information

Tracked for Impact Factor

CITESCORE 5.8

Review

Editor's Choice

Understanding the Blockchain Oracle Problem: A Call for Action

Giulio Caldarelli

MDPI

https://doi.org/10.3390/info11110509

information

Review

Understanding the Blockchain Oracle Problem: A Call for Action

Giulio Caldarelli

Department of Business Administration, University of Verona, 37129 Verona, Italy; giulio.caldarelli@univr.it

Received: 12 September 2020; Accepted: 28 October 2020; Published: 29 October 2020

Abstract: Scarce and niche in the literature just a few years ago, the blockchain topic is now the main subject in conference papers and books. However, the hype generated by the technology and its potential implications for real-world applications is flawed by many misconceptions about how it works and how it is implemented, creating faulty thinking or overly optimistic expectations. Too often, characteristics such as immutability, transparency, and censorship resistance, which mainly belong to the bitcoin blockchain, are sought in regular blockchains, whose potential is barely comparable. Furthermore, critical aspects such as oracles and their role in smart contracts receive few literature contributions, leaving results and theoretical implications highly questionable. This literature review of the latest papers in the field aims to give clarity to the blockchain oracle problem by discussing its effects in some of the most promising real-world applications. The analysis supports the view that the more trusted a system is, the less the oracle problem impacts.

Keywords: blockchain; smart contracts; oracles

1. Introduction

"Is the blockchain the greatest technological innovation since the internet . . . or the greatest load of hype ever raged around the history of technology? . . . Both" (Andreas Antonopoulos). Blockchain's primary innovation is that it allows business partners to transfer digital assets without the need for a centralized third party [1]. However, as blockchain can execute only simple transactions, "smart contracts" are necessary to settle the terms of an agreement [2,3]. Although available on bitcoin since 2012 with the introduction of Pay-to-Script-Hash (P2SH), smart contracts have become easier to program and more versatile thanks to the Ethereum Virtual Machine (EVM) [4,5]. With smart contract advanced features, above digital payments, blockchain projects could involve supply chain and traceability [6,7], healthcare [8,9], energy [10], intellectual property rights (IPRS) [11], contracting and law [12,13], academic records [14,15], and media and entertainment [16,17]. However, "buried" under the blockchain euphoria lies a fundamental issue with smart contracts rarely addressed in business and the literature. As blockchains are blind to the real world, they are always dependent on "Oracles" [18]. Oracles are centralized and trusted third parties that constitute the interface between blockchains and the real world [19]. As oracles reintroduce the concepts of trusted third parties and centralization, their implementation is often seen as a "problem" [20,21]. Although all real-world blockchain applications are affected by the oracle problem, it is unusual to read about how a business can overcome the oracle problem or how this issue can be overcome in the literature [22,23]. As a matter of fact, the oracle problem not only undermines the feasibility of a project, but it constitutes a severe threat to investors, consumers, and academics. A recent study from Pennsylvania University compared the blockchain codes of the fifty largest initial coin offerings (ICOs) by amounts raised in dollars with what the creator promised, and they discovered that an important portion was not even programmed for the attended purpose [24]. It was also shown that just 20% of the ICOs had mechanisms to protect investors embedded in the code [25]. Being aware of the principles underlying smart contracts

and issues related to the oracle problem could prevent investors from funding fraudulent projects, redirecting investments to more worthy and rewarding ICOs. Blockchain applications for traceability in food, chemical, and luxury areas, for example, claim to provide consumers with transparent and direct access to the supply chain, ensuring the safety and genuineness of products [1,26,27]. However, the oracle problem enables companies to decide what information is retrievable through the blockchain, leading to a more dangerous and controversial scenario. Consumers may end up trusting producers and products that, using former selection mechanisms based on experience, would have never been considered as safe or genuine [28]. In the end, from an academic perspective, we are seeing an overwhelming production of papers regarding blockchain and business implementation that, apart from a few contributions [3,19,21,22], rarely address the oracle problem. A recent systematic literature review on the subject showed that from a sample of 142 journal papers discussing blockchain real-world applications, only 15% considered the role of oracles, and less than 10% underlined the limitations of the oracle problem [23]. This emerging gap may lead to a considerable portion of the literature following a biased stream. Discussing the most recent literature on blockchain and real-world applications use cases, this paper aims at providing a broad understanding of the oracles and the oracle problem. As the oracle problem impacts differently according to the sector, a discussion on the selected cases should give a broad overview of the conditions and consequences of this issue.

The study supports the view that the more trustworthy a system is, the less the blockchain oracle problem impacts. Considering the almost complete absence of academic papers focused on the oracle problem, this work should provide a useful contribution for further research. The article proceeds as follows. Section 2 introduces blockchain technology as well as smart contracts. Section 3 outlines the concept of oracles and narrows the oracle problem. Section 4 gives a broader introduction of how the oracle problem affects the main real-world applications. Section 5 provides a discussion on the subject, while Section 6 concludes the paper, providing directions for further research.

2. Theoretical Background

2.1. What Is a Blockchain?

A blockchain records data in a sequential archive. The first blockchain was created by a man or a group of people under the pseudonym of Satoshi Nakamoto to provide the technical infrastructure for Bitcoin cryptocurrency [29,30]. On the blockchain (Bitcoin), all the full-nodes share the same copy of the ledger, where changes are immediately reflected for all the participants in the network [31]. When an agent creates a new transaction, it is broadcasted to the network, on which miners perform the verification and auditing tasks through a proof-of-work consensus mechanism. Once the transaction is approved, it is added (along with others) to the chain in a new block. A record of the transaction is then saved in all the full-nodes of the decentralized network [6]. On the bitcoin blockchain, data forgery is very unlikely to happen. The consensus mechanism (proof-of-work) requires a considerable amount of computing power for blocks to be added. Since every block is added (sequentially) every ten minutes (in media), a change in a previous block would require a computing power whose costs would largely exceed the benefit of the forgery [32]. The structure proposed by Nakamoto embodies essential characteristics that are indeed a source of hype around the technology [33].

- **Decentralization of consensus:** There is the absence of an authority that constitutes a single point of trust/failure to approve transactions.
- **Transparency**: Records are auditable by all the participants in the network.
- **Security and Immutability**: Only private-key owners can start a transaction, and once added to the blockchain, forgery is very unlikely to happen.
- **Censorship resistance**: The system is meant to prevent invalid transactions, not invalid users, so anyone—human, corporation, or even AI—may operate on the blockchain.
- **Borderless**: A blockchain network is not affected by distance or national borders. Even though the transaction happens in the same room or between two "poles", the rules remain the same [5].

Although blockchain has become famous and has generated massive hype because of these specific characteristics (which strictly belong to the Bitcoin network), currently there is not a universally accepted definition of blockchain in the literature [34]. Not all blockchains embody the same characteristics, as some (like private ones) operate under entirely different and often unknown rules. Communities of blockchain enthusiasts are often reluctant to recognize the validity of private blockchains. However, experiments, pilot projects, and innovation in the business field are indeed mostly managed with private blockchains (e.g., IBM/Hyperledger), whose lower costs and higher flexibility better match the uncertainty of the market [35,36]. Regardless of its type, blockchain can be implemented in many areas. Swan [37] represents at least three valuable implementations of the technology. The first is currency, along with remittances and e-payments. The second is social applications such as notary, voting, and healthcare. The third is smart contracts, which will be outlined in-depth in the next section.

2.2. From Blockchain to "Smart" Contracts

The idea of smart contracts comes from the cryptographer Nick Szabo [2], who provided the following definition: "a set of promises, specified in digital form, including protocols within which the parties perform on the other promises". However, the idea did not see the light until the emergence of blockchain technology [38]. The main aim of a smart contract is to automatically execute the terms of an agreement once the specified conditions are met. On the blockchain, smart contracts are defined as "self-executing code . . . that automatically implements the terms of an agreement between parties" [39]. Willing to be overcritical, those running on the blockchain should not be called smart contracts. Smart contracts are a piece of code executed without any "smart" implication, and usually without legal value. However, as time passed, the term "smart contract" somehow stuck [18]. Compared to traditional contracts, smart contracts do not rely on a trusted third party to operate, resulting in low transaction costs. Of particular interest regarding smart contracts are their immutable and deterministic components [1]. Once deployed, the smart contract code is immutable, and although it is possible to delete the contract, the transaction history remains embedded in the blockchain on which it operates. A contract's outcome is also the same for anyone who runs it, and even the contract creator has no exclusive right over it. To better explain how smart contracts function, it is mandatory to understand the separation between externally owned accounts (EOAs) and smart contracts. EOAs are accounts controlled by users through private keys, thanks to which they can execute transactions.

On the other hand, although created by an agent, smart contracts are self-owned. Smart contracts are not controlled by any private keys and cannot self-execute. While a smart contract could activate other smart contracts, the initial input can only be given by an EOA. A crypto swap (Figure 1) constitutes a classic example of how a smart contract operates.

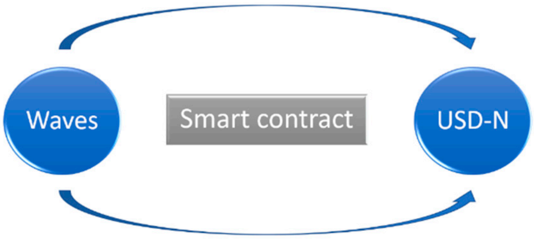

Figure 1. Example of a swap between waves and Neutrino USD (USD-N).

If an agent fears a market downturn and wishes to convert some volatile crypto such as waves into some stable coin such as USD-N, they send waves to the swap smart contract address, and once processed, they receive USD-N back. It is not a smart operation and does not have a legal value, but it is immutable as the term of the contract is not subject to variation, and it is deterministic because it always operates under the same rule regardless of who operates the contract. Furthermore, in case the contract is deleted, the swap operation will always be available for auditing. Thanks to their flexibility, smart contracts can be implemented in a wide variety of applications, such as

- Certificates, ownership and digital identity [15,40],
- Intellectual property rights [30,41],
- Energy production [42],
- Healthcare [8,43],
- Contracting and law [19,44], and
- Supply chain and data provenance [45,46].

Although deterministic and immutable, smart contracts are not perfect and trustless. Their main point of failure consists of the communication channel with the real world, the oracles, whose role and characteristics will be outlined in the next paragraph.

3. Understanding the Oracle Problem

3.1. What Are Oracles?

The term "oracle" comes from Greek mythology and refers to someone able to communicate directly with god and see the future. In ancient stories, people did not have enough information to make decisions, and turned to oracles for knowledge beyond their understanding [47]. In the blockchain environment, oracles are systems that provide blockchain with information coming from the real world. If smart contracts do not deal with crypto exchange but with a decentralized mechanism involving weather, stock prices, or political events, a gateway from the external world is needed [48]. As the blockchain problem is to reach consensus, extrinsic information cannot be provided along with transaction data, since other nodes would detect information coming from an "untrusted" source. Therefore, information coming from the real world should come from a third-party univocal source, whose reliability is undisputed for all nodes: the oracle. Unlike Greek mythology, oracles (on the blockchain) do not predict the future but retrieve information from the past. Oracles are not specific programs or devices, but "concepts". Anything providing external data to the blockchain can be classified as an oracle. To be precise, oracles, in general, do not insert information into the blockchain directly; conversely, they gather and store data from the real world. When a smart contract concerning extrinsic data is executed, the code then calls for the right information from a trusted oracle. Examples of oracles are IoT systems such as probes and sensors, platforms such as ERP, or in the case of private data, the very human that operates directly on the blockchain. Oracles act as a bridge that can digest external and non-deterministic information into a format that a blockchain can understand [49]. Examples of data gathered by oracles comprise the following:

- Lottery winners;
- Natural disasters along with risk measurements;
- Price and exchange rate of real/crypto assets;
- Static data (e.g., country codes);
- Dynamic data (e.g., time measurements);
- Weather conditions;
- Political events;
- Sporting events;
- Geolocation and traceability information;
- Accidents;
- Events in other blockchains.

To better understand how oracles are necessary for smart contracts, recall the trading example made in the last paragraph, involving waves and USD-N stable coins. In that case, critical information for the smart contract to succeed, such as the waves/USD-N exchange rate, was missing (Figure 2). Data such as these are external to the blockchain, and without an oracle that updates rates, the contract could not be executed.

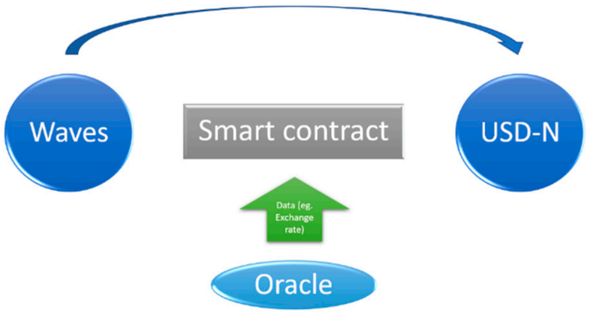

Figure 2. Crypto swap including an oracle.

This (decentralized) oracle's trustworthiness is somehow objective since, even if the oracle sets the price autonomously by merely browsing exchange prices online, any agent can verify if the exchange rate is correct or not. Different is the case where smart contracts operate in a situation in which oracles provide information that is hardly verifiable by the agents (centralized oracles). In those environments, the trustworthiness of oracles is fundamental. If the contracts involve highly valuable agreements, the oracle's chance to be compromised to benefit a particular party increases dramatically [50]. When all the parties cannot verify the oracle's data, and contract value increases, the oracle itself becomes a "problem".

3.2. Narrowing the Oracle Problem

The oracle problem is not a new concept in software testing. Anything able to verify the correct execution of a test application is called an "Oracle" [51]. According to Barr et al. [52], the problem arises when test oracles are unable to run in complete automation. If oracles are not automatized, an agent intervention is needed to determine whether the observed behavior is correct. Since human discretion is unable to foresee any possible outcomes, the uncertainty of data provided takes the name of "the oracle problem" [53,54].

Regarding blockchain and smart contracts, the oracle problem involves the trustworthiness and reliability of oracles. Curran [49] defined the oracle problem (in the blockchain) as "the security, authenticity, and trust conflict between third-party oracles and the trustless execution of smart contracts". To the best of the author's knowledge, the construct's origin can be spotted in a Reddit post by Dalovindj [20], definitely before the Ethereum environment for smart contracts was launched. The blogger realized that when executing an application on the bitcoin blockchain, regarding crowdfunding or gambling, verifying the reliability of extrinsic information without altering the consensus mechanism was indeed a problem: "*I think of it as 'The Oracle Problem'*".

In his dissertation, Egberts [28] extensively explained the drawbacks of the oracle problem, mainly describing it as a "*two step-back from decentralization*". As oracles are not distributed, they reintroduced the single-point-of-failure. Additionally, since they operate on non-deterministic data, their reliability needs to be trusted, removing trustless peer-to-peer interaction. Their implementation through smart contracts into the blockchain could also jeopardize users' trust who consider the blockchain as more reliable than legacy systems. Brilliantly shown by Antonopoulos [55], a system built on oracles can also fail in two ways. If the oracle is trusted and cannot be compromised, there is still a chance that the data on which it is working have been altered, and then, although being a trustworthy device, it will feed the smart contracts with data that are untrue.

On the other hand, if the data are trusted and verified, the oracle may fail to operate correctly on the smart contract either due to malfunction or deliberate tampering. From a game-theoretical approach, it can be shown that the higher the value of the smart contract, the higher the incentive for the system to be compromised [50]. The oracle problem is also triggered in the case of attaching real assets on the blockchain through smart contracts. In a well-known article, Song [56] explained that in decentralized contexts (e.g., blockchain/smart contracts), linking a physical to a digital asset, whether it be fruit, cars, or houses, constitutes a critical issue. Tangible assets are regulated by the jurisdiction in which they reside, meaning that they are subject to something else (in some case, predominant) other than the smart contract. Indeed, this implies trusting something in addition to the smart contract. If, for example, a smart contract involves the property transfer of a house between two agents, the code will indeed swap the certificate between parties.

On the other hand, what happens in the real world may not be affected by the smart contract, as the former owner could refuse to leave the house. Without the involvement of a third party (e.g., government) that supervises the smart contracts, their enforcement is indeed not ensured. The need to trust a third party removes the "killer feature" of trustless applications, which in environments plagued with corruption represents a significant limitation. A considerable attempt to limit the oracle problem was made by Chainlink [57]. The start-up proposed a system of decentralized oracles, based on reputation, to reproduce the consensus mechanism of a blockchain. When deciding which data to upload on the blockchain, it takes into account the majority of oracles with the same data and the reputational level of each oracle. The data confirmed by the majority of the oracle are then uploaded on the chain [58]. This powerful system effectively addresses oracle malfunction or failures; however, deliberate data tampering or collusion could still be performed by the companies controlling the service. When decentralization is not sufficient to address the oracle problem, and data authenticity cannot be objectively verified, a "trust model" is needed for the smart contract environment to keep a certain degree of reliability [18]. As explained in a recent paper, a trust model is an intuitive scheme that outlines the reasons why the smart contract application should be trusted [22]. Failing to address the oracle problem poses a severe threat to investigating and developing real-world blockchain applications.

4. How the Oracle Problem Affects Real-World Applications

Although heterogeneous, almost all real-world blockchain applications suffer from the oracle problem. However, the negative impact varies according to the nature of the business and institution involved. In this section, some of the most discussed smart contract applications are outlined, showing how and to what extent the oracle problem may affect their further development. The sectors under analysis are chosen according to their peculiar characteristics and oracle problem setbacks. Although real-world blockchain applications are countless, considering other sectors would have probably led to redundant results. Arguably, the outcomes of the analysis should reach a satisfying level of saturation.

4.1. IPRS Protection

As Yermack [29] showed, the original purpose of the blockchain, before the crypto 'era', was to "register" intellectual property rights. In the early 1990s, Haber and Stornetta [59] proposed the digital timestamping of documents in sequence to authenticate authorship of intellectual property. Nakamoto [60] then referred to this type of structure as a "chain of blocks" that we now call "blockchain". Overshadowed by financial applications, the IPRS protection role of blockchain again aroused interest after smart contract platforms (e.g., EVM) became operative. The music industry is thought to be the most affected by blockchain due to the unfair practices of record labels and the digital revolution [61]. Blockchain promises artists the ability to independently determine prices and autonomously license their works in a "direct-to-fan" fashion [30]. Examples and pilot projects are Micelii, Monegraf, PoE, and UJO. Those platforms let the authors directly receive the royalties shared according to the smart contract [62]. However, as Fink and Moscon [30] underlined, this procedure will not eliminate intermediaries but will simply create new ones. The critical aspect of this system consists of what Shatkovskaya [41] referred to as the "*Attestation Service*" (Oracles).

As soon as data about the IPRs are on the blockchain, assuming the system works perfectly, they are protected against tampering and efficiently share revenues among authors. The point of failure of this whole system remains the gateway between the author and the blockchain. Basically, anyone uploading a piece of art is recognized as the owner of the digital record. However, the system does not verify if the creation has been stolen or just given by someone else. Proof of authority (PoA), for example, offers the artist timestamped evidence of a digital creation that can be used for IPR claims but is unable to verify the real authorship of original productions. In the case of someone recognizing his work as registered by someone else, there will always be the need for a legal system that supervises the IPRs and enforces violations. In the absence of enforcing authorities, blockchain may end up being a first-come-first-serve platform, where the only thing that counts is to be the first to upload the creation. It is improbable that the system can be wholly automatized and self-sufficient. However, the decentralization of the service may reduce the power of centralized authorities and help artists to have more control over their creations. It is still hard to determine whether the record label or the authors themselves should constitute the most trustworthy oracle (Figure 3).

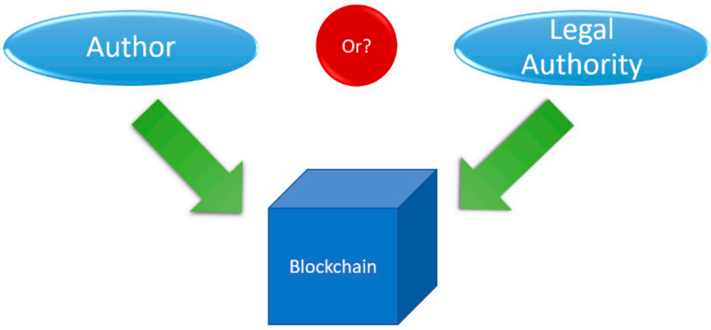

Figure 3. Selecting the appropriate oracle.

4.2. Academic Transcript

A considerable part of the non-financial blockchain application is dedicated to developing a better system in the education/academic field [14]. In particular, decentralized technologies are sought to solve issues related to privacy, security, and vulnerability in the "ubiquitous learning environment" [63]. Blockchain-based applications could enhance the digital accreditation of personal and academic learning [64], easing complex credit management such as European Credit Transfer Accumulation System (ECTS) [65]. In a recent paper, Ocheja et al. [15] showed that the most advanced institutions in that field are

- MIT University Media Lab that developed Blockcert on the Bitcoin protocol;
- The University of Nicosia, part of the Blockcert consortium that improved Blockcert also on the bitcoin protocol;
- Sony Corporation that developed Sony Global Education in cooperation with IBM Hyperledger Fabric.

Although Ethereum is the standard for smart contracts, the most advanced institutions in the field preferred the bitcoin network to store their information, despite the lower scalability and higher costs of Bitcoin blockchain. As Ocheja et al. [15] hypothesized, the reason bitcoin is preferred to create academic transcripts is that, since bitcoin is associated with robust financial investment, it has a better chance of survival. Blockcert, for example (built on bitcoin blockchain), aims to double the authenticity assurance of academic records. When a certificate is released, it is uploaded on the blockchain (Figure 4) and is ready for audit [40]. It is enough to go to the university website and upload the document to verify the certificate's genuineness and spot any tampering or mystification. The oracle problem, in the academic field, is indeed controversial. From a general point of view, its impact is maximum.

As directly uploaded by the certifying institutions, we are unable to verify the integrity of the data. As Antonopoulos and Woods [18] stated, for academic applications, "the universities are themselves Oracles", whose discretion cannot be altered or limited. However, for academic blockchain applications, what is perceived as a point of failure may well constitute its strongest characteristic. Universities as oracles have a long-standing reputation, which makes their information more or less reliable depending on their history. In general, if a certificate is on a blockchain, the authenticity can indeed be proven (Figure 4).

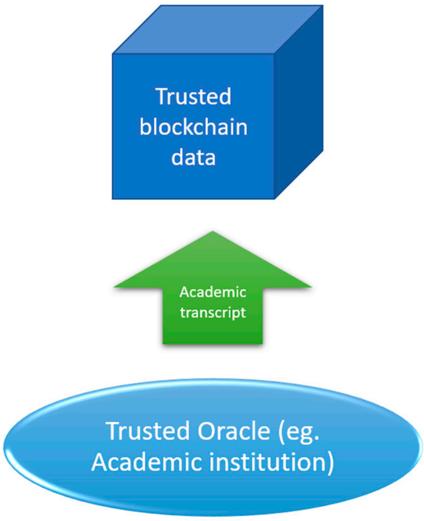

Figure 4. Academic institutions as trusted blockchain oracles.

What cannot be established is the truthfulness of the data that the certificate reports. If students obtain their degree from a low-ranked university, the fact that the certificate is on the blockchain does not give a higher value to their record. If a degree has been bought, the document will still show as "authentic" on the blockchain. The extrinsic value of an academic document is still given only and exclusively by the reputation of the institution issuing the certificate. The literature lacks a decentralized approach to recognizing the "skills" owned by students whose value could indeed exceed any degree or transcript. In this type of application, again, the role of the oracle is critical.

4.3. Supply Chain and Traceability

Blockchain applications for secure data provenance have been investigated and supported by many articles [46,66]. An immediate consequence was implementing the data provenance system for physical products, which has rapidly aroused the interest of scholars, institutions, and firms [26,45]. The security and immutability features of blockchain should help to ensure provenance and safety for shipments of drugs, food, and critical components [67]. However, in a recent speech, Antonopoulos [55] brilliantly explained why and how linking a real product to the blockchain should raise concerns on the reliability of this traceability system. When dealing with cryptocurrencies, the "provenance" of a bitcoin is guaranteed, since it has been issued on the blockchain. Every movement has been tracked in the immutable and transparent ledger from the first issuance. Regarding a real product, such as a "mango" sitting on a store shelf, this product's provenance is unknown to the blockchain, and data should be inserted by oracles [68].

For supply chain applications, oracles belong to the company producing goods that are being tracked, and this, for sure, constitutes a substantial conflict of interest. Blockchain/oracle service may be outsourced to a third party [27], but the control over information is indeed in the hands of the producing company [21]. Companies decide, then, what information to upload on the blockchain, and it is improbable to spot unwanted or inconvenient data [69]. It is plausible to deduce that, for tangible goods, information is immutable but not unquestionable, and information is as reliable as the company that owns the supply chain. In a recent paper, Kumar [1] also voiced doubts about the reliability of blockchain applications for supply chains due to the oracle problem, which emerges regardless of the blockchain type (public/private). However, the oracle problem for traceability can be partially overcome by creating the right trust model [18]. Research on the subject [22] outlines that for some products subject to a "*disciplinare*" (procedural guideline), providing false information would result in fines or license revocation (Figure 5).

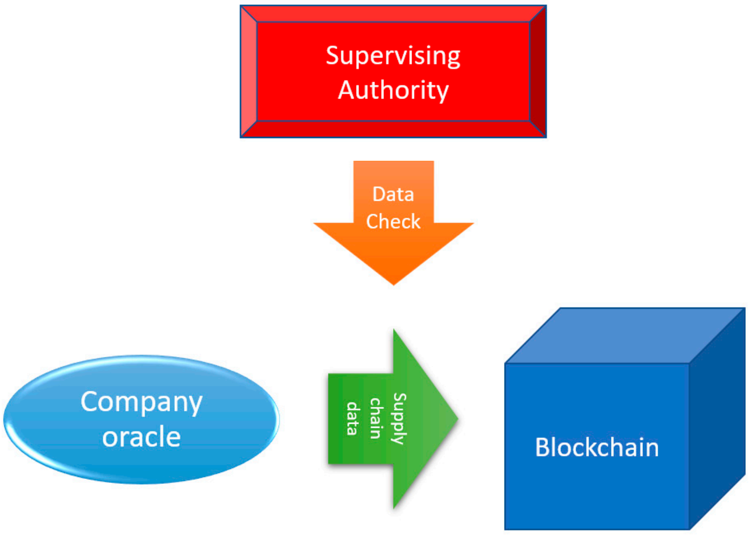

Figure 5. Example of a trust model [22].

Thus, the likelihood that information on the blockchain could diverge from reality is eventually low. It should be clear why the company has little incentive to cheat information provided on the blockchain through a trust model. The literature should then investigate the relationship between oracles, firms, and blockchains, understanding the mechanism through which companies should be incentivized not to cheat on the blockchain, which is unfortunately possible.

4.4. *Energy*

The most claimed advantages in introducing blockchain within the energy sector regard reduction in costs for the marketplace as well as increased transparency and decentralization [70]. Projects such as Energy internet and the notable Brooklyn micro-grid are undoubtedly raising expectations [71–73]. However, "details" of how blockchain could help to achieve those results are often neglected or even unmentioned. Surprisingly, to date, there is still no contribution that has addressed the oracle problem in the energy field, whose role is particularly critical for the system's complexity [23]. The oracle problem for the energy sector is, in fact, "dual". It affects inbound transactions as well as outbound transactions [19]. To understand in detail how complicated this system is, we may take as an example the case of a prosumer (Figure 6). The agent acquires energy from a centralized provider while having some equipment to produce his own (e.g., photovoltaic, hydro plant). He then sells to a marketplace the part that exceeds his consumption [61]. We also assume that this platform/marketplace operates on a blockchain. To let data about the prosumer contribution be uploaded on the blockchain, we may need at least one (inbound) oracle to collect data from his house. Having the oracle in his possession gives the agent the highest incentive to manipulate the sensor to send false data about its contribution [50]. For this anticipated event, the platform should have a second oracle to double check the data received from the agent or have a maintenance service that periodically checks the state of the sensors.

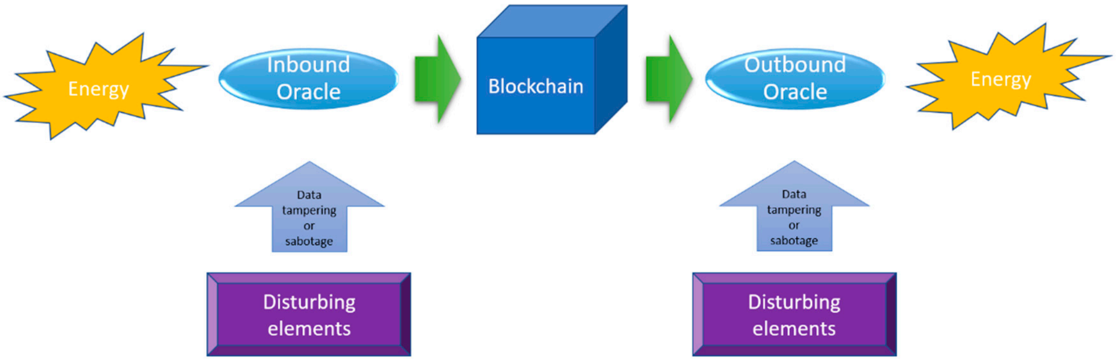

Figure 6. Example of the "dual" oracle problem.

While the platform could be decentralized and independent from a central authority (since nodes are spread globally, and their exact position is uncertain), oracles are unlikely to also be decentralized and autonomous [18]. Furthermore, oracles have to be localized where the event occurs, and, of course, their position is to be known to provide exact data about consumption and contribution [44]. The chance for those centralized sensors to be free and independent from a central authority, which can be an energy provider or the government, is indeed quite low. However, this problematic situation constitutes just half of the problem, since more insidious is the "*outbound*" oracle problem [19]. Considering the same example of a prosumer, we may also hypothesize that in a period where his production is insufficient, he would like to buy some energy from the blockchain platform using his cryptocurrencies. In that case, the transaction will be promptly executed by the blockchain, and the crypto transferred to the platform account. The blockchain should then communicate with an external platform or system to ensure that the exact amount of energy is sent to the agent. However, from that point, countless events may alter the procedure. Starting from a simple sensor malfunction, we may encounter a scarcity of resources, failures of the electric plants, wires sabotage, authority denial, or even the system could not exist at all! Even the absence of infrastructure in the real world may not prevent the smart contract from executing successfully [18]. An external authority monitoring those procedures is essential for the system to work correctly. Additionally, it may ensure that the agent is refunded in the case of malfunction [74]. Again, assuming that this external authority or organization is free or independent from the government is also very unlikely. Hypotheses of blockchain applications in the energy sector comprise many examples other than the prosumer case; however, the inbound/outbound oracle problem is shared among all of them. Efforts and contributions to the literature should then converge on how, and if, it is possible to maintain a blockchain platform that is decentralized and independent. Recognizing the role of oracles and building the appropriate "trust model" should also be prioritized.

4.5. Contracting and Law

According to Guadamuz [44], the first attempt to regulate smart contracts has been made in Arizona. There, smart contracts are defined as "event-driven programs, with a state that runs on a distributed, decentralized, shared and replicated ledger, and that can take custody over and instruct transfer of assets on that ledger" [75]. Stating that smart contracts run on "something" obliges the legislator to also define the platform on which they operate. They described the blockchain platform as "*distributed ledger technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto-economic or token-less. The data on the ledger is protected with cryptography, is immutable and auditable, and provides an uncensored truth*" [76]. As the literature still does not have a univocal definition of blockchain, this overly general statement bears a few contradictions. If private, a blockchain is not an open ledger and not distributed either [77].

Furthermore, the concept of "uncensored truth" is quite controversial; if the system runs well, we may have immutability, but the veracity of the information contained in the ledger can hardly be proven. From that point onward, papers realized that the interaction of smart contracts with the real world triggered the "*so-called oracle's problem*" [78,79]. Legally speaking, the literature eventually recognized that the problem with a smart contract involving data from the real world consists of the presence of third parties (oracles) external to the contractors whose legal state is yet to be identified [68]. When executing smart contracts, parties cannot fully trust each other, and an oracle is in the best position to manipulate data and collude with one of the parties. Damjan [19] noted that services offering oracles (e.g., Oraclize, Reality Keys) do not guarantee oracle impartiality and the veracity of the information provided. They thus negate the two necessary conditions for smart contracts to be legally viable. In his essay, Frankenreiter [3] underlined that even when hypothesizing the good faith of oracles, at least four critical issues could be identified. First, as an oracle is to be trusted, its identity is to be known, which poses a threat to its impartiality and independence. While the government cannot change information on the blockchain, it can influence oracles by exerting pressure on the organization controlling them [80]. Second, linking some real assets to a blockchain token is something that cannot be done without the intervention of legal authorities. As shown in the household example, successfully executing the smart contract does not guarantee that the property is also switched [56]. Third, as the system involves the oracles, which can be sensors or humans, they are not 100% reliable, even if trustworthy. In the event of a malfunction (or if the contract is not executed correctly), the platform cannot restore the original state or compensate for a breakdown. Cases like the DAO and ETC are classic examples of those recurring issues [81–83]. The presence of an authority capable of enforcing a malfunctioning smart contract is then necessary for parties to completely trust the system. Lastly, the decentralization of platforms on which smart contract run make them dependent on miners' actions. Miner contribution to the network is subject to compensation and highly influenced by market shocks. A decrease in the price of the currencies may result in a weakening of the platform due to the exit of miners, thus jeopardizing the reliability of the whole legal system [84]. What the literature still needs to conceptualize is the preferred legal nature of the oracles, whether they should be independent or legal entities. Secondly, due to the complex nature of the oracle's relationship with the contractor, it can hardly be coded with a smart contract and probably needs a formal contract to be legally viable. Lastly, some smart contracts, involving gambling activity, have proven to be nearly untraceable by legal authorities, raising a few concerns about exploitation for illegal purposes.

4.6. Healthcare

An interesting article by Radanovic and Likic [85] forecasted the possible implementations of blockchain in the healthcare domain. Supported also by the recent literature and pilot projects, technology integration may involve health records [66], health insurance [43], biomedical research [86], drug supply [87], and medical education [88]. Despite proposing different applications, the shared opinion is that blockchain technology could grant privacy and security improvements in the healthcare sector [89,90]. The aim is indeed justified since in the field of healthcare, privacy and security breaches exponentially increase every year. Recent research showed that 37 million medical records were illegally accessed between 2010 and 2017, with 300 violations only in 2017 [91,92]. Furthermore, there is still no unified system to store and distribute patients' information between various healthcare facilities [93]. Countless proposals and concepts of blockchain applications have been discussed to overcome those issues.

Among those, the following projects [94] are the most known and successful:

- **Dentacoin** ensures, through a system of stringent reviews, that the doctors are qualified to operate in the dental industry.
- **Solve.Care** provides a platform that manages accesses, care, and payments, making healthcare more handy and affordable
- **Medibloc** provides a private and reliable blockchain to store and distribute medical data.
- **Medicalchain** offers a solution for personal health records storage, also providing a direct link with insurance companies.

- **Blockpharma** ensures the traceability and authenticity of drugs using blockchain and IoT (Quick response code).
- **Humanscape** ensures cooperation between researchers to develop cures to tackle over 7000 incurable diseases.

Arguably, those projects may effectively store and share information in a secure way, using blockchain. However, just like all other real-world applications, the limit lies in the interface between the real world and the blockchain [19]. Discussing the oracle problem in the case of health records, which, according to a recent literature review, has received most of the academic contributions [95], the outcome is quite controversial. Assuming that the system will be based on a unique and private blockchain to protect patient privacy, in the long run oracles should, in theory, be distributed as shown in Figure 7.

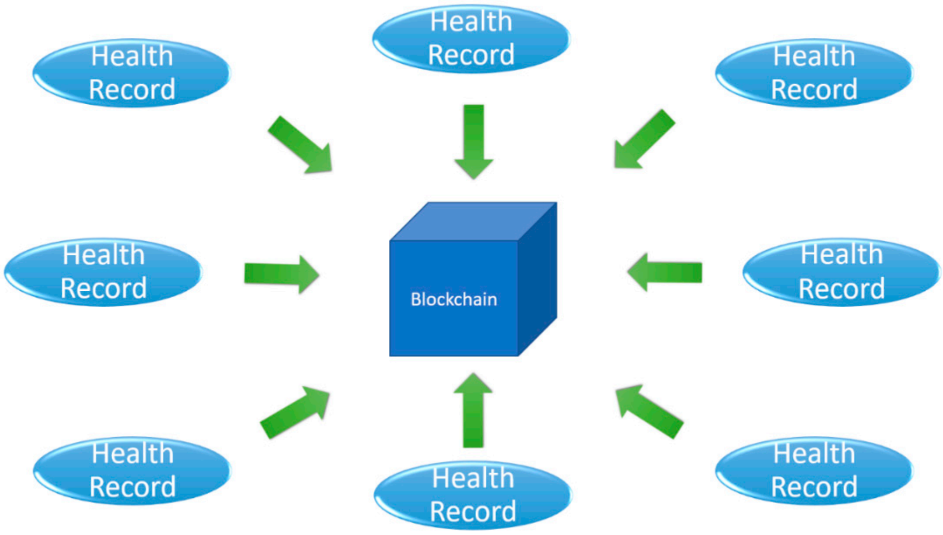

Figure 7. Example of distributed oracles.

As discussed before, distributed oracles are a powerful way to ensure that data uploaded on the blockchain have not been tampered with [96]. However, this is true if oracles process the same information and if data are publicly available and verifiable. For sensitive and private data, which are not publicly verifiable, having distributed oracles processing different information increases the chance of data tampering and leakage. Alternatively, the system may work with a single oracle, and all health institutions could communicate with it through legacy databases. However, confirming the inefficiency of a legacy database in the healthcare sector, Radanovic and Likic [85] also debated that mixing on-chain and off-chain data may undermine the very need for a blockchain in the healthcare sector. In order to tackle this issue, Solve.Care recently signed an agreement with Chainlink for using external oracles to supervise sensitive data inserted on the blockchain [97]. Although promising, the reliability of this project is yet to be verified.

5. Discussion

The real-world blockchain applications described above have helped shed light on the circumstances that create problems when implementing oracles on the blockchain. For academic transcripts, the oracle impact is directly proportional to the institution's reputation. As universities are themselves oracles, data on the blockchain are then as trustworthy as the university itself [18]. Arguably, what makes information on the blockchain more reliable is the level of trust that we directly put on the oracle (institution). Considering trust, not a dummy variable, the degree of trust owned by an oracle proportionally affects the reliability of the information stored on the blockchain. For supply chain management, since companies (apart from multinational) are only known in the area where they operate, there is the need for a third-party to supervise and ensure data integrity on the blockchain [97]. Their relationship should then be formalized through a "trust model" [18,22]. From a game-theoretical approach, the model should describe the reason why an oracle is not incentivized to cheat on the blockchain [50].

In the IPR field, which constitutes the first blockchain application, oracles still represent an issue [41]. On the other hand, numerous prototypes have already shown promising results [30]. The problem here is to understand and define "who", between the artist or the legal authority, should cover the role of the oracle. In the first case, companies such as recording firms would lose their power in favor of artists. In the second case, the situation will remain the same as it is at the moment. From a technical point of view, both oracles are valid, as they can be considered as twins. The choice of the oracle, however, has hugely different social outcomes [74]. However, it is clear that the legal aspect of protecting the IP is unlikely to be separated from central authorities [3]. The law literature offers, in fact, many contributions to the oracles and their legal implications [23]. As parties cannot fully trust each other, it is clear that neither of them can cover the role of the oracle. A third party is then necessary to settle the terms of a smart contract with legal value. The problem is that, according to law, contracts should be enforceable and not immutable [44]. This makes it necessary to establish a hierarchy of oracles thanks to which illegal agreements can be reverted. Technically, on the one hand we do not have many examples of smart contract reversions in history, and on the other hand, the chance of smart contracts being reverted would indeed limit their power [81,83]. However, recent studies have shown the implications of smart contracts as a means to speed up the law processes [79].

In the healthcare sector, as described in the last paragraph, blockchain could be implemented in many areas [85]. In some of them, the oracle problem impacts very similarly to other real-world applications. The presence of overlapping areas also supports the view that the analyzed sample has reached a sufficient heterogeneity and saturation level. For the traceability of drugs, in fact, a trust model could be sufficient to address the oracle problem. At the same time, given the importance of some pharmaceutical companies, as in the case of academic institutions, they may cover the role of oracles themselves [18,22]. For the problem of doctors' trustworthiness, an effective approach could be very similar to those offered by academic institutions for student credentials [98]. On the other hand, health record applications present some critical issues. First, as in the IPRS sector, it is not clear "who" between the patient and the institution should upload data on the blockchain [30]. Since information is sensitive and private, active blockchain projects leave, in fact, discretion to the patients for personal health data to be uploaded in the public ledger [93]. Using multiple oracles may undermine the safety and privacy of data inserted on the blockchain from a security point of view. It also erases the main reason for the blockchain to be implemented in the healthcare sector [85].

Lastly, the energy field is surprisingly more abstract in the literature, and the oracle problem, which for this field is undoubtedly critical, to the best of the author's knowledge, is not mentioned in any publication [23]. Since the oracle problem in the energy field is also dual, it seems very unlikely that the blockchain platform could operate without the supervision of an external authority. Solving the inbound oracle problem without solving the outbound oracle problem (or vice-versa) undermines data reliability on the blockchain regardless [19]. Unfortunately, we still lack ad hoc empirical research to better understand how to efficiently address the "dual" oracle problem in the energy and other sectors. Drawing upon the selected literature, it is possible to extend the conditions described by Frankenreiter [19] and Egberts [28], for which the oracles represent a problem. Table 1 summarizes the findings of this review.

Table 1. Oracle problem: conditions and implications.

Condition	Description	Implication	Example	Source
Trusted Oracle	To what extent a specific oracle is perceived trustworthy	Untrusted oracle leads to untrusted blockchain data	Academic Institutions, Supply Chain	Antonopoulos and Woods [18], Mougayar [69]
Dual Oracle	Condition in which oracles intervene in two (or more) different and unrelated stages of the blockchain application	Tampering or malfunction of one oracle would undermine the whole process	Resource management (e.g., energy)	Damjan [19]
Multiple Oracle	Data are verified and uploaded on the blockchain by multiple oracles	Practical for publicly available data, proven to be a point of failure for sensitive and private data	Health Records, Entertainment	Dale [58], Shawdagor [99]
Hierarch Oracle	Certain oracles have predominance over others	Smart contracts may be denied or reverted	Contracting and Law	Frankenreiter [3], Guadamuz [44]
Twin Oracle	Oracles are equally valid but are substitutes	The choice of oracle gives more power to one party over the other	IPRS Protection	Fink and Moscon [30], Shatkovskaya [41]

It is indeed evident that the oracle problem is hardly addressable from only a technical point of view. In the case of twin oracles, for example, it has only social impacts. A project like Chainlink is exceptionally effective against data tampering and oracle malfunction, but it can hardly fight “distrust”. Arguably, having a trustworthy rather than a “bug-free” environment constitutes a better starting point to address the oracle problem.

6. Conclusions

Too often, the words bitcoin and blockchain are confused, and it is evident that most of the papers address characteristics that strictly belong to Bitcoin, rather than to regular blockchains. Furthermore, the literature neglects that when implemented in the real world, smart contracts need oracles to operate. This paper investigates the roles of oracles in real-world applications. Oracles are the only means of communication for blockchain with the real world, and unlike blockchain nodes, they are centralized and exposed to tampering and manipulations. The risk of oracles being compromised and feeding the blockchain with false information is called the “oracle problem”. The oracle problem biases all real-world applications, but its impact varies according to the application itself. The most promising and discussed smart contract applications, such as IPR protection, energy production, healthcare, supply chain management, academic transcript, and legal contracts, are thus analyzed. The analysis provided in this study supports the view that the oracle problem inevitably affects real-world applications. However, the impact is different, and it strictly depends on the trustworthiness of the system in which it is implemented. As hypothesized by Antonopoulos and Woods [18], although less decentralized, the academic sector is one in which the oracle problem represents the lowest threat. On the other hand, in the energy sector, in which the oracle problem is dual and control over production is decentralized, the oracle problem represents a real issue.

By investigating the oracle problem within real-world blockchain examples, the following research question also emerge:

- **IPRs**: Who should supervise the oracles when uploading patents on the blockchain? Can the system be self-sufficient?

- **ACADEMIC RECORDS**: Considering reputation as the main counter to the oracle problem, is it possible to create a shared platform for systems such as ECTS? Can student skills be recorded on the blockchain?
- **ENERGY**: Considering oracles as weak points, is it possible to manage an energy market platform without a central authority? Can a trust model ensure the system to be self-sufficient and entirely decentralized?
- **SUPPLY CHAIN**: Can a firm reputation alone counter the oracle problem? If oracles are unable to prevent the upload of unwanted information, who will benefit from blockchain implementation?
- **HEALTHCARE**: Can patients themselves be oracles? Can a distributed system also guarantee privacy and security?
- **LAW**: What is the legal role of oracles? How can smart contracts be enforceable? How does one prevent illegal smart contracts?

Utilizing a sophisticated system such as Chainlink indeed reduces the chance of oracle malfunction; however, collusion or deliberate data tampering would still represent an issue. Counterintuitively, as Tsankov [74] explained, the solution to the oracle problem should be more social rather than technical. If research in the blockchain field has to go further, a significant effort from the academic and practitioner communities is required to readdress the focus of the analysis to the oracle problem. Cooperation between experts of social and technical sciences could also constitute a robust approach. On the other hand, journals could play a critical role by creating ad hoc special issues to address the oracle problem.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kumar, A.; Liu, R.; Shan, Z. Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. *Decis. Sci.* **2020**, *51*, 8–37. [CrossRef]
2. Szabo, N. Formalizing and Securing Relationships on Public Networks. Available online: https://journals.uic.edu/ojs/index.php/fm/article/view/548 (accessed on 15 February 2020).
3. Frankenreiter, J. The limits of smart contracts. *J. Inst. Theor. Econ.* **2019**, *175*, 149–162. [CrossRef]
4. Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 12 April 2020).
5. Antonopoulos, A.M. *The Internet of Money—Volume Two*; Merkle Bloom LLC: Seattle, WA, USA, 2018.
6. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
7. Chang, S.E.; Chen, Y.-C.; Lu, M.-F. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technol. Forecast. Soc. Chang.* **2019**, *144*, 1–11. [CrossRef]
8. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A.; Original, I.; Vieira, T. A Case Study for Blockchain in Healthcare: “ MedRec “ prototype for electronic health records and medical research data MedRec: Using Blockchain for Medical Data Access and Permission Management. *IEEE Technol. Soc. Mag.* **2016**, *13*, 13. [CrossRef]
9. Plant, L. Implications of open source blockchain for increasing efficiency and transparency of the digital content supply chain in the australian telecommunications and media industry. *Aust. J. Telecommun. Digit. Econ.* **2017**, *5*, 15–29. [CrossRef]
10. Hu, W.; Hu, Y.W.; Yao, W.H.; Lu, W.Q.; Li, H.H.; Lv, Z.W. A blockchain-based smart contract trading mechanism for energy power supply and demand network. *Adv. Prod. Eng. Manag.* **2019**, *14*, 284–296. [CrossRef]
11. Sung, H.-C. Prospects and challenges posed by blockchain technology on the copyright legal system. *Queen Mary J. Intellect. Prop.* **2019**, *9*, 430–451. [CrossRef]
12. Sheth, A.; Subramanian, H. Blockchain and contract theory: Modeling smart contracts using insurance markets. *Manag. Financ.* **2019**, *46*, 803–814. [CrossRef]

13. Millard, C. Blockchain and law: Incompatible codes? *Comput. Law Secur. Rev.* **2018**, *34*, 843–846. [CrossRef]
14. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
15. Ocheja, P.; Flanagan, B.; Ueda, H.; Ogata, H. Managing lifelong learning records through blockchain. *Res. Pract. Technol. Enhanc. Learn.* **2019**, *14*, 4. [CrossRef]
16. Jiang, L.; Zhang, X. BCOSN: A Blockchain-Based Decentralized Online Social Network. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1454–1466. [CrossRef]
17. Liao, D.-Y.; Wang, X. Applications of blockchain technology to logistics management in integrated casinos and entertainment. *Informatics* **2018**, *5*, 44. [CrossRef]
18. Antonopoulos, A.M.; Woods, G. *Mastering Ethereum—Building Smart Contracts and DAPPS*; O'Reilly: Sebastopol, CA, USA, 2018.
19. Damjan, M. The interface between blockchain and the real world. *Ragion Prat.* **2018**, *2018*, 379–406. [CrossRef]
20. Dalovindj, U. The Oracle Problem. Available online: https://www.reddit.com/r/Bitcoin/comments/2p78kd/the_oracle_problem/ (accessed on 2 March 2020).
21. Schaad, A.; Reski, T.; Winzenried, O. Integration of a Secure Physical Element as a Trusted Oracle in a Hyperledger Blockchain. In Proceedings of the 16th Internationla Joint Conference on e-Business and Telecommunications, Prague, Czech Republic, 26–28 July 2019; SCITEPRESS—Science and Technology Publications: Prague, Czech Republic, 2019; pp. 498–503.
22. Caldarelli, G.; Rossignoli, C.; Zardini, A. Overcoming the blockchain oracle problem in the traceability of non-fungible products. *Sustainability* **2020**, *12*, 2391. [CrossRef]
23. Caldarelli, G. Real-world blockchain applications under the lens of the oracle problem. A systematic literature review. In Proceedings of the IEEE International Conference on Technology Management, Operations and Decisions, Marrakech, Morocco, 25–27 November 2020.
24. Cohney, S.; Hoffman, D.A.; Sklaroff, J.; Wishnick, D. Coin-Operated Capitalism. *Columbia Law Rev.* **2019**, *119*, 591. [CrossRef]
25. Jamison, M.A.; Tariq, P. Five things regulators should know about blockchain (and three myths to forget). *Electr. J.* **2018**, *31*, 20–23. [CrossRef]
26. Lucena, P.; Binotto, A.P.D.; Momo, F.D.; Kim, H. A Case Study for Grain Quality Assurance Tracking based on a Blockchain Business Network. *arXiv* **2018**, arXiv:1803.07877.
27. Kamath, R. Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *J. Br. Blockchain Assoc.* **2018**, *1*, 1–12. [CrossRef]
28. Egberts, A. The Oracle Problem—An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems. *SSRN Electron. J.* **2017**. [CrossRef]
29. Yermack, D. Corporate governance and blockchains. *Rev. Financ.* **2017**, *21*, 7–31. [CrossRef]
30. Finck, M.; Moscon, V. Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC Int. Rev. Intellect. Prop. Compet. Law* **2019**, *50*, 77–108. [CrossRef]
31. Bauer, I.; Zavolokina, L.; Leisibach, F.; Schwabe, G. Exploring Blockchain Value Creation: The Case of the Car Ecosystem. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019. [CrossRef]
32. Antonopoulos, A.M. *The Internet of Money—Volume Three*; Merkle Bloom LLC: Seattle, WA, USA, 2019.
33. Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger* **2019**, *4*, 1–39. [CrossRef]
34. Glaser, F. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. In Proceedings of the 50th Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017; pp. 1543–1552. [CrossRef]
35. Grover, P.; Kumar Kar, A.V.I.P. Blockchain for Businesses: A Systematic Literature Review. *Int. Fed. Inf. Process.* **2018**, *7*, 325–336.
36. Mamun, M. How Does Hyperledger Fabric Works? Available online: https://medium.com/coinmonks/how-does-hyperledger-fabric-works-cdb68e6066f5 (accessed on 28 February 2020).
37. Swan, M. *Blockchain: Bluepring for a New Economy*, 1st ed.; O'Reilly: Sebastopol, CA, USA, 2015.
38. Alharby, M.; van Moorsel, A. Blockchain Based Smart Contracts: A Systematic Mapping Study. *arXiv* **2017**, arXiv:1710.06372.

39. Morkunas, V.J.; Paschen, J.; Boon, E. How blockchain technologies impact your business model. *Bus. Horiz.* **2019**, *62*, 295–306. [CrossRef]
40. Jirgensons, M.; Kapenieks, J. Blockchain and the Future of Digital Learning Credential Assessment and Management. *J. Teach. Educ. Sustain.* **2018**, *20*, 145–156. [CrossRef]
41. Shatkovskaya, T.V.; Shumilina, A.B.; Nebratenko, G.G.; Isakova, J.I.; Sapozhnikova, E.Y. Impact of technological blockchain paradigm on the movement of intellectual property in the digital space. *Eur. Res. Stud. J.* **2018**, *21*, 397–406. [CrossRef]
42. Sawa, T. Blockchain technology outline and its application to field of power and energy system. *Electr. Eng. Jpn.* **2019**, *206*, 11–15. [CrossRef]
43. Ben Fekih, R.; Lahami, M. *Application of Blockchain Technology in Healthcare: A Comprehensive Study*; Springer International Publishing: New York, NY, USA, 2020; Volume 12157, ISBN 9783030515164.
44. Guadamuz, A. All watched over by machines of loving grace: A critical look at smart contracts. *Comput. Law Secur. Rev.* **2019**, *35*, 105338. [CrossRef]
45. Kim, H.M.; Laskowski, M. Toward an ontology-driven blockchain design for supply-chain provenance. *Intell. Syst. Account. Financ. Manag.* **2018**, *25*, 18–27. [CrossRef]
46. Ramachandran, A.; Kantarcioglu, D.M. Using Blockchain and smart contracts for secure data provenance management. *arXiv* **2017**, arXiv:1709.10000.
47. Buck, J. Blockchain Oracles Explained. Available online: https://cointelegraph.com/explained/blockchain-oracles-explained (accessed on 1 March 2020).
48. Apla What Is a Blockchain Oracle? Available online: https://blog.apla.io/what-is-a-blockchain-oracle-2ccca433c026 (accessed on 1 March 2020).
49. Curran, B. What Are Oracles? Smart Contracts, Chainlink & "The Oracle Problem. Available online: https://blockonomi.com/oracles-guide (accessed on 29 October 2020).
50. Sztorc, P. The Oracle Problem. Available online: https://www.infoq.com/presentations/blockchain-oracle-problems (accessed on 3 March 2020).
51. Liu, H.; Kuo, F.-C.; Towey, D.; Chen, T.Y. How Effectively Does Metamorphic Testing Alleviate the Oracle Problem? *IEEE Trans. Softw. Eng.* **2014**, *40*, 4–22. [CrossRef]
52. Barr, E.T.; Harman, M.; McMinn, P.; Shahbaz, M.; Yoo, S. The Oracle Problem in Software Testing: A Survey. *IEEE Trans. Softw. Eng.* **2015**, *41*, 507–525. [CrossRef]
53. Pastore, F.; Mariani, L.; Fraser, G. CrowdOracles: Can the Crowd Solve the Oracle Problem? In Proceedings of the 2013 IEEE Sixth International Conference on Software Testing, Verification and Validation, Luxembourg, 18–22 March 2013; IEEE: Luxembourg, 2013; pp. 342–351.
54. Galson, S. The Oracle Problem. Available online: https://www.yld.io/blog/the-oracle-problem/ (accessed on 2 March 2020).
55. Antonopoulos, A.M. The Killer App: Bananas on the Blockchain? Available online: https://aantonop.com/the-killer-app-bananas-on-theblockchain (accessed on 3 March 2020).
56. Song, J. The Truth about Smart Contracts. Available online: https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f (accessed on 2 March 2020).
57. Harper, C. What Is ChainLink? A Beginner's Guide to Decentralized Oracles. Available online: https://coincentral.com/what-is-chainlink-a-beginners-guide-to-decentralized-oracles/ (accessed on 12 March 2020).
58. Dale, O. What Is Chainlink? Guide to The Decentralized Oracle Network. Available online: https://blockonomi.com/chainlink-guide/ (accessed on 12 March 2020).
59. Haber, S.; Stornetta, S. How to timestamp a digital document—Original blockchain paper 1991. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
60. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 9p. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 29 October 2020).
61. Hughes, A.; Park, A.; Kietzmann, J.; Archer-Brown, C. Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Bus. Horiz.* **2019**, *62*, 273–281. [CrossRef]
62. Grigoreva, E.A.; Garifova, L.F.; Polovkina, E.A. The future of digital technology in russia: Blockchain as one of the priority directions of development. *Int. J. Emerg. Technol.* **2019**, *10*, 42–46.
63. Bdiwi, R.; De Runz, C.; Faiz, S.; Cherif, A.A. Towards a New Ubiquitous Learning Environment Based on Blockchain Technology. In Proceedings of the Proceedings—IEEE 17th International Conference on Advanced Learning Technologies, ICALT 2017, Timisoara, Romania, 3–7 July 2017; pp. 101–102.

64. Camiller, A.G.A.F. *Blockchain in Education*; Publications Office of the European Union: Luxembourg, 2017; ISBN 9789279734977.
65. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
66. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
67. Treiblmaier, H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Manag. Int. J.* **2018**, *23*, 545–559. [CrossRef]
68. Mik, E. Smart contracts: Terminology, technical limitations and real world complexity. *Law Innov. Technol.* **2017**, *9*, 269–300. [CrossRef]
69. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2016.
70. Hou, J.; Wang, H.; Liu, P. Applying the blockchain technology to promote the development of distributed photovoltaic in China. *Int. J. Energy Res.* **2018**, *42*, 2050–2069. [CrossRef]
71. Mengelkamp, E.; Gärttner, J.; Weinhardt, C. Decentralizing energy systems through local energy markets: The LAMP-project. In Proceedings of the MKWI 2018—Multikonferenz Wirtschaftsinformatik, Lüneburg, Deutschland, 6–9 March 2018; Volume 2018, pp. 924–930.
72. Wu, J.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
73. Li, Z.; Bahramirad, S.; Paaso, A.; Yan, M.; Shahidehpour, M. Blockchain for decentralized transactive energy management system in networked microgrids. *Electr. J.* **2019**, *32*, 58–72. [CrossRef]
74. Tsankov, A. The "Oracle Problem" isn't a Problem, and Why Smart Contracts Makes Insurance Better for Everyone. Available online: https://medium.com/@antsankov/the-oracle-problem-isnt-a-problem-and-why-smart-contracts-makes-insurance-better-for-everyone-8c979f09851c (accessed on 2 March 2020).
75. *Arizona House Bill 2417: Signatures; Electronic Transactions; Blockchain Technology*; House of Representatives: Washington, DC, USA, 2017; pp. 1–3.
76. Jeffries, A. "Blockchain" Is Meaningless. Available online: https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning (accessed on 19 April 2020).
77. Gerard, D. The World Food Programme's Much Publicized "Blockchain" Has One Participant—i.e., It's a Database. Available online: https://davidgerard.co.uk/blockchain/2017/11/26/the-world-food-programmes-much-publicised-blockchain-has-one-participant-i-e-its-a-database/ (accessed on 17 March 2020).
78. Brownsword, R. Regulatory Fitness: Fintech, Funny Money, and Smart Contracts. *Eur. Bus. Organ. Law Rev.* **2019**, *20*, 5–27. [CrossRef]
79. Low, K.F.K.; Mik, E. Pause the blockchain legal revolution. *Int. Comp. Law Q.* **2019**, *69*, 135–175. [CrossRef]
80. Zhang, F.; Cecchetti, E.; Croman, K.; Juels, A.; Shi, E. Town Crier: An Authenticated Data Feed for Smart Contracts. Available online: https://eprint.iacr.org/2016/168.pdf (accessed on 5 March 2020).
81. Thomson, C. The DAO of ETHEREUM: Analyzing the DAO Hack, the Blockchain, Smart Contracts, and the Law. Available online: https://medium.com/blockchain-review/the-dao-of-ethereum-e228b93afc79 (accessed on 3 April 2020).
82. Graham, R. Ethereum/TheDAO Hack Simplified. Available online: https://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html (accessed on 14 April 2020).
83. Silva, D.M. Ethereum Classic is Under Attack. Available online: https://qz.com/1516994/ethereum-classic-got-hit-by-a-51-attack/ (accessed on 12 March 2020).
84. Sui, D.; Ricci, S.; Pfeffer, J. Are Miners Centralized? A Look into Mining Pools. Available online: https://media.consensys.net/are-miners-centralized-a-look-into-mining-pools-b594425411dc (accessed on 29 October 2020).
85. Radanović, I.; Likić, R. Opportunities for Use of Blockchain Technology in Medicine. *Appl. Health Econ. Health Policy* **2018**, *16*, 583–590. [CrossRef]
86. Tandon, A.; Dhir, A.; Islam, N.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
87. Yong, B.; Shen, J.; Liu, X.; Li, F.; Chen, H.; Zhou, Q. An intelligent blockchain-based system for safe vaccine supply and supervision. *Int. J. Inf. Manag.* **2020**, *52*, 102024. [CrossRef]

88. Rensaa, J.A.H.; Gligoroski, D.; Kralevska, K.; Hasselgren, A.; Faxvaag, A. VerifyMed-A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept. In Proceedings of the 2020 2nd International Electronics Communication Conference, IECC 2020, Singapore, 8–10 July 2020; pp. 73–80. [CrossRef]
89. Meinert, E.; Alturkistani, A.; Foley, K.A.; Osama, T.; Car, J.; Majeed, A.; Van Velthoven, M.; Wells, G.; Brindley, D. Blockchain implementation in health care: Protocol for a systematic review. *J. Med. Internet Res.* **2019**, *21*, e12439. [CrossRef]
90. Rupasinghe, T.; Burstein, F.; Rudolph, C.; Strange, S. Towards a Blockchain based Fall Prediction Model for Aged Care. In Proceedings of the Australasian Computer Science Week Multiconference, Sydney, NSW, Australia, 29–31 January 2019. [CrossRef]
91. Talesh, S.A. Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law Soc. Inq.* **2018**, *43*, 417–440. [CrossRef]
92. McCoy, T.H.; Perlis, R.H. Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA-J. Am. Med. Assoc.* **2018**, *320*, 1282–1284. [CrossRef]
93. Donald, T. The Most Promising Blockchain Healthcare Projects. 2020. Available online: https://blog.lumiwallet.com/the-most-promising-blockchain-healthcare-projects-2020/ (accessed on 20 October 2020).
94. Lielacher, A. Top Blockchain Healthcare Projects for 2020, Rated and Reviewed. Available online: https://www.bitcoinmarketjournal.com/top-blockchain-healthcare-projects-for-2019-rated-and-reviewed/ (accessed on 21 October 2020).
95. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef]
96. Patrick, C. What Is a Blockchain Oracle? Available online: https://medium.com/better-programming/what-is-a-blockchain-oracle-f5ccab8dbd72 (accessed on 21 October 2020).
97. Desk, A.N. Solve.Care Collaborates With Chainlink To Deliver Real-World Data For Blockchain Healthcare Services. Available online: https://aithority.com/technology/blockchain/solve-care-collaborates-with-chainlink-to-deliver-real-world-data-for-blockchain-healthcare-services/ (accessed on 20 October 2020).
98. Arenas, R.; Fernandez, P. CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018, Stuttgart, Germany, 17–20 June 2018.
99. Shawdagor, J. Solve.Care Partners with Chainlink to Revolutionize the Healthcare Sector. Available online: https://invezz.com/news/2020/10/20/solve-care-partners-with-chainlink-to-revolutionize-the-healthcare-sector/ (accessed on 22 October 2020).

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.