Blockchain-Based Money as the Ultimate Challenge to Sovereignty: Reflections from a Public Economic Law Perspective

Published version:

DOI:10.1163/22134514-00602004

Blockchain-Based Money as the Ultimate Challenge to Sovereignty: Reflections from a Public Economic Law Perspective

Riccardo de Caria [Assistant Professor of Comparative Public Law, University of Torino]

Abstract

The article considers the radical challenge that blockchain, and in particular the blockchain-based cryptocurrency Bitcoin, poses to state sovereignty. If blockchain ever succeeds to be adopted on a large scale, Bitcoin, or any other permissionless blockchain-based cryptocurrency for that matter, is a direct threat to one of the key tenets of sovereignty: the monopoly over money. Without this traditional monopoly, states will not be able to exist as they have so far. Building on this premise, the article argues that blockchain-based money is currently posing a serious challenge to state sovereignty and could therefore reshape public law.

This article also contends that Bitcoin in particular might collapse for technical reasons. However, if Bitcoin proves to be resilient enough to resist ongoing legal challenges, then the very "*basic norm*" of our legal systems will arguably change.

Keywords

blockchain; Bitcoin; cryptocurrencies; sovereignty; central banking; fiat money; permissionless; public economic law

1 Revolutionary by design: the invention of the (permissionless) blockchain and the challenge to the state monopoly over money

A significant part of the scientific literature on blockchain and Bitcoin refers to these extraordinary technological innovations as great opportunities.[1] While this enthusiasm is arguably to be endorsed, I would like to concentrate in this article instead on the opposite argument, namely on the aspects that make blockchain at the same time a considerable threat. Indeed, blockchain and Bitcoin, the cryptocurrency based on the incumbent blockchain,[2] pose a considerable threat to many traditional public institutions. Several of these institutions characterize the inner structure of many legal orders and thus of their public law. If these technologies succeeded in achieving the mass adoption that many envision[3]--which could happen even if Bitcoin happened to collapse,[4] many intermediary roles played by the central government could be threatened.[5] For example, the registration of land by certified notaries or the collection of royalties by official entities in the context of the protection of intellectual property rights.[6] In both cases these entities are vested with public powers and are an extension of state sovereignty.

---

[1] Among many, see for instance P.C. Mullan, *The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations* (Palgrave Pivot: New York, 2014), pp. 146-148 (the chapter entitled *Bitcoin Opportunity*).

[2] I will refer to it here as the cryptocurrency par excellence, but the discourse is applicable to any cryptocurrency sharing its essential characteristics, should it prevail in the future (in particular, its permissionless nature, on which see below, note 7). I will also refer to Bitcoin as the uttermost application of the blockchain, as it is the most relevant for the purposes of this article.

[3] See for instance the assessment by A.W. Baur, J. Bühler, M. Bick, C.S. Bonorden, "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co.", in: M. Janssen et al. (eds.), *Open and Big Data Management and Innovation. I3E 2015. Lecture Notes in Computer Science, vol 9373* (Cham: Springer, 2015) pp. 63-80. See also further references below, in note 43.

[4] For a reflection along these lines, see for instance M. O'Donnell, "Beyond bitcoin", in *Policy: A Journal of Public Policy and Ideas*, Vol. 34, No. 1, Mar 2018: 30-33.

[5] See for example J. Brito, A. Castillo, *Bitcoin. A Primer for Policymakers* (Arlington, VA: Mercatus Center, George Mason University) pp. 3-10.

[6] Both the Latin notary publics and collecting societies in the music industry act as middlemen to facilitate transactions: they lower the costs of the transactions in which they are involved, and they do so thanks to their public law authority, that makes their acts official and legally binding. According to many experts, the blockchain might provide a viable alternative to their role, without the need for public law powers in order to gain trust for the system to work: see for instance M. Crosby et al., "BlockChain Technology: Beyond Bitcoin", *Applied Innovation Review*, Issue No. 2, June 2016, 6 ff., in particular at 14-16.

This threat comes only from permissionless blockchains, that is, a "type of blockchain [that] is public and is open to all[, whereby] [t]he participant must have resources like computing power and software to validate transactions. […]. In other words, it means that anyone in the network (nodes) can join the network and validate the blocks, anyone can read the chain and add new blocks to it."[7] It can be argued that this version of blockchain is the one that is truly potentially disruptive for a key component of state sovereignty and public law.

In many cases, the threat to the middlemen or public central authorities was probably never the explicit intention of those who gave life to blockchain technology. Instead, the idea of many blockchain systems is to support multiple public tasks. There is nonetheless a field of public law in in which the challenge to the status quo has been expressed from the very beginning: the regulation of money.[8] Bitcoin and the (permissioned) blockchain, which is famously its fundamental technical

[7] This is the explanation offered by the T.K. Sharma, *Advantages and Disadvantages of Permissionless Blockchian* for the Blockchain Council (3 October 2018, retrieved 29 March 2019, www.blockchain-council.org/blockchain/advantages-and-disadvantages-of-permissionless-blockchain/); permissionless blockchains oppose to permissioned ones, i.e., again in Sharma's words, "system[s] […] based on a consortium of trusted validators. One needs the authorization to read the information in the chain which is not the case with permissionless blockchain."

[8] I draw this conclusion from the White paper by S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", bitcoin.org/bitcoin.pdf, retrieved 15 December 2018, and in particular from the following statement at p. 2: «The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received». The founder, or the founders of Bitcoin were therefore fully aware of the relevance of their initiative from the point of view of the potential alternative they were building to fiat money issued by central banks.

infrastructure, were born with the precise intention of offering a technological and market alternative to legal tender money, object of public monopoly by the states.[9]

Our current era of global markets is characterized by the partial erosion of some state prerogatives that, at least from 1648 onwards, constitute the most typical manifestations of sovereignty.[10] The public control of money remains one of the essential cornerstones of the latter. In Europe nineteen States have agreed to transfer such power to an authority – the European Central Bank ('ECB'). This supra-national institution is placed at a higher than the nation states. The transferral of powers from the state to other entities has happened in a framework of continuity, but money has remained subject to public monopoly. Even though the EU is certainly not a sovereign state under international law definitions,[11] its control over the issuance of the Euro currency – through the ECB – is an exercise of sovereign powers that were relinquished by nation states in its favour, as part of an ongoing shift of sovereign prerogatives to the EU level.

The transfer of the monopoly power from the Member States to the ECB has not altered the tight public law hold over money: the public monopoly over money remains thus very well established,

---

[9] This conclusion seems to receive confirmation by the message embedded by Satoshi Nakamoto in the so called "genesis block", i.e. "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." As explains J. Davis, "The Crypto-Currency. Bitcoin and its mysterious inventor", *The New Yorker*, October 10, 2011 issue, "This is a reference to a Times of London article that indicated that the British government had failed to stimulate the economy. Nakamoto appeared to be saying that it was time to try something new. The text, hidden amid a jumble of code, was a sort of digital battle cry."

[10] Arguably one of the best studies of the notion of sovereignty is the book by B. de Jouvenel, *Sovereignty: An Inquiry Into the Political Good* (Translated by J.F. Huntington, Chicago: The University of Chicago Press, 1957 [1955]); the classic reference is obviously to J. Bodin, *Six Books of the Commonwealth* (Abridged and translated by M.J. Tooley, Oxford: Blackwell's Political Texts, 1955 [1576]); on the current downsize of the reach of the powers entailed by national sovereignty, see for instance S. Sassen, *Losing Control?: Sovereignty in the Age of Globalization* (New York: Columbia University Press, 1996), and M. Loughlin, "The Erosion of Sovereignty", *Neth. J. Legal. P.* 45(2) (2016) 57.

[11] For an enlightening discussion of this point, see T.C. Hartley, *The Foundations of European Union Law* (Oxford: Oxford University Press, 2014, 8th edn).

also in Europe. The Bitcoin revolution could nonetheless disrupt this scenario, inevitably altering the shape and boundaries of public law.

In this article, I will first take the United States and Europe as paradigmatic examples and will examine the rules that regulate the public monopoly of money in these legal systems.[12] I shall focus on the meaning and the value of this monopoly (§ 2). I will then illustrate the scope of the legal challenge that issuing money based on a permissionless blockchain has launched (§ 3). In the concluding part of this article, I will consider the different possible outcomes of a scenario that has the potential of giving rise to multiple legal clashs, and will discuss the power struggle with all the relative broader implications for public economic law and public law in general (§ 4).

2 The laws establishing the public monopoly over money, and their significance

Money is a product of human activity, which historically was born as a market response to a series of practical needs.[13] Nobody in particular invented money or regulated it at its outset, but this occurred naturally in different countries and throughout history. The regulation of money happened by virtue of some of its intrinsic characteristics, including its physical nature,[14] which enabled them to respond satisfactorily to the three traditional functions of money: reserve of value, unit of account and means of exchange.

Metals, and above all gold, have earned the greatest favour of currency and exchange operators, who have elected them as privileged material for the production of money. From the metals, then,

---

[12] I maintain that Europe can and should be looked at, for our purposes, as a legal system, for the reasons and with the specifications made just above in the text: the Eu has inherited its powers in this area from nation states, so it has acquired from them a fundamental element of their sovereign powers.

[13] See the seminal work by L. von Mises, *The Theory of Money and Credit* (New Haven, CT: Yale University Press, 1953 [1912]).

[14] M.N. Rothbard, *What Has Government Done to Our Money?* (Auburn, AL: Ludwig von Mises Institute) (2005, fifth edn. [1963]).

the modern financial system has evolved in the direction of paper money, namely (at the origins) paper titles that represented physical gold.[15] Although the awareness has largely been lost, it should not be surprising that money has long been the subject of competition among the various subjects that issued it.[16] Currencies were in competition with each other, from the point of view of their greater or lesser reliability, regarding the correspondence between the face value declared, and the actual quantity of precious metal contained. The competition was then transferred to the banknotes that represented the gold deposited, whose holders were entitled to the conversion into gold of the quantity represented in them, from the point of view of the greater or lesser reliability of the issuer.[17]

For a series of historical reasons, which I have investigated elsewhere,[18] the progressive extension of states' powers went through a similar process in various systems. This process involved the gradual acquisition by the states themselves of control over money, since governments perceived the crucial and instrumental character of currency for the pursuit of their objectives. The public monopoly over money has thus become of comparable importance to the Weberian public monopoly on the legitimate use of force, because the control of money allows the state to alter the fundamental values of the economy and thus make its policies financially sustainable in the short-medium term.

In the United States, the path leading to the acquisition of the public monopoly of money is paradigmatic. This project was first carried out through an attack to gold, which – through a series of steps – eventually went as far as its requisition by the state, and its ban as a means of payment.[19]

---

[15] L. von Mises, *supra* note 13; M.N. Rothbard, *supra* note 14.
[16] L. von Mises, *supra* note 13; M.N. Rothbard, *supra* note 14.
[17] See D.S. Schlichter, *Paper Money Collapse: The Folly of Elastic Money, Second Edition* (Hoboken, NJ: Wiley) (2014).
[18] R. de Caria, "Quando il diritto altera la realtà", *Diritto Pubblico Comparato ed Europeo*, 14(4) (2012) 1621-1660.
[19] R. de Caria, *supra* note 18.

The only legitimate money became the one that was approved, or better issued, by the state. And if initially, this money retained at least a link with gold, in which it was guaranteed to be convertible, with the watershed moment of the abandonment of the gold standard, this last link was also lost, and the process of creation of fiat money was eventually accomplished.[20]

This turned out to be essential for states, representing the only possible remedy for them to cope with the debts arising from the many wars waged, as well as to pursue the ever increasing tasks undertaken with the advent of the welfare state. The combination of wars and welfare has therefore made the financial requirements of the states skyrocket. This made a financial system exclusively based on free market money unsustainable, and led states to perceive the need to take control over money in order to maintain their structure.[21]

The European story is in many ways similar. The European Union has inherited the monopoly on money from individual Member States, which had won it by a process comparable to the one that took place in the US. Thus, today, the ECB is the only institution in the Euro area authorized to establish the value of money with legal tender: in fact this institution is the one that has the unquestionable power to establish the quantity of euros that are placed on the market from which their relative value derive. The ECB is constitutionally disciplined only to a minimal extent.[22] Private parties cannot easily escape the public monopoly on money, since everyone has to pay taxes in euros, and creditors must accept payments in euros, under penalty of incurring in the penalties for

---

[20] R. de Caria, *supra* note 18. The assumptions at the basis of this article are derived from Austrian economic thinking (see the comprehensive collection by L.H. Rockwell (Ed.), *The Gold Standard: Perspectives in the Austrian School*, Auburn: Mises Institute, 1992): in this line of thought, gold standard is a (however suboptimal) safeguard against currency debasement by the government. A completely opposite view is the one advocated by J.M. Keynes, who (in)famously referred to the gold standard as a “barbarous relic” (J.M. Keynes, *A Tract on Monetary Reform*, London: MacMillan, 1923, 172); in a similar vein, more recently, see the attack launched by A. Pettifor, *Why the euro is the gold standard writ large – and like the gold standard, will fail*, Prime, 30 July 2015.

[21] Also due to the so called Cantillon effect, on which see M. Thorton, “Cantillon on the Cause of the Business Cycle”, *The Quarterly Journal of Austrian Economics* 9(3) (Fall 2006) 45–60.

[22] R. de Caria, *supra* note 18, pp. 1642-1647.

"*mora credendi*."[23] Admittedly, one could denominate contracts in different currencies, but in a world of fiat currencies, and with no more gold standard, this does not change at all the substance of the argument just put forward.

Of all the components of sovereignty, control over money appears to be one of the most central and indispensable: in the meantime, warfare continues to have its costs, on both sides of the Atlantic. However, welfare has continued to widen the boundaries of public intermediation, and therefore the governments' thirst for resources. The state could never spontaneously renounce to such power, because it is essential to the development of its other powers, and any different scenario, such as the one famously envisioned by Hayek in his 1976 book on *The Denationalization of Money*,[24] of private currencies returning to being in competition, would not be acceptable for the state.

The public monopoly of money is therefore co-essential to sovereignty and statehood: *simul stabunt, simul cadent* or you cannot have one without the other, since evidently the former derives from the monopoly on the legitimate use of force that also makes possible the enforcement of the monopoly over money, but also vice versa, since sovereign states would not hold up without fiat money[25].

[23] For instance, *see* Article 1206 of the Italian civil code: "The creditor is deemed to be in delay when, without a legitimate reason, he refuses to receive the payment offered to him pursuant to the procedures laid out in the following articles, or does not do what is necessary for the debtor to comply with her obligations."

[24] F. von Hayek, *The Denationalization of Money* (London: Institute of Economic Affairs, 1976); see also his *Monetary Nationalism and International Stability* (Eastford, CT: Martino Fine Books, 2012 [1937]).

[25] Admittedly, central bank money accounts for only a minor fraction of all the monetary based, that also includes, for instance, commercial bank money. However, it is still the government that decides in a binding way what amounts to money and what does not, so there is arguably no; in summary, the currently mainstream accounts of money creation are fundamentally misguided (for instance by M. McLeay, A. Radia and R. Thomas, "Money creation in the modern economy", *Bank of England Quarterly Bulletin* 2014 Q1, 14 ff. or by A. Pettifor, *The Production of Money: How to Break the Power of Bankers* (London-New York, Verso Books, 2017), while the account put forward by Austrian school's appears much more persuasive (see, among many, C. Menger, *On the Origins of Money*,

3 Bitcoin (and cryptocurrencies) as the ultimate challenge to sovereignty

If it is true that fiat money and sovereignty are mutually dependent on each other, any reform of the current system seems impractical. As mentioned in the previous section, the scenario of denationalization of money envisioned by Hayek is particularly difficult to achieve, if we consider setting up mechanisms of democratic or jurisdictional control similar to those used by the operations of central banks.[26] The topic also enjoys a prominent position in the current political agenda of the United States, where President Trump has made the Federal Reserve Bank the subject of major attacks because in his opinion it has been too restrictive in its monetary policy in recent years.[27] It seems that President Trump is trying to politicize the Federal Reserve so as to further pursue his objectives. It does not seem, therefore, that politics – on either side – support the thesis, which seems to me preferable, of those who instead invoke – even in the largely imperfect scenario as the one of the current monopoly – much more conservative policies directed at containing monetary inflation.[28]

This scenario appears to be repeated in a similar way in all modern democracies: in the United States as well as in the EU, but also in Japan, which has also experienced many years of ultra-expansive

Economic Journal 2 (1892), 239, and L. von Mises, *supra* note 13). Not surprisingly, Pettifor severely criticizes Hayek's theories (see for instance her interview to Dr Ian Cosh published in the MISC magazine, available at miscmagazine.com/future-money-interview-ann-pettifor-2/, last retrieved 2 April 2019).

[26] R. de Caria, "Alla ricerca del *remedy*: il difetto di tutela giurisdizionale contro alcune fondamentali decisioni in materia economico-finanziaria e alcune possibili contromisure", in: A. Sciarrone Alibrandi (ed.), *Atti del Convegno Annuale dell'Associazione dei Docenti di Diritto dell'Economia svoltosi a Trento il 30 novembre e 1 dicembre 2017* (Torino: Giappichelli, 2018) pp. 81-102.

[27] See for instance *Federal Reserve: Trump sharpens attack on central bank*, 24 October 2018, retrieved 15 December 2018, www.bbc.com/news/business-45961465.

[28] I advocated for this position in R. de Caria, "*Perseverare diabolicum*: the shortcomings of pre-crisis financial regulation, and the repetition of the same mistakes in the regulatory response to the crisis", *Revista da Associação Mineira de Direito e Economia*, no. 10-2013 (2013).

monetary policies, with largely unsatisfactory economic results.[29] Bearing this in mind, it would come as no surprise to learn that the intuition of Bitcoin as a proposal for alternative money, completely disengaged from the legitimization circuit of states and central banks, was indeed born in Japan, as the speculation goes[30].

Bitcoin emerged thanks to the extraordinary possibilities made available by technological evolution, and would not exist without it. It exploits these possibilities in a brilliant way and realizes, thanks to the contributions of a scientific-mathematical discipline such as cryptography, a form of money whose value depends only – exactly as for gold – on the value that users are willing to award to it, spontaneously and without any constraint.

The lack of materiality of Bitcoin has made some point out that, unlike gold, it would not have an intrinsic value, and therefore this value would be purely abstract and virtual.[31] I would contend that this thesis should be rejected because it is based on a flawed premise: even gold, in fact, has no "intrinsic value", an economics concept considered outdated,[32] and the fact that it is materialized in a physical medium does not change in any way this fact. The virtuality of Bitcoin and, for that matter, of other cryptocurrencies does not make Bitcoin different from gold from the point of view considered here.

What is realized with Bitcoin is therefore the possibility of creating a store of value, a unit of account and, under certain conditions, also a means of exchange, whose existence and maintenance depend

[29] See B. Powell, "Explaining Japan's Recession", *The Quarterly Journal of Austrian Economics* 5(2) (Summer 2002) 35–50.

[30] The hypothesis relies on the self-description by Satoshi Nakamoto on his profile on the P2P foundation's website, last retrieved 29 March 2019, p2pfoundation.ning.com/profile/SatoshiNakamoto.

[31] Among those who voiced this critique, there is former Fed Chairman Alan Greenspan: see the following rebuttal: M. Mihaly, "Bitcoin and Intrinsic Value: a Layman's Response to Alan Greenspan", 11 December 2013, retrieved 15 December 2018, www.coindesk.com/bitcoin-intrinsic-value-alan-greenspan.

[32] See, above all, C. Menger, *Principles of Economics* (Auburn, AL: Ludwig von Mises Institute, 2007 [1871]), Chapter III, *The Theory of Value*, pp. 114-174.

entirely on intrinsic requirements of validity. This development does not openly go *against* the State, but it launches a novel challenge: cryptocurrencies go *beyond* the State, in the sense that they are independent of it. Bitcoin is a form of money that can exist beyond the sovereign State, and that is in fact a potential candidate for its replacement as far as the money monopoly is concerned. Bitcoin is able to function peacefully even in the absence of any state framework.

In this regard, it appears very interesting, from the point of view of public law, the way in which decisions are made regarding the development of the blockchain and the protocol on which Bitcoin is based, i.e. the so called Bitcoin governance. The various forks,[33] the SegWit,[34] the creation of patches to cover potential bugs[35] are all phenomena subject to entirely private decisions,[36] typical of a world potentially devoid of statehood, whereby fundamental decisions do not need to go through the normal public law procedures. In this world, the political organization also takes different forms from the ones we have become acquainted with, returning to past forms of aggregation, or evolving into new forms that have not been previously put in practice.[37]

---

[33] See for instance F. Tschorsch, B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies"(2016) 18 (3) *IEEE Communications Surveys & Tutorials* 2084-2123.

[34] See T. Revell, "The toss of a coin" (2017) 234 *New Scientist* 22-23.

[35] For an analysis of how this this takes place, see J. Bohr, M. Bashir, "Who Uses Bitcoin? An exploration of the Bitcoin community", in: A. Miri et al. (eds.), *Proceedings of Twelfth Annual Conference on Privacy, Security and Trust (PST)*, (New York: IEEE Press, 2014), pp. 94-101

[36] From this perspective, the fact that some miners can play a disproportionate role in the community, and thus that the consensus mechanisms can be influenced by some users does not alter the fundamental assertion that the important decisions these users take are entirely private: no matter how few they are, they are still private actors who can decide (and so far have decided) regardless of any governmental interference, in spite of the technical failures that would appear to be present in the Bitcoin mining protocol and that some might deem to warrant government intervention (see the observations by I. Eyal, E. Gün Syrer, "Majority is not Enough: Bitcoin Mining is Vulnerable", available at www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf, retrieved on 2 April 2019).

[37] See, among many, G. Brunetta, S. Moroni, *Contractual Communities in the Self-Organising City: Freedom, Creativity, Subsidiarity* (Heidelberg: Springer, 2012); D.E. Andersson, S. Moroni (eds.), Cities and Private Planning: Property Rights, Entrepreneurship and Transaction Costs (Cheltenham, UK: Elgar, 2014); as well as F.E. Foldvary, *Public Goods and Private Communities: The Market Provision of Social Services* (Cheltenham, UK: Elgar, 1994).

Some prominent authors have pointed out that governments have in fact several means to influence Bitcoin,[38] but I believe they all come down to the various forms of government intervention in the economy. I will take these interferences into consideration in my last section, but I believe that they do not alter the Bitcoin governance: they are if anything, a response to the Bitcoin governance. However, Bitcoin as such remains an institution that can and should live without state interference. To be sure, such an interference in the Bitcoin governance has so far been quite limited worldwide. However, it appears very unlikely that states will remain indifferent to this real world experiment with Bitcoin which shows the feasibility of an economic life beyond their context. The growing use of Bitcoin shows that, despite its current technical limitations and limited acceptance a means of payment, this currency is nevertheless able to offer a viable way for the creation of exchange relationships that do not depend on the infrastructure of state money, and use a completely autonomous one. In this regard, it is also worth considering that Bitcoin, despite being the first mover and the incumbent in the context of cryptocurrencies, could easily be supplanted in the future by another virtual currency. This is likely to happen provided that such a currency is based on a permissionless blockchain.[39] It would not make any difference whether state sovereignty is disrupted precisely by Bitcoin or an alternative currency.

In some ways, states appear to have a positive attitude towards blockchain, as a possible tool to increase productivity, and generally as an opportunity for development as a new high-potential economic sector. However, states appear to have become more aware of the extent to which Bitcoin instead may threaten their sovereignty. The regulatory measures taken in different systems to begin

---

[38] See in particular P. De Filippi & B. Loveluck, "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure" (2016) 5(3) *Internet Policy Review*; and P. De Filippi & A. Wright, *Blockchain and the Law: The Rule of Code* (Cambridge: Harvard University Press, 2018), in particular Chapters 11 (pp. 173-192) and 12 (pp. 193-204).

[39] See X. Chen et al., "Blockchain challenges and opportunities: a survey" (2018) 14(4) *Int. J. Web and Grid Services* 352-375.

to put it on the edge of legality go in this direction. This pattern, significantly similar to the one that was followed with gold,[40] will lead states to wait and see, in order to be ready to increase the level of reaction in case Bitcoin becomes more successful and the threat to state sovereignty stops being merely hypothetical.

4 Conclusion: the possible future scenarios

In light of the considerations made in the preceding sections, I believe that some hypotheses can be formulated regarding the possible scenarios that are expected in the short and medium term, from the most to the less favourable case for the development of Bitcoin, to possible intermediate variables.

A first hypothesis, which is the one made by the so-called Bitcoin evangelists, is that Bitcoin represents the outpost of the overcoming of sovereignty, as we have known it from 1648 onwards. According to this approach, states are in crisis, under the weight of their increasingly unsustainable debt and their inability to keep up with technological evolution and globalization. These challenges have made state borders and traditional definitions of sovereignty porous and obsolete from the point of view of the free movement of goods, services and capital. We are also witnessing the gain of momentum of disruptive secession pressures, as in the emblematic cases of Catalonia regarding Spain, and the United Kingdom towards the European Union. The latter phenomena can be seen as power struggles against nation states and traditional institutions. If the self-determination case of Catalonia is self-explanatory, I argue that a similar claim can also be made as regards. Brexit is a reaction against the attempt to push the EU towards more unification and a nation state-like institutional architecture. It is of course true that the EU itself has been an extremely powerful source of abandonment of nation-state barriers and borders (thus contributing to a certain extent

[40] R. de Caria, *supra* note 18.

to the overcoming of nation states). However, the EU has more recently been perceived, rightfully or not, as instead an institutional engineering attempt to replace nation states with a larger version of them. From this perspective, Brexit is not necessarily to be interpreted as the alleged backlash against that freedom of movement, or an attempt at re-establishing national boundaries. Rather, Brexit can be regarded as a backlash against the possible evolution of nation states into a supranational quasi-statist organisation.

In this context, Bitcoin could represent a catalyst element of a process already in progress, an instrument for its acceleration, and a starting point for a world of territorial fragmentation, a world where nation state sovereignties, and *a fortiori* larger entities, gradually lose their appeal and hold on citizens and wealth. Bitcoin or another permissionless blockchain-based cryptocurrency could effectively become the digital gold promised or foreshadowed by many, a universal currency (or at least a store of value) that speaks the language of information technology. This language is by-definition a-national.[41]

The opposite hypothesis is that the reaction of the nation states is instead successful. They could indeed take action in time and outlaw Bitcoin as they – from a monetary point of view – outlawed gold, and this has allowed them to prolong their existence indefinitely so far. In some ways, initiatives restricting the use of Bitcoin have emerged in various jurisdictions,[42] and it is easy to imagine that, should Bitcoin's usage reach a critical mass that seriously endangered the

[41] From this point of view, the questions about the legal framework of Bitcoin, an asset that escapes the traditional categories and potentially puts them in crisis, would acquire a completely different relevance.

[42] For one of the most recent overviews, see O. Stratiev, "Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand" (2018) 33(2) *Banking and Finance Law Review* 173-212.

sustainability of fiat money,[43] states would intensify the reaction, and in this scenario they could effectively materialise this fatal threat to them.

One of the potential scenarios is that Bitcoin may collapse under the weight of technical problems that prove to be insurmountable to achieve the so-called scalability. These problems include a possible bug in the protocol, such as the one that emerged recently and was remedied before being exploited by criminals.[44] If this indeed happens, it can still be questioned whether another cryptocurrency will be able to receive the proverbial torch, or the current highly fragmented scenario will prevail, without the emergence of a comparable alternative to Bitcoin.

Finally, we can also envision the case that the situation proceeds for a long time like today, with the coexistence of cryptocurrencies and fiat money. This coexistence is characterized by the fact that the former has not yet reached a threshold of mass-scale adoption high enough to immediately worry fiat money. Moreover, the strength guaranteed to the latter by the legal tender is such that it is really very difficult for Bitcoin to get to the point of being able to make it possible to do without it. Therefore, it is possible that for a long time Bitcoin remains in this limbo, being an innovation potentially disruptive even for public law, but for the moment unexpressed in its full potential.

---

[43] Contrary to some prominent views (see e.g. N. Roubini, *The Big Blockchain Lie*, Project Syndicate, 15 October 2018, www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10?barrier=accesspaylog, retrieved 2 April 2019), the perspective of mass-scale adoption of Bitcoin does not seem to have been abandoned by its proponents and adopters: see, for instance, the FAQs on the Bitcoin.org website, stating that "New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses" (bitcoin.org/en/faq#what-are-the-disadvantages-of-bitcoin, retrieved 2 April 2019), as well as several press statements by crypto entrepreneurs; see also S. Pattekar, *Mass Crypto Adoption – why we're not there… yet*, 21 September 2018, www.datadriveninvestor.com/2018/09/21/mass-crypto-adoption-why-were-not-there-yet/. For some scholarly reflections on the adoption of these new technologies, see for instance L. Swartz, "What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology", in *Cultural Studies*, 32:4 (2018), 623; and T.C. Stratopoulos, V.X.Q., "Blockchain Technology Adoption" (May 31, 2018), available at SSRN: https://ssrn.com/abstract=3188470 (retrieved 2 April 2019).

[44] See J. Pearson, "A Major Bug In Bitcoin Software Could Have Crashed the Currency", 19 September 2018, retrieved 15 December 2018, motherboard.vice.com/en_us/article/qvakp3/a-major-bug-in-bitcoin-software-could-have-crashed-the-currency.

What appears certain are two final points I would like to make: firstly, the one scenario that does not seem foreseeable is one of a successful 'marriage' between blockchain-based money and state sovereignty. This combination of currencies has been discussed and has been implemented on an experimental basis by some central banks that were even looking into creating their own cryptocurrencies.[45] This would indeed be formally possible only with permissioned blockchains, which are arguably just an evolution of a database, but lack the potential disruptiveness for state monopoly over money that comes with permissionless blockchains. The money based on the latter is so challenging precisely because it is specifically designed to work without a central bank: if it is a central bank to design it, within a permissioned environment, the main novelty disappears, and the experiment might only be interesting, admittedly, for its own, other purposes[46].

Finally, if a "final clash" should in fact take place between fiat money and a cryptocurrency (be it Bitcoin or a different permissionless blockchain-based cryptocurrency), we might find ourselves faced with an epic "constitutional moment,"[47] such as to determine a possible reversal of the "basic norm." This notion was famously invented by Hans Kelsen, who explained it in the following terms: "If we ask why the constitution is valid, perhaps we come upon an older constitution. Ultimately we reach some constitution that is the first historically and that was laid down by an individual usurper or by some kind of assembly. […] It is postulated that one ought to behave as the individual, or the individuals, who laid down the constitution have ordained. This is the basic norm of the legal order under consideration."[48]

---

[45] See M.L. Bech, R. Garratt, "Central bank cryptocurrencies" (2017) September *BIS Quarterly Review* 55.

[46] For an opposite opinion, see N. Roubini, "Why central bank digital currencies will destroy bitcoin", *The Guardian*, 19 November 2018.

[47] *See generally* B. Ackerman, *We the People: Foundations* (Cambridge, MA: The Belknap Press of Harvard University Press, 1991).

[48] H. Kelsen, *The General Theory of Law and State* (New York: Russell and Russell, 1945), 115.

In this scenario, if states lose the challenge on the ultimate basis of providing money with legitimacy, they will inevitably also lose that of the monopoly of law and force, in favour of new (or old, but in any case reshaped) forms of legitimation based on the market, custom, free trade, freedom. Such a development would certainly entail an overturn of the current conditions of validity of the constitution, and their replacement with a different one.

All we are left for is to remain vigilant and observe the potential unfolding of this new "basic norm," while being aware that the process could take longer than we imagine. In any case, we could be in the middle of an event that will act as a watershed in public law and in the legal history (and beyond) of the whole mankind.