal punto di vista dell'approccio regolamentare-legale, l'assenza di una licenza valida implica la illiceità dell'uso delle informazioni, mentre sotto il profilo tecnico, al fine di impedire usi non autorizzati, si cerca di creare applicativi che automaticamente smettano di funzionare in assenza di una licenza valida.

Si immagini, per esempio, il caso di un programma per la video scrittura. Il software è esso stesso un insieme di informazioni memorizzate su un supporto digitale ed in quanto tale è facilmente replicabile su un numero infinito di dispositivi. Al fine di permettere la valorizzazione economica del programma secondo un modello basato sulla proprietà privata e sull'escludibilità dei beni, si opera simultaneamente su entrambi i livelli sopra richiamati. Sul piano dei rapporti tra gli agenti economici, la legge proibisce la copia non autorizzata tramite licenza dal titolare del diritto di proprietà intellettuale. Sul piano tecnologico, il produttore del *software* struttura l'applicativo in modo che possa essere usato solo a condizione che l'utilizzatore inserisca un codice che identifica univocamente una licenza valida: una password che viene associata al singolo utilizzatore e alla macchina con cui è usato il software. Attraverso questi meccanismi, la mera copia delle informazioni memorizzate che compongono il software (di per sé sempre possibile) non offre alcuna utilità.

Il problema della replicabilità delle informazioni digitali non riguarda, ovviamente, solo gli applicativi, ma si pone in termini simili anche con riferimento a documenti o registrazioni digitali o a qualsiasi altro file non eseguibile. La soluzione tecnica immaginata in questo caso è l'utilizzo di sistemi automatici di gestione dei diritti digitali (cd. Digital Rights Management, "DRM"), in forza dei quali il documento in circolazione può essere letto ed utilizzato solo attraverso programmi che sono in grado di verificare la legittimità del possesso e dell'utilizzo del file.

In entrambi i casi, la non replicabilità dell'informazione digitale è gestita mediante l'attribuzione di una licenza individuale e identificabile, abbinata al programma o inserita all'interno del file secondo le circostanze, la quale a sua volta presuppone l'esistenza di

un sistema di gestione delle licenze controllato da qualcuno, sia egli il detentore dei diritti di esclusiva ovvero, più frequentemente, un soggetto terzo[184].

In rapporto alla moneta digitale, la questione sopra posta si traduce nella necessità di garantire la genuinità e la scarsità del bene monetario, ossia nel simultaneo problema di come garantire la autenticità della moneta-bene digitale e al tempo stesso evitare che tale moneta-bene digitale sia copiata un numero infinito di volte. In termini monetari, alla replicabilità dei beni digitali corrisponde, quindi, il problema di come garantire la scarsità necessaria perché la moneta conservi il suo valore, risultato che si ottiene, trattandosi di beni creati artificialmente, solo se i meccanismi all'uopo predisposti riescano a garantire la "genuinità" del bene digitale evitando la contraffazione.

In altri termini, nel contesto digitale il problema della contraffazione è ribaltato: da un lato la digitalizzazione permette la perfetta conoscibilità del bene, sicché è molto più semplice impedire la circolazione di beni simili, ma non esattamente rispondenti ai criteri che definiscono il modello di moneta digitale in uso, mentre nel mondo reale l'ipotesi di circolazione di beni estremamente simili ma non perfettamente uguali rappresenta l'esempio tipico di contraffazione di monete; ma al tempo stesso la digitalizzazione permette di creare copie identiche ed indistinguibili dall'originale, sicché la contraffazione si presenta nella nuova veste della copia questa volta identica, ma sempre non autorizzata, di un bene digitale esistente. Stante la proprietà di perfetta replicabilità di un bene digitale – inteso come serie di informazioni registrate su un supporto digitale – è, dunque, logicamente impossibile concepire l'esistenza di un bene digitale "scarso" – *i.e.* rivale e limitato –, se non in relazione ad uno o più meccanismi che svolgano la funzione di produrre, gestire e garantire artificiosamente tale scarsità[185]. Esattamente come nel caso del programma di video scrittura o del brano musicale protetto

---

[184] Nel contesto della gestione delle licenze digitali hanno acquistato particolare importanza i negozi online integrati con i sistemi operativi dei *device* sui quali saranno eseguiti i programmi o saranno fruiti i file: si pensi al dispositivo *Kindle* di Amazon, all'*app store* di Apple e a *Google Play*.

[185] Tale considerazione permette di cogliere la complessità a al contempo la tensione irrisolvibile della sfida del movimento crittoanarchico di riuscire a creare un mezzo di pagamento per il quale è necessario un meccanismo che crei artificiosamente scarsità, sulla base di un modello concettuale di moneta in cui non si prevede un'istituzione in grado di controllare la quantità offerta di quel bene (il modello, cioè, della moneta merce, secondo cui certi metalli già presenti in natura e non artificialmente replicabili sono utilizzati come mezzo di pagamento). Sul punto si tornerà con maggiore attenzione in seguito.

da meccanismi di *Digital Rights Management*, il problema della creazione di una moneta digitale con il quale si sono confrontati i crittoanarchici si traduce nella sfida di creare un sistema che attribuisca scarsità e univocità a beni digitali facilmente scambiali salvaguardando l'anonimato degli utenti[186].

Si tratta, quindi, di un modello teorico diverso rispetto alla moneta intesa come bene materiale scarso esistente nel mondo reale. Si pensi al caso dei metalli per lungo tempo utilizzati nella tradizione occidentale come moneta: l'oro e l'argento. Questi metalli sono per natura scarsi, non occorre esista un sistema che "garantisca" la scarsità perché ne esiste una quantità limitata complessivamente disponibile in natura e perché sono beni rivali, il cui uso esclude l'uso simultaneo da parte di un altro soggetto. Mentre, si è visto, un bene digitale non è mai scarso per natura, al più se ne può restringere l'accesso o l'uso mediante l'implementazione di particolari regole nei sistemi di gestione dello stesso.

È possibile, invece, riscontrare il concetto espresso comparando l'ipotesi della creazione di una moneta digitale e la circolazione bancaria di denaro elettronico, seppur i due fenomeni presentino livelli di complessità e astrazione molto diversi. Nel caso di pagamenti tramite il sistema bancario per mezzo di ordini impartito in forma elettronica, per esempio un bonifico trasmesso via internet o un pagamento effettuato con il bancomat, l'informazione digitale trasmessa elettronicamente dall'utente alla banca è un ordine di trasferimento di valori iscritti sul conto corrente intestato all'utente a beneficio di un altro conto corrente aperto nella stessa o in altra banca. Assumiamo per semplicità che l'ordine riguardi due conti nella stessa banca e tralasciamo, per il momento, il fatto che tali valori rappresentino un credito nei confronti della banca ed il contesto giuridico entro cui si svolge tale scambio. I valori trasferiti tra i due conti sono, da un punto di vista informatico, informazioni digitali che la banca conserva e gestisce attraverso i propri software. Mediante l'uso di quei programmi la banca modifica l'ammontare di euro corrispondente a ciascun conto, cioè l'informazione digitale riguardante la quantità di moneta elettronica presente sul conto. Anche in questo caso, come si è prima evidenziato, l'esistenza di una rappresentazione digitale di valori monetari dipende dall'esistenza di

[186] Cfr. SZABO N., *Scarce Objects*, 2004, disponibile all'indirizzo http://nakamotoinstitute.org/scarce-objects/ (ultima visita 20 giugno 2017).

software e procedure gestionali che gestiscono le informazioni memorizzate garantendone la non riproducibilità o comunque l'inutilizzabilità di eventuali copie digitali.

La sfida lanciata dal movimento crittoanarchico di creare una moneta digitale anonima si deve intendere, quindi, più o meno esplicitamente, nei termini di una sfida a creare un sistema che permetta di limitare la replicabilità di beni digitali, senza ricorrere ad un ente centrale e ad identificativi personali che comprometterebbero l'anonimità degli utilizzatori.

1.2.2. *La gestione del problema della doppia spesa*

La perfetta replicabilità dei beni digitali comporta, lo si è evidenziato, il rischio che un certo bene digitale che identifica una determinata somma di unità monetarie sia copiata un numero infinito di volte: per questo occorre un sistema che gestisca e preservi – cioè, «regoli» – la scarsità della moneta digitale. Una volta che tale sistema sia creato, il problema della replicabilità e non rivalità delle informazioni digitali si manifesta concretamente nel rischio che una persona in possesso di una certa quantità di moneta digitale provi ad alienare la stessa a più persone contemporaneamente, cioè l'ipotesi di *double spending* o, in italiano, doppia spesa. A fronte di questo rischio si nota, peraltro, come nel contesto di un sistema di moneta digitale, poiché il valore d'uso della moneta – in questo contesto ancora intesa come mezzo di scambio assimilabile ad un bene – coincide, in linea di massima, con il trasferimento della stessa a terzi, la replicabilità delle informazioni digitali sia particolarmente problematica. Se si considera, poi, che nel mondo digitale la trasmissione delle informazioni è estremamente veloce ed è possibile interagire con più soggetti simultaneamente poiché non occorre essere fisicamente in un luogo specifico ma è sufficiente essere connessi, si deduce perché il problema della doppia spesa abbia catalizzato l'attenzione degli addetti ai lavori e sia considerato il primo dei problemi che un sistema di gestione di una moneta digitale deve risolvere: un vero e proprio banco di prova per qualsiasi nuova proposta.

A livello teorico, una soluzione che permette di risolvere il problema della replicabilità dei beni digitali non è utilizzabile come moneta digitale se non risolve, per lo meno entro un margine di ragionevolezza, anche il problema della doppia spesa, cioè

dell'uso simultaneo del bene scarso creato dal sistema; mentre la soluzione a questo secondo problema implica necessariamente che esista già un meccanismo capace di garantire la scarsità delle risorse digitali all'interno del sistema. Probabilmente per questo è raro che negli scritti che trattano di moneta digitale siano evidenziati entrambi i problemi teorici, che qui si sono voluti presentare entrambi, per evidenziare come l'esistenza di un sistema che disciplini l'attribuzione di moneta digitale sia indispensabile e che la capacità di gestire ipotesi di doppia spesa sia solo un attributo che qualifica l'affidabilità di tale sistema.

Nel contesto della moneta fiduciaria in uso ai nostri giorni nelle economie occidentali, il problema della doppia spesa nel contesto di mezzi di pagamento astratti è agevolmente risolto grazie all'intermediazione bancaria. Attraverso l'impiego di intermediari che registrano le disponibilità monetarie di ciascun soggetto è semplice verificare che tali risorse non siano utilizzate più di una volta. A livello teorico questa soluzione può essere descritta nei termini di una serie di registri contabili collegati alla posizione personale di ciascun soggetto, cui nel mondo reale corrispondono contratti di conto corrente stipulati tra utilizzatori e una banca, gestiti da un garante (la banca). Questo sistema non è compatibile con la protezione dell'anonimato, perché presuppone un rapporto di mandato tra il garante-gestore del conto corrente e l'utilizzatore.

In sintesi, abbiamo evidenziato due problemi tecnici che a livello teorico occorre risolvere al momento della creazione di una moneta digitale:

(i) la perfetta replicabilità e non rivalità di qualsiasi informazione registrata in modo digitale pone dei problemi rispetto all'attributo di scarsità che caratterizza ogni moneta, per ottenere la quale è necessario garantire la rivalità del bene; poiché la rivalità di un bene digitale dipende a sua volta dall'esistenza di un meccanismo di gestione esterno la cui esistenza presuppone tipicamente l'esistenza di un "garante", se ne deduce che per avere una moneta digitale occorre esista un meccanismo di "gestione della scarsità", un garante che regola la quantità di moneta in circolo e ne impedisce la contraffazione;

(ii) ancora in ragione degli attributi che caratterizzano il mondo digitale, il trasferimento di un bene digitale-moneta digitale tra un attore all'altro è

soggetto al forte rischio di *double spending* o doppia spesa; la gestione e minimizzazione di questo rischio costituisce il bando di prova dell'affidabilità del sistema.

Questi due problemi possono essere collegati a situazioni tipiche affrontate all'interno dei sistemi giuridici a noi più familiari:

(i) il primo problema richiama l'esigenza di garantire la certezza della proprietà mobiliare ed immobiliare in capo ai consociati, ed è anche ricollegabile alla posizione dell'emittente di strumenti finanziari e degli intermediari coinvolti nell'emissione i quali devono garantire la gestione degli strumenti finanziari dematerializzati e degli appositi registri;

(ii) il problema della doppia spesa corrisponde grossomodo alla fattispecie civilistica della doppia alienazione, ben conosciuta sin dall'epoca romana e risolta, dal punto di vista giuridico, o mediante un sistema di registro della proprietà o attraverso l'applicazione di presunzioni legale al possesso o al trascorrere del tempo.

Similmente, è possibile evidenziare i ragionamenti economici sottesi ai due temi oggetto di attenzione nei seguenti termini. Perché un bene digitale possa essere utilizzato come moneta occorre che:

(i) la quantità di tale bene disponibile sul mercato sia limitata e sia appropriabile dai partecipanti al mercato, giacché se non v'è scarsità del bene e rivalità nell'uso non è possibile attribuirgli un valore economico;

(ii) l'uso della moneta digitale deve comportare la minor assunzione possibile di rischi inerenti la validità del trasferimento: una moneta il cui uso come mezzo di scambio richieda particolari accorgimenti o ricerche comporta costi transattivi che ne rendono economicamente sconveniente l'uso.

1.3. I primi tentativi di creazione di monete digitali anonime

Svolte queste premesse teoriche circa il contesto in cui si sviluppano i primi tentativi di realizzazione di una moneta digitale anonima, è ora possibile presentare queste esperienze.

1.3.1. *Il Digital Cash di David Chaum*

Dal punto di vista tecnologico, i bitcoin non potrebbero esistere senza l'invenzione, negli anni settanta, della crittografia asimmetrica. Mentre nei sistemi di crittazione simmetrici la stessa chiave segreta è usata per cifrare e decifrare il messaggio che si vuole trasmettere, questo sistema, detto anche di crittografia a doppia chiave o crittografia a chiave pubblica, prevede l'utilizzo di due chiavi diverse per la cifratura e la decrittazione. Grazie alla presenza di due chiavi diverse è possibile comunicare apertamente la chiave di cifratura, che può essere conosciuta da chiunque e per questo viene chiamata «chiave pubblica». Una volta codificato il messaggio con una delle due chiavi, normalmente quella pubblica, solo chi conosce la corrispondente chiave, tenuta privata, può decodificarne il contenuto.

David Chaum è il primo programmatore che ha immaginato di ricorrere alla crittografia a chiave pubblica per la creazione di una moneta digitale. Il sistema è diverso rispetto all'impianto che sarà adottato con i bitcoin, ma rappresenta un primo importante tentativo di realizzare un mezzo di pagamento che garantisce l'anonimato al momento dello scambio. Questa è, inoltre, la prima ipotesi di moneta elettronica in cui si immagina che alle persone siano associate chiavi crittografiche asimmetriche personali.

Con i crittoanarchici Chaum condivide la preoccupazione che i sistemi di pagamento informatizzati possano ledere la privacy delle persone, ma al tempo stesso è preoccupato anche degli usi poco commendevoli che si potrebbero fare di una moneta che garantisca l'anonimato totale, quali, per esempio, la corruzione, l'evasione fiscale e l'uso nel mercato nero o in traffici illeciti[187]. Egli propone, quindi, di usare la crittografia asimmetrica per creare dei certificati al portare che rappresentano un credito nei confronti di una banca. Si tratta, essenzialmente, di un meccanismo di rappresentazione elettronica della valuta utilizzata nel mondo reale che ha la particolare caratteristica di garantire l'anonimato del possessore: un sistema di banconote private digitali ad emissione bancaria privata.

Il ragionamento del brillante programmatore si fonda sull'intuizione che la crittografia a doppia chiave permette non solo di trasmettere informazioni tra due persone

[187] CHAUM D., *Blind Signatures for Untraceable Payments*, in *Crypto* 82, 1982, pp. 199–203.

in modo riservato, ma anche di creare un collegamento univoco tra un soggetto e un bene digitale, che può essere usato per garantire il controllo esclusivo sullo stesso[188]. Il meccanismo di cifratura opera, in questo caso, in modo leggermente diverso rispetto alla trasmissione di informazioni riservate, perché l'obbiettivo non è informare selettivamente qualcuno a proposito di qualcosa impedendo a terzi di intercettare il messaggio, ma limitarne l'accesso a tali informazioni a tutti i terzi indistintamente, creando così un vincolo di utilizzabilità sul bene che riproduce nel mondo digitale una dinamica di possesso esclusivo su un bene reale. È sufficiente, infatti, che il possessore codifichi un file con una delle due chiavi per evitare che chiunque altro non sia in possesso della chiave privata possa accedere ed utilizzare quel file .

A partire da questa riflessione Chaum sviluppa un un meccanismo di doppia firma che chiama "*blind signatures*", che può essere impiegato in ambito monetario per gestire un sistema di pagamento tra due soggetti intermediato da una banca in cui non occorre svelare l'identità del dante causa alla banca al momento dell'incasso. Il sistema si fonda sull'applicazione di due chiavi di cifratura. Un primo soggetto (il dante causa) critta delle informazioni con la sua chiave pubblica e trasmette il file crittato ad un secondo soggetto (la banca), il quale a sua volta applica un algoritmo matematico di cifratura con la sua chiave pubblica[189]. Al momento della firma il secondo soggetto non sa quali informazioni sono state originariamente cifrate. Il primo soggetto, a questo punto, può decodificare il file ricevuto con la sua chiave privata, ottenendo una versione delle informazioni originali cifrate dal secondo soggetto (e di cui il secondo soggetto, la banca, è quindi in grado di riconoscere l'autenticità), che non contiene alcun riferimento alla sua identità[190].

Per comprendere come questo meccanismo possa permettere la creazione di un contante digitale occorre immaginare che il secondo soggetto sia una banca e che sia convenzionalmente stabilito che il file cifrato dalla banca valga una determinata somma di denaro. Il file ottenuto alla fine del procedimento della *blind signature* dal primo

---

188 Cfr. LESSIG L, *Code. Version 2.0*, Basic Books, 2006, p. 53. Questa è la particolare potenzialità della crittografia che permette l'automatizzazione di processi giuridici all'interno di *software* e lo sviluppo di *smart contracts* ad un livello altrimenti non immaginabile.

189 *Ibidem*.

190 Il sistema si chiama "*blind signatures*" perché il secondo soggetto firma un documento che non può leggere, ma che può comunque validamente firmare: da qui il nome di 'firma al buio'.

soggetto può, allora, essere fatto circolare come mezzo di pagamento e sarà restituito alla banca quando il possessore deciderà di farsi accreditare il controvalore del titolo digitale in valuta sul proprio conto corrente. Al momento della ricezione la banca non sa a chi abbia originariamente dato il titolo digitale che è circolato, ma può verificarne l'origine al momento dell'incasso decodificandolo con la propria chiave privata.

Chi compie il pagamento è, quindi, il primo soggetto dell'esempio precedente, che convenzionalmente nel mondo anglosassone è chiamato Alice. Alice si rivolge ad una banca consegnando un file cifrato. La banca firma il documento digitale, preleva l'equivalente in denaro dal conto corrente di Alice e le consegna il nuovo file cui sono state applicate, a questo punto, due chiavi di cifratura. Al momento di effettuare il pagamento, Alice applica la propria chiave di decodifica, rende anonimo e "spendibile" il documento digitale e lo trasmette a Bob. Bob può verificare il collegamento tra il documento e la banca, anche se in quel momento non sa se tale documento è già stato usato per pagare un altro bene o servizio. Per incassare il valore del titolo ricevuto, Bob trasmette alla banca il documento. La banca decodifica il documento con la propria chiave privata accertandosi dell'originalità del documento e di non avere già ricevuto il file per l'incasso. Se entrambe le verifiche hanno esito positivo, la banca accredita il valore del documento digitale in valuta sul conto corrente di Bob. Per effetto dell'applicazione della doppia firma e della successiva codifica della firma di Alice, al momento dell'incasso la Banca potrà verificare l'autenticità e la propria sottoscrizione dello stesso, ma non la provenienza originaria: non potrà cioè, in questo esempio, ricollegare il titolo ad Alice. In sostanza, il modello ipotizza la creazione di un assegno al portatore nel quale si possa fare a meno di indicare il disponente.

Il modello descritto fu ulteriormente elaborato da Chaum con altri due programmatori israeliani[191]: introducendo la possibilità di spendere il titolo originale a

[191] CHAUM D., FIAT A. e NAOR M., *Untraceable Electronic Cash*, in Goldwasser S. (a cura di), *Advances in Cryptology — CRYPTO' 88. Lecture Notes in Computer Science*, vol. 403, Springer, 1990. Espone sinteticamente il meccanismo anche FINLEY H., *Detecting Double-Spending*, 15 Ottobre 1993, 2 ed. 13 Marzo 1996, pubblicato all'indirizzo https://web.archive.org/web/20140410150152/http://www.finney.org/~hal/chcash2.html (ultima visita 20 giugno 2017); e cfr. anche CHAUM D., *Online Cash Checks*, 1989, disponibile all'indirizzo http://www.chaum.com/publications/Online_Cash_Checks.html 04/10/2016 (ultima visita 20 giugno 2017).

più riprese, tesaurizzando il resto per ulteriori spese future come se fosse un nuovo titolo, e rendendo più complesso il meccanismo di cifratura e decrittazione del documento digitale in modo tale che qualora il documento fosse stato utilizzato più di una volta, la banca sarebbe stata in grado, al momento della seconda richiesta di incasso, di risalire alla persona che ne aveva chiesto l'emissione[192].

Il lavoro di sviluppo di questo sistema di contante digitale proseguì sino ad uno stadio avanzato e Chaum provò a commercializzare la propria invenzione tramite una società dallo stesso fondata, raccogliendo l'interesse di importanti finanziatori, tra cui Microsoft, che intendeva includere il sistema come applicazione nativa all'interno del sistema operativo Windows 95, e il consorzio VISA, interessato ad elaborare nuovi sistemi di pagamento digitali[193]. Le parti non trovarono, però, un accordo commerciale soddisfacente. Il programma fu, così, marginalizzato e progressivamente superato da altre soluzioni alternative che agevolarono i pagamenti su internet sacrificando la privacy degli utenti in cambio di facilità e rapidità di utilizzo[194].

Il *digital cash* di Chaum resta in ogni caso un importante modello di sistema di pagamento, sia per la originalità della struttura immaginata, sia per la capacità di conciliare la tutela della privacy con l'infrastruttura monetaria esistente. Si tratta, infatti, di un sistema che non avrebbe provveduto all'emissione di una nuova moneta, cioè alla creazione di una nuova unità di conto e di nuovi mezzi di pagamento, con conseguente nuova distribuzione originaria di risorse, bensì avrebbe costituito unicamente una miglioria tecnologica delle modalità con cui le risorse esistenti possono essere trasferite tra consociati garantendo la privacy degli stessi. Un sistema di pagamento per certi versi simile rispetto a quelli oggi in uso cui si sarebbero probabilmente applicate le direttive Europee sui sistemi di pagamento e sugli emittenti di moneta elettronica, con la particolarità di garantire un certo livello di anonimato, non totale e non irreversibile, agli utilizzatori.

---

192 In questo modo Alice sarebbe disincentivata dal provare a spendere due volte la stessa il proprio denaro e Bob sarebbe indirettamente protetto dal rischio di doppia spesa.

193 FRISBY D., *Bitcoin, The Future Of Money?*, Unbound, 2014, capitolo 1.

194 Il *digital cash* trovò comunque spazio per una limitata implementazione in un progetto della Deutche Bank: Cfr. PITTA J., *Requiem for a Bright Idea*, 11 gennaio 1999, in https://www.forbes.com/forbes/1999/1101/6411390a.html (ultima visita 20 giugno 2017).

L'obbiettivo perseguito da Chaum era, infatti, separare l'uso del mezzo di pagamento dalla registrazione contabile sui conti correnti bancari e per questo è stato proposto un sistema automatico di pagamento con le seguenti tre caratteristiche:

(i) impossibilità per le parti terze di determinare colui che ha pagato;

(ii) la possibilità di mostrare una ricevuta del pagamento o di individuare colui che ha pagato in casi eccezionali; e

(iii) la possibilità di impedire l'uso di mezzi di pagamento rubati (o falsi).

In sintesi, l'intuizione di Chaum è stata utilizzare la crittografia per creare un sistema di titoli al portatore nei quali l'identità del portatore sia celata e possa essere rilevata solo in caso di double spending.

Nel modello teorico proposto da Chaum, la crittografia è usata per permettere la riconducibilità di un certo titolo di credito ad una banca e per tutelare l'anonimato del soggetto che compie il pagamento. L'implementazione della crittografia asimmetrica nel sistema di firma al buio permette, cioè, di anonimizzare al momento dell'uso il titolo di credito digitale originariamente emesso all'interno di un rapporto bilaterale in cui entrambe le parti sono note, salvaguardando il vincolo tra titolo ed emittente.

La moneta digitale di Chaum non è altro, quindi, che una rappresentazione digitale di un credito nei confronti della banca la cui emissione è strutturata in modo tale da garantire, a certe condizioni, l'anonimato del creditore originario. Il problema della doppia spesa è risolto al momento della presentazione del documento per l'incasso e dipende dalla capacità della banca di tenere correttamente un registro dei documenti già incassati. Tale soluzione impone a chi riceve il pagamento di presentare subito il documento digitale per l'incasso. La possibilità di rivelare l'identità del pagatore in caso di doppia spesa opera, però, come forte deterrente contro l'uso illecito del contante digitale.

1.3.2. *Una moneta fatta di calcoli: il* b-money *di Wei Dai*

Di diversa natura è la moneta concepita da Wei Dai, il quale non limita la sua riflessione alla ricerca di un mezzo di pagamento che permetta di trasferire depositi bancari in modo elettronico mantenendo l'anonimato, ma immagina una moneta

completamente autonoma ed indipendente dal sistema tradizionale bancario: un'unità di conto digitale provvista di un mezzo di pagamento digitale, il *b-money*[195].

Il punto di partenza da cui muove la riflessione è, ancora una volta, l'esigenza specifica che caratterizza il progetto politico crittoanarchico. Wei Dai è affascinato dalla teorizzazione della crittoanarchia di Tim May e dall'idea di realizzare comunità in cui la violenza sia resa impossibile perché ciascun soggetto agente è conosciuto solo grazie al suo pseudonimo e non per la sua vera natura fisica. Si immagina, quindi, una comunità sociale formata da individui connessi in rete che non si conoscono tra di loro se non mediante l'uso di pseudonimi, e si prova ad immaginare uno strumento di scambio universale condiviso che possa essere utilizzato senza dover svelare la propria identità. La riflessione parte dal presupposto che qualsiasi comunità per definirsi tale richiede un certo livello di cooperazione, che tale cooperazione si riduca essenzialmente alla possibilità di stipulare ed eseguire contratti e che per raggiungere tale obbiettivo occorra e sia sufficiente un mezzo di scambio. In piena sintonia con le visioni libertarie che lo accumunano ad altri critto anarchici, per Wei Dai la "cooperazione" che definisce una comunità ha quindi ben poco di "pubblico" o di comunitario: essa consiste unicamente nella possibilità di scambiare beni e servizi senza dover ricorrere all'esercizio del potere o del controllo da parte di un'autorità politica terza rispetto alle parti in causa[196]. L'obbiettivo perseguito con la proposta del *b–money* è quindi offrire un mezzo di scambio che possa essere utilizzato tramite pseudonimi senza necessità di dover rivelare la propria identità e quindi senza alcuna connessione con il sistema giuridico statale. Il contributo che Wei Dai apporta alla discussione è, quindi, significativo anche a livello concettuale, perché con questo autore il progetto politico generale è trasposto in ambito monetario concettualizzando il requisito dell'anonimità in termini di un sistema dove i due

---

[195] WEI DAI, *b-money*, 1 Novembre1998, in http://www.weidai.com/bmoney.txt (ultima visita 20 giugno 2017), disponibile anche in http://nakamotoinstitute.org/b-money/ (ultima visita 20 giugno 2017), propone una traduzione in italiano del paper CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Giuffré, 2015, p. 16.

[196] WEI DAI, op. cit., "*A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities*".

contraenti non abbiano bisogno dell'intervento di parti terze per concludere lo scambio: con questo autore il dibattito si orienta verso l'obbiettivo di creare una moneta *ex novo* che possa essere usata da tutti i membri indipendente dall'esercizio di funzioni pubbliche.

L'invenzione di un sistema completamente avulso dal contesto istituzionale esistente pone, in aggiunta alla questione della gestione del trasferimento di moneta digitale e del rischio di *double spending*, il problema di definire i meccanismi di creazione e distribuzione delle nuove unità. Per raggiungere questo scopo occorre, cioè, rispondere a due grandi questioni:

(i) la questione della distribuzione iniziale delle risorse, *id est*, nel caso specifico, la questione della creazione della moneta; e

(ii) la questione di come le risorse possono essere trasferite, *id est* la questione di come la moneta può essere trasferita tra i consociati, cui si ricollegano i problemi generali anticipati *supra*.

Con il suo contributo Wei Dai prova ad affrontare a livello astratto questi due grandi quesiti: non propone una specifica concretizzazione o un codice di programma, bensì unicamente due modelli teorici, che peraltro egli stesso riconosce essere, allo stato, ancora impraticabili, formulando idee nuove ed originali che saranno riprese nel contesto del protocollo bitcoin.

Alla prima domanda Wei Dai risponde immaginando che la moneta possa essere prodotta da chiunque ne abbia interesse e sia disposto a sopportare un costo in termini di impiego di capacità computazionale. Il principio matematico che sta alla base dell'idea era già stato suggerito nel contesto delle soluzioni tecnologiche proposte per risolvere il problema dello spamming di email. Lavorando sulle funzioni di *hash*, particolari funzioni matematiche attraverso le quali qualsiasi set di informazioni può essere tradotto in una stringa determinata di lettere e numeri[197], due matematici avevano inventato un sistema capace di produrre dei quesiti matematici la cui soluzione necessita l'impiego di una certa potenza di calcolo. Per risolvere il problema dello *spam* di email, si era, quindi, proposto di utilizzare queste funzioni per rendere computazionalmente costoso l'invio di un'email.

[197] BACK A., *Hashcash - A Denial of Service Counter-Measure*, 2002, in http://www.hashcash.org/papers/hashcash.pdf (ultima visita 20 giugno 2017); le proprietà di queste funzioni sono illustrate nel dettaglio *infra*.

Per ogni mail inviata il mittente avrebbe dovuto risolvere un certo quesito matematico, la cui soluzione può essere ottenuta solo mediante un procedimento che richiede ci compiere una serie di tentativi con una certa probabilità di successo per ogni tentativo. Fornendo la soluzione del problema matematico, la cd. *proof of work*, l'autore del messaggio avrebbe dimostrato di aver sopportato un costo pari all'impiego della propria capacità di calcolo al fine di trovare una soluzione al problema e, quindi, di essere realmente interessato all'invio del messaggio. Prendendo spunto da questo modello, Wei Dai suggerisce che la moneta digitale crittoanarchica avrebbe potuto essere prodotta da chi sarebbe stato disposto a svolgere un certo calcolo computazionale, accollandosene il costo. La moneta digitale così prodotta sarebbe stata sostanzialmente il prodotto di una funzione *proof of work* e la quantità di unità monetarie, nonché il valore delle stesse, avrebbe dovuto corrispondere al costo sostenuto per la produzione, cioè al valore di mercato della capacità computazionale impiegata[198].

L'intuizione di collegare la produzione di beni digitali a funzioni che richiedono una certa quantità di calcolo è molto interessante e risponde all'esigenza di stabilire un meccanismo comune a tutti i partecipanti, tuttavia il modello teorico è ancora molto lacunoso. Secondo Wei Dai: "*The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities. For example if a problem takes 100 hours to solve on the computer that solves it most economically, and it takes 3 standard baskets to purchase 100 hours of computing time on that computer on the open market, then upon the broadcast of the solution to that problem everyone credits the broadcaster's account by 3 units*"[199]. Questa supposta coincidenza tra valore economico delle unità e costo di produzione delle stesse comporta che tutto il beneficio della creazione di queste unità sarebbe speso per sopportare i costi di produzione, nonché un'evidente banalizzazione della moneta e dell'attribuzione di valore alla stessa. È chiaro che questo primo modello, in cui non si prevede un meccanismo che limiti la possibile creazione di moneta digitale, ha valore come intuizione di un possibile meccanismo di

198 WEI DAI, op. cit., in questi termini Dai propone di gestire la creazione di moneta: "*The creation of money. Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual*".

199 *Ivi*.

creazione di unità monetarie digitali, piuttosto che come modello compiuto di una nuova moneta. Lo stesso Wei Dai, peraltro, si rende conto nel proprio documento che il meccanismo di creazione di moneta (che egli associa implicitamente al problema dell'attribuzione di valore alle unità così prodotte) sia l'aspetto più fragile della sua teoria. Per ovviare al problema della possibile sovrapproduzione di moneta connesso anche allo sviluppo dei processori e al corrispondente costante adattamento del modello, l'autore suggerisce allora di creare un protocollo attraverso il quale i membri del sistema che custodiscono i registri contabili (su cui *infra*) si accordano sulla quantità di b-money che dovrà essere prodotta in un certo arco di tempo e indicono un'asta in cui chiunque può competere per assicurarsi dei problemi computazionali da risolvere (e produrre così nuove unità di moneta)[200].

Circa la seconda questione affrontata, relativa al trasferimento di *b-money,* occorre premettere che Wei Dai immagina che la creazione di *b-money* coinvolga un gruppo di persone collegate in un network in cui: (*i*) tutti utilizzano un sistema di crittografia asimmetrico, e (*ii*) ciascuno è rappresentato e conosciuto dagli altri solo tramite la sua chiave pubblica. Nel semplice modello teorico immaginato dal programmatore, ciascun membro del network mantiene una copia di un registro dove sono memorizzati i patrimoni, espressi in b-money, di tutti i membri. Ogni volta che nuove unità sono create il registro – *rectius* tutti i registri, uno per ogni utente – dovrebbero quindi essere aggiornati aumentando corrispettivamente le disponibilità del soggetto che ha risolto i nuovi problemi computazionali. Si immagina, seppur ciò non sia esplicitato nel breve saggio, che ciò avvenga a fronte della trasmissione della soluzione di tali problemi cifrata con chiave privata del soggetto cui devono essere accreditati i valori, in modo che la provenienza del messaggio sia garantita dalla corrispondenza con la sua firma pubblica. Un simile procedimento avverrebbe per ogni scambio di denaro: Alice invierebbe un messaggio cifrato con la propria chiave privata in cui impartisce l'ordine di trasferimento di una determinata somma di *b-money* dal proprio "conto" al "conto" di Bob, indicando le chiavi pubbliche di entrambi. Ogni trasferimento sarebbe quindi realizzato mediante l'invio al network delle informazioni relative lo scambio firmate dalla chiave personale del trasferente e la registrazione dell'operazione su tutti i registri completerebbe

[200] *Ivi*, Appendix A.

l'operazione di scambio, assicurando che non si possano verificare episodi di doppia spesa. È appena il caso di dire che il messaggio sarebbe ignorato nel caso non vi fossero sufficienti fondi intestati all'ordinante.

Anche in questo caso, è lo stesso autore ad ammettere che la soluzione immaginata sia impraticabile per le speciali caratteristiche che dovrebbe avere il network, giacché per evitare il rischio di doppia spesa e garantire l'accuratezza del registro le comunicazioni tra utenti dovrebbero essere ricevute da tutti in modo perfettamente sincrono e senza ritardi o errori di trasmissione. Per ovviare il problema Wei Dai suggerisce, quindi, un secondo modello dove solo alcuni partecipanti mantengano le copie del registro dei conti correnti dei partecipanti, il che comporta, però il rischio di frodi e un costo in termini della fiducia che i partecipanti dovrebbero riporre nei "custodi" del registro, che si traduce nella proposta di Wei Dai di completare l'architettura del sistema prevedendo che i custodi del registro depositino un certo ammontare di risorse in speciali account a garanzia del corretto adempimento delle loro funzioni e imponendo agli stessi obblighi di *disclosure* regolare degli interi database in modo che ciascun utente possa [*sic*] verificare la correttezza del proprio account[201].

La proposta di Wei Dai consta, quindi, di un modello teorico innovativo, ma ancora allo stato embrionale. Seppur non immediatamente implementabile, il contributo è estremamente significativo perché nel *b-money* sono tratteggiate molte delle caratteristiche essenziali delle future criptovalute; in particolare le seguenti idee saranno riprese da tutte le successive ipotesi di creazione di sistemi monetari basati sulla crittografia:

- la valuta è prodotta a condizione che sia svolta una certa quantità di lavoro computazionale, secondo il meccanismo della *proof of work*;
- qualsiasi utente può partecipare alla produzione della moneta;
- l'allocazione della moneta tra i consociati è definita da un registro comune, sia per quanto attiene la distribuzione iniziale (e, quindi, la produzione di nuove

[201] *Ivi*: "*Also, each server must periodically publish and commit to its current money creation and money ownership databases. Each participant should verify that his own account balances are correct and that the sum of the account balances is not greater than the total amount of money created. This prevents the servers, even in total collusion, from permanently and costlessly expanding the money supply*".

unità), sia per quanto attiene il trasferimento di risorse tra consociati, che deve essere riportato sul registro per acquisire validità generale;

- ciascun partecipante – almeno nella prima ipotesi – ha una copia del registro, quindi non si fa affidamento ad una controparte centrale o ad un gestore terzo, bensì la gestione del registro è un'attività svolta a livello collettivo;
- la partecipazione e gli scambi avvengono mediante il ricorso a un sistema di cifratura asimmetrica in cui:
    - gli utenti sono rappresentati da chiavi pubbliche, e
    - i trasferimenti di moneta sono realizzati medianti comunicazioni autenticate con le corrispondenti chiavi private.

Dieci anni dopo, questi concetti chiave saranno ripresi da Satoshi Nakamoto ed inclusi, seppur con una significativa rielaborazione, nell'architettura del protocollo Bitcoin, tanto che il saggio di Wei Dai sul *b-money* sarà incluso tra le poche fonti citate nel documento con cui saranno presentati per la prima volta i bitcoin.

Circa i limiti del *b-money*, può sottolinearsi quanto segue. Wei Dai risponde alla questione dell'attribuzione iniziale delle risorse con una risposta tecnica inerente le modalità di produzione delle unità digitali di *b-money* – far corrispondere nuove unità a fronte di lavoro computazionale certo –, ma come e secondo quali criteri la comunità debba riconoscere tale lavoro, quante risorse debbano essere riconosciute a fronte del lavoro svolto e in generale come regolare la produzione di nuove unità, anche a fronte del prevedibile evolversi della tecnologia e della potenza di calcolo degli ordinatori, erano tutte questioni ancora non definite. Inoltre, qui il limite più significativo della proposta di Dai, il modello ipotizza l'uso di un registro comune che tenga nota della quantità di unità di conto associata a ciascun utente, ma non è ancora in grado di spiegare in modo credibile come un simile registro possa essere gestito in modo collettivo senza delegare la responsabilità della sua tenuta a determinati soggetti: al contrario il modello reintroduce meccanismi di delega della gestione del registro a soggetti specifici senza offrire soluzioni credibili ai problemi di *agency* che verrebbero a crearsi. Ciò detto, il *b-money* è comunque il primo modello in cu si cerca di decentralizzare il sistema di gestione della moneta: sia sotto il profilo della creazione di moneta, sia sotto il profilo della tenuta dei registri contabili e dell'esecuzione degli scambi.

1.3.3. *Il «*Bit Gold*» e altri contributi di Nick Szabo*

In estrema sintesi, la proposta del *bit gold* concerne un meccanismo di creazione di beni digitali non replicabili la cui titolarità è garantita da un registro distribuito che tiene traccia dei trasferimenti[202]. La somiglianza, non solo nel nome, con il protocollo Bitcoin è molto forte, tanto che molti commentatori ritengono che Nick Szabo sia la persona che si cela dietro lo pseudonimo Satoshi Nakamoto: l'inventore dei bitcoin. Invero, oltre ad esservi forti somiglianze tra il protocollo Bitcoin e il *bit gold*, occorre aggiungere che la struttura di entrambi i modelli riflette ragionamenti e soluzioni teoriche anticipate da Nick Szabo in alcuni saggi pubblicati tra il 1997 e il 2008. Indipendentemente dalla questione di chi sia realmente l'inventore dei bitcoin e se Nick Szabo e Satoshi Nakamoto siano la stessa persona, è legittimo ritenere che tale pensatore ne abbia quantomeno influenzato lo sviluppo sia sotto il profilo dello sviluppo informatico, sia sotto il profilo delle riflessioni economico–giuridiche assunte a giustificazione e fondamento del modello. Sul punto è bene chiarire che non risultano citazioni esplicite di Szabo da parte di Satoshi Nakamoto, eppure la somiglianza dei modelli è tale che risulta difficile ritenere che essi originino, se non addirittura dalla stessa persona, da scuole di pensiero lontane tra loro. In particolare, i contributi che Szabo ha portato al dibattito inerente la creazione di nuovi sistemi monetari digitali concernono sue riflessioni: (*i*) sulle origini della moneta, (*ii*) sui costi transattivi connessi ai rapporti di agenzia e (*iii*) sui sistemi informatici di gestione di database distribuiti[203].

---

[202] SZABO N., *Bit Gold*, 2005, disponibile all'indirizzo: http://unenumerated.blogspot.it/2005/12/bit-gold.html (ultima visita 20 giugno 2017). Nel *paper* il modello dei *bit gold* è descritto solo a livello teorico, con numerosi richiami a teorie elaborate in precedenti scritti. Non viene fornita, invece, alcuna realizzazione concreta del modello nella forma di codice informatico.

[203] Tra i vari programmatori che hanno affrontato il tema della creazione di sistemi di pagamento digitali, Nick Szabo è, probabilmente, quello che più di altri ha sviluppato, parallelamente all'informatica, una particolare attenzione allo studio delle istituzioni sociali, economiche e giuridiche che nel mondo reale svolgono funzioni simili a quelle che avrebbero dovuto svolgere i programmi oggetto di sperimentazione, evidenziando frequentemente parallelismi tra un mondo e l'altro.

I «Collectibles»

Il primo di questi contributi che merita essere richiamato è connesso al tema delle origini della moneta e alle prime esperienze di creazione e uso di oggetti di valore[204]. Attingendo da studi di antropologia e archeologia, Szabo argomenta che nel corso della preistoria l'uomo ha manifestato una naturale tendenza a creare rapporti di collaborazione e socialità oltre la cerchia delle relazioni familiari, che hanno richiesto per varie ragioni il trasferimento di particolari oggetti cui veniva attribuito valore: talvolta come risarcimento per un danno subito, altre volte come dono o per tenere traccia di un evento passato, altre volte ancora come mezzo di scambio. L'autore definisce questi oggetti, che erano sostanzialmente gioielli di varia forma e natura, come "*collectibles*" e ne evidenzia alcune proprietà: l'avere un alto costo di produzione che li rende scarsi e difficilmente riproducibili, l'essere facilmente trasferibili e l'avere un basso costo di protezione contro lo smarrimento o il furto (per esempio perché indossabili).

La riflessione prosegue con l'osservazione che in ragione delle risorse e del tempo richiesti per la produzione di questi beni, ad essi veniva riconosciuto un valore da parte dei consociati e che tali "*unforgeably costly commodities*" venivano utilizzati per trasferire ricchezza all'interno di particolari circoli sociali[205].

Da queste considerazioni l'autore deduce che al fine di realizzare scambi all'interno di un gruppo sociale occorre avere dei beni il cui controllo e trasferimento implichi bassi costi e la cui copia sia, all'opposto, molto costosa, se non idealmente impossibile. Altra deduzione che Szabo ricava, implicitamente, dalle riflessioni svolte sulle origini della moneta, è che non occorre porsi il problema che tali beni, *collectibles*

---

[204] SZABO N., *Shelling Out -- The Origins of Money*, 2002, originariamente pubblicato in http://szabo.best.vwh.net/shell.html (non più accessibile), oggi disponibile all'indirizzo http://nakamotoinstitute.org/shelling-out/ (ultima visita 20 giugno 2017).

[205] La presenza di una cerchia sociale entro cui questi oggetti possano circolare è affermata come condizione stessa perché essi siano creati, per ragioni connesse all'ammortamento del costo di produzione; v. *Ibidem*: "*To be useful as a general-purpose store of wealth and means of wealth transfer, a collectible had to be embedded in at least one institution with a closed-loop cycle, so that the cost of discovering and/or manufacturing the object was amortized over multiple transactions. Furthermore, a collectible was not just any kind of beautiful decorative object. It had to have certain functional properties, such as the security of being wearable on the person, compactness for hiding or burial, and unforgeable costliness. That costliness must have been verifiable by the recipient of the transfer – using many of the same skills that collectors use to appraise collectibles today*".

o *scarse objects*, abbiano a priori un valore economico precostituito, come invece provava a fare Wei Dai con riferimento al *b-money*: l'importante è che abbiano determinate caratteristiche e che possano svolgere agevolmente la funzione di mezzo di scambio tra i consociati, sarà, poi, l'uso di questi beni che ne affermerà il valore.

Szabo riconosce in tali beni gli antesignani della moneta e dallo studio delle proprietà di questi beni deduce implicitamente le caratteristiche che deve avere un bene per poter essere utilizzato come mezzo di scambio. In coerenza con la tradizione catallattica e con l'ortodossia economica che concentra la propria attenzione sul bene utilizzato come mezzo di pagamento, l'autore considera solo marginalmente l'importanza delle regole sociali e giuridiche che caratterizzavano l'uso di tali strumenti per focalizzarsi sulle caratteristiche di tali beni e ricondurre ad esse e all'innato istinto per l'accumulazione attribuito a ciascun uomo le ragioni della nascita della moneta.

Il punto centrale dell'analisi sulle origini della moneta che sarà riflesso nel modello del *bit-gold* e nei bitcoin è l'idea che la moneta corrisponda ad un bene che è difficile produrre, nonché l'idea che non occorra tale bene abbia un valore economico d'uso o di scambio sin dal momento della sua creazione, giacché la scarsità del bene potrà contribuire all'affermazione del suo valore nel contesto degli scambi tra i consociati.

Trusted third parties *e il problema dei rapporti di* agency *nei sistemi informatici*

Un secondo ordine di contributi offerti da Nick Szabo concerne l'organizzazione di sistemi informatici riguardanti a vario titolo la gestione di rapporti commerciali, inclusi i sistemi di pagamento informatici[206]. La tesi elaborata dall'autore a questo riguardo è che occorre ridefinire le priorità e gli obbiettivi che ci si pone al momento della progettazione di tali sistemi per concentrare l'attenzione sull'esigenza di ridurre al minimo l'affidamento che occorre prestare a eventuali intermediari. Alla base del ragionamento c'è la definizione di "*trusted third party"*, o "TTP", che include tutti i soggetti che gestiscono meccanismi di intermediazione e da cui dipende a vario titolo la soddisfazione degli interessi di un partecipante, e la critica secondo cui al momento della creazione di

[206] V. SZABO N., *Trusted Third Parties Are Security Holes*, 2001, originariamente pubblicato in http://szabo.best.vwh.net/ttps.html (non più accessibile), disponibile all'indirizzo http://nakamotoinstitute.org/trusted-third-parties (ultima visita 20 giugno 2017).

sistemi informatici si dia per scontata la presenza di un amministratore in grado di intervenire sul sistema che assume la responsabilità di garantire il corretto funzionamento e la sicurezza dello stesso. La presenza di tali TTP comporta, di fatto, l'introduzione di un intermediario. In termini economici, la necessità di doversi affidare ad un terzo per la gestione dei propri interessi comporta sempre un certo grado di asimmetria informativa tra *principle*, il soggetto che usufruisce del servizio, e *agent*, l'operatore che concretamente gestisce il servizio, e tale asimmetria informativa comporta sempre dei costi legati alla divergenza di interessi tra mandante e agente e la difficoltà di controllo del primo sul secondo. Sulla scorta di queste considerazioni l'autore suggerisce che nel contesto dei sistemi informatici la gestione del rapporto di *agency* tra utilizzatori e gestore centrale costituisca di gran lunga il costo più significativo e suggerisce quindi che nella progettazione di tali meccanismi di intermediazione gli sforzi siano orientati alla minimizzazione del ruolo di tali controparti/amministratori centrali.

Le osservazioni che precedono nascono dall'osservazione che i sistemi informatici di gestione dei pagamenti online sono gestiti da soggetti terzi che hanno organizzato il proprio business operando come TTP e su tale ruolo hanno conseguito il successo economico. L'importanza sociale ed economica del contributo di tali attori, in particolare proprio nel settore dei pagamenti, è riconosciuta da Szabo che è perfettamente cosciente che il ricorso a meccanismi gestiti da tali soggetti permette di agevolare relazioni economiche e di ridurre costi di transazione che comunque si verificherebbero[207], tuttavia l'autore è convinto che eventuali nuovi modelli debbano cercare di minimizzare il più possibile il ruolo degli intermediari: in parte perché è consapevole delle forti barriere all'ingresso in questo settore di mercato e ritiene che il successo dei *first comer* non potrà comunque essere replicato, e, in parte, perché ritiene che l'uomo abbia un desiderio innato di poter controllare direttamente il proprio patrimonio e che questa volontà debba essere assecondata il più possibile, contrastando i costi impliciti ai sistemi basati sulla fiducia – *rectius*, su rapporti di agenzia –.

[207] Non da ultimo i costi connessi con la creazione di una relazione tra soggetti che non si conoscono. Szabo esprime questo concetto nei seguenti succinti termini: *Ibidem*, "*Companies like Visa, Dun and Bradstreet, Underwriter's Laboratories, and so forth connect untrusting strangers into a common trust network. Our economy depends on them*".

Ne consegue, per Szabo, che lo sforzo dei programmatori debba essere incentrato sulla creazione di sistemi dove il ruolo di controparti centrali o di gestori centrali che operano come agenti dei partecipanti debba essere minimizzato e che la matematica e la crittografia possano e debbano essere impiegate a questo scopo[208]:

> *"A far better methodology is to work starting from TTPs that either well known, or easy to characterize, and of minimal cost. The best "TTP" of all is one that does not exist, but the necessity for which has been eliminated by the protocol design, or which has been automated and distributed amongst the parties to a protocol. The latter strategy has given rise to the most promising areas of security protocol research including digital mixes, multiparty private computations, and Byzantine resiliant databases. These and similar implementations will be used to radically reduce the cost of current TTPs and to solve the many outstanding problems in privacy, integrity, property rights, and contract enforcement while minimizing the very high costs of creating and operating new TTP institutions"*[209].

L'indicazione programmatica di Nick Szabo trova nei bitcoin la sua più alta realizzazione: il bisogno di autonomia che i crittoanarchici giustificano in termini di *distrust* per il governo, Nick Szabo lo esprime in termini generali di riduzione dei costi transattivi. In ambito monetario, entrambi i discorsi si risolvono nel tentativo di progettare un sistema che gestisca in modo autonomo la creazione e il trasferimento dei mezzi di pagamento, esattamente come cerca di fare il protocollo Bitcoin.

Quanto alle modalità attraverso le quali si possa realizzare l'obbiettivo di strutturare nuovi sistemi informatici in cui gli utenti non debbano fare affidamento su TTP, è lo stesso Szabo ad anticipare che il ricorso alla crittografia possa essere determinante per immaginare database distribuiti in cui i compiti tradizionalmente svolti dalla TTP siano svolti dagli utenti del sistema stesso; in particolare nel contesto delle riflessioni elaborate in merito ai database distribuiti.

---

208 *Ibidem*, e SZABO N., *The God Protocols*, 1997, disponibile all'inirizzo http://nakamotoinstitute.org/the-god-protocols/ (ultima visita 20 giugno 2017).

209 SZABO, *Trusted Third Parties Are Security Holes*, cit..

La gestione di database informatici distribuiti

Al tema della gestione dei database distribuiti Szabo dedica specificatamente il saggio "*Advances in Distributed Security*". Pubblicato nel 2003, il documento consiste in una disamina delle recenti innovazioni introdotte in questo settore che risulta di particolare interesse per l'autore. L'idea più significativa evidenziata nel saggio è che l'introduzione della crittografia permette di sviluppare nuovi modelli collaborativi che prima non era possibile realizzare. Il punto teorico che sottende questo ragionamento è che in situazioni in cui informazioni sono archiviate su database distribuiti è talvolta impossibile raggiungere la certezza piena circa la loro "veridicità" o correttezza, senza affidarne la gestione ad una controparte centrale che svolge la funzione di TTP. L'introduzione della crittografia permette invece di elaborare meccanismi che pur non garantendo la certezza assoluta, permettono di trarre conclusioni caratterizzate da un altissimo grado di probabilità che può essere equiparato, quanto agli effetti, alla certezza non altrimenti raggiungibile[210]. Nelle parole di Szabo:

> *The old pessimism has been overturned. Old proofs of "impossibility", based on strict insistence in perfect certainty, have given way to new proofs demonstrating how to do the "impossible" by being satisfied with extremely high probability against a sophisticated but computationally bounded opponent – the assumption of cryptography – rather than of absolute certainty. This overturning of the old view has led to a raft of new possibilities for securing distributed applications. The simple protocol of*

[210] SZABO N., *Advances in Distributed Security*, 2003, disponibile all'indirizzo http://nakamotoinstitute.org/advances-in-distributed-security (ultima visita 20 giugno 2017): "*The last decade has witnessed a revolution in distributed security. Old, pessimistic proofs that security and fault tolerance were "impossible", based on assumptions that protocols had to be deterministic and security and fault tolerance properties had to be absolutely certain, have given way to new proofs and implementations of provable security based on the assumption of cryptography and other randomized protocols that achieving security with very high probability is sufficient. The old view "proved" that the integrity properties of a wide variety of services on which civilization depends, whether synchronized clocks, public directories, censorship-proof file sharing and publication, or issuing money or securities were "impossible" on asynchronous networks like the Internet unless we put unlimited faith in a third party to enforce many of the rules of the service. We now know how to provide such services with a high degree of integrity and availability, yet far more resilient to the possibility that any party might act in a malicious manner*".

the bell tower, which broadcast to every resident of a medieval town the same time, can now be implemented on a network – either through logical broadcast on the Internet or physical broadcast with radio. For the first time we can implement on the Internet the integrity properties on which civilization depends – including synchronized clocks, unforgeable transactions, and censorship-proof publishing. Where today's Internet, lacking this technology, fails to provide many of these properties, we now know how to provide them with a greater degree of integrity and availability than either the Internet or any previous media was capable of'[211].

Le conclusioni circa l'importanza di eliminare meccanismi di fiducia nei confronti delle terze parti sono riprese esplicitamente, sia nel *bit gold*, sia nei *bitcoin*.

Bit Gold

Nella proposta concernente la creazione di una nuova moneta denominata *Bit Gold*, si riassumono tutti i significativi contributi sin qui richiamati. Il bit gold è essenzialmente un tentativo di creare dell'oro digitale: un bene digitale scarso che possa circolare all'interno di una rete in forza di registrazioni su un registro contabile condiviso e non controllato da parti terze (TTP). L'obbiettivo è creare una moneta che non richieda l'affidamento a soggetti terzi: un sistema monetario senza emittenti o intermediari, che possa però permettere pagamenti su internet. Come prevedere creare un mezzo di pagamento astratto senza le garanzie dello Stato o di una banca? Szabo risponde facendo ricorso alla nozione di *collectibles*: la soluzione è creare dei beni informatici la cui costruzione richieda energia e tempo, scarsi e facilmente trasferibili.

Il problema che si pone è però come gestire l'archiviazione e il trasferimento di tali beni, giacché Szabo è perfettamente cosciente del problema della replicabilità dei beni digitali e della doppia spesa. Per risolvere questo problema Szabo sviluppa ricorre alla nozione di "*scarse objects*", definiti da Szabo "*computational objects that like physical objects are finite and excludable, and force the client to either conserve or consume (use*

[211] *Ibidem*.

up) their own rights to use the object"[212]. Poiché i beni digitali non sono, per natura, né finiti, né rivali, l'attribuzione di queste due caratteristiche implica l'esistenza di una struttura appositamente creata[213]: sostanzialmente un registro di proprietà. Il problema del dover fare affidamento ad un registro è però la necessaria fiducia che occorre riporre in tale sistema di proprietà, per questo, gli *scarse object* sono definiti altresì anche come "*distributed objects interacting across trust boundaries*"[214]: cioè dei beni digitali che sono assegnati in proprietà – distribuiti – da meccanismi che esulano dal diretto controllo del proprietario e richiedono, quindi, un certo grado di "fiducia", intesa come vulnerabilità o, genericamente, esposizione al rischio di malfunzionamenti, voluti o accidentali, del sistema[215].

A questo punto Szabo ricollega i suoi studi sulla gestione dei database distribuiti, sui collectibles e sui registri di proprietà distribuiti su reti[216] e propone di ricorrere ad un registro distribuito che facendo affidamento sui più recenti sviluppi della tecnologia in campo di crittografia[217] elimini *by design* il bisogno di affidarsi a parti terze (TTP). Inoltre, per semplificare la tenuta di tale registro propone, diversamente da Wei Dai, che esso sia strutturato su base reale e non personale.

Quanto ai beni che dovrebbero circolare come moneta, l'autore traspone la nozione di *collectibles* in ambito digitale immaginandosi dei file la cui produzione richieda una serie di calcoli[218], la cui titolarità sia riconosciuta sulla base dell'iscrizione del bene all'interno del registro di proprietà condiviso tra gli utenti.

---

212 SZABO, *Scarse objects*, *op. cit.*.

213 Cfr. *supra*, par. 2.3.

214 SZABO, *op. ult.* cit..

215 Sulla nozione di *trust* cui Szabo fa riferimento, si veda il paragrafo "*Unscrambling the Terminology*" in SZABO, *Trusted Third Parties Are Security Holes*, cit..

216 L'autore aveva già in precedenza sviluppato delle riflessioni teoriche sull'organizzazione di database distribuiti di proprietà in SZABO N., *Secure Property Titles with Owner Authority*, 1998, originariamente pubblicato su http://szabo.best.vwh.net/securetitle.html (non più accessibile), ora disponibile all'indirizzo: http://nakamotoinstitute.org/secure-property-titles/ (ultima visita 20 giugno 2017).

217 In particolare per quanto concerne la creazione di database resistenti ad attacchi Bizantini, su cui v. *infra*.

218 C.d. *proof of work*, concetto che sarà illustrato *infra* in maggior dettaglio.

Il modello che ne deriva è quindi strutturato così: sono messi a disposizione degli utenti problemi matematici di difficile soluzione che richiedono l'impiego di lavoro computazionale. Ciascun utente può provare a svolgere il problema. Una volta trovata la soluzione il risultato viene trasmesso sulla rete, riceve un'impronta temporale e viene iscritto nel registro delle transazioni che tiene traccia della proprietà del bene. La soluzione trasmessa costituisce parte del problema che occorre risolvere per produrre una nuova unità, mentre l'unità prodotta può circolare sulla base dell'attribuzione determinata dal registro.

Sebbene vi sia ancora qualche incertezza circa cosa debba veramente circolare tra gli utenti, può dirsi che la stragrande parte dell'architettura dei bitcoin sia già descritta e anticipata nel modello di *bit gold*. Rispetto a questo Satoshi Nakamoto avrà l'intuizione di separare il concetto di unità di conto e di mezzo di pagamento dal prodotto del lavoro computazionale svolto: nei bitcoin occorre ancora svolgere del lavoro computazionale per poter ricevere delle unità di bitcoin, ma una volta in circolo le unità sono trasferite semplicemente come rappresentazioni digitali dell'unità di conto bitcoin. Ciò che manca ai bit gold, inoltre, è la concreta scrittura del software.

1.4. La pubblicazione del paper di Satoshi Nakamoto e la nascita dei bitcoin

In data 1 novembre 2008, un soggetto presentatosi sul web con lo pseudonimo di Satoshi Nakamoto[219] pubblica sul sito http://www.bitcoin.org un breve *white paper* in formato pdf intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[220] e ne invia una copia alla mailing list creata da Hughes, May e Gilmore, "*The Cryptography Mailing List*". All'invio fa seguito un breve scambio di corrispondenza tra alcuni membri della

[219] Seppure siano state fatte molte speculazioni a riguardo, ancora oggi non si conosce l'identità vera della persona o del gruppo di persone che si celano dietro lo pseudonimo di Satoshi Nakamoto e la questione è ancora fonte di numerose speculazioni. v., *inter alia*, GUTTMANN B., *Bitcoin. Guida completa*, LSWR, 2014, pp. 52 ss..

[220] NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, disponibile all'indirizzo https://bitcoin.org/bitcoin.pdf (ultima visita 20 giugno 2017). Una traduzione non ufficiale in italiano è invece disponibile in GUTTMANN, op. cit., pp. 199 ss. ed in CAPACCIOLI S., op. cit., p. 21.

mailing list e lo stesso Satoshi Nakamoto che, dopo un paio di mesi, il 9 gennaio 2009, rilascia su internet la prima versione del software bitcoin e crea il primo bitcoin[221].

Il documento esplicativo pubblicato nel 2008 riassume e spiega tutta la struttura del protocollo, che sarebbe stata di lì a poco resa disponibile con la pubblicazione del software, e descrive in modo sintetico e puntuale il funzionamento dei bitcoin. L'autore ha certamente tratto spunto dai modelli di monete digitali elaborati prima del 2008 e dal dibattito che si era articolato intorno al tema, ma occorre specificare che prima della pubblicazione della versione finale del *paper* e poi del programma non sono mai state pubblicate bozze o lavori preparatori, né versioni incomplete o provvisorie del codice (cd. versioni "*alpha*"). Questo, in combinazione con l'anonimato entro cui è voluto restare l'inventore dei bitcoin, induce a cautela nel formulare ipotesi sulle teorie economiche o politiche sottese al progetto. Non essendo disponibili i "lavori preparatori" del codice, i collegamenti che si possono fare tra i bitcoin e altri esperimenti che li hanno preceduti devono essere inferiti dalle note del documento (come nel caso del *b-money* di Wei Dai che è direttamente citato da Nakamoto) o dalla somiglianza della struttura e degli assunti (questo è il caso del *bit gold* e delle teorie che ne sono alla base). Il collegamento tra i bitcoin e il movimento crittoanarchico lo si deduce, invece, dalla pubblicazione del progetto sulla mailing list dedicata e dal fatto che i primi sostenitori del progetto furono proprio persone che provenivano da quel mondo. Questo non permette, ovviamente, di argomentare che l'obbiettivo di Satoshi Nakamoto fosse rovesciare i governi costituiti secondo i visionari progetti di May, bensì più limitatamente che l'alveo culturale da cui è scaturito il progetto era segnato dal desiderio di creare alternative, anche radicali, al sistema tradizionale[222]. La coincidenza della pubblicazione dei bitcoin nell'anno della grande crisi finanziaria che ha sconvolto il sistema finanziario globale ha certamente giovato alla popolarità della moneta, ma non è spiegabile in termini di una risposta del movimento crittoanarchico a quell'evento. È innegabile che il creatore dei bitcoin fosse

[221] Il programma compilato in C++ era originariamente disponibile al sito: http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar, oggi il progetto è ospitato sul sito https://github.com/bitcoin/bitcoin (ultima visita 20 giugno 2017) e il programma Bitcoin Core può essere scaricato dal sito https://bitcoin.org/en/download (ultima visita 20 giugno 2017).

[222] NAKAMOTO S., *Re: Bitcoin P2P e-cash paper 2008-11-07 12:30:36 UTC*, disponibile all'indirizzo http://satoshi.nakamotoinstitute.org/emails/cryptography/4/ (ultima visita 20 giugno 2017).

molto critico nei confronti del sistema bancario contemporaneo e sulla creazione di moneta privata secondo lo schema della riserva frazionale: lo si evince dalle posizione esplicitamente assunte dallo stesso Nakamoto in occasione di interventi su mailing list o forum[223] e dal fatto che nel primo blocco della Bitcoin *blockchain* fosse crittata la frase "*the times 03/jan/2009 Chancellor on brink of second bailout for bansk*", riferimento agli articoli in prima pagina del quotidiano inglese The Times relativi agli sviluppi della crisi finanziaria[224]. Il lavoro di elaborazione del programma era, però, iniziato ben prima del manifestarsi della crisi. Nelle mail scambiate nei primi mesi dopo la pubblicazione del protocollo Satoshi Nakamoto afferma di aver lavorato su questo progetto per almeno un anno e mezzo prima di arrivare al rilascio pubblico del software, provando concretamente a compilare il programma e correggendo ed integrando il modello man mano che esso prendeva concretamente forma[225]. Solo successivamente l'intero schema è stato riassunto nel documento esplicativo. Questo tipo di approccio ha caratterizzato, d'altronde, il lavoro e gli sviluppi del progetto crittoanarchico durante i venti anni trascorsi dalla creazione della mailing list alla pubblicazione dei bitcoin: anni in cui la spinta politica di matrice più rivoluzionaria non si è sviluppata in sofisticate elaborazioni teoriche, si è concentrata sui problemi e le soluzioni tecniche via via elaborati con riferimento all'impiego della crittografia in ambito informatico. Ciò che risulta dall'analisi degli "esperimenti" che hanno preceduto i bitcoin e dal contesto generale entro cui il progetto si iscrive è, dunque, proprio un approccio molto concreto, *problem solving*, e l'attenzione al dettaglio tecnico, piuttosto che l'elaborazione della filosofia o del modello teorico sotteso.

---

223 NAKAMOTO S., *Bitcoin open source implementation of P2P currency*, pubblicato 11 febbraio 2009, ore 22:27, in http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (ultima visita 20 giugno 2017).

224 CAETANO R., *Bitcoin guida all'uso delle criptovalute*, Apogeo, 2016, p. 68 e ANTONOPOULOS A., *Mastering Bitcoin. Unlocking digital crypto currencies*, O'Reilly Media, 2015.

225 NAKAMOTO S., *Re: Bitcoin P2P e-cash paper (2008-11-09 14:13:34 UTC)*, disponibile all'indirizzo http://satoshi.nakamotoinstitute.org/emails/cryptography/6/ (ultima visita 20 giugno 2017).

Il 12 dicembre 2010 Satoshi Nakamoto firma un ultimo post sul forum dedicato ai bitcoin[226], cui seguirà solo un unico altro post pubblicato il 7 marzo 2014 in cui si limita ad affermare di non essere Dorian Nakamoto[227].

[226] NAKAMOTO S., *Added some DoS limits, removed safe mode (0.3.19)*, pubblicato il 12 dicembre 2010, sul sito https://bitcointalk.org/index.php?topic=2228.msg29479#msg29479 (ultima visita 20 giugno 2017).

[227] V. commento al fondo della pagina web http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186 (ultima visita 20 giugno 2017).

2. Il Funzionamento del protocollo Bitcoin

2.1. Sintesi e chiarimento terminologico

Il bitcoin è un progetto di moneta digitale caratterizzato da due tratti salienti: (*i*) l'uso di una specifica unità di conto non connessa formalmente ad altri sistemi monetari, chiamata bitcoin; e (*ii*) l'uso di un registro collettivo diffuso, distribuito tra gli utenti, non controllato e non gestito da una controparte centrale strutturato sulla base della tecnologia *blockchain*[228]. Il sistema coglie lo spunto di Wei Dai di realizzare una nuova moneta indipendente da ogni altro sistema e l'intuizione di Nick Szabo di realizzare un registro che tenga traccia dei singoli trasferimenti, non dell'ammontare complessivo dei beni posseduti da ciascuno secondo il modello dei conti correnti. Le nuove unità di bitcoin possono essere create da chiunque e la produzione è regolata dal meccanismo della *proof of work*, ma in modo più articolato e diverso rispetto a quanto immaginato nel *b-money*.

L'escludibilità e la rivalità delle unità di conto utilizzate come moneta sono garantite dalla presenza di un unico registro collettivo distribuito che determina l'allocazione delle risorse tra i partecipanti. Il meccanismo che disciplina l'aggiornamento e la conservazione di questo registro collettivo segna un momento di svolta tecnologica estremamente rilevante ed è molto più sofisticato rispetto a tutti i modelli precedenti ed in particolare rispetto a quello immaginato da Wei Dai. Il Bitcoin è, infatti, il primo sistema al mondo che implementa la *distributed ledger technology* ("DLT"): un meccanismo informatico che attraverso l'integrazione di funzioni *hash* usate per generare *proof of work* ha reso possibile la registrazione automatica di informazioni su un registro distribuito tra gli utenti di una rete, che può essere integrato da chiunque, ma che, al tempo stesso, una volta compilato non può più essere modificato[229]. Attraverso

---

[228] Sul funzionamento dei sistema bitcoin si vendano: AA.VV., *Bitcoin Developer Guide*, disponibile all'indirizzo https://bitcoin.org/en/developer-guide, (ultima visita 20 giugno 2017); Franco, P. *Understanding Bitcoin: Cryptography, Engineering and Economics*, John Wiley & Sons, 2014; ANTONOPOULOS, op. cit.; GUTTMANN, op. cit..

[229] Vedremo, in dettaglio, che questa affermazione è in realtà una semplificazione, sarebbe più corretto dire, infatti, che il registro può essere modificato, ma solo al verificarsi di determinate condizioni che comportano costi così elevati da rendere l'ipotesi di modifica inverosimile. Secondo un paradigma affermatosi nella matematica nel campo della crittografia, si è, in un certo senso, rinunciato alla

questi espedienti tecnologici è stato possibile, cioè, raggiungere l'obbiettivo di creare una rete di scambio che non richiede la presenza di una controparte centrale incaricata di registrare e aggiornare l'allocazione delle risorse tra le parti. Da questa caratteristica deriva l'attributo che la comunità di utenti e promotori di bitcoin rivendica con maggior orgoglio affermando di utilizzare un sistema monetario "*trustless*", cioè un sistema dove l'applicazione di funzioni matematiche ha permesso di realizzare scambi che non richiedono "fiducia" in terze parti, cioè non espongono l'utente a vulnerabilità derivanti dal dipendere da un servizio reso da un terzo e ai rischi e costi connessi)[230].

Come per le ipotesi di monete digitali "crittoanarchiche" che hanno anticipato i bitcoin, anche in questo caso il modello presuppone l'esistenza di una rete di persone connesse tra loro ed è strutturato come un sistema che gestisce pagamenti tra i membri della rete. In coerenza con la nozione di *scarse object* di Szabo, il sistema di pagamenti è concepito come un meccanismo attraverso cui i partecipanti possono scambiarsi beni limitati, difficili – *rectius* impossibili – da riprodurre, con costi di controllo relativamente contenuti. In altre parole la "moneta digitale" scambiata nel sistema ambisce concettualmente ad essere sostanzialmente la trasposizione informatica della "moneta merce", cioè di un bene fisico scarso accettato universalmente come controparte per gli scambi[231]: i bitcoin scambiati tra gli utenti non rappresentano un credito verso un emittente, né verso lo Stato. L'intero sistema, in effetti, si fonda ed è interamente regolato da meccanismi ed automatismi informatici: il ruolo dello Stato è del tutto marginale, se non completamente assente nel disegno istituzionale di questa "moneta".

L'attribuzione del controllo/proprietà delle unità di conto è regolata e garantita dal registro informatico condiviso tra gli utenti, indipendentemente da qualsiasi disposizione di legge e non esiste un emittente che si fa garante del meccanismo di emissione o del valore dei beni digitali messi in circolo, perché la moneta è autoprodotta dagli utenti[232]. Il valore economico di queste unità è, inoltre, attribuito autonomamente dai partecipanti

certezza assoluta in cambio di una probabilità molto alta di resilienza, protetta ulteriormente, nel caso dei bitcoin, dalla massima trasparenza. Sul punto v. *infra*.

230 V. *supra* quanto esposto circa la teoria dei TTP elaborata da Nick Szabo.

231 È lo stesso Satoshi Nakamoto a svolgere, per primo, un sotteso parallelismo tra oro e bitcoin nel *white paper*, v. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit., p. 4.

232 Sul punto, v. più diffusamente *infra*.

al sistema in ragione delle caratteristiche che definiscono i beni, non per effetto di un'entità esterna che ne garantisce la conversione in beni reali. Per tutte queste ragioni il Bitcoin appare come un sistema completamente autoreferenziale ed autonomo, capace di svolgere le proprie funzioni di mezzo di scambio indipendentemente dal contesto normativo ed economico in cui l'utilizzatore è inserito: una "moneta" che appartiene a tutti gli effetti al mondo digitale, dove i confini degli stati nazionali si fanno più labili e sembra prendere gradualmente forma un mercato globale senza frontiere.

Tutte queste caratteristiche presentano, evidentemente, vari livelli di sfida per il giurista e l'economista che vogliano comprendere il funzionamento dei bitcoin al fine di valutarne l'affidabilità economica o di disciplinarne, da un punto di vista legale, l'uso. A fronte della complessità e della novità del fenomeno vale, però, la pena concentrare inizialmente l'attenzione su come funziona, in dettaglio, il sistema Bitcoin, sino ad immergersi nei meandri dei meccanismi matematici e logici che definiscono le regole informatiche del sistema. Sebbene tale operazione possa apparire, a tratti, faticosa o fuorviante, si tratta di uno sforzo essenziale, perché solo dopo aver acquisito piena contezza del sistema è possibile apprezzarne gli elementi di forza e le criticità. Inoltre, nel contesto delle crittovalute il codice informatico ambisce a sostituire i ben altri codici cui i giuristi sono normalmente abituati, sicché può quasi dirsi che studiare le funzioni che all'interno del software regolano il comportamento degli utenti sia quasi come studiare, *mutatis mutandis*, le leggi e i regolamenti che disciplinano quel particolare sistema giuridico.

Prima di addentrarci nei risvolti tecnologici-normativi del sistema occorre una breve premessa terminologica circa l'uso della parola «bitcoin» e la differenza tra protocollo Bitcoin e unità di bitcoin scambiati tra gli utenti. Si è già rimarcato più volte, nei precedenti paragrafi, che un sistema di pagamento basato sullo scambio di "beni digitali" presuppone innanzitutto un meccanismo informatico che garantisca la finitezza e la rivalità di tali beni. Nel contesto dei bitcoin tale meccanismo è implementato da un registro collettivo distribuito tra i partecipanti della rete. L'insieme di regole informatiche che disciplinano il funzionamento dell'intero sistema di gestione del registro costituisce il «protocollo Bitcoin», perché le unità scambiate tra i partecipanti sono chiamate «bitcoin». Come nel caso di altre monete, anche qui lo stesso nome viene utilizzato per

descrivere, sia la moneta in senso lato, unità di conto, sia al mezzo di pagamento, le singole unità scambiate tra gli utenti. Nel presente contesto, peraltro, il riferimento ai singoli bitcoin scambiati è ancora più pregante rispetto alle monete tradizionali perché, come si avrà modo di scoprire, le unità scambiate pur essendo fungibili tra loro sono indicizzate nel registro collettivo. La parola "bitcoin", però, minuscola o maiuscola, non solo è utilizzata per descrivere le unità scambiate e il protocollo, ma anche per riferirsi al sistema monetario nel suo complesso, ed anche in quest'ultimo caso non si va esenti dal rischio di generare confusione. Poiché l'idea di moneta è un concetto poliedrico e sfuggente, il riferimento generico ad una particolare moneta, sia essa il bitcoin, l'euro o il dollaro, rimanda ad una pluralità di significati e può sottendere sia un richiamo all'unità di conto astratta, sia al valore economico corrispondente a ciascun bitcoin, euro o dollaro, sia un riferimento implicito all'insieme di regole che disciplinano l'esistenza della moneta. La distinzione tra queste accezioni nel contesto delle monete statali è più opaca, perché il complesso quadro istituzionale che disciplina la moneta statale include anche meccanismi volti ad assicurarne il valore commerciale ed è, in generale, più articolato e meno circoscrivibile rispetto al sistema informatico che disciplina i bitcoin. Nel contesto dei bitcoin, quantomeno, il riferimento all'insieme di regole che disciplinano il funzionamento del sistema – i.e. il protocollo Bitcoin – è, infatti, più intellegibile; tuttavia, la parola è anche utilizzata per indicare il modello ideale cui corrisponde la prima manifestazione storica di criptovaluta, che è un concetto più ampio rispetto all'estrinsecazione transeunte del modello all'interno del protocollo informatico che lo disciplina.

In breve, la parola "bitcoin", minuscola o maiuscola, è utilizzata in diverse accezioni: può indicare il mezzo di pagamento trasferito di volta in volta tra gli utenti, l'unità di conto astratta, il protocollo informatico che regola l'intero sistema di scambi, nonché il sistema monetario inteso genericamente come modello ideale o nella sua manifestazione storica, così come ancora può essere usata come apposizione per definire l'attributo dell'essere in rapporto con il sistema monetario bitcoin o con il protocollo. Nella letteratura sul tema talvolta si distingue tra «bitcoin» con l'iniziale minuscola per indicare le unità trasferite tra gli utenti e «Bitcoin» con l'iniziale maiuscola per riferirsi, in maniera sintetica, al protocollo informatico. Non si ritiene che tale convenzione sia

molto significativa, posto che non è sufficiente una distinzione tra iniziali maiuscole o minuscole per differenziare le varie accezioni con cui si può usare questo termine. Ci si riferirà, in seguito, al sistema nel suo complesso parlando semplicemente di bitcoin, al plurale.

Vediamo ora, dunque, come funziona questo sistema, iniziando dalla sua ossatura: la *blockchain*.

2.2. La tecnologia *blockchain* e la gestione di registri pubblici condivisi

Il problema centrale affrontato dagli sviluppatori di software in relazione alla creazione di *database* distribuiti (cioè *database* gestiti da un collettivo e non da un ente/soggetto singolo cui è delegata la funzione di garantire l'aggiornamento e la integrità del registro), è come garantire la resilienza del sistema nell'ipotesi in cui alcuni partecipanti non si comportino in modo onesto, cioè come ottenere che tutti i nodi concordino su una particolare versione dei dati condivisi (nell'ipotesi di una moneta digitale sulla allocazione delle risorse tra i consociati), quando all'interno della rete circolano più versioni concorrenti ed incompatibili tra loro, in ragione di comportamenti fraudolenti o di semplici errori tecnici di trasmissione o costruzione del set di dati.

2.2.1. *Il dilemma dei generali bizantini e la soluzione della blockchain*

Il problema è conosciuto come dilemma dei generali bizantini, perché è stato teorizzato e affrontato con l'esemplificazione di alcuni generali bizantini che devono raggiungere il consenso sulla strategia militare da intraprendere collettivamente comunicando tramite messaggeri. Si immagina, in particolare, una situazione in cui i generali devono ritirarsi o attaccare il nemico tutti insieme e devono decidere quale azione intraprendere individualmente sulla base dei messaggi che si scambiano tra loro e la questione in questa ipotesi è come possono accordarsi su una strategia comune nel caso in cui alcuni di essi siano traditori e provino ad ostacolare l'azione bellica comunicando informazioni false[233]. Nel contesto informatico i computer che compongono la rete informatica corrispondono ai generali e i messaggeri sono i collegamenti tra un computer

[233] LAMPORT L., SHOSTAK R, e MARSHALL P., *The Byzantine Generals Problem*, in *ACM Transactions on Programming Languages and Systems*, n. 4(3), 1982, pp. 382-401.

e l'altro. La presenza di errori nella comunicazione dei dati o la presenza di partecipanti ostili fa sì che sulla rete possano circolare versioni discordanti delle informazioni condivise: la sfida è risolvere queste controversie senza attribuire un particolare potere decisionale ad un soggetto singolo o ad un gruppo ristretto, ma, definendo, invece, un meccanismo cooperativo gestito collettivamente che permetta ai partecipanti rimanere tutti sullo stesso piano e di riuscire, ciononostante, a qualificare collettivamente un certo set di informazioni come il set "corretto" e scartare le altre informazioni discordanti.

Una prima soluzione avrebbe potuto essere l'applicazione di un criterio cronologico: su ogni blocco si sarebbe potuta apporre la data e l'ora a cui il blocco fosse stato prodotto, la c.d. *timestamp* inserita nell'*header*[234]. Tali dati sono, però, facilmente falsificabili, sicché non è possibile fare affidamento ad un criterio cronologico senza affidarsi ad un soggetto terzo che certifichi la corretta apposizione della marca temporale.

Viene qui ripreso, quindi, il tema della *proof work*, non, però, per rendere costosa la produzione di moneta, come nell'ipotesi del *b-money*, bensì quale strumento che permetta di determinare un criterio di primazia – che vedremo essere il criterio della catena più lunga –, per stabilire quale tra le possibili catene proposte sulla rete debba essere considerata la catena attendibile.

Nel protocollo Bitcoin si è quindi raggiunto l'obbiettivo di elaborare un criterio che permetta di scegliere la più opzioni quella da considerarsi corretta (*i*) collegando le informazioni tra loro in un'unica sequenza e (*ii*) rendendo l'aggiunta di nuove informazioni costosa in termini computazionali[235]. Data la proporzione matematica fissa tra lavoro impiegato e risultato raggiunto, la combinazione di queste due caratteristiche fa sì che la catena di informazioni più lunga sia sempre quella su cui la maggior parte della rete ha lavorato. Emerge quindi un criterio – il riferimento al set di informazioni elaborato dalla maggioranza della rete calcolata in termini di capacità computazionale – che può essere applicato in modo automatico per selezionare le informazioni che

---

234 Era questa la soluzione proposta nei *bit gold*.

235 ANDRESEN G., *Bitcoin. The World's First Person-to-Person digital currency*, 20 giugno 2011, disponibile all'indirizzo http://www.bitcointrading.com/pdf/GavinAndresenCIATalk.pdf (ultima visita 20 giugno 2017), p. 12: "*The key technical breakthrough that makes a decentralized digital currency possible is the combination of two existing ideas: a hash chain, and proof-of-work. Together they solve the general 'distributed time-stamping' problem*".

possono/devono essere ritenute affidabili da tutta la rete: stabilendo, infatti, la regola secondo cui la catena di informazioni più lunga è la catena cui tutti devono fare riferimento, si ottiene un meccanismo di formazione del consenso collettivo dinamico che non necessita controparti centrali o enti aggiudicatori.

Tale criterio è, inoltre, in grado di proteggere la rete in modo automatico da qualsiasi attacco che non riesca a concentrare più del 50% della capacità di calcolo dell'intera rete, rendendo, di fatto, il sistema molto resiliente ad attacchi. Questa tecnologia è stata chiamata da Satoshi Nakamoto "*blockchain*" – letteralmente: "*catena di blocchi*" –, o "*proof of work chain*", e ad essa oggi si fa riferimento con il termine più generale di *Distributed Ledger Technology*, letteralmente: "tecnologia per registri distribuiti".

Il sistema così costruito è piuttosto complesso: per discernerne i vari aspetti procederemo ad una prima descrizione in cui si assume che tutti i partecipanti collaborino attivamente e, solo in un secondo momento, si tratteranno le ipotesi di errore o attacco al sistema per evidenziarne la resilienza.

2.2.2. *Caratteristiche delle funzioni di* hash

L'intero meccanismo si fonda su alcune proprietà delle funzioni di *hash*. Queste sono funzioni matematiche non invertibili che permettono di estrapolare da un insieme arbitrario di dati una stringa di caratteri alfanumerici di lunghezza predefinita: la funzione *hash* SHA256 usata nel protocollo Bitcoin, per esempio, trasforma qualsiasi insieme di dati in una stringa di 256 bit rappresentata da 64 cifre esadecimali. Caratteristica saliente di queste funzioni è l'univocità del rapporto che esiste tra l'insieme casuale indeterminato di informazioni a cui si applica la funzione e l'output della stessa, in gergo tecnico chiamato *digest* o anche, per brevità, *hash*. A ciascun insieme di dati corrisponde, cioè, una determinata stringa, sicché ogni qualvolta la funzione sia applicata a quel preciso set di informazioni la stringa prodotta sarà sempre la stessa, mentre se anche solo una piccola parte delle informazioni è modificata (in ipotesi anche solo un bit), l'output sarà diverso. Per esempio, alla frase:

"I bitcoin sono stati inventati da Satoshi Nakamoto"

corrisponde l'*hash* SHA-256:

"b7d8ea328a3110525968042403a30ea85ac6f5bde8b6bac49ab4cdf91b42cb4d".

Mentre alla frase:

"I Bitcoin sono stati inventati da Satoshi Nakamoto"

corrisponde l'*hash* SHA-256:

"60cdcf2f6f115a011fc8a4f375d0fed1d29d05b90f746e1163f97f0fde27bb19".

La modifica di una sola lettera, da minuscola a maiuscola ha prodotto un *hash* completamente (ed imprevedibilmente) diverso. L'applicazione di tali funzioni permette, quindi, di produrre un'impronta digitale di un certo set di informazioni, cui si può fare riferimento per verificare in qualsiasi momento successivo che tali informazioni non siano state modificate[236].

Una seconda proprietà delle funzioni di *hash* è che tali funzioni non sono invertibili: non è possibile risalire dal risultato all'insieme dei dati originari. Questa caratteristica permette di usare le funzioni di *hash* come *proof of work*: di ricorrere, cioè, a questi algoritmi, per predisporre delle sfide matematiche che possono essere risolte solo svolgendo un certo numero di calcoli che richiedono una certa quantità di capacità computazionale[237]. Concretamente si richiede di trovare il valore arbitrario che sommato ad un valore predefinito produce un determinato di tipo di *hash*, per esempio un *hash* che abbia inferiore ad un certo valore «*target*» predeterminato in modo uguale per tutti i partecipanti alla sfida. Il fatto che l'*hash* di un certo set di informazioni sia minore del *target* è un evento del tutto casuale che dipende dai dati a cui è applicato l'algoritmo. Poiché la funzione *hash* non è invertibile, non è possibile né risalire dal risultato all'insieme di dati originari, né capire come modificare i dati su cui è applicata la funzione per ottenere il risultato atteso o incrementare le probabilità di successo. L'unico modo per risolvere una sfida di questo tipo è procedere per tentativi: occorre, cioè, provare a

---

[236] La funzione *md5sum* è un'esemplificazione di questo tipo di funzioni ed è usata in contesti in cui occorre verificare che i dati scaricati da internet siano stati trasferiti in modo corretto dal sito al computer. Per esempio, sul sito ufficiale del sistema operativo linux Ubuntu sono riportati i codici md5sum dei file che occorre scaricare per l'installazione, cosicché tutti gli utenti prima di provare ad installare il sistema possano verificare di avere scaricato in modo corretto tali file (cfr. http://wiki.ubuntu-it.org/Installazione/MD5Sum e http://cdimage.ubuntu.com/lubuntu/releases/16.10/release/).

[237] BACK, op. cit..

modificare poco a poco il valore variabile calcolando il risultato dell'algoritmo dopo ogni modifica, sino a quando si ottiene un valore che soddisfa il requisito definito nel *target*. Riuscire a trovare una soluzione a questo tipo di problema è, quindi, indice del fatto che della capacità computazionale è stata spesa per un certo tempo per elaborare un numero indefinito di tentativi e per questo le funzioni di *hash*, usate in questo modo "invertito", cioè partendo da un insieme limitato di possibili *hash* definito dal *target* per trovare gli input della funzione, possono essere usate come prove che sia stato effettuato un certo lavoro computazionale (cd. *proof of work*).

La probabilità di trovare una soluzione al problema dipende dunque dalla difficoltà del *target* prefissato e dalla velocità a cui si riescono a fare i tentativi. Un *target* inferiore comporta un minor numero di soluzioni possibili e quindi richiede maggiori computazioni, mentre un *target* più ampio permette statisticamente di trovare una soluzione dopo un minor numero di tentativi. Poiché, dato il *target*, è matematicamente possibile calcolare le probabilità di successo e sapere quanti calcoli saranno necessari, in media, per trovare la soluzione, è possibile anche, a condizione di conoscere la capacità di calcolo per secondo del processore che prova a risolvere il problema, prevedere il tempo che sarà necessario, in media, per risolvere il problema descritto e produrre una *proof of work*, così come è possibile calcolare la potenza di calcolo del processore impiegato sulla base del tempo con cui viene risolto, in media, il problema assegnato.

In sintesi, dunque, le funzioni di *hash* permettono:

(i) di creare delle impronte digitale univoche di qualsiasi set arbitrario di informazioni;

(ii) di creare sfide informatiche che richiedono un certo numero di calcoli per essere risolte.

L'uso combinato di queste due caratteristiche ha permesso a Satoshi Nakamoto di inventare la prima *blockchain*. La prima proprietà è utilizzata per collegare i vari blocchi di informazioni tra loro. Per fare questo è sufficiente che ciascun blocco contenga al suo interno l'*hash* del blocco precedente. Tale riferimento, che diventa parte integrante del blocco, assicura la concatenazione tra blocchi e la relativa immutabilità delle informazioni contenute in una determinata catena: se i dati contenuti in un qualsiasi blocco fossero modificati, l'*hash* di tale blocco sarebbe diverso. Poiché tale *hash* fa parte

dell'insieme di dati contenuti nel blocco successivo, anche l'*hash* del blocco successivo e di tutti i blocchi seguenti dovrebbero essere ricalcolati. Ne consegue che la modifica di un singolo blocco impone la riscrittura di tutti i blocchi che gli succedono nella catena. La seconda proprietà è utilizzata, invece, per raggiungere ulteriori due obbiettivi: (*i*) creare un sistema di *governance* del registro; e (*ii*) rendere la catena immune da attacchi da parte di soggetti non onesti.

2.2.3. *La costruzione della blockchain*

La *blockchain* serve a gestire in modo automatico la creazione di un registro condiviso da parte di un insieme di utenti connessi ad una rete informatica. Le caratteristiche di tale registro sono che ad esso possono sempre essere aggiunte nuove informazioni e che le informazioni ivi registrate non possono più essere modificate da nessuno. Perché il sistema funzioni si assume che vi siano degli utenti connessi tra loro che costantemente aggiornano tale registro collettivo[238]. Si distribuisce, quindi, tra i partecipanti, un programma informatico che disciplina il funzionamento della rete nel quale sono inserite le seguenti regole:

(i) ciascun nodo della rete conserva una copia della catena di blocchi;

(ii) il registro condiviso è suddiviso in blocchi di informazioni concatenati tra loro con continui richiami all'*hash* del blocco precedente secondo quanto anzidetto;

(iii) a ciascun blocco deve corrispondere un *hash* che soddisfa un certo *target*, ossia la creazione di ciascun nuovo blocco dipende dalla risoluzione di un problema matematico che non ha altra funzione se non quella di rendere computazionalmente costosa la creazione di nuovi blocchi, c.d. requisito della *proof of work*;

(iv) qualsiasi nodo della rete (i.e. qualsiasi computer connesso alla rete che condivide la *blockchain*) può aggiungere un nuovo blocco alla catena trasmettendolo agli altri nodi, a condizione che il blocco sia completo e soddisfi, quindi, il requisito della *proof of work*;

[238] Sul punto cfr. *infra*.

(v) tutti i nodi considerano sempre come valida ed autentica la catena di informazioni più lunga.

Ipotizziamo, ora, che tutti i nodi collaborino attivamente per la riuscita del sistema: un tale sistema funzionerebbe pressappoco così. Ogni nodo conserva una copia della catena più lunga a disposizione della rete: questo vuol dire che se alcuni nodi della rete hanno una catena di dieci blocchi, tutti i nodi che hanno una catena composta da nove o meno blocchi chiederanno una copia dei blocchi mancanti sino ad arrivare al decimo, verificando che gli stessi siano correttamente concatenati e siano blocchi validi. In questo scenario ciascun nodo prova a creare, simultaneamente agli altri nodi, il successivo blocco che sarà aggiunto alla rete, che contenga il riferimento al blocco precedente e soddisfi il requisito imposto dalla *proof of work.* Appena un nodo riesce a creare un blocco il cui *hash* rispetta il *target* definito dal software che regola la *blockchain*, lo trasmette a tutti gli altri nodi e inizia a lavorare per creare il blocco successivo. Gli altri nodi ricevono il blocco di informazioni, verificano, come sopra descritto, che contenga il riferimento al blocco precedente e che abbia un *hash* valido, trasmettono a loro volta il nuovo blocco agli altri nodi della rete in modo che il blocco trovato si propaghi il più in fretta possibile e iniziano anch'essi a lavorare al blocco successivo, che conterrà a sua volta il riferimento al blocco che hanno appena ricevuto.

Il riferimento all'*hash* del blocco precedente permette la concatenazione dei blocchi secondo un ordine stabile nel tempo che conferisce univocità alla catena, mentre il criterio di preferenza per la catena più lunga consente di scegliere sempre tra catene diverse entrambe valide che possano essere simultaneamente presenti sulla rete. L'applicazione di questi due attributi può essere descritto come un meccanismo decentralizzato di «*emerging consensus*» e costituisce il contributo più significativo di Satoshi Nakamoto alla teoria delle reti e di *governance* di registri decentralizzati. Il consenso è "*emergent*" perché non è raggiunto in uno specifico momento nel tempo, ma è costantemente rinnovato e mantenuto dall'applicazione di queste due regole nel contesto di continue interazioni asincrone tra migliaia di nodi sulla rete[239].

[239] V. ANTONOPOULOS, op. cit., pp. 176 ss. Il quale sottolinea che le proprietà dei bitcoin che ne permettono l'uso come moneta, quelle inerenti la gestione delle transazioni, nonché la sicurezza stessa del modello, derivano e dipendono tutte da questa invenzione.

2.2.4. *Le biforcazioni della catena di blocchi*

Perché il sistema funzioni in modo scorrevole, la difficoltà della *proof of work* deve essere tale da rendere poco probabile che due blocchi trovino simultaneamente la soluzione al problema[240]. In questo modo la rete è in grado di progredire in modo ordinato: ogni blocco è numerato in ordine crescente ed è aggiunto al precedente nella *blockchain* come se si costruisse una lunga torre di mattoni o una scalinata[241]. Per quanto possa essere statisticamente improbabile, è però sempre astrattamente possibile che due nodi trovino contemporaneamente o a brevissima distanza di tempo due soluzioni diverse al problema[242] e che, quindi, due soluzioni siano trasmesse legittimamente alla rete in modo quasi simultaneo. Presto, cioè nel tempo richiesto per la propagazione delle informazioni sulla rete, che si presume breve, tutti i nodi avranno ricevuto entrambe le versioni del nuovo blocco: una parte della rete riceverà per primo il blocco "A" e un'altra parte riceverà per primo il blocco "B"[243]. Questa ipotesi è descritta in gergo tecnico come *fork*, cioè biforcazione della *blockchain*, perché da quel momento esistono due catene che soddisfano i criteri del protocollo e sono quindi entrambe astrattamente valide: una che termina con il blocco A e l'altra che termina con il blocco B. In questo contesto ciascun nodo salva entrambe le versioni astrattamente valide dell'ultimo blocco, ma prosegue il lavoro di creazione della catena assumendo, temporaneamente, che la catena giusta sia

---

[240] La difficoltà della *proof of work* deve essere, più specificatamente, bilanciata in modo equilibrato. Una prova troppo semplice aumenta eccessivamente il rischio di soluzioni simultanee e sdoppiamenti della catena, rendendo meno lineare lo sviluppo della *blockchain* e potrebbe comportare il rischio, in ipotesi estreme, che la velocità della creazione di nuovi blocca ecceda la velocità di propagazione dei blocchi sulla rete, compromettendo la tenuta del sistema; una prova troppo complessa rischia, al contrario, di rallentare eccessivamente la produzione di blocchi comportando un rallentamento dell'aggiornamento del registro.

[241] Proprio in ragione della metafora della *blockchain* come una torre formata da blocchi posti l'uno sull'altro, il numero progressivo di ciascun blocco all'interno della *blockchain* è detto "altezza" del blocco.

[242] È invece impossibile che due nodi trovino la stessa identica soluzione al problema perché in ciascun blocco è registrato il codice del nodo che lo ha prodotto. Se anche così non fosse le probabilità di un simile evento sarebbero comunque tendenti a zero.

[243] In proposito è bene chiarire che il numero di possibili soluzioni al problema matematico che occorre risolvere per aggiungere un blocco alla catena sono considerevoli: occorre, sì, effettuare un determinato numero di computazioni prima di riuscire a compilare un blocco che soddisfi i requisiti imposti dal *target*, ma ciò non significa che vi sia una sola possibile soluzione. Si tratta di insiemi dell'ordine di miliardi di numeri.

quella con il blocco che ha ricevuto per primo: così, per esempio, se il nodo ha ricevuto per primo il blocco A, allora lavorerà per creare un nuovo blocco al cui interno è inserito il riferimento all'*hash* del blocco A. La biforcazione è risolta quando il successivo blocco viene creato e inviato alla rete: se il successivo blocco "C" è generato da un nodo che stava lavorando sulla catena con il blocco A, quella catena diventa la più lunga e, quindi, per applicazione del criterio generale, diventa la catena valida. Tutti i nodi della rete si uniformeranno, quindi, secondo questo criterio: i nodi che già lavoravano partendo dal blocco A copieranno C e proseguiranno normalmente, i nodi che stavano lavorando partendo dal blocco B alla ricezione di C aggiorneranno la propria copia del registro sostituendo il blocco B con i blocchi A e C. Si noti che in caso di biforcazione della catena i dati inseriti nei due blocchi concorrenti A e B sono, per un limitato periodo di tempo, iscritti in una catena di blocchi formalmente valida. Dal momento in cui una versione prevale sull'altra, i dati contenuti nel blocco che viene disconosciuto, che pure per un certo periodo di tempo sono stati temporaneamente e 'legittimamente' inseriti nella catena di blocchi, non sono più conservati sulla *blockchain*: perché vi siano inclusi occorrerà reinserirli copiandoli in un blocco successivo.

Astrattamente è possibile, specie se la rete è grande e il tempo di propagazione dei dati non ottimale, che ulteriori blocchi siano creati e trasmessi alla rete in modo quasi simultaneo, con l'effetto che la biforcazione prosegua per più blocchi; la probabilità di un tale evento si riduce, però, sempre più all'aumentare del numero di blocchi prodotti per la seguente ragione[244]. Date le proprietà della funzione di *proof of work*, la probabilità di trovare la soluzione e di creare un nuovo blocco sono grossomodo proporzionali alla percentuale di potenza di calcolo della rete impiegata: un nodo o un gruppo di utenti che controlla il 10% della capacità computazionale della rete (espressa in operazioni di calcolo per secondo), ha il 10% di probabilità di trovare il blocco successivo. Nell'ipotesi in cui due blocchi altrettanto validi siano diffusi contemporaneamente nella rete, fermo restando che ciascun nodo lavorerà sempre sul blocco che ha ricevuto per primo, è molto improbabile la diffusione sulla rete sia così perfettamente simultanea da comportare che

[244] Si noti che la difficoltà di creazione e quindi la frequenza con cui sono creati nuovi blocchi può essere regolata per tenere conto del tempo di trasmissione delle informazioni sulla rete con l'obbiettivo di minimizzare il rischio di biforcazioni. Se il sistema è strutturato a regola d'arte la probabilità di una biforcazione è, quindi, già molto bassa in partenza.

esattamente la metà dei nodi lavori su un blocco e l'altra metà sull'altro: quasi sicuramente si formerà una maggioranza di nodi che lavora su un blocco e una minoranza che lavora sull'altro. Poiché la probabilità di trovare un blocco dipende dalla potenza di calcolo impiegata, è più probabile che la maggioranza dei nodi (misurata in termini di potenza di calcolo) trovi il blocco successivo prima della minoranza. Assumendo la non perfetta divisione dei due gruppi, per ogni ulteriore blocco la probabilità che la catena minoritaria produca un nuovo blocco prima che il corrispondente blocco della catena su cui lavora la maggioranza sia diffuso nell'intera rete diminuisce esponenzialmente, sicché nel giro di poco tempo la catena su cui lavora la maggior parte della potenza di calcolo del sistema si afferma come la catena valida[245]. Quindi, l'applicazione del principio secondo cui la catena più lunga prevale, assicura, per effetto dell'applicazione delle leggi statistiche, che se anche non vi è una certezza assoluta che la *blockchain* non presenti biforcazioni, queste saranno gestite e risolte in maniera automatica.

2.2.5. *Prime considerazioni sulla blockchain e sul suo funzionamento*

Svolgiamo, allora, cinque considerazioni circa il meccanismo sopra descritto.

La prima è che quando un nodo riceve un nuovo blocco tutto il lavoro computazionale svolto sino a quel punto per cercare di creare tale nuovo blocco è perso. L'architettura del sistema è tale per cui tra i nodi si svolge una gara costante per produrre i nuovi blocchi della catena, nella quale per ogni nuovo blocco il vincitore "prende tutto" e il lavoro di tutti gli altri è inutile. Il fatto che ciascun nuovo blocco debba contenere l'*hash* del blocco precedente implica, infatti, da un lato, che non sia possibile iniziare a lavorare su un blocco se non si è ricevuto il blocco precedente; dall'altro che il lavoro svolto per cercare di produrre un blocco è completamente inutile rispetto alla creazione del blocco successivo[246].

---

[245] Ovviamente, maggiore è il tempo che occorre impiegare in media per trovare un nuovo blocco, minore è la probabilità di biforcazioni. Nel protocollo Bitcoin Satoshi Nakamoto ha calcolato che la probabilità che la catena minoritaria superi in lunghezza la catena maggioritaria sono quasi pari a zero dopo sei blocchi dalla biforcazione, v. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit., pp. 6 ss..

[246] La base di dati che occorrerà modificare poco alla volta dovrà infatti inglobare quantomeno un dato nuovo (l'*hash* del blocco precedente), sicché occorrerà ricominciare da zero a modificare poco alla volta tale nuovo set di informazioni.

La seconda considerazione è che la possibile presenza di biforcazioni comporta che i dati inseriti nella *blockchain* non siano immediatamente definitivi ed immodificabili: potrebbero, infatti, essere inseriti in un blocco appartenente al ramo di una biforcazione della catena che non sarà proseguito dalla comunità. Se così fosse, tali dati figurerebbero solo temporaneamente nella *blochain*: quando il successivo blocco è scoperto e il ramo abbandonato il blocco originariamente aggiunto è, infatti, cancellato e non resta alcuna traccia dei dati *ivi* inseriti. Anche per questa ragione, dunque, è richiesto a tutti i nodi di trattenere una copia di entrambi i possibili sviluppi della catena: in modo che i dati persi nel processo possano essere re-inseriti in un successivo blocco.

La terza considerazione è che il criterio della catena più lunga che governa la scelta dei blocchi che saranno mantenuti nella *blockchain* non è minimamente legato alle informazioni contenute in ciascun blocco: in caso di biforcazione entrambi i blocchi sono entrambi perfettamente validi e la scelta di quale resterà nella catena e quale sarà perso per sempre dipende esclusivamente dalla loro diffusione sulla rete e dai successivi sviluppi della catena, non dal contenuto degli stessi. Sotto quest'ultima angolazione possiamo operare una distinzione tra validità «relativa», o meglio coerenza interna della catena, e validità «assoluta», cioè validità definitiva all'interno della dinamica del sistema. Per validità «relativa» della catena di blocchi si intende che una catena di blocchi in cui ciascun blocco contiene il riferimento all'*hash* del blocco precedente e rispetta ogni altra regola relativa alla composizione formale dei blocchi è una catena astrattamente valida che risponde ai requisiti del protocollo. Per validità «sostanziale» della catena di blocchi, intendiamo, invece, sottolineare che il criterio della catena più lunga permette di risolvere la tipica esemplificazione concreta del dilemma dei generali bizantini che si pone quando circolano sulla rete due diverse catene astrattamente valide sotto il profilo dei requisiti del protocollo (cioè con blocchi perfettamente concatenati tra loro e rispondenti a tutti i criteri di validità imposti dal protocollo, incluso, per esempio, l'avere *hash* inferiori ad un certo *target*), perché permette di rispondere alla domanda: "quale delle due catene deve essere considerata attendibile?".

L'applicazione del criterio della catena più lunga funziona, però, a condizione che la *blockchain* sia costantemente aggiornata: abbiamo visto, infatti, che è l'aggiunta di ulteriori blocchi il criterio che permette di dirimere i dubbi che sorgono in caso di

biforcazioni. La quarta considerazione è, quindi, che la presenza di un gruppo di utenti connessi tra loro che costantemente aggiornano il registro collettivo non è solo una premessa teorica necessaria per spiegare il funzionamento del sistema, bensì una precisa condizione da cui dipende il funzionamento dello stesso. Il punto non è, ovviamente, affermare che la *blockchain* funziona solo se c'è un gruppo di utenti connessi in rete tra i quali è distribuita una copia del registro: questa tecnologia definisce la gestione di un registro collettivo, quindi è ovvio che occorre vi siano più utenti connessi. Il punto è, invece, che il funzionamento del sistema e la conseguente immutabilità dei dati immagazzinati nella *blockchain* dipendono dalla continua espansione della stessa: il consenso in termini «assoluti» circa la validità delle informazioni condivise è sempre temporaneo e deve essere, quindi, perennemente rinnovato per restare tale.

La quinta e ultima considerazione è che il sistema di *blockchain* sopra descritto permette ai nodi della rete di dissociarsi e riassociarsi in un tempo successivo un numero indeterminato di volte, così come permette a nuovi nodi di entrare nella rete in qualsiasi momento. Ogni qual volta un nodo si connette è sufficiente, infatti, che interroghi la rete cercando la catena più lunga disponibile e che integri le informazioni eventualmente in suo possesso sino ad ottenere tutti i blocchi disponibili, dopodiché potrà operare esattamente come tutti gli altri nodi. L'applicazione del criterio della catena più lunga, unitamente alla concatenazione dei blocchi secondo un ordine preciso ed immutabile nel tempo, garantiscono, quindi, oltre all'immutabilità delle informazioni contenute nella *blockchain*, anche la modularità della rete.

2.2.6. *La gestione di comportamenti non onesti da parte dei nodi*

Esaminato il funzionamento della *blockchain*, veniamo ora a considerare l'ipotesi di comportamenti non onesti o collaborativi da parte dei componenti della rete, in particolare le ipotesi di (*i*) opportunismo; (*ii*) inserimento di dati "falsi" e (*iii*) attacco fraudolento per modificare il contenuto di dati registrati sulla *blockchain*.

Una prima ipotesi di comportamento non onesto di un nodo è il caso di un nodo che abbia scoperto il successivo blocco della catena, in ipotesi il centesimo, e non lo divulghi subito al resto della rete per iniziare a lavorare al blocco successivo prima degli altri. Assumendo che l'interesse del nodo sia produrre più blocchi possibili della catena

(si immagini, per esempio, il caso in cui ogni nodo sia remunerato in baso al numero di nuovi blocchi aggiunti alla catena), un siffatto comportamento sarebbe controproducente perché comporta un rapporto tra costi e benefici sbilanciato. Le probabilità che tale nodo sia in grado di trovare, lavorando da solo, il centunesimo blocco prima che altri nodi trovino un altro centesimo blocco sono irrisorie, sicché è immaginabile che il blocco si troverebbe a competere con un altro blocco in una biforcazione. In tale ipotesi, assumendo che il blocco concorrente sia pubblicato sulla rete prima che il nodo egoista trasmetta il suo, il vantaggio nella corsa verso il centunesimo blocco in termini di calcoli effettuati dal nodo egoista andrebbero a contrapporsi con la potenza di calcolo complessiva dei nodi che lavorano sull'altra catena disponibile. Nel caso la maggioranza della rete lavori sull'altra catena, è estremamente probabile che quella sia la catena prosegua e che il blocco trovato dal nodo egoista sia, per l'effetto, scartato: l'immediata comunicazione del blocco scoperto comporta il vantaggio che la maggioranza della rete lavorerà per la continuazione della catena con quel blocco, mentre tenere segreto un blocco comporta il rischio, concreto, che il blocco diventi "inutile". La *governance* della *blockchain* non incentiva, quindi, comportamenti opportunistici individuali.

La seconda ipotesi concerne il caso in cui un nodo inserisce dei dati "falsi" o "erronei" all'interno di un blocco. Circa questa ipotesi occorre specificare meglio il significato del concetto di "falso" o "erroneo". La *blockchain* è una tecnologia che permette ad una rete di maturare un consenso dinamico su una serie di informazioni distribuite senza alcuna delega di potere ad una controparte centrale. La valutazione circa la validità delle informazioni inserite all'interno di ciascun blocco è un esame di tipo formale svolto da ciascun nodo al momento della ricezione di un nuovo blocco ed operato secondo i criteri formali imposti dal programma. Dal punto di vista del sistema, quindi, non esistono informazioni false o vere, esistono soltanto blocchi di informazioni costruiti secondo le regole formali imposte dal software che gestisce la rete e blocchi di informazioni che non soddisfano tali requisiti: i primi saranno riconosciuti come validi da ciascun nodo e saranno inseriti nella *blockchain*, mentre i secondi saranno ignorati dai nodi e non entreranno a far parte della catena di blocchi distribuita. Immaginiamo, per esempio, una *blockchain* in cui sono registrati trasferimenti di proprietà di automobili ovvero una *blockchain* in cui sono registrate opere di poesia originali al fine di garantire

la titolarità del diritto d'autore. Nel primo come nel secondo caso il sofware può richiedere che le informazioni contenute in ciascun blocco siano registrate secondo uno standard predefinito: nel primo caso, per esempio, si chiede che ciascuna transazione sia riportata indicando in sequenza il codice fiscale del compratore, il codice fiscale dell'acquirente, la targa e il prezzo, separati da virgole, mentre nel secondo caso si richiede che il testo delle poesie sia riportato in caratteri minuscoli. Blocchi generati nelle rispettive *blockchain* con punti al posto delle virgole o caratteri maiuscoli non sarebbero accettati dai nodi della rete, mentre blocchi composti rispettando le regole formali che riportano, però, acquisti di macchine mai avvenuti o con prezzi falsi, piuttosto che poesie copiate da altri autori, sarebbero comunque regolarmente registrati sulla *blockchain*. Tra le regole riguardanti le informazioni contenute in ciascun blocco che possono essere inserite nel programma informatico che gestisce la rete sono particolarmente interessanti quelle che concernono collegamenti tra dati contenuti in diversi blocchi, come si avrà modo di vedere in seguito con riferimento al caso specifico dei bitcoin. Poiché, infatti, i nodi che gestiscono la *blockchain* conservano una copia dell'intero registro, è possibile prevedere regole che impongano ai nodi di verificare le informazioni contenute in ciascun nuovo blocco alla luce di tutte le *informazioni* contenute in tutti gli altri blocchi della *blockchain*. Ovviamente, perché il controllo circa la validità di ciascun blocco nei termini anzidetti operi in modo efficace e coerente, occorre, ed è sufficiente, che tutti i nodi utilizzino lo stesso identico programma o, quantomeno, lo stesso set di regole.

La terza ipotesi di comportamenti non onesti riguarda il caso di un soggetto che voglia "attaccare" la *blockchain* per modificare il contenuto dei blocchi. Ciascun nodo conserva una copia della *blockchain* ed è in grado di verificarne la validità «relativa», sicché l'unico modo per modificare dei dati contenuti in un blocco è produrre una catena alternativa altrettanto valida sotto il profilo del rispetto delle regole del protocollo e rendere questa seconda versione valida in termini «assoluti» all'interno della rete. L'applicazione ferrea della regola secondo cui la catena più lunga è sempre la catena valida in termini assoluti rende questa serie di operazioni astrattamente possibile: è sufficiente, infatti, che la catena alternativa prodotta da chi attacca la rete sia più lunga della catena "originaria". Per produrre una *blockchain* alternativa occorre, tuttavia, ricalcolare una alla volta in sequenza le *proof of work* di tutti i blocchi che occorre

modificare, a partire dal blocco in cui è contenuta l'informazione sino all'ultimo blocco disponibile[247]. Perché tale catena alternativa sia più lunga della catena altrimenti esistente occorre, inoltre, che l'attaccante compia le computazioni necessarie più velocemente di quanto occorra agli altri nodi "onesti" per continuare la catena "originaria". Nell'ipotesi più semplice, in cui un nodo "ostile" intende modificare dei dati inclusi l'ultimo blocco aggiunto alla *blockchain*, occorre che tale nodo riesca a produrre da solo più blocchi di quanti riesce a produrne il resto della rete. L'unico modo in cui tale nodo può ottenere la "modifica" dei dati appena inseriti nel registro è, infatti, produrre una catena alternativa a quella che si svilupperebbe in modo naturale come continuazione di tale blocco. Anche ammesso che tale nodo riesca a produrre immediatamente un blocco alternativo in cui sono inseriti i dati rivisti, il primo risultato che riuscirebbe ad ottenere è unicamente quello di aver creato una biforcazione della *blockchain*. Perché l'attacco abbia successo occorre che la catena si sviluppi come continuazione del blocco creato artatamente dal nodo "ostile": occorre cioè, che lo stesso nodo ostile riesca a produrre per primo il blocco successivo. Per poter sperare di avere successo in questa competizione, l'attaccante deve controllare almeno la metà della capacità di calcolo dell'intera rete: solo così ci saranno più probabilità che la sua catena alternativa riesca ad eguagliare e a diventare più lunga della catena prodotta dal resto della rete[248].

Tale caso estremo illustra perfettamente, invero, il limite di funzionamento intrinseco al modello di *blockchain* basato sul criterio della catena più lunga. Il singolo nodo che controlla più del 50% delle capacità di calcolo dell'intera rete è, infatti, in grado di sviluppare autonomamente una catena alternativa di pari lunghezza rispetto a quella che è in grado di sviluppare la rimanente parte della rete. In questa condizione di

---

[247] L'impiego delle funzioni di *hash* nei termini sopra descritti implica, infatti, che, indipendentemente dal tipo di informazioni memorizzate sulla *blockchain*, qualsiasi modifica influisca sull'*hash* del blocco interessato, che dovrà essere ricalcolato nel rispetto del *target*, nonché, poiché tutti i blocchi sono legati tra loro, la modifica di tutti i successivi blocchi e il calcolo dei relativi *hash*. Tale operazioni, peraltro, dovranno essere eseguite in ordine una dopo l'altra poiché, come già è stato sottolineato, non è possibile creare un nuovo blocco senza avere l'*hash* del precedente.

[248] Si noti, peraltro, che anche in tale ipotesi l'attacco potrebbe avere ad oggetto solo la modifica dei dati inseriti nell'ultimo blocco. Per modificare dati contenuti in blocchi precedenti l'aggressore dovrebbe ricalcolare tutte le *proof of work* di tutti i blocchi successivi a quello contenente i dati modificati sino a raggiungere e superare la catena degli altri nodi onesti, che nel contempo continuerebbe a elaborare nuovi blocchi. V. *infra* il prossimo paragrafo.

superiorità, tale soggetto potrebbe comunicare pubblicamente dei dati e lasciare che siano inseriti nel ramo sviluppato dalla rete, mentre segretamente elabora un ramo alternativo con dati diversi, per poi pubblicare la propria versione della *blockchain* sostenendola fintantoché non diventa la catena più lunga riconosciuta da tutta la rete. In una tale circostanza il sistema di gestione non sarebbe in grado di reagire automaticamente all'attacco e sarebbe compromesso.

2.2.7. *La governance della rete secondo il modello di* emerging consensus

Torniamo ora, però, al tema della immutabilità dei dati iscritti nella *blockchain* e all'ipotesi di tentativi di modificazione degli stessi, per chiarire che se invece di considerare i dati appena iscritti facessimo riferimento a dati contenuti in blocchi distanti dal termine della *blockchain*, le probabilità di successo di un attacco sono ritenute sostanzialmente nulle[249]. In primo luogo perché all'aumentare del numero di blocchi che occorre riscrivere la quantità di calcoli che occorre compiere aumenta e un eventuale attaccante dovrebbe, quindi, effettuare un numero di calcoli irragionevolmente grande. Si pensi, per esempio, all'ipotesi in cui un nodo "ostile" voglia modificare un dato che è stato registrato nella *blockchain* un anno prima. Per produrre la stessa quantità di blocchi esistenti al momento in cui il soggetto decide di compiere l'attacco, occorre impiegare l'intera potenza di calcolo della rete per un anno e a quel punto si dovrebbero comunque ancora riscrivere tutti i blocchi generati dalla rete nel frattempo. Perché l'ipotesi sia verosimile occorre che l'attaccante disponga della quasi totalità della potenza di calcolo dell'intera rete e comunque l'attacco richiederebbe un tempo molto lungo: più che di un attacco dovrebbe trattarsi, verosimilmente, di una decisione collettiva assunta dall'intera rete di azzerare i progressi fatti e ripartire dalla catena come era in uso ad una certa data[250]. In secondo luogo, anche volendo immaginare che una scoperta tecnologica abbia effettivamente permesso ad un singolo nodo di sviluppare individualmente una capacità

[249] Tale ordine di considerazioni largamente condiviso nella letteratura sviluppatasi sul tema sconta, però, un'approssimazione importante: in realtà l'attacco è sempre astrattamente realizzabile a condizione che la percentuale di capacità di calcolo della rete sia tanto più sbilanciata a favore dell'attaccante quanto più difficile si fa l'attacco.

[250] Ipotesi che potrebbe verificarsi quale reazione estrema ad un attacco che comprometta in una certa misura la *blockchain*. v. *infra*.

di calcolo di gran lunga superiore a quella della rete (tale per cui la riscrittura della *blockchain* potrebbe avvenire in tempi più ragionevoli), in ogni caso l'attacco avrebbe l'effetto di compromettere il sistema, rendendo verosimilmente inutile lo sforzo di riscrittura del registro. Occorre, infatti, tenere presente che il contenuto del registro è condiviso sulla rete e quindi conosciuto da tutti i membri che ne hanno una copia memorizzata: l'imposizione di una nuova versione alternativa (che peraltro comporterebbe lo scaricamento improvviso da un unico nodo di una grande quantità di blocchi) non passerebbe inosservata e sarebbe certamente scoperta. Sotto il profilo della *governance* tecnologica la nuova catena di blocchi sarebbe riconosciuta come la catena teoricamente valida in modo assoluto all'interno della rete, quantomeno dal punto di vista del protocollo *software* in uso sino a quel momento, ma la credibilità del sistema sarebbe compromessa perché si verrebbe a sapere che c'è un individuo o un gruppo di individui capace di riscrivere a propria discrezione la *blockchain* ed è verosimile che l'effetto porterebbe ad un abbandono della rete o ad una riscrittura immediata del software che renda vano l'attacco e ripristini la precedente versione della catena. In altre parole, in un simile contesto, la frattura tra la storia realmente svoltasi e originariamente trascritta nella prima versione della *blockchain* e la storia "ri-scritta" nella nuova versione della *blockchain* sarebbe tale da causare la rottura del sistema: anche per questa ragione, quindi, è inverosimile, seppure non astrattamente impossibile, che i dati contenuti nella *blockchain* e sepolti sotto un numero considerevole di blocchi siano modificati.

Le riflessioni svolte in merito a queste ultime ipotesi di comportamenti scorretti da parte degli utenti che si trasformano in veri e propri attacchi alla rete ci induce a riflettere, ancora per un momento, sul fatto che qualsiasi contenuto elaborato all'interno della *blockchain* non è mai completamente immutabile dal punto di vista teorico e che l'immutabilità dei dati dipende dalla distribuzione del potere di calcolo impiegato nella rete. Può dirsi, invero, che l'attributo di immutabilità dei dati iscritti, così come il concetto di validità «assoluta» impiegato per descrivere la soluzione al dilemma dei generali bizantini all'interno dei sistemi di *blockchain* siano precari, perché devono costantemente essere rinnovati tramite la prosecuzione della catena dei blocchi. In altri termini, all'interno di un sistema *blockchain*, la "verità" riconosciuta dalla rete è sempre, in una certa misura, relativa, o, meglio «dinamica», perché dipende da un criterio di validazione

– il criterio della catena più lunga disponibile sulla rete – che a sua volta richiede che la maggior parte del potere di calcolo impiegato sulla rete sia distribuito e cooperi per il costante rinnovamento della catena mediante l'apposizione di nuovi blocchi. Corollario di questo principio è che da tale dinamica dipendono non solo l'immutabilità dei dati iscritti nel sistema, ma anche, conseguentemente, l'affidabilità del sistema e la resilienza contro attacchi esterni.

2.2.8. *La blockchain oltre i bitcoin: la distributed ledger technology*

Il modello sopra descritto corrisponde grossomodo al modello impiegato nel sistema bitcoin e costituisce il primo modello di *blockchain* creato. Questa innovazione tecnologica è, oggi, considerata uno dei più importanti lasciti del sistema bitcoin e in numerosi settori si è iniziato a studiarne le potenzialità[251]: l'applicazione di questa tecnologia è, infatti, molto interessante per tutti gli ambiti in cui occorre sviluppare e conservare un registro comune a più soggetti. In particolare il mondo della finanza sta studiando con molta attenzione la possibile implementazione di questa tecnologia. Nel contempo la riflessione si sviluppa anche riguardo le possibili diverse regole che sarebbe preferibile definire nella creazione di nuove *blockchain*: per esempio immaginando un diverso meccanismo di selezione dei nuovi blocchi[252], oppure immaginando catene gestite con accesso ristretto, in cui solo alcuni membri selezionati possono contribuire allo sviluppo della catena. L'aspetto comune a queste riflessioni è l'impostazione di fondo che caratterizza la *blockchain* e tutti i futuri sviluppi della *distributed ledger technology*: l'organizzazione delle informazioni in blocchi concatenati tra loro in modo irreversibile

---

[251] Cfr., tra molti, U.K. GOVERNMENT CHIEF SCIENTIFIC ADVISER, *Distributed Ledger Technology : beyond block chain*, 2016 (a cura di Mark Peplow), disponibile al sito www.gov.uk/go-science (ultima visita 20 giugno 2017); PARLAMENTO EUROPEO, *Distributed ledger technology and financial markets*, 2016, European Parliamentary Research Service (a cura di Angelos Delivorias), PE 593.565; Biella M. e Zinetti V., *Blockchain Technology and Applications from a Financial Perspective*, Unicredit, 2016; COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES, *Digital currencies*, Bank for International Settlements, 2015, p. 15. Cfr. anche: https://bitcoinmagazine.com/articles/survey-shows-overwhelming-support-*blockchain*-tech-financial-services-executive-boards/ (ultima visita 20 giugno 2017).

[252] v. BANCA CENTRALE EUROPEA, *Virtual Currency Schemes – a further analysis*, 2015, disponibile sul sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (ultima visita 20 giugno 2017), pp. 9 ss..

e la presenza di un criterio che permette di individuare la sequenza di informazioni "corretta".

2.3. Il protocollo Bitcoin

Chiarito il funzionamento della *blockchain*, che costituisce il più grande contributo in termini teorici e tecnologici apportato dai bitcoin, è possibile ora descrivere in maggior dettaglio come Satoshi Nakamoto sia riuscito ad utilizzare questa tecnologia per creare una moneta digitale crittoanarchica, cioè un sistema che permette di effettuare pagamenti all'interno di una rete senza una controparte centrale e garantendo l'anonimato degli utenti. Il perno su cui regge l'intera struttura è il registro distribuito sul quale sono registrate le transazioni degli utenti. Il registro, a sua volta, si regge su programma informatico nel quale sono inserite le regole che disciplinano le modalità di creazione e tenuta del registro pubblico distribuito, sia per quanto attiene il profilo della struttura del registro, sia per quanto attiene il contenuto dello stesso, cioè le informazioni che sono registrate nei blocchi, che sono essenzialmente di due tipi: (*i*) informazioni concernenti la creazione di nuovi bitcoin; e (*ii*) informazioni concernenti il trasferimento di bitcoin. Le regole che disciplinano l'iscrizione delle singole transazioni all'interno dei blocchi della *blockchain* determinano, indirettamente, le modalità attraverso cui gli utenti possono scambiarsi bitcoin. Il modo più semplice per spiegare il funzionamento dell'intero sistema è quindi partire dal funzionamento di una singola transazione. Successivamente vedremo come ciascuna transazione sia iscritta nel registro collettivo, come le nuove unità di bitcoin siano create e come tale registro sia mantenuto aggiornato e sicuro, cioè protetto da eventuali attacchi.

2.3.1. *Le transazioni in Bitcoin: elementi necessari ed elementi accessori*

Assumiamo che Alice possegga cinque bitcoin e voglia trasferirne tre a Bob. Tutti i bitcoin in circolazione sono associati a degli "indirizzi" che possiamo intendere approssimativamente come il corrispettivo di un conto corrente bancario, o, meglio, di un IBAN. Ad ogni indirizzo corrisponde una coppia di chiavi di crittografia asimmetrica. Più specificatamente, ogni indirizzo è composto partendo dall'*hash* di una chiave pubblica, che viene elaborato attraverso particolari funzioni e al quale sono aggiunti alcuni caratteri

di controllo[253], può dirsi, però, semplificando, che ogni indirizzo Bitcoin sia costituito da una chiave pubblica. Chiunque possegga la corrispondente chiave privata è in grado di utilizzare i bitcoin associati a quell'indirizzo. Il numero di coppie di chiavi pubbliche e private che possono essere usate per creare indirizzi bitcoin è enorme: ogni utente può creare un numero indeterminato di indirizzi. La creazione degli indirizzi e la gestione degli stessi avviene solitamente attraverso dei programmi che creano dei file denominati *wallet*, «portafogli», che contengono al loro interno, in modo ordinato, le copie di chiavi. Alice, dunque, ha un *wallet* all'interno del quale sono memorizzati i suoi indirizzi bitcoin, insieme alle corrispondenti chiavi private. Il fatto che essa possieda cinque bitcoin significa che il saldo complessivo dei bitcoin associati ai suoi indirizzi è pari a cinque. Per poter trasferire tre bitcoin a Bob è necessario che anche Bob crei almeno un indirizzo Bitcoin e lo comunichi ad Alice. A questo punto Alice potrà creare una «transazione», cioè una comunicazione diretta alla rete bitcoin nella quale comunica che un determinato numero di bitcoin associati ad un certo indirizzo devono essere trasferiti ad un altro indirizzo. La transazione deve contenere, nei suoi elementi essenziali, (*i*) l'indirizzo di origine da cui sono presi i bitcoin, (*ii*) l'indirizzo di destinazione e (*iii*) la firma dell'operazione, realizzata mediante l'utilizzo della chiave privata associata all'indirizzo di origine. Non è invece in alcun caso necessario che nella transazione figuri la chiave privata associata all'indirizzo di destinazione, che, anzi, deve restare sempre segreta. Nella transazione non occorrerà, inoltre, specificare l'identità del titolare degli indirizzi bitcoin indicati: si tratta di un dato non necessario perché la titolarità dei bitcoin trasferiti dipende esclusivamente dal possesso della chiave privata associata all'indirizzo di destinazione, che dovrà essere utilizzata in occasione del successivo trasferimento. Questo da un lato garantisce l'anonimato all'interno della rete, dall'altro lato, implica che il possesso della chiave privata conferisce il pieno controllo dei corrispondenti bitcoin, con tutto ciò che ne consegue in caso di perdita o furto della stessa.

Il numero di indirizzi di origine e destinazione inseriti in ciascuna transazione può variare a seconda delle esigenze. Per esempio, nel caso in cui Alice non possegga un singolo indirizzo cui sono associati tre bitcoin, occorrerà che nella transazione siano inseriti più indirizzi di origine, nel qual caso la transazione dovrà essere firmata mediante

[253] Per maggiori dettagli v. CAETANO R., op. cit., pp. 74 ss..

l'impiego di tutte le chiavi private corrispondenti agli indirizzi di origine utilizzati. Nel caso vi siano più indirizzi di destinazione occorre, altresì, che sia indicata la quantità di bitcoin che sarà associata a ciascuno di essi, mentre non occorre indicare la quantità di bitcoin che deve essere presa dall'indirizzo di origine perché ogni volta che un indirizzo di origine (o meglio, come si vedrà a breve, l'*output* di una transazione precedente associata a quell'indirizzo) è utilizzato in una transazione, tutti i bitcoin associati a quell'indirizzo sono automaticamente riversati in tale transazione: come un salvadanaio che occorre rompere ogni qual volta si voglia utilizzare anche solo una delle molte monete che contiene. Questo significa che la somma dei bitcoin associati agli indirizzi di origine prima della transazione deve sempre essere uguale alla somma dei bitcoin che saranno associati negli indirizzi di destinazione. Nell'ipotesi in cui vi sia differenza tra l'ammontare contenuto nell'indirizzo di origine e la quantità di bitcoin che si intende trasferire – per gestire, cioè, il "resto" – occorre indicare un proprio indirizzo Bitcoin tra gli indirizzi di destinazione, come se si effettuasse un auto-trasferimento: in tal modo si "ricostruisce" un nuovo salvadanaio in cui confluiscono le monete non spese. Tale indirizzo può anche essere uno degli indirizzi di origine, sebbene per ottenere una maggiore privacy sia consigliato creare un indirizzo nuovo ad ogni transazione, in modo che le transazioni non siano associabili tra di loro (procedimento effettuato in automatico da numerosi *wallet*). Per esempio, se Alice possiede un solo indirizzo a cui sono associati cinque bitcoin verrà creata una transazione in cui figura: l'indirizzo di origine di Alice, la firma realizzata con la chiave privata associata a tale indirizzo, l'indirizzo di destinazione di Bob con l'indicazione del numero di bitcoin che dovranno essere associati a tale indirizzo e un indirizzo di destinazione di Alice, lo stesso di origine o un altro, con l'indicazione dei bitcoin che dovranno essere associati a tale indirizzo.

Tra gli elementi accessori che una transazione può contenere vi è anche l'indicazione dell'ammontare delle commissioni che il pagatore intende versare a colui che iscriverà la transazione nel registro. Tali somme saranno automaticamente dedotte dalla transazione, creando un'apparente divergenza tra *input* e *output* e figureranno sul

registro come transazioni a favore dell'indirizzo Bitcoin controllato dalla persona che ha annotato la transazione sul registro[254].

La corrispondenza tra *input* e *output* di una transazione e la gestione dei resti come ri-trasferimenti sul proprio conto sono gestiti così perché nel sistema bitcoin gli output di una transazione, cioè i bitcoin associati al termine di una transazione ad un determinato indirizzo, costituiscono gli input di ulteriori transazioni e viceversa: gli input di una transazione sono output di transazioni precedenti. Il fatto che Alice possedesse cinque bitcoin significa, quindi, che all'interno del registro distribuito erano trascritte delle transazioni per effetto delle quali 5 bitcoin erano stati trasferiti, o "associati", agli indirizzi contenuti nel portafoglio di Alice[255].

L'intero registro è costituito, cioè, una sequenza di transazioni concatenate tra loro. Se per semplificare immaginassimo che i bitcoin fossero unità indivisibili, partendo da una transazione sarebbe estremamente facile risalire tutta la catena di transazioni fino al momento in cui il bitcoin è stato creato[256]. Nella realtà non è esattamente così, perché ciascun bitcoin è divisibile sino all'ottavo decimale e i valori di output ed input sono semplicemente multipli e sottomultipli di bitcoin, valori numerici che possono essere combinati tra loro in qualsiasi modo. Si comprende, dunque, come mai il principio della perfetta corrispondenza tra il numero di bitcoin in entrata e in uscita in ciascuna transazione è un principio cardine del sistema al punto: se il numero di bitcoin in entrata fosse maggiore di quelli in uscita si perderebbero dei bitcoin in maniera irrimediabile, mentre se il numero di bitcoin in uscita fosse maggiore dei bitcoin in entrata vorrebbe dire che si sta cercando di "creare" nuovi bitcoin dal nulla, cioè che il pagatore non ha disponibilità dei fondi che vorrebbe trasferire. Simili transazioni sono invalide ai sensi del protocollo e non possono essere trascritte sul registro. La somma totale dei bitcoin in

---

254 Sul punto v. *infra*.

255 Per questo ogni volta che si impiega un indirizzo sostanzialmente si richiama una precedente transazione associata a tale indirizzo e tutti i bitcoin ricevuti in tale transazione entrano nella nuova transazione.

256 Questo era, grosso modo, il modello di moneta digitale immaginato da Nick Szabo: un registro dove sarebbero stati trascritti trasferimenti di *proof of work* dal valore fisso ed indivisibile. Cfr. SZABO N., *Bit Gold*, *op. cit*..

circolazione corrisponde, quindi, alla somma di tutti gli output di transazioni bitcoin non ancora spesi (definiti, in gergo tecnico "*unspent output transactions*", in breve "UTXO").

Perché la transazione tra Alice e Bob sia efficace occorre, ancora, che essa sia inserita all'interno di un blocco della *blockchain*. Solo compiuto questo ulteriore passo, l'intera rete saprà che all'indirizzo di Bob sono associati 3 bitcoin, che Bob potrà allora spendere riutilizzando quello stesso indirizzo come input di una nuova transazione.

2.3.2. *L'inserimento delle transazioni nella blockchain e la creazione di nuovi bitcoin: il lavoro dei miner*

Alice, dunque, per rendere efficace il trasferimento di bitcoin a Bob trasmette la transazione sulla rete affinché sia trascritta sul registro colletivo distribuito gestito tramite la tecnologia *blockchain*. L'operazione di trascrizione è compiuta grazie alla collaborazione dei *miner*, i nodi della rete che contribuiscono alla scrittura del registro collettivo.

I nodi connessi alla rete bitcoin non sono tutti uguali: essi si distinguono in base alle funzioni che esercitano[257]. I nodi che conservano una copia intera della *blockchain* in locale sono chiamati *full nodes*[258]. Avendo una copia intera del registro questi nodi sono in grado di verificare autonomamente la validità di ciascuna transazione: sia di quelle in cui sono parte, sia di quelle che ricevono casualmente dalla rete. Il processo di verifica e validazione è il primo passo verso l'annotazione sul registro distribuito e consiste in una serie di operazioni attraverso le quali si controlla l'idoneità della transazione ad essere annotata sul registro, cioè il rispetto di tutte le regole del protocollo che disciplinano la forma e il contenuto delle transazioni[259]. L'aspetto più importante di quest'operazione consiste nella verifica della provvista del dante causa: si controlla, cioè, che agli input

---

[257] Sul punto v. la descrizione molto efficace del network e dei vari tipi di nodi di ANTONOPOULOS, op. cit., pp. 138 ss..

[258] Il numero di *full nodes* presenti sulla rete a livello globale più variare e non è predeterminato, nel corso dell'ultimo anno tale numero è oscillato tra i 5.500 e i 6.000, con picchi massimi e minimi di 8.095 e 5.115 unità. Fonte: https://bitnodes.21.co/dashboard/?days=365 (19 febbraio 2017). Sulle funzioni svolte da un *full node* cfr. anche la pagina web https://en.bitcoin.it/wiki/Full_node (ultima visita 20 giugno 2017), in particolare la sezione "*Why should you run a full node?*".

[259] V. la lista completa delle operazioni che il software realizza per compiere la *Independent Verification of Transactions* in ANTONOPOULOS, op. cit., pp. 177-178.

della transazione corrispondano precedenti output iscritti sul registro, cioè che gli indirizzi di origine abbiano precedentemente ricevuto dei bitcoin che non sono ancora stati spesi[260]. Se il nodo riscontra un'anomalia la transazione non è ritrasmessa, se invece la transazione soddisfa tutti i requisiti è considerata valida e viene propagata agli altri nodi sulla rete. Il lavoro svolto da tutti i *full nodes* contribuisce, quindi, a filtrare e distribuire le transazioni, ma non porta direttamente alla pubblicazione sul registro.

Tale attività è svolta esclusivamente dai *miner*. Questi sono nodi che oltre a conservare una copia completa della *blockchain* contribuiscono alla prosecuzione della catena creando nuovi blocchi. L'origine del nome "*miner*" ha a che vedere con un paragone svolto da Satoshi Nakamoto per spiegare l'impiego delle funzioni di *proof of work* nel procedimento di creazione di nuovi bitcoin. Per ogni nuovo blocco che viene aggiunto sul registro, nuovi bitcoin sono creati ed attribuiti con una transazione originaria detta "*coinbase transaction*" al *miner* che ha prodotto il blocco. Come i cercatori d'oro scavavano nelle miniere per cercare l'oro, anche i moderni *miner* di criptovalute digitali, secondo il parallelismo, svolgono lavoro computazionale impiegando risorse hardware, tempo ed energia elettrica, al fine di "estrarre" nuovi bitcoin. Tale nome, in realtà non è completamente corretto perché mette in evidenza solo una delle due facce del loro lavoro, quella inerente la produzione di nuovi bitcoin, in origine più redditizia e per questo attraente e mediaticamente significativa, ma anche destinata ad interrompersi nel corso del tempo, mentre l'altra faccia del loro lavoro, quella dell'aggiornamento costante del registro, è parimenti centrale e proseguirà fintantoché esisteranno i bitcoin. Più corretto sarebbe stato, quindi, chiamare questi nodi «*keepers*», cioè custodi del registro, in quanto, come si è visto parlando in generale del funzionamento della tecnologia *blockchain*, il loro lavoro che permette sia l'aggiornamento, sia la sicurezza, del registro distribuito.

Il lavoro di creazione di nuovi blocchi rispecchia quanto già descritto *supra* a proposito della tecnologia *blockchain* e si compone di due fasi: la fase di preparazione del corpo del blocco e la fase di ricerca della *proof of work* necessaria per inserire il blocco nella *blockchain*. In parallelo a queste attività, i *miner* continuano a ricevere e a verificare, al pari di ogni altro *full node*, nuove transazioni ricevute dalla rete, solo che in questo

[260] Per compiere questa operazione tutti i *full nodes* conservano, unitamente alla copia della *blockchain*, un database che contiene tutte le *unspent output transactions*.

caso tutte le transazioni valide non ancora inserite nella *blockchain*, oltre ad essere ritrasmesse sulla rete, vengono aggregate all'interno di un apposito pool, chiamato *memory pool* o *transaction pool*. Ogni qualvolta inizia un ciclo di produzione di un nuovo blocco, il *miner* deve assemblare un nuovo *candidate block*, cioè una bozza di blocco, che, come ogni blocco definitivo, è composta da tre parti: (*i*) l'*header* o intestazione; (*ii*) la *coinbase transaction* e (*iii*) un elenco di transazioni prese tra quelle contenute nella *memory pool*.

L'annotazione delle transazioni nella blockchain

Per prima cosa, dunque, i *miner* eliminano dalla *memory pool* le transazioni inserite nel blocco appena ricevuto. Subito dopo avviene la selezione delle transazioni rimaste da inserire nel blocco: anche questo procedimento non è casuale, ma è disciplinato dal protocollo. Per ciascuna transazione è calcolata la c.d. "priorità" secondo un criterio che tiene conto del valore della transazione e dell'anzianità dell'output non speso utilizzato come input, in modo che le transazioni di valore alto o con input che risalgono indietro nella *blockchain* siano preferite alle transazioni di basso valore e più recenti. Le transazioni la cui priorità eccede una determinata soglia sono considerate ad "alta priorità", ad esse sono riservati i primi 50 kilobytes di ogni blocco: questo significa che queste transazioni possono essere inserite nel *candidate block* anche se non prevedono la corresponsione di commissioni. La restante parte del blocco è riempita, nei limiti della dimensione massima consentita per blocco, con le rimanenti transazioni, escludendo quelle che non prevedono commissioni e dando priorità a quelle che prevedono commissioni più alte (in termini di commissione per kilobyte di transazione). Le transazioni che non rientrano nel blocco restano nella *memory pool* per essere eventualmente inserite nel blocco successivo. L'implementazione di questo meccanismo fa sì che sia data priorità alle transazioni che prevedono una remunerazione più alta dei *miner*, permettendo però che anche transazioni senza commissioni possano eventualmente essere inserite, con tempi più lunghi, nella *blockchain*: col passare del tempo, infatti, la priorità della transazione aumenta sino eventualmente a diventare ad "alta priorità" ed essere quindi comunque inserite nella parte dedicata. La permanenza nella *memory pool* comporta che la transazione non diventi definitiva, nonché un rischio

marginale di non essere registrata, poiché quando il nodo del *miner* è riavviato la *memory pool* viene azzerata. In teoria una transazione comunicata sul network dovrebbe essere stata memorizzata da più *miner*, tuttavia non è escluso il rischio che essa si perda, per questo alcuni *wallet* sono configurati per re-inviare la transazione con una commissione più alta se la stessa non è inserita nella *blockchain* entro un certo tempo. Tale meccanismo di selezione, peraltro, se da un lato permette teoricamente l'invio di transazioni senza commissioni, al tempo stesso incentiva gli utenti ad incrementare il corrispettivo del servizio, specie nei momenti di congestione della rete.

La coinbase transaction

Selezionate tutte le transazioni, il *miner* procede a calcolare la *Coinbase transaction* che è la prima transazione inserita nel blocco dopo l'intestazione. Si tratta, invero, di una transazione *sui generis* attraverso la quale sono creati i nuovi bitcoin: l'output corrisponde ad un numero di bitcoin predeterminato dal protocollo cui sono sommate le commissioni di tutte le transazioni inserite nel protocollo; la somma di questi valori viene assegnata all'indirizzo del miner che ha coniato il blocco. Diversamente da tutte le altre transazioni, però, in questo caso non sono indicati *input*: i nuovi bitcoin sono semplicemente creati dal nulla attraverso l'attribuzione originaria al *miner*, mentre le commissioni sono estratte dalle altre transazioni riportate nel blocco. Inoltre, gli output delle *coinbase transaction* non possono essere spesi prima che siano stati minati almeno altri cento blocchi: quest'impostazione costringe i *miner*, specie nella fase inziale di vita del protocollo, a sostenere per un certo tempo la scrittura del registro, creando un temporaneo effetto di *lock-in* nel sistema.

Al momento della pubblicazione del protocollo, Satoshi Nakamoto ha deciso arbitrariamente che sarebbero stati prodotti complessivamente soltanto 21 milioni di bitcoin ad un ritmo esponenzialmente decrescente, secondo una regola che vuole dimezzata la ricompensa riconosciuta ai *miner* ogni 210.000 blocchi, cioè ogni circa quattro anni, sino al raggiungimento del ventunmilionesimo bitcoin. Per i primi quattro anni, dunque, la ricompensa per ogni nuovo blocco è stata pari a 50 bitcoin; dopo quattro anni è scesa a 25 bitcoin ed è oggi pari a 12,5 bitcoin. Tale regola è dunque iscritta nel

protocollo e fa parte del set di regole che disciplina il processo di validazione dei blocchi prodotti e distribuiti sulla rete.

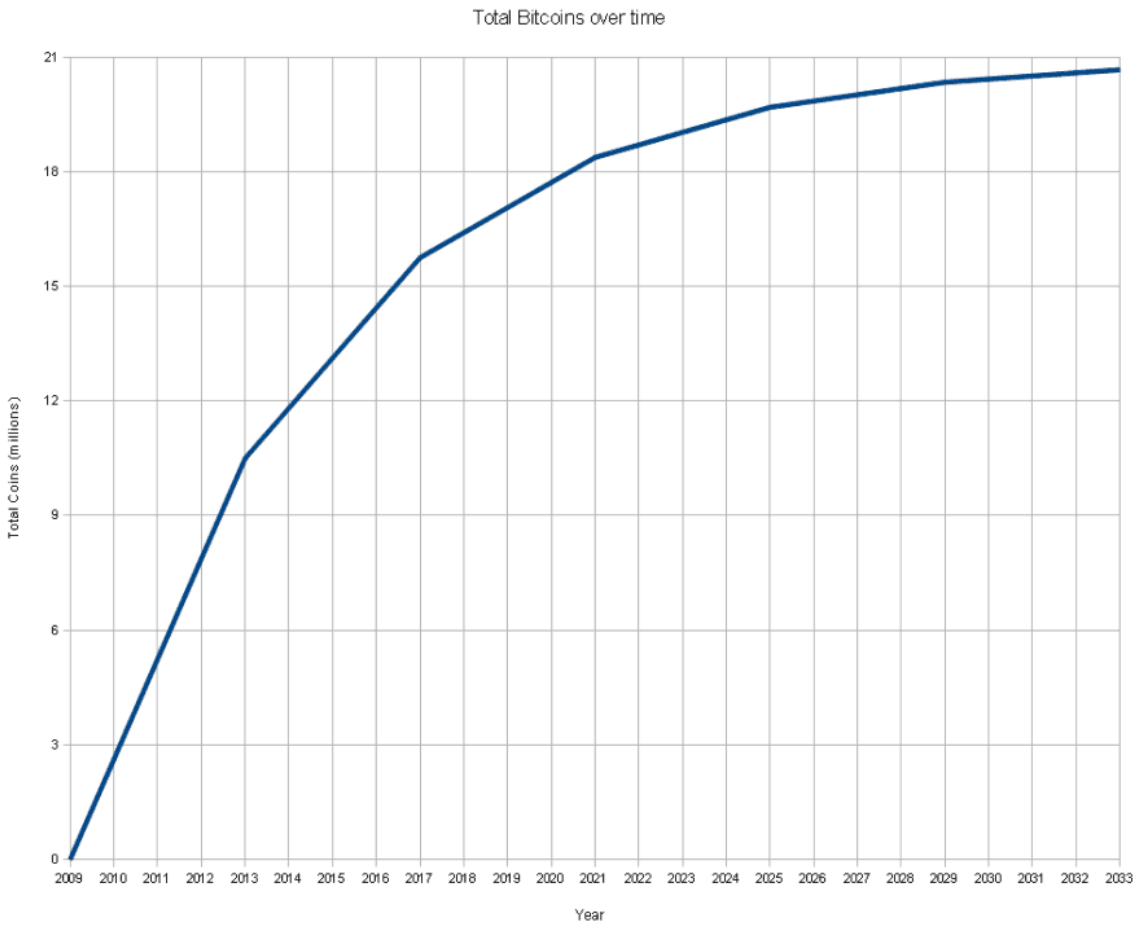


Fig. 1, stima della produzione totale di bitcoin (in mil.) per anno[261]

L'intestazione del blocco

L'ultima parte che viene compilata è l'intestazione del blocco. Essa è strutturata con criteri molto rigidi e contiene le informazioni relative alla concatenazione dello stesso all'interno della *blockchain*; vi si trova l'*hash* del blocco precedente[262], l'indice di tutte

[261] Fonte: https://upload.wikimedia.org/wikipedia/commons/5/54/Total_bitcoins_over_time.png (20 giugno 2017).

[262] Più specificatamente è contenuto il *digest* della funzione SHA-256 dell'*header* del blocco precedente. Poiché nell'header sono ricompresi i valori che definiscono il numero di transazioni inserite nel blocco e il *merkel root* che sintettiza gli *hash* di ciascuna transazione inserita nel blocco, di fatto l'*hash* dell'*header* riguarda tutti i dati compresi nel blocco.

le transazioni inserite nel blocco, nonché i valori del *nonce*[263] e la *proof of work* del blocco, che il *miner* proverà a calcolare per far diventare il *candidate block* definitivo. Una volta assemblate le transazioni e costruito il *candidate block* inizia, quindi, la seconda fase di creazione del blocco che consiste nella modifica graduale del *nonce* sino ad ottenere un blocco il cui *hash* soddisfa il *target* imposto dal protocollo[264]. Durante questa fase, peraltro, il *miner* continuerà a ricevere transazioni, a validarle e ad inserirle nella *memory pool*, da cui saranno riprese al momento della creazione del blocco successivo.

Proof of work e difficoltà nel protocollo Bitcoin

La *proof of work* nel protocollo Bitcoin consiste nel trovare un *hash* con l'algoritmo SHA256 il cui valore espresso in cifre esadecimali inizi, semplificando leggermente il discorso, con una serie di zeri (sia cioè inferiore ad un certo numero, sebbene ragionare in numeri a fronte di valori di 256 bit non sia affatto intuitivo). La difficoltà di tale operazione, varia in funzione della difficoltà del *target* imposto dal sistema che è modulata sulla base del numero di zeri richiesti all'inizio dell'*hash*: ad un maggiore numero di zeri iniziale corrisponde un valore del *target* minore e, quindi, un minore numero di *hash* che potenzialmente soddisfano il requisito. Un minor numero di probabilità di successo implica che occorrerà eseguire un maggior numero di tentativi e, quindi, un maggior impiego di capacità di calcolo.

Il protocollo è impostato affinché ciascun nodo aggiusti in modo automatico il grado di difficoltà della *proof of work* in funzione della capacità di calcolo totale impiegata sulla rete, in modo che occorrano approssimativamente 10 minuti per la creazione di un nuovo blocco[265]. Ogni 2.100 blocchi ciascun nodo verifica quanto tempo

---

263 Il *nonce* è un numero arbitrario che non rappresenta alcunché, il suo inserimento nell'intestazione del blocco ha solo la funzione di permettere la modulazione del *candidate block* perché possa essere costruito un blocco finale con un *hash* adeguato. Con l'inserimento del *nonce*, infatti, ciascun blocco viene a comporsi di due parti: una "fissa", che contiene le transazioni in bitcoin che si intende registrare sulla *blockchain*, la transazione *coinbase* e l'*hash* del precedente blocco, e l'altra "variabile" che può essere liberamente modificata al fine di ottenere un *hash* valido.

264 Il meccanismo che regola l'inserimento di nuovi blocchi nella catena è lo stesso che è stato descritto per illustrare il funzionamento di una *blockchain*; v. *supra*.

265 Cfr. Per un maggiore dettaglio, CAPOTI D., COLACCHI E. e MAGGIONI M., *Bitcoin revolution. La moneta digitale alla conquista del mondo*, Hopeli, Milano, 2015, pp. 50 ss..

ha impiegato la rete a creare i nuovi blocchi: se il tempo effettivamente impiegato è inferiore all'aspettativa di 10 minuti per blocco, la difficoltà del *target* è aumentata proporzionalmente, se il tempo è stato superiore la difficoltà è, invece, ridotta. In questo modo il sistema è in grado di adattarsi automaticamente all'aumento della potenza di calcolo della rete, che può essere dovuta sia all'impiego di tecnologie più avanzate, cioè ad hardware che permettono un maggior numero di calcoli per secondo, sia all'aumento del numero di *miner*. Si noti, in proposito, che il grado di difficoltà richiesto per minare nuovi blocchi è indipendente dal numero delle transazioni, dal loro valore e dalla loro dimensione in byte: esso dipende esclusivamente dalla potenza di calcolo impiegata nel network, che a sua volta dipende dal numero di *miner* e dalla quantità di risorse investite (in termini di hardware e di costo dell'energia elettrica utilizzata). Poiché il mercato del *mining* è un mercato aperto a cui tutti possono potenzialmente partecipare, la quantità di risorse investite dipende, a sua volta, dalla profittabilità del servizio. La difficoltà della *proof of work*, e quindi anche l'impatto ambientale dell'attività di *mining* dovuto all'impiego di energia elettrica per calcoli che, lo si è già sottolineato, non hanno alcuna funzione pratica se non quella di creare una gara tra più nodi, dipendono quindi, in ultima istanza, dal rapporto tra il costo dell'hardware e dell'energia elettrica impiegata[266], da una parte, e il valore economico della ricompensa riconosciuta ai *miner* espresso nella moneta con cui si paga l'energia e l'hardware, dall'altra parte, mentre sono del tutto indipendenti dal numero di transazioni in bitcoin registrate sulla *blockchain*[267].

Stabilità della blockchain Bitcoin

Una volta trovato il *nonce* che permette di ottenere un *hash* che soddisfa il *target* in quel momento vigente, il blocco è completo e viene trasmesso alla rete. Tutti i *full nodes* che ricevono il nuovo blocco verificano che esso sia stato preparato rispettando tutte le regole del protocollo: si verifica, quindi, che il nuovo blocco contenga il richiamo al blocco precedente, che tutte le impostazioni riguardanti la *proof of work* siano

[266] V. ANTONOPOULOS, op. cit., p. 197: "*The primary influence on the mining market is the price of one kilowatt-hour in bitcoin, because that determines the profitability of mining and therefore the incentives to enter or exit the mining market*".

[267] *Ibidem*, p. 196.

soddisfatte e che la *proof of work* calcolata sia corretta, che le transazioni inserite nel blocco siano valide e che l'indicizzazione delle stesse contenuta nell'intestazione sia valida. Se il blocco risulta corretto in ogni sua parte è aggiunto alla copia della catena posseduta dal nodo e inoltrato sulla rete.

Valgono qui, ora, tutte le considerazioni svolte circa la tecnologia *blockchain* nei precedenti paragrafi. La concatenazione dei blocchi e l'implementazione del meccanismo della *proof of work*, unitamente al continuo lavoro dei *miner*, permettono la gestione collettiva automatizzata del registro distribuito e garantiscono la resilienza del sistema nel suo complesso e la sostanzialmente non modificabilità delle informazioni annotate nei blocchi del registro. Nel contesto di una moneta digitale la cui allocazione tra gli utenti dipende dai dati contenuti nella catena-registro collettivo, tali attributi sono estremamente importanti, giacché la possibilità di riscrivere una parte del registro dove sono immagazzinate le transazioni significa concretamente che tali transazioni diventano reversibili e, quindi, non più affidabili, e che gli utenti sono esposti al rischio di "doppie spese" con la conseguente perdita dei bitcoin ricevuti. Sotto questi profili, come già anticipato nella fase di descrizione del funzionamento della *blockchain*, il protocollo Bitcoin è in astratto vulnerabile ad attacchi di doppia spesa da parte di un soggetto che riesca ad assumere il controllo di oltre la metà della capacità di calcolo dell'intera rete, così come è possibile che si verifichino biforcazioni accidentali della *blockchain*.

2.3.3. *Validità, efficacia e definitività delle transazioni*

Nel protocollo bitcoin, il problema della riproducibilità dei beni digitali e il rischio di doppia spesa, cioè di doppia alienazione di bitcoin, sono affrontati stabilendo che possono essere spesi solo output di transazioni già iscritte nel registro, cioè conferendo efficacia traslativa all'iscrizione della transazione sul registro. Poiché, però, l'inserimento di nuove annotazioni sul registro può essere controllato da chi detiene la metà del potere di calcolo, c'è il rischio, più teorico che pratico, che attraverso la fraudolenta gestione di questo potere siano commessi abusi. Il rischio è più teorico che pratico non perché non sia possibile che un tale potere di calcolo sia concentrato nelle mani di un soggetto o di

un gruppo[268], ma per le due seguenti ragioni. In primo luogo si deve chiarire che poiché i fondi attribuiti a ciascun utente – *rectius* a ciascun indirizzo Bitcoin – sono protetti da chiavi private, il controllo della produzione di nuovi blocchi sul registro non comporta altro vantaggio se non quello di poter spendere più di una volta i propri bitcoin. È tecnicamente possibile, cioè, per un soggetto che controlli più del 50% del potere di calcolo della rete far apparire come annotata su un nuovo blocco del registro una transazione e poi generare artatamente una biforcazione per sostituire il blocco ed "annullare" tale transazione. Non è, invece, possibile, per quel soggetto, creare un numero maggiore di bitcoin di quanti normalmente il sistema creerebbe, né trasferire bitcoin di altri utenti senza il loro consenso. Perché la doppia spesa sia realizzata, occorre, inoltre, che la falsa transazione generata per illudere la controparte di aver correttamente ricevuto il pagamento sia rimossa dal registro entro breve tempo (dieci, forse venti, massimo trenta minuti); l'attacco non funzionerebbe, quindi, in tutte quelle situazioni in cui l'esecuzione della controprestazione non è immediata o è reversibile, mentre per tutte le altre ipotesi per neutralizzare l'attacco sarebbe comunque sufficiente che la controparte attenda che alcuni blocchi siano aggiunti al registro perché l'ipotesi di riscrittura del blocco diventi inverosimile ed il trasferimento di bitcoin non possa più essere revocato. Ciò riduce enormemente il potenziale di un attacco del genere, al punto da rendere più probabile che nella realtà dei fatti il soggetto che eventualmente controlli tale potenza di calcolo tragga maggiore vantaggi dal comportarsi in modo onesto. La seconda ragione, già anticipata affrontando queste ipotesi con riferimento generale alla tecnologia *blockchain*, è che il registro è pubblico ed accessibile a tutti. Ciò implica a sua volta due considerazioni: la prima è che attacchi di doppia spesa risulterebbero palesi a chiunque sulla rete, sicché l'abuso della posizione dominante inficerebbe la fiducia nel sistema e causerebbe il crollo del valore dei bitcoin, rendendo anti-economico l'attacco; la seconda è che la rete è in grado di accorgersi delle concentrazioni di capacità di calcolo e una concentrazione pari o vicina al 50% desterebbe forti preoccupazioni e reazioni collettive che sfocerebbero, quantomeno, in un maggior grado di attenzione e di controllo collettivo. La trasparenza della rete, unitamente ai limitati vantaggi che è possibile trarre e l'elevato costo

[268] L'ipotesi potrebbe configurarsi, e si è in effetti configurata, con riferimento a gruppi di *miner* che collaborano insieme per svolgere collettivamente l'attività di *mining*.

opportunità che comporta la scelta di agire in modo non onesto, neutralizzano, quindi, nella pratica il rischio teorico di malfunzionamento del sistema che si verifica nella particolare ipotesi affrontata.

Le eventuali biforcazioni della *blockchain* sono risolte automaticamente dal protocollo Bitcoin tramite la continuazione del lavoro di *mining* e l'applicazione del criterio della prevalenza della *blockchain* più lunga. Nel momento in cui il conflitto tra due diversi rami della catena di blocchi è risolto, le transazioni registrate sui blocchi appartenenti al ramo che viene eliminato si hanno come non effettuate, a meno che esse siano state simultaneamente annotate anche nel ramo su cui prosegue il registro. Per evitare che siano definitivamente perse, prima di eliminare la copia dei blocchi temporaneamente inseriti nella *blockchain* e poi divenuti "orfani", i *miner* copiano le transazioni *ivi* contenute che non siano già state inserite nella *blockchain* nelle proprie *memory pool*, affinché possano essere nuovamente prese in considerazione nella preparazione dei successivi blocchi. Normalmente, quindi, tali transazioni dovrebbero essere re-inserite nella *blockchain*. Durante questa fase, tuttavia, è possibile che il dante causa di una di queste transazioni dolosamente o colpevolmente riutilizzi gli output usati in una di queste transazioni come input di altre transazioni, realizzando un'ipotesi di doppia spesa, ovvero che gli output di una transazione poi rimossa e non re-inserita nel registro siano usati come input di nuove transazioni anch'esse rimosse dal registro. Per queste ragioni si ritiene che una transazione che una transazione appena inserita nella *blockchain* possa essere considerata definitiva ed immutabile solo dopo che un certo numero di blocchi siano aggiunti successivamente al blocco in cui è annotata la transazione.

2.4. Gli attori del sistema

2.4.1. *Ancora sul ruolo dei miner*

I *miner* svolgono, dunque, un ruolo essenziale per il funzionamento del protocollo Bitcoin: rendono le transazioni efficaci *erga omnes* mediante l'annotazione sul registro distribuito; garantiscono l'affidabilità e l'immutabilità del registro; e, infine, producono e mettono in circolazione nuovi bitcoin. Per incentivare questa categoria di nodi o, meglio, per indurre i nodi a compiere attività di *mining*, Satoschi Nakamoto ha previsto

due tipi di remunerazioni: l'attribuzione di nuovi bitcoin e il pagamento di commissioni da parte degli utenti che trasferiscono bitcoin. La prima modalità di remunerazione attribuisce, di fatto, ai *miner* i benefici del signoraggio di questa nuova moneta. La remunerazione non è certa: quando, e se, riesce a produrre un blocco che viene inglobato nella rete, il *miner* riceve in cambio del lavoro svolto i bitcoin della *coinbase transaction*; se invece un altro *miner* riesce a trovare il blocco per primo, tutto il lavoro compiuto sino a quel momento è perso. Considerando, tuttavia, che la probabilità di produrre un blocco valido dipende dalla percentuale del potere di calcolo della rete controllata, nel lungo periodo l'incertezza legata alla produzione del singolo blocco lascia spazio alla prevedibilità su base statistica e si trasforma in calcolo dei costi e benefici del lavoro svolto. Per ovviare al rischio di dover aspettare troppo tempo prima di ottenere dei benefici economici, inoltre, i *miner* si sono presto raccolti in gruppi nei quali il lavoro è distribuito in modo che la potenza di calcolo di ciascuno sia sommata a quella di tutti gli altri del gruppo e sia, così, più facile ottenere dei bitcoin nel breve-medio periodo[269].

Via via che il numero di nuovi bitcoin creati con l'aggiunta di ogni nuovo blocco diminuisce, l'importanza delle commissioni per la remunerazione dell'attività di *mining* aumenta[270]. Le prospettive connesse a tale sviluppo sono di difficile lettura e dipendono altresì dalle dimensioni massime di ciascun blocco e quindi dal numero di transazioni che possono esservi inserite[271].

In entrambe le ipotesi di remunerazione, il guadagno dei *miner* è soggetto ad un continuo e forte rischio di cambio, perché esso corrisponde alla differenza tra le entrate, espresse in bitcoin, e i costi sostenuti in valuta locale per l'elettricità e l'hardware[272]. Ogni analisi di costi e benefici legata allo sviluppo dell'attività di mining dipende quindi da numerose variabili: gli sviluppi tecnologici legati alla creazione di nuovi hardware più

---

269 Gli accordi che regolano e disciplinano l'attività dei pool di *miner* sono di diverso tipo e variano soprattutto in funzione delle modalità di riconoscimento dei benefici al singolo *miner*. Si noti in proposito che i *pool* tendono a essere territorialmente determinati, ciò rende più facilmente individuabile la legge eventualmente applicabile e il regime giuridico cui soggiace l'accordo di collaborazione.

270 Cfr. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit., p. 4.

271 La definizione della dimensione massima dei blocchi è un tema molto discusso tra i *miner* e tra gli sviluppatori del software bitcoin, v. *infra*.

272 Cfr. CAPOTI e al., op. cit., pp. 65 ss..

performanti, la velocità di circolazione dei bitcoin e la quantità di transazioni che saranno inserite in ciascun blocco e, soprattutto, il valore di cambio tra bitcoin e moneta locale. Ciò rende difficile prevedere che impatto avrà la graduale diminuzione della remunerazione con nuovi bitcoin sulla percentuale di commissioni che saranno richieste per ogni transazione.

Sino ad oggi il mercato è stato remunerativo e ha riscontrato molto successo (in parte forse riconducibile all'entusiasmo di appassionati più che a precisi calcoli economici), il che ha portato allo sviluppo di nuovi hardware appositamente creati per compiere un numero elevatissimo di calcoli al secondo con bassi consumi energetici. Tali sviluppi hanno provocato il forte innalzamento della difficoltà del *target*, trasformando l'attività di *miner* in un'attività sostanzialmente imprenditoriale ed escludendo dalla competizione per la creazione di nuovi blocchi l'utente occasionale.

2.4.2. *Exchange, gestori di wallet e la comunità degli utenti*

Il successo mediatico ed economico dei bitcoin ha portato alla nascita di altre figure professionali che operano al di fuori dell'ambito del protocollo, pur svolgendo servizi ad esso connessi: gli *exchange* e i gestori di *wallet*. L'insieme di questi operatori contribuisce a formare quello che è stato definito "l'ecosistema Bitcoin"[273], cioè una rete di soggetti coinvolti a vario titolo in rapporti che permettono agli utenti comuni di utilizzare i bitcoin come fossero una moneta. Sotto il profilo dello sviluppo dei bitcoin, oltre alle figure già richiamate è corretto anche ricordare l'importante ruolo svolto dai siti web specializzati e dai forum dedicati.

Gli *exchange* sono soggetti che prestano servizi inerenti il cambio di bitcoin contro altre valute. La stragrande maggioranza di questi operatori offrono servizi di acquisto e vendita di bitcoin tramite piattaforme elettroniche accessibili da Internet: alcuni *exchange* si propongono come controparte diretta per gli scambi con gli utilizzatori, altri svolgono, invece, un servizio di mediazione tra acquirenti e venditori raccogliendo ordini di segno opposto in modo simile a quanto avviene sui mercati finanziari telematici. Esistono,

[273] MANCINI M., *Valute virtuali e Bitcoin*, cit., p. 121; BANCA CENTRALE EUROPEA, *Virtual Currency Schemes – a further analysis*, 2015, cit., p. 4.

infine, delle piattaforme che permettono di pubblicare annunci per la compravendita di bitcoin su base locale.

I gestori di *wallet* sono soggetti che offrono il servizio di conservazione e gestione di *wallet* sia *online*, sia attraverso dispositivi di *cold storage*. Nei *wallet* sono salvate tutte le chiavi private di un utente: questo significa che perdere il controllo di questi file comporta la perdita di tutti i propri bitcoin, che, nella peggiore delle ipotesi, non potranno più essere usati da nessuno. L'uso di un servizio di backup del proprio portafoglio *online* su server dedicati permette di evitare questo tipo di inconvenienti, ma espone anche al rischio di *mala gestio* e al rischio che altri utenti riescano ad impossessarsi delle chiavi private e a rubare tutti i bitcoin. Taluni di questi gestori replicano le funzioni tipicamente svolte da un *wallet* agendo però come gestori di fondi collettivi di bitcoin: ciascun utente apre una sorta di conto corrente / conto titoli con il provider del servizio, sul quale tiene traccia del suo saldo giornaliero, ma a ciascun suo ordine non corrisponde un'annotazione sulla *blockchain* perché è il provider che mantiene direttamente per conto e nell'interesse degli utenti i bitcoin. Questo permette di operare scambi tra gli utenti del medesimo servizio modificando le posizioni di credito degli stessi nei confronti del provider, senza svolgere annotazioni sulla *blockchain*: al vantaggio in termini di semplificazione dello scambio corrisponde, però la reintroduzione di un rapporto di fiducia e dipendenza da un intermediario[274].

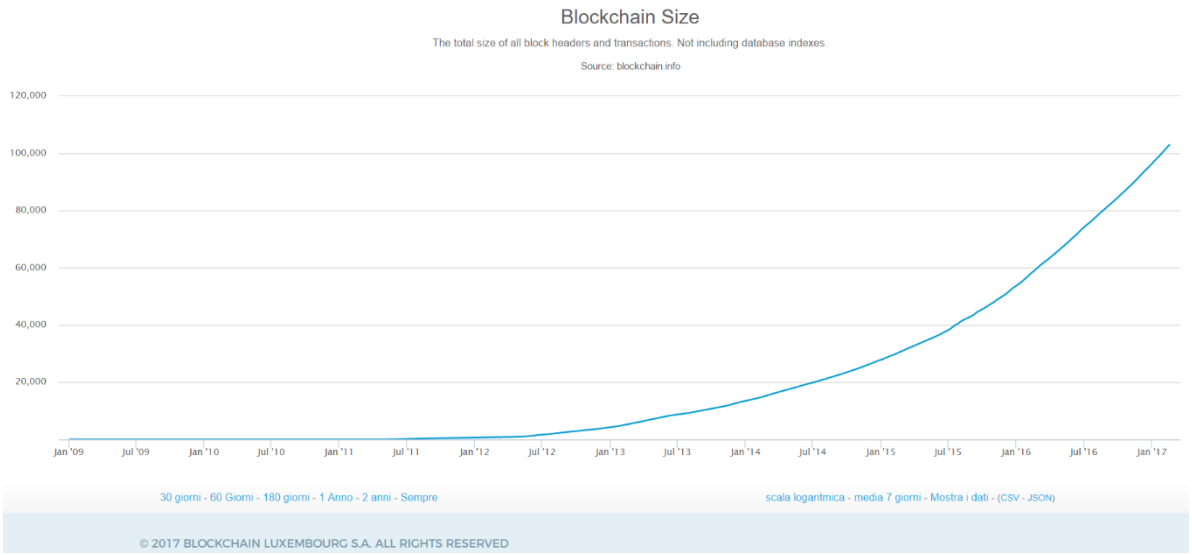
Il mercato degli *exchange* e dei gestori di *wallet* è un mercato dinamico dal punto di vista dell'innovazione tecnologica, ma molto concentrato e spesso lo stesso provider svolge entrambe le attività offrendo diverse articolazioni del servizio. A differenza di quanto concerne il funzionamento della *blockchain*, in cui ogni passaggio è gestito da un sottile equilibrio di funzioni matematiche ed incentivi comportamentali tali con l'obbiettivo di autoregolamentare il sistema, questi servizi sono svolti sulla base di relazioni contrattuali disciplinate dalle leggi locali. Sotto questo profilo sorgono interessanti questioni relativamente al rispetto delle riserve di attività economica, in

[274] Un altro tipo di transazioni in bitcoin che non vengono annotate sulla *blockchain* consiste nella consegna delle chiavi private. Si è provato ad utilizzare tale metodo per incorporare bitcoin in beni materiali. Il problema con questo tipo di operazioni è che nel caso in cui il dante causa conservi una copia della chiave privata sussiste un rischio di frode e di doppia spesa che non riceve alcuna tutela tecnologica dal protocollo.

particolare per quanto riguarda le ipotesi di configurazione di tali servizi come attività di raccolta del risparmio, di intermediazione finanziaria e di cambiavalute. L'applicazione di tali regole si scontra, però, con il problema della definizione giuridica dei bitcoin e con il principio di interpretazione restrittiva delle leggi che derogano al principio della libertà di attività economica. Il tema, evidentemente, presenta profili di grandissimo interesse per il legislatore e per le agenzie predisposte al controllo delle attività finanziarie e bancarie, per il momento, tuttavia, il settore resta, salvo qualche limitata eccezione, largamente non regolato[275].

Chi sono invece gli utenti che utilizzano i bitcoin? È molto difficile descrivere chi effettivamente utilizzi i bitcoin in questo momento. Inizialmente è ragionevole pensare che sia stato utilizzato soprattutto da persone vicine al mondo dell'informatica incuriositi dal nuovo sistema, da appassionati di crittografia o da simpatizzanti delle idee crittoanarchiche; un vasto bacino di utenza è stato composto inizialmente da persone che acquistavano beni illegali su mercati neri, il più famoso dei quali è stato *Silk Road*. Nel corso degli anni il bacino di utenza si è però diversificato e un'analisi sociologica degli utenti di questa moneta sarebbe qui fuori luogo. È possibile e doveroso, invece, chiedersi, poste le regole disciplinano il protocollo, che tipo di utenti possano connettersi a questo sistema e in che modo. Dal punto di vista della tecnologia impiegata, il protocollo Bitcoin permette a chiunque di avere accesso diretto ed integrale al registro collettivo, così da beneficiare pienamente della sicurezza tecnologica garantita dal sistema e poter controllare direttamente senza intermediari la validità e l'annotazione sul registro delle transazioni che lo riguardano. Per raggiungere questo livello di partecipazione occorre, tuttavia, scaricare integralmente una copia della *blockchain* sul proprio computer e mantenerla regolarmente aggiornata. Poiché sulla *blockchain* sono trascritte tutte le transazioni, la dimensione della *blockchain* è considerevole ed in costante crescita: ha superato la soglia dei 100 Gigabyte ed è in continua, esponenziale, crescita, come illustrato nel seguente grafico.

[275] Sul punto v. *infra*.



https://blockchain.info/it/charts/blocks-size?timespan=all

La maggior parte degli utilizzatori non si collega, quindi, alla rete Bitcoin come *full node*, non partecipa al meccanismo di verifica e validazione dei blocchi e non partecipa al processo di *mining*. Per evitare che essi debbano fare affidamento ad intermediari connessi alla rete come *full nodes* per avere contezza dei suoi bitcoin, è stato prevista, sin dal principio, una modalità semplificata di comunicazione con la rete chiamata "*simplified payment verification*", che permette agli utenti di scaricare le intestazioni di tutti i blocchi della *blockchain* e di richiedere in un secondo tempo solo le parti del registro in cui sono annotate operazioni di interesse per l'utente (per esempio la parte di un blocco su cui è annotata una transazione a favore di uno dei suoi indirizzi pubblici). Attraverso appositi software è quindi ancora possibile, a condizione di essere disposti a compiere qualche sforzo per comprendere il funzionamento del sistema[276], connettersi direttamente alla rete, senza ricorre ai servizi di un intermediario[277].

In tutti quei casi in cui l'accesso diretto alla rete non è la soluzione adeguata alle esigenze del potenziale utilizzatore di bitcoin, intervengono i servizi offerti all'interno dell'ecosistema Bitcoin, che è, ovviamente, organizzato in modo da essere il più inclusivo possibile e permettere a più persone possibili di trasferire, acquistare e vendere con

276 V. LEMME e PELUSO, op. cit., p. 16.

277 Cfr. la pagina di istruzioni https://bitcoin.org/it/come-iniziare (ultima visita 20 giugno 2017) ed in particolare https://bitcoin.org/it/scegli-il-tuo-portafoglio (ultima visita 20 giugno 2017), dove è sottolineato ed evidenziato l'avvertimento "*Prendi tempo per apprendere*".

facilità Bitcoin, attraverso interfacce semplici ed intuitive, utilizzabili anche direttamente su smartphone [278].

È interessante notare che in questo emergente mercato giochino un ruolo così significativo i cambiavalute. Questo da un lato è logico considerato il meccanismo che regola la creazione di bitcoin. Lo sviluppo della concorrenza nel *mining* ha, infatti, comportato l'innalzamento del livello di difficoltà del target e ha portato alla creazione di macchine hardware appositamente studiate per eseguire un numero sempre maggiore di calcoli con minori consumi di elettricità, rendendo il *mining* un'attività che richiede investimenti e modalità organizzative tipiche di un'impresa. La professionalizzazione di questo ruolo non permette, quindi, all'utente comune di procurarsi bitcoin attraverso questo metodo, ma lo costringe, viceversa, ad acquistare bitcoin offrendo in cambio altre monete, beni o servizi. Per converso, i *miner* hanno tutto l'interesse – e la necessità, stanti i costi di gestione sopportati in valute locali – a cedere i bitcoin guadagnati con il loro lavoro in cambio di valute nazionali. In effetti, tutti i bitcoin in circolazione sono stati inizialmente posseduti da un *miner* e da questo rivenduti sul mercato, nella stragrande maggioranza dei casi in cambio di valute tradizionali[279]. Dall'altro lato, i volumi significativi di transazioni gestiti dagli *exchange*, la nascita di servizi di *trading* e la presentazione dei bitcoin come una moneta il cui valore crescerà nel tempo con significative prospettive di realizzazione di plus valore, sono indici del fatto che i bitcoin sono utilizzati, come avremo modo di approfondire, non solo come mezzo di pagamento, ma anche come investimento speculativo. In entrambi i casi, l'utilizzatore comune si avvicina al mondo dei bitcoin, nella maggior parte dei casi, acquistandoli contro valute tradizionali.

Il successo che i bitcoin hanno avuto in questi anni, la crescita di valore e del numero di servizi offerti agli utenti ha segnato, dunque, una profonda evoluzione nella

---

[278] Sono numerosissimi i siti che presentano i bitcoin come uno strumento alla portata di chiunque. Oltre ai siti commerciali dei provider che offrono servizi a pagamento, si veda, per un esemplificazoine di questo approccio, il sito (www.bitcoin.org), i numerosi video disponibili sulla piattaforma *Youtube*, nonché la letteratura divulgativa sul punto, dove spesso si comincia con lo spiegare passo, passo, come acquistare e vendere Bitcoin, per tutti GUTTMANN, op. cit..

[279] La persona comune che voglia iniziare ad utilizzare i Bitcoin può alternativamente iniziare ad accettarli in pagamento in cambio dei servizi e prodotti che produce o, più semplicemente, acquistarli in cambio di valute tradizionali.

compagine degli utilizzatori. Da moneta di nicchia utilizzata soprattutto da programmatori entusiastici e per acquisti illegali sottobanco, i bitcoin sono diventati, non da ultimo grazie ai positivi riscontri sulla tecnologia *blockchain*, un fenomeno *mainstream* e la rete di utilizzatori si è segmentata tra: (*i*) gli utilizzatori più o meno occasionali che potremmo considerare consumatori del servizio di pagamento Bitcoin, *ivi* inclusi coloro che acquistano bitcoin con finalità di investimento, coloro che usano i bitcoin per acquistare beni e servizi e gli imprenditori che decidono di accettare bitcoin come mezzo di pagamento e coloro che usano i bitcoin a fini illegali, quali il commercio su internet di beni o servizi illeciti (droga *in primis*) o le estorsioni basate su virus informatici; (*ii*) le imprese che esercitano attività connesse all'utilizzo di questi servizi di pagamento (inclusi i *miner*); e (*iii*) il nucleo più ristretto di utilizzatori molto sofisticati, che attivamente contribuiscono alla risoluzione dei problemi legati alla rete e allo sviluppo di migliorie del protocollo. Dello spirito originario, di slancio entusiasta e a tratti sovversivo, oggi resta traccia soprattutto nel contesto delle attività svolte da questo ristretto gruppo di utenti, di revisione, aggiornamento e miglioramento del software e nella narrativa sviluppata dai più fervidi sostenitori e divulgatori di questa "nuova moneta".

2.5. La *governance* del protocollo Bitcoin

Si è chiarito, sinora, come funziona il sistema di scambi bitcoin e chi sono i principali attori che vi operano. Al cuore di tutto risiede una rete di computer che comunicano tra loro attraverso uno specifico software: ciascun nodo riceve e propaga informazioni sulla rete; tutti i *full nodes* verificano e validano le transazioni e i nuovi blocchi trasmessi sulla rete, conservando una copia della catena di blocchi più lunga; i *miner*, oltre a verificare e validare le transazioni, producono i nuovi blocchi e, attraverso questa attività, annotano le transazioni sulla *blockchain* e creano, nei limiti fissati dal protocollo, nuovi bitcoin. Il coordinamento di tutte queste operazioni permette di gestire un registro collettivo distribuito conoscibile da chiunque, che può essere aggiornato senza il bisogno di un ente centrale, poiché la rete è in grado di far emergere in modo spontaneo ed automatico il consenso circa la versione del registro da ritenersi valida. Tale risultato

è conseguito attraverso l'implementazione di particolari funzioni matematiche[280]: le funzioni di *hash* permettono di garantire la continuità del registro, ne regolano la velocità di aggiornamento e sorreggono il criterio della catena più lunga, che è utilizzato per determinare la scelta tra eventuali versioni discordanti; le funzioni di crittografia a doppia chiave permettono di usare pseudonimi nella creazione di transazioni, così da garantire l'anonimato degli utenti, e garantiscono la sicurezza dell'attribuzione dei bitcoin a ciascun partecipante.

2.5.1. *Protocollo,* consensus rules *e* software *in un sistema* blockchain

Il ricorso a tali funzioni matematiche è presentato come uno dei punti centrali del sistema bitcoin ed è invero difficile sottostimare la loro importanza all'interno del progetto bitcoin: l'introduzione della *blockchain* e l'invenzione della *distributed ledger technology* si basano sostanzialmente su queste funzioni e sono le loro proprietà matematiche che garantiscono sicurezza e resilienza al sistema. Il loro impiego, però, non è diretto, bensì mediato dalle regole iscritte nel protocollo, senza il quale non sarebbe possibile utilizzare tali strumenti. Se è vero, infatti, che senza la crittografia non potrebbero esistere i bitcoin, è altrettanto vero che il progetto è pur sempre basato e presuppone una rete di computer connessi tra loro in grado di comunicare con un unico linguaggio condiviso e solo all'interno di tale rete ha senso ricorrere alle funzioni matematiche sopra descritte come strumenti di *governance* per disciplinare in modo automatico i comportamenti degli agenti. Sebbene quindi non sia sbagliato dire che i bitcoin si fondano sulla crittografia, nel descrivere il funzionamento del sistema è più corretto spiegare che i bitcoin si fondano sulla condivisione all'interno della rete di un unico protocollo che coordina le attività dei soggetti partecipanti attraverso la predisposizione di regole comuni e l'utilizzo di funzioni matematiche, secondo un disegno complessivo che bilancia i vari interessi dei partecipanti per rendere possibile la gestione decentrata di un registro comune, e che tale protocollo ricorre, *inter alia*, all'uso di funzioni di crittografia.

[280] "*Vires in numeris*" è il motto stampato su copie fisiche di bitcoin prodotte da Mike Caldwell, v. DODD, op. cit., cap. 7.

In particolare, l'attività degli agenti è regolata dal protocollo attraverso la definizione dei requisiti che le transazioni e i blocchi diramati sulla rete devono soddisfare per essere inseriti all'interno della *blockchain*. La sanzione per il mancato rispetto di questi criteri e la conseguente invalidità di un blocco o di una transazione, è, per converso, che essi saranno ignorati dagli altri membri della rete e quindi non figureranno nella catena distribuita[281]. Attraverso la precisa modulazione dei criteri di validazione delle transazioni e dei blocchi e la minaccia di questa sanzione, applicata in modo automatico da tutti i partecipanti della rete che condividono in modo uniforme i criteri di validazione, sono implementate tutte le regole di funzionamento della *blockchain* sopra descritte, incluse: (*i*) le regole che riguardano il meccanismo della *proof of work* e la definizione della difficoltà della stessa; (*ii*) le regole sulla quantità di bitcoin prodotti per ogni nuovo blocco, da cui discende il limite massimo di produzione di ventun milioni di bitcoin; (*iii*) le regole sulla firma delle transazioni, che garantiscono l'univocità dell'attribuzione di un numero determinato di bitcoin in capo ad un soggetto; e (*iv*) le regole che impediscono il riutilizzo di un output speso, rendendo irrealizzabili le ipotesi di doppia spesa.

L'insieme dei criteri di validazione delle transazioni e dei blocchi e le regole ad essi implicitamente sottesi costituiscono le *consensus rules* applicate nel protocollo in un certo momento storico. La *governance* all'interno di un certo protocollo è quindi principalmente definita dall'applicazione (automatica da parte del *software* utilizzato dai nodi) di questi criteri (cui corrispondono *policy* e regole che a loro volta disciplinano il comportamento degli utenti), che, unitamente all'applicazione del principio di preferenza della catena più lunga, concorrono alla formazione del consenso su una specifica manifestazione storica della catena distribuita sulla rete.

Il protocollo è formato, oltre che dalle *consensus rules*, dalle regole operative che disciplinano la trasmissione di informazione tra i nodi e gli standard necessari per l'interoperabilità con altri sistemi esterni alla rete. Esso si distingue dalla nozione di *software*: il protocollo è l'insieme coordinato di tutte le regole che permettono ai

[281] Per tale intendendosi la versione della catena memorizzata e considerata valida dai nodi che condividono il set di criteri di validazione applicati, posto che in presenza di due o più set di criteri di validazione confliggenti e concorrenti è astrattamente possibile, come si illustrerà a breve, che uno o più gruppi di utenti facciano affidamento ad una catena che non è riconosciuta come valida dal resto della rete.

computer appartenenti ad una specifica rete – in questo caso la rete bitcoin – di dialogare tra loro, è il linguaggio comune utilizzato dagli elaboratori elettronici; il software è invece l'applicativo memorizzato ed eseguito su ciascun elaboratore che contiene le istruzioni che saranno eseguite dal calcolatore elettronico. Il protocollo bitcoin è quindi l'insieme di regole che disciplinano le iterazioni tra computer sulla rete bitcoin, il software bitcoin è l'applicativo utilizzato dai computer.

Perché il meccanismo della *blockchain* funzioni occorre, ovviamente, che le *consensus rules* siano applicate in modo uniforme da tutti i membri della rete. Ciò è reso possibile, normalmente, mediante la trascrizione del protocollo all'interno di un software e l'esecuzione dello stesso da parte di tutti i nodi della rete. Non è, però, necessario che tutti i nodi della rete utilizzino esattamente lo stesso *software*: ve ne possono invece essere diversi, purché tutti rispettino e incorporino al loro interno lo stesso protocollo[282]. È quindi possibile che alcuni nodi della rete bitcoin eseguano un *software* diverso rispetto a quello adottato dalla maggioranza degli utenti senza che questo comporti una frattura della *blockchain*, a condizione che il protocollo adottato sia lo stesso e che soprattutto le *consensus rules* siano le stesse. La presenza di criteri di validazione diversi potrebbe infatti condurre alla creazione di catene concorrenti riconosciute solo da alcuni nodi e non da altri, frazionando la rete secondo il protocollo adottato da ciascun nodo. Questa ipotesi di frazionamento della rete può verificarsi per effetto di una precisa scelta "politica" di rottura con il paradigma vigente da parte di un gruppo che intenda volontariamente separarsi dagli altri nodi ovvero può accadere accidentalmente in occasione di un aggiornamento del protocollo o del software che lo contiene.

[282] Si pensi al caso della navigazione sulla rete internet, in cui diversi software (i più diffusi sono Internet Explorer, Firefox, Chrome e Safari) utilizzano gli stessi protocolli http e https. Si noti peraltro che nel presente scritto si utilizza una nozione di protocollo più ampia rispetto alla nozione normalmente utilizzata in informatica. In informatica il protocollo è normalmente definito come l'insieme di regole che costituiscono il linguaggio con cui gli elaboratori elettronici si scambiano informazioni su una rete; nel caso di specie la nozione è estesa a ricomprendere tutte le regole che disciplinano la cooperazione tra computer al fine di costruire il registro distribuito condiviso e comprende, quindi, oltre alle regole che disciplinano lo scambio di informazioni, quindi la comunicazione in senso stretto, anche le *consensus rules*, che riguardano la cooperazione e l'esecuzione di un progetto comune. L'uso di questa accezione più ampia è diffuso nella letteratura sullo specifico tema dei bitcoin e appare quindi pienamente giustificata per questa ragione.

Sia il *software*, sia il protocollo sono, infatti, sempre modificabili. La modifica del protocollo comporta a cascata e si concretizza con l'aggiornamento di tutti i software che ad esso fanno riferimento, mentre la modifica del software deve essere sempre realizzata ponendo particolare attenzione al rispetto del protocollo e alle possibili incompatibilità che la modifica può apportare. In entrambi i casi le modifiche pensate e decise da chi pubblica il software diventano operative solo nella misura in cui gli utilizzatori del software aggiornano la loro versione: senza questo passaggio le modifiche influiscono solo sul modello, non sulle versioni correnti in uso da parte dei membri della rete.

2.5.2. *Il software bitcoin e il suo aggiornamento*

Nella fattispecie oggetto di esame, il protocollo immaginato da Satoshi Nakamoto è stato direttamente inserito nella prima versione del software da lui pubblicata. L'adozione e l'esecuzione di tale programma da parte di tutti i nodi della rete ha permesso la comunicazione tra gli stessi e la progressiva compilazione della *blockchain*.

In merito alle possibili modifiche del software bitcoin, la filosofia adottata da Satoshi Nakamoto sin dagli arbori è stata di pubblicare insieme all'applicativo il codice sorgente del programma, questo sia per ragioni di trasparenza, perché la pubblicazione del codice sorgente avrebbe permesso a chiunque di verificare il funzionamento del software e sincerarsi della corrispondenza tra quanto dichiarato e quanto inserito nel programma e della solidità dello stesso, sia per permettere ad altri programmatori di proporre migliorie al codice. Oggi il software originariamente prodotto da Satoshi Nakamoto si è sviluppato in un progetto *open source* chiamato «Bitcoin Core» che pubblica e aggiorna il software Bitcoin Core[283], chiamato in gergo anche «Satoshi». Nel corso del tempo sono stati rilasciati numerosi aggiornamenti del programma – se ne contano più di centosessantotto[284] –, che hanno visto via via l'introduzione di nuove funzioni, piccole migliorie e la risoluzione di bug. Come molti altri progetti *open source*,

[283] Al momento è in uso la versione 0.14.2 del programma, v. https://bitcoin.org/it/scarica (ultima visita 20 giugno 2017), nonché https://github.com/bitcoin/bitcoin/releases (visita 20 giugno 2017)

[284] V. https://github.com/bitcoin/bitcoin (ultima visita 20 giugno 2017)

i *repository* del programma sono ospitati sulla piattaforma di programmazione Github[285], dove si trovano pure tutte le versioni del programma a partire dal settembre 2009 sino ad oggi e i forum su cui le proposte di modifiche sono discussi. Il sito www.bitcoincore.org offre, invece, una panoramica *user friendly* del progetto e chiarimenti sulle modifiche introdotte nelle varie versioni.

La partecipazione via *web* al processo di aggiornamento del *software* è libera ed aperta a tutti: chiunque può liberamente contribuire proponendo idee o codice. L'adozione di tali proposte e la pubblicazione di nuove versioni del software sono invece competenze riservate esclusivamente ad un ristretto numero di sviluppatori[286], alcuni dei quali coinvolti sin dalle origini nel progetto, che svolgono un ruolo di moderatori ed arbitri finali dei dibattiti sviluppati via web[287]. Le mere correzioni di *bug* nel codice sono implementate sulla base del consenso diffuso all'interno della mailing list degli sviluppatori e nel forum. È sufficiente, quindi, che un programmatore evidenzi il problema pubblicamente e che all'interno del forum o della mailing list emerga una soluzione ragionevole pubblica e condivisa, che verrà quindi inserita nel successivo aggiornamento del programma. Per le modifiche più significative di interesse collettivo che riguardano il protocollo o programmi connessi è prevista, invece, una articolata procedura che richiede la pubblicazione sul sito Github di un *Bitcoin Improvement Proposal* ("BIP"), un breve documento strutturato secondo un modello ben definito, che descrive in modo specifico la proposta di modifica e la *ratio* che le giustifica.

---

285 La pagina del progetto Bitcoin, in particolare, è la seguente: https://github.com/bitcoin/ (ultima visita 20 giugno 2017)

286 Questi si distinguono in «Maintainers» e «Contributors». I primi hanno pieni poteri di amministrazione (in senso informatico) sulle pagine del sito da cui è pubblicato il software e sono quindi gli unici che possono effettivamente rilasciare una nuova versione dello stesso; il secondo gruppo comprende, invece, tutti i programmatori che partecipano allo sviluppo del software. Al momento (ultima visita: 28 febbraio 2017) i *maintainers* sono 3: Wladimir J. van der Laan, Jonas Schnelli e Marco Falke. Il loro numero non è fisso e in passato Gavin Andresen ha fatto parte di tale gruppo. V. il sito https://bitcoincore.org/en/team/. V. anche il sito https://bitcoin.org/it/sviluppo (ultima visita 28 febbraio 2017), nonché https://github.com/orgs/bitcoin/people (ultima visita 28 febbraio 2017) dove sono segnalati i maggiori contributori.

287 CANDILORO D., *La sicurezza informatica di bitcoin*, in *Ciberspazio e diritto*, 2015, pp. 331 ss., p. 354; v. anche GUTTMANN, op. cit., pp. 30 ss..

Tale procedura è stata definita per la prima volta nel 2011 con il BIP-001, "*BIP Purpose and Guidelines*"[288] e poi aggiornata, nel corso del 2016, con l'adozione del BIP-002, "*BIP process, revised*"[289].

Preliminarmente, si richiede di presentare la nuova idea alla comunità Bitcoin, per sondare il terreno e capire se la proposta suscita interesse e approvazione. Il successivo passaggio consiste nel presentare una bozza del nuovo BIP alla *Bitcoin development mailing list*, perché i membri possano verificare la correttezza formale della proposta, la fattibilità dal punto di vista informatico ed eventualmente possano già suggerire chiarimenti o integrazioni. Ricevuti questi commenti, l'autore può caricare il testo del nuovo BIP sul sito Github, dove un editor incaricato della gestione di questi processi verificherà la rispondenza del BIP ai requisiti formali: se tutti i requisiti sono soddisfatti, la proposta è ritenuta sufficientemente specifica, chiara e ben dettagliata, allora il BIP viene numerato e formalmente inserito nella lista dei BIP aperti alla discussione[290]. Si

[288] Del 19 agosto 2011, disponibile sul sito: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki (ultima visita 20 giugno 2017).

[289] Del 3 febbraio 2016, in seguito solo "BIP-002", disponibile sul sito: https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki (ultima visita 20 giugno 2017). Tale procedura ricalca i meccanismi decisionali in uso nella Internet Engineering Task Force, che a sua volta costituisce un esempio di una *best practice* diffusa tra le organizzazioni non gerarchiche operanti nel settore del *web*, basata sulla presentazione di proposte al commento di tutti i membri (nel caso della IETF si hanno *Internet-Drafts* e *Request for Comments*, con diffusione talvolta limitata ai gruppi di lavoro interessati) e l'adozione di decisioni sulla base della formazione di un "consenso approssimativo". La definizione di quest'ultimo e la descrizione del procedimento decisionale che caratterizza questo metodo sono contenuti nel breve saggio di RESNICK P., *On Consensus and Humming in the IETF*, in Internet Engineering Task Force (IETF), RFC n.7282 giugno 2004 (disponibile all'indirizzo https://tools.ietf.org/html/rfc7282, ultima visita 20 giugno 2017), esplicitamente richiamato, seppur in modo marginale, nei documenti che definiscono il processo decisionale che occorre seguire perché una modifica sia inserita nel protocollo Bitcoin.

[290] I BIP sono classificati in tre categorie a seconda del contenuto: (*i*) gli *Standard Track BIP* descrivono modifiche riguardano la maggior parte tutte le implementazioni dei bitcoin, come le modifiche al protocollo del network, modifiche alle regole che definiscono la validità di un blocco o di una transazione, o qualsiasi altra modifica che interessa l'interoperabilità delle applicazioni che riguardano i bitcoin; (*ii*) gli *Informational BIP* descrivono problemi relativi al design dei Bitcoin o forniscono *guidelines* generali o informazioni alla comunità bitcoin, ma non propongono nuove modifiche; (*iii*) i *Process BIP* descrivono processi connessi ai o propongono modifiche di tali processi, sono strutturalmente simili ai *Standard Track BIP*, ma non riguardano direttamente il protocollo bitcoin. V. BIP-002. Le regole per la proposizione di BIP cambiano a seconda del tipo di BIP che si intende proporre, v. BIP-123 "*BIP Classification*", in seguito "BIP-123", disponibile sul sito https://github.com/bitcoin/bips/blob/master/bip-0123.mediawiki#1_Consensus_Layer (ultima visita 20 giugno 2017).

apre quindi una seconda fase in cui l'autore si adopera per far convergere ed emergere il consenso e l'approvazione della comunità sulla sua proposta, eventualmente integrandola e motivandola di fronte alle critiche. Lo status del BIP passa da "bozza" a "attivo" quando la comunità raggiunge un «consenso approssimativo» valutato sulla base dei commenti pubblicati in risposta al BIP, cioè quando una proposta è discussa sulla mailing list e per un mese non ci sono stati commenti contrari. Il raggiungimento del consenso sui canali pubblici comporta, in teoria, l'inserimento delle modifiche discusse all'interno della successiva versione del software che diventeranno operative solo al momento dell'adozione dello stesso da parte dei nodi della rete[291]. In ragione della natura decentrata del sistema, ogni modifica al software richiede, infatti, un certo grado di partecipazione e cooperazione da parte degli utenti: non essendoci un organismo centrale che impone decisioni, perché la proposta diventi definitivamente operativa occorre, cioè, che la comunità Bitcoin si comporti in modo coeso e inizi ad usare il software modificato.

In linea teorica, modifiche attinenti il protocollo Bitcoin potrebbero essere implementate semplicemente con l'inserimento di nuove linee di codice all'interno della versione aggiornata del software e con il graduale aggiornamento dello stesso da parte dei nodi della rete. Nell'ipotesi di modifiche di scarso impatto che riguardano il protocollo questo è il modo con cui si procede, sicché, in buona sostanza, l'adozione del programma aggiornato da parte degli utenti *full nodes*, tra cui in particolare i *miner*, attua semplicemente la decisione assunta con il metodo del consenso approssimativo rendendola efficace.

Nel caso di modifiche più significative che incidono sul protocollo ed in particolare sulle *consensus rules*, la cui implementazione può portare a biforcazioni della *blockchain* [292], vige oggi invece una procedura più articolata. Le proposte di modifica che

---

[291] Con maggiore precisione può dirsi che il BIP è considerato "*final*", cioè la modifica è ritenuta implementata ed operativa, solo quando si verificano particolari condizioni nel mondo reale che variano a seconda del tipo di proposta: nel caso di *service BIP* occorre che il servizio sia adottato da almeno l'1% dei nodi per un mese; modifiche riguardanti API/ARC e applicativi legati ai Bitcoin devono essere adottate da almeno due programmi diversi indipendenti l'uno dall'altro; mentre per le modifiche significative del protocollo si segue l'iter descritto oltre nel testo. Circa i criteri che determinano la definitiva implementazione dei BIP v. il paragrafo "*Progression to final status*" del BIP-002; circa le categorie v. BIP-123.

[292] Il caso più significativo di *fork* sulla *blockchain* Bitcoin si è manifestato nel 2013 proprio a causa di un problema di compatibilità tra un aggiornamento del software e le versioni precedenti; v. BUTERIN V.,

interessano le regole di riconoscimento della validità dei blocchi si dividono in *soft fork* e *hard fork*. Le prime introducono modifiche che mantengono la compatibilità con il modello precedente, per cui se anche non tutti i nodi aggiornano il *software* resterà comunque una sola *blockchain* (la biforcazione sarà dunque a livello di *software* non di *blockchain*). Nel secondo caso, invece, la modifica comporta che i blocchi costruiti secondo le nuove regole non saranno riconosciuti dai nodi che non hanno aggiornato il *software*, con l'effetto di provocare una biforcazione permanente della catena (cioè una biforcazione della *blockchain* che non può essere risolta mediante il meccanismo dell'*emerging consensus*).

2.5.3. *Le modifiche ai criteri di validazione di transazioni e blocchi: la* soft fork *e il meccanismo di voto* version bits.

Le «*soft fork*»[293] concernono, dunque, le ipotesi in cui si intende introdurre una modifica la cui esecuzione è compatibile con versioni precedenti del software: "soft", quindi, nel senso che si verifica una divisione nella rete tra coloro che adottano il software aggiornato, e quindi applicano la nuova regola, e coloro che non lo fanno, ma tale divisione non comporta il rischio di duplicazione o scissione della *blockchain*. Per gestire

Bitcoin Network Shaken by Blockchain Fork, in *Bitcoin Magazine*, 12 Marzo 2013, disponibile sul sito https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/ (ultima visita 20 giugno 2017). L'episodio è menzionato anche in GRUBER S., *Trust, identity and disclosure: are bitcoin exchanges the next virtual havens for money laundering and tax evasion?*, in *Quinnipiac law review*, vol. 32, 2013, pp.163 ss..

[293] La definizione formale dell'ipotesi di *soft work* è formulate nei seguenti termini nel BIP-123 (cit.): "*In a soft fork, some structures that were valid under the old rules are no longer valid under the new rules. Structures that were invalid under the old rules continue to be invalid under the new rules*"; cioè una situazione in cui per effetto della modifica introdotta alcune strutture che erano valide ai sensi delle regole vigenti smettono di essere valide ai sensi delle nuove regole, mentre le strutture espressamente vietate continuano ad essere vietate (ciò che permette la compatibilità delle nuove regole con le regole precedenti). Un esempio concreto di *soft fork* è l'aggiunta di un certo tipo di informazioni all'interno di un blocco (v. per esempio la proposta contenuta nel BIP-034, "*Block v2, Height in Coinbase*", https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki, di aggiungere il valore dell'altezza del blocco all'interno della *coinbase transaction*). I nodi che eseguono la versione del software aggiornata producono blocchi inserendo tale nuovo valore, ma riconoscono come validi anche i blocchi senza tale dato, così come i nodi che non hanno eseguito l'aggiornamento riconoscono come validi ai sensi del vecchio software i blocchi che contengono tale dato, il cui inserimento non è incompatibile con le regole precedentemente vigenti. In questo modo c'è una differenziazione all'interno della rete tra chi ha aggiornato il software e chi non lo ha fatto, ma la *blockchain* resta unica, condivisa da entrambi i gruppi.

al meglio l'introduzione di tali modifiche il procedimento di modifica del protocollo è aggravato da un meccanismo di voto che condiziona l'esecutività della nuova regola all'approvazione da parte di una maggioranza qualificata di *miner* che esercitano il loro voto al momento dell'inclusione di un blocco da loro preparato nella *blockchain*[294]: qualora entro un certo lasso di tempo[295] il 75% dei nuovi blocchi aggiunti alla *blockchain* contenga un voto favorevole nei confronti dell'aggiornamento, la modifica è approvata e diventa operativa per tutti quelli che hanno aggiornato il programma; se, invece, tale soglia di approvazione non è raggiunta la modifica viene ignorata e il codice non muta[296].

---

294 La conta dei voti e l'applicazione delle modifiche secondo l'esito della votazione sono operazioni eseguite automaticamente dal software. Il primo tentativo di creazione di un meccanismo che regolasse ipotesi di *soft fork* è contenuto nel BIP-016, pubblicato da di Gavin Andresen il 3 gennaio 2012, https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki , nel quale si prevedeva che l'introduzione di un nuovo tipo di transazioni diventasse operativa solo a seguito di riscontro positivo in almeno 55% dei blocchi prodotti entro un certo lasso di tempo. La procedura è oggi formalizzata e regolata dal meccanismo del *version bits*, creato, tra gli altri, da Pieter Wuille e Gregory Maxwell, e introdotto nel sistema con il BIP-009, "*Version bits with timeout and delay*", del 4 ottobre 2015 (https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki, ultima visita 20 giugno 2017; sul punto v. anche la pagina esplicativa *Version bits FAQ for miners*, https://bitcoincore.org/en/2016/06/08/version-bits-miners-faq/, ultima visita 20 giugno 2017). Per procedere alla votazione si fissa una finestra temporale attraverso l'indicazione di una determinata serie di blocchi ad una certa altezza futura della catena: per esempio, si dice che saranno presi in considerazione i 1000 blocchi successivi al blocco n. 323.734. I *miner* che intendono pronunciarsi a favore della modifica scaricheranno la nuova versione del software e inseriranno, quindi, nei blocchi che riusciranno a creare un particolare codice numerico. Al termine del periodo prestabilito il software verifica automaticamente quanti blocchi contengono tale codice, calcola la percentuale di voti a favore e di voti contrari e trae le opportune conclusioni rendendo la modifica operativa ovvero inefficace secondo quanto previsto nel codice.

295 Per esempio al tempo della scrittura è in corso un processo di soft fork su segwit con una finestra temporale la cui chiusura è prevista a novembre 2017. V. https://github.com/bitcoin/bips/blob/master/bip-0009/assignments.mediawiki (ultima visita 20 giugno 2017); nonché https://blockchain.info/charts/bip-9-segwit (ultima visita 20 giugno 2017).

296 I quorum deliberativi non sono fissati in modo univoco e possono variare in funzione di quanto deciso nel singolo BIP, le percentuali indicate nel testo sono però quelle emerse nella prassi dal confronto tra i più importanti programmatori che partecipano al processo di costante aggiornamento del programma e sono, quindi, dotate di una certa autorevolezza: v., in particolare, la discussione tra Gavin Andresen, Gregory Maxwell e Luke Dashjr, attuale moderatore dei BIP, sull'introduzione del meccanismo nel BIP-034, https://github.com/bitcoin/bitcoin/pull/1526 (ultima visita 20 giugno 2017). Cfr. anche il BIP-002, in cui si suggerisce, anche alla luce della sempre maggiore aggregazione dei *miner* in *pools*, di fissare la soglia per l'approvazione della modifica non al di sotto del 95%, salvo particolari esigenze specifiche (v. BIP-002, cit.).

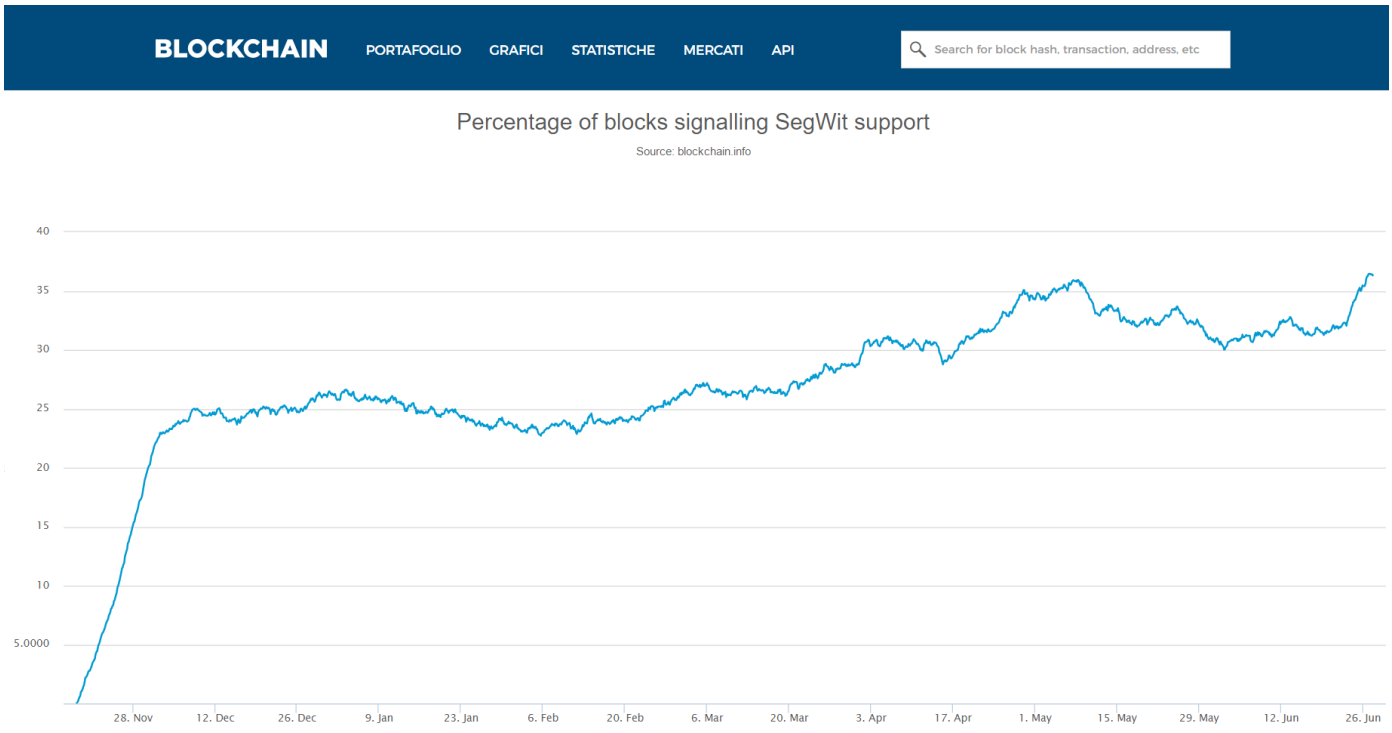


Fig. 2, percentuale di blocchi che esprimono voto favorevole per la *soft fork* SegWit[297]

Questo meccanismo di voto, denominato «*version bits*» perché l'indicazione di voto è espressa tramite un riferimento contenuto nei bit che descrivono la versione del blocco in uso, si completa con un ulteriore regola che riguarda l'abrogazione delle regole contenute nella precedente versione del protocollo potenzialmente incompatibili con la nuova disciplina. Per mantenere la compatibilità tra le due versioni, le regole sono introdotte in modo che i blocchi prodotti secondo quanto stabilito dal software prima della modifica siano riconosciuti come blocchi validi anche da chi ha effettuato l'aggiornamento, quando però tutta la rete si è allineata alla volontà tacitamente espressa dalla maggioranza, si ritiene che sia possibile rendere obbligatoria l'applicazione dei nuovi standard. In questo caso il quorum deliberativo è fissato al 95% e la verifica del raggiungimento di tale soglia è effettuata in modo costante prendendo a riferimento un certo numero di blocchi partendo dall'ultimo aggiunto in ordine temporale. Quando tale soglia di adozione della nuova versione del *software* è raggiunta, il protocollo modifica

297 Fonte: https://blockchain.info/it/charts/bip-9-segwit (27 giugno 2017)

automaticamente le proprie regole di validità e inizia a rifiutare i blocchi prodotti secondo le regole stabilite dalla versione precedente, che diventano quindi blocchi "orfani", cioè esclusi dalla *blockchain*, Rendendo, di fatto, obbligatorio per tutti l'aggiornamento e l'adozione delle nuove regole. A questo punto la condizione di *soft fork* è superata perché la rete torna ad utilizzare un unico set di regole uguali per tutti.

Il "voto" che determina l'approvazione di un BIP nella procedura *version bits* è espresso attraverso l'indicazione di un particolare codice all'interno dei nuovi blocchi. Poiché la quantità di nuovi blocchi che ciascun *miner* è in grado di produrre dipende dalla potenza di calcolo di cui dispone, questo significa che il voto è ponderato in base alla contribuzione in termini di potenza di calcolo al sistema e che quindi i *miner* e i *pool di miner* più forti hanno maggiore influenza sull'implementazione di tali decisioni[298]. Inoltre, questo implica che solo i *miner* hanno diritto di voto nel sistema.

2.5.4. *La* hard fork *e la creazione di Bitcoin Unlimited*

Diverso dal caso di modifiche suscettibili di produrre *soft fork* è l'ipotesi di modifiche al protocollo per effetto delle quali strutture che prima non erano valide diventano valide. In questo caso i blocchi prodotti da chi ha aggiornato il *software* secondo le nuove regole non sarebbero riconosciuti come blocchi validi da chiunque esegua ancora la precedente versione, con l'effetto, nel caso in cui non tutti aggiornino il *software*, di scindere la *blockchain* tra i due gruppi: da qui la definizione di *hard fork*. Questa categoria comprende le modifiche potenzialmente più significative e stravolgenti, tra cui l'ipotesi – mai realmente discussa all'interno della comunità Bitcoin – di rimozione del limite del numero massimo di bitcoin che potranno mai essere prodotti, o la scelta di modificare il meccanismo della *proof of work* oggi in uso, da taluni considerata l'*extrema*

[298] La capacità dei *pool* di *miner* di aggregare potenza di calcolo è variata grandemente nel corso del tempo, arrivando a concentrare enormi percentuali in capo a pochi pools. Col tempo il panorama si è frammentato, ma la tendenza a concentrare la capacità di calcolo in grandi gruppi resta piuttosto alta: i primi tre *pool* aggregano il 40% circa della potenza di calcolo, mentre se si considerano i primi 10 gruppi allora la percentuale aggregata supera l'80% della potenza totale della rete (calcoli svolti sulla base dei blocchi prodotti tra il 17 e il 21 febbraio 2017, fonte: https://*blockchain*.info/pools?timespan=4days, 21 febbraio 2017).

ratio che potrebbe permettere alla comunità Bitcoin di reagire ad un abuso di potere da parte dei *miner* rimettendo in discussione la loro influenza.

Indipendentemente dal contenuto della proposta, l'ipotesi di introduzione di una *hard fork* ha un impatto notevole sul sistema per il solo rischio di scissione della *blockchain* che esso comporta: mettere in discussione l'unità della catena equivale sostanzialmente a creare una nuova valuta alternativa rispetto al modello esistente in quel momento. Inoltre, un'eventuale scissione comporterebbe enormi problemi in termini di quale delle due catene risultanti dovrebbe essere ritenuta valida. Nella vita del protocollo *Bitcoin* è accaduto solo una volta che un aggiornamento abbia coinciso con un'ipotesi di *hard fork*: si è trattato di una modifica che interessava un protocollo di comunicazione tra i nodi che non poteva essere implementata in altro modo. Per evitare problemi, l'attivazione del nuovo codice inserito nell'aggiornamento è stata pianificata a distanza di due anni dalla pubblicazione della nuova versione del software, cosicché tutti i nodi avessero tempo di effettuare l'aggiornamento[299].

Negli ultimi anni le proposte di *hard fork* che hanno suscitato interesse ed attenzione nella comunità Bitcoin hanno riguardato il complesso tema della dimensione massima dei blocchi, su cui la comunità Bitcoin è molto frammentata. Sul punto sono state formulate nove diverse proposte di BIP[300], molti esponenti dell'industria si sono espressi a favore della rimozione del limite di 1Mb inserito da Satoshi Nakamoto nel 2010, ma non si è ancora giunti all'inserimento di una modifica all'interno del client.

---

[299] V. annuncio *February 20, 2012 Protocol Changes*, pubblicato in https://bitcoin.org/en/alert/2012-02-18-protocol-change (ultima visita 20 giugno 2017).

[300] BIP-101, "Increase maximum block size", di Gavin Andresen (poi ritirata), https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki (ultima visita 20 giugno 2017); BIP-102, "Block size increase to 2MB", di Jeff Garzik, https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki (ultima visita 20 giugno 2017); BIP-103, "Block size following technological growth", di Pieter Wuille, https://github.com/bitcoin/bips/blob/master/bip-0103.mediawiki (ultima visita 20 giugno 2017); BIP-105, "Consensus based block size retargeting algorithm", di BtcDrak, https://github.com/bitcoin/bips/blob/master/bip-0105.mediawiki (ultima visita 20 giugno 2017); BIP-106, "Dynamically Controlled Bitcoin Block Size Max Cap", di Upal Chakraborty, https://github.com/bitcoin/bips/blob/master/bip-0106.mediawiki (ultima visita 20 giugno 2017); BIP-107, "Dynamic limit on the block size", di Washington Y. Sanchez, https://github.com/bitcoin/bips/blob/master/bip-0107.mediawiki (ultima visita 20 giugno 2017); BIP-109, "Two million byte size limit with sigop and sig*hash* limits", Gavin Andresen, https://github.com/bitcoin/bips/blob/master/bip-0109.mediawiki (ultima visita 20 giugno 2017).

L'*impasse* generatosi ha spinto alcuni programmatori a sviluppare dei software alternativi alla versione "ufficiale" del client in risposta all'immobilismo del client ufficiale riguardo alla questione del limite alla dimensione dei blocchi: (*i*) il *client* Bitcoin XT, ideato da Gavin Andresen, storico manutentore di Bitocin Core, e Mike Heam, molto diffuso nel 2016 ma già in disuso agli inizi del 2017; (*ii*) il *client* Bitcoin Unlimited[301]; e il *client* Bitcoin Classic[302].

Il dibattito che ha accompagnato l'introduzione di queste proposte concorrenti al *software* tradizionale è stato a tratti molto duro e polemico con accuse di censura organizzata sui forum di riferimento e di collusione con interessi di alcune società private rivolte al gruppo di programmatori che gestiscono i processi di aggiornamento del *software* originariamente lanciato da Satoshi Nakamoto[303]. Il punto della questione è che la comunità è divisa tra chi ritiene che si debba superare il limite di grandezza del singolo blocco oggi fissato a 1 Mb, chi si oppone a tale modifica e chi ignora il problema. La proposizione di nuovi software quali i *client* Bitcoin Unlimited e Bitcoin Classic sono stati un modo di permettere ai *miner* di 'votare' in merito alla questione mediante l'utilizzo del *software* alternativo rispetto al tradizionale *bitconi core*. La diffusione di questi *client* alternativi, che corrisponde ad un voto di protesta e disaccordo nei confronti dei gestori del *client* ufficiale, ha raggiunto proporzioni vicine al 40% del potere di calcolo della rete.

Tutto ciò è indicativo del fatto che il protocollo è soggetto a pressioni da parte di gruppi di interesse diversi circa la necessità o l'opportunità di introdurre modifiche e che non si può in astratto escludere che tali tensioni possano in futuro sfociare nell'introduzione in una *hard fork* da parte di un gruppo dominante. Si noti, inoltre, che anche in questo contesto la definizione delle regole del sistema può avere effetti distributivi. L'esempio della dimensione del blocco è, in questo senso, indicativa: il limite

---

301 Oggi è utilizzato da circa il 20% dei nodi (POTENZA DI CALCOLO) della rete, fonte http://xtnodes.com/ (ultima visita 22 febbraio 2017), dato calcolato sui blocchi prodotti nella settimana dal 15 al 21 febbraio 2017.

302 V. sito https://bitcoinclassic.com/ (ultima visita 20 giugno 2017).

303 Cfr. per tutti, i due *public service announcement* pubblicati sul sito http://xtnodes.com/ (ultima visita 20 giugno 2017), e cfr. https://en.bitcoin.it/wiki/Block_size_limit_controversy (ultima visita 20 giugno 2017).

alla dimensione massima incentiva gli utenti ad accettare di corrispondere ai *miners fees* più alte per non dover aspettare molto tempo prima di vedere la transazione validata, mentre con blocchi più grandi potrebbe essere possibile processare un numero maggiore di transazioni per blocco[304].

Fig. 3, percentuale di blocchi che segnalano supporto per *Bitcoin Unlimited* [305]

Nelle more della scrittura della tesi, il tema della misura dei blocchi si è sviluppato in modo inedito. Dopo anni di dibattito in rete, il 23 maggio 2017 un gruppo di 58 società coinvolte nell'economia bitcoin, che insieme rappresentano più dell'80% del potere di calcolo dell'intera rete ha raggiunto un'intesa, chiamata "*New York Agreement*", e hanno

304 v. https://bitcointalk.org/index.php?topic=1347.msg17804#msg17804 (ultima visita 20 giugno 2017).

305 Fonte: https://blockchain.info/it/charts/bitcoin-unlimited-share (27 giugno 2017)

dichiarato di impegnarsi per l'attivazione di una *hard fork* entro il termine di sei mesi che incrementi la dimensione massima di ciascun blocco da 1 a 2 Mb[306].

[306] V. dichiarazione: *Bitcoin Scaling Agreement at Consensus 2017*, del 23 maggio 2017 disponibile sul sito: https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77 (ultima visita 20 giugno 2017).

Capitolo III

Il «sistema monetario» bitcoin

1. I bitcoin come sistema monetario

1.1. La creazione del sistema monetario bitcoin

Nel corso del precedente capitolo si è provata a ricostruire la genealogia dei bitcoin tracciandone le origini nella visione politica anarco–liberarle del movimento *cypherpunk*, il quale si proponeva di rivoluzionare l'ordinamento sociale attraverso l'uso crittografia[307]. All'interno di questo movimento era emersa l'esigenza di sviluppare un sistema di pagamento digitale che permettesse ad individui connessi ad una rete informatica di concludere scambi in modo anonimo. Dopo alcuni primi tentativi, nel 2008 qualcuno, sotto lo pseudonimo di Satoshi Nakamoto, inventa un nuovo sistema di pagamento basato su un libro giornale condiviso tra gli utenti di una rete gestito dalla rete stessa in modo pienamente autonomo, decentrato e distribuito. Nei documenti ufficiali che presentano il progetto bitcoin non si fa alcuna menzione del progetto politico crittoanarchico e della esigenza di garantire una moneta alla nuova società critto-anarco-liberale e non si intende qui implicare che Satoshi Nakamoto perseguisse gli obbiettivi rivoluzionari della frangia più estrema del movimento *cypehrpunk*. I documenti citati nel *white paper*[308] e le soluzioni adottate nel modello, però, lasciano intendere una certa consonanza di interessi e obbiettivi con coloro che, nella traccia aperta dal movimento crittoanarchico, hanno provato a creare o ad immaginare sistemi di pagamento o monete digitali negli anni precedenti. In particolare, è significativo il fatto che anche il progetto

[307] Cfr. FRISBY, op. cit., capitolo 2.

[308] NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit., p. 9.

bitcoin si proponga di creare un mezzo di pagamento che possa essere usato universalmente indipendentemente da qualsiasi garanzia o sostegno da parte di uno Stato, nonché il fatto che i bitcoin siano strutturati secondo il modello di moneta teorizzato dalla scuola catallattica: come beni scarsi che diventano preziosi in ragione della loro scarsità e dell'uso che se ne fa come mezzi di scambio. Nel contesto del progetto *cypherpunk* il ricorso a questa concezione della moneta è ricollegabile sia alla matrice liberale che caratterizza il pensiero economico dei crittoanarchici, sia alla carenza di alternative possibili, posto che il rifiuto di qualsiasi rapporto con lo Stato rende impossibile l'imposizione centrale di una moneta fiduciaria sorretta, vuoi fiscalmente dalla spesa pubblica e dalla tassazione, vuoi dall'imposizione di norme giuridiche sotto la minaccia dell'esercizio della violenza. Il progetto bitcoin eredita e condivide questa impostazione di fondo. In questo contesto, il rifiuto della moneta statale è giustificato in ragione della sfiducia nei confronti del sistema finanziario ed in nome della riduzione dei costi di agenzia connessi alla presenza di intermediari e di un ente centrale in grado di garantire, ma anche di influenzare, il funzionamento del sistema[309]. Da una critica esplicitamente radicale e politica si passa, in concreto, ad una critica esternata in linguaggio economico e dai toni più morbidi, che dietro la facciata mantiene, però, una componente 'anti-sistema' molto forte. Il *fil rouge* che collega queste due visioni, che si è provato ad evidenziare nella ricostruzione di una genealogia del progetto bitcoin, è l'obbiettivo concreto di creare un sistema informatico decentrato che assicuri in modo certo il trasferimento di beni digitali nel rispetto della privacy degli individui, in aperta contrapposizione a qualsiasi centralizzazione e controllo esterno.

Inizialmente, dunque, la pretesa di autonomia del sistema, intesa nel senso più strettamente etimologico del termine, come indipendenza del sistema da qualsiasi norma giuridica esterna, è conseguenza diretta del rifiuto politico dei *cypherpunk* di qualsiasi autorità centrale che eserciti un monopolio della violenza. Nei bitcoin essa è presentata in stretta connessione alla decentralizzazione e al coinvolgimento diretto dei partecipanti nella gestione del sistema monetario bitcoin, contraltare del rifiuto di attribuire

[309] V. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit., p. 1.

competenze e responsabilità ad enti centrali o intermediari di sorta[310]. Il percorso che porta, senza una chiara soluzione di continuità, dai *cypherpunk* ai bitcoin è segnato dalle sfide che via via si sono poste nell'elaborazione concreta di un modello informatico che concretizzasse l'obbiettivo posto.

Durante questo percorso ci si è chiesti come fosse possibile assicurare l'anonimato delle persone, come si potessero gestire gli scambi e come eventualmente gestire la produzione dei beni digitali che sarebbero stati scambiati. Sono state progressivamente elaborate risposte a questi problemi: l'utilizzo della crittografia a doppia chiave per creare vincoli univoci su beni digitali che non richiedessero la manifestazione della propria identità; la concettualizzazione dello scambio come registrazione di una partita contabile su un registro collettivo; e l'utilizzo delle funzioni di *proof of work* per regolare la creazione della moneta digitale.

L'introduzione della tecnologia *blockchain* ha permesso di risolvere l'ultimo problema rimasto aperto: la decentralizzazione del registro. Si è così potuto creare un sistema di gestione di risorse rappresentative di una nuova unità di conto ideale completamente avulso dal contesto istituzionale statale: un sistema monetario interamente basato su un protocollo informatico.

1.2. Oggetto del sistema: cosa sono 'i bitcoin'?

Oggetto di questo sistema è, dunque, *in primis*, la creazione e la distribuzione di nuovi bitcoin, e, *in secundis,* la gestione dei trasferimenti di bitcoin tra soggetti diversi. Questo risultato è raggiunto attraverso la creazione di un registro di transazioni nel quale sono riportate: (*i*) le '*coinbase transaction*' cioè delle transazioni fittizie che creano nuovi bitcoin e li attribuiscono al *miner* che ha compilato il blocco; e (*ii*) le transazioni che

[310] Si è visto, in realtà, che anche nel contesto dei bitcoin si sviluppano figure professionali che svolgono il ruolo di intermediari finanziari, ciò non toglie, tuttavia, che il sistema sia congegnato per funzionare anche senza l'ausilio di tali soggetti, allorché nel paradigma monetario del *fractional reserve banking* la presenza di banche è quintessenziale al funzionamento del modello. La differenza cruciale risiede nel fatto che nel sistema monetario tradizionale le banche svolgono un duplice ruolo di intermediarie nel sistema di pagamenti e creatrici di nuova liquidità. Nel contesto dei bitcoin l'intermediazione di gestori di *wallet* non è indispensabile, mentre il lavoro dei *miners* è predeterminato dal protocollo, sicché ad essi non è formalmente delegato alcun potere decisionale (salvo il caso estremo della modifica del protocollo stesso).

rappresentano il trasferimento di bitcoin tra utenti. Queste ultime consistono in ordini impartiti al sistema di sbloccare dei fondi registrati a nome dal dante causa in favore del ricevente. Più specificatamente, il trasferimento di bitcoin concerne l'ordine di 'spendere' i bitcoin ricevuti ad un certo indirizzo per effetto di una precedente operazione di trasferimento registrando tali somme a favore di altri indirizzi. L'utilizzo di chiavi crittografiche private associate agli indirizzi su cui sono registrati i bitcoin permette di attribuire univocamente ad un soggetto la titolarità della prerogativa di impartire l'ordine di pagamento: ciò consente, sia di verificare la provenienza e l'autenticità dell'ordine, sia di individuare pagatore e ricevente senza che sia necessario svelare la vera identità dei due (o più) soggetti che partecipano alla transazione; fermo restando che chiunque può trasmettere validamente un ordine di trasferimento di bitcoin purché sia in possesso della chiave segreta associata all'indirizzo a cui sono stati originariamente trasferiti. Tutto ciò chiarito ci si può chiedere, allora, cosa siano esattamente i bitcoin: cosa è, esattamente, che viene trasmesso da un soggetto all'altro in occasione di un trasferimento di bitcoin?

Ebbene, ora che si ha maggiore contezza di come funzioni esattamente il sistema, si comprende che la domanda "cos'è un bitcoin?" non è così semplice come appare a prima vista. Un primo tentativo intuitivo di risposta consiste nel dire che si trasferiscono dei beni digitali[311]. Nel linguaggio comune si parla infatti di bitcoin come di cose che possono essere trasferite tra le persone secondo una logica proprietaria riconducibile allo schema dei diritti reali: una perfetta trasposizione di beni materiali, in particolare di beni preziosi, quali l'oro, in ambito digitale.

La risposta non è convincente perché semplifica eccessivamente il fenomeno: i bitcoin, infatti, non solo non sono beni materiali, ma non sono nemmeno identificabili come documenti digitali separati dal registro contabile[312].

Dal punto di vista delle informazioni registrate su supporti digitali, non vi sono documenti informatici a sé stanti che possono essere chiamati 'bitcoin', ma al più registrazioni di transazioni per effetto delle quali un certo numero di bitcoin è associato ad un indirizzo pubblico, contenute dentro blocchi di informazioni concatenati nella

311 Cfr. MANCINI M., *Valute virtuali*, cit., p. 126.

312 GUTTMANN, op. cit., p. 24.

blockchain, e chiavi private che permettono di smobilitare tali fondi mediante la trasmissione di un ordine alla rete. I bitcoin trasferiti tra gli utenti possono essere catalogati come 'beni digitali' solo nell'accezione di *scarse objects*[313]: informazioni registrate su supporti digitali caratterizzate dagli attributi di finitezza e rivalità. I bitcoin sono solo valori numerici la cui titolarità è attribuita, all'interno del registro condiviso, ad un determinato soggetto rappresentato da una chiave pubblica.

La discrasia tra la narrativa comune, che immagina i bitcoin come dei beni materiali 'digitalizzati' e il reale funzionamento del sistema è frutto di una semplificazione terminologica ed intellettuale del sistema, che riporta lo schema del mezzo di pagamento astratto la cui finitezza è gestita da un sistema entro termini che sono propri del mezzo di pagamento concreto: dalla logica dei beni immateriali alla logica e al lessico tipico dell'esercizio del diritto di proprietà privata su beni corporali, in cui un soggetto esercita il dominio su un bene e nell'esercizio di tale dominio può decidere di trasferirne il possesso (e la proprietà) ad altrui. Tale semplificazione è figlia dell'applicazione in ambito digitale di un modello monetario che concepisce la moneta come un bene scarso, cui, in ragione della sua scarsità, è riconosciuto un valore particolare[314]. Essa è utile nella misura in cui si vogliano spiegare in modo semplice e intuitivo alcune potenzialità del sistema e qualora si voglia evidenziare un parallelismo tra la scarsità dei beni materiali e la scarsità (indotta, perché dipende dalle regole del sistema) dei bitcoin (o di altri 'beni digitali' costruiti secondo il modello teorico degli *scarse object*), ma è riduttiva e nasconde la ben più complessa struttura dello schema.

Il sistema bitcoin è concepito e raccontato nella vulgata comune come una replica digitale di beni materiali distribuiti secondo una logica di proprietà privata, tuttavia, in realtà i beni digitali finiti e rivali creati all'interno del protocollo non sono altro che valori numerici e la 'proprietà' di tali beni corrisponde esclusivamente all'aspettativa di poter modificare il registro comune in favore di un altro utilizzatore: 'possedere' un bitcoin tecnicamente significa, cioè, vedersi attribuita dal sistema la facoltà di richiedere una modifica del registro che determini una diversa allocazione di quel bitcoin (attraverso l'attribuzione al ricevente della facoltà di richiedere, a sua volta, un successivo

313 V. SZABO, *Scarce Objects*, cit..

314 *Ivi*.

trasferimento); 'spendere' un bitcoin significa esercitare tale facoltà, trasmettendola ad altrui.

I bitcoin non sono, quindi, un bene digitale solo nei termini sopra descritti: ciascun bitcoin o frazione di esso rappresenta unicamente una certa quantità dell'unità astratta attribuita dal protocollo Bitcoin all'utente, trasferibile ad altri partecipanti solo attraverso il protocollo stesso.

Per rispondere alla domanda "cosa è un bitcoin" senza incorrere in forti semplificazioni non è sufficiente fare riferimento unicamente ai concetti di proprietà e di bene, ma occorre, invece, calarsi all'interno delle regole del protocollo immaginando lo stesso come un sistema giuridico autonomo in grado di attribuire il controllo esclusivo sopra certe risorse immateriali[315]. Sotto questo profilo, l'uso della nozione di sistema monetario permette di evidenziare ad un tempo, sia il fatto che i bitcoin sono suscettibili di appropriazione e possono essere scambiati tra gli utenti, sia l'importanza ed le funzioni delle regole e della struttura istituzionale che permette tali scambi. Da questo punto di vista è quindi possibile rispondere alla domanda che ci si è posti concludendo che i bitcoin che vengono scambiati tra gli utenti sono un mezzo di pagamento astratto che permette la rappresentazione contabile dell'unità di conto 'bitcoin' e che la peculiarità della loro natura si spiega nel contesto del sistema monetario in cui sono inseriti.

Elemento caratterizzante che distingue il sistema bitcoin da ogni altro sistema monetario è la scelta di regolare tale sistema attraverso l'implementazione di funzioni matematiche crittografiche all'interno di un software, le cui caratteristiche permettono di affidare la gestione di un registro condiviso ad un gruppo indeterminato di computer connessi in rete senza la supervisione di un ente centrale. Per la prima volta nella storia, quindi, grazie alla tecnologia *blockchain*, un software, cioè un insieme di regole codificate in un protocollo informatico, assume il ruolo tradizionalmente svolto dalle regole sociali

315 Sulla nozione di sistema giuridico v. SACCO R. e ROSSI P., *Introduzione al diritto comparato*, in "Trattato di Diritto Comparato", diretto da R. Sacco, UTET, 2015, pp. 165 ss.. Uno dei numerosi ambiti in cui la ricerca sui bitcoin può essere approfondita consiste proprio nel chiedersi se e in che misura, in considerazione della pretesa autonomia rispetto al diritto statale e della particolare estensione geografica potenzialmente illimitata, il protocollo e/o l'intero sistema monetario bitcoin possano essere descritti come un sistema giuridico. Sulla descrizione del codice informatico in termini giuridici v. LESSIG, op. cit., e BROWNSWORD R. e YEUNG K. (a cura di), *Regulating technologies*, Hart Publishing, 2008.

e giuridiche di determinare ed influenzare il comportamento degli agenti secondo un modello predeterminato. La trasformazione in atto è resa ancora più significativa dal fatto che l'esecuzione del software sia affidata ad un numero variabile di computer, che non occorre identificare o autorizzare: chiunque, cioè, può partecipare alla gestione del registro pubblico condiviso assumendo la funzione di *miner*, semplicemente connettendosi alla rete ed eseguendo il software. Le regole del protocollo regolano altresì la registrazione dei valori contabili sul registro collettivo e permettono, quindi, che la creazione e il trasferimento di bitcoin siano gestiti direttamente dalla rete di computer, senza la presenza di una controparte centrale e di un ente regolatore[316].

I bitcoin si distinguono, quindi, da ogni altra forma di moneta[317]. Essi si distinguono dalla moneta merce – con la quale pure condividono alcune caratteristiche, quali la finitezza e la scarsità (pur se artificialmente costruita e quindi tecnicamente sempre revocabile) che sono determinanti per l'attribuzione di valore (su cui *infra*) – perché non sono una merce materiale cui è riconosciuto un valore monetario: i bitcoin sono *ab origine* mezzi di pagamento astratti dematerializzati. Si distinguono dalla moneta scritturale e dalla moneta elettronica, perché non sono un credito verso una banca o un altro emittente. Non sono, certo, banconote, né *fiat money* perché non hanno corso legale e non sono base monetaria perché non corrispondono ad una riserva presso la banca centrale. Essi sono la diretta rappresentazione dell'unità di conto 'bitcoin', specifica al sistema monetario bitcoin e in questo sembrano l'espressione di una forma monetaria "pura", in cui v'è perfetta corrispondenza tra l'unità di conto e il mezzo di pagamento[318].

Le unità di bitcoin trasferite tra gli utenti, cioè i bitcoin 'mezzi di pagamento', sono, quindi, nient'altro che un valore numerico memorizzato su supporti digitali

316 Si noti, però, che la gestione, per la prima volta, non è affidata ad un terzo, bensì è autogestita dal sistema secondo un complesso bilanciamento di crittografia, teoria dei giochi e teoria delle reti. Per una descrizione del protocollo bitcoin nell'ottica di questi tre elementi, v. ALI R., BARRDEAR J., CLEWS R. e SOUTHGATE J., *Innovations in payment technologies*, op. cit., *passim*.

317 Cfr. *ibidem*, p. 263, dove si ricorda che il sistema tradizionale di gestione di mezzi di pagamento astratti basati sulla moneta scritturale è rimasto strutturalmente invariato per secoli, dal XVI secolo, essendo cambiate solo le modalità attraverso cui sono registrati i crediti nei confronti delle banche e come le banche a loro volta eseguano e compensino tra loro gli ordini di pagamento; mentre il sistema bitcoin presenta per converso caratteristiche peculiari innovative (che gli autori non escludono possano essere riutilizzate nel contesto del sistema monetario statale).

318 Cfr. AMATO e FANTACCI, op. cit., p. 131.

disciplinato da un particolare sistema informatico, basato sulla tecnologia *blockchain*, che ne assicura la rivalità e la finitezza e che ne permette l'associazione con chiavi pubbliche che ne determinano la proprietà; con l'ulteriore specificazione che la *blockchain* è caratterizzata dall'essere un registro condiviso aggiornato da una rete composta da un numero variabile di computer che collaborano secondo le regole imposte dal protocollo bitcoin partecipando ad una competizione continua inerente la continuazione (e, quindi, l'aggiornamento) del registro stesso.

2. I primi tentativi di classificazione giuridica dei bitcoin

Le peculiarità di questo sistema monetario, sopra descritte, ne hanno reso molto difficile la classificazione entro le categorie giuridiche esistenti[319]: la dottrina che si è adoperata in questo sforzo ha potuto evidenziare, per lo più, le differenze tra i bitcoin e i modelli esistenti, senza pervenire a conclusioni dirimenti circa la loro natura e le regole che vi si dovrebbero applicare[320]. La Banca Centrale Europea, a fronte di questa problematicità, ha sviluppato una nuova nozione con la quale ha inteso descrivere modalità innovative di rappresentazione di valore con mezzi digitali ed ha così elaborato la categoria delle "valute virtuali", rivedendone la definizione nel corso del tempo. Nei successivi paragrafi si cercherà di completare l'analisi teorica sin qui proposta illustrando succintamente: i riferimenti legislativi dai quali si deduce che i bitcoin si distinguono giuridicamente dalla moneta statale e da altre categorie in uso nel diritto monetario e finanziario oggi vigente; quali sono gli elementi essenziali della nozione di «valuta virtuale» proposta dalla BCE; e qual è stato l'orientamento della Corte di Giustizia in un caso concernente l'applicazione dell'IVA a operazioni di cambio di bitcoin in moneta statale.

2.1. La valuta avente corso legale ai sensi del diritto dell'Unione Europea

È evidente, per tutto quanto si è detto sinora, che i bitcoin non sono, innanzitutto, una valuta avente corso legale nell'Unione Europea. A mente dell'art. 3, par. 4 del Trattato sull'Unione Europea, "*l'Unione istituisce un'unione economica e monetaria la cui moneta* ["*currency*" nel testo in lingua inglese; "*monnaie*" nella versione francese] *è*

---

319 v. GASPARRI, op. cit.; MANCINI M., op. cit.,; VARDI, op. cit.; AMENTA, op. cit.; ARANGÜENA, op. cit.; BERTARINI, op. cit.; e v. anche GRINBERG, op. cit.; KAPLANOV, op. cit.; KIEN M. e MENG L., op. cit.; TURPIN, op. cit.; BAYERN S., *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, in *Walsh. & Lee L. Rev. Online*, vol. 71, 2014, p. 22. Cfr. anche BRITO J., SHADAB H.B. e CASTILLO A., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling* (August 10, 2014), disponibile all'indirizzo http://ssrn.com/abstract=2423461 (ultima visita 20 giugno 2017).

320 Cfr., per tutti, GASPARRI, op. cit., p. 416, dove i bitcoin vengono provocatoriamente definiti un "UFO giuridico" (virgolettato nell'originale): "*tale «UFO giuridico» sembra, a prima vista, possedere caratteristiche così originali e innovative da sfuggire a un preciso inquadramento tra le numerose categorie dogmatiche che strutturano l'attuale sistema bancario e finanziario*".

l'euro". L'art. 2 del Regolamento (CE) n. 974/98 relativo all'introduzione dell'euro[321] stabilisce, più specificatamente, che "*A decorrere dal 1° gennaio 1999, la moneta* ["*currency*" nella versione in lingua inglese; "*monnaie*" nella versione francese] *degli Stati membri partecipanti è l'euro. L'unità monetaria è un euro. Un euro è diviso in cento cent*". Ne consegue che la moneta avente corso legale e, quindi, capacità solutoria delle obbligazioni pecuniarie *ex lege*, in Italia è l'euro. In particolare, il corso legale è riconosciuto solo alle banconote emesse dalla Banca Centrale Europea o per sua autorizzazione. L'art. 128 (*ex* art. 106 del TCE) del Trattato sul funzionamento dell'Unione Europea, inerente i compiti della Banca Centrale Europea, chiarisce, infatti, che a tale istituzione è conferito "*il diritto esclusivo di autorizzare l'emissione di banconote in euro all'interno dell'Unione*" e che le banconote così emesse "*costituiscono le uniche banconote aventi corso legale* ["*the status of legal tender*" nella versione inglese; "*cours légal*" nella versione francese] *nell'Unione*"[322].

2.2. Moneta elettronica e bitcoin

Sotto il profilo della disciplina dei pagamenti, alle banconote sono equiparate la moneta scritturale e la moneta elettronica[323].

I bitcoin non rientrano certamente nella prima categoria, giacché non sono crediti immediatamente esigibili che i consociati vantano nei confronti di enti creditizi autorizzati alla raccolta del risparmio[324]. Quanto alla nozione di moneta elettronica essa

---

321 Regolamento del Consiglio, del 3 maggio 1998, relativo all'introduzione dell'euro (GU L 139 dell'11.5.1998, pag. 1).

322 Cfr. anche l'art. 119, par. 2, del Trattato sul funzionamento dell'Unione Europea fa riferimento a "*una moneta unica, l'euro* ["*une monnaie unique*" nella versione francese del testo; "*a single currency*" nella versione inglese]". Cfr., inoltre, la definizione di «valuta» di cui all'art. 2, lett. a), *Direttiva 2014/62/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, sulla protezione mediante il diritto penale dell'euro e di altre monete contro la falsificazione e che sostituisce la decisione quadro 2000/383/GAI del Consiglio (GU L 151 del 21.5.2014, pag. 1)*, a mente del quale sono "*«valuta» le banconote e le monete metalliche la cui circolazione sia legalmente autorizzata, comprese le banconote e le monete metalliche la cui immissione in circolazione è legalmente autorizzata ai sensi del regolamento (CE) n. 974/98*".

323 V. art. 4 della Direttiva 2007/64/CE, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, cit..

324 v. paragrafo 12.10 del parere della BCE del 26 aprile 2006 riguardo ad una proposta di direttiva relativa ai servizi di pagamento nel mercato interno (BCE/2006/21)(2006/C 109/05). V. FARENGA, *op. cit.*.

offre maggiori punti di somiglianza con i bitcoin: neppure in questo caso, però, la disciplina risulta applicabile.

La moneta elettronica è una categoria elaborata dal diritto dell'Unione per permettere la creazione di mezzi di pagamento digitali che permettano agli utenti un più agevole uso dei propri fondi attraverso internet o altri canali di comunicazione[325]. Essa concerne "*tutte le situazioni nelle quali il prestatore di servizi di pagamento emetta un valore prepagato memorizzato in cambio di fondi, che può essere utilizzato come strumento di pagamento poiché è accettato da terzi come pagamento*"[326]. La disciplina è strutturata secondo il modello dell'intermediazione di un soggetto terzo rispetto all'operazione di pagamento con il quale entrambi il pagatore e il ricevente intrattengono un rapporto contrattuale e che si rende garante del valore della moneta elettronica utilizzata nello scambio. Lo schema prevede, quindi, la costituzione di un 'istituto di moneta elettronica', con capitale minimo di 350.000 euro e soggetto ad autorizzazione e a vigilanza[327], che può emettere "*moneta elettronica al valore nominale dietro il ricevimento di fondi*"[328] e che garantisce in ogni tempo la convertibilità della moneta elettronica emessa[329].

---

325 v. scheda di sintesi "*Moneta elettronica: attività e vigilanza prudenziale*" della Commissione Europea (http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:mi0042&rid=1, ultima visita 20 giugno 2017). La moneta elettronica è stata introdotta con La Direttiva 2000/46/CE del Parlamento europeo e del Consiglio, del 18 settembre 2000, riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, ed è ora regolata, a livello europeo, dalla Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pagg. 7-17), (in seguito "**EMD2**"). In italia si è data attuazione a tali disposizioni con l'introduzione nel D.Lgs. 1 settembre 1993, Testo unico delle leggi in materia bancaria e creditizia, "TUB", del Titolo V-bis "*Moneta elettronica e istituti di moneta elettronica*", emendato da ultimo con il d.lgs. 16 aprile 2012, n. 45, in attuazione della Direttiva EMD2. Cfr. MANCINI N., *Il nuovo assetto normative dei servizi di pagamento*, in *Banca, Impresa e Società*, 2013, p. 139.

326 V. considerando n. 7, EMD2.

327 V. art. 114–*bis*, comma I e art. 114–*quinquies.2*, TUB. V. anche le Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica del 17 maggio 2016, pubblicate nella Gazzetta Ufficiale Serie Generale n. 127 dell' 1° giugno 2016.

328 Art. 11, EMD2.

329 L'art. 11, comma 2, EMD2, recita: "*Gli Stati membri assicurano che, su richiesta del detentore di moneta elettronica, gli emittenti di moneta elettronica rimborsino, in qualsiasi momento e al valore nominale, il valore monetario della moneta elettronica detenuta*", laddove con l'uso della locuzione

La moneta elettronica si differenzia dai rapporti di credito che possono sorgere con enti creditizi in ragione del diverso tipo di regolamentazione che definisce le modalità di creazione del mezzo di pagamento. Gli enti creditizi possono, infatti, raccogliere depositi ed emettere crediti e sono soggetti ad un diverso regime di vigilanza e regolamentazione prudenziale[330]. La moneta elettronica consiste, invece, in un'alternativa digitale al contante: sotto questo profilo assomiglia ai bitcoin, che pure sono una rappresentazione digitale di un valore monetario, che permette di realizzare operazioni di pagamento. A differenza dei bitcoin, però, la moneta elettronica rappresenta sempre un credito nei confronti di un emittente[331], la cui "convertibilità" è assicurata dalla legge ai fini di salvaguarda la fiducia nello strumento. Sebbene la moneta elettronica non sia, quindi, tecnicamente, una moneta (*rectius*: un mezzo di pagamento) avente corso legale, la fiducia nel mezzo di pagamento è preservata dall'ordinamento mediante l'imposizione della convertibilità alla pari in mezzi di pagamento aventi corso legale e attraverso l'esercizio dell'attività di vigilanza sugli emittenti. Inoltre, la moneta elettronica è denominata secondo l'unità di conto statale – *rectius*, secondo l'unità di conto dell'unione monetaria –, mentre il sistema bitcoin utilizza una propria unità di conto.

2.3. I Sistemi di Pagamento

In ragione dell'uso che può essere fatto dei bitcoin quale mezzo di pagamento, ci si chiede, infine, se la disciplina dell'Unione Europea in tema di servizi di pagamento sia applicabile ai bitcoin. Anche in questo caso la risposta è negativa[332].

'valore monetario della moneta elettronica' si intende esprimere il concetto che all'utilizzatore che chiede il rimborso dovranno essere conferiti contanti o moneta scritturale in numero pari alle unità di conto rappresentante dalla moneta elettronica posseduta.

330 Cfr. i considerando 13 e 25, EMD2.

331 A mente dell'art. 2, EMD2, la «moneta elettronica» è "*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica*".

332 BANCA CENTRALE EUROPEA, *Virtual Currency Schemes*, 2012, cit., p. 43; GASPARRI, op. cit., p. 424.

La materia è attualmente regolata dalla Direttiva 2007/64/CE[333] e a partire dal 13 gennaio 2018 sarà invece regolata dalla Direttiva (UE) 2015/2366 del 25 novembre 2015[334]. In entrambi i testi legislativi, la nozione di pagamento è caratterizzata come collocazione, trasferimento o ritiro di «fondi», definiti a loro volta come "*banconote e monete, moneta scritturale o moneta elettronica*"[335]. Poiché i bitcoin non rientrano in nessuna delle tre categorie anzidette, non si ritiene che la disciplina in esame possa essere applicata ai bitcoin. Inoltre, si sottolinea che tali categorie sono tutte caratterizzate dall'essere dichiarate a corso legale ovvero dall'essere crediti emessi da emittenti soggetti ad autorizzazione, vigilanza e regolamentazione prudenziale, all'interno, quindi, di un *framework* regolamentare che tutela *ex lege* la fiducia e l'affidamento dell'utilizzatore. Queste tre categorie di 'moneta' sono, cioè, diversi mezzi di pagamento tutti appartenenti al sistema monetario pubblico–privato regolamentato dallo Stato e descritto come modello monetario unico nella teoria istituzionale della moneta. Ciò implica che i pagamenti oggetto della regolamentazione dell'Unione Europea sono pagamenti ricollegabili al potere liberatorio riconosciuto alle monete aventi corso legale. I bitcoin, *a contrario*, non sono crediti emessi da un emittente, sono rappresentazioni di un'unità di conto diversa da quella usata come moneta legale e la loro accettazione è su base volontaria. A fronte di tutte queste differenze e della esplicita circoscrizione dell'ambito di applicazione della direttiva alle tre categorie sopra richiamate, non pare che si possa ipotizzare neppure un'applicazione analogica della disciplina della direttiva ai pagamenti in bitcoin, seppure sia indubbio che anche in tale contesto sono prestati servizi inerenti attività del tutto paragonabili alle attività definite come attività di pagamento dalla direttiva[336]. Non escludendo, quindi, che in futuro parte della regolamentazione

[333] Direttiva del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE (GU L 319 del 5.12.2007, pagg. 1-36), attuata in Italia dal D.Lgs. 27 gennaio 2010, n. 11, che ha introdotto nel TUB il Titolo V-ter "*Istituti di pagamento*".

[334] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pagg. 35-127).

[335] Art. 4, n. 14, Direttiva 2007/64/CE e Art. 4, n. 25, Direttiva (UE) 2015/2366.

[336] Cfr. Banca Centrale Europea, *Virtual Currency Schemes*, 2012, cit., p. 17.

applicabile ai sistemi di pagamento possa essere estesa nel contesto dei bitcoin o di altri sistemi monetari simili ai bitcoin, non si ritiene che la disciplina sia applicabile senza un esplicito intervento legislativo sul punto.

2.4. I bitcoin e la categoria dei prodotti finanziari

Ampliando l'orizzonte della regolamentazione eventualmente applicabile ai bitcoin, in considerazione della natura immateriale, dell'attribuzione di valore, della facilità con cui i bitcoin sono scambiati sul mercato, e, infine, del fatto che il valore commerciale dei bitcoin è cresciuto nel tempo arricchendo chi ne aveva acquistati quando il valore era basso, ci si è chiesti se essi possano rientrare nella categoria dei prodotti finanziari.

A mente dell'art. 1, comma 1, lett. u) del D.Lgs. 24 febbraio 1998, n. 58, Testo unico delle disposizioni in materia di intermediazione finanziaria, "TUF", sono prodotti finanziari: (*i*) gli "strumenti finanziari", definiti dall'elenco tassativo di cui all'art. 1, comma 2, e (*ii*) "ogni altra forma di investimento di natura finanziaria". La definizione si compone quindi di una parte costituita da un elenco tassativo di prodotti e una seconda parte "aperta". La normativa di settore disciplina in modo specifico l'offerta al pubblico di prodotti finanziari (artt. 94 ss. TUF) e la prestazione di servizi che hanno per oggetto gli strumenti finanziari (art. 1, comma 5, TUF)[337].

L'ipotesi che i bitcoin possano essere considerati strumenti finanziari è da escludere in considerazione del fatto che essi non rientrano in nessuna delle categorie tipiche *ivi* previste[338]: i bitcoin non sono e non rappresentano crediti, non sono contratti e non sono titoli che danno luogo a crediti nei confronti di nessuno. Inoltre, l'art. 1, comma 4, TUF esplicitamente esclude dal novero degli strumenti finanziari i "*mezzi di pagamento*". Senza dare per scontato che i bitcoin rientrino in tale nozione – la quale potrebbe essere circoscritta in via interpretativa ai mezzi di pagamento denominati in

[337] *Amplius*, FRATINI M., Art. 1, 1° co., lett. U); co. 1-*bis*, lett. a), b), c); co. 1-ter; 2° co., *Prodotti finanziari, valori mobiliari e strumenti finanziari*, in M. FRATINI e G. GASPARRI (a cura di), *Il testo unico della finanza*, t. 1, UTET, 2012. V. anche FERRO-LUZZI P., *Attività e "prodotti" finanziari*, in *Rivista di diritto civile*, 2010, p. 133.

[338] GASPARRI, op. cit., p. 426–427.

valute avente corso legale – e siano perciò esclusi dall'applicazione della disciplina per questa ragione[339], resta la considerazione che i mezzi di pagamento siano esclusi dal novero degli strumenti finanziari "*in quanto più prossimi alla sfera del consumo che non a quella dell'impiego del risparmio in vista di un ritorno economico*"[340]. Non solo, quindi, i bitcoin non corrispondono a nessuna delle esemplificazioni tassative della nozione di strumento finanziario, ma anche il fatto che essi siano concettualmente assimilabili ad un mezzo di pagamento tradizionale induce a confermare la conclusione anzidetta.

Pare doversi escludere, altresì, che i bitcoin non possano essere considerati un prodotto finanziario atipico, cioè che essi non possano essere caratterizzati come "un investimento di natura finanziaria", seppur in questo caso occorre svolgere qualche riflessione in più. Alla luce degli orientamenti della CONSOB in materia, si considerano prodotti finanziari "atipici" le proposte di investimento caratterizzate dai seguenti tre elementi: (*i*) l'impiego del capitale; (*ii*) l'aspettativa di un rendimento di natura finanziaria; e (*iii*) l'assunzione di un rischio direttamente connesso e correlato all'impiego del capitale[341]. La CONSOB ha inoltre chiarito, nel caso di acquisto di beni suscettibili di apprezzarsi nel tempo, che ciò che distingue un acquisto di natura finanziaria è che l'aspettativa di rendimento atteso deve dipendere da una gestione condotta da altri o da un obbligo di riacquisto e non dal mero aumento del valore di mercato del bene (come può avvenire, per esempio, nel caso di acquisto di opere d'arte), che la componente di aspettativa di crescita del valore del bene deve essere effettivamente prevalente sull'aspettativa di uso del bene.

Ora, in merito alla ipotetica assimilazione dei bitcoin a questa categoria, essa origina da una particolare valutazione, in concreto, che si intende dare del progetto bitcoin e delle finalità per le quali un soggetto acquista bitcoin. Se si considerano i bitcoin come uno strumento che permette di intermediare gli scambi, allora è indubbio che essi siano strutturati secondo il modello teorico che si è descritto come sistema monetario. È possibile, però, anche volgere l'attenzione al fatto che qualsiasi mezzo di pagamento può essere esso stesso oggetto di acquisto e di vendita. In generale si ritiene che le leggi della

339 VARDI, op. cit., p. 448; GASPARRI, op. cit. 427.

340 *Ibidem*, p. 431.

341 V., per tutti, FRATINI, op. cit., p. 21.

domanda e dell'offerta influenzino il valore della moneta e nella prospettiva di scambi che hanno ad oggetto la moneta questa dinamica emerge in modo chiaro: se l'offerta cresce e la domanda resta la stessa il valore diminuisce; se la domanda cresce e l'offerta resta la stessa il valore aumenta.

Le particolari regole che sorreggono il sistema monetario bitcoin includono, lo si è visto, la previsione di un limite fisso massimo di bitcoin. Questo induce a ritenere che essi possano attraversare, a condizione che la domanda per i bitcoin sia in crescita, una fase deflazionistica in cui il valore dei bitcoin relativo alle merci e alle altre monete aumenta. In questa fase, incentivata dalla particolare struttura del sistema e quindi non accidentale, è possibile (ed anzi probabile, v. *infra*) che taluni soggetti acquistino bitcoin a fini speculativi per poter rivendere la moneta in un secondo momento quando il valore è aumentato: in questa prospettiva si può paragonare l'acquisto di bitcoin ad un investimento di capitale in uno strumento soggetto a rischio di cambio di valore nell'ottica di un ottenere un rendimento che non dipende dal comportamento dell'investitore, ed ipotizzare così che i bitcoin possano essere classificati come prodotti finanziari atipici.

Tale impostazione non è, però, condivisibile e possono essere avanzate in merito due critiche. La prima è che il rischio assunto con l'acquisto di bitcoin non corrisponde ad un rischio finanziario tipico: non c'è un'impresa sottostante o un'attività commerciale dal cui successo dipenda l'incremento di valore, se non il funzionamento stesso del sistema monetario bitcoin, che è frutto di una valutazione sociale che si è descritta come tipica dei fenomeni monetari e per ciò non riconducibile nell'ambito finanziario. Rileva, qui, il fatto che il valore dei bitcoin dipenda dal comportamento collettivo di un numero indeterminato di persone e non sia riconducibile ad un singolo emittente[342]. La seconda critica è connessa alla irragionevolezza delle conseguenze regolamentari che tale tesi comporterebbe. Qualora i bitcoin fossero considerati un prodotto finanziario atipico ne conseguirebbe l'applicazione della disciplina dettata in materia di offerta al pubblico (artt. 94 ss. TUF) e la disciplina concernente l'offerta fuori sede (art. 30 TUF). Entrambe sono strutturate secondo una logica che presuppone un emittente che beneficia dell'emissione

[342] Altrimenti detto, il rischio assunto non sarebbe direttamente connesso e correlato all'impiego del capitale. In quest'ottica l'esplicita esclusione dei mezzi di pagamento dal novero degli strumenti finanziari è indicativa delle diverse logiche che sottendono i rispettivi ambiti monetario e finanziario.

dello strumento e dai cui risultati dipenda il valore del prodotto finanziario[343]. Nel contesto dei bitcoin questa struttura non è replicabile: è vero che i *miner* producono bitcoin e li offrono in vendita al pubblico, ma il loro ruolo è diverso da quello dell'emittente di un prodotto finanziario: lungi dall'avere qualsiasi connessione con il valore dei bitcoin, il *miner* svolge una funzione predeterminata in modo standardizzato dalle regole del sistema, inoltre, non essendoci in origine una concentrazione di bitcoin in capo ad un emittente, la "offerta pubblico" è frazionata ed sostanzialmente indistinguibile da ogni altra transazione in bitcoin. Alla luce di queste considerazioni risulta ancora più convincente la tesi secondo cui i bitcoin non rientrano nella categoria dei prodotti finanziari.

Ciò detto, è indubbio che la particolare e complessa natura dei bitcoin sia tale per cui sussiste un interesse pubblico alla diffusione di un più alto grado di informazione circa i rischi connessi all'acquisto e all'uso di questa moneta e per questo la logica sottesa alla regolamentazione dell'offerta pubblica di prodotti finanziari troverebbe fruttuosamente applicazione anche nel contesto dei bitcoin. La soluzione del problema non pare, alla luce di queste brevi considerazioni, poter essere perseguita direttamente mediante un'interpretazione molto espansiva della nozione di prodotto finanziario, quanto piuttosto richiede un tipo di regolamentazione diversa che intervenga sui soggetti che facilitano lo scambio di bitcoin in altre valute. La questione, evidentemente, è suscettibile di ulteriori approfondimenti che non si ha modo di svolgere in questa sede.

2.5. La nozione di "*Virtual Currency*" e di "*Virtual Currency Scheme*"

Nel corso di questi ultimi anni l'interesse verso i bitcoin e la tecnologia *blockchain* è andato crescendo e numerosi enti pubblici, parlamenti, autorità di regolamentazione finanziaria o bancaria, organizzazioni internazionali e associazioni di categoria, si sono interessati al tema producendo un cospicuo numero di report, pareri, avvisi e documenti

[343] V., per esempio, l'art. 94, comma 2, TUF: "*Il prospetto contiene, in una forma facilmente analizzabile e comprensibile, tutte le informazioni che, a seconda delle caratteristiche dell'emittente e dei prodotti finanziari offerti, sono necessarie affinché gli investitori possano pervenire ad un fondato giudizio sulla situazione patrimoniale e finanziaria, sui risultati economici e sulle prospettive dell'emittente e degli eventuali garanti, nonché sui prodotti finanziari e sui relativi diritti*".

informativi[344]. In molti di questi documenti si è provato a tratteggiare il funzionamento del sistema bitcoin e ad evidenziare vantaggi, svantaggi e rischi connessi all'utilizzo di tale strumento o di strumenti costruiti in modo simile attraverso l'uso della tecnologia *blockchain*. Tra tutti questi il primo studio della Banca Centrale Europea del 2012 ha una rilevanza particolare perché in tale documento la BCE, assumendo una funzione tradizionalmente svolta dalla dottrina, ha provato a elaborare una nuova categoria concettuale comprendente un vasto insieme di nuovi fenomeni monetari o para-monetari, tra i quali i bitcoin, sotto il *nomen* di "*Virtual Currency Schemes*", tradotto dalla Banca d'Italia e nei successivi atti europei in lingua italiana come "*valute virtuali*"[345]. Tale categoria è stata successivamente ripresa dalla BCE stessa nel secondo studio del 2015 "*Virtual Currency Schemes – a further analysis*", nel quale se ne suggerisce una nuova definizione, e in numerosi altri studi e pareri, entrando nel lessico comune utilizzato per descrivere il fenomeno. La European Banking Authority ha fatto uso del termine *virtual currency* nel proprio parere del 4 luglio 2014 nel quale ha evidenziato numerosi fattori di rischio associati all'uso di queste nuove monete, invitando le autorità nazionali a dissuadere gli enti creditizi dall'offrire servizi legati a tali strumenti. Da ultimo, l'espressione «*valute virtuali*» è utilizzata nella Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che

---

344 Si segnalano: BLUNDELL-WIGNALL A., *The Bitcoin Question: Currency versus Trust-less Transfer Technology*, OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing. Disponibile all'indirizzo http://dx.doi.org/10.1787/5jz2pwjd9t20-en (ultima visita 20 giugno 2017); MARINI P. E MARC F., *Rapport d´information fait au nom de la commission des finances sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles*, Senato della Repubblica Francese, Sessione straordinaria del 2013-2014, N° 767 rectifié, Enregistré à la Présidence du Sénat le 23 juillet 2014; FEDERAL BUREAU OF INVESTIGATION, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*, 2012, disponibile all'indirizzo http://cryptome.org/2012/05/fbi-bitcoin.pdf (ultima visita 20 giugno 2017); ALI R., BARRDEAR J., CLEWS R. e SOUTHGATE J., *The economics of digital currencies*, in *Bank of England Quarterly Bulletin*, Vol. 54, 2014, No. 3, pp. 276–86; BARRDEAR J. e KUMHOF M., *The macroeconomics of central bank issued digital currencies*, Bank of England Staff Working Paper No. 605, disponibile all'indirizzo http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf (ultima visita 20 giugno 2017); ALI e al., *Innovations in payment technologies*, cit..

345 v. BANCA D'ITALIA, *Comunicazione del 30 gennaio 2015*, in Bollettino di Vigilanza n. 1, gennaio 2015, p. II.15; e BANCA CENTRALE EUROPEA, *Parere del 12 ottobre 2016 su una proposta di direttiva del Parlamento Europeo e del Consiglio che modifica la Direttiva (UE) 2015/849*.

modifica la direttiva 2009/101/CE, presentata dalla Commissione il 5 luglio 2016 (COM(2016) 450 final), e potrebbe trovare, quindi, utilizzo in un testo normativo qualora l'*iter* fosse concluso.

2.5.1. *Lo studio* 'Virtual Currency Scheme*' della Banca Centrale Europea (2012)*

La Banca Centrale Europea si è interessata al fenomeno in ragione della propria competenza di supervisione e vigilanza sul regolare funzionamento del circuito dei sistemi di pagamento. Adottando un approccio quasi dottrinale, la BCE si interessa al problema chiedendosi come possano essere descritti i nuovi schemi di pagamento basati su sistemi informatici e se essi comportino rischi di tipo sistemico, elabora una nuova categoria concettuale e conclude osservando che in considerazione della dimensione ancora piuttosto contenuta del fenomeno eventuali rischi concernono, per l'istante, solo gli utilizzatori di tali sistemi.

Lo studio parte dalla constatazione che esistono delle comunità virtuali, definite come luoghi nel ciberspazio dove individui interagiscono e perseguono obbiettivi comuni[346], all'interno delle quali circolano strumenti utilizzati per lo scambio di beni e servizi che sembrano svolgere almeno due delle tre funzioni tipicamente associate alla moneta: quella di mezzo di scambio e di unità di conto[347]. Tali strumenti sono chiamati *virtual currency* e sono definiti come:

> *"a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"*[348].

Se ne propone una suddivisione in tre categorie secondo la disciplina dello scambio tra valute tradizionali (che hanno corso legale in almeno uno Stato sovrano) e valute virtuali adottata in ciascuno schema:

---

346 BANCA CENTRALE EUROPEA, *Virtual Currency Schemes*, 2012, cit., p. 11.

347 *Ibidem*, p. 5.

348 *Ibidem*, p. 13.

(i) i "*closed virtual currency schemes*" sono schemi che non hanno alcuna connessione con l'economia reale, nei quali non è possibile acquistare o vendere valuta virtuale in cambio di monete tradizionali;

(ii) nei "*virtual currency schemes with unidirectional flow*" è possibile acquistare valuta virtuale contro valuta tradizionale, ma non il contrario: tutta la valuta virtuale acquistata deve essere spesa all'interno del circuito;

(iii) nei "*Virtual currency schemes with bidirectional flow*" è possibile, invece, acquistare e vendere valuta virtuale liberamente senza alcuna restrizione.

Nel corso dello studio sono descritti diversi modi in cui possono essere strutturate le monete virtuali e si evidenziano rischi connessi al potere che si concentra in capo all'emittente – nell'ipotesi, non rilevante per i bitcoin, di schemi di valute virtuali controllati da un ente centrale – in ragione della denominazione di tali strumenti in unità di conto diverse rispetto alle valute tradizionali e della mancanza di qualsiasi obbligo di convertibilità[349]. Si accenna inoltre al fatto che una delle ragioni per cui tali schemi sono costruiti è la possibilità di guadagnare attraverso l'emissione di valuta virtuale e attraverso operazioni speculative di acquisto e vendita di valuta virtuale[350] e, infine, si sottolinea che tali schemi sono esposti ai rischi tipici dei sistemi di pagamento[351].

Sono, inoltre, svolti due *case study*: sui Linden Dollar, una valuta virtuale utilizzata all'interno di Second Life, e sui bitcoin. In merito a quest'ultimi, la BCE sottolinea che lo schema si ispira direttamente alle dottrine economiche monetarie della scuola austriaca, che la rigidità nell'offerta di moneta può esacerbare i cicli economici e produrre spirali deflazionistiche[352] e sussiste un forte rischio di asimmetria informativa in considerazione della complessità del sistema e della semplicità con cui qualsiasi utilizzatore può acquistare bitcoin[353]. Nello studio si sottolinea, inoltre, che lo schema dei bitcoin potrebbe essere paragonato ad uno schema di Ponzi[354]. L'ipotesi è molto

349 *Ibidem*, p. 16.

350 *Ibidem*, p. 19.

351 *Ibidem*, p. 40.

352 *Ibidem*, p. 24-25.

353 *Ibidem*, p. 27.

354 *Ivi.*

interessante. In finanza si chiama schema di Ponzi una truffa nella quale i fondi ricevuti da un intermediario non sono investiti secondo quanto promesso, ma sono usati per ripagare interessi ai primi investitori, trasmettendo così al mercato la percezione che l'investimento proposto dall'intermediario sia molto fruttuoso e redditizio. L'apparente successo del prodotto finanziario permette di attrarre in continuazione nuovi fondi che alimentano la truffa nel tempo, permettendo il coinvolgimento di un numero sempre maggiore di investitori sino a quando la truffa non è smascherata e si comprende che il capitale investito è andato perduto. Sul punto la BCE afferma di non avere sufficienti conoscenze per trarre una conclusione.

In realtà, i bitcoin si differenziano dallo schema di Ponzi in modo radicale perché ad essi non corrisponde un investimento in una particolare attività finanziaria e non c'è alcuna promessa di restituzione del capitale investito. Non essendoci, a monte, una promessa di restituzione della valuta tradizionale spesa per acquistare bitcoin, è impossibile che in un certo momento si denunci il *bluff* e lo schema crolli.

È vero, invece, come nota la BCE, che il valore dei bitcoin aumenta grazie al sempre maggiore interessamento delle persone, che è provocato anche dall'aumento di valore del bene sottostante secondo uno schema circolare che ricorda la struttura dello schema di Ponzi; è vero, altresì, che l'assenza di una controparte centrale espone al rischio di non trovare una controparte disposta ad acquistare il bene in un'ipotesi di deprezzamento dello stesso; ed è certo che qualora tutti decidano di vendere i propri bitcoin il valore della moneta crollerebbe, sicché potrebbe verificarsi una situazione di *choc* simile a quella che si verifica quando uno schema di Ponzi viene smascherato. In questa seconda ipotesi, però, il valore dell'investimento crolla perché emerge una verità dei fatti diversa da quella dichiarata: l'investimento non c'è stato *tout court*, o esso ha riguardato una piccola parte del capitale investito. Una simile ipotesi non può verificarsi nel contesto dei bitcoin perché non è stata fatta alcuna promessa circa la redditività o l'aumento di valore del bene. Questo rende strutturalmente diversa la fattispecie[355].

Al termine dello studio la BCE conclude che le valute virtuali non devono essere considerate forme monetarie sicure; che il livello di affidabilità di questi sistemi è, in

[355] V. anche *infra*.

generale, di gran lunga inferiore rispetto al sistema bancario tradizionale soggetto a vigilanza prudenziale; e che l'uso di tali sistemi comporta l'assunzione di importanti rischi da parte dell'utilizzatore, che non sono mitigati dal diritto. In ragione della modesta rilevanza, in termini quantitativi, del fenomeno, la BCE conclude che eventuali crisi non dovrebbero avere significative ripercussioni, allo stato dei fatti, all'interno del sistema finanziario e monetario tradizionale, ed esclude, quindi, vi siano rischi di tipo sistemico anche per quanto attiene la salvaguardia del funzionamento dei sistemi di pagamento tradizionali[356]. Si evidenzia, però, un possibile rischio reputazionale connesso all'ipotesi in cui alcune di queste valute dovessero collassare e si afferma che il fenomeno potrebbe interessare più direttamente gli ambiti di competenza della Banca Centrale Europea qualora l'importanza di tali valute e il loro uso continuasse a crescere nel tempo.

Lo studio della Banca Centrale Europea sconta il limite di essere uno dei primi tentativi di elaborazione sistematica dottrinale di questo nuovo fenomeno, ma ha il pregio di aver evidenziato alcune importanti differenze tra questi strumenti e la valuta tradizionale, di aver voluto riflettere tali differenze promuovendo l'utilizzo di una nuova categoria concettuale e di aver prestato attenzione alle regole che disciplinano la produzione e la distribuzione di tali strumenti. Il riferimento alla nozione di schema che regola e disciplina la valuta virtuale è consonante alla descrizione della moneta nei termini di sistema monetario: seppure evidentemente sussistano delle differenze tra i due modelli, si apprezza lo sguardo istituzionale adottato dalla BCE, che permette a quest'ultima di porsi domande assolutamente rilevanti sulla sostenibilità degli schemi studiati e sull'allocazione di rischi e vantaggi tra utilizzatori ed emittenti. Da ultimo, si sottolinea l'inziale connessione tra 'valute virtuali' e corrispondenti 'comunità virtuali', che non sarà ripresa nella successiva versione della definizione di *virtual currency* resa dalla BCE nel 2015.

[356] *Contra* TWOMEY P., *Halting a shift in the paradigm: the need for bitcoin regulation*, in *Trinity College Law Review*, vol. 16, 2013, p. 67; e per una visione originale del problema: PLASSARAS N.A., *Regulating digital currencies: bringing bitcoin within the reach of the IMF*, in *Chicago Journal of international Law*, vol. 14, 2013, p. 377.

2.5.2. *Il parere della European Banking Authority (2014)*

L'impostazione della *European Banking Authority Opinion on 'virtual currencies'* del 4 luglio 2014 è molto meno dottrinale rispetto allo studio della BCE ed è connotata da un approccio pratico orientato ad evidenziare i rischi sui quali è opportuno intervenga un processo di regolamentazione. Essa si compone di una prima parte introduttiva in cui è proposta una nuova definizione di valute virtuali, una seconda parte in cui si evidenziano i vantaggi connessi all'uso di questi strumenti, una terza parte dedicata alla esposizione di una lunga serie di rischi collegati a tale uso e una quarta parte conclusiva dedicata alla regolamentazione del fenomeno.

La definizione di *virtual currency* proposta è la seguente:

> *"a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a (conventional) fiat currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically"*[357].

In tale definizione, il riferimento alla rappresentazione digitale di valore è inteso in senso quasi equivalente alla nozione di unità di conto, che, lo chiarisce esplicitamente la stessa EBA, non viene utilizzata direttamente per permettere di considerare le valute virtuali sia come una moneta, sia come un bene e per non implicare che il valore delle valute virtuali debba restare costante nel tempo[358]. La scelta di utilizzare un lessico particolare risponde all'obbiettivo di limitare il meno possibile l'ambito di applicazione della definizione: in questo si evidenzia l'approccio orientato al risultato operativo di espandere l'applicazione di eventuali regolamentazioni, piuttosto che l'interesse ad elaborare una definizione teorica puntuale del fenomeno. Ciò chiarito, è possibile rileggere la definizione proposta nel parere nell'ottica della nozione di sistema monetario elaborata in questa tesi ed evidenziare il fatto che ciò che l'EBA implicitamente afferma è che per aversi valuta virtuale occorre vi sia un'unità di conto diversa rispetto alle monete tradizionali, che vi siano meccanismi di rappresentazione digitale di tali unità appropriabili e trasferibili tra gli utilizzatori, e che tali rappresentazioni siano usate come

---

357 EUROPEAN BANKING AUTHORITY, *Opinion on 'virtual currencies'*, 2014, EBA/Op/2014/08, p. 11.

358 *Ivi*.

mezzo di pagamento tra gli utenti. In buona sostanza, quindi, per valute virtuali si intendono i sistemi monetari la cui regolamentazione non dipende dallo Stato e in cui i mezzi di pagamento sono, principalmente, virtuali.

Il parere prosegue con l'elencazione di una lunga serie di rischi e si conclude con un duplice suggerimento sul fronte della regolamentazione. Nel breve periodo si suggerisce di isolare il sistema finanziario da questo fenomeno e si raccomanda alla autorità nazionali di scoraggiare le banche e gli altri enti finanziari dal comprare, detenere e vendere valute virtuali[359]. Nel lungo periodo, si suggerisce di sviluppare un corposo insieme di previsioni normative, tra le quali spicca la proposta di imporre, per ciascuna valuta virtuale, la presenza di una "*scheme governance authority*": un ente che sia responsabile, nei confronti dello Stato e delle autorità indipendenti che soprintendono la regolamentazione del settore, delle regole adottate all'interno dello schema di valuta virtuale[360]. Tale richiesta evidenzia, da un lato, l'importanza della convenzione monetaria e, più in generale, la definizione della struttura del sistema monetario, sotto il profilo dell'allocazione dei benefici e dei rischi tra i partecipanti; dall'altro lato, presenta problemi di implementazione molto complessi nel contesto di valute virtuali come i bitcoin, in cui le regole del protocollo non sono direttamente modificabili da un ente centrale, ma una volta adottate sono implementate in modo collettivo dall'insieme dei partecipanti allo schema – *rectius*, dai *full nodes* e, in particolare, dai *miner* –.

2.5.3. *Il secondo studio della Banca Centrale Europea (2015)*

Nel 2015 la Banca Centrale Europea affronta nuovamente il tema con un secondo studio chiamato '*Virtual Currency Schemes – a futher analysis*'[361]. In questo nuovo documento la BCE si concentra principalmente sulle valute virtuali bidirezionali, in particolare quelle decentrate – la categoria che comprende le criptovalute e i bitcoin –; offre una descrizione dei principali attori coinvolti all'interno 'dell'ecosistema' che si crea intorno a questo tipo di valute virtuale; elabora nuovi possibili criteri di

[359] *Ibidem*, p. 6 e p. 44. Sul punto, per quanto concerne l'Italia, v. BANCA D'ITALIA, *Comunicazione del 30 gennaio 2015*, cit., p. II.15.

[360] EUROPEAN BANKING AUTHORITY, *Opinion*, cit., p. 39.

[361] BANCA CENTRALE EUROPEA, *Virtual Currency Schemes – a further analysis*, 2015, cit..

differenziazione tra i vari schemi (evidenziando la differenza strutturale tra schemi centralizzati e schemi decentrati[362] e offrendo una panoramica sulle diverse soluzioni adottate rispetto ad alcuni elementi determinanti per la creazione di uno schema di valuta virtuale[363]); descrive i diversi modelli di *business* adottati ed evidenzia alcuni rischi e vantaggi per gli utilizzatori. Da ultimo, la BCE torna sulla definizione delle valute virtuali al fine di specificare che esse non possono essere considerate "moneta" né sotto un profilo economico, né sotto un profilo giuridico.

Quanto all'analisi economica, la Banca Centrale Europea dichiara che le valute virtuali, inclusi i bitcoin, non realizzino le tre funzioni tipiche della moneta: (*i*) non sono propriamente mezzi di scambio in ragione della limitata accettabilità da parte del pubblico generale; (*ii*) l'alta volatilità dei prezzi le rende inadatte come riserva di valore; e (*iii*) la combinazione della scarsa accettazione da parte del pubblico insieme alla alta instabilità del valore le rende inadatte a svolgere il ruolo di unità di conto[364]. La BCE abbandona, quindi, ogni riferimento a comunità virtuali circoscritte per verificare se le valute virtuali svolgano le funzioni monetarie all'interno dell'economia reale e, parametrando a questo contesto l'esercizio delle tre funzioni, conclude che i bitcoin non sono una moneta dal punto di vista economico.

Sotto il profilo giuridico, nello studio si afferma che è moneta "*anything that is used widely to exchange value in transactions*" e si ricollega il termine "*currency"* ('valuta') "*to the specific form of money that is in general use within a country*". Ciò chiarito, partendo dalla constatazione che le valute virtuali "*are not used widely to exchange value*", si conclude che esse non siano moneta in senso giuridico ("*legal money*") e che esse non siano neppure, tecnicamente, "*currencies*". Lo studio prosegue inoltre evidenziando che alle valute virtuali non si applica il regime del corso legale, che invece è riconosciuto alle banconote delle valute tradizionali per legge, e che ciò le differenzia non solo dalle banconote, ma anche da ogni altra forma di moneta scritturale ed elettronica tradizionale[365]. Il ragionamento della BCE sul punto non è per niente

362 *Ibidem*, p. 9.

363 *Ibidem*, p. 10–11.

364 *Ibidem*, p. 23.

365 *Ibidem*, p. 24.

lineare. Mentre inizialmente la Banca sembra concludere che i bitcoin non sono moneta in senso legale sulla base di un riscontro fattuale, successivamente pare che il punto centrale di discrimine sia che essi, non essendo soggetti alla disciplina del corso legale e quindi all'obbligo di accettazione da parte dei consociati, possono essere scambiati solo in forza di accordi volontari. La BCE evidenzia, inoltre, che la regolamentazione attuale inerente la moneta elettronica e i sistemi di pagamento non trova applicazione nel contesto dei bitcoin e che non ravvede ragioni per modificare tali discipline in questa fase in cui le valute virtuali si stanno ancora sviluppando e il loro futuro appare incerto[366].

In conclusione, la BCE dichiara di voler emendare la definizione offerta nel 2012 eliminando ogni riferimento alla parola «moneta», perché ritiene che le valute virtuali non abbiano raggiunto un sufficiente grado di liquidità e di accettazione comunemente associato a tale nozione. La Banca rimuove, inoltre, tacitamente, ogni riferimento a «comunità virtuali» e propone quindi una nuova definizione di *virtual currency* nei seguenti termini:

> *"a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money"*[367].

La BCE sottolinea, inoltre, di utilizzare nel documento anche la nozione di "*virtual currency scheme*" per descrivere "*both the aspect of value and that of the inherent or in-built mechanisms ensuring that value can be transferred*"[368].

Rispetto alla definizione proposta nel 2012, il documento del 2015 ridimensiona molto il ruolo dei circuiti delle valute virtuali. Lo sforzo di definizione teorica del fenomeno lascia lo spazio a considerazioni di tipo più pratico e la Banca è molto netta nell'affermare di voler rimuovere ogni riferimento che possa indurre a ritenere le valute virtuali assimilabili alla moneta[369]. Il cambiamento più significativo consiste nel voler

---

366 *Ivi*.

367 *Ibidem*, p. 25.

368 *Ivi*.

369 Cfr. anche BANCA CENTRALE EUROPEA, *Parere del 12 ottobre 2016*, cit., par. 1.1.3.: "*la BCE raccomanda di definire le valute virtuali in modo più specifico, in modo da chiarire espressamente che le valute virtuali non costituiscono moneta legalmente istituita o denaro*".

considerare le valute virtuali all'interno del mercato tradizionale, senza riconoscere alcun rilievo alle funzioni che esse possono svolgere all'interno di mercati più ristretti. Così, mentre nel 2012 si affermava che le valute virtuali svolgono le funzioni di unità di conto e di mezzo di scambio all'interno di specifiche comunità virtuali e si chiedeva se potessero essere considerate anche riserva di valore (soprattutto in ragione della loro instabilità)[370], nel 2015 la Banca conclude che nessuna valuta virtuale, neppure i bitcoin che sono i più diffusi, svolge alcuna delle tre funzioni normalmente associate alla moneta[371]. La differenza cruciale nell'approccio sta nell'aver attribuito rilievo all'uso, seppur circoscritto entro un numero limitato di rapporti sociali, di un'unità di conto originale e diversa, nel primo caso; mentre nel secondo caso si è ritenuto di dare maggiore peso alla dimensione della frequenza effettiva degli scambi denominati in tale unità di conto all'interno del sistema economico nel suo complesso. La differenza, così radicale, nelle conclusioni e nell'approccio seguito, ci riporta alla questione della definizione della moneta e del sistema monetario sollecitando una riflessione circa la necessità, o meno, che a un meccanismo istituzionale strutturato secondo lo schema del sistema monetario debba corrispondere l'uso diffuso nell'intera economia, ovvero se sia sufficiente che tale sistema operi all'interno di una comunità sociale limitata[372]. La Banca Centrale Europea non nega, infatti, che i bitcoin siano strutturati secondo il modello del sistema monetario – ed infatti richiama, nella propria definizione, le parole utilizzate dall'EBA, che si è visto sottendono un ragionamento strutturato sulla triade unità di conto-mezzo di pagamento-uso diffuso –, ma asserisce che le peculiarità di tali istituti e la limitatezza dell'uso impediscono, nel caso concreto, di poter considerare questo strumento come moneta. La categoria delle *valute virtuali* non è più, quindi, inserita all'interno di un lungo processo storico di evoluzione della moneta, né è più considerata come un sottoinsieme della moneta caratterizzato da particolari attributi, ma ad essa è riconosciuto un carattere del

370 BANCA CENTRALE EUROPEA, *Virtual Currency Schemes*, 2012, cit., p. 11.

371 BANCA CENTRALE EUROPEA, *Virtual Currency Schemes – a further analysis*, 2015, cit., p. 23.

372 Sottesa a questa considerazione v'è poi l'ulteriore questione se una moneta come i bitcoin svolga davvero la funzione di unità di conto all'interno di una comunità virtuale, ovvero se esso sia solo uno strumento usato in modo parallelo alle valute tradizionali. Tale domanda non è, però, posta in modo esplicito dalla BCE.

tutto originale ed indipendente che trae origine da particolari sviluppi tecnologici nel campo informatico e dallo sviluppo del web[373].

2.6. La pronuncia della Corte di Giustizia in materia di tassazione e bitcoin

Prima di concludere la panoramica sulle ipotesi di classificazione dei bitcoin all'interno del quadro normativo esistente, è opportuno menzionare che la Corte di Giustizia dell'Unione Europea si è pronunciata sulla natura dei bitcoin, seppur nel limitato quadro di una domanda pregiudiziale relativa all'interpretazione di alcune fattispecie di esenzione dal pagamento dell'imposta sul valore aggiunto[374]. La questione sottoposta alla Corte riguardava la classificazione, ai fini IVA, del servizio di cambio di bitcoin contro valute statali tradizionali: in particolare, se tali operazioni dovessero essere fatte rientrare in una delle tre categorie di operazioni finanziarie esenti dall'applicazione dell'imposta.

Ai sensi dell'art. 135, par. 1, della Direttiva 2006/112/CE del 28 novembre 2006, relativa al sistema comune d'imposta sul valore aggiunto ("Direttiva IVA"), sono esenti, *inter alia*:

> *d) le operazioni, compresa la negoziazione, relative ai depositi di fondi, ai conti correnti, ai pagamenti, ai giroconti, ai crediti, agli assegni e ad altri effetti commerciali, ad eccezione del ricupero dei crediti;*
>
> *e) le operazioni, compresa la negoziazione, relative a divise, banconote e monete con valore liberatorio, ad eccezione delle monete e dei biglietti da collezione ossia monete d'oro, d'argento o di altro metallo e biglietti che non sono normalmente utilizzati per il loro valore liberatorio o presentano un interesse per i numismatici;*
>
> *f) le operazioni, compresa la negoziazione ma eccettuate la custodia e la gestione, relative ad azioni, quote parti di società o associazioni, obbligazioni e altri titoli, ad esclusione dei titoli rappresentativi di merci e dei diritti o titoli di cui all'articolo 15, paragrafo 2*.

---

373 Cfr. l'introduzione, *Ibidem*, pp. 6 ss..

374 Sentenza della Corte (Quinta Sezione) del 22 ottobre 2015, *Skatteverket* c. *David Hedqvist*, Causa C-264/14.

La Corte esclude l'applicazione dell'esenzione di cui alla lett. *f)* in ragione del fatto che i bitcoin non sono titoli rappresentativi di quote di proprietà su persone giuridiche, ed esclude l'applicazione dell'esenzione di cui alla lett. *d)*, poiché ritiene che essa riguardi la prestazione di specifici servizi di trasferimento di fondi, tra i quali peraltro non figura quello di cambio tra valute, e poiché ritiene che esistendo un'esenzione che riguarda specificatamente le operazioni su valute, *sub* lett. *e)*, il caso debba essere risolto sulla base dell'applicazione o della non applicazione di quest'ultima.

Sul punto, sia la Corte, sia l'avvocato generale, partono dal presupposto che i bitcoin siano uno strumento utilizzato tra privati come mezzo di pagamento[375] e che essi si differenzino dalla valuta tradizionale perché non hanno corso legale. Il centro della questione è dunque sapere se l'esenzione in esame si applichi solo alle operazioni di cambio tra valute aventi entrambe corso legale[376] o se essa può essere applicata anche a operazioni tra una valuta avente corso legale e un "*mezzo di pagamento contrattuale*"[377]. Appurato che esiste una diversità tra le varie traduzioni della norma in questione, la Corte ritiene di decidere il caso in base alla *ratio* ricollegabile al particolare contesto della norma in esame, che è di esentare dall'applicazione dell'IVA le operazioni puramente finanziarie in cui è difficile determinare la base imponibile e conclude che tra queste devono essere comprese anche le operazioni in cui siano scambiate monete non aventi corso legale, a condizione che tali monete "*siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento*"[378], accogliendo quindi la tesi secondo cui nell'ipotesi di cambio tra valute legali e bitcoin è molto difficile determinare la base imponibile e l'importo dell'IVA detraibile, esattamente come è difficile eseguire tale operazione nel contesto di cambi tra valute aventi corso legale in Stati diversi. La Corte conclude, dunque, che l'esenzione che si applica agli scambi tra

---

375 In particolare la Corte afferma in proposito che "*Nel procedimento principale, è pacifico che la valuta virtuale «bitcoin» non abbia altre finalità oltre a quella di un mezzo di pagamento e che essa sia accettata a tal fine da alcuni operatori*" (CGUE, C–264/14, *Hedqvist*, par. 52).

376 Conclusioni dell'Avvocato Generale Juliane Kokott, del 16 luglio 2015, Causa C-264/14, *Skatteverket* c. *David Hedqvist*, par. 29.

377 CGUE, C–264/14, *Hedqvist*, par. 42.

378 *Ibidem*, par. 49.

valute aventi corso legale debba essere applicata anche nel caso di operazioni di cambio tra bitcoin e valute tradizionali.

Nello sviluppare le argomentazioni che portano a tali conclusioni, i giudici di Lussemburgo sembrano, però, molto restii a fare propria l'equiparazione tra valute aventi corso legale e valute "private", come i bitcoin, proposta, seppur sempre nei soli limiti dell'applicazione della direttiva IVA, dall'avvocato generale, la quale, pur giungendo a conclusioni equivalenti, sviluppa una tesi parzialmente diversa rispetto a quella della Corte. Ella suggerisce che lo scopo di applicare esenzioni dal pagamento dell'imposta IVA sia quello di ridurre i costi del servizio e che nel caso del cambio tra valute (di cui all'art. 135, par. 1, lett. *e)*, Direttiva IVA) l'esenzione persegua lo scopo specifico di facilitare la convertibilità di qualsiasi valuta nell'interesse della fluidità delle operazioni di pagamento[379]. L'AG equipara, in questa prospettiva, i mezzi di pagamento sprovvisti di status legale ai mezzi aventi corso legale in un paese, ritenendo che entrambi svolgano la medesima funzione di intermediazione degli scambi, e rigetta le argomentazioni presentate dalla Repubblica Tedesca, secondo cui l'instabilità di valore ed il rischio di frodi legato ai bitcoin avrebbero giustificato una differenziazione tra le due forme monetarie[380]. Richiamato, quindi, il principio di neutralità, a mente del quale identiche operazioni devono essere tassate nello stesso modo, l'AG conclude che l'esenzione debba essere applicata anche alle operazioni di cambio che concernono i bitcoin.

Dalla pronuncia della Corte deduciamo, dunque, che ai bitcoin è riconosciuta ed attribuita, nel caso di specie, l'esclusiva funzione di operare quale mezzo di pagamento che permette di intermediare gli scambi e che essi sono considerati, quindi, alla stregua di un mezzo di pagamento privato. In considerazione del particolare ragionamento svolto in merito alla natura finanziaria delle operazioni e alle difficoltà di definizione della base imponibile e della specificità della questione, che riguardava un'ipotesi di esenzione dall'IVA, non molto di più può essere ricavato dalla sentenza in termini generali.

È, invece, molto interessante la tesi dell'avvocato generale, secondo cui non vi è sostanziale differenza tra mezzi di pagamento supportati dal corso legale e mezzi di

379 Conclusioni AG, C–264/14, *Hedqvist*, par. 39-40.

380 *Ibidem*, par. 42-44.

pagamento privi di questo attributo giuridico in quanto "*entrambe le forme di pagamento assolvono la medesima funzione, nella misura in cui vengono accettati negli scambi come mezzi di pagamento*"[381]. Così come è molto interessante che il governo tedesco abbia eccepito l'instabilità dei bitcoin come una delle possibili ragioni di differenziazione tra i due mezzi di pagamento.

Come si vedrà *infra*, l'approccio istituzionalista alla moneta evidenzia il fatto che c'è una sostanziale differenza tra i sistemi monetari strutturati secondo logiche che mirano a garantire la continuità del valore della moneta nel tempo e che fanno affidamento sulla disciplina del corso legale, e un sistema come i bitcoin, che rinuncia a tale strumento e si affida a meccanismi diversi per sostenere la fiducia degli utilizzatori nel valore futuro della moneta che comportano, strutturalmente, un più alto rischio di fluttuazioni del valore. Se da tale differenza debbano essere tratte conclusioni di rilievo giuridico che giustifichino un differente trattamento tra i due sistemi resta, in ogni caso, una questione aperta, così come resta la domanda, cui per ragioni di spazio non si proverà a dare risposta in questa tesi, se tale differenziazione sarebbe giustificabile, in particolare, nel contesto dell'applicazione della direttiva IVA.

[381] *Ibidem*, par. 42. Se ne deduce che l'avvocato generale Kokott adotta nel caso di specie una definizione di moneta sostanzialmente coincidente con l'idea di mezzo di scambio, che non attribuisce rilievo alla dimensione istituzionale della stessa e alla disciplina dell'istituto. La conclusione di un simile ragionamento non può che essere, dunque, che "*se, dunque, i bitcoin rappresentino una valuta «buona» o «cattiva» non ha alcun rilievo ai fini del presente procedimento*" (*ibidem*, par. 44).

Capitolo IV

Osservazioni sul nuovo modello di sistema monetario ‘bitcoin’

"*Bitcoin è un sistema di pagamento estremamente innovativo e potenzialmente molto efficace associato a un sistema monetario antiquato e pericoloso*”[382]

Volgendo verso il termine della tesi, si ha ora maggiore contezza della pluralità di significati con cui può essere intesa la parola «bitcoin» e di cosa essi siano. Le unità di ‘bitcoin’ (mezzo di pagamento) trasferite tra gli utenti del sistema sono registrazioni di valori numerici scritte in un registro collettivo digitale secondo le regole stabilite dal protocollo informatico ‘Bitcoin’. Essi non rappresentano beni o crediti nei confronti di particolari emittenti, ma delle unità di conto immaginarie, proprie di questo sistema, denominate ‘bitcoin’ (unità di conto). Il protocollo che gestisce la registrazione di questi valori è il cuore del sistema: per questo se n’è voluto illustrare in dettaglio il funzionamento. Il sistema così creato è strutturato sulla falsa riga del modello di ogni sistema monetario: è prevista un’unità di conto con la quale possono essere misurati i valori dei beni e nella quale possono essere denominati gli obblighi assunti dagli utilizzatori di questa moneta; sono previsti dei mezzi di pagamento astratti, sia sotto il

[382] AMATO e FANTACCI, op. cit., p. 1.

profilo dell'incorporeità, poiché sono valori numerici memorizzati su supporti digitali, sia sotto il profilo del loro valore, perché non sono convertibili in beni fisici; e tra essi è stabilito un rapporto di parità uno ad uno, per cui v'è perfetta corrispondenza tra l'unità mezzo di pagamento e l'unità di conto. Diversamente da ogni altro sistema monetario conosciuto, in questo caso il sistema ambisce a regolare scambi monetari tra soggetti che non si conoscono tra loro senza l'ausilio di un corpo politico terzo che svolga le funzioni di garante o supervisore delle operazioni. Tale obbiettivo è perseguito mediante l'impiego della tecnologia *blockchain*, che permette di realizzare uno strumento originale ed innovativo.

La creazione, l'allocazione e il trasferimento dei mezzi di pagamento tra gli utilizzatori sono quindi gestiti interamente dal protocollo informatico che disciplina la tenuta del registro: tale insieme di regole deve essere considerato parte integrante del sistema monetario sia perché definisce il funzionamento del mezzo di pagamento rendendone possibile l'uso, sia perché disciplina la politica monetaria del sistema, stabilendo le modalità di creazione di nuovi mezzi di pagamento. In quanto sistema monetario, i bitcoin realizza, infatti, una duplice risultato: offre un sistema di pagamento, in quanto permette il trasferimento di unità tra utilizzatori, e crea potere d'acquisto, in quanto crea nuovi strumenti utilizzabili come moneta.

Alla luce di quanto esposto nella tesi, nei prossimi paragrafi esporremo alcune riflessioni sulle caratteristiche proprie di questo innovativo sistema monetario rispetto a ciascuno di questi due ambiti.

1. Caratteristiche del sistema monetario bitcoin come strumento di gestione di pagamenti

Gli aspetti operativi di gestione dei trasferimenti e di aggiornamento del registro collettivo sono regolati dal protocollo informatico nei termini che sono stati analizzati nel dettaglio nel precedente capitolo. Tralasciando per il momento gli aspetti prettamente monetari della questione, sotto il profilo dell'esecuzione di ordini di pagamento, l'impiego della tecnologia *blockchain* per la realizzazione di un sistema di pagamento decentrato di questo tipo offre una serie di vantaggi considerevoli rispetto ai sistemi di pagamento tradizionali centralizzati. Senza pretesa di esaustività, si evidenziano le seguenti caratteristiche.

Alta resilienza ed autonomia del sistema

In primo luogo, la tecnologia *blockchain* permette di creare un sistema di gestione delle risorse autonomo ed estremamente resiliente.

Si è visto nel corso del precedente capitolo, che la concatenazione dei blocchi tramite l'impiego delle funzioni di *hash* permette di creare registri caratterizzati da un altissimo grado di affidabilità. Per modificare un dato registrato in un blocco si dovrebbe riscrivere quel blocco e tutti i blocchi successivi più velocemente di quanto il resto della rete riesca ad aggiungere nuovi blocchi alla catena: ciò implica che per potere avere delle chance di successo il *miner* o il gruppo di *miner* disonesti dovrebbero controllare più della metà della capacità di calcolo dell'intera rete e comunque anche in questa ipotesi l'attacco potrebbe riguardare solo i blocchi più recenti. Data la trasparenza del sistema, sussiste in ogni caso l'alta probabilità che un attacco di questo tipo sia scoperto. Inoltre, considerando che un simile comportamento potrebbe compromettere la fiducia nel sistema, è difficile immaginare ipotesi in cui i *miner* possano trarre convenienza da un simile attacco. Nel complesso, quindi, il sistema è estremamente resiliente.

Il criterio di preferenza per la catena più lunga consente di scegliere in modo automatico quale tra diverse versioni del registro collettivo concorrenti debba essere preferita e permette, quindi, di decentrare il sistema e di fare a meno di una controparte o

di un garante *super partes*. Ciò ha permesso di conseguire l'obbiettivo di realizzare un sistema autonomo rispetto all'ordinamento giuridico.

Vocazione universale

L'autonomia del sistema permette di svincolare i bitcoin da qualsiasi rapporto con comunità o territori specifici e di proporsi come una forma di gestione di risorse autenticamente sovranazionale a vocazione universale[383]. Questo significa: (*i*) che chiunque abbia la possibilità di connettersi a Internet può mandare ordini alla rete ed utilizzare i bitcoin; e (*ii*) che la distanza e la soggezione a diverse giurisdizioni tra pagatore e ricevente non ha alcuna incidenza sui tempi e sui costi del trasferimento di bitcoin.

Minimizzazione del ruolo degli intermediari

L'automatizzazione del sistema permette di accedervi in modo quasi diretto, senza bisogno di intermediari: questo riduce enormemente i costi di gestione complessivi e dovrebbe permettere una forte riduzione dei costi di ciascuna transazione. Il sistema permette, in teoria, a chiunque di scaricare l'intera blockchain e di connettersi alla rete come *full node* o addirittura come *miner*, anche se oggi è difficile che ciò avvenga. La competizione per la produzione di nuovi blocchi ed il particolare sistema di benefici che incentiva il sovrainvestimento in risorse hardware ha portato la difficoltà del *mining* ad un livello tale per cui oggi l'utente comune è escluso da tali processi. La grandezza della *blockchain* (in termini di dimensione complessiva dei dati), inoltre, incentiva il ricorso a intermediari o a sistemi semplificati di verifica dei pagamenti. Pur a fronte di tali specificazioni, il sistema resta strutturalmente legato a bassi costi di gestione: l'unica attività su cui l'utente deve necessariamente fare affidamento è l'attività di *mining*, che resta comunque fortemente regolata dal protocollo, e i costi relativi delle transazioni

[383] Tale indipendenza è mitigata dal fatto che l'attività dei *miner*, indispensabile per il funzionamento del sistema, è localizzata e resta soggetta alle leggi vigenti nel territorio dove questi operano, e lo stesso vale, in una certa misura, anche per gli altri servizi che sono prestati in relazione allo scambio e alla conservazione di bitcoin.

dipendono soprattutto da tale attività di registrazione dell'operazione sul registro[384]; mentre tutti gli altri intermediari svolgono funzioni che agevolano l'uso dei bitcoin ma che non sono indispensabili e possono essere sostituite da software. Nella prima fase di affermazione della moneta, fintantoché ai *miner* sono attribuiti nuovi bitcoin, tali costi sono contenuti dall'attribuzione ai *miner* dei vantaggi del signoraggio (il valore dei bitcoin "coniati", meno i costi di produzione). Col passare del tempo la quota di guadagno dei *miner* legata alla produzione di nuove unità diminuisce e i costi di produzione dovranno essere coperti attraverso l'imposizione di spese di transazione più alte. Data la semplicità della struttura del protocollo non è irragionevole pensare che tali costi possano essere complessivamente inferiori rispetto ai costi di supervisione e organizzazione del sistema bancario.

Trasparenza del sistema

Poiché il sistema si basa sulla condivisione delle informazioni inerenti le transazioni e sulla creazione di un registro comune, vi è un altissimo grado di trasparenza riguardo tutte le informazioni trascritte nella *blockchain* (che è interamente accessibile e scaricabile da chiunque). È inoltre possibile studiare il codice sorgente dei principali programmi usati dai nodi della rete e ciò implica che tutte le regole contenute nel protocollo sono pubbliche ed accessibili. Anche le discussioni inerenti le proposte di modifica sono tendenzialmente pubbliche e accessibili via internet, anche se su questo ambito è più difficile trarre conclusioni[385]. È più limitata, invece, la trasparenza nel contesto dei servizi offerti all'interno dell'ecosistema bitcoin, dove l'*audit* e la *disclosure* dipendono dalle prassi sviluppate nel mercato e dalle leggi statali di volta in volta applicabili ai gestori dei servizi.

Protezione della privacy

Attraverso l'uso della crittografia asimmetrica si permette un elevato grado di privacy a qualsiasi utente, imparagonabile rispetto alla quantità di informazioni che sono

384 Cfr. AMATO e FANTACCI, op. cit., pp 4. e 5; e ANDRESEN, op. cit., pp. 9 e 10.

385 Cfr. PASQUALE F., *The black box society*, Harvard University Press, 2015, *passim*.

trasmesse agli intermediari nel contesto dei sistemi di pagamento astratti tradizionali[386]. Poiché per compiere una transazione è sufficiente conoscere una delle chiavi pubbliche del ricevente, per trasferire bitcoin non occorre neppure che le parti si conoscano tra loro[387]: per questo i bitcoin sono stati correttamente paragonati al 'contante digitale'[388].

Basso costo di conservazione

Il fatto che i bitcoin siano unità astratte registrate su supporti informatici riduce sensibilmente il costo della loro conservazione, che in gran parte è esternalizzato sulla collettività che mantiene in uso il registro collettivo, mentre al singolo utilizzatore compete solo di salvare in modo sicuro le chiavi private corrispondenti ai propri indirizzi.

Possibilità di usi extra legem o contra legem

Il forte livello di *privacy* offerto, l'autonomia rispetto all'ordinamento giuridico tradizionale e la vocazione universale e transnazionale dei bitcoin ne permettono l'uso in contesti di attività vietate dal legislatore.

Ciò detto circa alcuni attribuiti che il sistema bitcoin offre come meccanismo di gestione dei pagamenti volgiamo ora lo sguardo ai primi tentativi di classificazione giuridica dei bitcoin.

---

386 Ma cfr. anche SPAGNUOLO M., MAGGI F. e ZANERO S., *BitIodine: Extracting Intelligence from the Bitcoin Network*, in *Financial Cryptography and Data Security. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, a cura di M. Brenner, Springer, 2014 (anche in http://fc14.ifca.ai/papers/fc14_submission_11.pdf, ultima visita 20 giugno 2017).

387 Per quanto sia statisticamente più raro che si concludano operazioni commerciali con perfetti sconosciuti, questa proprietà si rileva particolarmente utile nel cotesto di mercati illeciti.

388 AMATO e FANTACCI, op. cit., pp. 3-4.

2. Considerazioni sul sistema monetario bitcoin come moneta

"*The vices of strict commodity standards are the other side of their virtues*"

(Milton Friedman[389])

2.1. Il valore economico dei bitcoin e i meccanismi di sostegno della fiducia in un sistema monetario decentrato

La nostra ricerca è partita dalla constatazione del fatto che c'è una nuova unità monetaria scambiata nel mondo a cui è attribuito valore nonostante essa non sia legata ad alcuno Stato e non rappresenti alcun bene reale. Nel corso del breve tempo di vita di questo nuovo sistema monetario, il valore di scambio dei bitcoin è cresciuto da zero fino a quasi a toccare i 3.000 dollari per unità[390]. Chiedersi come sia possibile che ad unità di conto che non rappresentano altro che se stesse sia riconosciuto un simile valore, significa interrogarsi sulle strutture del sistema monetario che sostengono la fiducia degli utilizzatori in questa moneta.

Si è visto nel primo capitolo, infatti, che il valore dell'unità di conto è collegato alla capacità di acquisto futura attesa e viene determinato dall'uso della moneta da parte dei consociati. Nel contesto di incompletezza informativa che caratterizza lo scambio monetario e, in generale, l'uso della moneta, questo valore è influenzato e determinato dai meccanismi istituzionali che regolano il sistema monetario, i quali: (*i*) sorreggono la fiducia degli utilizzatori, incidendo sulle loro aspettative future, e (*ii*) determinano l'offerta di mezzi di pagamento, che a sua volta interagisce con la domanda di mezzi di pagamento da parte dei consociati.

Il sistema monetario tradizionale di fonte statale oggi in uso utilizza mezzi di pagamento astratti e persegue le due funzioni anzidette attraverso l'imposizione del corso

---

389 FRIEDMAN M., *Commodity-Reserve Currency*, in *Journal of Political Economy*, Vol. 59, 1951, p. 206.

390 Secondo quanto riportato dal sito www.blockchain.info, il giorno 11 giugno 2017 un bitcoin era scambiato contro 2.967 dollari.

legale; la presenza di un sistema bancario privato regolamentato cui è affidata la funzione di creazione di strumenti di debito sostanzialmente parificati ai mezzi di pagamenti; e l'affidamento delle competenze inerenti la determinazione della politica monetaria ad una banca centrale indipendente dal governo, che è tenuta ad esercitare tali competenze con il mandato di salvaguardare il valore della moneta nel tempo[391].

L'offerta di moneta è quindi gestita attraverso un articolato bilanciamento tra interessi privati e supervisione pubblica: il fatto che la moneta scritturale sia strutturata come un credito di cui l'emittente è garante, la regolamentazione che impone alle banche private di costituire riserve presso la banca centrale in funzione della loro esposizione debitoria e il fatto che la banca centrale possa modulare il tasso di interesse sono gli accorgimenti istituzionali attraverso i quali si cerca di ottenere un sistema che permetta di adattare l'offerta di moneta in modo flessibile rispetto alla domanda del mercato, cercando di evitare, per quanto possibile, fenomeni di sovrapproduzione di mezzi di pagamento. L'affidamento delle competenze di politica monetaria ad un'autorità indipendente dovrebbe altresì concorrere al sostegno della fiducia dei consociati nella moneta, in ragione del fatto che il governo non può più, in questo contesto, espandere arbitrariamente l'offerta di moneta astratta per finanziare la propria spesa pubblica.

La fiducia dei consociati nel valore della moneta è poi sostenuta, in maniera molto più diretta ed incisiva, dall'imposizione del corso legale. La moneta legale acquista, attraverso questa norma giuridica, il potere di liberare da qualsiasi obbligazione di tipo patrimoniale, sia essa di natura fiscale, di natura penale, di origine extracontrattuale o contrattuale: la moneta diventa, così, lo strumento attraverso il quale si dà concreta ed efficace attuazione al principio cardine della responsabilità patrimoniale di cui all'art. 2740 cod. civ.. L'uso della moneta avente corso legale, quindi, è tutelato e sorretto dalla forza coercitiva dello Stato che ne impone l'accettazione *ex lege*: l'aspettativa di uso futuro che i consociati ripongono nel sistema monetario è sorretta dall'ordinamento giuridico e la moneta diventa, per forza di legge, misura di qualsiasi prestazione a contenuto patrimoniale. Corollario del corso legale è il principio nominalistico, che

[391] SAINZ DE VICUÑA, op. cit..

sancisce la perfetta corrispondenza tra il mezzo di pagamento e l'unità di conto con cui sono denominati gli obblighi giuridici.

L'uso dei bitcoin non è, invece, sorretto dal corso legale: l'accettazione dei bitcoin è puramente volontaria. Cosa sorregge, allora, in questo secondo tipo di sistema monetario la fiducia dei consociati sull'utilizzabilità futura della moneta? Cosa induce a ritenere che i bitcoin avranno un valore di scambio?

Il valore dei bitcoin non è sorretto da alcun tipo di rapporto con dei beni fisici, né diretto, né indiretto: essi rappresentano solo sé stessi in un rapporto di perfetta coincidenza tra unità di conto e mezzo di pagamento astratto. Ad essi non corrisponde un valore della quantità di energia o dell'apparecchiatura utilizzata per la loro creazione, né rappresentano un paniere di beni o di altre monete, né un credito nei confronti di un emittente indirettamente garantito dal patrimonio di quest'ultimo. Ciascun bitcoin o frazione di esso rappresenta unicamente una certa quantità dell'unità astratta attribuita dal protocollo Bitcoin all'utente, trasferibile ad altri partecipanti. Ma come si può dare un valore a qualcosa che non esiste nella realtà e che non ha alcun referente materiale? Tale valore non potrà che scaturire unicamente dalla relazione che si instaura nella prassi tra esso e gli altri beni: in altre parole, il valore dipende esclusivamente dall'uso che si fa di questo strumento. Si ritorna, qui, al tema trattato nel primo capitolo del rapporto circolare tra l'attribuzione di un certo potere d'acquisto all'unità di conto e l'attribuzione di un prezzo (espresso in termini di unità di conto) ai beni con i quali l'unità di conto è scambiata. Se, allora, il valore dei bitcoin dipende dal fatto che essi siano scambiati, su base volontaria, con altri beni, la domanda che ci stiamo ponendo può essere anche riformulata nei seguenti termini: cosa ha indotto le persone ad utilizzare i bitcoin?

Un insieme di svariati fattori hanno concorso all'iniziale adozione del sistema. Sicuramente le caratteristiche del sistema di pagamento sopra descritte hanno esercitato un fascino verso certe categorie di persone. La possibilità di avere una moneta completamente indipendente da qualsiasi intromissione dello Stato è stata un fattore di richiamo per le persone politicamente orientate verso ideali ultraliberali[392]. La possibilità

[392] ANDRESEN, op. cit., p. 30.

di utilizzare questa moneta nel *dark web*[393] per acquistare beni su mercati illeciti ha avuto, per un certo periodo iniziale, molta importanza, forse più per la risonanza mediatica del caso *silk road*[394] che in termini effettivi di volumi di scambio[395], e tutt'oggi è senza dubbio una ragione d'uso di questa moneta. Inoltre, la possibilità di eseguire pagamenti a distanza e tra ordinamenti giuridici diversi ad un costo molto basso è un vantaggio specifico dei bitcoin. Ma le ragioni che più di altre hanno favorito il successo di questo sistema sono da ricercare nella sua architettura, ed in particolare: (*i*) nella scelta di distribuire tra i *miner* i vantaggi economici legati alla produzione di nuove unità; (*ii*) nella scelta di fissare in modo arbitrario un limite massimo al numero di unità che saranno mai prodotte dal sistema; e (*iii*) nella eliminazione della figura della controparte centrale.

L'attribuzione dei benefici derivanti dal signoraggio ai *miner* ha avuto due effetti importanti: ha favorito il loro coinvolgimento, offrendo un incentivo concreto e diretto per lo svolgimento di questa importante funzione, e ha inizialmente ridotto i costi delle transazioni, trasferendo indirettamente parte del beneficio a tutti gli utenti. I *miner*, infatti, essendo già remunerati dall'attribuzione di nuovi bitcoin per effetto della *coinbase transaction* non avevano necessità di richiedere spese di transazione agli utenti per rientrare dei costi dell'elettricità consumata e degli investimenti in *hardware*. Non appena il valore dei *bitcoin* è iniziato a salire, l'incentivo ricevuto si è tradotto in lauti guadagni e l'attività di *mining* si è rivelata molto vantaggiosa, attraendo così molte più persone interessate alla possibilità di conseguire un profitto attraverso la creazione di bitcoin, il ché, a sua volta, ha aumentato la notorietà e la diffusione dei bitcoin.

Il secondo elemento dell'architettura del sistema bitcoin, che è stato, ed è tuttora, determinante, è la regola che prevede un limite massimo di produzione dei bitcoin. Questa regola, che rende artificiosamente scarsi i bitcoin, permette di presentare questi valori contabili alla stregua di qualsiasi altro bene scarso di tipo materiale, ha conferito

---

393 v. SCHIAROLI I.W., *Dark web & bitcoin: la nuova era della rete*, Lantana, 2012; e MEGGIATO R., *Il lato oscuro della Rete: Alla scoperta del Deep Web e del Bitcoin*, Apogeo Editore, 2014

394 *Silk road* era un negozio virtuale strutturato come *amazon* o *ebay* dove gli utenti potevano vendere e acquistare droga contro bitcoin che è stato chiuso a seguito di un'operazione della FBI che ha avuto grande eco mediatica negli Stati Uniti; v., per tutti, TURPIN, op. cit., p. 357.

395 v. NATHAN A. (a cura di), *All about Bitcoin*, in *Top of mind*, Goldman Sachs Global Investment Research, n. 11, 2014, p. 9.

credibilità al progetto e rende possibile l'esistenza stessa di una domanda per i bitcoin e, quindi, di un mercato per questo bene. La determinazione esplicita del tasso di produzione e della quantità di bitcoin che sarà prodotta nel corso del tempo rende, inoltre, conoscibile *ex ante* l'offerta futura di moneta ed elimina, così, una variabile di incertezza sul futuro.

Con il passare del tempo, il successo commerciale dei bitcoin, l'aumento della loro notorietà e il fatto che non siano previsti limiti all'espansione del fenomeno hanno indotto nel mercato l'aspettativa di un progressivo aumento della domanda di bitcoin: la correlazione tra questa e la scarsità programmata si traduce nella previsione di deflazione, cioè di progressivo aumento del potere di acquisto dei bitcoin[396]. L'aspettativa che in futuro il valore possa aumentare e il basso costo di conservazione concorrono nel determinare la volontà di acquisire alcune unità indipendentemente dalla necessità o dall'intenzione di utilizzarle come strumento di intermediazione degli scambi, ma unicamente allo scopo di accumulare uno strumento di riserva di valore suscettibile di apprezzarsi, in termini reali, nel tempo.

Il terzo elemento che contribuisce a sostenere la fiducia dei consociati nel sistema è connesso al tentativo di eliminare il rischio di comportamenti opportunistici da parte del gestore del sistema cercando di ridurre l'attività di gestione a mera esecuzione di un software precompilato, senza esercizio alcuno di discrezionalità. Il sistema è quindi strutturato in modo che la responsabilità per l'esecuzione del programma sia condivisa tra tutti gli utenti della rete e non vi sia una controparte centrale cui è affidato il potere di intervenire sulla politica monetaria del sistema (e la connessa responsabilità di garantire il funzionamento dello stesso). Il protocollo "costituzionalizza" all'interno del codice informatico le scelte inerenti la politica monetaria rendendole vincolanti per tutti gli utilizzatori del sistema. Questo, contribuisce a rendere certo[397] e prevedibile il

---

396 DODD, op. cit., p. 368.

397 Si è detto che sarebbe tecnicamente possibile rimuovere il vincolo di produzione fissato a 21 milioni di bitcoin, esattamente come è possibile modificare qualsiasi parte del programma. Tuttavia, in considerazione dell'importanza che tale regola riveste all'interno del sistema è *politicamente* estremamente improbabile che ciò possa avvenire se non a fronte di una grave crisi che ne stia compromettendo il funzionamento. Proseguendo la comparazione tra codice del protocollo e ordinamento legislativo, si può dire che non solo il limite massimo di bitcoin è costituzionalizzato all'interno del codice, ma anche che esso è riconosciuto dagli utilizzatori/consociati come principio fondante del sistema.

comportamento futuro ‘dell’emittente’ (protocollo) e consente così di eliminare l’incompletezza e l’asimmetria informativa relativa alla offerta futura di moneta sul mercato e il rischio di comportamenti opportunistici espropriativi di sovrapproduzione della moneta.

Da quanto evidenziato emerge, quindi, una sostanziale differenza tra le modalità attraverso le quali i due sistemi monetari sostengono la fiducia degli utilizzatori nel potere d’acquisto della moneta: da un lato il sistema monetario tradizionale ne impone l’accettazione attraverso la minaccia coercitiva dello Stato, dall’altro lato il sistema bitcoin persuade all’adozione offrendo uno strumento in grado di eseguire pagamenti ad un costo inferiore rispetto al sistema tradizionale e in contesti in cui il sistema monetario non può essere usato; e, soprattutto, attraverso la distribuzione dei benefici connessi alla creazione di potere d’acquisto, la protezione radicale contro comportamenti opportunistici dell’emittente centrale attuata mediante l’eliminazione di tale figura e la programmazione *ex ante* della politica monetaria, e la connessa rappresentazione di possibili guadagni futuri connessi all’accumulazione di bitcoin. In questa prospettiva, il sistema monetario bitcoin, in particolare il protocollo, può essere considerato un «*gentle issuer*», il cui successo non dipende dalla forza, ma dalla persuasione.

All’intero di questo quadro, l’affidabilità tecnologica del sistema è determinante per la credibilità della proposta: sia perché garantisce stabilità e certezza all’attribuzione proprietaria dei bitcoin, sia perché attraverso il decentramento e la collettivizzazione del processo di gestione e aggiornamento del registro concorre a creare meccanismi di fiducia nell’immutabilità della politica monetaria e a costruire una percezione di affidabilità del sistema in quanto tale.

Nessun sistema monetario è, però, perfetto. La creazione di un’istituzione comporta sempre dei compromessi tra obbiettivi diversi e così a ciascuna delle tre modalità cardine attraverso le quali il sistema monetario bitcoin sostiene la fiducia degli utilizzatori nella moneta può essere fatta corrispondere una criticità del sistema.

2.2. La tensione tra aspettativa deflazionistica e la funzione di mezzo di scambio e di unità di conto

Il primo e più importante elemento di criticità corrisponde proprio al punto centrale del sistema monetario bitcoin: l'aver fissato un limite massimo al numero di bitcoin prodotti dal sistema. In un sistema in cui non ci deve essere nessun soggetto cui sia conferito il potere di determinare arbitrariamente la quantità di moneta in circolazione, il tasso di produzione deve essere predeterminato e la scelta ricade su due possibili opzioni: stabilire un numero massimo di unità monetarie che saranno complessivamente prodotte ovvero fissare un tasso di crescita costante nel tempo. Seguendo l'impostazione teorica della scuola austriaca, Satoshi Nakamoto ha deciso di seguire la prima strada, organizzando i bitcoin secondo lo schema della moneta–merce, la cui quantità è limitata e l'offerta è rigida. Nella prospettiva dell'inventore di questo nuovo sistema monetario la scelta si giustifica perché incentiva l'adozione e l'iniziale diffusione della moneta[398].

Il primo problema che si pone, però, è che avere fiducia nel successo di una moneta caratterizzata da un'offerta rigida genera un'aspettativa deflazionistica che induce l'operatore economico ad accumulare il mezzo di pagamento piuttosto che a spenderlo. Ciò significa che si crea un incentivo per l'acquisto di bitcoin come strumento suscettibile di esercitare la funzione di riserva di valore (*rectius* come strumento capace di incrementare il proprio valore nel tempo), ma disincentiva l'uso dei bitcoin come mezzo di scambio.

Vi è poi un'ulteriore considerazione che complica il problema. A fronte di un'offerta rigida, il valore della moneta resta constante se anche la domanda è constante, se invece la domanda aumenta o diminuisce il potere d'acquisto della moneta rifletterà tali flessioni. Quindi, nell'ipotesi in cui si diffonda l'aspettativa che in futuro il valore della moneta aumenti e aumenti la domanda di moneta, tale rapporto diretto tra domanda e valore comporta un aumento del valore della stessa. A sua volta, l'incremento del valore

[398] NAKAMOTO S., *Re: Bitcoin v0.1 released 2009-01-17 09:58:44 UTC*, disponibile all'indirizzo http://satoshi.nakamotoinstitute.org/emails/cryptography/17/ (ultima visita 20 giugno 2017).

può essere letto dal mercato come indice di successo della moneta e di un futuro ulteriore apprezzamento, generando una bolla speculativa pro-ciclica che si autoalimenta[399].

È difficile da prevedere quale possa essere l'effetto finale di questo meccanismo. Giova ricordare, in proposito, che a differenza di altri strumenti finanziari che sono sempre collegati, in modo più o meno diretto, a dei beni o ad attività commerciali reali, la moneta non ha un collegamento diretto con uno specifico bene. Nella prima parte della tesi si è evidenziato che il valore economico della moneta-unità di conto, il suo potere d'acquisto, è determinato da un particolare flusso circolare di informazioni, che sono acquisite dai contraenti e restituite ai consociati in occasione di ciascuno scambio monetario, cui consegue la determinazione di un rapporto tra unità di conto e beni reali. Tale meccanismo di valorizzazione è tipico ed esclusivo della moneta e discende dalla sua peculiare idoneità a misurare il valore degli altri beni. L'apprezzamento – cioè l'attribuzione o il riconoscimento di uno specifico rapporto tra beni e moneta – che ciascun consociato compie in questo contesto è determinato sia dalle informazioni ricevute dal mercato sul valore attuale della moneta, sia dalle aspettative future di incremento o diminuzione di tale valore.

Il valore della moneta riflette, cioè, anche le aspettative circa la capacità d'acquisto futura, cioè l'aspettativa di poter usare in futuro quella moneta per acquistare beni diversi e soddisfare ulteriori bisogni.

Il valore della moneta dipende, quindi, dalla capacità della stessa di conservare il proprio valore nel tempo: intesa come riserva di valore, la moneta è suscettibile di essere considerata essa stessa come un bene. In questa prospettiva la questione del suo valore si capovolge per riflettere le risultanze dell'incontro tra domanda e offerta: altrimenti detto, il fatto che vi sia una domanda di moneta si spiega in ragione della sua capacità di conservare il valore nel tempo, se questa capacità viene meno la domanda crolla, il valore della moneta crolla e si verifica un fenomeno di inflazione. In quest'ottica la moneta (mezzo di pagamento) può essere considerata essa stessa come un bene.

Nei sistemi monetari tradizionali, in cui la moneta è utilizzata per denominare qualsiasi rapporto di valore all'interno dell'economica, le pressioni inflazionistiche e

[399] AMATO e FANTACCI, op. cit., pp. 32–33.

deflazionistiche sono mitigate dall'uso quotidiano e, in ultima analisi, dalle tensioni sociali che scaturiscono per effetto di squilibri eccessivi, che si traducono in modifiche del sistema monetario[400]. In altri termini, mentre le aspettative circa l'apprezzamento o il deprezzamento futuro esercitano pressioni sul valore reale dei mezzi di pagamento, la denominazione dei crediti e dei debiti pecuniari in termini di unità di conto stempera tali pressioni.

Una buona moneta deve essere in grado di conservare in modo costante il suo valore del tempo, in un complesso gioco di bilanciamento tra la funzione di riserva di valore e l'esercizio della funzione di mezzo di scambio, le quali trovano realizzazione in comportamenti dei consociati antitetici (rispettivamente di accumulo o di cessione del mezzo di pagamento). In questa prospettiva, il corso legale e il principio nominalistico contribuiscono a limitare le oscillazioni di valore connesse a speculazioni sul valore futuro della moneta.

Ai bitcoin non si applica, però, il corso legale: la denominazione di obbligazioni e di offerte al pubblico in bitcoin avviene unicamente su base volontaria e perché uno scambio sia concluso in bitcoin c'è bisogno che entrambe le parti decidano di non utilizzare la moneta tradizionale e di sostituirla con i bitcoin. Nella determinazione dei prezzi e nell'esecuzione degli scambi i bitcoin subiscono la concorrenza dei mezzi tradizionali di pagamento, rispetto ai quali risultano essere vantaggiosi solo in specifiche circostanze (per esempio per scambi transfrontalieri). Per contro, in ragione della presunta aspettativa deflazionistica della moneta, i bitcoin si prestano non solo ad essere utilizzati come riserva di valore, ma addirittura come fonte di reddito para–finanziario: "para–finanziario" perché l'eventuale incremento di valore dello strumento non dipende da un'attività commerciale sottostante ma dall'andamento generale della moneta. Questo rende i bitcoin interessanti soprattutto in riferimento al loro utilizzo come riserva di valore piuttosto che come mezzo di scambio.

Un siffatto contesto non può che esacerbare una dinamica di bolla speculativa, in un modo simile, lo si è anticipato, a quanto succede in uno schema di Ponzi, in cui il successo (apparente) dei primi investitori spinge un numero sempre maggiore di nuovi

[400] Cfr. GRAEBER, op. cit., *passim*.

investitori dentro lo schema, che si autoalimenta grazie a questa continua espansione. A differenza, però, di quanto avviene in tale fattispecie, in cui si vendono titoli ad un valore di gran lunga superiore a quello a cui dovrebbero essere venduti perché si crea artatamente l'impressione che essi siano effettivamente molto redditizi, nel caso in esame i titoli su cui si 'investe' – i bitcoin venduti in cambio di valute tradizionali a chi "entra" nel sistema – non hanno un sottostante o un referente reale cui rimandano: non esiste un valore "giusto" a cui avrebbero dovuto essere venduti semplicemente perché in assoluto non esiste astrattamente un valore giusto o sbagliato dell'unità di conto, se non quello che le è conferito da parte dei consociati. Nel contesto della moneta tradizionale i consociati conferiscono valore alla moneta soprattutto attraverso l'uso nei rapporti economici.

Nel contesto dei bitcoin il valore è attribuito soprattutto in occasione di scambi tra bitcoin e altre valute, che hanno spesso una finalità speculativa. Quanto detto implica, da un lato, che non ci sono raggiri la cui scoperta e denuncia pubblica possa far crollare il valore dei bitcoin, dall'altro che la moneta è strutturalmente instabile. È plausibile, dunque, immaginare che si potranno susseguire momenti di ottimismo e disillusione sul futuro della moneta che avranno forti impatti sul suo valore, che resterà molto instabile fintantoché essa non sarà utilizzata in modo diffuso per denominare il valore dei beni e dei servizi del mercato. Ad oggi, però, non ci sono stipendi, rendite, mutui o tasse denominati in bitcoin che permettano di proiettare il valore reale della moneta in un arco temporale medio lungo[401] ed è difficile che, in considerazione della instabilità del potere d'acquisto dei bitcoin, qualcuno inizi spontaneamente a denominare crediti e debiti futuri in bitcoin.

In sintesi, i bitcoin sono soprattutto oggetto di una domanda di natura speculativa, che ne scoraggia l'uso come mezzo di scambio e ne rende difficile l'uso come unità di conto nei rapporti di durata.

Tale caratteristica non è accidentale, ma dipende dall'architettura stessa del sistema monetario che si fonda su un meccanismo di sostegno della fiducia che esalta la funzione di riserva di valore a discapito di quella di mezzo di scambio, in un contesto in cui i bitcoin si trovano a competere con mezzi di scambio affermati e protetti dal diritto.

[401] AMATO e FANTACCI, op. cit., p. 30.

Questo comporta un capovolgimento del paradigma consueto: mentre la moneta è solitamente descritta come uno strumento usato per intermediare gli scambi, che per adempiere tale funzione deve conservare il proprio valore nel tempo, qui la moneta è essenzialmente uno strumento usato a fini speculativi, che viene scambiata per conseguire un profitto di tipo para–finanziario.

2.3. Discrezionalità controllata vs. instabilità dei prezzi

La seconda criticità è connessa a quella sopra evidenziata e consegue alla scelta di non avere una controparte centrale in grado di adattare l'offerta di moneta alla domanda del mercato. In merito agli effetti di tale scelta sul valore della moneta, oltre a ricordare che la rigidità dell'offerta causa l'instabilità del valore della moneta, si osserva che l'assenza di una controparte centrale non permette di intraprendere azioni di politica monetaria finalizzate a contrastare bolle speculative. Come già evidenziato, l'instabilità del potere d'acquisto disincentiva l'uso dei bitcoin per l'assunzione di crediti e debiti e ne limita l'adozione come metro di misura dei beni e servizi dell'economia.

La predeterminazione della quantità massima di moneta in circolazione, del suo tasso di creazione e, in generale, l'esclusione di ogni discrezionalità, riduce, dunque, il rischio di comportamenti opportunistici a danno degli utilizzatori del sistema monetario, ma consegue questo risultato al caro prezzo di impedire anche le politiche monetarie a sostegno della stabilità del potere d'acquisto della moneta.

2.4. Incentivi e *miners*: un sistema monetario veramente *trust–less* ?

Un terzo ordine di considerazioni riguarda la politica di distribuzione dei benefici del signoraggio e, più in generale, la regolamentazione della funzione esercitata dai *miners*.

Il punto di partenza della riflessione è che il sistema monetario basato su *blockchain* nasce con l'ambizione di eliminare il bisogno di affidarsi a intermediari terzi. Il sistema complessivamente riduce enormemente la dipendenza da terzi ed in particolare riduce il rischio di *moral hazard*, prevedendo che non vi sia una figura centrale in grado di modificare i termini della convenzione monetaria secondo la propria discrezionalità. Per quanto il sistema si adoperi in questo senso, non è, però, possibile eliminare del tutto

alcune figure che giocano un ruolo importante nella costruzione del sistema monetario. La prima è la figura dell'emittente: trattandosi di un sistema monetario che crea potere d'acquisto è strutturalmente impossibile che ciò avvenga senza riconoscere a qualcuno la titolarità originaria dei mezzi di pagamento creati *ex novo*. La brillante soluzione del protocollo bitcoin è frazionare nel tempo l'emissione in tantissime micro emissioni consentendo a chiunque, in linea teorica, di esercitare tale attività e beneficiare dei vantaggi ad essa connessi.

Il secondo ruolo che non può essere del tutto eliminato nel contesto di una moneta astratta è quello del gestore del registro. Anche in questo caso, la soluzione adottata è di permette a chiunque di esercitare tale funzione. Per convincere qualcuno a sopportare i costi connessi a tale lavoro occorre, però, predisporre adeguati incentivi. Il problema è risolto, per la prima fase della vita dei bitcoin, facendo coincidere le due figure: a chi svolge il ruolo di manutentore del registro è riconosciuto anche il ruolo di emittente, è il suo lavoro è compensato (principalmente) con i benefici del signoraggio. Questa è una soluzione brillante del problema perché consente altresì di diffondere in via indiretta i benefici del signoraggio a tutti gli utenti. La previsione di un limite massimo di bitcoin comporta, però, che tale incentivo finisca: con la graduale diminuzione della creazione di nuovi bitcoin, il lavoro dei *miner* sarà retribuito con le *fees* che gli utenti saranno disposti a corrispondere per usare i loro bitcoin.

A questo punto è bene svolgere un paio di considerazioni. Si è visto che il meccanismo di competizione tra *miner* assegna tutti i benefici che derivano dalla creazione di un blocco al vincitore e lascia insoddisfatti tutti gli altri. Questo, oltre a comportare un significativo spreco di energie, incentiva i *miner* a investire sempre di più nelle macchine usate per fare *mining* per superare la concorrenza in potenza di calcolo. Si è visto altresì, che la difficoltà dei calcoli computazionali si adatta alle capacità di calcolo della rete, sicché non c'è limite al numero di computer che possono essere aggiunti e allo sviluppo tecnologico che può essere implementato nella rete: non c'è limite, cioè agli investimenti in capacità di calcolo. La combinazione di questi due fattori comporta da un lato l'incentivo a sovra investire nello sviluppo e nell'infrastruttura, dall'altro spinge fuori dal mercato gli attori più piccoli, che hanno meno capacità di

attrarre investimenti di capitale di lungo termine. Ne consegue una tendenza alla concentrazione limitata solo dall'organizzazione dei *miners* in grandi *pool*.

Dal punto di vista della distribuzione degli incentivi e dei ruoli all'interno del sistema monetario queste trasformazioni hanno un effetto preciso. Se il principio iniziale è di dividere il potere e la responsabilità di aggiornare continuamente il registro tra tutti i partecipanti in modo che nessuno possa assumere una posizione di controllo, la concentrazione del *mining* in capo ad alcune società e *mining farm* ha l'effetto opposto di raggruppare tale potere in capo a centri di interesse chiaramente individuabili. Ne è esempio il *New York Agreement* del 23 maggio 2017, che è stato siglato da un gruppo di *miner* che rappresentavano al momento della conclusione dell'accordo più dell'80% del potere di calcolo della rete.

Il punto che si intende sottolineare è, dunque, che si possono eliminare dal modello le *third central parties*, ma non tutte le *third parties*, e che per quanto si provi a distribuire la responsabilità e il potere tra i vari membri della rete, c'è sempre qualcuno che è ultimamente responsabile e che esercita il potere sull'aggiornamento del registro. Si sottolinea, inoltre, che esercitare, anche in modo collettivo, il potere sull'aggiornamento del registro equivale ad esercitare il potere sui termini della convenzione monetaria, poiché le regole che disciplinano il sistema bitcoin sono tutte riconducibili ai meccanismi di validazione dei nuovi blocchi. Si è visto nel precedente capitolo che il software ed il protocollo sono modificabili a condizione che tutti i *full nodes* aggiornino il software e l'esempio del New York Agreement[402], con il quale si è deciso di introdurre una modifica al protocollo della quale si è discusso per almeno due anni, è un perfetto esempio del fatto che il protocollo è in grado di regolare se stesso, ma l'accordo esterno di un numero di soggetti sufficientemente influenti sul sistema può provocare un cambiamento del protocollo stesso.

Cosa succederà in futuro se le *fees* dovessero aumentare esponenzialmente? Cosa succederà qualora l'attività dei *miner* non fosse economicamente sostenibile? Chi deciderà come e in che modo dovrà eventualmente essere modificato il protocollo? Le riflessioni presentate suggeriscono che per quanto eleganti, le soluzioni adottate

[402] Occorrerà verificare, però, se e come si darà esecuzione a tale accordo.

all'interno del protocollo bitcoin per decentralizzare il potere ed evitare situazioni di comportamenti opportunistici di tipo estrattivo che intervengano sui termini o sull'esecuzione della convenzione monetaria, tale rischio non è del tutto eliminato.

2.5. Garanzie istituzionali di lunga durata

Il tema appena sollevato porta a considerare la questione di quali meccanismi tutelano nel lungo periodo la tenuta del sistema sotto il profilo del bilanciamento degli interessi dei vari soggetti coinvolti.

In proposito occorre dire, provando a rispondere alle ultime domande appena sollevate, che l'intero sistema monetario bitcoin gioca sull'interazione tra regole del software, incentivi e teorie dei giochi, rendendo più profittevole per i (pochi) soggetti cui è affidato un ruolo con un certo (ristretto) margine decisionale comportarsi nell'interesse della collettività, a favore della salvaguardia della fiducia degli utilizzatori nel sistema, piuttosto che perseguire interessi di parte volti all'estrazione di benefici personali.

Ciò detto, si svolgono però due osservazioni. La prima è che non sempre la scelta è tra un comportamento che compromette la fiducia nel sistema e una che invece a tale prezzo avvantaggia gli interessi del soggetto agente. Spesso le distinzioni sono più sottili e vi possono essere compromessi ugualmente validi per il sistema nel suo complesso, che distribuiscono costi e benefici in modo diverso tra i partecipanti (per esempio tra *miner* piccoli e *miner* che controllano grosse *mining farm*). Le scelte inerenti la modifica, o la non modifica, del protocollo in base all'evoluzione del sistema sono scelte di tipo politico e la politica è il luogo del dialogo e del compromesso. Il problema, allora, non è tanto il rischio che un certo numero di *miner* prenda decisioni che possano compromettere la fiducia nel sistema, quanto piuttosto il fatto che il sistema monetario bitcoin non preveda spazi di discussione politica organizzati: i dibattiti sulle modifiche che software sono svolti su forum regolati in modo ambiguo e non ci sono meccanismi di rappresentanza delle varie *consituencies* perché alla base non si riconosce il fatto che il protocollo possa (e debba) essere adattato agli sviluppi dell'economia bitcoin.

La seconda considerazione concerne la concentrazione di bitcoin all'interno dell'economia bitcoin. Uno studio di qualche anno fa evidenziava un altissimo grado di

ineguaglianza all'interno dell'economia bitcoin[403]. Tale diseguaglianza è dovuta, *in primis*, al fatto che la quantità di bitcoin distribuiti come premio per la creazione di un nuovo blocco si è dimezzata nel tempo, nonché, in misura minore, a quanto si è detto circa la concentrazione dell'attività di *mining*. Il concetto può essere sintetizzato in una riga: chi è arrivato per primo si è servito abbondantemente e ha potuto continuare a servirsi nel tempo accumulando grosse riserve. Si consideri, inoltre, che poiché tutti i bitcoin sono originariamente attribuiti a dei *miner*, la circolazione di un bitcoin dipende originariamente dalla scelta di spesa di un *miner*, ovvero, nei termini della speculazione sopra descritta, si può dire che ogni bitcoin in circolazione sia il frutto di una scelta di 'disinvestimento' di un *miner*. Queste considerazioni lasciano supporre che esista un conflitto latente strutturale tra gli interessi di chi ha accumulato e non vuole 'svendere' il proprio patrimonio denominato in bitcoin e chi vorrebbe prendere immediatamente parte al progetto. È questo il tipico rapporto di tensione sociale che si viene a creare con la moneta, che tutto parifica ma al tempo stesso tutto ordina, dividendo il mondo tra chi ha (i creditori) e chi non ha (i debitori). Nel contesto dei bitcoin questa tensione potrebbe non essere così significativa: non c'è rischio che sfoci in un conflitto politico o sociale aperto perché i bitcoin non denominano i rapporti di lungo periodo che caratterizzano il vivere sociale all'interno di una certa comunità. Tuttavia, l'impressione che si ricava da questi dati e l'assenza di qualsivoglia meccanismo che permetta di modulare la convenzione monetaria per ripristinare un qualche equilibrio tra gli utilizzatori suggeriscono che molto probabilmente la dimensione speculativa continuerà a prevalere sulla funzione di misura, comparazione e scambio e che l'instabilità del potere d'acquisto – che potrebbe migliorare laddove debiti di lunga durata fossero denominati in bitcoin – non si stabilizzerà nel breve o medio periodo.

[403] KONDOR D., PÓSFAI M., CSABAI I. e VATTAY G., *Do the rich get richer? An empirical analysis of the Bitcoin transaction network*, in *PLoS ONE*, vol. 9, 2014, p. 1.

Conclusioni

Questa ricerca ha avuto per oggetto lo studio di un fenomeno sociale ed economico molto particolare. Si è partiti dall'osservazione della realtà: la presenza di una moneta digitale non riconosciuta e non sostenuta da alcuno Stato sovrano, che viene scambiata tra i consociati contro altre valute e che alcuni consociati utilizzano per effettuare degli scambi. Questa realtà interroga il giurista in modo originale, perché non appare essere riconducibile alle categorie tradizionali utilizzate dal diritto. Ci si è proposti, dunque, di comprendere innanzitutto quale fosse la vera natura dei bitcoin: come funzionano e se essi possono davvero essere considerati una moneta.

Attraverso lo studio del protocollo informatico che regola il sistema si è potuto concludere che i bitcoin scambiati tra gli utenti non sono altro che valori numerici iscritti su un registro digitale decentrato. A tali valori non corrispondono posizioni di debito e credito – per questo il registro si differenzia dalle tradizionali scritture contabili e dal modello di conto corrente –, né quantità di beni materiali: essi rappresentano unicamente quantità di un'unità di conto immaginaria inventata in occasione della creazione del sistema. Il registro ricorda, piuttosto, un registro di proprietà: su esso sono iscritte le transazioni tra gli utenti e i diritti di proprietà sui 'bitcoin' sono attribuiti in funzione delle annotazioni sul registro. Più specificatamente, *ivi* ciascun bitcoin o frazione di esso è associato ad un indirizzo pubblico di una chiave asimmetrica e la titolarità di tale bitcoin è riconosciuta al possessore della corrispondente chiave privata.

Il registro è strutturato come una catena di blocchi di informazioni ed è condiviso su una rete di computer che provvede ad aggiornarlo in continuazione attraverso l'esecuzione ininterrotta di un apposito programma informatico. L'esecuzione di tale programma permette di individuare in modo casuale e volta per volta all'interno di un certo gruppo di soggetti quello che concretamente aggiungerà una serie di annotazioni sul registro ed è in grado di risolvere in modo automatico eventuali conflitti tra versioni diverse di nuovi blocchi attraverso il criterio della preferenza per la catena di blocchi più lunghi. Questo consente di non dover individuare un soggetto centrale incaricato di garantire la correttezza e la manutenzione del registro comune e, inoltre, garantisce un

alto livello di resilienza e di affidabilità delle registrazioni, il cui inserimento dopo un breve lasso di tempo diventa sostanzialmente definitivo.

Nel corso della tesi si è chiarito, dunque, che i bitcoin sono stati concepiti come un bene digitale scarso: valori informatici facilmente trasferibili di cui fosse garantita la finitezza e l'attribuzione in capo a specifici soggetti attraverso un sistema decentrato. Ricollegando le origini dei bitcoin al pensiero criptoanarchico si è chiarito che tale sistema nasce con lo scopo di offrire una moneta anonima e digitale, non soggetta al controllo dello Stato o di qualsiasi altro emittente.

Si è provato, quindi, a capire se, a fronte delle peculiarità di questo sistema, i bitcoin possono essere considerati una moneta e che cosa questo implichi. La risposta non è scontata: per un verso i bitcoin si presentano, infatti, come una moneta, hanno una propria unità di conto e possono essere usati come mezzo di scambio o riserva di valore; per altro verso, essi non sono usati in modo diffuso per determinare i prezzi dei beni e dei servizi nell'economia, sono accettati solo su base volontaria da un ristretto numero di persone e il loro valore è soggetto a notevoli fluttuazioni. Dal punto di vista giuridico, inoltre, non vi è alcuna legge che ne disciplini o ne vieti l'uso, che resta quindi circoscritto all'interno della sfera dei rapporti consensualistici tra privati.

Per rispondere al quesito posto si è ritenuto, dunque, di non poter utilizzare definizioni della moneta basate sulle funzioni che essa assolve in un'economia, né di potersi limitare a considerare gli strumenti che lo Stato ufficialmente definisce moneta legale. Si è provato, invece, ad elaborare una nozione di moneta che potesse aiutare a chiarire il fenomeno oggetto di studio.

L'analisi della moneta in ottica istituzionale: la nozione di «sistema monetario» e le dinamiche sottese alla creazione e alla gestione di sistemi monetari

A tale proposito si è suggerito, dunque, che il fenomeno sociale, economico, giuridico e politico cui si fa riferimento con la parola «moneta» debba essere inteso come un'istituzione complessa e che esso possa essere meglio compreso e descritto attraverso l'uso della nozione di «sistema monetario».

Alla base del sistema monetario vi è una convenzione monetaria, cioè un accordo circa l'uso di un'unità di conto numerica astratta e la definizione dei mezzi di pagamento, gli strumenti che permettono di rendere concreta nella realtà dei rapporti tra consociati le unità di conto astratte, permettendone l'appropriazione e il trasferimento. La convenzione monetaria concerne, infine, anche la definizione del rapporto tra unità di conto e mezzi di pagamento, nonché le modalità attraverso cui i mezzi di pagamento possono essere creati.

Il sistema monetario istituisce, quindi, secondo i termini della convenzione monetaria, un'unità di conto e dei mezzi di pagamento che i consociati possono utilizzare, la prima, per definire il contenuto di obblighi e obbligazioni giuridiche e per comparare il valore dei beni e dei servizi presenti sul mercato, i secondi, per immagazzinare e trasferire ricchezza.

L'uso di questi strumenti presenta però dei problemi strutturali che il sistema monetario è chiamato a gestire.

In primo luogo, l'uso e l'accettazione della moneta per l'intermediazione degli scambi e per la definizione dei rapporti di durata (come il lavoro salariato, mutui immobiliari ed emissioni obligazionarie) dipende dall'aspettativa di poterla utilizzare nuovamente in futuro per ottenere ulteriori beni e servizi che soddisfino i propri interessi reali: occorre, cioè, che la moneta conservi nel tempo il proprio valore. Poiché è impossibile prevedere il futuro, ne consegue che l'uso della moneta implica sempre una situazione di incompletezza informativa, i cui costi sono inversamente proporzionali alla fiducia nella capacità della moneta di conservare il suo potere di acquisto.

In secondo luogo, i mezzi di pagamento sono oggetto di domanda da parte dei consociati. Tale domanda varia nel tempo ed incide sul loro valore e, quindi, sul valore in termini reali dell'unità di conto. Per garantire la stabilità del potere d'acquisto della moneta sarebbe quindi preferibile un sistema che permetta di gestire l'offerta di mezzi di pagamento in modo flessibile, in modo che essa possa essere adattata alle esigenze del mercato. Storicamente, questa esigenza si è manifestata soprattutto con l'espansione dei mercati e il crescere del numero di scambi, che ha richiesto una maggiore produzione di mezzi di pagamento ed ha così indotto il sistema ad orientarsi verso l'adozione di mezzi di pagamento di tipo astratto, privi di valore intrinseco. La maggiore flessibilità nella produzione di mezzi di pagamento implica, però, che vi sia un soggetto cui viene conferita

una certa discrezionalità, che può essere esercitata nell'interesse collettivo, così come per perseguire interessi 'privati' propri di quel soggetto, a danno della collettività. Si viene a creare, così, una tensione irrisolvibile tra l'interesse ad una maggiore flessibilità volta a tutelare la stabilità del valore nel tempo e l'interesse a limitare i comportamenti opportunistici di tipo estrattivo da parte dei soggetti cui è affidata la gestione della produzione di mezzi di pagamento.

Per far fronte a questi due problemi strutturali il sistema monetario deve quindi prevedere: (*i*) dei meccanismi istituzionali che sostengano la fiducia dei consociati nel valore futuro della moneta; e (*ii*), ove sia prevista una certa flessibilità nella produzione di mezzi di pagamento (o nella definizione del rapporto tra mezzi di pagamento e unità di conto), dei meccanismi istituzionali che tutelino gli utilizzatori contro il rischio di comportamenti espropriativi. Poiché la flessibilità è funzionale alla conservazione del potere d'acquisto della moneta, questi due obbiettivi sono anch'essi in tensione tra loro[404].

Nel sistema monetario statale oggi vigente si prova a gestire questa tensione mediante l'affidamento delle competenze di politica monetaria a banche centrali indipendenti, con il mandato di esercitare tali poteri per salvaguardare il potere d'acquisto della moneta nel tempo.

In questo quadro il diritto è lo strumento attraverso cui la politica organizza e gestisce un sistema monetario pubblico. In particolare, si è visto che la disciplina del corso legale e il principio nominalistico svolgono un ruolo diretto e molto importante nel sostenere l'aspettativa di poter utilizzare la moneta in futuro, il suo potere d'acquisto e, quindi, l'uso stesso da parte dei consociati. L'imposizione di una certa unità di conto per la denominazione di tutti gli obblighi di fonte pubblicistica e l'imposizione dell'accettazione di determinati mezzi di pagamento nei rapporti privati contribuiscono a garantire l'uso futuro della moneta e a ridurre l'incompletezza informativa; mentre il principio nominalistico contribuisce a stabilizzare il valore dell'unità di conto.

[404] Si evidenzia, cioè, una tensione tra l'esercizio delle funzioni di mezzo di scambio e di riserva di valore, di cui non si ha alcuna percezione laddove si dia per scontato che la moneta eserciti tutte tre le funzioni che le sono normalmente attribuite.

I bitcoin: un sistema monetario innovativo basato su blockchain

La conclusione cui si è potuti giungere attraverso l'elaborazione della nozione di sistema monetario è che i bitcoin sono strutturati e concepiti secondo tale schema e sotto questo profilo possono, dunque, essere assimilati alla moneta.

Si è evidenziato, allora, che nel contesto dei bitcoin l'organizzazione e la gestione del sistema è demandata all'esecuzione del protocollo informatico che contiene, sia tutte le regole tecniche di funzionamento dei pagamenti, sia la disciplina della politica monetaria, *ivi* incluse, in particolare, la disciplina relativa alla produzione di nuovi mezzi di pagamento, il cui tasso di generazione e numero massimo totale sono stati fissati *ex ante* al momento della creazione di questo nuovo sistema monetario.

A fronte di ciò l'intero sistema bitcoin potrebbe essere paragonato ad un sistema giuridico a sé stante che concerne la creazione e lo scambio di unità monetarie, in cui la principale fonte di regole è il protocollo bitcoin e la regolamentazione è implementata attraverso l'esecuzione del software che lo contiene. Un tale approccio permette di sottolineare l'esautoramento del diritto di fonte statuale e/o sociale, cui si preferisce una regolamentazione che discende dalla scrittura e dall'esecuzione di protocolli informatici, nonché il carattere marcatamente sistemico che caratterizza qualsiasi moneta. A ciò corrisponde un tentativo di eliminare il 'politico', inteso come l'insieme di istituzioni e prassi che disciplinano l'esercizio di poteri discrezionali che hanno incidenza su una collettività, per lasciare spazio a sistemi predeterminati attraverso funzioni informatico–matematiche e alla libertà assoluta delle persone, cui è consegnata un'istituzione gestita da una collettività in cui tutti partecipano ma nessuno assume formalmente alcuna responsabilità (né alcun potere decisionale) sul progetto.

A fronte dell'alto grado di innovazione che li caratterizza, i bitcoin possono essere considerati come il modello di un nuovo paradigma di sistemi monetari, in cui lo spazio decisionale tradizionalmente occupato dalla politica è sacrificato in nome della ricerca di una forma di artefatta stabilità implicita, sostenuta dalla solidità della tecnologia crittografica e dalla fede nel libero mercato: in contrapposizione ad un modello di un emittente che *impone* attraverso la legge un certo sistema monetario, si propone un modello di *gentle issuer*, un emittente che persuade gli agenti ad utilizzare il sistema

monetario in modo volontario sulla base di una supposta superiorità nell'architettura del sistema.

Più specificatamente, nel bitcoin il modello rinuncia all'imposizione coercitiva e al sostegno offerto dal diritto in favore di una supposta maggiore stabilità economica di lungo periodo che dovrebbe essere garantita dalla stabilità e resilienza del sistema informatico e dall'assenza di una controparte centrale che possa modificare arbitrariamente l'offerta di moneta perseguendo scopi opportunistici estrattivi. Alla capacità di adattare la quantità di moneta in circolazione in funzione delle fasi economiche e della domanda di moneta è preferita, dunque, la predeterminazione matematica delle unità in circolazione: alla decisione politica, la rigidità di un algoritmo matematico. A ciò, e all'indipendenza da ogni potere, consegue altresì la volontarietà dell'accettazione dei bitcoin, cui si è già fatto cenno, per effetto della quale tale strumento libera dall'obbligazione solo nella misura in cui il creditore abbia accettato volontariamente il loro uso.

Lo studio approfondito del sistema ha permesso, però, di evidenziare che la pretesa immutabilità del protocollo è relativa, e che anche nel contesto di un sistema così decentrato sorge l'esigenza di provvedere a modifiche dell'accordo costitutivo iniziale. Il contenuto del protocollo informatico può essere, infatti, modificato a condizione che tutti gli utenti del sistema aggiornino il proprio software. In proposito sono state create spontaneamente all'interno della comunità dei programmatori che aggiorna il software delle regole procedurali inerenti la proposizione e l'approvazione di modifiche, che avviene per consenso. Si è osservato, però, che nelle ipotesi di modifiche rilevanti tali sistemi non funzionano, con il rischio di lunghe fasi di stallo decisionale che possono essere risolte solo attraverso la convergenza "extra costituzionale" dei soggetti che controllano direttamente o attraverso accordi di *mining pool* la maggior parte della capacità computazionale della rete.

La comparazione tra il sistema monetario basato sull'imposizione sovrana e il sistema fondato sulla capacità di persuasione dell'algoritmo ha inoltre permesso di evidenziare alcuni importanti limiti strutturali dei bitcoin sotto un profilo monetario.

Una delle caratteristiche più importati del sistema monetario bitcoin è di avere predeterminato l'offerta di moneta (mezzi di pagamento) nel tempo secondo un preciso

calcolo matematico. Tale strategia permette di conseguire dei vantaggi, ma presenta un costo molto alto, che rischia di compromettere in modo strutturale la natura stessa dei bitcoin come sistema monetario. Essa consegue: (*i*) alla scelta di rinunciare ad una controparte centrale e (*ii*) al bisogno di incentivare l'adozione della moneta da parte di un numero sempre più vasto di persone in un contesto in cui non è possibile fare affidamento sul diritto statale e sull'imposizione del corso legale.

Sotto il primo dei due profili evidenziati, la scelta di fissare *ex ante* la quantità di moneta in circolazione permette di ridurre l'incompletezza informativa che caratterizza strutturalmente lo scambio monetario e, in particolare, elimina alla radice la possibilità di comportamenti opportunistici di tipo estrattivo da parte dell'emittente connessi alla sovrapproduzione di potere d'acquisto. Per converso, il sistema è così caratterizzato da un'altissima rigidità dell'offerta di moneta, che a sua volta produce una forte instabilità dei prezzi a fronte della (normale) fluttuazione della domanda di moneta.

La fissazione di un limite massimo predeterminato di moneta e l'assenza di qualsivoglia meccanismo di aggiustamento di tale quantità può essere interpretata anche nell'ottica del secondo profilo sopra evidenziato, come strumento volto a sostenere la fiducia nella moneta e a promuoverne l'adozione. La rigidità del sistema informatico che disciplina i bitcoin permette, infatti, di avere a disposizione uno strumento di scambio conveniente, caratterizzato dagli attributi di trasferibilità tipici dei mezzi di pagamento astratti e – in ragione della particolare struttura del sistema – da costi di conservazione molto contenuti, ma non soggetto al rischio di replicabilità e di sovrapproduzione. Questi attribuiti positivi, unitamente alla paventata immutabilità della regola concernente il numero massimo di bitcoin, suscitano, inoltre, aspettative deflazionistiche circa il valore futuro dei bitcoin. Questo meccanismo è funzionale a promuovere il successo e la diffusione di questa moneta, ma al tempo stesso ne compromette l'utilizzabilità come mezzo di scambio e unità di conto, contribuendo all'affermazione di bolle speculative che esasperano ulteriormente l'instabilità del valore dei bitcoin. Ne consegue che il 'successo' dei bitcoin si riduce ad essere un successo di tipo *commerciale* dei bitcoin come prodotto su cui investire a fini speculativi, piuttosto che essere un successo di tipo *istituzionale* che coincide con l'adozione dei bitcoin come sistema monetario utilizzato per organizzare lo scambio e l'allocazione di risorse all'interno di un'economia.

In questi termini può essere letta, allora, l'attribuzione di valore economico a beni digitali che non ne avrebbero, altrimenti, alcuno. In tutte le ipotesi in cui un sistema monetario viene creato, i beni che estrinsecano l'unità ideale utilizzata (talvolta sovrapponendosi in modo uguale ad essa) acquistano un valore di scambio distinto rispetto al loro valore d'uso originario: il «*cash premium*». Il valore del singolo bitcoin in teoria è completamente costituito dal potere di acquisto atteso, posto che il bene non ha altrimenti alcun valore d'uso originario proprio, ma in ragione della particolare architettura del sistema tale valore pare discendere dall'aspettativa di poter rivendere i bitcoin ad un prezzo più alto in futuro, piuttosto che dall'aspettativa di poter acquistare beni e servizi ad un certo valore. In sintesi, sembra potersi dire che il valore dei bitcoin sia da attribuire alla presenza di uno «*speculative premium*», piuttosto che ad un «*cash premium*», e questo rischia di compromettere strutturalmente la stabilità del potere d'acquisto dei bitcoin e la capacità stessa dei bitcoin di esercitare le funzioni comunemente attribuite ad un sistema monetario, pur essendo strutturati secondo tale modello. La differenza è sottile: i bitcoin possono ancora, infatti, essere usati per acquistare beni e servizi, a condizione di trovare una controparte disposta a concludere scambi, ma difficilmente saranno usati, per ragioni di convenienza ed opportunità, per denominare posizioni giuridiche in rapporti di durata. È difficile, quindi, se non sostanzialmente impossibile, immaginare che essi possano esercitare una funzione organizzativa della produzione e dell'allocazione di risorse all'interno dell'economia.

In proposito si trae la conclusione che l'instabilità monetaria appena descritta – da molti considerata il problema principale per cui i bitcoin non possono essere considerati moneta da un punto di vista funzionale[405] – e la ricorrenza di dinamiche che ricordano le bolle speculative pro-cicliche che alimentano tale instabilità, sono conseguenze dirette della architettura del sistema monetario bitcoin e sono riconducibili, in ultima analisi, alla necessità di sostenere la fiducia nel sistema in un contesto in cui non trova applicazione il diritto di fonte statale. Per converso, si evidenzia che proprio il corso legale unitamente alla presenza di meccanismi che promuovo una flessibilità ragionevole dell'offerta della

[405] Per tutti, BANCA CENTRALE EUROPEA, *Virtual Currency Schemes – a further analysis*, 2015, cit..

moneta concorrono a salvaguardare la stabilità del potere d'acquisto nel contesto delle valute tradizionali. Da tutto ciò consegue che i bitcoin possono essere considerati, quindi, un tipo molto particolare di moneta – *rectius*, sistema monetario –, ma altresì che tale modello si sistema monetario in questo momento non funziona affatto bene e non sembra essere caratterizzato da meccanismi istituzionali che potranno correggerne i limiti di funzionamento in futuro. Ne consegue, altresì, che il sistema bitcoin non può essere paragonato *sic et simpliciter* ad una truffa, quanto piuttosto ad una illusione collettiva.

Queste ultime riflessioni ci inducono a domandarci, infine, se sia concettualmente possibile disporre di una molteplicità di monete all'interno di un'economia e se questo possa portare dei vantaggi. Il tema meriterebbe maggiore sviluppo nell'ambito di ricerche successive, qui ci si limita a cogliere l'occasione per formulare qualche riflessione conclusiva ed osservare, in primo luogo, che la funzione di comparazione dei valori dei beni e dei servizi su un mercato, che permette di gestire l'economia secondo criteri razionali richiede che si usi un unico metro di misura, e, in secondo luogo, che la questione ci riporta al tema degli usi pubblici che la società fa della moneta.

Il sistema monetario non serve, infatti, soltanto a permettere gli scambi tra consociati e a permettere lo scambio di informazioni sul mercato (sia relative a prezzi, sia relative a posizioni finanziarie: si pensi al bilancio di una società per azioni), bensì anche a permettere la riscossione delle tasse e il regolare svolgimento dell'attività di pacificazione del conflitto sociale operato mediante l'esercizio della giurisdizione civile[406] e della giurisdizione penale[407], nonché la prestazione di tutti i servizi di assistenza sociale e di produzione di beni e servizi pubblici all'interno dell'economia. In tutti questi ambiti lo Stato ha interesse e necessità di fare riferimento ad un unico sistema monetario per garantire l'uniformità di trattamento e l'uguaglianza di fronte alla legge che caratterizzano lo stato di diritto.

[406] In cui, per effetto del principio della responsabilità patrimoniale personale, l'importanza della moneta si estende ben oltre i confini della gestione dei rapporti sinallagmatici volontari, sino a comprendere, in particolare, la materia del risarcimento del danno extracontrattuale, estremamente importante nella società moderna per la effettiva tutela dei diritti della persona.

[407] Sia nel suo risvolto repressivo, sia nella sua componente preventiva, in tutte le ipotesi di sanzione pecuniaria e di commutazione della pena detentiva.

Da questo punto vista, ci si può allora addirittura chiedere se la presenza di sistemi monetari concorrenti non infici l'esercizio delle funzioni pubbliche dello Stato moderno al punto da suggerirne il divieto. L'utilizzo di diverse unità di conto comporterebbe, infatti, un certo grado di segmentazione del vivere sociale entro sistemi di misurazione e di attribuzione del valore economico che rispondono a logiche e dinamiche diverse tra loro. In ipotesi di fluttuazioni di tali valori questo ostacolerebbe l'equiparazione delle situazioni personali e potrebbe compromettere la corretta applicazione del principio di uguaglianza tra tutti i cittadini, che è per converso resa possibile attraverso l'utilizzo di un unico sistema di riferimento per la misurazione dei valori economici all'interno dell'economia nazionale. Se ne conclude che è strutturalmente necessario che il corso legale sia applicato ad un unico sistema monetario e che la questione della meritevolezza di tutela di contratti denominati in unità di conto che in nessun ordinamento sono sorrette dal principio del corso legale è suscettibile di ulteriori approfondimenti e riflessioni.

In conclusione, i bitcoin costituiscono il primo modello concreto di un nuovo tipo di sistema monetario sostanzialmente avulso dal contesto dell'ordinamento giuridico e politico statale, la cui realizzazione è stata resa possibile dall'uso di una nuova tecnologia.

Il futuro della tecnologia *blockchain* è molto promettente, per il momento, la sua implementazione nei bitcoin ne ha permesso la resilienza, l'indipendenza dal sistema monetario tradizionale e un certo grado di successo commerciale. Al tempo stesso, le caratteristiche strutturali del sistema monetario bitcoin espongono questo strumento monetario a dinamiche speculative e a fluttuazioni di valore tali da comprometterne, almeno in parte, la capacità di essere usato diffusamente come misura del valore dei beni e dei servizi e come mezzo di scambi in rapporti di durata.

L'attuale instabilità dei bitcoin impedisce altresì che essi possano essere utilizzati da enti pubblici senza incorrere in un forte rischio di violazione del principio di uguaglianza. Il loro uso resta, dunque, circoscritto ad una porzione ristretta dell'economia e del vivere sociale, circoscritta agli scambi volontari sinallagmatici a prestazioni immediate. In questo contesto, specie in situazioni transfrontaliere o in cui l'anonimato delle parti è importante, i bitcoin possono assolvere a funzioni tipicamente esercitate dagli strumenti monetari tradizionali. È inoltre plausibile che la maggior parte delle transazioni in bitcoin risponda a finalità speculative di scommessa sull'aspettativa deflazionistica

legata alla limitazione della quantità complessiva di moneta che potrà circolare. Sotto questo profilo i bitcoin sembrano assolvere la funzione tipica di riserva di valore di un bene rifugio, piuttosto che quelle di una moneta.

Con queste considerazioni finali di sintesi si conclude il lavoro di elaborazione teorica e di analisi dei bitcoin come sistema monetario che ci si era proposti di compiere con questa tesi, nella consapevolezza che molte questioni possono essere ulteriormente approfondite e nella speranza che il lavoro possa essere utile per l'elaborazione di eventuali riflessioni e proposte in merito alla regolamentazione dei bitcoin o di sistemi simili e/o per l'elaborazione stessa di ulteriori modelli di sistemi monetari.

BIBLIOGRAFIA

AA.VV., *Bitcoin Developer Guide*, disponibile all'indirizzo https://bitcoin.org/en/developer-guide, (ultima visita 20 giugno 2017)

Ali R., Barrdear J., Clews R. e Southgate J., *Innovations in payment technologies and the emergence of digital currencies*, in *Bank of England Quarterly Bulletin*, Vol. 54, 2014, No. 3, pp. 262–75

– *The economics of digital currencies*, in *Bank of England Quarterly Bulletin*, Vol. 54, 2014, No. 3, pp. 276–86

Allara M., *Le nozioni fondamentali del diritto civile*, I, 5° ed., Giappichelli, 1958

Amato M. e Fantacci L., *Per un pugno di Bitcoin*, Università Bocconi Editore, 2016

Amenta V., *'Fourth generation' payment sistems: Bitcoins*, in *Ciberspazio e diritto*, vol. 15, 2014, p. 11

Andresen G., *Bitcoin. The World's First Person-to-Person digital currency*, 20 giugno 2011, disponibile all'indirizzo http://www.bitcointrading.com/pdf/GavinAndresenCIATalk.pdf (ultima visita 20 giugno 2017)

Antonopoulos A., *Mastering Bitcoin. Unlocking digital crypto currencies*, O'Reilly Media, 2015

Arangüena G., *Bitcoin: una sfida per policymakers e regolatori*, in *Quaderni di Diritto Mercato Tecnologia*, 2014, p. 19.

Arrighi G., *The Long Twentieth Century: Money, Power, and the Origins of Our Times*, Verso, 2010

Ascarelli T., *La moneta, considerazioni di diritto privato*, Cedam, 1928

– *Obbligazioni Pecuniarie*, in *Commentario al Codice Civile Scialoja-Branca*, Zanichelli, 1968 (1956)

Back A., *Hashcash - A Denial of Service Counter-Measure*, 2002, in http://www.hashcash.org/papers/hashcash.pdf (ultima visita 20 giugno 2017).

Baglioni A., *Il mercato monetario e la banca centrale. Liquidità bancaria, politica monetaria, sistemi di pagamento*, Bologna, Il Mulino, 2004

Banca Centrale Europea, *Virtual Currency Schemes*, 2012, disponibile sul sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (ultima visita 20 giugno 2017)

– *Virtual Currency Schemes – a further analysis*, 2015, disponibile sul sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (ultima visita 20 giugno 2017)

Banca d'Italia, *Comunicazione del 30 gennaio 2015*, in Bollettino di Vigilanza n. 1, gennaio 2015, p. II.15

Barcellona E., *Ius monetarium. Diritto e moneta alle origini della modernità*, Il Mulino, 2012

Barrdear J. e Kumhof M., *The macroeconomics of central bank issued digital currencies*, Bank of England Staff Working Paper No. 605, disponibile all'indirizzo http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf (ultima visita 20 giugno 2017)

Bayern S., *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, in *Walsh. & Lee L. Rev. Online*, vol. 71, 2014, p. 22

Bertarini B., *Valute virtuali: problematiche giuridiche e prospettive*, in *Innovazione e Diritto*, vol. 5, 2015, p. 40

Biella M. e Zinetti V., *Blockchain Technology and Applications from a Financial Perspective*, Unicredit, 2016.

Blanc J., *Beyond the quantity theory: a reappraisal of Jean Bodin's monetary ideas*, in Giacomin A. e Marcuzzo M.C. (a cura di), *Money and Markets. A doctrinal approach*, Routledge, 2007**,** pp. 135 ss

Blundell-Wignall A., *The Bitcoin Question: Currency versus Trust-less Transfer Technology*, OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing. Disponibile all'indirizzo http://dx.doi.org/10.1787/5jz2pwjd9t20-en (ultima visita 20 giugno 2017)

Boffito C., *Moneta*, in *Enciclopedia*, Einaudi, 1980

Brito J., Shadab H.B. e Castillo A., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling* (August 10, 2014), disponibile all'indirizzo http://ssrn.com/abstract=2423461 (ultima visita 20 giugno 2017)

Brownsword R. e Yeung K. (a cura di), *Regulating technologies*, Hart Publishing, 2008

Buterin V., *Bitcoin Network Shaken by Blockchain Fork*, pubblicato il 12 Marzo 2013, ore 11:14 PM EST, sul sito https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/ (ultima visita 20 giugno 2017).

Caetano R. *Bitcoin guida all'uso delle criptovalute*, Apogeo, 2016

Candiloro D., *La sicurezza informatica di bitcoin*, in *Ciberspazio e diritto*, 2015, 331

Capaccioli S., *Criptovalute e bitcoin: un'analisi giuridica*, Giuffré, 2015

Capoti D., Colacchi E. e Maggioni M., *Bitcoin revolution. La moneta digitale alla conquista del mondo*, Hopeli, Milano, 2015

Capriglione F., *Moneta*, in *Enc. del Dir.*, Giuffré, Agg. III, 1999

Cecchetti S.G. e Schoenholtz K.L., *Money, Banking, and Financial Markets*, McGraw-Hill Education, 4 ed., 2015

Chaum D., *Blind Signatures for Untraceable Payments*, in *Crypto* 82, 1982, 199–203 ..

– *Online Cash Checks*, 1989, disponibile all'indirizzo http://www.chaum.com/publications/Online_Cash_Checks.html 04/10/2016 (ultima visita 20 giugno 2017)

Chaum D., Fiat A. e Naor M., *Untraceable Electronic Cash*, in Goldwasser S. (a cura di), *Advances in Cryptology — CRYPTO' 88. Lecture Notes in Computer Science*, vol. 403, Springer, 1990

Committee on Payments and Market Infrastructures, *Digital currencies*, Bank for International Settlements, 2015

Crawford M.H., *La moneta in Grecia e a Roma*, Roma–Bari, Laterza, 1982

Cuffaro V. (a cura di), *Delle obbligazioni*. *Art. 1277-1320, Comm. Gabrielli,* tomo 3, UTET, 2013

Davidson L. e Block W.E., *Bitcoin, the Regression theorem, and the emergence of a new medium of exchange*, in *The Quarterly Journal of Austrian Economics,* n. 3, 2015, p. 18

De Soto Jesús Huerta, *Money, bank credit, and economic cycles*, Ludwig von Mises Institute, 3 ed., 2012,

Desan C., *Making Money: Coin, Currency, and the Coming of Capitalism*, Oxford University Press, 2014

– *Money as a legal institution*, in Fox. D. e Enrst W. (a cura di), *Money in the Western Legal Tradition,* Ofxord University Press, 2016

Di Majo A., *Obbligazioni pecuniarie*, in *Enc. Dir.*, XXIX, Giuffré, 1979, p. 226

– *Le obbligazioni pecuniarie*, Giappichelli, 1996

Dodd N., *The Social Life of Money*, Princeton University Press, 2014

European Banking Authority, *Opinion on 'virtual currencies'*, 2014, EBA/Op/2014/08

Fantacci L., *La moneta: storia di un'istituzione mancata*, Marsilio, 2005

Farenga L., *La moneta bancaria*, Giappichelli, 1997

Federal Bureau of Investigation, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*, 2012, disponibile all'indirizzo http://cryptome.org/2012/05/fbi-bitcoin.pdf (ultima visita 20 giugno 2017)

Felix M., *Money. The unauthorized biography*, Alfred A. Knopf, 2013 (e-book, ISBN 978-0-307-96244-7)

Ferro-Luzzi P., *Attività e "prodotti" finanziari*, in *Rivista di diritto civile,* 2010, p. 133

– *Lezioni di diritto bancario*, vol. 1, *Parte Generale*, 3° ed., Giappichelli, 2012

Finley H., *Detecting Double-Spending*, 15 Ottobre 1993, 2 ed. 13 Marzo 1996, pubblicato all'indirizzo

https://web.archive.org/web/20140410150152/http://www.finney.org/~hal/chcash2.html (ultima visita 20 giugno 2017)

Franco, P. *Understanding Bitcoin: Cryptography, Engineering and Economics*, John Wiley & Sons, 2014.

Fratini M., *Art. 1, 1° co., lett. U); co. 1-bis, lett. a), b), c); co. 1-ter; 2° co., Prodotti finanziari, valori mobiliari e strumenti finanziari*, in M. Fratini e G. Gasparri (a cura di), *Il testo unico della finanza*, t. 1, UTET, 2012

Frediani C., *Ho comprato un virus che infetta e ricatta i vostri pc. Vi spiego come funziona*, pubblicato il 30 marzo 2016 sulla versione on-line de La Stampa all'indirizzo http://www.lastampa.it/2016/03/30/italia/cronache/ho-comprato-un-virus-che-infetta-e-ricatta-i-vostri-pc-vi-spiego-come-funziona-4M7Po8sYe9X1cnuOLmvtCJ/pagina.html

Friedman M., *Commodity-Reserve Currency*, in *Journal of Political Economy*, Vol. 59, 1951, p. 202

Frisby D., *Bitcoin, The Future Of Money?*, Unbound, 2014

Gallino L., *Finanzcapitalismo, la civiltà del denaro in crisi*, Einaudi, 2011

– *Il colpo di Stato di banche e governi: l'attacco alla democrazia in Europa*, Einaudi, 2013.

– *Il denaro, il debito e la doppia crisi*, Einaudi, 2015

Gasparri G., *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di problema?*, in *Il diritto dell'informazione e dell'informatica*, 2015, p. 415

Genta F., *Con il virus "Cryptolocker" estorcevano denaro on line ad aziende e privati*, La Stampa, 9 luglio 2015, http://www.lastampa.it/2015/07/09/italia/cronache/con-il-virus-cryptolocker-estorcevano-denaro-on-line-ad-aziende-e-privati-07KemCX4Ug0cDWZEf4wvRI/pagina.html (ultima visita 20 giugno 2017)

Giacomin A. e Marcuzzo M.C. (a cura di), *Money and Markets. A doctrinal approach*, Routledge, 2007

Giannini C. *L'età delle banche centrali: forme e governo della moneta fiduciaria in una prospettiva istituzionalista*, Il Mulino, 2004

Goodhart C., *The Two Concepts of Money: Implications for Optimal Currency Areas*, in *European Journal of political economy*, 14, 1998, pp. 407-432

Graeber D., *Debito: i primi 5000 anni*, Il saggiatore, 2012

Graf K.S., *On The Origins Of Bitcoin. Stages Of Monetary Evolution*, 3 novembre 2013, disponibile online all'indirizzo https://konrad-graf.squarespace.com/s/On-the-Origins-of-Bitcoin-Graf-031113.pdf

Gregory C. A., *Savage Money: The Anthropology and Politics of Commodity Exchange*, Harwood Academic, 1997

Grinberg R., *Bitcoin: An Innovative Alternative Digital Currency*, in *Hastings Science & Technology Law Journal*, Vol. 4, 2012, p. 160

Gruber S., *Trust, identity and disclosure: are bitcoin exchanges the next virtual havens for money laundering and tax evasion?*, in *Quinnipiac law review*, vol. 32, 2013, p. 135

Guttmann B., *Bitcoin. Guida completa*, LSWR, 2014

Hart K., *Money in an Unequal World: Keith Hart and His Memory Bank*, Textere, 2001.

Hayek F.A., *Denationalisation of money. The argument refined : an analysis of the theory and practice of concurrent currencies*, The Institute of Economic Affairs, 2 ed. , 1978

Ingham G., *Schumpeter and Weber on the Institutions of Capitalism*, in *Journal of Classical Sociology*, 2003, pp. 297 ss.

– *The Nature of Money*, Polity, 2004

Inzitari B., *Obbligazioni Pecuniarie*, in *Commentario al Codice Civile Scialoja-Branca*, Zanichelli, 2011

Jeans E.D., *Funny money or the fall of fiat: bitcoin and forward-facing virtual currency regulation*, in *Journal on Telecommunication & High Technology Law*, vol. 13, 2015, p. 99

Kancs d'A., Ciaian P. e Rajcaniova M., *The Digital Agenda of Virtual Currencies: Can BitCoin Become a Global Currency?*, European Commission Joint Research Centre, Institute for Prospective Technological Studies, Luxemburg, Publications of the European Union, 2015 (Report EUR 27397 EN)

Kaplanov N.M., *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, in *Loyola Consumer Law Review*, 2015, vol. 25, pp. 111 ss.

Keynes J.M., *La riforma monetaria*, Feltrinelli, 1975

Kien M. e Meng L., *Coining Bitcoin's «Legal-Bits»: Examining The Regulatory Framework For Bitcoin And Virtual Currencies*, in *Harvard Journal of Law & Technology*, vol. 27, 2014, p. 587

Knapp G.F., *The State Theory of Money*, Macmillan & Company Limited, 1924

Kondor D., Pósfai M., Csabai I. e Vattay G., *Do the rich get richer? An empirical analysis of the Bitcoin transaction network*, in *PLoS ONE*, vol. 9, 2014, p. 1

Krawisz D., *Bitcoin is the Best Unit of Account*, 10 maggio 2014, pubblicato on line e disponibile sul sito http://nakamotoinstitute.org/mempool/bitcoin-is-the-best-unit-of-account/ (ultima visita 20 giugno 2017).

– *Bitcoin as a Store of Value, Unit of Account, and Medium of Exchange*, 12 gennaio 2015, pubblicato on line e disponibile sul sito: http://nakamotoinstitute.org/mempool/bitcoin-as-a-store-of-value-unit-of-account-and-medium-of-exchange/ (ultima visita 20 giugno 2017);

Kreitner R., *The Jurisprudence of Global Money*, in *Theoretical Inquiries in Law*, vol. 11, 2010, p. 177.

Lamport L., Shostak R, e Marshall P., *The Byzantine Generals Problem*, in *ACM Transactions on Programming Languages and Systems*, n. 4(3), 1982, pp. 382-401.

Langois R.N. (a cura di), *Economics as process*: *essays in the new institutional economics*, Cambridge University Press, 1990

Lee D.K.C. (a cura di), *Handbook of digital currency. Bitcoin, innovation, financial instruments and big data*, Elsevier, 2015

Lemme G. e Peluso S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Rivista di Diritto Bancario*, dirittobancario.it, 2016, p. 43

Lessig L, *Code. Version 2.0*, Basic Books, 2006

Lumini C., *La continuità dei contratti alla prova dell'euro*, in *Riv. Notariato*, 1998, f. 1-2, pt. 1, pp. 27-54

Mancini M., *Valute virtuali e Bitcoin*, in *Analisi Giuridica dell'Economia*, 2015, pp. 117 ss.

Mancini N., *Il nuovo assetto normative dei servizi di pagamento*, in *Banca, Impresa e Società*, 2013, p. 139

Mankiw N.G., *Macroeconomics*, Worth Publishers, 6 ed., 2007

Marchetta D., *La moneta*, in *Diritto amministrativo speciale, tomo terzo, I servizi pubblici finanza pubblica e privata*, in *Trattato di Diritto Amministrativo*, a cura di Sabino Cassese, Giuffré, 2003, pp. 3035 ss.

Marini P. e Marc F., *Rapport d´information fait au nom de la commission des finances sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles*, Senato della Repubblica Francese, Sessione straordinaria del 2013-2014, N° 767 rectifié, Enregistré à la Présidence du Sénat le 23 juillet 2014

May T., *The Crypto Anarchist Manifesto*, 1988, disponibile all'indirizzo http://nakamotoinstitute.org/crypto-anarchist-manifesto/ (ultima visita 20 giugno 2017)

– *Crypto anarchy and virtual communities*, 1994, disponibile all'indirizzo http://nakamotoinstitute.org/virtual-communities/

– *The Cyphernomicon*, 1994, disponibile all'indirizzo http://nakamotoinstitute.org/static/docs/cyphernomicon.txt (ultima visita 20 giugno 2017)

Meggiato R., *Il lato oscuro della Rete: Alla scoperta del Deep Web e del Bitcoin*, Apogeo Editore, 2014.

Menger C., *On the Origin of Money*, in *The Economic Journal*, 2, 1892, pp. 239-255

– *Principles of Economics*, Ludwig von Mises Institute, 2007

Mishkin F.S., Giuliodori M. e Matthews K., *The Economics of Money, Banking, and Financial markets (European Edition)*, Pearson Education Limited, 7 ed., 2013

Mitchell Innes, A., *What Is Money?*, in *Banking Law Journal*, 1913, 30(5), 377–408

– *The Credit Theory of Money* in *Banking Law Journal*, 1914, 31(2), 151–168

Nakamoto S., *Bitcoin P2P e-cash paper*, messaggio del 31–10–2008, disponibile al sito http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html (ultima visita 20 giugno 2017)

– *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, disponibile all'indirizzo https://bitcoin.org/bitcoin.pdf (ultima visita 20 giugno 2017).

– *Re: Bitcoin P2P e-cash paper 2008-11-07 12:30:36 UTC*, disponibile all'indirizzo http://satoshi.nakamotoinstitute.org/emails/cryptography/4/ (ultima visita 20 giugno 2017)

– *Re: Bitcoin P2P e-cash paper 2008-11-09 14:13:34 UTC*, disponibile all'indirizzo http://satoshi.nakamotoinstitute.org/emails/cryptography/6/ (ultima visita 20 giugno 2017)

– *Re: Bitcoin v0.1 released 2009-01-17 09:58:44 UTC*, disponibile all'indirizzo http://satoshi.nakamotoinstitute.org/emails/cryptography/17/ (ultima visita 20 giugno 2017)

– *Bitcoin open source implementation of P2P currency*, pubblicato 11 febbraio 2009, ore 22:27, in http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (ultima visita 20 giugno 2017)

– *Re: Bitcoin does NOT violate Mises' Regression Theorem*, commento pubblicato il 27 Agosto *2010, 05:32:07 PM*, sul sito https://bitcointalk.org/index.php?topic=583.0 (ultima visita 20 giugno 2017)

– *Added some DoS limits, removed safe mode (0.3.19)*, pubblicato il 12 dicembre 2010, sul sito

https://bitcointalk.org/index.php?topic=2228.msg29479#msg29479 (ultima visita 20 giugno 2017)

Nathan A. (a cura di), *All about Bitcoin*, in *Top of mind*, Goldman Sachs Global Investment Research, n. 11, 2014

Norrbin S. e Melvin M., *International Money and Finance*, Elsevier, 8 ed., 2013

Nussbaum A., *Das Geld in Theorie und Praxis des deutschen und auslandischen Rechts*, J. C. B. Mohr, 1925

– *Money in the Law, National and International. A comparative study in the borderline of law and economics*, The Foundation Press Inc., 1950

Olivecrona K., *La struttura dell'ordinamento giuridico*,Etas Kompass, 1972

Parlamento Europeo, *Distributed ledger technology and financial markets*, 2016, European Parliamentary Research Service (a cura di Angelos Delivorias), PE 593.565

Pasquale F., *The black box society*, Harvard University Press, 2015

Pigou, A.C., *The veil of Money*, Macmillan, 1949

Pini R., *Il denaro pubblico*, vol. I, *Problemi generali*, Cedam, 1984

Pitta J., *Requiem for a Bright Idea*, 11 gennaio 1999, in https://www.forbes.com/forbes/1999/1101/6411390a.html (ultima visita 20 giugno 2017)

Plassaras N.A., *Regulating digital currencies: bringing bitcoin within the reach of the IMF*, in *Chicago Journal of international Law*, vol. 14, 2013, p. 377

Proctor C., *Mann on the Legal Aspect of Money*, Oxford University Press, 7 ed., 2012

Radford R.A., *The economic organization of a POW camp*, in *Economica*, 1945, 189

Resnick P., *On Consensus and Humming in the IETF*, in Internet Engineering Task Force (IETF), RFC n.7282 giugno 2004

Sacco R. e Rossi P., *Introduzione al diritto comparato*, in "Trattato di Diritto Comparato", diretto da R. Sacco, UTET, 2015

Sáinz de Vicuña A., *An institutional theory of money*, in Giovanoli M. e Devos D. (a cura di), *International monetary and financial law*, Oxford University Press, 2010, pp 517 ss.

Scalcione R., *Gli interventi delle autorità di vigilanza in materia di schemi di valute virtuali*, in *Analisi Giuridica dell'Economia*, 2015, 1, p. 139

Schiaroli I.W., *Dark web & bitcoin: la nuova era della rete*, Lantana, 2012.

Schumpeter J., *A history of economic analysis*, Routledge, 1994 (trad. it. *Storia dell'analisi economica*, Torino, Boringhieri, 1960)

Semeraro M., *Pagamento e forme di circolazione della moneta*, Edizioni Scientifiche Italiane, 2008

Simpson T.D., *Financial Markets, Banking and Monetary Policy*, Wiley, 2014

Spagnuolo M., Maggi F., Zanero S., *BitIodine: Extracting Intelligence from the Bitcoin Network*, in *Financial Cryptography and Data Security*. *18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, a cura di M. Brenner, Springer, 2014 (anche in http://fc14.ifca.ai/papers/fc14_submission_11.pdf)

Sraffa P., *The works and Correspondence of David Ricardo*, vol. 1, Cambridge University Press, 1951

Stammati G., *Moneta*, in *Enc. del Dir.*, Giuffré, XXVI, 1976

Szabo N., *The God Protocols*, 1997, disponibile all'inirizzo http://nakamotoinstitute.org/the-god-protocols/ (ultima visita 20 giugno 2017)

– *Secure Property Titles with Owner Authority*, 1998, originariamente pubblicato su http://szabo.best.vwh.net/securetitle.html (non più accessibile), ora disponibile all'indirizzo: http://nakamotoinstitute.org/secure-property-titles/ (ultima visita 20 giugno 2017)

– *Trusted Third Parties Are Security Holes*, 2001, originariamente pubblicato in http://szabo.best.vwh.net/ttps.html (non più accessibile), disponibile all'indirizzo http://nakamotoinstitute.org/trusted-third-parties (ultima visita 20 giugno 2017)

– *Shelling Out -- The Origins of Money*, 2002, originariamente pubblicato in http://szabo.best.vwh.net/shell.html (non più accessibile), oggi disponibile all'indirizzo http://nakamotoinstitute.org/shelling-out/ (ultima visita 20 giugno 2017)

– *Advances in Distributed Security*, 2003, disponibile all'indirizzo http://nakamotoinstitute.org/advances-in-distributed-security (ultima visita 20 giugno 2017)

– *Scarce Objects*, 2004, disponibile all'indirizzo http://nakamotoinstitute.org/scarce-objects/ (ultima visita 20 giugno 2017).

– *Bit Gold*, 2005, disponibile all'indirizzo: http://unenumerated.blogspot.it/2005/12/bit-gold.html (ultima visita 20 giugno 2017)

Turpin J. B., *Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework*, in *Indiana Journal of Global Legal Studies*, 2014, vol. 21, p. 335

Twoney P., *Halting a shift in the paradigm: the need for bitcoin regulation*, in *Trinity College Law Review*, vol. 16, 2013, p. 67

U.K. Government Chief Scientific Adviser, *Distributed Ledger Technology : beyond block chain*, 2016 (a cura di Mark Peplow), disponibile al sito www.gov.uk/go-science (ultima visita 20 giugno 2017)

Vardi N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Il Diritto dell'informatica e dell'informazione*, 2015, p. 443

Von Mises L., *The Theory of Money and Credit*, Jonathan Cape, 1912

Wei Dai, *b-money*, 1 Novembre1998, in http://www.weidai.com/bmoney.txt (ultima visita 20 giugno 2017), disponibile anche in http://nakamotoinstitute.org/b-money/ (ultima visita 20 giugno 2017)

Will Rodger, *R.I.P. Cypherpunks*, in *SecurityFocus*, 2001-11-29, disponibile all'indirizzo http://www.securityfocus.com/news/294 (ultima visita 20 giugno 2017)

Williamson O.E., *The new institutional economics: taking stock, looking ahead*, in *Journal of Economic Literature*, 2000, p. 599

Wray L. R., *From the State Theory of Money to Modern Money Theory: An Alternative to Economic Orthodoxy*, Levy Economics Institute Working Paper n. 792, 2014

XC, *Bitcoin does NOT violate Mises' Regression Theorem*, post pubblicato il 27 luglio 2010, 02:09:27 AM, sul sito https://bitcointalk.org/index.php?topic=583.0 (ultima visita 20 giugno 2017)

INDICE