University of Verona

Department of Business Administration

Beyond Oracles – A Critical Look at real-world Blockchains

By: Giulio Caldarelli

Ph.D. Advisor:

Prof. Cecilia Rossignoli

Graduate School of Economics and Law

Doctoral Program in Economics and Management

Beyond Oracles – A Critical Look at Real-World Blockchains

by Giulio Caldarelli

A dissertation submitted on January, 31, 2022, to the Graduate School of Economics and Management of the University of Verona, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Dissertation Committee:

NAME	QUALIFICATION	DISCIPLINE	S.S.D.	INSTITUTION
Tamara Fioroni	Professoressa associata	Economia politica	SECS-P/01	Università degli Studi di Verona
Francesca Imperiale	Professoressa associata	Economia aziendale	SECS-P/07	Università del Salento
Mauro Romanelli	Professore associato	Organizzazione aziendale	SECS-P/10	Università degli Studi di Napoli “Parthenope”
Expert in the field				
Eleonora Veglianti	Associate Professor	Management	---	Université Catholique de Lille

Table of Contents

Thesis Introduction

In 2008, a man or a group of people under the pseudonym Satoshi Nakamoto [1] released the whitepaper for a digital currency called bitcoin. The power of bitcoin over digital currencies such as euros or dollars lay in its property of being completely autonomous and independent from central authorities and banking institutions. Thanks to its structure, bitcoin was also anonymous, transparent, immutable, borderless, and censorship resistant. Additionally, the Bitcoin protocol was programmable and allowed developers to further improve the platform, creating dedicated applications exploiting the underlying blockchain properties [2]. However, in its early development, bitcoin[1] was labeled as "illegal money" due to its anonymity features that attracted questionable activities. Therefore, although Bitcoin was considered valuable and exploitable for enterprise solutions, it was difficult to propose and advertise its technology [3]. In order to alienate the mark of "illegal money" from the underlying technology, it was relabeled as "blockchain" since the Bitcoin structure was described as a "chain of blocks" by its creator [4]. The rebranding worked, as blockchain soon began to trend; at the same time, the name change contributed to a critical misconception. Defining blockchain as the underlying technology of Bitcoin gives the idea that the two concepts are different and separable. Furthermore, referring to blockchain as the underlying technology of Bitcoin led to the idea that blockchain was responsible for the characteristics of bitcoin [5]. Therefore, some blockchain enthusiasts hypothesized that by applying blockchain to other sectors, it would be possible to replicate the same degree of decentralization transparency and security found in bitcoin.

However, apart from this imprecise assumption, another crucial characteristic of blockchain was ignored in its integration with legacy businesses. Blockchains are de facto isolated from the external world and are therefore unable to communicate with other entities or process data retrieved outside their ecosystems [6]. To "virtually" attach a real-world application to the blockchain, a communication channel between the two is required.

This communication channel was given the name oracle. In Greek mythology, oracles were able to see the future by communicating directly with the gods. On the blockchain, oracles are obviously unable to see the future, but just like the oracles of Athens, they enable communication between two separate worlds [7]. Since their role in data processing is vital for smart contract execution, oracles are allowed to bypass the complex consensus mechanism enabled by the blockchain in order to add immutable information [8]. This feature, known as "the oracle paradox" (or oracle problem), constitutes a single point of failure for real-world blockchains [9]. Considered a contradiction to blockchain principles, oracles have been said to be "two-steps back from decentralization" [10].

Therefore, proposing or launching a blockchain project without considering the role and limitations of oracles is certain to undermine its feasibility and consistency [11]. If the aim of introducing blockchain is to ensure transparency and trustworthiness in a system, adopting an unsecured and untrusted oracle would clearly not serve this purpose. A famous talk by Andreas Antonopoulos titled "banana on the blockchain" broadly discussed how the hype fueled by misconceptions about the real potential of blockchain was moving the concept more toward imagination than reality [12]. False expectations and misinterpretations of blockchain technology were rampant not only among enthusiasts and practitioners but also among the academic sector. Failing to consider the limitations imposed by oracles, many

[1] According to the literature, Bitcoin with capital B refers to the protocol, while lowercase bitcoin refers to the cryptocurrency [3].

academic papers (often published in high-impact journals) proposed blockchain applications that were unrealistic [13]. Having identified this bias in the literature, this thesis intends to provide answers to the following questions:

1) What is the oracle problem, and how do the limitations of oracles affect different real-world applications?
2) What are the characteristics of the portion of the literature that leaves the oracle problem unaddressed?
3) Who are the main contributors to solving the oracle problem, and which issues are they focusing on?
4) How can the oracle problem be overcome in real-world applications?

The first chapter aims to answer the first question through a literature review of the most current papers published in the field, bringing clarity to the blockchain oracle problem by discussing its effects in some of the most promising real-world blockchain applications. Thus, the chapter investigates the sectors of Intellectual Property Rights (IPRs), healthcare, supply chains, academic records, resource management, and law. By comparing the different applications, the review reveals that heterogeneous issues arise depending on the sector. The analysis supports the view that the more trusted a system is, the less the oracle problem has an impact.

The second chapter presents the results of a systematic review intended to highlight the state-of-the-art of real-world blockchain applications using the oracle problem as a lens of analysis. Academic papers proposing real-world blockchain applications were reviewed to see if the authors considered the oracle's role in the applications and related issues. The results found that almost 90% of the inspected literature neglected the role of oracles, thereby proposing incomplete or irreproducible projects.

Through a bibliometric analysis, the third chapter sheds light on the institutions and authors that are actively contributing to the literature on oracles and promoting progress and cooperation. The study shows that, although there is still a lack of collaboration worldwide, there are dedicated authors and institutions working toward a similar and beneficial cause. The results also make it clear that most areas of oracle research are poorly addressed, with some remaining untouched.

The fourth and last chapter focuses on a case study of a dairy company operating in the northeast region of Italy. The company applied blockchain technology to support the traceability of their products worldwide, and the study investigated the benefits of their innovation from the point of view of sustainability. The study also considers the role of oracle management, as it is a critical aspect of a blockchain-based project. Thus, the relationship between the company, the blockchain oracle, and the supervising authority is discussed, offering insight into how sustainable innovations can positively impact supply chain management.

This work as a whole aims to shed light on blockchain oracles as an academic area of research, explaining why the study of oracles should be considered the backbone of blockchain literature development.

CHAPTER 1.

UNDERSTANDING THE BLOCKCHAIN ORACLE PROBLEM. A CALL FOR ACTION

1.1. 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 [14]. However, as blockchain can execute only simple transactions, "smart contracts" are necessary to settle the terms of an agreement [15][6]. 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) [16][5]. With smart contract advanced features, above digital payments, blockchain projects could involve supply chain & traceability [17][18], healthcare [19][20], energy [21], Intellectual Property Rights (IPRS) [22], Contracting & Law [23] [24], academic records [25][26], and Media & Entertainment [27][28]. However, "buried" under the blockchain euphoria lies a fundamental issue with smart contracts rarely addressed in business and literature. As blockchains are blind to the real world, they are always dependent on "Oracles" [29]. Oracles are centralized and trusted third parties that constitute the interface between blockchains and the real world [30]. As Oracles reintroduce the concepts of trusted third parties and centralization, their implementation is often seen as a "problem" [31][32]. 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 [33][13]. As a matter of fact, the oracle problem not only undermines the feasibility of a project, but also 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 [34]. It was also shown that just 20% of the ICOs had mechanisms to protect investors embedded in the code [35]. 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 [36][37][14]. 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 [10]. 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 [30][32][6][33], rarely addresses 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 [13]. This emerging gap may lead to a considerable portion of 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.

1.2. Theoretical Background

1.2.1. 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 [38][39]. 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 [40]. 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 [17]. 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 [41]. The structure proposed by Nakamoto embodies essential characteristics that are indeed a source of hype around the technology [42].

- **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 & 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**: 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 [43]. 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 [44][45]. Regardless of its type, blockchain can be implemented in many areas. Swan [46] represents at least three valuable implementations of the technology. The first is currency, along with remittances and E-Payments. The second is social applications like notary, voting, and healthcare. The third is smart contracts, which will be outlined in-depth in the next section.

1.2.2. From Blockchain to "Smart" Contracts

The idea of smart contracts comes from the cryptographer Nick Szabo [15], 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 [47]. 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" [48]. 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 [29]. Compared to traditional contracts, smart contracts do not rely on a trusted third party to operate, resulting in low transaction costs. Particularly arousing interest over smart contracts is their <u>immutable</u> and <u>deterministic</u> components [14]. Once deployed, 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 EOAs (Externally owned accounts) 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 1.1) constitutes a classic example of how a smart contract operates.

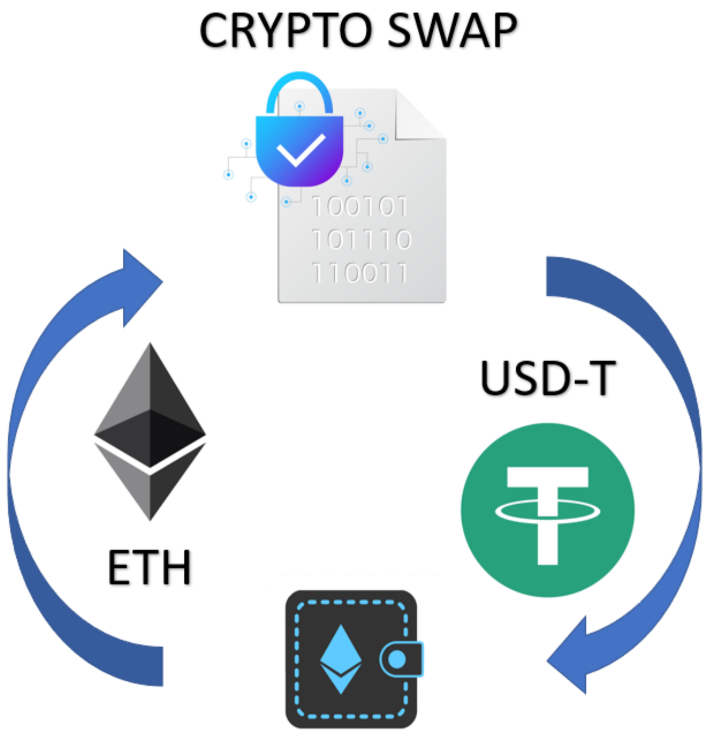

Figure 1.1. Example of a swap between Ether and USD-T

If an agent fears a market downturn and wishes to convert some volatile crypto-like Eth into some stable coin such as USD-T, she sends Ether to the swap smart contract address, and once processed, she receives USD-T 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 [49][26],
- Intellectual property rights [50][39],
- Energy production [51],
- Healthcare [19], [52],
- Contracting & Law [30], [53], and
- Supply chain & data provenance [54][55].

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.

1.3. Understanding The Oracle Problem

1.3.1. 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 [56]. In the blockchain environment, oracles are systems that provide blockchain with info coming from the real world. If smart contracts do not deal with crypto transfer but with a decentralized mechanism involving weather, stock prices, or political events, a gateway from the external world is needed [57]. 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 on 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 the right information from a trusted oracle. Examples of oracles are IoT systems like probes and sensors, platforms like 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 [58]. 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 Ether and USD-T stable coins. In that case, critical information for the smart contract to succeed, such as the Eth/USD-T exchange rate, was missing (Figure 1.2). Data like these are external to the blockchain, and without an oracle that updates rates, the contract could not be executed.

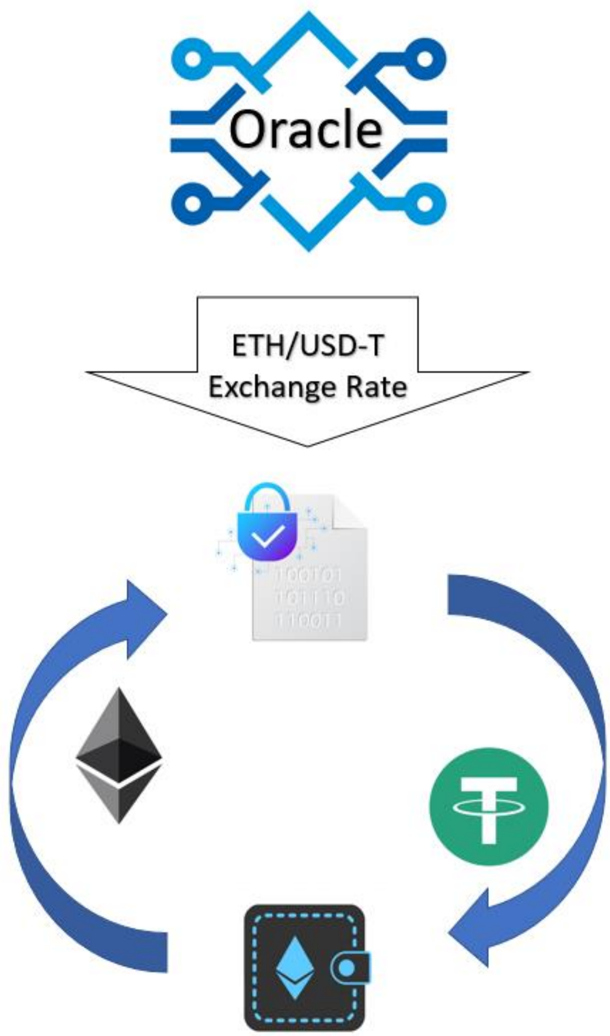

Figure 1.2. Crypto swap including an oracle

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 [59]. When all the parties cannot verify the oracle's data, and contract value increases, the oracle itself becomes a "problem".

1.3.2. 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" [60]. According to Barr et al. [61], 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" [62][63].

Regarding blockchain and smart contracts, the oracle problem involves the trustworthiness and reliability of oracles. Curran [58] 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 [31], 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 [10] extensively explains 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 more reliable than legacy systems. Brilliantly shown by Antonopoulos [12], 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 deliberated 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 [59]. 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 [64] explains 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 has been made by Chainlink [65]. 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 [66]. 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 [29]. 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 [33]. Failing to address the oracle problem poses a severe threat to investigating and developing real-world blockchain applications.

1.4. 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 the 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 additional sectors would have probably led to redundant results. Arguably, the outcome of the analysis should have reached a satisfying level of saturation.

1.4.1. IPRS Protection

As Yermack [38] shows, the original purpose of the blockchain, before the crypto 'era', was to "register" intellectual property rights. In the early 90s, Haber & Stornetta [67] proposed the digital timestamping of documents in sequence to authenticate authorship of intellectual property. Nakamoto [1] 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 [68]. Blockchain promises artists to independently determine prices and autonomously license their works in a "direct-to-fan" fashion [39]. 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 [69]. However, as Fink & Moscon [39] underlined, this procedure will not eliminate intermediaries but will simply create new ones. The critical aspect of this system consists of what Shatkovskaya [50] refers 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 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 1.3).

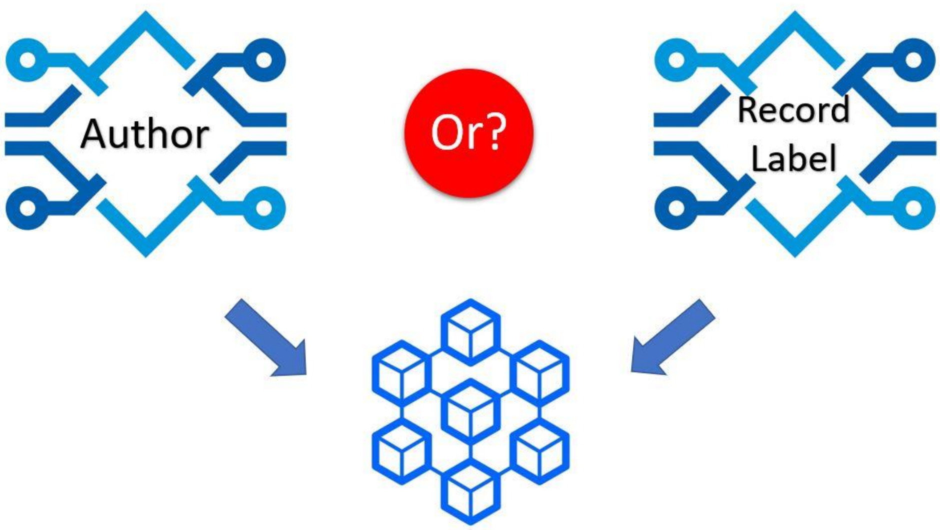

Figure 1.3. Selecting the appropriate oracle

1.4.2. Academic Transcript

A considerable part of the non-financial blockchain application is dedicated to developing a better system in the Education/Academic field [25]. In particular, decentralized technologies are sought to solve issues related to privacy, security, and vulnerability in the "ubiquitous learning environment" [70]. Blockchain-based applications could enhance the digital accreditation of personal and academic learning [71], easing complex credit management such as European Credit Transfer Accumulation System ECTS [72]. In a recent paper, Ocheja et al. [26] 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. [26] 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 1.4) and is ready for audit [49]. 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 & Woods [29] state, 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 1.4).

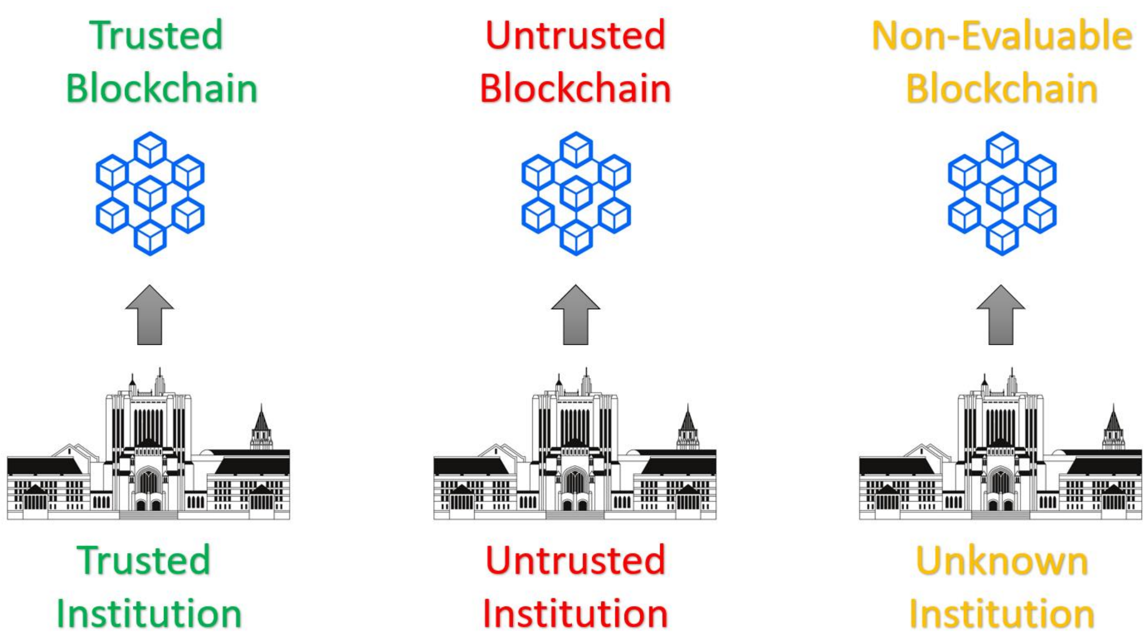

Figure 1.4. Academic institutions as trusted blockchain oracles

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.

1.4.3. Supply Chain & Traceability

Blockchain applications for secure data provenance have been investigated and supported by many articles [73][55]. An immediate consequence was implementing the data provenance system for physical products, which has rapidly aroused the interest of scholars, institutions, and firms [36][54]. The security and immutability features of blockchain should help to ensure provenance and safety for shipments of drugs, food, and critical components [74]. However, in a recent speech, Antonopoulos [12] brilliantly explains 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 [75].

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 [37], but the control over information is indeed in the hands of the producing company [32]. Companies decide then what information to upload on the blockchain, and it is improbable to spot unwanted or inconvenient data [4]. 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 [14] also shows 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 [29]. Research on the subject [33] outlines that for some products subject to a “*disciplinare*” (procedural guideline), providing false information would result in fines or license revocation (Figure 1.5).

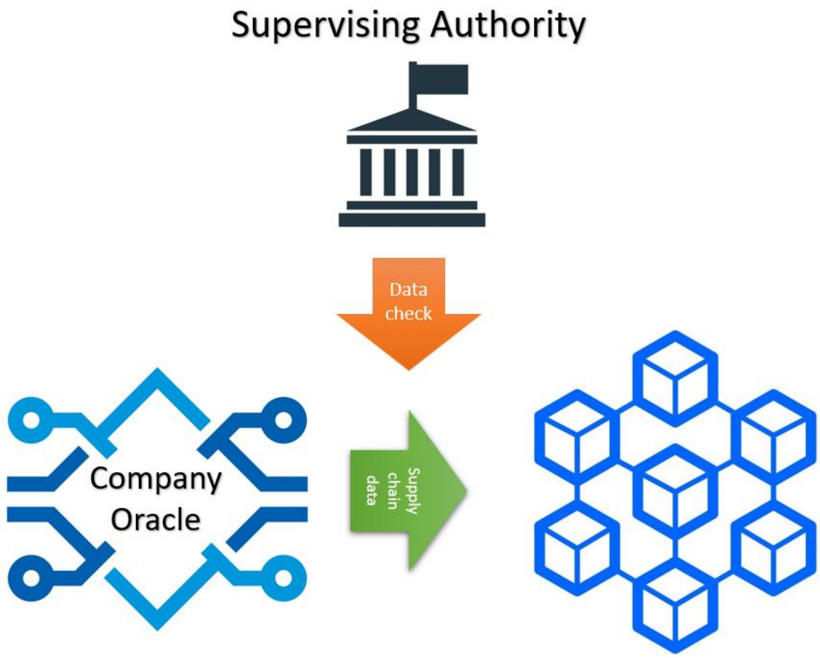

Figure 1.5. Example of a trust model [33]

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. 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.

1.4.4. 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 [76]. Projects like Energy internet and the notable Brooklyn micro-grid are undoubtedly raising expectations [77][78][79]. 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 [13]. The oracle problem for the energy sector is, in fact, "dual". It affects inbound transactions as well as outbound transactions [30]. To understand in detail how complicated this system is, we may take as an example the case of a prosumer (Figure 1.6). 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 [68]. 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 [59]. 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.

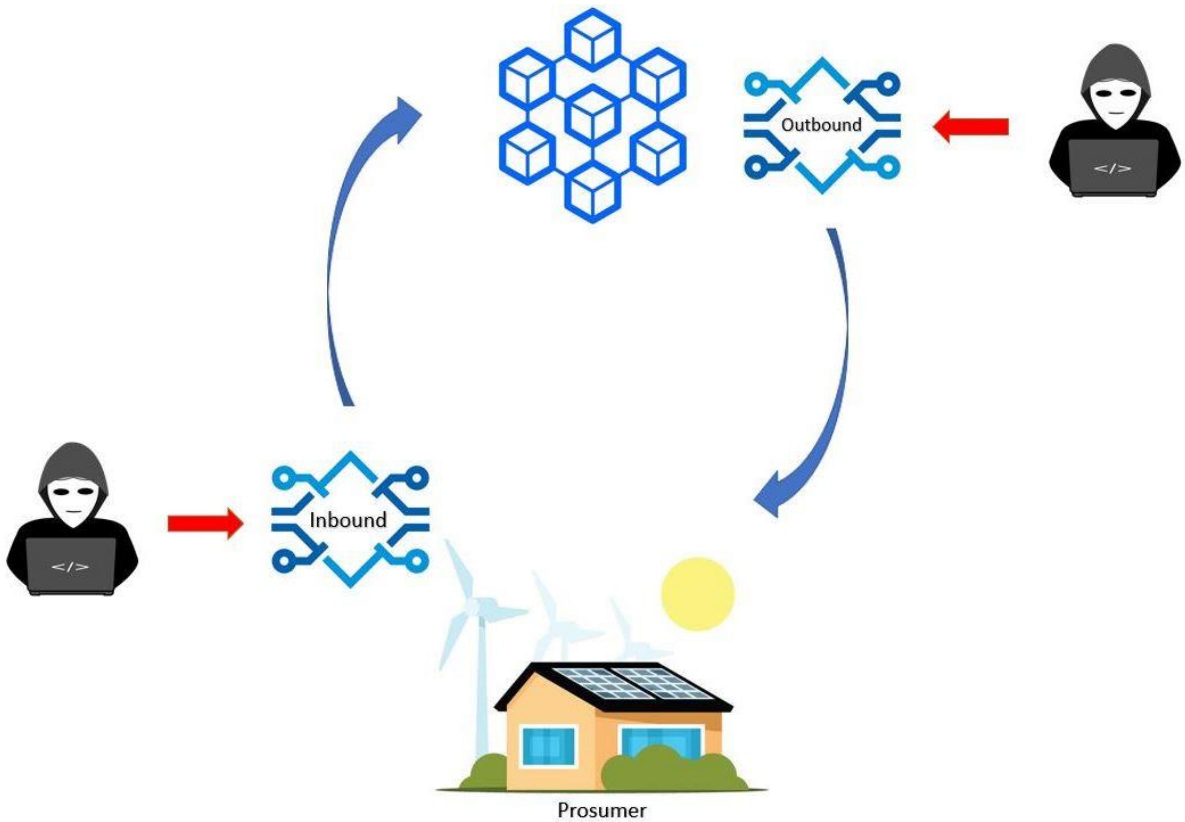

Figure 1.6. Example of the "dual" oracle problem

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 [29]. 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 [53]. 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 [30]. 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! The absence of infrastructure in the real world may not prevent the smart contract to execute successfully [29]. An external authority monitoring those procedures is essential for the system to work correctly. Additionally, it may ensure that the agent is refunded in case of malfunction [80]. 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, 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.

1.4.5. Contracting & Law

According to Guadamuz [53], 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" [81]. 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*" [82]. As 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 [83].

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*" [84], [85]. 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 [75]. 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 [30] notes that services offering oracles (e.g., Oraclize, Reality Keys) do not guarantee oracle impartiality and veracity of the information provided. They are, thus, negating the two necessary conditions for smart contracts to be legally viable. In his essay, Frankenreiter [6] underlines 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, they can influence oracles by exerting pressure on the organization controlling them [86]. 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 [64]. 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 [87]–[89]. 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 [90]. What 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.

1.4.6. Healthcare

An interesting article by Radanovic & Likic [91] forecasted the possible implementations of blockchain in the healthcare domain. Supported also by recent literature and pilot projects, technology integration may involve health records [73], health insurance [52], biomedical research [92], drug supply [93], and medical education [94]. Despite proposing different applications, the shared opinion is that blockchain technology could grant privacy and security improvements in the healthcare sector [95], [96]. The aim is indeed justified since in the field of healthcare, privacy and security breaches exponentially increase every year. Recent research shows that 37 million medical records were illegally accessed between 2010 and 2017, with 300 violations only in 2017 [97], [98]. Furthermore, there is still no unified system to store and distribute patients' information between various healthcare facilities [99]. Countless proposals and concepts of blockchain applications have been discussed to overcome those issues.

Among those, the following projects [100] 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.
- **Lockpharma** 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 [30]. Discussing the oracle problem in the case of health records, which, according to a recent literature review, has received most of the academic contributions [101], 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 figure 1.7 shows.

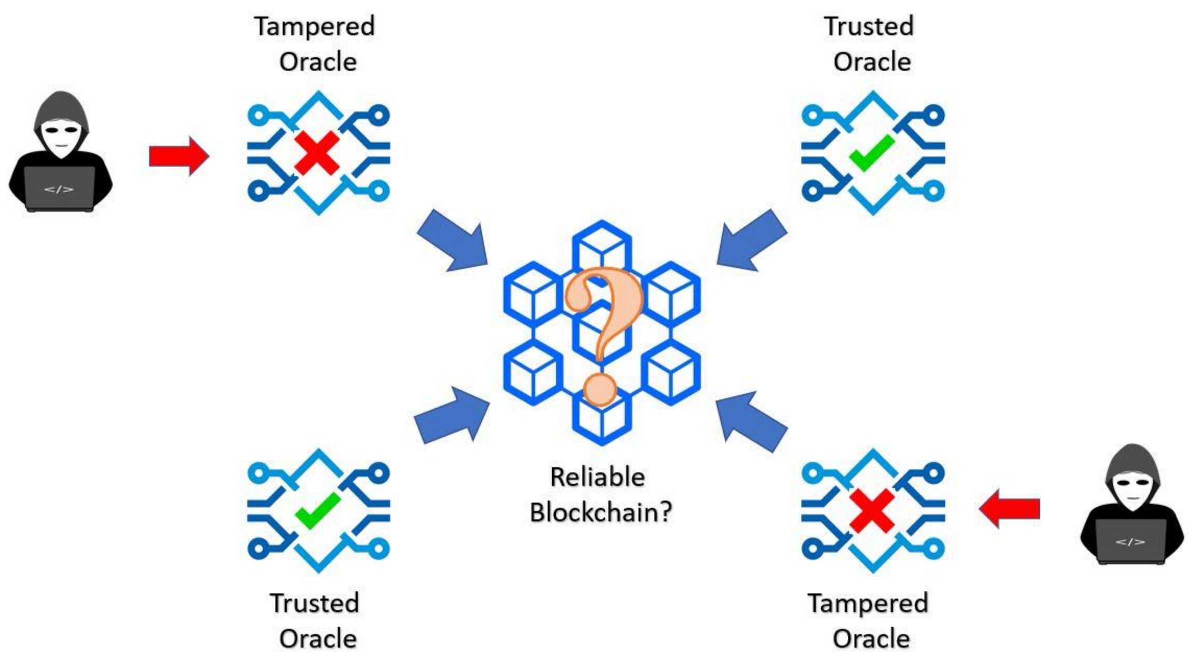

Figure 1.7. Example of distributed oracles

As discussed before, distributed oracles are a powerful way to ensure that data uploaded on the blockchain have not been tampered with [102]. 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 & Likic [91] also debate 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 has recently signed an agreement with Chainlink using external oracles to supervise sensitive data inserted on the blockchain [103]. Although promising, the reliability of this project is yet to be verified.

1.5. 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 [29]. 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 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[103]. Their relationship should then be formalized through a "trust model" [29][33]. From a game-theoretical approach, the model should describe the reason why an oracle is not incentivized to cheat on the blockchain [59].

In the IPR field, which constitutes the first blockchain application, oracles still represent an issue [50]. On the other hand, numerous prototypes have already shown promising results [39]. 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 [80]. However, it is clear that the legal aspect of protecting the IP is unlikely to be separated from central authorities [6]. Law literature offers, in fact, many contributions to the oracles and their legal implications [13]. 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 [53]. 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 to be reverted would indeed limit their power [87], [89]. However, recent studies have shown the implications of smart contracts as a means to speed up the law processes [85].

In the healthcare sector, as described in the last paragraph, blockchain could be implemented in many areas [91]. 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 [29], [33]. For the problem of doctors' trustworthiness, an effective approach could be very similar to those offered by academic institutions for student credentials [104]. 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 [39]. 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 [99]. 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 [91].

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 [13]. 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 [30]. 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 [30] and Egberts [10], for which the oracles represent a problem. Table 1.1 summarizes the findings of this review.

Table 1.1. 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	Anotonopoulos & Woods [29], Mougayar [4]
Dual Oracle	Condition in which oracles intervene in two (or more) different and unrelated stages of the blockchain	Tampering or malfunction of one oracle would undermine the whole process	Resource management (e.g., energy)	Damjan [30]
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 [66], Shawdagor [105]
Hierarch Oracle	Certain oracles have predominance over others	Smart contracts may be denied or reverted	Contracting & Law	Frankenreiter [6], Guadamuz [53]
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 & Moscon [39], Shatkovskaya [50]

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.

1.6. Conclusion

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, 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 to be compromised and feed 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 then 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 & Woods [29], 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-administrated?
- **ACADEMIC RECORDS**: Considering reputation as the main counter to the oracle problem, is it possible to create a shared platform for systems like 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-administrated 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 to prevent illegal smart contracts?

Utilizing a sophisticated system like Chainlink indeed reduces the chance of oracle malfunction; however, collusion or deliberate data tampering would still represent an issue. Counterintuitively, as Tsankov [80] explains, 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.

CHAPTER 2

REAL-WORLD BLOCKCHAIN APPLICATIONS UNDER THE LENS OF THE ORACLE PROBLEM. A SYSTEMATIC LITERATURE REVIEW

2.1. Introduction

"*When the water recedes, you can tell who on the beach was not wearing a swimsuit!*" (A.M. Antonopoulos). A group of researchers from the University of Pennsylvania compared the blockchain codes of the 50 largest initial coin offerings (ICOs) by the amount raised in dollars with what the creator promised; the researchers demonstrated that a significant portion of code was not even programmed for the planned purpose [34]. The same study also showed that only 20% of the ICOs lacked mechanisms to protect investors embedded in the code [35]. A crucial issue with smart contracts which is rarely addressed both in business and the literature has been overshadowed by blockchain euphoria. Since blockchains are blind in the real world, they are always dependent on oracles [10]. Considering that oracles reintroduce the concept of a trusted third party and centralization, their implementation is often seen as a problem [32]. Awareness of how a project addresses the oracle problem is essential for investors to make a cautious decision regarding investments, avoid fraudulent proposals and reward more realistic ICOs. The academic world, however, raises no fewer concerns. We are, in fact, assisting in the creation of an overwhelming number of papers regarding blockchain and business implementations which, apart from a few contributions [30][32][6], do not seem to address the oracle problem. Neglecting the oracle problem may lead researchers to follow unrealistic lines of enquiry based on misconceptions. Although the blockchain is famous for being trustless and immutable, real-world applications do not share the same properties. This discrepancy is the gap on which this paper investigates. The study thus aims to shed light on the state of the art of real-world blockchain applications through a systematic literature review (SLR), using the oracle problem as the lens of analysis. As the oracle problem is considered to be a major concern in the literature [3], the criterion is to recognize significative papers that mentioned and addressed this; we discarded those that did not, as their contributions would hardly be useful for practical or academic purposes. The research questions of this paper are twofold: first, we aim to determine the extent to which the literature on blockchain real-world applications is biased by not considering the oracle problem; second, we aim to discover which works have provided the most contributions to address and overcome the oracle problem. The results of the SLR show that only a fraction of the literature addresses the oracle problem; this is mostly represented by law contributions. The paper proceeds as follows. Section two introduces blockchain technology and broadly explains the importance of the oracle problem. Section three outlines the methodology. Section four summarizes the results. Section five analyzes the oracle problem contributions. Section six concludes the paper by discussing limitations and hints for further research.

2.2. blockchain oracles and the oracle problem

A blockchain is a distributed ledger and was created by a man—or a group of people—under the pseudonym of Satoshi Nakamoto to provide the technical infrastructure for the Bitcoin currency [1] [38]. Nodes on the blockchain share an exact copy of the ledger, and once approved by miners, transactions are added to the chain into new blocks [17]. Thanks to the consensus mechanism, at least on the Bitcoin blockchain, data forgery is very unlikely to happen. Depending on the consensus type, changes to the blockchain would require an enormous amount of energy or stake (currency), which may counter any benefit of a successful forgery [41]. The most known attacks on the blockchain, such as the Decentralized Autonomous Organization (DAO) and Ethereum Classic (ETC) attacks, were determined by vulnerabilities in smart contracts or an insufficient user base [87][89]. In the case of real-world applications, forgery is thus more likely to happen as smart contracts are necessary, and the user base is usually low. Despite the hype, there is not a universally accepted definition of the blockchain in the literature [43]. This is also because not all blockchains embody the same characteristics, as they may be composed of multiple types (e.g., public, private, Proof-of-Work and Proof-of-Stake). Regardless of their types, blockchains can be implemented in many areas. Swan [46] presented at least three valuable implementations of the technology: currency, along with remittances and e-payments; social applications such as notary and voting applications; and smart contracts. The idea of smart contracts was presented by the cryptographer Nick Szabo [15], but the concept did not see use until the emergence of blockchain technology [47]. On the blockchain, smart contracts are defined as "self-executing code…..that automatically implements the terms of an agreement between parties" [48].

In contrast to traditional contracts, smart contracts do not rely on a trusted third party to operate, leading to a reduction in costs. Factors particularly arousing interest for smart contracts are their immutable and deterministic components [14].

Once deployed, the smart contract code is immutable. Even deleting the contract will not cancel the transaction history that remains embedded in the blockchain on which it operates. A contract's outcome is also the same for anyone who runs it. Exclusive rights over smart contracts are not even granted to its creator. Given their characteristics, smart contracts can be implemented in a wide variety of applications such as certificates of ownership, health care, intellectual property rights, law, energy production, traceability, tourism, and entertainment. Being deterministic and immutable, however, is not sufficient to consider smart contracts as perfect and trustless. As running on a close ecosystem, they have limited ability to draw data from the external world. On the blockchain, real-world data (e.g., weather, stock prices, political events) cannot be provided along with transaction data, as other nodes would detect data coming from an untrusted source. Accordingly, data from the real world should arrive from a third party that is considered trusted and reliable by all the nodes: the oracle. Anything capable of providing external data to the blockchain can be classified as an oracle (e.g., software, sensors, humans, A.I.). Upon the execution of a smart contract concerning extrinsic data, the code will then call the right information from a trusted oracle. Oracles work as communication channels that can digest external and nondeterministic information into a format that a blockchain can understand [58]. In the case of a smart contract involving a bet for a football match, the knowledge of the winner provided by the oracle is verifiable by all the participants to the network since information about football matches is publicly available. However, in a situation in which oracles provide information that is hardly verifiable by the agents, the situation becomes different (e.g., traceability, academic records, energy production). In those environments, the trustworthiness of oracles is crucial. When all the parties are unable to verify the oracle's data, and the contract value is considerable, the oracle's presence becomes a problem [11]. In his dissertation, Egberts explained that oracles reintroduced the single point of failure and, operating on nondeterministic data, remove trustless peer-to-peer interaction. Curran [58] defined the oracle problem as "the security, authenticity and trust conflict between third-party oracles and the trustless execution of smart contracts". When attaching real assets (e.g., fruit, cars, houses) on the blockchain through a smart contract, the oracle problem is always triggered [64]. Tangible assets are indeed regulated by the jurisdiction in which they reside, meaning that they are subject to something above smart contracts. When swapping a real asset's property, such as a car, with a smart contract, the real asset location is clearly not affected by the transaction. Thus, even if its ownership has changed, the former user may not yield the asset to the new owner. In the absence of a trusted third party (e.g., government) supervising the smart contracts, their enforcement is not assured. The need for a trusted third party removes the main advantages of trustless application, which in environments afflicted by corruption represents an important constraint. Decentralized oracles effectively address oracle malfunction or failures; however, deliberate data tampering or collusion could still be performed by 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 [29][33]. Despite its indisputable importance and impact, however, only a few articles have addressed the oracle problem.

2.3. Methodology

Undertaking an SLR on real-world blockchain applications using the oracle problem as a pivot is not an easy task. First, real-world blockchains have no specific literature, and there is no particular keyword to identify this type of research. Building on the work of Song [64] and Sharma [106], real-world blockchains are those that, instead of having cryptocurrency exchange as a goal, involve transactions of services and tangible assets (e.g., copyright protection, supply chain, academic records). Intuitively, without a specific keyword, narrowing the search to the right literature cannot be completely automated. The second issue concerns the oracle problem concept itself. As the scarcity of research does not support any precise definition, the process of identifying contributions addressing the oracle problem cannot be done with software. Different authors may refer to the problem while naming it differently, or they could relate to the problem's outcome without addressing it directly. Contributions thus need to be identified by reading entire papers. This study aims to identify the most representative sample of academic papers regarding real-world blockchain applications and investigate whether they addressed the oracle problem by thoroughly reading them. The steps to find the research sample (summarized in Table 2.1) were the following: for the sample to be as inclusive as possible, only two keywords were used (blockchain, smart contracts) in the TITLE-ABS-KEY/Topic on the Scopus and Web of Science Core Collection databases. This first research returned, respectively, 2516 and 1268 entries (13/04/2020). After dropping double entries, those documents were then merged to create a unique sample. However, as the aim was to narrow real-world applications, other restrictions were added, which led to a total of 789 entries. Papers involving cryptocurrencies or specific aspects of technology and smart contracts were dropped. The first reason for this was that our sample should include only blockchain applications involving oracles. The second reason was that papers on coding or smart contract features may not address the oracle problem since they focus on other aspects. The sample was further reduced by dropping conference papers.

Although conference papers are innovative, as an incomplete piece of research, their inclusion would constitute a bias for our sample.

Table 2.1: Systematic literature review (SLR) STEPS.

Review steps	**N° Entries**
Papers gathered from SCOPUS and Web of Science Core Collection using blockchain and smart contracts as keywords	3784
Dropping papers of unrelated fields and double entries	-2995
Dropping conference papers	-576
Dropping non-English publications	-31
Dropping off-topic papers by reading abstracts and introductions	-40
Final sample	142

Basically, since the aim of this paper was to shed light on the portion of complete research that failed to address the oracle problem, including conference papers may have led to unreliable results. From a sample of 213 entries, the number was further reduced to 182, retaining only publications written in English. At this stage, all the papers were downloaded, and the abstracts and introductions were read to make sure that the content was consistent with the aim and scope of the research. The sample was then reduced to 142 entries, applying the same excluding criteria. All the papers included in the final sample counted only real-world applications not related to cryptocurrencies and not to the technical aspects of blockchains and smart contracts. All the final sample documents were read in their entirety, searching for contributions to the literature and the oracle problem. The results of the SLR are outlined in the next paragraph.

2.4. Review Results

Unfortunately, as Figure 2.1 shows, results from this literature review reflected our expectations. Of 142 analyzed papers published in academic journals, only 15 (10%) mentioned the oracle problem, although they all addressed real-world applications. Furthermore, half of them (seven articles) did not specify the oracle problem directly but outlined issues related to oracle implementations. On the other hand, oracles, which are essential for real-world applications, were mentioned only in 26 (18%) papers.

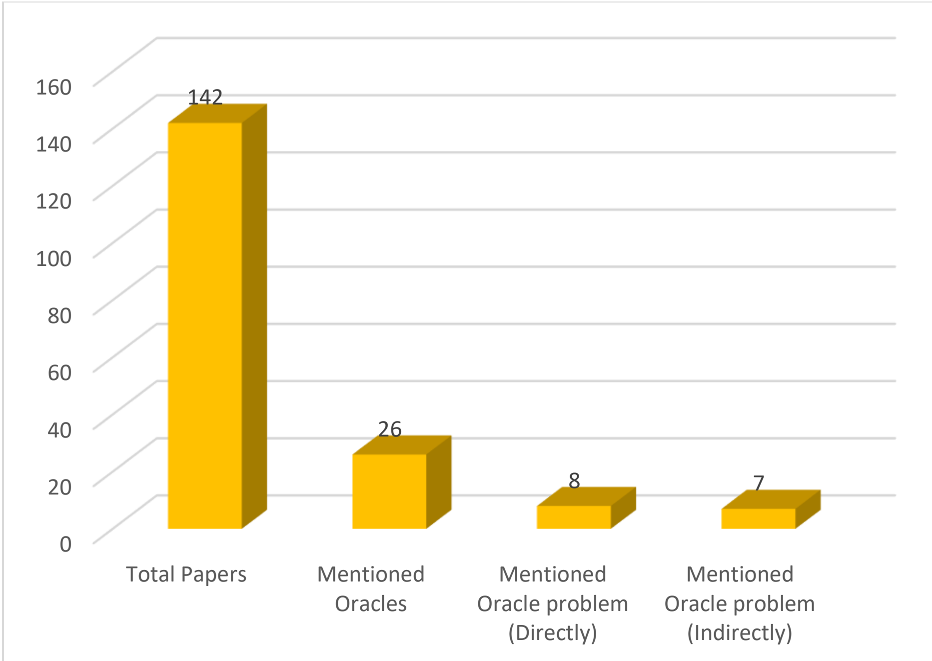

Figure 2.1. Papers addressing the oracle problem

A wide range of sectors were covered by the sample. Fields with more contributions, as shown in Figure 2.2, include energy, accounting, law, traceability and intellectual property rights.

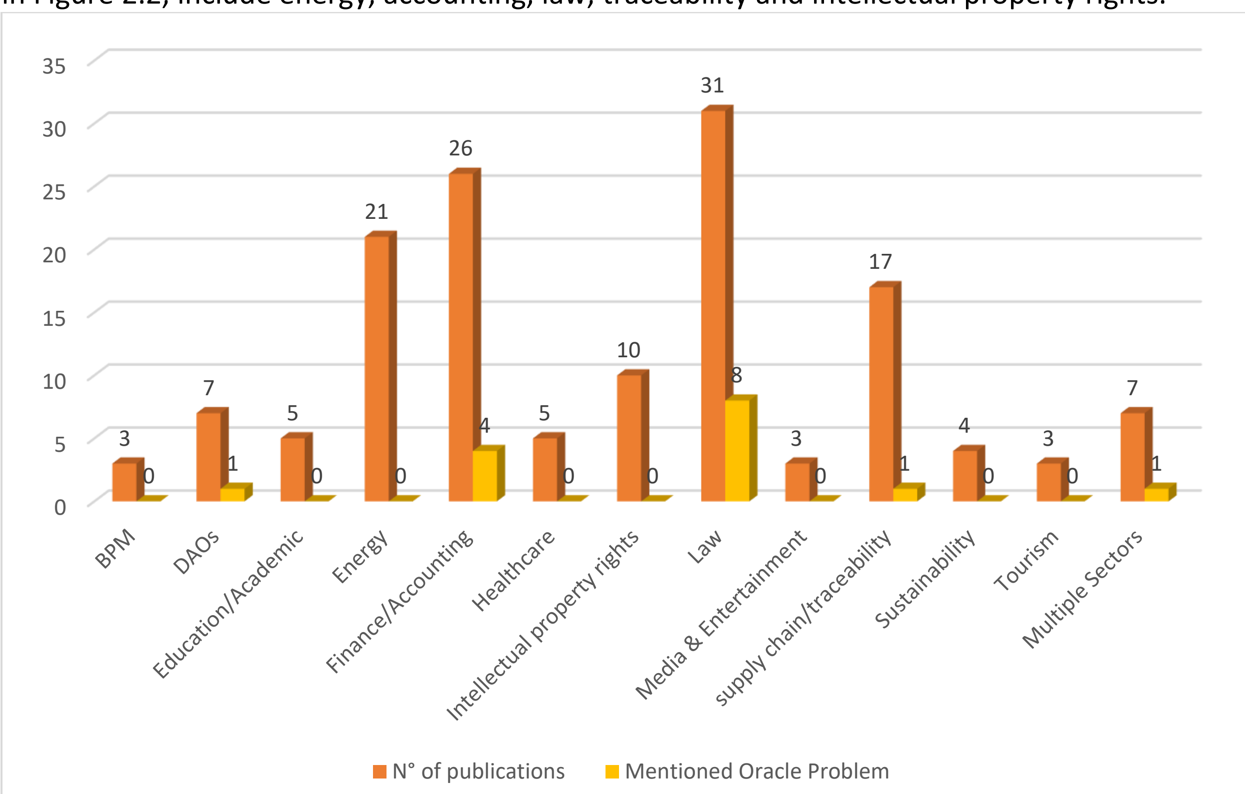

Figure 2.2. Publications/Sectors

Despite the failure of the DAO [87], the Decentralized Autonomous Organizations have continued to attract rising interest for academics, as the publication number is low but continually increasing. Entertainment, tourism and business process management (BPM) are the fields with the lowest number of contributions (three), and this trend does not seem to be increasing. On the other hand, when considering the oracle problem, the results are quite controversial. Most of the literature made no contribution to the oracle problem field. Intuitively, law and accounting count for a significant number, followed by traceability and DAO, with one contribution, while other topics were not referenced. The most surprising outcome regards the energy sector, which, despite having the second largest number of publications, did not contribute to the oracle problem issue. This gap raises several concerns about the consistency of the entire literature on the subject. Another aspect to consider is that all the papers addressing the oracle problem clearly specified the technology used for smart contracts. As the chosen technology is a critical aspect in the development of a project, it is arguable that papers defining the selected technology are more grounded and realistic. It is clear that every blockchain has specific and often unique characteristics, so building hypotheses without specifying the chosen network may hardly provide a concrete contribution. In some practitioner communities, the word blockchain is a synonym of Bitcoin, but in the academic world, those terms do not overlap [82][107].

Regarding this heterogeneity, the SLR provided another interesting research result. As Figure 2.3 shows, of 142 reviewed articles, while 73 considered Ethereum and nine were based on Hyperledger, 54 (38%) did not specify their platform. This unexpected outcome tells that, for a consistent part of the literature, the blockchain technology is somehow homogeneous, and it does not matter on which platform the smart contract operates. However, as contributions to the oracle problem show, blockchain technology is heterogeneous, and the oracles' impacts on real-world applications are dissimilar. As outlined in the next paragraph, an analysis of the oracle problem not only underlines those differences but also sheds light on the most advanced literature in real-world blockchain applications.

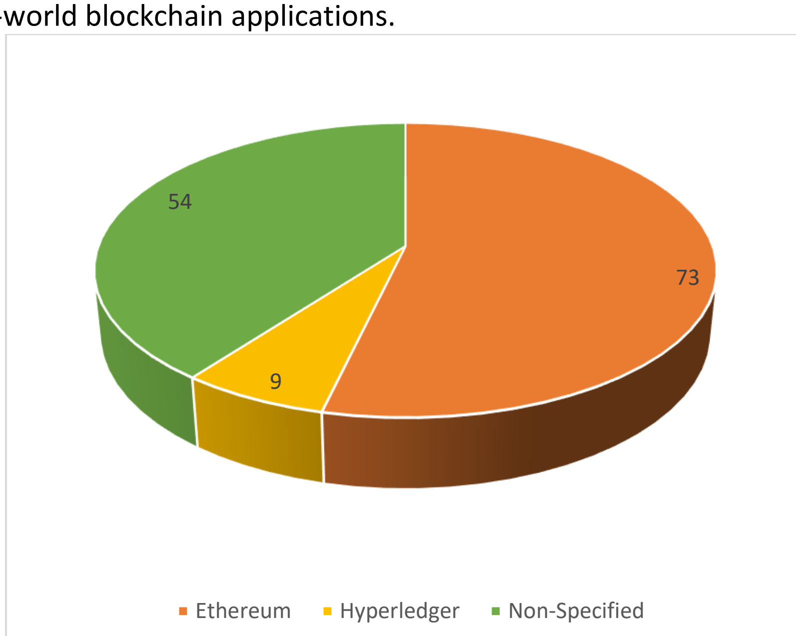

Figure 2.3: Technology Distribution

2.5. Contributions to the Oracle Problem

From Figure 2.2, it is quite clear that the law literature provided most of the contributions to the oracle problem; however, the contributions were not sufficient to respond to our second research question. Having the highest number does not imply a higher relevance of provided contributions. Despite all being real-world applications, a different sector may look at the oracle problem from different perspectives, providing a different advancement level. A comprehensive analysis (summarized in Table 2.2) is therefore offered. Addressing smart contract applications in business processes, Pereira et al. [108] argued for the inconvenience of smart contracts due to the high verification costs for the information provided by oracles. If smart contracts reduce transaction costs from one side, the issue of ensuring the trustworthiness of oracles eventually increases the costs. Although broadly negative, opinions regarding smart contracts and the oracle's role are not homogeneous, as Kumar [14] saw some positive implications for the supply chain sector. The author claimed that, compared to the improvements in the traceability system, the risk of imprecise information provided by oracles can be considered as negligible. An improved track and trace system for the fresh produce supply chain, for example, would easily spot contaminated products, which in global supply chains (GSC) are almost impossible to detect [37]. If BPM and supply chains address the oracle problem from a transaction cost perspective, different approaches might involve finance, law and DAOs, although the proposals hardly face what is legally and technologically feasible. As Rozario and Vasarhelyi [109] discussed, smart contracts have the potential to improve and enable real-time accounting; however, too many conditions need to be met for this system to work properly. The provenance of oracles needs to be trusted, as well as the data stored by them, along with their security and integrity. Cuccurù's [110] vision of blockchain stock exchange applications was less pessimistic, which, although they concern extrinsic information supplied by oracles, involve publicly accessible data. Sharing the same opinion, Dmitreva and Kessen [111] stated that publicly available information such as stock prices, although arising from centralized and untrusted sources (oracles), could create a market in an untrusted environment. The idea is that, since stock prices are public, it is easy to spot unreliable oracles, guaranteeing platform functionalities in trustless environments. Crowdfunding platforms, as another example, have already benefited from smart contract applications. As Subramanian [112] stated, despite all limits of oracles, the main obstacle to the widespread adoption of smart contracts is the lack of standardization. The presence of a reliable and univocal standard may generate the necessary trust to address and overcome the oracle problem. Indeed, trust is considered pivotal when addressing the oracle problem. Reyes [113], in her dissertation, explained that the DAO fails because it is seen as a trustless entity. Thinking of the DAO as a business trust indeed solves the oracle problem but limits its area of application. The role of trust was also stressed by Reinsberg [114], who claimed the necessity of trusted third parties to supervise the oracles' activity and for smart contract execution. Smart contracts operating across multiple nations (e.g., foreign aids) may be very unlikely to be executed in a trustless model, as an institution or a central authority is needed to ensure that goods or services are delivered to the intended receiver. If trustless operations are challenging at a transnational level, as Brownsword [84], Frankenreiter [6], and Damjan [30] explained, peer-to-peer interactions are not less complicated. When untrusted parties have to sign a contract, they should at least trust the contract law and institutions that enforce them. When signing smart contracts, people need to trust the code and the oracles that feed external information to the contracts and decide its outcome. To be trusted, an oracle's identity must be known, but in that case, its independence and impartiality are not ensured. Any member of the party or a powerful institution could indeed put pressure to alter the information provided by oracles. Mik [75] realized that smart contracts might only succeed if they can ensure perfect performance and lower transaction costs resulting from the elimination of intermediaries and traditional enforcement mechanisms. Furthermore, their code should correctly reflect the parties' commercial agreement, containing no coding errors and no security loopholes. Considering the unlikeliness of those conditions, Werbach and Cornell [115] stated that smart contracts would not determine the destruction of contract law but its improvement. The authors further explain that contract law is necessary for smart contracts and ex-post procedures; however, they can automate the execution of complex contract law. Building on this view, Guadamuz [53] hypothesized that the best use of smart contracts involves transactions of digital goods, which are unlikely to require human intervention or adjustments once settled, thus avoiding the oracle problem. On the other hand, contract law involving digital assets would be highly facilitated by smart contract implementation.

Table 2.2: Real-World Blockchain literature: state-of-the-art

Sector	State of the art
Supply chain Traceability	The advantage of having a completely traceable Global Supply Chain is greater than the risk of receiving imprecise data from oracles. However, in local supply chains, the benefit is lower.
Business Process Management	Due to oracle implementations, the reduction in transaction costs is outweighed by the increased verification costs.
Decentralized Autonomous Organizations	According to Reyes [113], the only viable business model based on the DAO, efficiently addressing the oracle problem, is the business trust.
Finance Accounting	Already proven as useful, blockchain-based platforms for crowdfunding or stock exchange only need standardization to stem the oracle problem. On the other hand, real-time accounting requires too many conditions to work properly.
Law	Due to the presence of oracles, smart contracts are unable to replace legal authorities. On the other hand, new regulations are needed for smart contracts to be efficiently implemented. Eventually, simple digital transactions, automated with smart contracts, will simplify the contract law for digital goods.

2.6. Conclusions

"Two steps back from decentralization"—with those words, Egberts [10], in the paper that contributed most to the research into the oracle problem, defined the implementation of oracles into the blockchain. With an SLR, this paper tries to shed light on the portion of biased or incomplete literature, utilizing the oracle problem as a pivot. The sample under investigation was only composed of papers analyzing blockchain and smart contracts for real-world applications, since the oracle problem is triggered in all of these situations. The SLR results showed that the majority of the published documents did not address the oracle problem, raising concerns regarding the concreteness of the currently undertaken research. It also emerged that the law literature, which made the greatest contribution to the oracle problem, seemed to be the most grounded and advanced. Investigating smart contracts from a legal point of view forces researchers and practitioners to explore the oracles' role, eventually addressing the oracle problem.

On the other hand, the fact that the energy sector provided no contributions to the oracle problem raises a few concerns regarding the concreteness of the related research. Furthermore, indirect results show that there are still many misconceptions around blockchain technology, as a consistent portion of the literature saw it as univocal. This piece of research does not question the quality of the published papers but aims to raise concerns about their real contributions for academics and practitioners. As the sample is limited, other similar research works could strengthen or evaluate the impact of the provided results using different methodologies or data.

CHAPTER 3.

OVERVIEW OF BLOCKCHAIN ORACLE RESEARCH.

3.1. Introduction

"Although oracles play a critical role … the underlying mechanics of oracles are vague and unexplored" [116]. A preliminary study on Decentralized Finance (DeFi) oracles from the University of Singapore shows that despite the massive amount of money managed by oracles on DeFi platforms, their functions and roles are still widely neglected. Despite the plethora of papers involving blockchains, less than 15% consider oracles, and an even smaller percentage further investigates related issues [13]. The subject of blockchain oracles is critical because the whole concept of blockchain applications revolves around the idea of decentralization and trustless transactions. Those pillars, however, are undermined while gathering real-world data; blockchain applications rely on centralized and trusted third parties. This issue, either addressed as an oracle problem [10] or an oracle paradox [117], makes the community of blockchain enthusiasts quite skeptical about real-world applications [13], [29]. Proposing a robust blockchain application against the oracle problem requires the redaction and discussion of the so-called "trust model," a document or scheme that broadly explains how data are fetched by oracles in a decentralized and trustless way [33], [118]–[120]. A robust trust model should first include information concerning how data collected by oracles are validated before being pushed into the smart contract. Second, it should specify how the security and unforgeability of data are ensured from the time they are collected to the moment they are permanently stored on the ledger. Third, it should outline the incentive mechanism implemented to prevent collusion or the deliberate tampering of data feeds for selfish purposes [120]–[122]. Defining and adopting a robust trust model is not only essential for a blockchain application to work properly but is also often considered the key to mass adoption [123]. However, academic contributions concerning oracles or those discussing a detailed "trust model" [13] remain scarce. On the one hand, proposing a real-world blockchain application without analyzing the oracle's role in depth poses serious doubts about the feasibility and genuineness of the underlying project [124]. On the other hand, proposals with a detailed trust model would greatly help researchers and practitioners analyze oracle-related features and issues and reproduce successful projects, respectively [11].

Therefore, knowing which institutions are actively undertaking research on blockchain oracles and which ones are already implementing them in real-world applications is interesting and important. Scholarly interest in blockchains has resulted in some literature reviews on this topic, but none has yet undertaken research through a bibliometric analysis on blockchain oracles [25], [125], [126]. A bibliometric analysis aims to identify how the body of knowledge on blockchain oracles has evolved in the last few years in terms of the leading publication outlets, the geographical distribution of research communities, the density of collaboration, and methodological approaches. Unlike classic literature reviews, a bibliometric analysis provides a quantitative and structural overview of the investigated scientific field, reducing the chances of subjective biases [127]. The advantages of undertaking this type of study are the representation of a phenomenon in a formal and objective way, ensuring the robustness and reproducibility of results. A bibliometric analysis is also meant to guide scholars who are interested in undertaking research in that sector to understand the research gaps, methodologies used, and appropriate outlets for publication. To ensure the significance, usability, robustness, and replicability of the research, this paper will follow a standard bibliometric approach that has been used in several studies across different disciplines [128]–[132]. The methodology will be extensively explained so that any individual can reproduce every passage, regardless of their expertise. The data extracted will be motivated by the associated meaning and will be presented with the aid of figures and tables. Following prior bibliometric analyses in other sectors, the collected sample will be organized based on the categories and sub-categories of the topics [131], [133]. In this study, three areas will be investigated. First, an overview of the most productive institutions (in terms of papers published), the most cited authors, and the most common publication outlets will be provided. The authors will then have a better overview of the venues that support research in this domain. Second, ongoing studies will be further investigated to identify common streams of research, themes, and research directions to incentivize cooperation and progress in the field. Third, by discussing the reviewed literature, we will highlight areas that require further investigation. The following are the objectives of the study:

Objective 1) Identify the most cited authors and productive institutions to find institutions and authors focused on the subject of the study.

Objective 2) Identify research themes, directions, and converging studies to promote cooperation and progress.

Objective 3) Highlight the areas that require further investigation**.**

We consider this study necessary, given the massive resonance of blockchain-related research and the slight growth in oracle-related investigations [11], [25]. The contributions provided in this study will help researchers and entrepreneurs know which institutions are actively involved in a specific real-world blockchain application, how oracles are implemented, and which aspects the academic studies are focusing on. Discussing the key findings of the reviewed papers can also help other academics improve the quality and speed of research in related fields [13], [106]. In contrast to other bibliometric analyses in the field of blockchains, this study focuses on oracles, a specific aspect of the technology that particularly affects real-world applications. Specific bibliometric analyses on cryptocurrencies and blockchains in healthcare or supply chains already exist, but to the best of the author's knowledge, none has focused on oracles yet.

To better understand the value and contribution of this paper, we should point out that real-world blockchains to which this study refers are applications other than cryptocurrencies, such as healthcare, supply chain, DeFi, and resource management. Therefore, specific studies on blockchain characteristics, ecosystems, and cryptocurrencies are not considered in this paper because they are not directly related to blockchain–oracle ecosystems. Furthermore, a certain degree of subjectivity, especially in the selected categories, cannot be excluded despite the rigorous research design. Given the absence of prior studies, a predetermined framework was also not available to build upon. Given the scarcity of data and the increasing academic interest in the subject, the data presented in this study may also face early obsolescence.

This paper is organized as follows: Section 2 covers the literature background, and Section 3 outlines the methodology. Section 4 summarizes the results, and Section 5 reviews the literature, identifying common themes, research directions, and converging studies. Section 6 discusses the review results and identifies areas that need further investigation. Section 7 concludes the paper by providing suggestions for further research.

3.2. Literature Background

The power of Bitcoin lies not only in its decentralized features but also in its programmability. Experts, such as Antonopoulos, address it as “programmable money” [3]. Just by using “scripts” and without the intervention of third parties, premade “agreements,” such as timelocks, Pay-to-Script-Hash, multi-signatures, can be executed on transactions [2]. However, because of Vitalik Buterin and the introduction of the Ethereum virtual machine with smart contracts, blockchains became more developer-friendly and could be easily programmed for applications above the simple exchange of cryptocurrencies [29]. Nonetheless, the Ethereum blockchain needs to be a closed ecosystem operating on data that are already on the blockchain to reproduce Bitcoin’s trustless and deterministic setting [29]. This condition is necessary to ensure that all the required data for smart contracts are publicly verifiable and auditable by all nodes [29], [82]. Without the data coming from the external world, the range of possible automated contracts would have been extremely limited [30]. Therefore, a means to deliver extrinsic data to the blockchain was needed to broaden the use of smart contracts, [6], [10], [134]. This method is called an oracle. The oracle is an entire ecosystem that permits the collection from and the transfer and insertion of external data to the decentralized application [135], [136]. As displayed in Figure 1, the oracle ecosystem usually comprises the following three parts.

Data Source: This is the source from which the data are collected and stored. It may or may not eventually be used by a decentralized application. The data source can be a Web Application Programming Interface (API), a sensor, or a human aware of a specific knowledge or event [102].

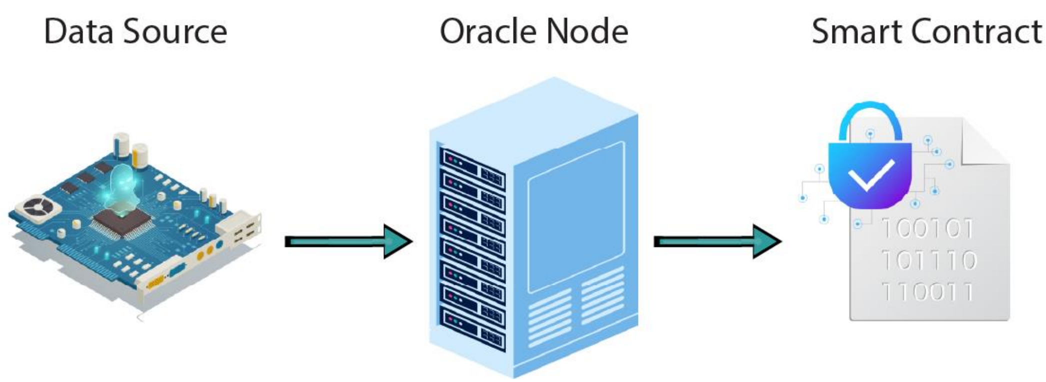

Figure 3.1. Oracle ecosystem

Communication Channel: This is usually referred to as “node.” It collects the data from the data source and delivers them to a smart contract so that the latter can be executed. Sometimes, oracle nodes coincide with blockchain nodes, but this is not always the case [30], [137].

Smart Contract: This contains the code that establishes how the collected data can be managed. Usually, it has prespecified quality criteria for data to be accepted or rejected. If necessary, it may also perform computations to deliver the appropriate data to the contract [138], [139].

Depending on how these three parts are organized and interact with each other, multiple types of oracles can be designed [123]. These three parts of an oracle are not always separate from each other, as the same entity may sometimes cover two or three roles at once. A human, for

example, can serve as a data source and communicate the data directly to a smart contract [140]. In actuality, having more than one entity that covers the role of data source/node is possible and desirable. Relying on multiple entities is, in fact, crucial to ensure the execution of smart contracts, especially when one or more data sources/nodes are malfunctioning or offline [141].
The above-described oracle ecosystem is typical of blockchains that support smart contracts (e.g., Ethereum, Tron). Instead, oracles are implemented differently for blockchains, such as Bitcoin, where smart contracts (apart from a few scripts) are unavailable. If smart contracts are unavailable, oracles are usually implemented through M-of-N (e.g., 3 out of 5) multi-signature wallets, requiring more than one signature to broadcast a transaction [142]. Therefore, the owner of a key plays the role of an oracle and executes the transaction when a certain condition is met. In that case, the oracle covers both the role of the node and the data source—for example, an agreement that sets a payment upon the delivery of a parcel (Figure 2).

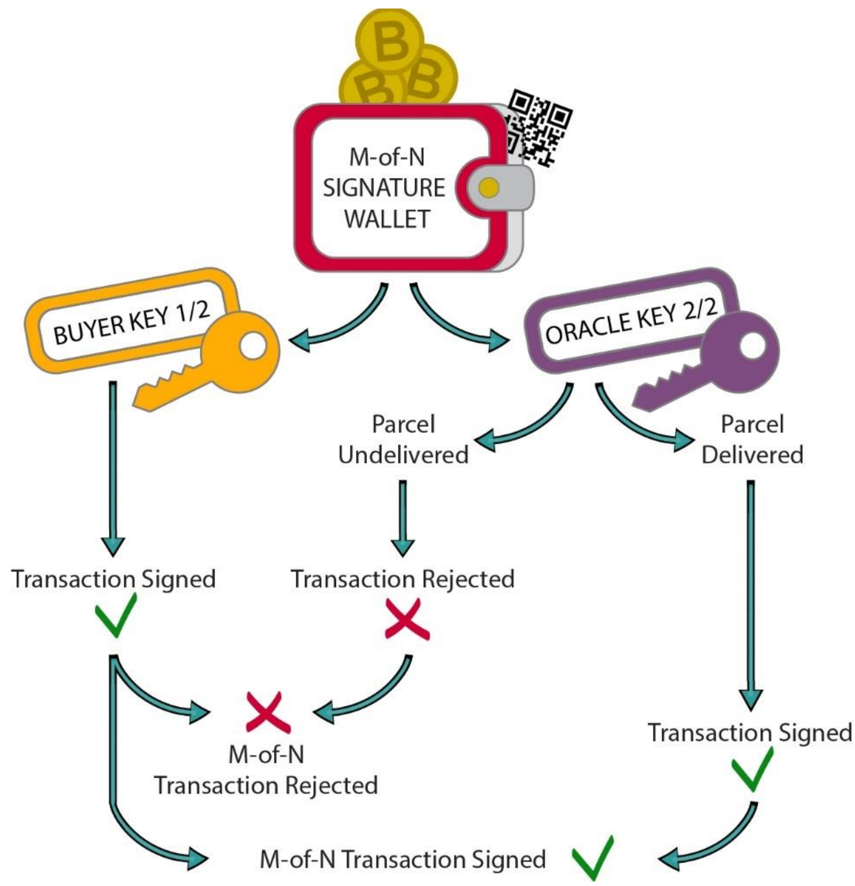

Figure 3.2. M-of-N Oracle Example

A multi-signature wallet must be set up in which one of the keys has to be entrusted to a third party that performs the role of an oracle. When the buyer acquires the product, she signs the transaction with her key. However, given that the second signature has not been inserted, the transaction remains on hold. When the parcel is delivered, the entity in control of the oracle key signs the transaction, allowing for successful execution of the transaction. Evidently, the choice of the entity that possesses the oracle key plays a crucial role in those types of ecosystems [10].

This is a trivial example of an oracle solution on the Bitcoin blockchain implemented in traceability; however, the most commonly used cases belong to the finance/gambling field [31]. A thorough explanation of all oracle types is beyond the scope of this study; however, further information can be found in dedicated papers and web articles listed in references [10], [31], [40], and [41]. Given that oracle ecosystems operate in a different way with respect to blockchains, characteristics such as immutability, transparency, and trustless execution are not ensured [14]. This discrepancy in attributes implies that when blockchain-based applications need data from the external world, the characteristics of oracles are to be taken into serious consideration. If the data source is unreliable, the node is not trusted (or private), and the smart contract is poorly audited, the fact that an application runs on the blockchain is practically irrelevant [10], [11], [145]. Depending on third parties, blockchain technology alone cannot represent a solution to centralization, trust, and security issues.

This condition, widely explained by blockchain experts such as Andreas Antonopoulos and Paul Sztorc [12], [59] and labeled by Dalovindj [31] as "the oracle problem," must be considered at the time of integrating blockchain with applications in the area of the supply chain, healthcare and academic credentials. Various consequences may be faced, depending on the faulty oracle part and the application type [8], [11], [140]. In the healthcare sector, the presence of oracles constitutes another possible source of data breach, exposing patient records to theft or manipulation [95]. In the DeFi sector, the dependency on oracles would expose decentralized applications that rely on centralized or insecure data sources to risk millions of dollars of invested capital [8], [146].

In the traceability sector, blockchain technology has been proposed, relying principally on the misconception that considering that the origin and movement of a cryptocurrency on the blockchain can be traced in a secure and trustless manner, the same can be done with a tangible asset, such as food, clothes, and medicine [12]. Because dependency on oracles for real-world applications makes it unlikely to reproduce the same level of tracking accuracy, only a few traceability projects show some robustness against that issue [14], [33]. Lately, with Non-Fungible-Tokens (NFTs) and stablecoin technology, the blockchain-based traceability of tangible products is also following another path [147]–[149]. Rather than directly tracking a real product with blockchains, companies are instead creating a representation of those on the blockchain (NFTs) to guarantee genuineness and ownership.

Because of the oracle problem, numerous critiques and concerns also arise for other blockchain applications, such as intellectual property rights management, e-government and resource management [6], [39], [75], [85].

For these applications to run genuinely decentralized and trustless, oracle ecosystems should be structured to ensure the same characteristics as blockchains. However, unlike blockchain technology, which has a history and development of nearly thirty years (considering the work of Haber and Stornetta [67] as its precursor), oracle ecosystems are relatively newer and unexplored spaces with few actors and limited literature [13]. This is the gap in which this study finds its legitimacy. It aims to shed light on academic contributions concerning blockchain oracles and promote cooperation and progress.

3.3. Methodology

An appropriate methodology should be chosen to fulfill the purpose of this study. Furthermore, an in-depth description of the steps followed had to be provided to ensure the reproducibility of the results. A bibliometric analysis was perceived as the appropriate method for reaching the goals of this research. Also, its standardized and systematic approach would ensure the reproducibility of results [128], [150]. Building on prior bibliometric analysis [151], [152], the methodology description will first involve database selection, inclusion, and exclusion criteria and, finally, data extraction variables. Regarding the data collection, the intention is to include as many articles as possible, as long as they are of an academic nature. Therefore, gray literature, such as whitepapers, opinion posts, and news, will not be considered in this research. On the one hand, although not peer-reviewed, this analysis will also consider preprints. The reason for this choice is that the included preprints are written by academics for submission to academic journals. On the other hand, non-peer-reviewed material, such as opinion posts, is not meant to follow an academic path. Following Buttice and Ughetto [133] and Martinez-Climent et al. [150], the selected databases were Scopus and Web of Science (WoS), but Google Scholar was also queried. As the analysis also comprises preprints and unpublished manuscripts, limiting the research to Scopus and WoS would not have been a coherent choice. Including a third database would also increase the chance of retrieving other relevant articles. For the three databases, the research was conducted on March 02, 2022. When “blockchain” and “oracle” were used as keywords in the TITLE-ABS-KEY of Scopus database, 312 articles were identified. In the WoS database, two strings were implemented in the “Topic” section so that articles containing the word “oracles” were also included and identified. The research returned 143 results. The Google Scholar database was queried using the same keywords as those used on the Scopus database, but the queries returned more than 10,000 entries because of their structural differences with Scopus and WoS. For that reason, and due to saturation of results, the author decided to stop the research on Page 35 (which presents 350 entries organizing results in ten per page). Table 1 summarizes the queried databases, along with the selected research strings. Appropriate exclusion criteria were adopted to narrow down the most appropriate data sample, with the aim of balancing inclusiveness with relevance. However, no restrictions based on language or timeframe were applied because of the nascency of the topic and the research goal. Given that the goal was to gather all the relevant information about oracle research, related authors, and institutions, adding a time or language restriction was a coherent choice.

Table 3.1. Databases and Research Strings**.**

Database	**Research String**
Scopus	(TITLE-ABS-KEY (blockchain) AND TITLE-ABS-KEY (oracle))
Web of Science	blockchain oracle (Topic) and blockchain oracles (Topic)
Google Scholar	blockchain, oracle (anywhere in the article)

First, the abstract and introduction were read to retrieve and exclude evidently off-topic papers. Many documents were included in the sample for mentioning “random oracles” or “test oracles,” which, despite a similar name, were not the oracles on which this study investigates. Other papers that mention Oracle, the name of a company, were also included, which, although involved in some blockchain projects, is again unrelated to the oracles discussed in this study. After following these steps, 163, 69, and 189 articles were removed from the Scopus, WoS, and Google Scholar samples, respectively. Given that gray literature was also retrieved from the Google Scholar sample, 7 other articles were removed because they were neither written by academics nor published in academic venues. After duplicates were removed, the three samples were merged, obtaining a nonredundant sample of 282 entries.

With the steps mentioned above, the obtained sample was composed of papers that included the "oracle" keyword and specifically referred to the communication channels between the blockchain and the real world. However, the aim of this paper was to present the portion of literature that not only mentioned the oracles or explained their use but also offered a direct contribution to the oracle literature. Therefore, to further skim the results, all PDF articles were downloaded and inspected one by one with a word processor. All occurrences of the word "oracle" were contextualized and analyzed. The criterion was that if oracles were mentioned in the introduction or literature review but did not constitute a central part of the analysis, the article was not included in the sample. To better explain this research step, the table in Appendix A provides a list of the research and inclusion criteria.

With this criterion, nearly half of the sample (120 papers) were discarded. Therefore, the final selection was reduced to 162 entries. In summary, because of these research steps, articles that not only mentioned blockchain oracles but also discussed their role and contributed to their development were retrieved. Table 2 broadly summarizes the methodology followed.

Table 3.2. Research Steps

Steps	**Databases**			**Total**
	Scopus	Web of Science	Google Scholar	
Papers are retrieved using research strings	312	143	350*	805
Off-topic papers are removed	163	69	189	–421
Duplicates are removed				–102
Unrelated papers are removed				–120
Final sample				162

3.3.1. Data Extraction

Appropriate extraction variables (displayed in Table 3) were identified to extract as much information as possible from the selected sample. As is probably the first bibliometric analysis on blockchain oracles, building upon existing or prior research was impossible. However, given that the aim of bibliometric analyses is relatively homogeneous, extraction variables could be taken from similar papers investigating other literature domains [133], [150], [153]. First, the "year of publication" is considered to place the literature within a specific timeframe, whereas the "element type" shows the most usual outlet for retrieved publications. "Authors," "institutions," and "countries" of provenance geographically contextualize the paper sample, highlighting the contributors to the academic advancements in the sector.

Table 3.3. Extraction variables

Variable	Description
Category	The research field of analysis
Item Type	Journal, conference, book chapter, or preprint
Year	Year of publication
First Author	Name of the first author
Authors	Full author list
Title	Title of the paper
Citations	Google Scholar citations
Outlet	Name of the journal/conference/book
Publisher	Name of the publisher
Keywords	Indexing keywords
Country	Country of the first author
Continent	The continent of the first author
Institution	Institution of the first author
Study type	Theoretical, empirical, or review

Citations and keywords were used to analyze metrics. Finally, as in Butticè and Ughetto [133], articles were further divided based on their specific fields of analysis. This categorization of papers serves to investigate whether streams of literature exist where researchers are more contributing and others that require more attention. Although it may constitute a bias, in line with prior research, articles were associated with only one field category to avoid double entries [133]. First, two main categories were identified, mainly to distinguish between studies concerning oracles themselves and oracles applied to other sectors.

Second, the papers were divided to further differentiate them based on their specific fields of analysis. Although inspired by related research, category selection embodies a certain degree of subjectivity. Therefore, a description of these categories, starting with the main ones, is provided hereafter.

Oracle Theory (OT): Under this category, papers specifically focused on blockchain oracles, either from a theoretical or a practical point of view, were included.

Oracle Applied (OA): This category included papers that focused on real-world applications, such as healthcare, finance, and business process management, and also provided a detailed analysis of the role of oracles in these fields with theoretical or experimental approaches.

The main categories were further divided into sub-categories. Hereafter, those that belong to OT are listed as follows:

Architecture: With an empirical or theoretical approach, papers in this category performed analyses on the oracle framework to improve technical aspects, highlight current challenges, and identify new avenues for research. Unlike proposals or OA papers, this group includes works that have investigated existing oracle schemes that are not directly applied to a specific sector.

Proposal: These papers propose new oracle frameworks that may be implemented in real-world applications. These may still be at a conceptual or prototype stage.

Oracle Problem: These articles focused on aspects related to the trustworthiness of oracles and their limits to decentralization. Whereas all papers should outline trustworthy oracle environments, the papers in this category focused on the involved actors' incentives to cheat and the consequences of a deviation on the underlying applications.

Sub-categories belonging to OA, such as healthcare and energy, are intuitive, but those that require clarification are described hereafter.

Data Management: Articles concerning the transfer of data from the real world to blockchain pertain to the main category of OT. In this field, articles that analyzed access data management for reputation, privacy, or GDPR purposes were considered. Cloud-computing-related research was filed under its own category, given that it mainly concerned data elaboration.

Finance: In this category were grouped articles that involved oracles applied in financial applications and those that explored timeliness and gas usage of transactions. Those concerning asset management on blockchains were also included.

IoT: This category comprised papers investigating oracles as efficient IoT systems but did not refer to a specific real-world application. A paper concerning IoT in the supply chain, for example, would instead be inserted into the "supply chain and traceability" category.

Business Process Management: This category included works that proposed blockchain integration in business processes, clearly identifying the role of oracles. Although supply chain is part of the business processes, articles specifically investigating this field were filed under their own categories.

Artificial Intelligence: Papers filed under this group concerned research toward the integration of blockchain technology into existing AI tech through the use of oracles or AI to improve oracle efficiency and reliability.

Transport: This category included papers investigating blockchain integration into intelligent vehicle development and the transport industry in general. Research on IoT device/sensors specifically implemented in the transport field were also filed in this category.

Supply Chain and Traceability: Papers investigating the benefit of integrating blockchains in the local or global supply chain belong to this category. Also included were works that concerned the traceability of physical products or documents. Works investigating the traceability of financial assets (e.g., stocks or crypto) were included instead to the finance field.

Only the first author was taken into consideration to extract the country and institution provenance of the paper. Considering all the authors would have created a bias toward articles with a higher number of authors. We were aware that this choice may eventually affect the final results, but any other option would have done the same. Regarding the authors' affiliation, the choice was to take the one declared in the last published paper to avoid the problem of double affiliation. With this criterion, some affiliations may have changed by the time the paper was published. Finally, citations were taken from Google Scholar because it was the only database in which all the papers in the sample could be retrieved. We were aware that prior studies cited in this paper utilized ad hoc programs, such as VOSviewer, for the elaboration of the result graphs. However, considering the extremely limited size of the retrieved sample, Excel tables and charts were considered to be much more intuitive. Furthermore, considering preprints from Google Scholar, software such as Bibliometrix could not be implemented. Therefore, a non-automated analysis was perceived as the most reasonable option.

3.4. Results

In this section of the paper, the results of the bibliometric analysis are reported. With a quantitative approach, the status and trends of the literature on blockchain oracles are shown. The analysis first covers the time and space of the research and then focuses on the outlets, authors, and field of analysis.

3.4.1. Number of Publications Per Year

The first academic papers considering blockchain oracles appeared in 2016 and were equally distributed among the categories "oracle theory (OT)" and "oracle applied (OA)" [154], [155]. As Figure 3 shows, interest in the topic remained low until 2018. Until 2019, the number of papers concerning OT were slightly more than those discussing OA. The increase and the shift in the trend can be observable from 2019, with 2020 having four times more publications than in 2018 and 2021 having more than double the number of publications of 2019. Moreover, the number of papers regarding OA started to exceed that of OT by 2021. Although the 2022 sample concerns only the first two months, the imbalance in the number of publications appears to be confirmed. These data reveal that the topic has gained more impact and attention among academics, probably because of the higher developments of blockchain-related platforms.

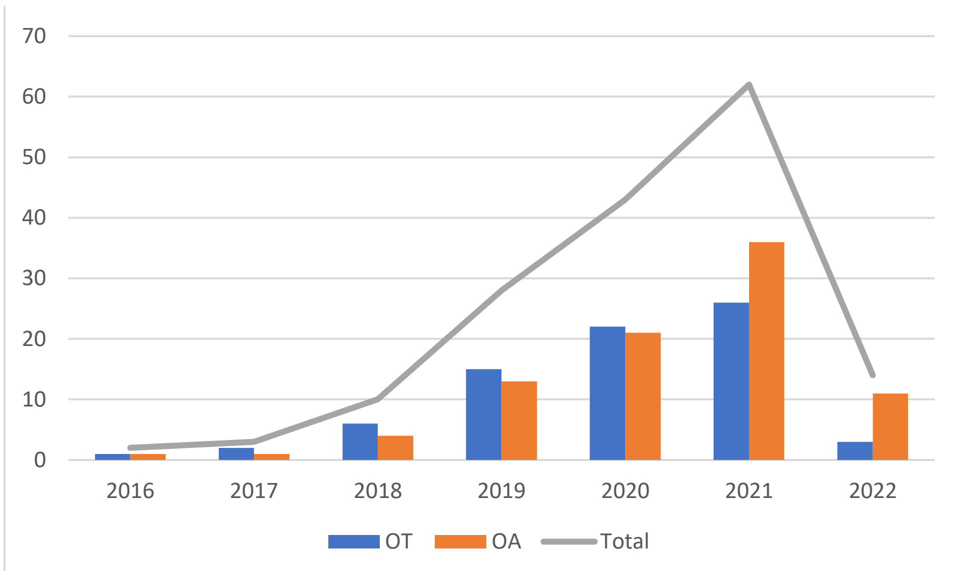

Figure 3.3. Publications per year

However, in absolute terms, the overall numbers remain low, with a peak of 62 publications in 2021 and only 162 publications in all six years of academic production. These numbers show that this is still a niche subject.

3.4.2. Productivity Rate by Geographical Distribution.

Tables 4 and 5 present the distribution of papers by country and continent, respectively. We can observe that the continents with the highest productivity are Europe and Asia, with more than 70% of total paper production. Asia, however, appears to be more focused on OA than Europe, which, although with practically the same OA contributions, presents a balance between the two main categories.

Table 3.4. Distribution among the ten most productive countries

Country	OT	OA	Total
China	10	13	23
Italy	7	11	18
USA	11	4	15
Canada	7	8	15
Germany	7	7	14

UAE	1	12	13
Australia	7	2	9
France	2	3	5
Austria	4	0	4
India	2	1	3

OT = oracle theory, OA = oracle applied.

Table 3.5. Distribution by continent

Continent	OT	OA	Total
Europe	31	36	67
Asia	18	35	53
America	18	12	30
Oceania	8	2	10
Africa	0	2	2

OT = oracle theory, OA = oracle applied.

Concerning countries, the situation partially reflects what is observed with continents. The most productive countries are China and Italy, followed by the USA and Canada. Only those four countries together accounted for more than 44% of total publications. Concerning fields, countries appear to be sufficiently balanced, except for the UAE, which is more focused on OA, whereas Australia, USA, and Austria mostly contribute to OT research.

3.4.3. Publications by Outlets and Publishers

As Figure 4 shows, the majority of papers published in this field are journals (73) and conference papers (60). However, a small portion consists of book sections (20) and preprints (9). These data contrast previous blockchain technology reviews, showing that the number of conference contributions is four times more than that of journal publications [13], [125].

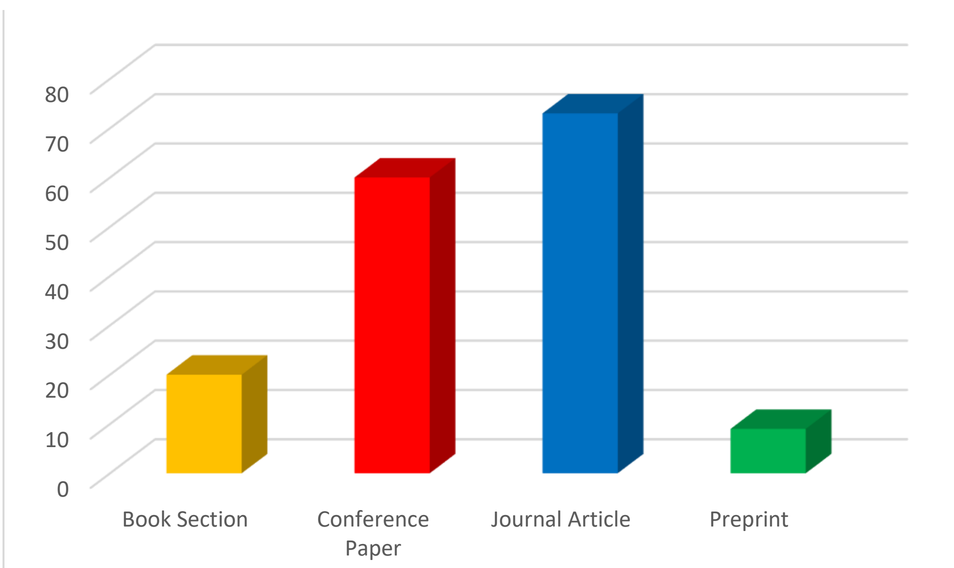

Figure 3.4. Publications per type

This finding supports the idea that there seems to be no dedicated conference venue on blockchain oracles. Table 6 and Figure 5 show the distribution of papers by journal and publisher, respectively. We observed that the majority of papers (61) are published in IEEE outlets and venues, whereas 25, 15, and 13 papers are published in Springer, Elsevier, and MDPI, respectively. However, if we consider only journal publications, the weight of the contributions would slightly change, given that 43 IEEE documents were conference papers, and of 25 Springer entries, 20 were book sections.

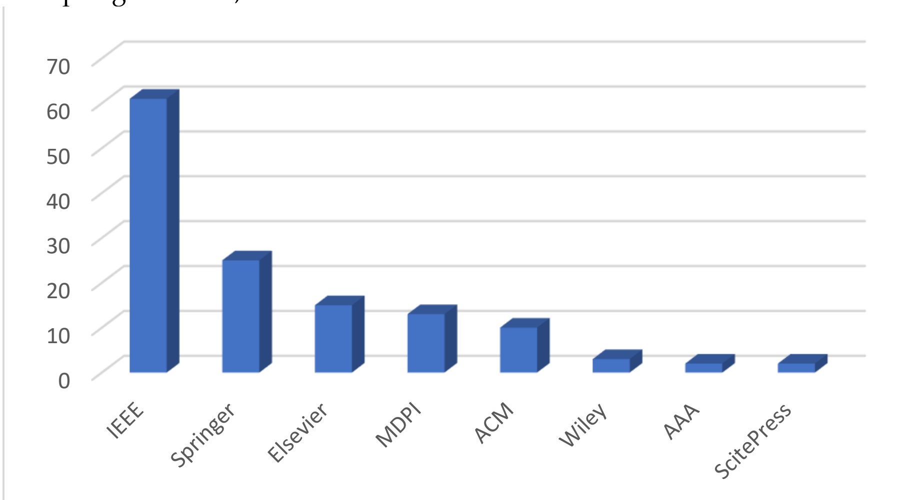

Figure 3.5. Documents by publisher**.**

Then, excluding non-journal publications, we would have IEEE with 18 publications, followed by Elsevier with 15, MDPI with 13, and Springer with 5. This information is incredibly insightful when considering Table 7, which shows that only four journals published more than two papers on the subject. Conference venues and book sections, except for two venues, contributed with no more than one document.

As shown in Table 6, the journals that published more contributions are *IEEE Access* and *Future Generation Computer Systems*, both with eight contributions. Among the other venues, the only notable is *Business Process Management: Blockchain and Robotic Process Automation Forum*, which contributed five book chapters.

Table 3.6. Documents by Journal/Venue

	Journal/Venue Name	Publisher	Contributions
Journal	IEEE Access	IEEE	8
	Future Generation Computer Systems	Elsevier	8
	Applied Sciences	MDPI	3
	IEEE Internet of Things Journal	IEEE	3
Conference	2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)	IEEE	2
	2021 IEEE Information Theory Workshop (ITW)	IEEE	2
Workshop	Business Process Management: Blockchain and Robotic Process Automation Forum	Springer International	5
	Financial Cryptography and Data Security. FC 2021 International Workshops	Springer Berlin Heidelberg	2

3.4.4. Article Type, Fields, and Keywords

Table 7 provides an overview of the paper types determined by fields based on the main categories and sub-categories indicated in the Data Extraction (3.1) section. It emerges as more than half (103); precisely, 63% are empirical papers, 23% are theoretical papers, and 14% are reviews. At the general level, the majority of academic research over oracles is of an empirical nature. Nevertheless, these data still need to be distinguished by field of research.

Concerning division by category, despite the higher number of sub-categories, the total number of papers belonging to OT (75) is slightly below those on OA (87). This is understandable, considering that oracles are still in their early-stage development, and a heterogeneity of views on how they should function and operate still exists. Although the majority of articles are still empirical, they are well balanced with theoretical and review types for the "architecture" and "oracle problem" sub-categories.

The second thing that emerges is that proposals are mainly of empirical/experimental nature, which bodes well for the birth of oracle frameworks in cooperation among or fully developed by academic institutions.

Table 3.7. Distribution by category and article type

Field		Article Type			Total
Main categories	Subcategories	Empirical	Theoretical	Review	
Oracle Theory	Oracle Problem	6	6	6	18
	Proposal	19	3	0	22
	Architecture	18	8	9	35
Oracle Applied	Finance	16	2	4	22
	Data Management	9	5	0	14
	IoT*	9	2	1	12
	BPM*	4	3	1	8
	Supply Chain & Traceability	6	1	1	8
	AI*	4	3	0	7
	Cloud Computing	4	1	0	5
	Healthcare	4	0	0	4
	Transport	2	2	0	4
	Energy	2	1	0	3

*IoT = Internet of things, BPM = business process management, AI = artificial intelligence.

Regarding "oracle applied (OA)" papers being ideally a more practical area compared to OT, why an imbalance (except for BPM, AI, and transport) exists between empirical and theoretical papers is understandable. Furthermore, the smaller category size explains why only seven review papers were retrieved. By analyzing sub-categories, we can observe that some areas have fewer contributions than others. The finance sector is leading, with 22 contributions, followed by data management (14) and the IoT (12). Given the higher advancement level of blockchain applications in these sectors and the empirical nature of academic contributions, why other sectors, such as healthcare, transport, and energy, have less than five contributions is also understandable.

Keywords are also an important parameter to consider when evaluating a sample. A total of 650 keywords were extracted from the sample, which means a media of 3,9 per article. While some articles had six or more keywords, others (mainly preprints) had none. After duplicates and plurals were removed, 307 unique keywords were found. To avoid biases with the research strings used, however, we excluded keywords such as "blockchain" and "oracle(s)" from the analysis. Keywords composed of multiple words (e.g., Smart Contract) were considered unique, and those composed of banned keywords, such as "price-oracles," were not excluded. The choice to leave keywords composed of the two banned words lies in the idea that, while those keywords alone are common for all papers, composed keywords, such as centralized oracle or blockchain interoperability, are proper in specific sectors, which will benefit from homogeneous keyword usage. Plurals were also merged with singular forms (e.g., contract/contracts). Figure 6 shows the word cloud made with all the keywords in the sample. Notably, the most frequently used keywords are smart contract and Ethereum, with 67 and 21 occurrences, respectively. Whereas the keyword smart contract says very little about our sample, the recurrence of "Ethereum" surely reflects the most common study environment on oracles that appear to be the Ethereum network. Other keywords used are internet of things (8), consensus (7), and cryptocurrencies (5), whereas some have a lower currency rate. Interestingly, of the whole sample of 307 keywords, the majority (250) occurred just once. Keywords were also divided into categories to achieve good data breakdown.

Figure 3.6. Keywords word cloud

After the most common keywords (e.g., Ethereum, Smart Contract) were excluded, excessive heterogeneity was still apparent, even after dividing them by categories. Composite keywords, such as "business process monitoring" and "business process management," were merged (e.g., business process) for consistency. In Table 8, keywords with higher occurrences divided by categories are listed. These data are useful for indexing purposes and for research to be easily retrieved by the appropriate audience. The "transport" category was excluded from the table because of excessive heterogeneity.

Table 3.8. Keywords by category

Category	Keyword	Number	Category	Keyword	Number
Architecture	Architecture	3	**AI**	Artificial Intelligence	2
	Consensus	2		Machine Learning	2
	Data	3	**BPM**	Business Process	4
	Decentralized	3		Privacy	2
	Pattern	3		Service Composition	2
	Transaction	2	**Cloud Computing**	Cloud Computing	2
	Zero Knowledge Proof	2		Fog Computing	2
Finance	Cryptocurrencies	4	**Data Management**	5G	2
	Decentralized Finance	3		Certificate	2
	DeFi	3		Cross-Chain	2
	Gas	6		Data	5
	Financial	2	**Energy**	peer-to-peer	2
	Security	2	**Healthcare**	Healthcare	2
	Transaction-fees	2		Personal Health Records	2
IoT	Internet-of-things	5	**Supply chain**	Internet-of-things	3
	IoT	5		Supply chain management	3
Proposal	Consensus	3	**Oracle Problem**	Trust	3
	Decentralized Oracle	3		Real-World	2

3.4.5. Contribution by Author/Institution and Metric

The most cited papers, authors, and contributing institutions are displayed in Tables 9, 10, and 11, respectively. Building on prior bibliometric analyses [156]–[159], the papers were ordered in terms of citations; therefore, the ten papers displayed in Table 10 are the most cited ones. However, institutions were ordered in terms of the papers produced. The list was not limited to ten but is restricted to those who provided at least three contributions. The most cited authors were selected with a mixed approach. Ordering authors by citation would have resulted in a biased list because of papers with many coauthors and citations. Therefore, to be inserted into the list, one requirement is to have produced at least two publications and to be the first author for at least one of them. The requirement of at least two publications is to avoid the insertion of authors who have randomly contributed to a related paper. Then, assuming that the first author is the lead or the most contributing author, having first-authored a paper appears to also be a necessary requirement. However, to also provide visibility to coauthors, Appendix B shows a list of coauthors who contributed to at least three papers. We were aware that a higher number of papers produced or a higher number of citations would not necessarily imply a higher impact or contribution in the field of oracle research. Such a claim would require a thorough study of academic contributions to the development of successful oracle applications, which is beyond the scope of a bibliometric analysis. In this research, a parameter, such as citations or produced papers, will correspond to a notable interest in the produced research of an author or a major effort from the institution to investigate the related field. The retrieved parameters do not reflect or question, in any case, the quality of an author's or institution's publication.

Table 3.9. Ten most cited papers

#	Title	Author/s	Year	Cit*	Institution	I/T*
1	The Blockchain as a Software Connector	Xu, Xiwei; Pautasso, Cesare; Zhu, Liming; et al.	2016	524	UNSW Sidney	CP
2	Architecture for Blockchain Applications	Xu, Xiwei; Weber, Ingo; Staples, Mark	2019	180	UNSW Sidney	BS
3	Astraea: A Decentralized Blockchain Oracle	Adler, John; Berryhill, Ryan; Veneris, Andreas; et al.	2018	121	University of Toronto	CP
4	Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System	Marbouh, Dounia; Abbasi, Tayaba; Maasmi, Fatema; et al.	2020	107	Khalifa University	JA
5	Trust management in a blockchain based fog computing platform with trustless smart oracles	Kochovski, Petar; Gec, Sandi; Stankovski, Vlado; et al.	2019	98	University of Ljubljana	JA
6	A Pattern Collection for Blockchain-based Applications	Xu, Xiwei; Pautasso, Cesare; Zhu, Liming; Lu, et al.	2018	80	UNSW Sidney	CP
7	Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges	Al-Breiki, Hamda; Rehman, Muhammad Habib Ur; Salah, Khaled; et al.	2020	77	Khalifa University	JA
8	Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance	Paik, Hye-Young; Xu, Xiwei; Bandara, H. M. N. Dilum; et al.	2019	73	UNSW Sidney	JA
9	TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing for Disintermediation	Ritzdorf, Hubert; Wüst, Karl; Gervais, Arthur; et al.	2018	58	ETH Zurich	JA

10	Blockchain for 5G: Opportunities and Challenges	Chaer, Abdulla; Salah, Khaled; Lima, Claudio; et al.	2019	55	Khalifa University	CP

*Cit = Citations (Google Scholar), I/T = Item Type, CP = Conference Paper, JA = Journal Article, BS = Book Section

As explained, information gathered with the above-mentioned approaches is provided in separate tables for clarity, but they should be discussed together to better grasp the meaning of the data.
The most cited author is Xu Xiwei (908 citations) from the University of New South Wales (UNSW) CSIRO-DATA61. She had co-authored the first two most-cited papers and four among the first ten. She started contributing to the subject in 2016, and given that her last paper on the topic was published in 2021, she appears to be still investigating the subject. All the included papers published by the UNSW are first-authored by her, except for one by Lo Sing Kuang, who is also among the most cited authors (116 citations). UNSW ranks third among the most productive institutions, with research mainly focused on oracles' architectures. The second most cited author is John Adler from the University of Toronto, who authored the third most cited paper (133 citations). In the University of Toronto, Merlini Marco is also among the most cited authors, and this institution is particularly focused on investigating decentralized oracle mechanisms. The sixth and seventh most cited authors are Omar Ilhaam A. and Al-Breiki Hamda from Khalifa University, with 107 and 97 citations, respectively. From the same university are also Battah, Ammar, and Madine, Mohammad Moussa, who are also among the most contributing authors but with fewer citations (50 and 49, respectively). Notably, Khalifa University is the most productive institution in the field, with 13 documents produced, of which 3 were among the ten most cited and 4 were among the first twenty. Observing the coauthorship, apart from the four most cited first authors, many other authors from the same university also participated in the research. Among them, Muhammad Habib Ur Rehman and Davor Svetinovic are the most cited, with 144 citations each. These findings give an idea of institutions that are heavily investing in this sector. Furthermore, this institution contributed at least one paper to every oracle application category (except for business process management [BPM] and energy). Furthermore, besides offering contributions to the healthcare and data management fields, they also produced research to address the oracle problem. Also focused on addressing the oracle problem is the University of Verona, which is ranked second by the number of articles produced.

Table 3.10. Twenty most-cited authors.

#	Name	Institution	Documents	Citations
1	Xu, Xiwei	UNSW, CSIRO-DATA61	6	908
2	Adler, John	University of Toronto	2	133
3	Lo, Sin Kuang	UNSW, CSIRO-DATA61	2	116
4	Kochovski, Petar	University of Ljubljana	2	115
5	Caldarelli Giulio	University of Verona	5	109
6	Omar Ilhaam A.	Khalifa University	2	107
7	Al-Breiki, Hamda	Khalifa University	2	97
8	Liu Xiaolong	Fujian Agriculture and Forest University	2	54
9	Carminati Barbara	University of Insubria	3	50
10	Rondanini Christian	University of Insubria	3	50
11	Battah, Ammar	Khalifa University	3	50
12	Madine, Mohammad Moussa	Khalifa University	3	49
13	Beniiche, Abdeljalil	INRS Montreal	2	44

14	Moudoud, Hajar	Sherbrook University	3	34
15	Tucci-Piergiovanni Sara	CEA-LIST	2	30
16	Di Ciccio, Claudio	Sapienza University of Rome	3	29
17	Ellul, Joshua	University of Malta	3	29
18	Merlini Marco	University of Toronto	2	26
19	Yeh, Lo-Yao	National Chi Nan University	2	18
20	Pierro, Giuseppe	University of Cagliari	2	17

However, publications from this institution are relatively recent and are not among the top-cited publications. From the same country (Italy), the University of Insubria is also among the most productive institutions, and two authors, Carminati Barbara and Rondanini Christian, are among the most cited (50 citations each). Works from this university and its researchers were mainly concerned with OA as an IoT in business processes. Another notable institution is the University of Ljubljana, whose contributions focus on cloud/fog computing and the oracle problem. The institution also belongs to the fifth most cited paper [160] and the fourth most contributing author, Petar Kochovsky, with 115 citations.

Among the most productive institutions, five other institutions emerged, whose researchers were also among the most impactful ones. These institutions include Beijing University, Technische Universität Berlin, the University of Potsdam, and the Institut national de la recherche scientifique (INRS) of Montreal. Beniiche, Abdeljalil from INRS of Montreal, is the most cited in this group (44 citations), and his main contributions focused on OT. Finally, from Technische Universität Berlin is Ingo Weber, which, although not the first author of any of the papers in the sample, has coauthored some of the most cited ones (303 total citations).

Table 3.11. Most productive institutions

#	Institution	Number	OT	OA
1	Khalifa University	13	1	12
2	University of Verona	8	5	3
3	UNSW, CSIRO-DATA61	6	5	1
4	University of Toronto	5	5	0
5	Beijing University	4	2	2
6	Technische Universität Berlin	3	1	2
7	University of Insubria	3	0	3
8	University of Ljubljana	3	1	2
9	University of Potsdam	3	0	3
10	INRS Montreal	3	1	2

3.5. Converging Studies, Research Themes, and Research Directions.

This section of the paper is dedicated to reviewing and discussing the collected studies, with the aim of extracting critical features concerning the related fields and the research direction. The objective is to understand which aspects of oracles have been investigated, which methods are used, and what results have been generated to highlight emerging research trends. Furthermore, by comparing research papers, converging studies are highlighted to promote cooperation between institutions. Appendix C also provides a complete list of papers sorted by institutions and categories to better understand the research distribution.

3.5.1. Oracle Theory

Subjects pertaining to the OT and the oracle architecture comprise many different studies. Given that oracles are a niche area of investigation, they are not officially classified by type, and their characteristics have yet to be defined. A group of studies has been dedicated to investigating common patterns that emerge from oracle architectures, with the aim of classification and improvement [143], [161]–[164]. Pasdar et al. [143] differentiated reputation-based and voting-based oracles, explaining how each design provides the answer to the smart contract. Muhlberger et al. [161] instead distinguished oracles between inbound and outbound, depending on the direction of the data flow (push and pull). Inbound oracles provide data to the blockchain, whereas outbound ones transfer data from the blockchain to the real world. Specific examples are also made of blockchain applications, where data are pushed or pulled into the smart contract. Xu et al. and Mammadzada et al. built a framework to select the most appropriate oracle design (in terms of security and data management) according to different blockchain applications [135], [162], [164].
Other works from the University of Colorado [165], Jiamusi University [166], and Hong Kong University [167] focused on the security and privacy challenges of Oracle-based smart contracts. Their research mainly concerned how to identify and prevent oracle malfunction (integrity), guarantee that data collected is exploited solely by the smart contract (confidentiality), and prevent downtime or censorship attempts (availability). A group of works from Montana State University [168], University of Sfax [169], and the University of Cagliari [170] focused instead on oracle fees and gas-price oracle malfunctions. The work of Montana State University investigated the reasons that led to gas price oracle failures, and the study from the University of Cagliari outlined the failure rate of gas price oracles with an empirical approach. The paper from the University of Sfax compared different gas-pricing techniques with the aim of improving oracle reliability.
Another central subject in OT is the oracle problem issue, for which many contributions were retrieved. A group of papers focused on explaining the oracle problem, whereas others focused more on empirically investigating the subject to overcome the issue. Two papers from the University of Ljubljana and Max-Planck Institute introduced the oracle problem from a legal point of view [6], [30]. In this paper, the oracle's role as legal actors and their responsibility as a trusted entity were investigated. A similar discussion can also be retrieved in Mezquita et al. [171], which, however, focused on the legal audit of smart contracts. A thorough discussion of the audit of the smart contract in light of the oracle problem could instead be found in two works by Mark Sheldon D. [124], [172], which first introduced the problem of auditing contracts and then offered insights for future auditors to perform the task better.
Other papers from the University of Verona and Khalifa University focused on investigating trust models and the consequences of having untrusted oracles in various sectors, such as Intellectual Property Rights (IPRs), DeFi and supply chain [118], [120]. Considering the amount of money managed by DeFi platforms, the financial implications are alarming [8], [11]. Singapore University has also confirmed this result with research focused on investigating the reliability of oracles in DeFi applications [116]. Finally, studies from the Chiba University of Technology and the University of Dallas explored, with empirical data, the incentives of oracles to cheat or fail to transmit information [173], [174]. The focus of these studies has mainly concerned the issue of how trust can be built or undermined in digital economies and how collective intelligence helps prevent selfish individuals from performing disruptive actions in the community.
The last subject of OT pertains to oracle proposals. Proposals concern elaboration from scratch or improvements of oracle trust models, such as the one discussed by Al-Breiki et al. [118]. However, because of excessive heterogeneity, finding research themes and research directions was not feasible for this category. Furthermore, proposals were retrieved in a balanced distribution among institutions in various countries, apart from being heterogeneous. Therefore, a considerable convergence of studies among institutions could not be retrieved.

Table 3.12. Oracle theory: Themes, directions, and converging studies.

Research Themes	Research Directions	Converging Studies
Oracle Architecture		

Oracle pattern	-Find a univocal Oracle Taxonomy -Distinguish between oracle types and features	Macquarie University [143] Vienna University [161]
Oracle privacy and security	-Identify and prevent oracle malfunction -Ensure data confidentiality -Guarantee censorship resistance and limit downtime periods	University of Colorado [165] Jiamusi University [166] Hong Kong University [167]
Oracle pricing and fees	-Oracle pricing techniques -Gas pricing reliability	Montana State University [168] University of Sfax [169] University of Cagliari [170]
Oracle Problem		
Oracle as a legal actor	-Define the relationship between oracles and other parties -Define oracles' responsibilities	University of Ljubljana [30] Max-Planck Institute [6]
Oracle auditing	-Define the means to detect improperly designed oracles	University of Salamanca [171] John Carroll University [124], [172]
Trust model	-Adapt a trust model design to specific blockchain applications	University of Verona [120] Khalifa University [118]
Incentive to cheat	-Define the nature and driver of trust in digital economies -Develop means to prevent selfish behavior	Chiba University of Technology [174] University of Dallas [173]

3.5.2. Oracle Applied

Oracle applied research is focused on various sectors. As expected, because of the resonance and hype that cryptocurrencies attract, finance applications constitute the widest sample. Although multiple institutions have investigated the subject, they show similarities in their focus. Studies from Concordia University, the University of Houston, and the University of Singapore focused on the very role of DeFi oracles: how they work, how they are designed, and how they interact with the underlying blockchain. Existing oracle types are also compared (in terms of efficiency), analyzing how data are retrieved, aggregated, and pushed into the blockchain [116], [146]. Kaleem and Shi [175] also provided an overview of the percentage of DeFi oracle calls over total oracle calls. They discovered that almost 75% of ChainLink oracle calls are from Synthetics, a derivative-based DeFi project. Other studies from the University of Verona and Delhi Technological University focus on known threats to DeFi oracles. Although some, such as technical malfunctions or Sybil attacks, are efficiently spotted and addressed, others, such as frontrunning or flash loans, are still difficult to prevent and sometimes even to spot [8], [176]. Three studies from Concordia University, Delhi University, and Delft University of Technology focused on the role of the oracle as a means to manipulate the market, showing the possible risks connected with its use and misuse [146], [176], [177]. Whereas the first two have a more theoretical slant, the third one with an empirical approach investigates how arbitrageurs exploit oracle vulnerabilities.

Empirical research from the Oxford-Hainan Blockchain Research Institute, Singapore University of Technology and Design, and Delft University of Technology further contributed to this field of study. The first proposed BLOCKEYE, a device able to hunt attacks on DeFi and oracle manipulations, for which the research team had already presented some experimental results [178]. Using primary data, the second showed the deviance rates of four oracle services to enlighten the oracle's reliability and possible malfunctions [116]. Finally, the third investigates how arbitrageurs' activities can influence or manipulate price oracle data feeds [177].

Another group of studies discussed how oracles intervene according to a specific financial application (e.g., loans, trading platforms, trust services) [8], [179]; however, apart from two papers from Khalifa University and the University of Clermont Auvergne, which both investigated e-auctions, the rest had heterogeneous aims. Both studies on e-auction had an experimental approach and proposed a new auction service based on the Ethereum blockchain, specifying the role of oracles and how to overcome possible security issues [180], [181]. Three studies also investigated the role of oracles in cross-chain asset transfers. Whereas the study from the University of Lisbon provides an overview of different cross-chain techniques, the work from the University of Verona discusses the utilities of the transferred tokens based on their provenance [149], [182]. Another study from Beihang University proposes PracticalAgentChain, an intermediary between the data oracle and provenance blockchains (e.g., Bitcoin, Ethereum) [183]. The system works as a reputation-based trading pool and utilizes Town Crier for reliable oracle service.

Business process management research is mainly built toward the ability of blockchains to monitor business processes efficiently. Di Ciccio et al. [184] provide an overview of how the monitoring business process with blockchain can be achieved and discuss the challenges eventually faced. An extensive description of oracle implications is provided, first by discussing how oracles should be synchronized (time management) to avoid delay of reports. Second, the reliability of oracles is discussed to ensure that the data are not manipulated. Third, the flexibility of oracles should be guaranteed so that the smart contract can select the best data source according to the monitored event. Fourth, blockchain data are aligned with real-world data so that the event sequence is not misrepresented. Concerning the timeliness and alignment of oracles, a group of works by the University of Potsdam [185]–[187] proposed a "deferred choice pattern," given that the time of transaction is not known in advance. Their model involves an extended oracle architecture to make all historical process data available (history oracle), sensitive to any unexpected change (publish–subscribe oracle), and preserve privacy and data efficiency. The last is achieved by performing part of the computation and variable evaluation off-chain (conditional oracle variants). More focused on the privacy of business process execution, works from the University of Insubria have proposed an encryption mechanism to ensure data confidentiality, even in the presence of an untrusted oracle. The works also verify the encryption data consequences on smart contracts and transaction overhead [188], [189].

As for the supply chain and traceability fields, the works seem heterogeneous, although eight entries were retrieved. Construction, fashion, and food supply chains were investigated, as well as the traceability of vehicles and COVID-19 infections [190]–[192]. Sanchez-Gomez et al. proposed that, for a blockchain traceability solution to work, it must operate on a dedicated layer/network, with traceability data separated from the blockchain data, in which a reliable data verification mechanism should be implemented. Oracles and external APIs, in their design, play a critical role [193]. Following this approach, Moudoud et al. [192] proposed collecting traceability data on a cloud, where a network of trusted oracles (recognized by the signature) approves the most reliable information. Concerning the reliability of oracles, a study by Marbouh et al. [194] proposed rules to evaluate an oracle's reputation in tracing COVID-19 cases. Thresholds also determine the oracles' inclusion or exclusion from the trusted network.

Focusing on the construction supply chain, Lu et al. [190] proposed the use of smart construction objects (SCOs) as blockchain oracles, given their intrinsic characteristics. SCOs are, in fact, able to sense the surrounding environment and efficiently communicate the information acquired. Lastly, they have the autonomy to respond to certain situations based on predefined rules. Victor and Zickau [191] proposed network operator companies as tracking oracles, given the massive presence of cellular radio towers. Finally, Powell et al. [195]discussed the issues of attaching a physical product to the blockchain in order for it to be traced by an oracle. Works from the University of Verona have also investigated this specific aspect

[33], [196]. All of these studies support the idea that a known oracle identity is fundamental to achieving this task.

For healthcare, only four papers were retrieved and were all focused on the security and access control of patients' records [197], [198]. Madine et al. [198] proposed a decentralized reputation-governed trusted oracle network for patient records to promote competition among oracles and ensure quick and reliable data transmission. However, they also proposed that, because of the sensitive nature of data transmitted, oracles should be approved by a regulatory agency. In a subsequent work in which they proposed a system of tokens to ensure patients' control of their medical records, they also debated the necessity of having a second oracle type for a time-based trigger events [197]. Research by Goncalves et al. [199] focused on the same objective but proposed a specific oracle solution with the Chainlink oracle provider and Ethereum blockchain.

Seven entries regarding applications in AI were retrieved. The central focus was to exploit automation and oracles to guarantee trust in data gathering and processing. As in the original idea of the software oracle problem, the objective was to reduce external parties' intervention in automated procedures. Works from Toulouse University and INRS Montreal investigated AI-based oracles to provide non-forged results [200], [201]. Whereas the first aimed to complete the automation of the oracle ecosystem, the second proposed a more hybrid system between humans and machines. In particular, Beniice et al. [200] demonstrated that the presence of a third party, a human or social robot, plays an important role in a blockchain-enabled trust game. The works of El Fezzazi et al. [202] and Richard et al. [203] aimed to exploit blockchain oracle features to improve machine learning processes and predictive models to reduce dependency on third-party data feeds. Both offered a theoretical overview of the blockchain implementation outcome at the concept stage.

The IoT sector has 12 publications, and the main issue of investigation is the problem faced while ensuring that the data gathered by IoT devices are trustworthy and private. Gordon [204] and Vari-Kakas et al. [205] outlined the problem of secure and trustworthy data provenance within IoT systems. The first focuses on the problem of authentication of IoT oracles on blockchains to ensure that data are submitted only by trusted oracles. It proposes that oracles submit their addresses along with data so that blockchain applications can easily verify data provenance. The second is focused on the statistical probability for an IoT oracle to deliver reliable data to the blockchain. In response to this issue, Shi et al. [206] proposed a secure and lightweight triple-trusted architecture to guarantee the unforgeability of data collected by trusted oracles. In their research, however, the premise is that oracles are trustworthy in the first place. By contrast, contributions from Khalifa University and Insubria University approached the confidentiality of the IoT. The first proposes implementing cloud computing and different access privileges to guarantee against unwanted data leakage. The second proposes an encryption model in which IoT and related data are only accessible by the intended users [119], [207]. Whereas the first is more oriented toward the technical feasibility of IoT-based blockchain data gathering, Moudoud et al. [208] proposed an ad-hoc blockchain architecture based on sharding and a peer-to-peer oracle network in order to manage IoT devices. Although at an early stage, the prototype already shows some experimental results.

As for cloud computing, only five studies were retrieved. Two were published at the University of Ljubljana and focused on how oracles can enhance trust and efficiency in a cloud computing platform. Defining the drivers of trust, a trust management scheme is proposed to show how a trusted data flow can be achieved between application components (e.g., camera, fog node, cloud storage) [160]. In subsequent work, the research is extended, showing how oracles can increase scalability and cost efficiency in federated edge-to-cloud computing environments by allowing transactions to be executed off-chain [209]. Tao and Hafid [210] also proposed introducing a computing oracle to reduce the on-chain network usage. In line with these studies, Taghavi et al. [211] proposed oracles as a monitoring service for service-level-agreement violations in cloud environments. Utilizing a Stackelberg differential game, they also investigated the perfect balance between quality verification requests and monitoring prices.

A consistent group of papers applied oracles for data management. Comuzzi et al. [212] investigated how oracles impact data quality in terms of the timeliness, costs, and availability of data. They showed that availability increases by querying an external oracle service, but so do also costs. Battah et al. [213] proposed

a reputation system to reward better-performing oracles to improve accessibility and costs, eventually increasing data quality. In subsequent work, the authors better specified the drivers to discover trusted and better-performing oracles, also showing simulation results [214].
Other authors have focused on data communication between blockchains. Mitra et al. [215] proposed DE-PEG, a modification of the PEG algorithm said to reduce the cost of data availability oracles and thought to also prevent stalling attacks. Gao et al. [216] explored active communication between blockchains through oracles, specifying which type of data should be transmitted. However, in their research, they assumed that the oracle is always trusted, so they also did not provide a scheme to prevent oracle data manipulation. Finally, Ouyang [217] proposed HBRO, an oracle system that enables communication between permissioned and permissionless blockchains concerning digital rights management (DRM). Once DRMs are elaborated on the permissioned chain, they are securely transmitted through the data oracle to a permissionless blockchain with a notary mechanism.
Works in the transport sector have focused on the security, privacy [218], [219], and efficient identification of vehicles [220], as well as data processing for intensive transport environments, such as commercial waterways [221]. Whereas the works from Khalifa University and Guangxi University discussed the implementation of Chainlink for autonomous vehicle test-case repositories and identification, the works from other universities proposed their own oracle design for efficient data transmission in the transport industry.
Finally, three entries were retrieved for the energy sector. All three were published between late 2021 and early 2022. The shared vision aims at decentralizing the energy market, but with a different focus. Antal et al. [222] proposed an energy flexibility token to incentivize renewable energy production at the local level. Zeiselmair et al. [223] implemented a decentralized oracle system and zkSNARKs to improve renewable energy certificate allocation. Lastly, Weixian et al. [224] investigated efficient oracle designs to guarantee secure and unforgeable data transmission between actors involved in the energy market.

Table 3.13. Oracle applied: Themes, directions, and converging studies.

Research Themes	Research Directions	Converging Studies
	Finance	
DeFi Oracle	-Functioning of DeFi oracles. -Compare the efficiency of existing DeFi oracles. -Analyze the DeFi oracles network usage	Concordia University [146] University of Singapore [116] University of Houston [175]
DeFi oracle manipulation	-Common attack vectors -Oracle defense mechanisms -Evaluate arbitrageurs' influence over oracle price feeds	University of Singapore [116] University of Verona [8] Delhi Technological University [176] Oxford-Hainan Blockchain Research Institute [178]
Defi applications in cross-chain transactions.	-DeFi applications and specific oracle designs -Cross-chain cryptocurrency transfer data management	China Merchant Group [179] University of Verona [8], [149] University of Lisbon [182] Beihang University [183] Khalifa University [180] Toulouse University [181]
	Business Process Management	
Business process monitoring	-Auditing of processes -Timeliness of execution	Sapienza University of rome [184]

	-Privacy and data efficiency	University of Potsdam [185]–[187] University of Insubria [188], [189]
Supply Chain Management		
Supply chain oracles	-Define the most appropriate oracle for supply chains -Define rules to establish trusted oracle inclusion/exclusion	Khalifa University [194] University of Hong Kong [190] Technische Universit¨at Berlin [191]
Supply chain data transmission.	-Define appropriate traceability data storage platforms -Discuss the attachment vector between the physical product and the blockchain	Universit´e de Sherbrooke [192] University of Seville [193] Queensland University of Technology [195] University of Verona [33]
Healthcare		
Patient records	-Healthcare oracle management -Oracle tasks in the healthcare sector	Khalifa University [197], [198] University of Antwerp [199]
Artificial Intelligence		
AI-based oracles	-Improve oracle efficiency through automation	Toulouse University [201] Montreal University [200]
Oracles and machine learning	-Reduce dependency on oracles exploiting predictive models	Sidi Mohamed Ben Abdellah University [202] Bina Nusantara University [203]
Internet of Things		
IoT as data oracles	-Ensure that data collected by IoT sensor is not forged -Ensure that only intended IoT devices are allowed to upload data on the ledger	Saint Mary's University [204] University of Oradea [205] National University of Defense Technology [206]
IoT confidentiality	-Ensure that IoT data are not leaked -Allow IoT data to be accessed only by the intended users	Khalifa University [119] University of Insubria [207]
Cloud Computing		
Application management	-Oracles as a means to reduce transaction costs and increase scalability -Oracles for Service Level Agreement management and monitoring	University of Ljubljana [160], [209] Khalifa University [211] University of Montreal [210]
Data Management		
Data privacy and quality	-Balance availability and costs	Polytechnic University of Milan [212]

	-How to prevent unwanted data access	Khalifa University [213]
Cross-chain communication	-How to prevent stalling attacks -Discuss allowed data type	University of California [215] Jinan University [217] Beijing University [216]
Transport		
Vehicle management	-Guarantee privacy in the vehicle identification -Process autonomous vehicle data	Khalifa University [218] Guangxi University [220]
Energy		
Energy market management	-Incentivize renewable energy production -Improve privacy in the energy market	Technical University of Cluj-Napoca [222] Technical University of Munich [223]

3.6. Discussion

The literature review showed some interesting insights about themes covered by the existing studies and areas that require more attention. Although a group of studies have tried to classify oracles, the very concept of oracle is still not clearly defined. Oracles are generally identified as data-feeding ecosystems, which can come in various forms or structures, but if this is the purpose of oracles, then anything that provides data for a blockchain is an oracle. Therefore, rollups or bridges should also be considered oracles. We could argue, for example, that the lighting network is an oracle for the bitcoin network, but then we may also have oracles on the lighting network. Therefore, the boundaries of what can be defined as an oracle should be clearly settled.

Classification of oracles is also quite heterogeneous, and it often reduces the clarity of the presented research. Besides software and hardware, we also have reverse, centralized, decentralized, computation, consensus, and voting-based oracles. Often, they refer to the same type with different names or to different types with the same name (e.g., decentralized and consensus-based oracles). Similarly, the issue of having trusted entities in trustless environments, often referred to as the "oracle problem," has also been labeled in some research as the "oracle paradox." Likewise, the coexistence of inbound and outbound oracles is referred to equally as the "dual-oracle problem" or "dual simplex communication." Therefore, efforts should be made in this regard so that research can build on a common oracle taxonomy.

Concerning investigation of oracle trust models, this seems to still be a niche field, and despite few contributions, the very concept of trust lacks a broader discussion and clarification. Indecisiveness on whether an oracle should be trustless or "provably honest" is apparent, which is, in theory, not really the same concept.

With regard to oracle proposals, they are heterogeneous, but almost all focus on decentralized or consensus-based oracle systems. Centralized oracles, such as the ones proposed in [217], [225], [226], should also be worthy of investigation. For certain data types that are not in the public domain and where data sources are limited, a centralized and secure data channel would be more appropriate than a slow, expensive, and probably less secure decentralized oracle type. A trusted oracle is indeed a single point of failure, but it is undoubtedly more efficient as long as it resists attacks and behaves honestly. Therefore, more research is expected and needed in that direction. Furthermore, despite the plethora of emerging oracle solutions on the market, on the academic side, the trend is to propose a new oracle solution or utilize only the most known or advertised ones (e.g., Chainlink or Provable). Therefore, an exploration of emerging oracle solutions by academic researchers is expected and required.

Another issue that emerged in this study is that studies concerning oracle solutions for DRM, such as the one by Ouyang [217], are limited. As the original idea of blockchain proposed by Haber and Stornetta [67] was to authenticate digital documents, more attention to this sector was also expected in blockchain oracle research.

Finally, concerning a well-known issue discussed in 2018 by Song [64], that is, how to link a physical object to the blockchain, an effective method to fill this gap has not been developed despite the plethora of research and proposals. This considerable limitation greatly undermines the feasibility of blockchain-based proposals and applications, especially for the traceability sector (but also in healthcare or BPM). Therefore, more than speculating on the hypothetical advantages of having a blockchain-based tracing system, a considerable effort should be made to understand whether a physical product can be “attached” to the blockchain in the first place. Building on the above-mentioned limitations, Table 14 suggests some research themes, along with their expected/desired outcomes.

Table 3.14. Suggested research themes

Field	Theme/s	Expected/desired outcomes
Oracle theory	-Contribute to a univocal oracle taxonomy	-Make oracle literature more accessible to a broader audience -Attract more research in the oracle field
	-Define the boundaries of oracles' definition	-Reduce heterogeneity within oracle literature -Improve consistency of research
	-Define the theoretical background to which the “trust” discussed in oracle literature should adhere	-Develop more robust trust models -Reduce the heterogeneity of proposals
	-Investigate resistant and trusted centralized oracle types	-Adapt oracles to specific data types with limited sources.
Oracle applied	-Integrate oracles in digital rights management	-Broaden blockchain-based intellectual property use cases.
	Investigate robust links between physical products and the blockchain	-Improve any blockchain-based application involving physical products (e.g., traceability).
	-Investigate emerging oracle solutions	-Promote active collaborations between academia and oracle providers

3.7. Conclusion

This paper undertook a bibliometric analysis of published studies about blockchain oracles. The aim was to display publication trends along with preferred outlets and publishers. The most-cited papers and authors and the most contributing institutions are also shown. After the selected literature was reviewed, emerging themes, research directions, and converging studies were discussed to promote innovation and cooperation between institutions.

The obtained results show that, within seven years of academic production, only 162 papers (including non-peer-reviewed) were retrieved in scholarly databases. This result supports the view that blockchain oracle is still a widely neglected subject, despite its crucial importance. The review also reveals heterogeneity in the oracle literature; therefore, major effort is required to find a widely accepted oracle taxonomy. Furthermore, limited oracle selection suggests the need for more active collaboration between practitioners and academia. Finally, more theoretical work is required on the underlying trust concept that identifies oracles as “trusted” ones.

The findings of this research are useful for academics, students, and practitioners. Offering an overview of institutions investigating a specific field, this study can promote cooperation between existing or entering research teams in the blockchain oracle domain. This, in turn, can constitute a reference for entrepreneurs undertaking blockchain-based projects. Students and other academics can then utilize a resource on the state-of-the-art knowledge of related fields and investigate emerging gaps (e.g., missing resource management contributions) or create other research by building on existing studies.

This paper also has limitations, given the scarcity of retrieved material that determined low numbers in absolute terms in all the tables and figures. As specified in Section 3, a degree of subjectivity in the presented results cannot be excluded. Whereas previous studies inspired the method and bibliometric research, the author had to select them arbitrarily. Subjectivity can also be found in the sample classification, given that the division of topics into categories and sub-categories had to be performed manually. Again, the author wishes to reiterate that the data provided in this paper should not, in any case, be interpreted as a quality evaluation of the cited works. Because of the selection criteria, some works or authors may have been excluded inadvertently. Further studies can build on this bibliometric analysis to investigate the trust models adopted and presented in the published literature and the preferred oracle applications for academic investigations.

Appendix 3.A. Relevant contribution example

Paper Title	**Oracle Contribution**	**Reference**
The limits of smart contracts	Provides an analysis of the role of oracle from a legal point of view	[6]
LoC—a new financial loan management system based on smart contracts	Discusses how oracles can be implemented to ensure data privacy in loan management	[227]
A pattern collection for blockchain-based applications	Describes different oracle types and how to recognize the most suitable one according to the needs	[162]
On the characterization of blockchain consensus under incentives	Compares blockchain consensus and oracle consensus under specific incentive mechanisms	[228]
Distributed network slicing management using blockchains in e-health environments	Shows the implementation of a decentralized oracle solution for the management of patient records	[199]
Blockchain for COVID-19: review, opportunities, and a trusted tracking system	Outlines a means to recognize a trusted oracle network for tracking purposes	[194]
To chain or not to chain: a reinforcement learning approach for	Presents a blueprint of a private network in which oracle contracts	[229]

blockchain-enabled IoT monitoring applications	improve their efficiency according to data collected by IoT sensors	
Blockchain as a platform for secure inter-organizational business processes	Discusses oracle data correctness and confidentiality in business process management	[188]

Appendix 3.B. Notable coauthors

Full Name	Institution	Citations	Documents
Zhu, Liming	UNSW, CSIRO-DATA61	612	3
Ingo, Weber	Tu-Berlin	303	5
Jayaraman, Raja	Khalifa University	179	5
Veneris, Andreas	University of Toronto	160	5
Berryhill, Ryan	University of Toronto	147	3
Veira, Neil	SoundHound Toronto	147	3
Muhammad Habib Ur Rehman	Khalifa University	144	3
Davor Svetinovic	Khalifa University	144	3
Ellaham, Samer	Khalifa University	142	3
Yaqoob, Ibrar	Khalifa University	66	4
Ferrari, Elena	University of Insubria	50	3
Weske, Mathias	University of Potsdam	14	3

Appendix 3.C. Complete list of articles sorted by categories.

Oracle Architecture	Entries
Beihang University	[230]
CEA LIST Paris-Saclay University	[228], [231]
Eindhoven University of Technology	[232]
ETH Zurich	[233]
Fujian Agriculture and Forest University	[134], [234]
TU-Berlin	[235]
INRS, Montr´eal	[136]
IST Austria	[236]
Jinan University	[237]
Langfang National University	[238]
Macquarie University	[143]
Nirma University	[239]
RMIT University	[7]
Hong Kong University	[167]
University of Canterbury	[240]
University of Dallas	[173]
University of Salamanca	[171]
University of Tartu	[135]

University of Toronto	[241]
UNSW Sidney CSIRO DATA61	[154], [162]–[164], [242]
Vienna University of Economics and Business	[161]
Jiamusi University	[166]
Sapienza University of Rome	[243]
University of Colorado	[165]
Carnegie Mellon University	[244]
University of Malta	[245]
Politecnico di Milano	[246]
Montana State University	[168]
University of Rijeka	[247]
Oracle Problem	Entries
Chiba, Institute of Technology	[174]
EBS University	[10]
IST Austria Klosterneuburg	[248]
John Caroll University	[124], [172]
Khalifa University	[118]
Max Planck Institute	[6]
Montclair state University	[117]
Technical University Munich	[249]
University of Applied Sciences Offenburg	[32]
University of Ljubljana	[30]
University of Verona	[11], [13], [33], [120], [140]
Imperial College London	[250]
University of Connecticut	[251]
Oracle Proposal	Entries
Beijing University of Technology	[252], [253]
Chungnam National University	[225]
Delft University of Technology	[254]
Kleros Cooperative	[255]
Kyushu University	[256]
National Taiwan University	[257]
Sogang University	[258]
Swiss Federal Institute of Technology	[259]
Technische Universit¨at Berlin	[260]
University of Illinois	[261]
University of Toronto	[262]–[265]
Hamburg University of Technology	[266]
South Asian University	[267]
Dublin City University	[268]
South China Normal University	[269]
Rensselaer Polytechnic Institute	[270]
University of Applied Sciences - Kufstein	[271]

Shanghai Jiao Tong University	[226]
Finance	Entries
Aalborg University Copenhagen	[272]
China Merchants Group	[179]
Concordia University Montreal	[146]
Cornell University	[155]
Delhi Technological University	[176]
Khalifa University	[180]
Nanjing University	[273]
NTNU Norway	[227]
Oxford-Hainan Blockchain Research Institute	[178]
SUTD Singapore	[116]
Universit´e Clermont Auvergne	[181]
University of Cagliari	[170], [274]
University of London	[275]
University of Potsdam	[187]
University of Sfax	[169]
University of Houston	[175]
University of Luxembourg	[276]
Beihang University	[183]
University of Verona	[8], [149]
Delft University of Technology	[177]
Artificial Intelligence	Entries
Bina Nusantara University	[203]
INRS Montreal	[200]
Khalifa University	[277]
Universidade da Beira Interior	[278]
University of Luxembourg	[279]
University of Toulouse	[201]
Sidi Mohamed Ben Abdellah University	[202]
Business Process Management	Entries
KAUST	[280]
University of Insubria	[188], [189]
University of L'Aquila	[281]
University of Postdam	[185], [186]
UEST – China	[282]
Sapienza University of Rome	[184]
Cloud Computing	Entries
Khalifa University	[211]
University of Ljubljana	[160], [209]
Université de Montréal	[210]
North Carolina State University	[283]
Data Management	Entries
Beijing University	[216], [284]
Chiba Institute of Technology	[285]
Kaunas University of Technology	[286]

Khalifa University	[213], [214], [287]
Rennes University	[288]
Shenzhen Technology University	[289]
UNIST - South Korea	[212]
UNSW Sidney CSIRO DATA61	[290]
University of Sherbrooke	[291]
University of California	[215]
Jinan University	[217]
Energy	Entries
Technical University of Munich	[223]
Technical University of Cluj-Napoca	[222]
Electric Power Research Institute - Beijing,China	[224]
Healthcare	Entries
Khalifa University	[194], [197], [198]
University of Antwerp	[199]
Internet of Things	Entries
Khalifa University	[119]
National Chi Nan University	[292]
NUDT - China	[206]
Qatar University	[293]
Saint Mary's University	[204]
Technische Universit¨at Berlin	[294]
University of Insubria	[207]
INRS, Montr´eal	[295]
Wayne State University	[296]
University of Oradea	[205]
Blockchain 5.0 OÜ	[297]
University of Sherbrooke	[208]
Supply Chain & Traceability	Entries
University of Sherbrooke	[192]
Carlo Cattaneo University	[298]
Khalifa University	[299]
Technische Universit¨at Berlin	[191]
University of Hong Kong	[190]
University of Seville	[193]
University of Verona	[196]
Queensland University of Technology	[195]
Transport	Entries
Guangxi University	[220]
National Taiwan University	[219]
Khalifa University	[218]
Fraunhofer FIT & RWTH Aachen University	[221]

CHAPTER 4.

OVERCOMING THE BLOCKCHAIN ORACLE PROBLEM IN THE TRACEABILITY OF NON-FUNGIBLE PRODUCTS.

4.1. Introduction

As recently shown by Politecnico di Milano Observatory [300], at an international level, more than 580 projects involving blockchain as the main subject can be observed, with an increment of 76% since 2017, although the number of real applications barely exceeds 10%. Many blockchain applications involve financial technology, whereas we are assisting with a slight but progressive increase in non-financial projects, such as logistics, production, and traceability [48]. Recent literature has shown that blockchain is being tested [301]–[303], mainly in the Chinese and US markets, to track product information, and to improve product traceability. In 2011, China experienced a massive mislabeling of pork meat, together with a contamination problem where donkey meat was secretly mixed with fox meat [304], [305]. In 2017, Papayas in the US were linked with a multi-state outbreak of salmonella, leading to 173 cases of salmonellosis, 53 hospitalizations, and one death across 21 states [306]. Traceability improves food safety and public confidence, pinpointing the exact product to be discarded without compromising the entire supply line [307]. Kamath [37], Mearin [308], and Corkery and Popper [309], extensively described Walmart's efforts involving the adoption of blockchain and cryptography to trace the products sold in their stores. Supported by government entities, cooperating with IBM, and utilizing Linux Hyperledger [310], they managed to improve the time taken to trace a product from one week to few seconds, in addition to providing updated information, such as the temperature, humidity, and a roadmap. Their pilot project concerning mangos aimed to demonstrate transferability and accountability across borders; while successful, the maintenance costs for the whole system to work were quite high [311]. Blockchain for a sustainable agri-food market is mostly intended to solve social problems rather than technical or economic problems [312]. In contrast, in Italian markets, blockchain applications for traceability are also considered a valuable resource for the protection of the "Made-in-Italy" brand. Federalimentare's (2018) data show that the capitalization of agri-food products utilizing the "Made-in-Italy" brand is around 135 billion euros [313], with an added value of more than 61 billion euros. Italian agri-food products are protected by the "Designation of Origin" (DOP, DOCG), which reached the value of 15 billion euros in early 2017, representing nearly 18% of the entire agri-food sector and comprising 822 products subject to regulations and checks.

However, the same protection system limits the growth of production, exponentially enlarging the gap between demand and offer. As the solution cannot involve production adjustments, as a result of DOP constraints, Italian small to medium enterprises (SMEs) are fighting the phenomenon, incentivizing client awareness of product provenance and transportation, and lately also considering blockchain.

Sustainability-driven blockchain adoption involves a very narrow but important aspect of the economy, making models and inference less applicable on a broader scale. In contrast, a value-driven approach to blockchain adoption undertaken by Italian SMEs could be easier to replicate for companies entering the market or simply changing their business model to a blockchain orientation. Further, for managers trying to replicate a sustainable supply chain, being aware of how it can promote also financial sustainability could also represent the right incentive for the investment to be encouraged.

Early evidence supports the usefulness of the blockchain in the financial sector to lower costs and facilitate faster transactions [314], [315]. Non-financial applications are still in the pilot/early stages, and no robust findings have been produced so far. What the literature neglects about blockchain implication for traceability and sustainability is the so-called oracle problem, and the trustworthiness of information written in smart contracts. Few have made an attempt to address the problem, and those who have, work mainly in the light literature of the insurance/finance sector [316], [317]. Although the problem is less worrying for fungible products [12], in non-fungible products it can undermine the worthiness of entire projects. Seeking to make a solid contribution to the literature addressing blockchain social and economic implications, this paper focuses on two main research questions. First, how does blockchain technology adoption affect organizational effectiveness, and second, how can the oracle problem be effectively overcome for sustainable supply chains?

Undoubtedly, addressing the critical gap in the literature that neglects the oracle problem is mandatory when developing further empirical/theoretical papers on traceability and smart-contract-driven blockchain. Above all, the concept is critical when smart contracts are used for sustainability purposes where information reliability and transparency constitute essential aspects. To answer our two research questions, we will take a knowledge-based-view of a modified Gold et al. [318] model to analyze a single case study of an Italian agri-food company undertaking a blockchain-based traceability project. The paper proceeds as follows. Section 2 provides a background to the literature on blockchain technology and the oracle's problem, addressing streams of literature on Gold et al. [318], and on the implications of knowledge process capabilities [319]. In Section 3, the methodology of this research is explained along with a detailed illustration of the data gathered. In Section 4, an in-depth analysis of the research questions is provided, along with the most significative data. Section 5 provides the concluding remarks, limitations, implications for academics and practitioners, and hints for further research.

4.2. Theoretical Background

The concept of blockchain was introduced by Haber and Stornetta's [67] paper that promoted the idea of the digital stamping of documents. In a subsequent work, they, along with other authors, proposed to bundle large volumes of transactions together into blocks and arrange them in a chronological sequence according to a hash code. The first to refer to this particular "chain of block" appears to be Nakamoto in 2008 [1], who connected the concept of blockchain to a public ledger, constantly updated by multiple users. Motivated by distrust in financial establishments, Nakamoto [1] introduced a blockchain framework for his cryptocurrency (Bitcoin) with no central organization to supervise the creation of blocks [1], [2]. Blockchain technology is defined as a distributed ledger [320], able to record transactions (of any kind) in a secure, transparent, efficient, decentralized, and low-cost way [321]. There are several types of blockchain (public, private, hybrid) that vary according to the degree of freedom to access information [322], [323]. Swan presents a list of potential blockchain applications [46], divided into three categories: the first area is related to currencies, payments, and invoices; the second regards smart contracts in financial and non-financial markets; and the third pertains to social applications, such as voting, and healthcare identification. Regarding the second type of application, smart contracts are defined by Morkunas et al. [48] as a self-executing code on a blockchain that automatically implements the terms of an agreement between parties. When operating with smart contracts, a problem related to the insertion of data on the blockchain arises. Smart contracts for applications other than cryptocurrency transfer involve the role of an "oracle" to insert extrinsic data into the blockchain. An example of the information added by oracles is provided below.

When dealing with cryptocurrencies, the provenance of a bitcoin, ether, or another token is certain, since the token itself is on the blockchain, and therefore, all its information is available to the smart-contract. For example, if a smart contract pertains to delayed payments, all the required information will be drawn from the data stored on the blockchain. As blocks are timestamped, the information about time is available within the same ecosystem. Therefore, the required data for the smart contract is also considered undisputedly true and immutable. For smart contracts such as food traceability, tracking information about things that are not part of the "locked chain" but happen outside (such as weather effects, temperature, or product provenance) constitutes an externality to the blockchain. For example, In the case of a pack of cheese sitting on a store shelf, the information about that product is not present within the block data, and so it has to be inserted by an "oracle". An oracle is essentially a gateway between a smart-contract environment and the external world [29], [32]. It obtains information about something that has occurred outside the blockchain and then provides that information to the smart contract through a specific communication channel (e.g., platforms, probes). The main difference of intrinsic and oracle drawn data is that for the first, the information is true and immutable (if the system has not been compromised) since it is drawn from the blockchain itself, while, for the latter, the information is indeed immutable, since it is protected by the blockchain, but its truth or trustworthiness is dependent on the trustworthiness of the "oracle" that inserted it. Many blockchain communities are skeptical about oracle-dependent applications, especially for sustainable domains, because of the problem of the oracle's credibility, also pointing out the following arguments. If the oracle is trusted, then it becomes a single trusted party, which produces a "counterparty risk" because if lies can be fed to the oracle, or if it is compromised, then the smart contract will work on data that is "untrue." There are significant financial incentives to compromise such systems, since they are perceived to be safer and more trustworthy than the legacy ones. The implementation of Internet of Things (IoT) is considered to have solved the problem using sensors to track various physical objects as they move through the supply chain. However, the problem of trust still applies to the sensor, as well as its placement, its scanning ability, and its communication channels with the oracle, returning us again to the problem of the oracle. For fungible products (goods), such as crude oil, this problem can be efficiently addressed since the product is easier to track [12]. Think of a certain amount of crude oil loaded onto a tanker and then tracked on the other side as it is unloaded from a ship—all of which information is recorded to the blockchain. Since crude oil is fungible, it does not matter whether the same molecules of oil are tracked or not. For fungible goods, we intend products, that are equivalent or consist of many identical parts such that, for practical purposes, they are interchangeable[2].

Unfortunately, to date, there is still not an efficient way to address the problem of non-fungible products, and, to the best of our knowledge, many of the current applications in the supply chain suffer from the oracle's problem, leading to the risk of creating a false trustworthy environment in which the consumer is not sufficiently safeguarded. Non-fungible products are, unlike fungible ones, goods that are not of homogeneous value. Therefore, when tracking a load of 100 wheels of cheese, for example, moving from one place to another, it is not sufficient to check if the wheels of cheese are 100 and in good shape on arrival. It is vital that the 100 wheels received are the same wheels that were initially shipped without undergoing any manipulation. For these reasons, ensuring reliable and trustworthy traceability of non-fungible products on the blockchain is much more challenging.

To address this problem, and more broadly, the two research questions of this paper, we decided to utilize the knowledge-based view, and in particular, a modified Gold et al. [318] model (Figure 4.1), as knowledge management and information sharing are the main aspects affected by the oracle problem. A further explanation of the theoretical construct is provided below.

[2] Fungible goods definition: https://www.investopedia.com/terms/f/fungibles.asp

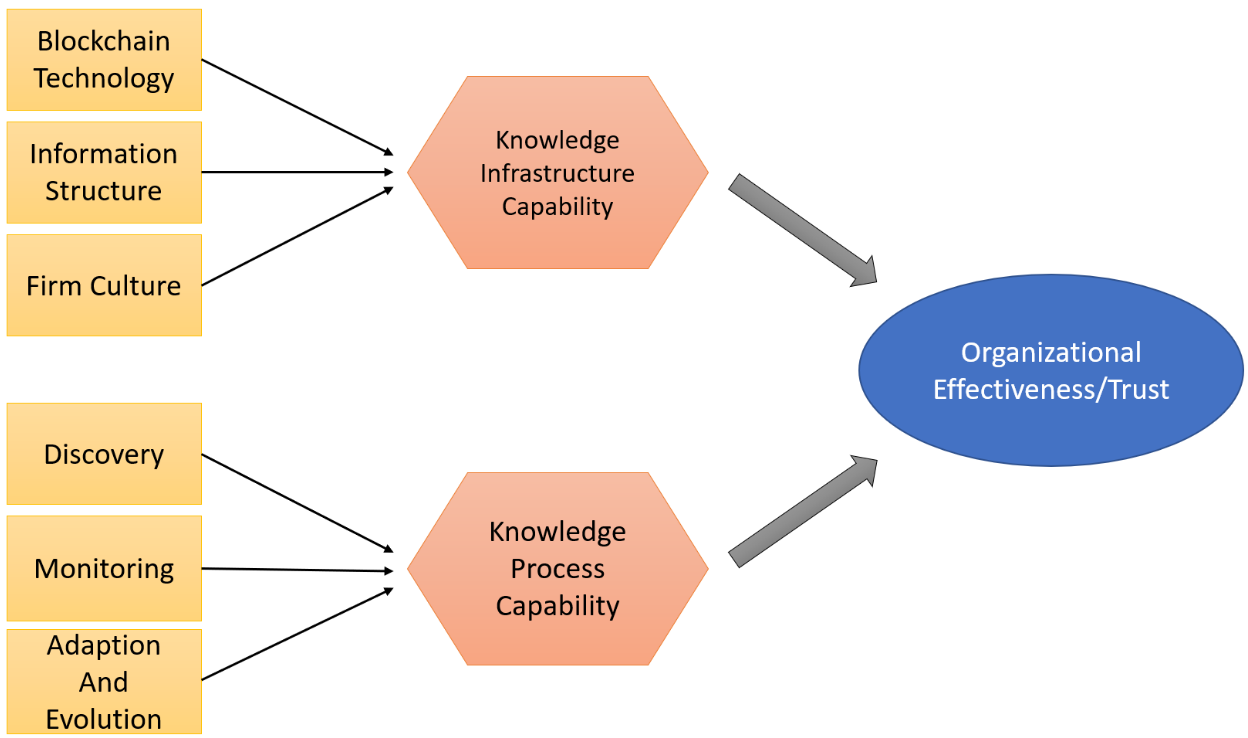

Figure 4.1. Modified Gold et al. model [318]

The construct of "knowledge management" (KM) as Gao declares [324], embodies a higher value than the separate concepts of knowledge and management alone. It is defined as a formal and well-defined way to shape information that will advantage companies over others while, at the same time, crafting information to be willingly available for those who require it [325]–[329]. Confirming the importance of KM, Gharakhani and Mousakhani suggested that knowledge management creates new capabilities for organizations, enables superior performance, encourages innovation, and enhances customer value [330]. Cho added that an effective KM helps organizations to become flexible, respond quickly to changing conditions, become innovative, and improve decision-making capacities and productivity [331]. Denford [332], in his dissertation on KM capabilities, distinguished resource-based capability as comprising a technological structure and a culture of knowledge-based capabilities, including expertise, learning, and information, which are needed for organizations to efficiently manage knowledge. Resource-based capabilities were renamed by Gold et al as "knowledge infrastructure," and will constitute a central part of this article's analysis [318], since we are investigating how they are affected by the adoption of blockchain. As Smith stated [333], the concept of KM infrastructure is mostly associated with modular products that support KM actions in organizations. KM infrastructure analysis is divided into two main capabilities: technical and social. The technical capabilities comprise IT infrastructure, physical devices, and components, whereas social capacity comprises cultural, human, and governance resources [334]. We then analyze the technical and social capabilities separately according to their blockchain implications, finding that organizations should make every effort to expand their infrastructure capabilities, not only in terms of hardware and software, but also in terms of technology, structure, people, and culture. Regarding the concept of culture, Masa'deh [335] stated that "Organizational culture not only defines the value and advantage of knowledge for organizations, it also influences the ability of employees to share knowledge" [336]. Organizational culture is necessary for encouraging interaction and collaboration between individuals to facilitate the flow of knowledge. It also provides individuals with the ability to self-organize their personal knowledge to facilitate problem-solving and the sharing of knowledge [337]. We contribute to the literature by showing how blockchain adoption affects a firm's culture and also, how that culture determines successful blockchain implementation. As extensively underlined by researchers, one of the most important elements of culture for knowledge sharing is trust. Kushwaha and Rao stated that high levels of trust reduce the reluctance of individuals to share knowledge and decrease the associated risk of losing competitiveness [334]. Further, organizational culture influences the way strategic decisions are implemented in firms [338]. Barney and Hansen have asserted that trust is beneficial to interfirm exchanges and can be a source of competitive advantage [339]. However, the literature reveals an ambiguity in the nature of trust, as transaction cost theory, for example, implies that firms tend to behave opportunistically [340], [341]. A fundamental challenge in conceptualizing the role of trust lies in extending the micro-foundational phenomenon to the organizational level. Many authors have agreed that viewing opportunism and trust as characteristics of firms anthropomorphizes organizations [342], [343]. With the advent of blockchain, the element of trust has been digitalized and separated by the idiosyncratic human correlation. Trust in the blockchain is no more an exclusive outcome of a micro-level; it can be generated directly at the macro level. A recent study by Zaheer et al. showed a direct link between inter-organizational trust and performance [344], but not between interpersonal trust and performance, whereby even if interpersonal trust is low, inter-organizational trust remains high. This perfectly supports the modifications that we are applying to Gold et al.'s model [318], in which trust is included in organizational effectiveness and seen as one of the major drivers of firm performance.

4.3. Methodology

To answer our research questions, we decided to build on Gold et al.'s model to conduct our case study [318], as a quantitative data analysis still did not constitute a valid alternative. The first part of the research involved a thorough investigation of the existing literature to locate the keywords needed to build the model. As demonstrated by Lin et al. [345], the literature lacks seminal papers associating blockchain technology with sustainable agri-food or agribusiness. Switching from a broad analysis to a more in-depth investigation, segmenting "management" and "business" keywords, Lin et al. identified only ten papers [345]. The same results were obtained by Bermeo-Almeida et al. [301], who added that most of the papers (seven out of ten) were written by Asiatic authors. Aware of the limited background, we decided to address the situation using the Scopus platform. We used a specific string—"blockchain" AND "food" (OR "agriculture" OR "agricultural delivery" OR "agricultural supply chain"—obtaining more than 130 potential results (12/07/2019). Controlling for "knowledge management," we arrived at slightly more than

20 papers (22), of which 14 were published in peer-reviewed journals, and eight had been presented at international conferences. From the most influential and available literature, we were able to extract the following keywords: blockchain technology [125], information structure [346], and firm culture [347]. In our knowledge process capability model, we included products and production processes [348], along with their management insertion rules [349]. Finally, to the "organizational effectiveness" construct, we added the value of trust [350], as well as transparency, auditability, and immutability characteristics—these latter constructs bearing a dual interpretation. We considered trust a higher grade of consumer faith when evaluating product acquisition and consumption. Further, with blockchain, companies benefit from increased levels of trust among their supply-chain partners, as even the smallest non-compliance episode can be tracked and registered [345]. Since Gold et al.'s sample was quite extensive and mainly involved large companies [318], some modifications were required. First, as stated above, large companies are not the main sources of KM activity, and drivers for knowledge management innovation are also less evident in large organizations. Second, items generating knowledge are reduced according to the sample and because of developments in the literature over recent years [351]–[353]. However, since the most intriguing part of the paper is the model (as also stated by the same authors), we gave high priority to the drawing process. The model was slightly adapted, although the scope of its application remained the same in focusing on the relation between knowledge infrastructure capabilities, knowledge process capabilities, and organizational effectiveness/trust. The major changes regarding knowledge infrastructure capability were implemented according to Mendling et al. [319], who introduced in theoretical terms the possible impacts of blockchain technology adoption on business process management (BPM). Further developing Mendling et al. [319], we inserted into the model the parts that, according to our case study, seemed most affected by the application of the blockchain technology, specifically, discovery, monitoring, adaptation, and evolution. Guided by Pettigrew [354], our approach to the case study involved team visits to the site. We managed three visits to the case study site and conducted a total of nineteen interviews. Our team comprised two professors from the organization department of Business Administration who led and conducted the face to face interviews, one PhD student from the same department who submitted the research questionnaires, and two master's degree students who transcribed the notes and interviews. The registered interviews were conducted in a semi-structured form. According to prior studies [355]–[358], our dataset retained a certain degree of flexibility, along with our research questions, which were often updated according to ongoing feedback and unexpected events. The semi-structured interviews lasted 50 minutes on average and were conducted with directors involved with the blockchain project, entrepreneurs associated with the cooperative, and service providers. The data and results were presented to the main actors in the organization and to its directors. The analysis of the case study commenced in June 2018 and finished in November 2019. From the data collected, sentences were extracted and associated to keywords using the "concept coding" [359]. Sentences matched to keywords found in the model are then further investigated and discussed. This research was undertaken without preconceptions and without

the need to prove anything in advance; we were solely moved by the disinterested aim of contributing to the agri-food sector and the academic literature.

4.3.1 Data Collection

For our case study, we decided to analyze the "San Rocco Dairy" cooperative in Tezze sul Brenta (VI). The company was founded on August 25, 1966, from a congregation of breeders, with the aim of producing homogeneous local food, while maintaining excellence (mainly in cheese). At the time of the study, the cooperative counted 19 associates across three different districts of the Veneto region. Its main aggregations were in Vicenza, Treviso, and Padova. The size of the companies was, on average, quite small, and their most common structure was that of a family business that occasionally employed external staff, but rarely more than two. All the companies shared the same structure, except for two that were more prominent. Trusting the quality of their products, the employees suggested competing at national and international levels to increase awareness of the food's excellence. Since then, the cooperative has received countless prizes, including the Caseus Veneti and the World Cheese Award; it has also been included in the Super Gold Ranking of "Asiago DOP (Fresh & Aged)," and is thus listed among the best cheeses in the world. To defend its strong brand, strengthened through many years of hard work, the cooperative agreed to test the potential of blockchain (public/ETH), and the IoT technology, utilizing a specific quick response (QR) code to guarantee its certification information and to be directly validated by institutions, company partners, and final consumers.

Table 4.1. Data collection

Collected Data	**Number**	**Note**
Interviews	19	Four informal interviews collected during a first visit to San Rocco Dairy. Eleven direct, semi-structured interviews during two official visits and four phone calls to the technology provider. Direct interviews and phone calls were digitally recorded and transcribed.
Direct observation	5	The authors attended the San Rocco Dairy three times, visiting the offices, the farms, and the shops. Two of the associates also came to the authors' office twice.
Notes from observations and interviews	47 pages	The authors collected 34 pages of notes from the interviews and 13 pages of direct observations.
Data collected online	4	The authors searched for data on the cooperative website and social media.
Data from press	16	16 articles were analyzed to find information about the firm's awards and the blockchain project.

The underlying strategy adopted by the consortium was to redefine the information systems to create a completely tracked supply chain. Data were monitored from the production of milk to the finished products (blocks of cheese), guaranteeing a secure and certified product provenance to consumers. Improvements involved not only monitoring the safety and quality of products, but also information awareness, and procedure compliance, so that well-informed consumers, aware of the supply chain, had become the best contributors to the processes of optimization and engagement. As studies on traceability are few but increasing, our research contributes to the literature as its motivations and the products being analyzed differ slightly from those of other studies.

4.3.2 Data Analysis

The examined consortium began blockchain integration in September 2018, introducing the first blocks of Asiago DOP cheese to the market by January 2019. The consortium also implemented an IoT system based on a QR code to facilitate interaction with its main stakeholders. Data were collected from the beginning of April 2019. The main data stored in the blockchain and retrievable through the QR code comprised the company ID code (for the General Data Protection Regulation (GDPR) compliance), the liters of milk provided, data about milk entry, and milk analysis. Regarding the specific activities for transformation and storage, the cooperative decided to include in the blockchain temporal identification data about the entry and exit of every semi-finished product according to the different phases that characterized the critical activities. All information relative to a specific process was stored in a single block to ensure easier traceability of the entire supply-chain process.

Table 4.2. Data analysis

Data Type	Period	Purpose
Informal interviews	June 2018	Verify the genuineness of the project and the availability to cooperate.
First round of semi-structured interviews	September 2018	Understand motives leading to blockchain implementation and the roles of people involved.
Second round of semi-structured interviews	September 2019	Through targeted questions, analyze the impact of blockchain on organizational effectiveness.
Phone interviews to service provider	November 2019	Check consistency with the aims of the cooperative and the limits of the technology.
Direct observation and interviews notes	2018–2019	Understand the usefulness of the blockchain application and its implications for the oracle's problem.
Online and press data	2018–2019	Analyze the way the cooperative tries to spread its core values through the blockchain.

The QR code was utilized both by clients and intermediaries, returning precious information to San Rocco's Dairy. When a user scans the QR code, that user releases to the network critical data, such as their gender, their job, the device used, their location, the time, and the number of times the specific QR has been scanned. Extracted data from the 100 blocks for Asiago cheese shows that almost 87% of the products scanned were consumed by Italian clients. Around 10% were French users and the remaining 3% were north-European consumers. The product was most often scanned on Fridays during the daytime (10.00–13.00 hours), and the most frequently requested information was from the timeline in reference to the production, the history of firm, and the prizes awarded. In relation to customer retention, it was discovered that nearly 10% of clients observed the same type of product once a week for at least for four weeks. Aware that the value of the data on the blockchain was quite low for consumers, we focused on the changes that this implementation made to organizational effectiveness and whether its application violated the insidious oracle problem. In the first round of informal interviews, we concentrated on company availability to cooperate with our department and on business acquaintance with this new technology, to be sure that the decision for undertaking the project was not merely based on marketing benefits, driven by the hype that blockchain has lately experienced. To clarify the intentions, the first official round of semi-structured interviews had the goal of understanding why the cooperative had chosen to undertake a blockchain-based project and whether they had evaluated it in relation to other alternatives. We asked participants about their plans for the future, and of course, whether they were experiencing any unpredicted issues. After exactly one year, we started a second round of semi-structured interviews, with the aim of understanding what had changed in the organization after the project had been executed and whether the cooperative was planning to improve or abandon it. Considering it necessary to double-check the information provided by the firms, we also contacted the technology provider via phone-call interviews to understand whether there was an alignment between what the firms aimed to obtain through the technology and the exact potential of the implemented service. Further information was taken from the company website and social media, as well as from newspapers, in which San Rocco’s project is often described. The authors transcribed all the interviews and details from direct observations, writing nearly 50 pages of notes that were used to link the data gathered with the Gold et al. [318] model and to understand its implications for the oracle’s problem.

4.4. Discussions

To better clarify how the company addressed the insidious oracle’s problem in a sustainable supply chain context, details on the blockchain’s impact on organizational effectiveness must first be provided. Drawing from the informal interviews with the consortium directors, problems linked to the valorization of the brand and to the internalization of products emerged. As underlined by one participant: the “dairy market bears some difficulties generated by the presence of small wholesalers, and the large-scale retail trade.” The constant presence of intermediaries with high commercial competence was helpful in compensating for the low levels of territorial and market control, since San Rocco only has two registered shops. Dealers help consumers to receive the product, but the issue of ensuring that the quality is linked with the San Rocco brand has not been solved. One common vision of the consortium’s top management involved the need to more directly reach final consumers, to reduce the information bias generated by intermediaries. Further, one interviewed executive extensively underlined the issues related to the internationalization and safety of the products/brand as a result of the massive presence of counterfeiters: “Asiago is very famous in California … but only a few wheels of cheese are genuine Asiago”. The massive presence of counterfeit products not only undermines company trustworthiness but can also have negative social implications. As a matter of fact, counterfeit products do not differ from the original just in terms of taste and shape. Non-subject to strict regulation and checks, they constitute a threat to consumer health. The outcome of blockchain application in terms of value creation cannot be detected at present since the data is insufficient; however, extensive results were already visible in the effects of the blockchain’s application at the organizational level. To obtain these results, many areas were addressed according to the Gold et al. model [318]. The blockchain impacts on organizational effectiveness are summarized in Table 4.3.

The appeal of blockchain technology arises from its distinctive characteristics, that makes it a valuable implementation for sustainability purposes [17], [360], such as the immutability of its data, the availability of the information, and its transparence, as well as its distributed certification and reliability. During the first official round of interviews, the quality manager stated, “we are a peculiar dairy company, since every employee has the passion for information technology.” Although able to create its own blockchain, the company decided to outsource the technical aspects to limit the chances of failure. As the project grows, they plan to fully automate it with probes and microchips. One of the associates that operates the blockchain remarked, “we need to automatize the system as soon as possible, since if we produce milk today, the data needs to be immediately inserted on the blockchain. Delays of any sort can affect the reliability of data.” Of course, the company also utilized Enterprise Resource Planning (ERP), but they preferred to invest in local software houses, rather than using the best-known alternatives. As one of the directors declared: “we always tried to cooperate with the local companies … even for services not directly related to our production”. Further, the cooperative installed a remote-control system for the “CASARO” (chief cheesemaker), which allowing for the checking of every production site in real time to quickly adjust production gaps. According to the participants, the limitations of the cloud technology with respect to blockchain involved the “malleability” of the data. Being milk a very delicate raw material, the date of production should be immediately known and certain. The firm’s structure was quite controversial. As, one of the directors indicated: “our cooperative has a pretty controversial governance structure, since the board of the director’s members are also the shareholders.” Every member had to choose whether to defend the cooperative’s interests, his company’s interests, or his own. This could easily create conflicts of interests and difficulties in making decisions; it could also lead to associates’ withdrawal. Despite this, the director had managed to govern the cooperative for more than 40 years without any major issues, and as he stated, the hardest problem to solve consisted of finding a successor. In San Rocco’s Dairy, employees were considered part of the decision-making team, and they also introduced valuable innovations such as blockchain technology since their mean age was very low. The blockchain adoption was actually promoted by one of the youngest associates, who had studied its application during his master's degree and had proposed the innovation to the directors. He stated: "the cooperative is always open for innovation … although not aware of the technology, they understood its potential!" The blockchain adoption required no considerable changes to the company structure, as all interviewed agreed during the second round. However, some changes were made in task distribution after the blockchain's adoption. As well as contracting a consultant for the implementation, management also awarded employees specific roles and responsibilities related to the blockchain. Further, they planned to hire highly qualified professionals when the project reached a significant level of growth. Nonetheless, changes were not always welcomed, as one of the associates remarked: "It was not easy to present the new technology to the employees, since it means more work for people already overburdened." The culture of the consortium was stable and strong, and it aimed to strengthen coordination between producers and processors, exploiting the firm's core sustainability values (economic, social, environmental, cultural, and ethical). Identifying these common values, the cooperative invested in the project of defining a common information structure, transferring to its clients and associates the positive elements that the company pursued, such as the absence of chemical agents, environmental protection, and employee protection. Blockchain implementation, as agreed by almost all those interviewed, brought no changes to the company culture, but the participants also stressed that one of the main motives to undertake this adventure was to better reach the customers and make them aware of the consortium's core values. One of the associates stated: "Blockchain will help us promote our company values directly to the client and deliver product information at 360 degrees." Further, the company culture fostered the adoption of the blockchain as its type of innovation was technologically driven. The company's will to reach clients did not just have a promotional role; it also served as a canvas to build and strengthen trust. Trust was a critical value for San Rocco's Dairy, which participants were eagerly trying to defend. The threats to this trust were multiple. At an international level, Asiago cheese appeared to be a highly requested product, but the narrowed site of production (DOP protection) did not allow for the complete satisfaction of the constantly increasing demand, leaving promising opportunities for counterfeiters. The role of the blockchain for the consortium is not to "create" trust but to maintain the high level of trust built over many years of hard work. This aim is quite controversial because, in the early literature, the blockchain was viewed as a means for creating trust, while it is now widely held that blockchain provides a way to transact in a trustless environment [361], [362]. For the consortium, the technology should work in an environment where trust is at a maximum, defending it from external threats. When prompted about this issue, the quality manager affirmed: "we firmly believe in the quality of our products … blockchain ensures that third parties will not alter client awareness." From the data gathered, there was not strong evidence of the blockchain's capability of defending trust in those environments; however, theoretically, this remains quite a robust conjecture. Regarding the intra/interorganizational environment, by definition, it acts more as a monitoring authority than a trust enhancer, as assumed in Mendling et al. [319]. The associates and the quality manager stressed that they were surprised about the high level of blockchain involvement in business processes. As a consequence of its structure and functionality, the adoption of blockchain required the company to clearly map and divide all their business processes for information to be uploaded to the ledger. One of those interviewed stated: ”Yes, blockchain requires mapping for all business processes … It clearly helps to define the supply chain.” The quality manager stressed that although the technology was helpful for that task, its compliance with the “disciplinare” (policy document) already required a high level of understanding and control of company processes. Conversely, applying the technology, the consortium realized that some of its processes needed to be changed to remain consistent with blockchain’s potential. The participants noticed that the blockchain’s adoption required the packaging process to be internalized. Outsourcing the packaging process created some doubts about the last “steps” of the supply chain’s traceability. Since the tracking devices are on the packaging, the outsourcing of this last step is perceived as a threat to the whole traceability process. One of the associates that interacts with large-scale retailers stated: “retailers strongly believe in the potential of the technology, but they offer only standardized packaging … we must focus on products that we can pack ourselves.” To ensure the trustworthiness of the process, the packaging step cannot be outsourced. Further, in opposition to the expectations of previous literature [319], [363], the business process (at least for this case study) was not automated through blockchain smart contracts but remained a function of human action; while the immutability of the ledger created the “trigger” for an ease in monitoring activity. The blockchain manager proudly stated: “we can enjoy a double outcome for [the] blockchain application, first to reach our clients and also to detect potential malfunctions and loss of efficiency.” However, the adaptation of process constitutes a limitation for this technology. While BPM aims at the continuous improvement of processes [361], blockchain technology, as a result of its very origin and purpose, offers fewer degrees of freedom in the field, since, when a process changes, it will not affect the data already on the blockchain. A private blockchain would probably prove to be more efficient, as the quality manager declared: “For now, it works … but sooner or later we may have to build our own system” [32].

Table 4.3. Blockchain effects on organizational effectiveness

Components of the “modified” Gold et al. model [318]		**Blockchain effects**	**Quote**
Knowledge Infrastructure Capabilities	Technology	Requires high levels of technological understanding or delegation to a specialized company.	*“The cooperative is always open for innovation … although not aware of the technology, they understood its potential!”*
	Structure	Not directly affected by the technology. If the company is unable to hire specialized professionals, employees are required to receive more tasks and responsibilities.	*“It was not easy to present the new technology to the employees, since it means more work for people already overburdened.”*

	Culture	Technology does not affect culture but helps to spread the firm's core values effectively.	*"Blockchain will help us promote our company values directly to the client."*
Knowledge Process Capabilities	Discovery	Data rationalization can easily lead to process discovery.	*"Yes, blockchain requires mapping for all business processes. It clearly helps to define the supply chain."*
	Monitoring	Even if not automated, the blockchain constitutes a "trigger" for faulty processes.	*"[Blockchain] detects potential malfunctions and loss of efficiency."*
	Adaptation and evolution	Blockchain hardly adapts to process innovations.	*"For now, it works … but sooner or later we may have to build our own system."*
Organizational Effectiveness	Trust	Unlike the financial sector, traceability can only work in highly trusted environments.	*"We firmly believe in the quality of our products … blockchain ensures that third parties will not alter clients' awareness."*

One further critical contribution to the literature is to analyze how and whether the organization effectively addressed the oracle's problem, which significantly affects the meaning of blockchain projects dependant on real-world data. As specified in Section 2, the oracle's problem arises when connecting a physical asset or commodity to a virtual token that tracks it on a blockchain [56], [57]. Although other papers/articles describe practical cases of blockchain technology for product traceability, none are robust in relation to the oracle's problem, keeping the blockchain community firmly skeptical about the reliability of those applications. When blockchain is implemented for sustainability reasons, trustworthiness and transparency are often pointed to as the core characteristics that make it suitable for the purpose [74], [364], [365]. However, since information on sustainability comes from the company itself [29], [32], trustworthiness and transparency should be no more given for guaranteed. As a matter of fact, studies on the sustainability-driven blockchain should focus on oracles and not only on the mere technology. Conversely, whether the company operates directly on the blockchain or with an external consultant, whether the blockchain is proprietary or public, whether a Bitcoin or Ethereum blockchain is utilized, the oracle's problem remains unmentioned in literature, since it has clearly still not been sufficiently addressed. In our case study, we noticed an important implication for trust involving a specific type of products, which may greatly affect the extent of the oracle's problem. For high-quality products, and precisely, for products with a certified provenance (especially DOP or DOCG), trustworthiness has rarely been questioned. The Italian Government, for instance, imposes strict laws on food producers, which are among the most severe in the world. Companies producing DOP products, for example, must precisely track all production phases to ensure the correct provenance of all raw materials used in the production. Utilizing blockchain in these supply chains requires the company to upload on the blockchain only information that has been strictly verified by the certification authority. Consequently, there are no apparent incentives to alter product data. Companies should be extra cautious when inserting information into the blockchain, as they are definitely under the "eyes" of the authority. From the interviews, it emerged that the choice of Asiago as a pilot for the blockchain project arose from the policy surrounding DOP products, which requires information to be already tracked and secure. One of the executives declared: "the choice of tracing our Asiago DOP on the blockchain also derives from the large availability of data on the supply chain that it is strictly supervised by the authority and has to comply with the "disciplinare" [policy document]." The aim of the blockchain utilization was not to guarantee the safety of the product, which was already supervised by the authorities, but to fight counterfeiters operating outside the domain of the authorities. The trust involving information uploaded to the blockchain is then shifted from the firm to the certification authority. Basically, in that "protected environment," the information on products' traceability uploaded to the blockchain falls under the supervision of the certification authority. Being on the blockchain, information can hardly be altered by counterfeiters even outside the authority's domain. The oracle ecosystem created by the company is explained in Figure 4.2.

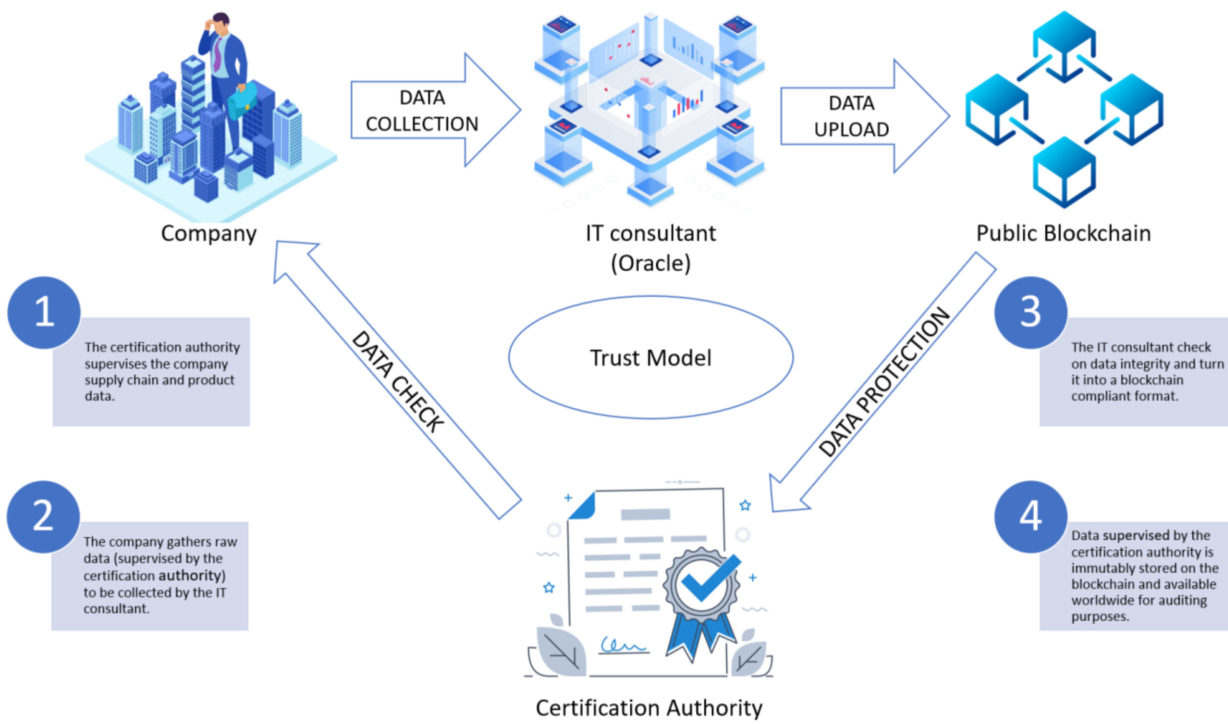

Figure 4.2. Relationships between the company, IT provider, blockchain, and certification authority

Any other addition, such as implementing IoT in the blockchain (sensors or probes), requested by the "disciplinare," will be verified by the authority, ensuring that only trustworthy information is uploaded to the blockchain. The quality manager further explained: "Once the Asiago DOP project reaches an appropriate speed, we will then start with the Grana Padano DOP, which is another product with a strong 'disciplinare'." It is quite clear that, for the consortium, the blockchain does not represent a certification authority by itself, but a means to defend the integrity of information gathered and supervised in compliance with the "disciplinare."

Implementing blockchain with this aim clearly reduces the impact of the oracle's problem, as the need for trusted, third-party input is fulfilled by the certification authority (especially the DOP or DOCG). Without a trusted third-party, external to the firm, the information uploaded to the blockchain is no more trustworthy than that written by the company itself on the labels of its products and does not really improve quality or consumer protection.

4.5. Conclusions

This paper sought to address the oracle's problem for smart contracts based blockchain implemented in the traceability of specific non-fungible products. To do so, we first contextualized the issue through a case study of a dairy company in northeastern Italy, whose interest in blockchain was mainly related to brand protection. As the literature lacks empirical studies involving blockchain technology's adoption, our first research question addressed its impact on organizational effectiveness, building on three precise literature streams: KM [324], knowledge infrastructure [318], and trust [344]. Data show that successful technology implementation is strictly connected to a firm's attitude to innovation and to employee involvement in the innovation process. However, highly specialized consultants are probably required for the process to be undertaken smoothly and in a reasonable time frame. Company culture does not seem to be affected by blockchain's adoption. However, reaching clients and spreading firm culture is one of the main reasons for firms to undertake blockchain projects. From the interviews, it emerged that blockchain does not really affect governance structures, but requires the introduction of new professional figures, or role extensions for existing employees, creating conditions for job enrichment and promotions. Processes are also affected by the implementation of the technology in three different ways. First the blockchain's structure helps the quality managers to better rationalize processes and the supply chain. Second, ledger immutability can create a "trigger" for faulty processes to be promptly located and addressed. Third, blockchain may constitute an obstacle to process innovation, as updates are by nature more difficult on (public) blockchains. Regarding the concept of trust, we may argue that, from this research, no clear evidence emerges on trust improvement, while, on the contrary, blockchain seems to be useful only in environments where trust is already established, enabling defense mechanisms against external threats, such as counterfeiters. With a clear vision of how blockchain affected organizational effectiveness, we were able to narrow our second research question as to how the oracle's problem could be overcome in sustainable supply chain environments. As already stated by blockchain experts [29], the oracle's problem has the lowest impact in cases with trusted, third-party mechanisms that supervise and certify in a coercive manner information uploaded to and stored on the blockchain (although it may lead to counterparty risk). As information on the blockchain is immutable but not necessarily true, without a trusted third party to verify the data to be inserted, the details provided should not be considered any more trustworthy that those contained in a legacy database. Further, although in such environments, the impact of the oracle's problem is low, doubts arise as to the need for a blockchain to be implemented at all. To enlighten possible solutions to this dilemma, the case study analyzed in this paper, by way of example, involved a blockchain project undertaken by San

Rocco's Dairy for the traceability of the Asiago DOP (non-fungible product). In this specific case, the certification authority (DOP) constituted a strong third party whose verified data inserted into the blockchain became public and highly secure. The presence of a highly trusted third-party reduced the impact of the oracle's problem. Nonetheless, blockchain technology proved to be more effective than legacy technologies, since it guaranteed the protection of products outside the domain of the authority. The results provided in this research should be useful for academics, allowing further studies on real-world blockchains and the oracle's problem to build on them. Managers can also exploit these results to decide whether their company might benefit from blockchain's application and how to implement it in the most profitable way. When addressing sustainable development, it may be useful to consider this case study as to understand how blockchain implementation can also impact profitability. Conversely, limitations regarding the qualitative approach and the single case study need to be taken into consideration when making inferences at a broader scale. Furthermore, while the study addresses the problem of the trustworthiness of data on the blockchain, it does not provide any advancement or solution to the problem of attaching a physical product to the blockchain, which still proves to be a severe threat to blockchain-based supply chains. Further studies may try to replicate the results of this paper addressing a different sector and market, or perhaps comparing countries where authorities have multiple degrees of enforcement or different certifications. Samples could also include more structured companies as results on processes are highly influenced by company size, which in this paper is small to medium. As soon as there are enough data to undertake a quantitative study, it would be interesting to compare companies utilizing blockchain to see which sector benefits more from the adoption of the technology.

Thesis Conclusion

The chapters of this Ph.D. thesis present four related papers discussing the oracle problem. The first paper describes the oracle's role and the implications of its use in various contexts. The second reveals the magnitude of the literature that fails to consider the problem of oracle-dependent blockchains. The bibliometric analysis presented in the third paper was inspired by the need to identify the institutions and researchers actively involved in oracle-related projects to promote progress and cooperation. Finally, the fourth and last paper looked for a solution to the oracle problem through consideration of a case study involving the traceability of specific products subject to procedural guidelines.

While the four papers were well received by the academic community, obtaining a decent number of citations, they do have limitations. While some weaknesses were improved by responding to insightful reviewer comments, others could not be adjusted. The remaining limitations are discussed below.

As one of the reviewers commented, the first paper appears to be a hybrid of a classic review and a conceptual research paper, suggesting that its category should have been clearly stated. I specified in the text that it was a classic review; however, I acknowledge that it lacks a robust description of the methodology used to gather relevant papers. I later realized that a broad discussion on the oracle problem in the decentralized finance sector was also needed, which is not provided in this paper. Due to the complexity of the subject, I have decided to discuss this issue in a subsequent paper dedicated to the sector.

The paper presented in the second chapter was reviewed by conference peers. One expressed some concerns about the choice to include only journal papers. As specified in the paper, the choice was arbitrary, driven mainly by the following considerations: Discussions of oracles and the oracle problem can be quite long and complex, and the length restrictions of a conference paper may cause aspects to be overlooked in a study taking a general-overview approach. Since the conference paper sample was far larger than the journal paper sample, the results may have been biased by sample discrepancies. This assumption was confirmed by the research done in the third paper, which shows that the percentage of conference papers discussing oracles is even lower than that of journal papers.

The third paper has undergone multiple revisions and review rounds before getting published. The reviewers complained that the bibliometric analysis alone was not sufficiently significant; therefore, a review of the literature and a discussion had to be implemented in the final release. As a matter of fact, given the limited overall numbers of the bibliometric analysis, the emerged results could not be considered sufficient for a journal release. The review of the literature gave indeed also more value to the whole papers and the discussion highlighted areas of the research that were not adequately investigated. Finally, unlike cited bibliometric analysis, this study did not rely on specialized software, such as Bibliometrix, to display the results; however, given the low number of entries, effective data processing was done using Excel tables.

The fourth paper was the first published, with the goal of discussing the oracle problem in relation to food traceability. A reviewer argued that, since we affirmed in the paper that the need for a blockchain in our case study was not clear, the study's purpose was unclear. It must be said that there were no other empirical publications on the issue when the paper was published. Furthermore, given the scarcity of active projects in the field, it was extremely hard to investigate the issue from a practical point of view.

However, it must also be stated that the conjecture that emerged in this paper—the need for a third party to decentralize the trust placed in oracles—is a standard guideline for blockchain traceability today.

In summary, real-world blockchain technology is still in the early stage, and most concern the financial world. Despite the hype and expectations, multiple issues and drawbacks prevent companies from undertaking practical blockchain-based projects. Cost-saving and decentralization often come at the price of security, and it is difficult to find a balance between these elements (referred to as the blockchain trilemma). This thesis marks the starting point of my journey to understand the blockchain oracle, with the intent of continuing to monitor the companies studied in the current research while looking for new opportunities to widen the analysis to other sectors.

Bibliography

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. https://bitcoin.org/bitcoin.pdf (accessed Jun. 11, 2019).

[2] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd ed. O’Reilly, 2017.

[3] A. M. Antonopoulos, *The Internet of Money: A collection of Talks by Andreas Antonopoulos*, 1st ed. CreateSpace Independent Publishing Platform, 2016.

[4] W. Mougayar, *The Business Blockchain: : Promise, Practice, and Application of the Next Internet Technology*. Wiley, 2016.

[5] A. M. Antonopoulos, *The Internet of Money - Volume Two*. 2018.

[6] J. Frankenreiter, “The Limits of Smart Contracts,” *J. Institutional Theor. Econ. JITE*, vol. 175, no. 1, pp. 149–162, 2019, doi: 10.1628/jite-2019-0021.

[7] M. Poblet, D. W. E. Allen, O. Konashevych, A. M. Lane, and C. A. Diaz Valdivia, “From Athens to the Blockchain: Oracles for Digital Democracy,” *Front. Blockchain*, vol. 3, no. September, pp. 1–11, 2020, doi: 10.3389/fbloc.2020.575662.

[8] G. Caldarelli and J. Ellul, “The Blockchain Oracle Problem in Decentralized Finance - A Multivocal Approach,” *Appl. Sci.*, vol. 11, no. 16, p. 7572, Aug. 2021, doi: 10.3390/app11167572.

[9] J. Rodriguez, “The Middleman of Trust: The Oracle Paradox and Five Protocols that can Bring External Data into the....,” *Hackernoon*, 2018. https://hackernoon.com/the-middleman-of-trust-the-oracle-paradox-and-five-protocols-that-can-bring-external-data-into-the-df39b63e92ae (accessed Oct. 19, 2020).

[10] A. Egberts, “The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems,” *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.3382343.

[11] G. Caldarelli, “Understanding the Blockchain Oracle Problem : A Call for Action,” *Information*, vol. 11, no. 11, 2020, doi: 10.3390/info11110509.

[12] A. M. Antonopoulos, “The Killer App: Bananas on the Blockchain?,” *Coinscrum Meetup on*

13 June 2019 at Monzo Bank HQ, London, UK, 2019, 2019. https://aantonop.com/the-killer-app-bananas-on-theblockchain (accessed Mar. 03, 2020).

[13] G. Caldarelli, "Real-world blockchain applications under the lens of the oracle problem. A systematic literature review," in *2020 IEEE International Conference on Technology Management, Operations and Decisions, ICTMOD 2020, Marrakech, Morocco, 25–27 November 2020*, Nov. 2020, pp. 1–6, doi: 10.1109/ICTMOD49425.2020.9380598.

[14] A. Kumar, R. Liu, and Z. Shan, "Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities," *Decis. Sci.*, vol. 51, no. 1, pp. 8–37, Feb. 2020, doi: 10.1111/deci.12396.

[15] Szabo Nick, "Formalizing and securing relationships on public networks," 1997. https://journals.uic.edu/ojs/index.php/fm/article/view/548 (accessed Feb. 15, 2020).

[16] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2013. https://github.com/ethereum/wiki/wiki/White-Paper (accessed Apr. 12, 2020).

[17] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.

[18] S. E. Chang, Y.-C. Chen, and M.-F. Lu, "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process," *Technol. Forecast. Soc. Change*, vol. 144, pp. 1–11, 2019, doi: 10.1016/j.techfore.2019.03.015.

[19] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, I. Original, and T. Vieira, "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.*, pp. 1–13, 2016, doi: 10.1109/OBD.2016.11.

[20] L. Plant, "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.*, vol. 5, no. 3, pp. 15–29, 2017, doi: 10.18080/ajtde.v5n3.113.

[21] W. Hu, Y. W. Hu, W. H. Yao, W. Q. Lu, H. H. Li, and Z. W. Lv, "A blockchain-based smart contract trading mechanism for energy power supply and demand network," *Adv. Prod. Eng. Manag.*, vol. 14, no. 3, pp. 284–296, 2019, doi: 10.14743/apem2019.3.328.

[22] H.-C. H.-C. Sung, "Prospects and challenges posed by blockchain technology on the copyright legal system," *Queen Mary J. Intellect. Prop.*, vol. 9, no. 4, pp. 430–451, 2019, doi: 10.4337/qmjip.2019.04.04.

[23] A. Sheth and H. Subramanian, "Blockchain and contract theory: modeling smart contracts using insurance markets," *Manag. Financ.*, p. MF--10--2018--0510, 2019, doi: 10.1108/MF-10-2018-0510.

[24] C. Millard, "Blockchain and law: Incompatible codes?," *Comput. Law Secur. Rev.*, vol. 34, no. 4, pp. 843–846, 2018, doi: 10.1016/j.clsr.2018.06.006.

[25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[26] P. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, "Managing lifelong learning records through blockchain," *Res. Pract. Technol. Enhanc. Learn.*, vol. 14, no. 1, p. 4, 2019, doi: 10.1186/s41039-019-0097-0.

[27] L. Jiang and X. Zhang, "BCOSN: A Blockchain-Based Decentralized Online Social Network," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1454–1466, 2019, doi: 10.1109/TCSS.2019.2941650.

[28] D.-Y. Liao and X. Wang, "Applications of blockchain technology to logistics management in integrated casinos and entertainment," *Informatics*, vol. 5, no. 4, 2018, doi: 10.3390/informatics5040044.

[29] A. M. Antonopoulos and G. Woods, *Mastering Ethereum – Building Smart Contracts and DAPPS*. O'Reilly, 2018.

[30] M. Damjan, "The interface between blockchain and the real world," *Ragion Prat.*, vol. 2018, no. 2, pp. 379–406, 2018, doi: 10.1415/91545.

[31] U. Dalovindj, "The Oracle Problem," 2014. https://www.reddit.com/r/Bitcoin/comments/2p78kd/the_oracle_problem/ (accessed Mar. 02, 2020).

[32] A. Schaad, T. Reski, and O. Winzenried, "Integration of a Secure Physical Element as a Trusted Oracle in a Hyperledger Blockchain:," in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, 2019, pp. 498–503, doi: 10.5220/0007957104980503.

[33] G. Caldarelli, C. Rossignoli, and A. Zardini, "Overcoming the blockchain oracle problem in the traceability of non-fungible products," *Sustain.*, vol. 12, no. 6, 2020, doi: 10.3390/su12062391.

[34] S. Cohney, D. A. Hoffman, J. Sklaroff, and D. Wishnick, "Coin-Operated Capitalism," *SSRN Electron. J.*, 2018, doi: 10.2139/ssrn.3215345.

[35] M. A. M. A. Jamison and P. Tariq, "Five things regulators should know about blockchain (and three myths to forget)," *Electr. J.*, vol. 31, no. 9, pp. 20–23, 2018, doi: 10.1016/j.tej.2018.10.003.

[36] P. Lucena, A. P. D. Binotto, F. da S. Momo, and H. Kim, "A Case Study for Grain Quality Assurance Tracking based on a Blockchain Business Network," *arXiv1803.07877 [cs]*, Mar. 2018, Accessed: Mar. 20, 2020. [Online]. Available: http://arxiv.org/abs/1803.07877.

[37] R. Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with

IBM," *J. Br. Blockchain Assoc.*, vol. 1, no. 1, pp. 1–12, Jul. 2018, doi: 10.31585/jbba-1-1-(10)2018.

[38] D. Yermack, "Corporate governance and blockchains," *Rev. Financ.*, vol. 21, no. 1, pp. 7–31, 2017, doi: 10.1093/rof/rfw074.

[39] M. Finck and V. Moscon, "Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0," *IIC Int. Rev. Intellect. Prop. Compet. Law*, vol. 50, no. 1, pp. 77–108, 2019, doi: 10.1007/s40319-018-00776-8.

[40] I. Bauer, L. Zavolokina, F. Leisibach, and G. Schwabe, "Exploring Blockchain Value Creation: The Case of the Car Ecosystem," *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, no. October, 2019, doi: 10.24251/hicss.2019.822.

[41] A. M. Antonopoulos, *The Internet of Money - Volume Three*. Merkle Bloom LLC, 2019.

[42] P. Tasca and C. J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," *Ledger*, vol. 4, pp. 1–39, Feb. 2019, doi: 10.5195/ledger.2019.140.

[43] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis," *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, pp. 1543–1552, 2017, doi: 10.24251/hicss.2017.186.

[44] P. Grover, A. Kumar Kar, and P. Vigneswara Ilavarasan, "Blockchain for Businesses: A Systematic Literature Review," *Int. Fed. Inf. Process.*, vol. 7, no. July, pp. 325–336, 2018.

[45] Mamun M., "How does hyperledger Fabric works?," 2018. https://medium.com/coinmonks/how-does-hyperledger-fabric-works-cdb68e6066f5 (accessed Feb. 28, 2020).

[46] Swan M., *Blockchain: Blueprint for a New Economy*, 1st Editio. O'Reilly, 2015.

[47] M. Alharby and A. van Moorsel, "Blockchain Based Smart Contracts : A Systematic Mapping Study," in *Computer Science & Information Technology (CS & IT)*, Aug. 2017, pp. 125–140, doi: 10.5121/csit.2017.71011.

[48] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," *Bus. Horiz.*, vol. 62, no. 3, pp. 295–306, 2019, doi: 10.1016/j.bushor.2019.01.009.

[49] M. Jirgensons and J. Kapenieks, "Blockchain and the Future of Digital Learning Credential Assessment and Management," *J. Teach. Educ. Sustain.*, vol. 20, no. 1, pp. 145–156, 2018, doi: 10.2478/jtes-2018-0009.

[50] T. V. Shatkovskaya, A. B. Shumilina, G. G. Nebratenko, J. I. Isakova, and E. Y. Sapozhnikova, "Impact of technological blockchain paradigm on the movement of intellectual property in the digital space," *Eur. Res. Stud. J.*, vol. 21, no. Special Is, pp. 397–406, 2018.

[51] T. Sawa, “Blockchain technology outline and its application to field of power and energy system,” *Electr. Eng. Japan*, vol. 206, no. 2, pp. 11–15, Jan. 2019, doi: 10.1002/eej.23167.

[52] R. Ben Fekih and M. Lahami, *Application of Blockchain Technology in Healthcare: A Comprehensive Study*, vol. 12157 LNCS. Springer International Publishing, 2020.

[53] A. Guadamuz, “All watched over by machines of loving grace: A critical look at smart contracts,” *Comput. Law Secur. Rev.*, vol. 35, no. 6, p. 105338, 2019, doi: 10.1016/j.clsr.2019.105338.

[54] H. M. H. M. Kim and M. Laskowski, “Toward an ontology-driven blockchain design for supply-chain provenance,” *Intell. Syst. Accounting, Financ. Manag.*, vol. 25, no. 1, pp. 18–27, Jan. 2018, doi: 10.1002/isaf.1424.

[55] A. Ramachandran and D. M. Kantarcioglu, “Using {Blockchain} and smart contracts for secure data provenance management,” *arXiv1709.10000 [cs]*, Sep. 2017, Accessed: Feb. 11, 2020. [Online]. Available: http://arxiv.org/abs/1709.10000.

[56] Buck J., “Blockchain Oracles Explained,” 2017. https://cointelegraph.com/explained/blockchain-oracles-explained (accessed Mar. 01, 2020).

[57] Apla, “What is a Blockchain Oracle?,” 2018. https://blog.apla.io/what-is-a-blockchain-oracle-2ccca433c026 (accessed Mar. 01, 2020).

[58] B. Curran, “What are Oracles? Smart Contracts, Chainlink & “The Oracle Problem,” 2018. https://blockonomi.com/oracles-guide (accessed Apr. 12, 2019).

[59] P. Sztorc, “The Oracle Problem,” 2017. https://www.infoq.com/presentations/blockchain-oracle-problems (accessed Mar. 03, 2020).

[60] H. Liu, F.-C. Kuo, D. Towey, and T. Y. Chen, “How Effectively Does Metamorphic Testing Alleviate the Oracle Problem?,” *IEEE Trans. Softw. Eng.*, vol. 40, no. 1, pp. 4–22, Jan. 2014, doi: 10.1109/TSE.2013.46.

[61] E. T. Barr, M. Harman, P. McMinn, M. Shahbaz, and S. Yoo, “The Oracle Problem in Software Testing: A Survey,” *IEEE Trans. Softw. Eng.*, vol. 41, no. 5, pp. 507–525, May 2015, doi: 10.1109/TSE.2014.2372785.

[62] F. Pastore, L. Mariani, and G. Fraser, “CrowdOracles: Can the Crowd Solve the Oracle Problem?,” in *2013 {IEEE} {Sixth} {International} {Conference} on {Software} {Testing}, {Verification} and {Validation}*, Mar. 2013, pp. 342–351, doi: 10.1109/ICST.2013.13.

[63] S. Galson, “The Oracle Problem,” 2019. https://www.yld.io/blog/the-oracle-problem/ (accessed Mar. 02, 2020).

[64] J. Song, “The truth about Smart Contracts,” 2018. https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f (accessed Mar. 02, 2020).

[65] C. Harper, “What is ChainLink? A Beginner’s Guide to Decentralized Oracles,” 2018. https://coincentral.com/what-is-chainlink-a-beginners-guide-to-decentralized-oracles/ (accessed Mar. 12, 2020).

[66] O. Dale, “What is Chainlink? Guide to The Decentralized Oracle Network,” 2019. https://blockonomi.com/chainlink-guide/ (accessed Mar. 12, 2020).

[67] S. Haber and S. Stornetta, “How to timestamp a digital document - original blockchain paper 1991,” *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, 1991.

[68] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, “Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms,” *Bus. Horiz.*, vol. 62, no. 3, pp. 273–281, 2019, doi: 10.1016/j.bushor.2019.01.002.

[69] E. A. Grigoreva, L. F. Garifova, and E. A. Polovkina, “The future of digital technology in russia: Blockchain as one of the priority directions of development,” *Int. J. Emerg. Technol.*, vol. 10, no. 2, pp. 42–46, 2019.

[70] R. Bdiwi, C. De Runz, S. Faiz, and A. A. Cherif, “Towards a New Ubiquitous Learning Environment Based on Blockchain Technology,” in *Proceedings - IEEE 17th International Conference on Advanced Learning Technologies, ICALT 2017*, 2017, pp. 101–102, doi: 10.1109/ICALT.2017.37.

[71] A. G. A. F. Camiller, *Blockchain in Education Luxembourg : Publications Office of the European Union*, no. September. 2017.

[72] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, “EduCTX: A blockchain-based higher education credit platform,” *IEEE Access*, vol. 6, pp. 5112–5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[73] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[74] H. Treiblmaier, “The impact of the blockchain on the supply chain: a theory-based research framework and a call for action,” *Supply Chain Manag. An Int. J.*, vol. 23, no. 6, pp. 545–559, Sep. 2018, doi: 10.1108/SCM-01-2018-0029.

[75] E. Mik, “Smart contracts: terminology, technical limitations and real world complexity,” *Law, Innov. Technol.*, vol. 9, no. 2, pp. 269–300, 2017, doi: 10.1080/17579961.2017.1378468.

[76] J. Hou, H. Wang, and P. Liu, “Applying the blockchain technology to promote the development of distributed photovoltaic in China,” *Int. J. Energy Res.*, vol. 42, no. 6, pp. 2050–2069, 2018, doi: 10.1002/er.3984.

[77] E. Mengelkamp, J. Gärttner, and C. Weinhardt, “Decentralizing energy systems through local energy markets: The LAMP-project,” in *MKWI 2018 - Multikonferenz Wirtschaftsinformatik*, 2018, vol. 2018-March, pp. 924–930, [Online]. Available:

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048816947&partnerID=40&md5=9898e6f9b9401ee21861702927f6fb66.

[78] J. Wu and N. K. Tran, "Application of blockchain technology in sustainable energy systems: An overview," *Sustain.*, vol. 10, no. 9, 2018, doi: 10.3390/su10093067.

[79] Z. Li, S. Bahramirad, A. Paaso, M. Yan, and M. Shahidehpour, "Blockchain for decentralized transactive energy management system in networked microgrids," *Electr. J.*, vol. 32, no. 4, pp. 58–72, 2019, doi: 10.1016/j.tej.2019.03.008.

[80] A. Tsankov, "The 'Oracle Problem' isn't a Problem, and why Smart Contracts makes Insurance better for everyone," 2018. https://medium.com/@antsankov/the-oracle-problem-isnt-a-problem-and-why-smart-contracts-makes-insurance-better-for-everyone-8c979f09851c (accessed Mar. 02, 2020).

[81] *Arizona House Bill 2417: signatures; electronic transactions; blockchain technology*. Arizona: House of Representatives, 2017, pp. 1–3.

[82] A. Jeffries, "'Blockchain' is Meaningless," *Verge*, 2018. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning (accessed Apr. 19, 2020).

[83] D. Gerard, "The World Food Programme's much publicized 'blockchain' has one participant – i.e., it's a database," 2017. https://davidgerard.co.uk/blockchain/2017/11/26/the-world-food-programmes-much-publicised-blockchain-has-one-participant-i-e-its-a-database/ (accessed Mar. 17, 2020).

[84] R. Brownsword, "Regulatory Fitness: Fintech, Funny Money, and Smart Contracts," *Eur. Bus. Organ. Law Rev.*, vol. 20, no. 1, pp. 5–27, 2019, doi: 10.1007/s40804-019-00134-2.

[85] K. F. K. K. Low and E. Mik, "PAUSE THE BLOCKCHAIN LEGAL REVOLUTION," *Int. Comp. Law Q.*, vol. 69, no. 1, pp. 135–175, Jan. 2020, doi: 10.1017/S0020589319000502.

[86] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town Crier: An Authenticated Data Feed for Smart Contracts," 2016. https://eprint.iacr.org/2016/168.pdf, (accessed Mar. 05, 2020).

[87] C. Thomson, "The DAO of ETHEREUM: Analyzing the DAO hack, the Blockchain, Smart contracts, and the Law," *Medium*, 2016. https://medium.com/blockchain-review/the-dao- of- ethereum- e228b93afc79 (accessed Apr. 03, 2020).

[88] R. Graham, "Ethereum/TheDAO hack simplified," *Errata Security Blog*, 2016. https://blog.erratasec.com/2016/06/ etheriumdao- hack- similfied.html (accessed Apr. 14, 2020).

[89] M. De Silva, "Ethereum Classic is under attack," *Quartz*, 2019. https://qz.com/1516994/ethereum- classic- got- hit- by- a- 51- attack/ (accessed Mar. 12, 2020).

[90] D. Sui, S. Ricci, and J. Pfeffer, "Are Miners Centralized? A Look into Mining Pools," 2018.

https://media.consensys.net/ are- miners- centralized- a- look- into- mining- pools-b594425411dc.

[91] I. Radanović and R. Likić, "Opportunities for Use of Blockchain Technology in Medicine," *Appl. Health Econ. Health Policy*, vol. 16, no. 5, pp. 583–590, 2018, doi: 10.1007/s40258-018-0412-8.

[92] A. Tandon, A. Dhir, N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.*, vol. 122, 2020, doi: 10.1016/j.compind.2020.103290.

[93] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," *Int. J. Inf. Manage.*, vol. 52, no. March, p. 102024, 2020, doi: 10.1016/j.ijinfomgt.2019.10.009.

[94] J. A. H. Rensaa, D. Gligoroski, K. Kralevska, A. Hasselgren, and A. Faxvaag, "VerifyMed-A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept," *ACM Int. Conf. Proceeding Ser.*, pp. 73–80, 2020, doi: 10.1145/3409934.3409946.

[95] E. Meinert *et al.*, "Blockchain Implementation in Health Care: Protocol for a Systematic Review," *JMIR Res. Protoc.*, vol. 8, no. 2, p. e10994, Feb. 2019, doi: 10.2196/10994.

[96] T. Rupasinghe, F. Burstein, C. Rudolph, and S. Strange, "Towards a Blockchain based Fall Prediction Model for Aged Care," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3290688.3290736.

[97] S. A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," *Law Soc. Inq.*, vol. 43, no. 2, pp. 417–440, 2018, doi: 10.1111/lsi.12303.

[98] T. H. McCoy and R. H. Perlis, "Temporal trends and characteristics of reportable health data breaches, 2010-2017," *JAMA - J. Am. Med. Assoc.*, vol. 320, no. 12, pp. 1282–1284, 2018, doi: 10.1001/jama.2018.9222.

[99] T. Donald, "The Most Promising Blockchain Healthcare Projects [2020]," *LumiBLOG*, 2020. https://blog.lumiwallet.com/the-most-promising-blockchain-healthcare-projects-2020/ (accessed Oct. 20, 2020).

[100] A. Lielacher, "Top Blockchain Healthcare Projects for 2020, Rated and Reviewed," *Bitcoinmarketjournal*, 2020. https://www.bitcoinmarketjournal.com/top-blockchain-healthcare-projects-for-2019-rated-and-reviewed/ (accessed Oct. 21, 2020).

[101] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *Int. J. Med. Inform.*, vol. 134, no. May 2019, p. 104040, 2020, doi: 10.1016/j.ijmedinf.2019.104040.

[102] P. Collins, "What Is a Blockchain Oracle?," *Medium.com*, 2020. https://medium.com/better-programming/what-is-a-blockchain-oracle-f5ccab8dbd72 (accessed Oct. 21, 2020).

[103] A. N. Desk, "Solve.Care Collaborates With Chainlink To Deliver Real-World Data For Blockchain Healthcare Services," *AiThority*, 2020. https://aithority.com/technology/blockchain/solve-care-collaborates-with-chainlink-to-deliver-real-world-data-for-blockchain-healthcare-services/ (accessed Oct. 20, 2020).

[104] R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," 2018, doi: 10.1109/ICE.2018.8436324.

[105] J. Shawdagor, "Solve.Care partners with Chainlink to revolutionize the healthcare sector," *NVEZZ*, 2020. https://invezz.com/news/2020/10/20/solve-care-partners-with-chainlink-to-revolutionize-the-healthcare-sector/ (accessed Oct. 22, 2020).

[106] T. K. Sharma, "TOP 10 REAL-WORLD APPLICATIONS OF BLOCKCHAIN TECHNOLOGY," *Blockchain Council*, 2019. https://www.blockchain-council.org/blockchain/top-10-real-world-applications-of-blockchain-technology/ (accessed Apr. 02, 2020).

[107] F. J., "Bitcoin Maximalism," *Investopedia*, 2018. https://www.investopedia.com/terms/b/bitcoin-maximalism.asp (accessed Apr. 16, 2020).

[108] J. Pereira, M. M. Tavalaei, and H. Ozalp, "Blockchain-based platforms: Decentralized infrastructures and its boundary conditions," *Technol. Forecast. Soc. Change*, vol. 146, no. April, pp. 94–102, 2019, doi: 10.1016/j.techfore.2019.04.030.

[109] A. M. Rozario and M. A. Vasarhelyi, "Auditing with smart contracts," *Int. J. Digit. Account. Res.*, vol. 18, no. December 2017, pp. 1–27, 2018, doi: 10.4192/1577-8517-v18_1.

[110] P. Cuccuru, "Beyond bitcoin: An early overview on smart contracts," *Int. J. Law Inf. Technol.*, vol. 25, no. 3, pp. 179–195, 2017, doi: 10.1093/ijlit/eax003.

[111] H. Eenmaa-Dimitrieva and M. J. Schmidt-Kessen, "Creating markets in no-trust environments: The law and economics of smart contracts," *Comput. Law Secur. Rev.*, vol. 35, no. 1, pp. 69–88, 2019, doi: 10.1016/j.clsr.2018.09.003.

[112] H. Subramanian, "Security tokens: architecture, smart contract applications and illustrations using SAFE," *Manag. Financ.*, vol. 46, no. 6, pp. 735–748, Aug. 2019, doi: 10.1108/MF-09-2018-0467.

[113] C. L. Reyes, "If Rockefeller were a coder," *George Washington Law Rev.*, vol. 87, no. 2, pp. 373–429, 2019, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065259661&partnerID=40&md5=77c37c70224ff445cdc8dc0ff94e45de.

[114] B. Reinsberg, "Blockchain technology and the governance of foreign aid," *J. Institutional Econ.*, vol. 15, no. 3, pp. 413–429, 2019, doi: 10.1017/S1744137418000462.

[115] K. Werbach and N. Cornell, "Contracts ex machina," *Duke Law J.*, vol. 67, no. 2, pp. 313–382, 2017, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034790368&partnerID=40&md5=e696f8d48267cfbd95df24d0003a23ab.

[116] B. Liu, P. Szalachowski, and J. Zhou, "A First Look into DeFi Oracles," *arXiv*, no. March, May 2020, [Online]. Available: http://arxiv.org/abs/2005.04377.

[117] A. Albizri and D. Appelbaum, "Trust but Verify: The Oracle Paradox of Blockchain Smart ContractsTrust but Verify: The Oracle Paradoxof Smart Contracts," *J. Inf. Syst.*, Mar. 2021, doi: 10.2308/ISYS-19-024.

[118] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges," *IEEE Access*, vol. 8, pp. 85675–85685, 2020, doi: 10.1109/ACCESS.2020.2992698.

[119] H. Al Breiki, L. Al Qassem, K. Salah, M. Habib Ur Rehman, and D. Sevtinovic, "Decentralized access control for IoT data using blockchain and trusted oracles," in *Proceedings - IEEE International Conference on Industrial Internet Cloud, ICII 2019*, 2019, pp. 248–257, doi: 10.1109/ICII.2019.00051.

[120] G. Caldarelli, "Formalizing Oracle Trust Models for blockchain-based business applications. An example from the supply chain sector," Feb. 2022, doi: 10.48550/arxiv.2202.13930.

[121] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," *J. Comput. High. Educ.*, vol. 32, no. 1, pp. 109–134, 2020, doi: 10.1007/s12528-019-09209-y.

[122] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, "A Quantifiable Trust Model for Blockchain-Based Identity Management," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1475–1482, doi: 10.1109/Cybermatics_2018.2018.00250.

[123] G. Caldarelli, *Blockchain Oracles and the Oracle Problem: A practical handbook to discover the world of blockchain, smart contracts, and oracles —exploring the limits of trust decentralization.*, 1st ed. Naples, Italy: Amazon Publishing, 2021.

[124] M. D. Sheldon, "Auditing the blockchain oracle problem," *J. Inf. Syst.*, vol. 35, no. 1, pp. 121–133, 2021, doi: 10.2308/ISYS-19-049.

[125] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," *PLoS One*, vol. 11, no. 10, p. e0163477, Oct. 2016, doi: 10.1371/journal.pone.0163477.

[126] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram, "Blockchain - Literature survey," in *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings*, 2017, vol. 2018-Janua, pp. 2145–2148, doi: 10.1109/RTEICT.2017.8256979.

[127] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review*," *Br. J. Manag.*, vol. 14, pp. 207–222, 2003.

[128] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, “How to conduct a bibliometric analysis: An overview and guidelines,” *J. Bus. Res.*, vol. 133, no. April, pp. 285–296, 2021, doi: 10.1016/j.jbusres.2021.04.070.

[129] A. S. Chaudhary, S. H. Mandalia, S. P. Chaudhari, and A. B. Parmar, “Lincoln Bibliometric study of SAARC Countries Research Trends in Public Health using Scopus database Bibliometric study of SAARC Countries Research Trends in Public Health using,” *Libr. Philos. Pract.*, 2021.

[130] L. Philosophy, N. Dulla, and S. C. Swain, “Global Exploration on Bibliometric Research Articles : A Bibliometric Analysis,” *Libr. Philos. Pract.*, 2021.

[131] M. R. A. Aziz, M. Z. Jali, M. N. M. Noor, S. Sulaiman, M. S. Harun, and M. Z. I. Mustafar, “Bibliometric Analysis Of Literatures On Digital Banking And Financial Inclusion Between 2014-2020,” *Libr. Philos. Pract.*, vol. 2021, pp. 1–31, 2021.

[132] M. J. Cobo, M. A. Martínez, M. Gutiérrez-Salcedo, H. Fujita, and E. Herrera-Viedma, “25 years at Knowledge-Based Systems: A bibliometric analysis,” *Knowledge-Based Syst.*, vol. 80, pp. 3–13, 2015, doi: 10.1016/j.knosys.2014.12.035.

[133] V. Buttice and E. Ughetto, “What, Where, Who, and How? A Bibliometric Study of Crowdfunding Research,” *IEEE Trans. Eng. Manag.*, pp. 1–22, 2021, doi: 10.1109/TEM.2020.3040902.

[134] X. Liu, R. Chen, Y.-W. Chen, and S.-M. Yuan, “Off-chain Data Fetching Architecture for Ethereum Smart Contract,” 2018, doi: 10.1109/ICCBB.2018.8756348.

[135] K. Mammadzada, M. Iqbal, F. Milani, L. García-Bañuelos, and R. Matulevičius, *Blockchain Oracles: A Framework for Blockchain-Based Applications*, vol. 393 LNBIP. 2020.

[136] A. Beniiche, “A study of blockchain oracles,” *arXiv*, pp. 1–9, 2020.

[137] J. Thevenard, “Decentralised Oracles: a comprehensive overview,” *Medium.com*, 2019. https://medium.com/fabric-ventures/decentralised-oracles-a-comprehensive-overview-d3168b9a8841 (accessed Apr. 19, 2020).

[138] H. Huilgolkar, “Razor Network : A decentralized oracle platform,” 2021. https://razor.network/whitepaper.pdf (accessed Feb. 18, 2021).

[139] L. Breidenbach *et al.*, “Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks,” 2021. [Online]. Available: https://research.chain.link/whitepaper-v2.pdf.

[140] G. Caldarelli and J. Ellul, “Trusted academic transcripts on the blockchain: A systematic literature review,” *Appl. Sci.*, vol. 11, no. 4, pp. 1–22, 2021, doi: 10.3390/app11041842.

[141] T. K. Sharma, “Centralized Oracles VS. Decentralized Oracles,” *Blockchain Council*, 2020. https://www.blockchain-council.org/blockchain/centralized-oracles-vs-decentralized-oracles/ (accessed Feb. 11, 2021).

[142] A. Larsens, “Multisignature Wallet: How does it work?,” *Techzone360*, 2021.

https://www.techzone360.com/topics/techzone/articles/2021/07/21/449512-multisignature-wallet-how-does-it-work.htm (accessed Aug. 10, 2021).

[143] A. Pasdar, Z. Dong, and Y. C. Lee, “Blockchain Oracle Design Patterns,” pp. 1–25, Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.09349.

[144] T. Kumar Sharma, “WHAT IS A BLOCKCHAIN ORACLE? A DETAILED OVERVIEW,” *Blockchain Council*, 2020. https://www.blockchain-council.org/blockchain/what-is-a-blockchain-oracle-a-detailed-overview/ (accessed Jul. 09, 2021).

[145] G. Anadiotis, “Off-chain reporting: Toward a new general purpose secure compute framework by Chainlink,” *ZdNet*, 2021. https://www.zdnet.com/article/off-chain-reporting-towards-a-new-general-purpose-secure-compute-framework-by-chainlink/ (accessed Mar. 19, 2021).

[146] S. Eskandari, M. Salehi, W. C. Gu, and J. Clark, “SoK: Oracles from the Ground Truth to Market Manipulation,” *Proc. Under Rev. (May 2021)*, vol. 1, no. 1, Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.00667.

[147] M. Pahulje, “What are NFTs & What does it Mean for Supply Chains?,” *Flexis Blog*, May 18, 2021. https://blog.flexis.com/what-are-nfts-what-does-it-mean-for-supply-chains (accessed Nov. 02, 2021).

[148] C. Kameir, “NFT’s Real World Use Case: Supply Chain | Hacker Noon,” *Hackernoon*, Mar. 28, 2021. https://hackernoon.com/nfts-real-world-use-cases-exhibit-that-the-show-is-just-getting-started-mm3f33b8 (accessed Nov. 02, 2021).

[149] G. Caldarelli, “Wrapping Trust for Interoperability: A Preliminary Study of Wrapped Tokens,” *Inf. 2022, Vol. 13, Page 6*, vol. 13, no. 1, p. 6, Dec. 2021, doi: 10.3390/INFO13010006.

[150] C. Martínez-Climent, A. Zorio-Grima, and D. Ribeiro-Soriano, “Financial return crowdfunding: literature review and bibliometric analysis,” *Int. Entrep. Manag. J.*, vol. 14, no. 3, pp. 527–553, 2018, doi: 10.1007/s11365-018-0511-x.

[151] F. Caviggioli and E. Ughetto, “A bibliometric analysis of the research dealing with the impact of additive manufacturing on industry, business and society,” *Int. J. Prod. Econ.*, vol. 208, no. December 2018, pp. 254–268, 2019, doi: 10.1016/j.ijpe.2018.11.022.

[152] F. Tenca, A. Croce, and E. Ughetto, “Business Angels Research in Entrepreneurial Finance: a Literature Review and a Research Agenda,” *J. Econ. Surv.*, vol. 32, no. 5, pp. 1384–1413, 2018, doi: 10.1111/joes.12224.

[153] O. Ramona, M. S. Cristina, and S. Raluca, “Bitcoin in the scientific literature - A bibliometric study,” *Stud. Bus. Econ.*, vol. 14, no. 3, pp. 160–174, 2020, doi: 10.2478/sbe-2019-0051.

[154] X. Xu *et al.*, “The blockchain as a software connector,” *Proc. - 2016 13th Work. IEEE/IFIP Conf. Softw. Archit. WICSA 2016*, pp. 182–191, 2016, doi: 10.1109/WICSA.2016.21.

[155] A. Dubey, G. D. Hill, E. G. Sirer, and R. Escriva, “Weaver: A high-performance, transactional graph database based on refinable timestamps,” *Proc. VLDB Endow.*, vol. 9, no. 11, pp. 852–863, 2016, doi: 10.14778/2983200.2983202.

[156] A. Firdaus, M. F. A. Razak, A. Feizollah, I. A. T. Hashem, M. Hazim, and N. B. Anuar, “The rise of ‘blockchain’: bibliometric analysis of blockchain study,” *Scientometrics*, vol. 120, no. 3, pp. 1289–1331, Sep. 2019, doi: 10.1007/s11192-019-03170-4.

[157] B. Musigmann, H. von der Gracht, and E. Hartmann, “Blockchain Technology in Logistics and Supply Chain Management—A Bibliometric Literature Review From 2016 to January 2020,” *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 988–1007, Nov. 2020, doi: 10.1109/TEM.2020.2980733.

[158] L. Ante, F. Steinmetz, and I. Fiedler, “Blockchain and energy: A bibliometric analysis and review,” *Renew. Sustain. Energy Rev.*, vol. 137, no. October 2020, p. 110597, Mar. 2021, doi: 10.1016/j.rser.2020.110597.

[159] L. Ante, “Smart contracts on the blockchain – A bibliometric analysis and review,” *Telemat. Informatics*, vol. 57, no. October 2020, p. 101519, Mar. 2021, doi: 10.1016/j.tele.2020.101519.

[160] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, “Trust management in a blockchain based fog computing platform with trustless smart oracles,” *Futur. Gener. Comput. Syst.*, vol. 101, pp. 747–759, 2019, doi: 10.1016/j.future.2019.07.030.

[161] R. Mühlberger *et al.*, “Foundational Oracle Patterns: Connecting Blockchain to the Off-chain World,” *Lect. Notes Bus. Inf. Process.*, vol. 393 LNBIP, pp. 35–51, Jul. 2020, doi: 10.1007/978-3-030-58779-6_3.

[162] X. Xu, C. Pautasso, L. Zhu, Q. Lu, and I. Weber, “A pattern collection for blockchain-based applications,” *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3282308.3282312.

[163] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*. 2019.

[164] X. Xu, H. M. N. Dilum Bandara, Q. Lu, I. Weber, L. Bass, and L. Zhu, “A Decision Model for Choosing Patterns in Blockchain-Based Applications,” *Proc. - IEEE 18th Int. Conf. Softw. Archit. ICSA 2021*, no. February, pp. 47–57, 2021, doi: 10.1109/ICSA51549.2021.00013.

[165] C. Hendrix and R. Lewis, “Survey on Blockchain Privacy Challenges,” *Ceur-Ws.org*, 2021. https://www.semanticscholar.org/paper/Survey-on-Blockchain-Privacy-Challenges-Hendrix-Lewis/d2e0112490911091de39ea82fb97cd4f7aa829f4 (accessed Mar. 18, 2022).

[166] S. Y. Lin, L. Zhang, J. Li, L. li Ji, and Y. Sun, “A survey of application research based on blockchain smart contract,” *Wirel. Networks*, vol. 28, no. 2, pp. 635–690, 2022, doi: 10.1007/s11276-021-02874-x.

[167] W. Zhang, L. Wei, S. Li, Y. Liu, and S. C. Cheung, “Đarcher: Detecting on-chain-off-chain synchronization bugs in decentralized applications,” *ESEC/FSE 2021 - Proc. 29th ACM Jt. Meet. Eur. Softw. Eng. Conf. Symp. Found. Softw. Eng.*, pp. 553–565, Aug. 2021, doi:

10.1145/3468264.3468546.

[168] K. Turksonmez, M. Furtak, M. P. Wittie, and D. L. Millman, “Two Ways Gas Price Oracles Miss the Mark,” *2021 IEEE Int. Conf. Omni-Layer Intell. Syst. COINS 2021*, Aug. 2021, doi: 10.1109/COINS51742.2021.9524148.

[169] R. Mars, A. Abid, S. Cheikhrouhou, and S. Kallel, “A machine learning approach for gas price prediction in ethereum blockchain,” in *Proceedings - 2021 IEEE 45th Annual Computers, Software, and Applications Conference, COMPSAC 2021*, Jul. 2021, pp. 156–165, doi: 10.1109/COMPSAC51774.2021.00033.

[170] G. A. Pierro, H. Rocha, S. Ducasse, M. Marchesi, and R. Tonelli, “A user-oriented model for Oracles’ Gas price prediction,” *Futur. Gener. Comput. Syst.*, vol. 128, pp. 142–157, Mar. 2022, doi: 10.1016/J.FUTURE.2021.09.021.

[171] Y. Mezquita, D. Valdeolmillos, A. González-Briones, J. Prieto, and J. M. Corchado, “Legal aspects and emerging risks in the use of smart contracts based on blockchain,” *Commun. Comput. Inf. Sci.*, vol. 1027, pp. 525–535, 2019, doi: 10.1007/978-3-030-21451-7_45.

[172] M. D. Sheldon, “Preparing Auditors for the Blockchain Oracle Problem,” *Curr. Issues Audit.*, vol. 15, no. 2, pp. P27–P39, Sep. 2021, doi: 10.2308/CIIA-2021-007.

[173] R. M. Murimi and G. G. Wang, “On elastic incentives for blockchain oracles,” *J. Database Manag.*, vol. 32, no. 1, pp. 1–26, 2021, doi: 10.4018/JDM.2021010101.

[174] K. Yutaka and A. Fujihara, “ken-system: Experimental performance evaluation on avoidance of blockchain oracle problem using collective intelligence,” Accessed: Jul. 24, 2021. [Online]. Available: https://www.ieice.org/ken/paper/20210305kCcu/eng/.

[175] M. Kaleem and W. Shi, “Demystifying Pythia: A Survey of ChainLink Oracles Usage on Ethereum,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12676 LNCS, pp. 115–123, 2021, doi: 10.1007/978-3-662-63958-0_10/FIGURES/5.

[176] M. Kumar, N. Nikhil, and R. Singh, “Decentralising Finance using Decentralised Blockchain Oracles,” in *2020 International Conference for Emerging Technology (INCET)*, Jun. 2020, pp. 1–4, doi: 10.1109/INCET49848.2020.9154123.

[177] K. Tjiam, R. Wang, H. Chen, and K. Liang, “Your Smart Contracts Are Not Secure: Investigating Arbitrageurs and Oracle Manipulators in Ethereum,” *CYSARM 2021 - Proc. 3rd Work. Cyber-Security Arms Race, co-located with CCS 2021*, pp. 25–35, Nov. 2021, doi: 10.1145/3474374.3486916.

[178] B. Wang *et al.*, “BLOCKEYE: Hunting For DeFi Attacks on Blockchain,” pp. 1–4, 2021, [Online]. Available: http://arxiv.org/abs/2103.02873.

[179] L. Bai, “Oracle’s Application in Finance,” in *Advances in Intelligent Systems and Computing*, vol. 1303, 2021, pp. 65–70.

[180] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, “Implementing

decentralized auctions using blockchain smart contracts," *Technol. Forecast. Soc. Change*, vol. 168, no. May 2020, p. 120786, 2021, doi: 10.1016/j.techfore.2021.120786.

[181] P. Lafourcade *et al.*, "Security Analysis of Auctionity : a blockchain based e-auction," 2019.

[182] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," *ACM Computing Surveys*, vol. 54, no. 8. ACM PUB27 New York, NY, pp. 1–41, Nov. 30, 2022, doi: 10.1145/3471140.

[183] Y. Hei, D. Li, C. Zhang, J. Liu, Y. Liu, and Q. Wu, "Practical AgentChain: A compatible cross-chain exchange system," *Futur. Gener. Comput. Syst.*, vol. 130, pp. 207–218, May 2022, doi: 10.1016/J.FUTURE.2021.11.029.

[184] C. Di Ciccio, G. Meroni, and P. Plebani, "On the adoption of blockchain for business process monitoring," *Softw. Syst. Model.*, pp. 1–23, Jan. 2022, doi: 10.1007/S10270-021-00959-X/TABLES/2.

[185] J. Ladleif and M. Weske, "Time in Blockchain-Based Process Execution," *Proc. - 2020 IEEE 24th Int. Enterp. Distrib. Object Comput. Conf. EDOC 2020*, pp. 217–226, 2020, doi: 10.1109/EDOC49727.2020.00034.

[186] J. Ladleif, I. Weber, and M. Weske, *External Data Monitoring Using Oracles in Blockchain-Based Process Execution*, vol. 393 LNBIP. 2020.

[187] J. Ladleif and M. Weske, "Which Event Happened First? Deferred Choice on Blockchain Using Oracles," 2021, [Online]. Available: http://arxiv.org/abs/2104.10520.

[188] B. Carminati, E. Ferrari, and C. Rondanini, "Blockchain as a platform for secure inter-organizational business processes," *Proc. - 4th IEEE Int. Conf. Collab. Internet Comput. CIC 2018*, pp. 122–129, 2018, doi: 10.1109/CIC.2018.00027.

[189] B. Carminati, C. Rondanini, and E. Ferrari, "Confidential Business Process Execution on Blockchain," in *Proceedings - 2018 IEEE International Conference on Web Services, ICWS 2018 - Part of the 2018 IEEE World Congress on Services*, 2018, pp. 58–65, doi: 10.1109/ICWS.2018.00015.

[190] W. Lu, X. Li, F. Xue, R. Zhao, L. Wu, and A. G. O. Yeh, "Exploring smart construction objects as blockchain oracles in construction supply chain management," *Autom. Constr.*, vol. 129, 2021, doi: 10.1016/j.autcon.2021.103816.

[191] F. Victor and S. Zickau, "Geofences on the blockchain: Enabling decentralized location-based services," in *IEEE International Conference on Data Mining Workshops, ICDMW*, 2019, vol. 2018-Novem, pp. 97–104, doi: 10.1109/ICDMW.2018.00021.

[192] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT Blockchain Architecture Using Oracles and Smart Contracts: The Use-Case of a Food Supply Chain," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2019, vol. 2019-Septe, doi: 10.1109/PIMRC.2019.8904404.

[193] N. Sánchez-Gómez, M. M. Risoto, J. M. Ramos-Cueli, T. Wojdyński, D. Lizcano, and J. Torres-Valderrama, "The current limitations of blockchain traceability: Challenges from industry," *WEBIST 2020 - Proc. 16th Int. Conf. Web Inf. Syst. Technol.*, no. Webist, pp. 373–380, 2020, doi: 10.5220/0010213503730380.

[194] D. Marbouh *et al.*, "Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System," *Arab. J. Sci. Eng.*, vol. 45, no. 12, pp. 9895–9911, 2020, doi: 10.1007/s13369-020-04950-4.

[195] W. Powell, M. Foth, S. Cao, and V. Natanelov, "Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains," *J. Ind. Inf. Integr.*, vol. 25, p. 100261, Jan. 2022, doi: 10.1016/J.JII.2021.100261.

[196] G. Caldarelli, A. Zardini, and C. Rossignoli, "Blockchain adoption in the fashion sustainable supply chain: Pragmatically addressing barriers," *J. Organ. Chang. Manag.*, vol. 34, no. 2, pp. 507–524, 2021, doi: 10.1108/JOCM-09-2020-0299.

[197] M. M. Madine *et al.*, "Blockchain for Giving Patients Control over Their Medical Records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020, doi: 10.1109/ACCESS.2020.3032553.

[198] M. M. Madine *et al.*, "Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records," *IEEE Access*, vol. 8, pp. 225777–225791, 2020, doi: 10.1109/ACCESS.2020.3045048.

[199] J. P. B. Gonçalves, H. C. de Resende, R. S. Villaca, E. Municio, C. B. Both, and J. M. Marquez-Barja, "Distributed Network Slicing Management Using Blockchains in E-Health Environments," *Mob. Networks Appl.*, 2021, doi: 10.1007/s11036-021-01745-1.

[200] A. Beniiche, S. Rostami, and M. Maier, "Robonomics in the 6G Era: Playing the Trust Game with On-Chaining Oracles and Persuasive Robots," *IEEE Access*, vol. 9, pp. 46949–46959, 2021, doi: 10.1109/ACCESS.2021.3068239.

[201] B. Sata, A. Berlanga, C. P. C. Chanel, and J. Lacan, "Connecting AI-based Oracles to Blockchains via an Auditable Auction Protocol," *2021 3rd Conf. Blockchain Res. Appl. Innov. Networks Serv. BRAINS 2021*, pp. 23–24, Sep. 2021, doi: 10.1109/BRAINS52497.2021.9569808.

[202] A. El Fezzazi, A. Adadi, and M. Berrada, "Towards a Blockchain based Intelligent and Secure Voting," *5th Int. Conf. Intell. Comput. Data Sci. ICDS 2021*, 2021, doi: 10.1109/ICDS53782.2021.9626751.

[203] Richard, M. M. Surya, and A. C. Wibowo, "Converging artificial intelligence and blockchain technology using oracle contract in ethereum blockchain platform," Nov. 2020, doi: 10.1109/ICIC50835.2020.9288611.

[204] G. Gordon, "Provenance and Authentication of Oracle Sensor Data with Block Chain Lightweight Wireless Network Authentication Scheme for Constrained Oracle Sensors," p. 222, 2017.

[205] S. Vári-Kakas, O. Poszet, A. Mirela Pater, E. Valentina Moisi, and A. Vári-Kakas, "Issues Related to the Use of Blockchains in IoT Applications," *2021 16th Int. Conf. Eng. Mod. Electr. Syst. EMES 2021 - Proc.*, Jun. 2021, doi: 10.1109/EMES52337.2021.9484103.

[206] P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT," *Softw. - Pract. Exp.*, 2019, doi: 10.1002/spe.2739.

[207] C. Rondanini, B. Carminati, and E. Ferrari, "Confidential discovery of IoT devices through blockchain," in *Proceedings - 2019 IEEE International Congress on Internet of Things, ICIOT 2019 - Part of the 2019 IEEE World Congress on Services*, 2019, pp. 1–8, doi: 10.1109/ICIOT.2019.00014.

[208] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "Towards a Scalable and Trustworthy Blockchain: IoT Use Case," *IEEE Int. Conf. Commun.*, Jun. 2021, doi: 10.1109/ICC42927.2021.9500535.

[209] P. Kochovski *et al.*, "Smart Contracts for Service-Level Agreements in Edge-to-Cloud Computing," *J. Grid Comput.*, vol. 18, no. 4, pp. 673–690, 2020, doi: 10.1007/s10723-020-09534-y.

[210] X. Tao and A. S. Hafid, "ChainSensing: A Novel Mobile Crowdsensing Framework with Blockchain," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2999–3010, Feb. 2022, doi: 10.1109/JIOT.2021.3094670.

[211] M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "A Blockchain-Based Model for Cloud Service Quality Monitoring," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 276–288, 2020, doi: 10.1109/TSC.2019.2948010.

[212] M. Comuzzi, C. Cappiello, and G. Meroni, "An Empirical Evaluation of Smart Contract-Based Data Quality Assessment in Ethereum," *Lect. Notes Bus. Inf. Process.*, vol. 428, pp. 51–66, 2021, doi: 10.1007/978-3-030-85867-4_5/TABLES/2.

[213] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. Jayaraman, "Blockchain-based multi-party authorization for accessing iPFS encrypted data," *IEEE Access*, vol. 8, pp. 196813–196825, 2020, doi: 10.1109/ACCESS.2020.3034260.

[214] A. Battah, Y. Iraqi, and E. Damiani, "Blockchain-based reputation systems: Implementation challenges and mitigation," *Electron.*, vol. 10, no. 3, pp. 1–20, 2021, doi: 10.3390/electronics10030289.

[215] D. Mitra, L. Tauz, and L. Dolecek, "Communication-Efficient LDPC Code Design for Data Availability Oracle in Side Blockchains," 2021, [Online]. Available: http://arxiv.org/abs/2105.06004.

[216] Z. Gao, H. Li, K. Xiao, and Q. Wang, "Cross-chain oracle based data migration mechanism in heterogeneous blockchains," in *Proceedings - International Conference on Distributed Computing Systems*, 2020, vol. 2020-Novem, pp. 1263–1268, doi: 10.1109/ICDCS47774.2020.00162.

[217] R. Ouyang and R. Ouyang, “HBRO: A Registration Oracle Scheme for Digital Rights Management Based on Heterogeneous Blockchains,” *Commun. Netw.*, vol. 14, no. 1, pp. 45–67, Dec. 2021, doi: 10.4236/CN.2022.141005.

[218] A. Al Zaabi, C. Y. Yeun, and E. Damiani, “Trusting Testcases Using Blockchain-Based Repository Approach,” *Symmetry 2021, Vol. 13, Page 2024*, vol. 13, no. 11, p. 2024, Oct. 2021, doi: 10.3390/SYM13112024.

[219] L. Y. Yeh, N. X. Shen, and R. H. Hwang, “Blockchain-Based Privacy-Preserving and Sustainable Data Query Service Over 5G-VANETs,” *IEEE Trans. Intell. Transp. Syst.*, 2022, doi: 10.1109/TITS.2022.3146322.

[220] P. Lv, X. Zhang, J. Liu, T. Wei, and J. Xu, “Blockchain Oracle-Based Privacy Preservation and Reliable Identification for Vehicles,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12939 LNCS, pp. 512–520, 2021, doi: 10.1007/978-3-030-86137-7_54/TABLES/2.

[221] T. Osterland and T. Rose, “Oracle-based process automation in DLT dominated ecosystems with an application to German waterway transportation,” in *ACM International Conference Proceeding Series*, 2021, pp. 130–136, doi: 10.1145/3456126.3456132.

[222] C. Antal *et al.*, “Blockchain based decentralized local energy flexibility market,” *Energy Reports*, vol. 7, pp. 5269–5288, Nov. 2021, doi: 10.1016/j.egyr.2021.08.118.

[223] A. Zeiselmair, B. Steinkopf, U. Gallersdörfer, A. Bogensperger, and F. Matthes, “Analysis and Application of Verifiable Computation Techniques in Blockchain Systems for the Energy Sector,” *Front. Blockchain*, vol. 0, p. 37, Sep. 2021, doi: 10.3389/FBLOC.2021.725322.

[224] W. Weixian, C. Ping, P. Mingyu, L. Xianglong, L. Zhuoqun, and H. Ruixin, “Design of Collaborative Control Scheme between On-chain and Off-chain Power Data,” in *2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, Sep. 2021, pp. 1–6, doi: 10.1109/ICISCAE52414.2021.9590719.

[225] J. Park, H. Kim, G. Kim, and J. Ryou, “Smart contract data feed framework for privacy-preserving oracle system on blockchain,” *Computers*, vol. 10, no. 1, pp. 1–12, 2021, doi: 10.3390/computers10010007.

[226] L. Chen, R. Yuan, and Y. Xia, “Tora: A Trusted Blockchain Oracle Based on a Decentralized TEE Network,” *2021 IEEE Int. Conf. Jt. Cloud Comput.*, pp. 28–33, Aug. 2021, doi: 10.1109/JCC53141.2021.00016.

[227] H. Wang, C. Guo, and S. Cheng, “LoC — A new financial loan management system based on smart contracts,” *Futur. Gener. Comput. Syst.*, vol. 100, pp. 648–655, 2019, doi: 10.1016/j.future.2019.05.040.

[228] S. Tucci-Piergiovanni, “Invited Paper: On the Characterization of Blockchain Consensus Under Incentives,” in *Lecture Notes in Computer Science (including subseries Lecture*

Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, vol. 11914 LNCS, pp. 1–15, doi: 10.1007/978-3-030-34992-9_1.

[229] N. Mhaisen, N. Fetais, A. Erbad, A. Mohamed, and M. Guizani, "To chain or not to chain: A reinforcement learning approach for blockchain-enabled IoT monitoring applications," *Futur. Gener. Comput. Syst.*, vol. 111, pp. 39–51, 2020, doi: 10.1016/j.future.2020.04.035.

[230] W.-T. Tsai, W. Xiang, R. Wang, and E. Deng, *LSO: A Dynamic and Scalable Blockchain Structuring Framework*, vol. 1385 CCIS. 2021.

[231] H. Roussille, Ö. Gürcan, and F. Michel, "AGR4BS: A Generic Multi-Agent Organizational Model for Blockchain Systems," *Big Data Cogn. Comput. 2022, Vol. 6, Page 1*, vol. 6, no. 1, p. 1, Dec. 2021, doi: 10.3390/BDCC6010001.

[232] B. Grooteman and T. U. Eindhoven, "Providing Trusted Datafeeds to the Blockchain," 2019.

[233] H. Ritzdorf, K. Wust, A. Gervais, G. Felley, and S. Capkun, "TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing," 2018, doi: 10.14722/ndss.2018.23272.

[234] X. Liu, K. Muhammad, J. Lloret, Y.-W. Chen, and S.-M. Yuan, "Elastic and cost-effective data carrier architecture for smart contract in blockchain," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 590–599, 2019, doi: 10.1016/j.future.2019.05.042.

[235] J. Heiss, J. Eberhardt, and S. Tai, "From oracles to trustworthy data on-chaining systems," in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, 2019, pp. 496–503, doi: 10.1109/Blockchain.2019.00075.

[236] H. Abusalah, J. Alwen, B. Cohen, D. Khilko, K. Pietrzak, and L. Reyzin, *Beyond hellman's time-memory trade-offs with applications to proofs of space*, vol. 10625 LNCS. 2017.

[237] X. Liu and J. Feng, "Trusted Blockchain Oracle Scheme Based on Aggregate Signature," *J. Comput. Commun.*, vol. 09, no. 03, pp. 95–109, 2021, doi: 10.4236/jcc.2021.93007.

[238] Y. Wang, H. Liu, J. Wang, and S. Wang, "Efficient data interaction of blockchain smart contract with oracle mechanism," 2020, pp. 1000–1003, doi: 10.1109/ITAIC49862.2020.9338784.

[239] N. S. Patel, P. Bhattacharya, S. B. Patel, S. Tanwar, N. Kumar, and H. Song, "Blockchain-envisioned trusted random oracles for IoT-enabled Probabilistic Smart Contracts," *IEEE Internet Things J.*, 2021, doi: 10.1109/JIOT.2021.3072293.

[240] B. Adams and M. Tomko, "A critical look at cryptogovernance of the real world: Challenges for spatial representation and uncertainty on the blockchain," in *Leibniz International Proceedings in Informatics, LIPIcs*, 2018, vol. 114, doi: 10.4230/LIPIcs.GIScience.2018.18.

[241] M. Merlini, N. Veira, R. Berryhill, and A. Veneris, "On Public Decentralized Ledger Oracles via a Paired-Question Protocol," in *ICBC 2019 - IEEE International Conference on*

Blockchain and Cryptocurrency, 2019, pp. 337–344, doi: 10.1109/BLOC.2019.8751484.

[242] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," *Comput. Electr. Eng.*, vol. 83, p. 106582, May 2020, doi: 10.1016/j.compeleceng.2020.106582.

[243] D. Basile, V. Goretti, C. Di Ciccio, and S. Kirrane, "Enhancing Blockchain-Based Processes with Decentralized Oracles," vol. 1, pp. 102–118, 2021, doi: 10.1007/978-3-030-85867-4_8.

[244] V. Goyal, J. Raizes, and P. Soni, "Time-Traveling Simulators Using Blockchains and Their Applications."

[245] J. Ellul and G. J. Pace, "Towards External Calls for Blockchain and Distributed Ledger Technology Towards External Calls for Blockchain and Distributed Ledger Technology," 2021. doi: 10.13140/RG.2.2.34630.60482.

[246] F. Bruschi, V. Rana, A. Pagani, and D. Sciuto, "Tunneling Trust into the Blockchain: A Merkle Based Proof System for Structured Documents," *IEEE Access*, vol. 9, pp. 103758–103771, 2021, doi: 10.1109/ACCESS.2020.3028498.

[247] S. Simunic, D. Bernaca, and K. Lenac, "Verifiable Computing Applications in Blockchain," *IEEE Access*, vol. 9, pp. 156729–156745, 2021, doi: 10.1109/ACCESS.2021.3129314.

[248] K. Chatterjee, A. K. Goharshady, and A. Pourdamghani, "Probabilistic smart contracts: Secure randomness on the blockchain," in *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, 2019, pp. 403–412, doi: 10.1109/BLOC.2019.8751326.

[249] U. Gallersdorfer and F. Matthes, "Towards Valid Use Cases: Requirements and Supporting Characteristics of Proper Blockchain Applications," in *2020 7th International Conference on Software Defined Systems, SDS 2020*, 2020, pp. 202–207, doi: 10.1109/SDS49854.2020.9143999.

[250] N. Truong, G. M. Lee, K. Sun, F. Guitton, and Y. K. Guo, "A blockchain-based trust system for decentralised applications: When trustless needs trust," *Futur. Gener. Comput. Syst.*, vol. 124, pp. 68–79, Nov. 2021, doi: 10.1016/J.FUTURE.2021.05.025.

[251] Z. Motaqy, G. Almashaqbeh, B. Bahrak, and N. Yazdani, "Bet and Attack: Incentive Compatible Collaborative Attacks Using Smart Contracts," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13061 LNCS, pp. 293–313, 2021, doi: 10.1007/978-3-030-90370-1_16.

[252] S. Wang, H. Lu, X. Sun, Y. Yuan, and F.-Y. Wang, "A Novel Blockchain Oracle Implementation Scheme Based on Application Specific Knowledge Engines," in *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, Henan Province, China, 11–13 October 2019; IEEE: Piscataway, NJ, USA*, Nov. 2019, vol. 2, pp. 258–262, doi: 10.1109/SOLI48380.2019.8955107.

[253] S. Wang and X. Yu, "Research on Trusted Identification of Blockchain Uploaded Data,"

Proc. 2020 IEEE Int. Conf. Artif. Intell. Comput. Appl. ICAICA 2020, pp. 1036–1044, 2020, doi: 10.1109/ICAICA50127.2020.9181948.

[254] B. Van Der Laan, O. Ersoy, and Z. Erkin, “Muscle: Authenticated external data retrieval from multiple sources for smart contracts,” in *Proceedings of the ACM Symposium on Applied Computing*, 2019, vol. Part F1477, pp. 382–391, doi: 10.1145/3297280.3297320.

[255] W. George and C. Lesaege, “A smart contract oracle for approximating real-world, real number values,” in *OpenAccess Series in Informatics*, 2020, vol. 71, doi: 10.4230/OASIcs.Tokenomics.2019.6.

[256] L. Ma, K. Kaneko, S. Sharma, and K. Sakurai, “Reliable decentralized oracle with mechanisms for verification and disputation,” in *Proceedings - 2019 7th International Symposium on Computing and Networking Workshops, CANDARW 2019*, 2019, pp. 346–352, doi: 10.1109/CANDARW.2019.00067.

[257] Y.-J. Chen, J.-L. Wu, Y.-C. Hsieh, and C.-W. Hsueh, “An oracle-based on-chain privacy,” *Computers*, vol. 9, no. 3, pp. 1–15, 2020, doi: 10.3390/computers9030069.

[258] S. Woo, J. Song, and S. Park, “A distributed oracle using intel SGX for blockchain-based IoT applications,” *Sensors (Switzerland)*, vol. 20, no. 9, 2020, doi: 10.3390/s20092725.

[259] N. Goel, C. van Schreven, A. Filos-Ratsikas, and B. Faltings, “Infochain: A Decentralized, Trustless and Transparent Oracle on Blockchain,” in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence*, Jul. 2020, vol. 2021-Janua, pp. 4604–4610, doi: 10.24963/ijcai.2020/635.

[260] M. Muller, S. Rodriguez Garzon, and A. Kupper, “COST: A Consensus-Based Oracle Protocol for the Secure Trade of Digital Goods,” *Proc. - 2020 IEEE Int. Conf. Decentralized Appl. Infrastructures, DAPPS 2020*, pp. 72–81, 2020, doi: 10.1109/DAPPS49028.2020.00008.

[261] P. Sheng, B. Xue, S. Kannan, and P. Viswanath, “ACeD: Scalable Data Availability Oracle,” pp. 1–33, 2020, [Online]. Available: http://arxiv.org/abs/2011.00102.

[262] Y. Cai, G. Fragkos, E. E. Tsiropoulou, and A. Veneris, “A Truth-Inducing Sybil Resistant Decentralized Blockchain Oracle,” in *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*, 2020, pp. 128–135, doi: 10.1109/BRAINS49436.2020.9223272.

[263] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, “Astraea: A Decentralized Blockchain Oracle,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1145–1152, doi: 10.1109/Cybermatics_2018.2018.00207.

[264] K. Nelaturu *et al.*, “On Public Crowdsource-Based Mechanisms for a Decentralized Blockchain Oracle,” *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1444–1458, Nov. 2020, doi: 10.1109/TEM.2020.2993673.

[265] Y. Cai, | Nafis Irtija, | Eirini, E. Tsiropoulou, A. Veneris, and E. E. Tsiropoulou, “Truthful Decentralized Blockchain Oracles,” 2021, doi: 10.1002/nem.2179.

[266] M. Sober, G. Scaffino, C. Spanring, and S. Schulte, “A Voting-Based Blockchain Interoperability Oracle,” pp. 160–169, Jan. 2022, doi: 10.1109/BLOCKCHAIN53845.2021.00030.

[267] M. S. Chishti, F. Sufyan, and A. Banerjee, “Decentralized On-Chain Data Access via Smart Contracts in Ethereum Blockchain,” *IEEE Trans. Netw. Serv. Manag.*, 2021, doi: 10.1109/TNSM.2021.3120912.

[268] J. Ducrée, “Digital Twin: An Oracle for Efficient Crowdsourcing of Research & Technology Development through Blockchain,” Oct. 2021, doi: 10.20944/PREPRINTS202110.0148.V1.

[269] S. Chen, J. Zhu, Z. Lin, J. Huang, and Y. Tang, “How to Make Smart Contract Smarter,” *Commun. Comput. Inf. Sci.*, vol. 1330 CCIS, pp. 705–713, 2021, doi: 10.1007/978-981-16-2540-4_54/FIGURES/3.

[270] F. Mohsin, X. Zhao, Z. Hong, G. de Mel, L. Xia, and O. Seneviratne, “Ontology aided smart contract execution for unexpected situations,” in *CEUR Workshop Proceedings*, 2019, vol. 2599.

[271] B. Berger, S. Huber, and S. Pfeifhofer, “OraclesLink: An architecture for secure oracle usage,” in *2020 2nd International Conference on Blockchain Computing and Applications, BCCA 2020*, 2020, pp. 66–72, doi: 10.1109/BCCA50787.2020.9274455.

[272] F. Adamik and S. Kosta, “SmartExchange: Decentralised Trustless Cryptocurrency Exchange,” in *Lecture Notes in Business Information Processing*, vol. 339, 2019, pp. 356–367.

[273] Y. Ji *et al.*, “SEBF: A single-chain based extension model of blockchain for fintech,” in *IJCAI International Joint Conference on Artificial Intelligence*, Jul. 2020, vol. 2021-Janua, pp. 4497–4505, doi: 10.24963/ijcai.2020/620.

[274] G. Antonio Pierro, H. Rocha, R. Tonelli, and S. Ducasse, “Are the Gas Prices Oracle Reliable? A Case Study using the EthGasStation,” in *IWBOSE 2020 - Proceedings of the 2020 IEEE 3rd International Workshop on Blockchain Oriented Software Engineering*, 2020, pp. 1–8, doi: 10.1109/IWBOSE50093.2020.9050186.

[275] S. Galanis, “No Trade in a Blockchain,” *SSRN Electron. J.*, pp. 1–13, 2020, doi: 10.2139/ssrn.3581822.

[276] L. Yu, M. Zichichi, R. Markovich, and A. Najjar, “Enhancing Trust in Trust Services: Towards an Intelligent Human-input-based Blockchain Oracle (IHiBO),” *Proc. 55th Hawaii Int. Conf. Syst. Sci.*, Jan. 2022, doi: 10.24251/HICSS.2022.712.

[277] M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, “Blockchain for explainable and trustworthy artificial intelligence,” *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 10, no. 1, pp. 1–13, 2020, doi: 10.1002/widm.1340.

[278] V. Lopes, N. Pereira, and L. A. Alexandre, “Robot workspace monitoring using a blockchain-based 3D vision approach,” in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2019, vol. 2019-June, pp. 2812–2820, doi: 10.1109/CVPRW.2019.00340.

[279] L. Yu, “Argumentation in Trust Services within a Blockchain Environment,” Accessed: Mar. 26, 2022. [Online]. Available: http://data.europa.eu/eli/dir/2011/61/oj.

[280] Y. Alowayed *et al.*, “Picking a Partner: A Fair Blockchain Based Scoring Protocol for Autonomous Systems,” 2018, doi: 10.1145/3232755.3232785.

[281] M. Autili, F. Gallo, P. Inverardi, C. Pompilio, and M. Tivoli, “Introducing trust in service-oriented distributed systems through blockchain,” *Proc. - 2019 IEEE 30th Int. Symp. Softw. Reliab. Eng. Work. ISSREW 2019*, pp. 149–154, 2019, doi: 10.1109/ISSREW.2019.00065.

[282] B. Adjei-Arthur *et al.*, “A blockchain-adaptive contractual approach for multi-contracting organizational entities,” *Futur. Gener. Comput. Syst.*, vol. 132, pp. 93–107, Jul. 2022, doi: 10.1016/J.FUTURE.2022.02.003.

[283] M. Hasan, K. Ogan, and B. Starly, “Hybrid Blockchain Architecture for Cloud Manufacturing-as-a-service (CMaaS) Platforms with Improved Data Storage and Transaction Efficiency,” *Procedia Manuf.*, vol. 53, pp. 594–605, Jan. 2021, doi: 10.1016/J.PROMFG.2021.06.060.

[284] C. Zhang, L. Zhu, C. Xu, and K. Sharif, “PRVB: Achieving Privacy-Preserving and Reliable Vehicular Crowdsensing via Blockchain Oracle,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 831–843, 2021, doi: 10.1109/TVT.2020.3046027.

[285] A. Fujihara, *Proposing a blockchain-based open data platform and its decentralized oracle*, vol. 1035. Springer International Publishing, 2020.

[286] V. Drungilas, E. Vaičiukynas, M. Jurgelaitis, R. Butkienė, and L. Čeponienė, “Towards blockchain-based federated machine learning: Smart contract for model inference,” *Appl. Sci.*, vol. 11, no. 3, pp. 1–21, 2021, doi: 10.3390/app11031010.

[287] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, “Blockchain for 5G: Opportunities and challenges,” 2019, doi: 10.1109/GCWkshps45667.2019.9024627.

[288] E. Anceaume, A. Del Pozzo, R. Ludinard, M. Potop-Butucaru, and S. Tucci-Piergiovanni, “Blockchain abstract data type,” *Annu. ACM Symp. Parallelism Algorithms Archit.*, pp. 349–358, 2019, doi: 10.1145/3323165.3323183.

[289] J. Zhao, Z. Lin, X. Huang, Y. Zhang, and S. Xiang, “TrustCA: Achieving Certificate Transparency through Smart Contract in Blockchain Platforms,” 2020, doi: 10.1109/HPBDIS49115.2020.9130581.

[290] H. Y. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee, and S. K. Lo, “Analysis of data management in blockchain-based systems: From architecture to governance,” *IEEE*

Access, vol. 7, pp. 186091–186107, 2019, doi: 10.1109/ACCESS.2019.2961404.

[291] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An Overview of Blockchain and 5G Networks," pp. 1–20, 2022, doi: 10.1007/978-3-030-77185-0_1.

[292] L. Y. Yeh, P. J. Lu, S. H. Huang, and J. L. Huang, "SOChain: A Privacy-Preserving DDoS Data Exchange Service over SOC Consortium Blockchain," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1487–1500, 2020, doi: 10.1109/TEM.2020.2976113.

[293] N. Mhaisen, N. Fetais, A. Erbad, A. Mohamed, and M. Guizani, "To chain or not to chain: A reinforcement learning approach for blockchain-enabled IoT monitoring applications," *Futur. Gener. Comput. Syst.*, vol. 111, pp. 39–51, Oct. 2020, doi: 10.1016/J.FUTURE.2020.04.035.

[294] M. Müller and S. R. Garzon, *Blockchain-Based Trusted Cross-organizational Deliveries of Sensor-Equipped Parcels*, vol. 11997 LNCS. 2020.

[295] M. Maier, "6G as if People Mattered: From Industry 4.0 toward Society 5.0 : aper)," in *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, Jul. 2021, vol. 2021-July, doi: 10.1109/ICCCN52240.2021.9522181.

[296] Y. Lin *et al.*, "A Novel Architecture Combining Oracle with Decentralized Learning for IIoT," *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2022.3150789.

[297] F. Raheman, T. Bhagat, A. Dayma, A. Raheman, and S. Anwar, "The Blockchain Paradox: Testing the DISC Hypothesis," *Int. J. Innov. Sci. Res. Technol.*, vol. 6, no. 7, 2021, Accessed: Mar. 26, 2022. [Online]. Available: https://angel.co/blockchains.

[298] N. Etemadi, P. Van Gelder, and F. Strozzi, "An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity," *Sustain.*, vol. 13, no. 9, 2021, doi: 10.3390/su13094672.

[299] R. Wasim Ahmad, H. Hasan, I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, "Blockchain for aerospace and defense: Opportunities and open research challenges," *Comput. Ind. Eng.*, vol. 151, 2021, doi: 10.1016/j.cie.2020.106982.

[300] A. Perego, D. Sciuto, V. Portale, and F. Bruschi, "Blockchain & Distributed Ledger," 2019. https://www.osservatori.net/it/ricerche/osservatori-attivi/blockchain-distributed-ledger (accessed Nov. 12, 2019).

[301] O. Bermeo-Almeida, M. Cardenas-Rodriguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas, and W. Bazán-Vera, "Blockchain in Agriculture: A Systematic Literature Review," *Commun. Comput. Inf. Sci.*, vol. 883, pp. 44–56, Nov. 2018, doi: 10.1007/978-3-030-00940-3_4.

[302] C. Xie, Y. Sun, and H. Luo, "Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking," *Proc. - 2017 3rd Int. Conf. Big Data Comput. Commun. BigCom 2017*, pp. 45–50, Nov. 2017, doi: 10.1109/BIGCOM.2017.43.

[303] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply

information security,” *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, vol. 2017-December, pp. 1357–1361, Feb. 2018, doi: 10.1109/IEEM.2017.8290114.

[304] K. Bradsher, “Wal-Marts in China City Closed for Pork Mislabeling - The New York Times,” *N.Y. Times*, 2011. https://www.nytimes.com/2011/10/11/business/global/wal-marts-in-china-city-closed-for-pork-mislabeling.html (accessed Oct. 19, 2021).

[305] S. Clemons, “China’s Latest Food Scandal: Fox-Tainted Donkey Meat - The Atlantic,” *The Atlantic*, 2014. https://www.theatlantic.com/international/archive/2014/01/chinas-latest-food-scandal-fox-tainted-donkey-meat/282776/ (accessed Oct. 19, 2021).

[306] M.-J. A *et al.*, “A Multistate Outbreak of Human Salmonella Agona Infections Associated With Consumption of Fresh, Whole Papayas Imported From Mexico-United States, 2011,” *Clin. Infect. Dis.*, vol. 66, no. 11, pp. 1756–1761, May 2018, doi: 10.1093/CID/CIX1094.

[307] H. Bottemiller, “IBM and China Team Up to Build Pork Traceability System - Food Safety News,” *Food Safety Network*, 2011. https://www.foodsafetynews.com/2011/12/ibm-and-china-team-up-to-build-pork-traceability-system/#.WZjWBCiGPIU (accessed Oct. 19, 2021).

[308] L. Mearin, “Q&A: Walmart’s Frank Yiannas on the use of blockchain for food safety | Computerworld,” *Computerworld*, 2018. https://www.computerworld.com/article/3309656/qa-walmarts-frank-yiannas-on-the-use-of-blockchain-for-food-safety.html (accessed Oct. 19, 2021).

[309] M. Corkery and N. Popper, “From Farm to Blockchain: Walmart Tracks Its Lettuce - The New York Times,” *N.Y. Times*, 2018. https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html (accessed Oct. 19, 2021).

[310] T. Tiwari, “PROFIT ALERT: Walmart is adopting the blockchain right now... | Palm Beach Research Group,” *Palm Beach Research Group*, 2016. https://www.palmbeachgroup.com/palm-beach-daily/profit-alert-walmart-is-adopting-the-blockchain-right-now/ (accessed Oct. 19, 2021).

[311] L. Burkitt, “Wal-Mart to Triple Spending on Food-Safety in China - WSJ,” *N.Y. Times*, 2017. https://www.wsj.com/articles/wal-mart-to-triple-spending-on-food-safety-in-china-1402991720 (accessed Oct. 19, 2021).

[312] W. Duberstein, “My Interview With IBM’s Vice President of Blockchain Technologies, Jerry Cuomo -- Part 1 | The Motley Fool,” *The Motley Fool*, 2018. https://www.fool.com/investing/2018/01/07/my-interview-ibms-vice-president-of-blockchain.aspx (accessed Oct. 20, 2021).

[313] Federalimentare, “Report conclusivo Federalimentare 2018,” *Federalimentare*, 2018. http://www.federalimentare.it/new2016/Comunicazione/ComunicatiStampa.asp?Anno=2018 (accessed Jun. 12, 2019).

[314] C. Fisch, "Initial coin offerings (ICOs) to finance new ventures," *J. Bus. Ventur.*, vol. 34, no. 1, pp. 1–22, 2019, doi: 10.1016/j.jbusvent.2018.09.007.

[315] A. Zharova and I. Lloyd, "An examination of the experience of cryptocurrency use in Russia. In search of better practice," *Comput. Law Secur. Rev.*, vol. 34, no. 6, pp. 1300–1313, 2018, doi: 10.1016/j.clsr.2018.09.004.

[316] J. Davis, "A discussion of the oracle problem | Hacker Noon," *Hackernoon*, 2019. https://hackernoon.com/a-discussion-of-the-oracle-problem-6cbec7872c10 (accessed Oct. 21, 2021).

[317] P. A. Lyons and R. E. Kahn, "Blocks as digital entities: A standards perspective," *Inf. Serv. Use*, vol. 38, no. 3, pp. 173–185, 2018, doi: 10.3233/ISU-180021.

[318] A. H. Gold, A. Malhotra, and A. H. Segars, "Knowledge management: An organizational capabilities perspective," *J. Manag. Inf. Syst. Summer*, vol. 18, 2001.

[319] J. Mendling *et al.*, "Blockchains for business process management - Challenges and opportunities," *ACM Trans. Manag. Inf. Syst.*, vol. 9, no. 1, 2018, doi: 10.1145/3183367.

[320] P. Godsiff, "Distributed ledger technology: Beyond block chain," 2016. Accessed: Oct. 21, 2021. [Online]. Available: https://youtu.be/4sm5LNqL5j0.

[321] D. Schatsky and C. Muraskin, "Beyond bitcoin: Blockchain is coming to disrupt your industry | Deloitte Insights," *Deloitte. Insights*, 2018. https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html (accessed Oct. 21, 2021).

[322] D. He *et al.*, "Virtual Currencies and Beyond: Initial Considerations INTERNATIONAL MONETARY FUND Monetary and Capital Markets, Legal, and Strategy and Policy Review Departments Virtual Currencies and Beyond: Initial Considerations Authorized for distribution by The IMF staff team comprised Dong He," 2016.

[323] V. Buterin, "On Public and Private Blockchains | Ethereum Foundation Blog," *Ethereum Foundation Blog*, 2015. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed Oct. 21, 2021).

[324] F. Gao, M. Meng, and S. Clarke, "Knowledge, management, and knowledge management in business operations," *J. Knowl. Manag.*, vol. 12, no. 2, pp. 3–17, Apr. 2008, doi: 10.1108/13673270810859479.

[325] M. Al-Lozi, " Total Quality Management in the Civil Service institutions in Jordan," *Preprint*, 2003. https://www.researchgate.net/publication/276882667_Total_Quality_Management_in_the_Civil_Service_institutions_in_Jordan (accessed Oct. 21, 2021).

[326] S. K. Singh, "Role of leadership in knowledge management: a study," *J. Knowl. Manag.*, vol. 12, no. 4, pp. 3–15, Jul. 2008, doi: 10.1108/13673270810884219.

[327] N. H. J. AL-Syaidh, D. R. (Moh'd T. Masa'deh, P. M. Al-Lozi, and J. S. AlHarrasi,

"Transformational Leadership and its Role on the Effectiveness of Employees' Behavior: A Theoretical Study," *J. Bus. Manag.*, vol. 4, no. 1, pp. 14–35, 2016, Accessed: Oct. 21, 2021. [Online]. Available: https://ideas.repec.org/a/jso/coejbm/v4y2016i1p14-35.html.

[328] N. H. J. AL-Syaidh, R. (Moh'd T. Masa'deh, and Z. Al-zu'bi, "Transformational Leadership and its Impact on the Effectiveness of Employees' Behavior in the Public and Private Jordanian Hospitals," *Jordan J. Bus. Adm.*, vol. 11, no. 1, Feb. 2015, Accessed: Oct. 21, 2021. [Online]. Available: https://journals.ju.edu.jo/JJBA/article/view/8345.

[329] S. Rateb Mahmoud Darawsheh, A. Soud ALshaar, ed Moh, T. Masa, M. Al-Lozi, and A. Professor of Management, "The degree of heads of departments at the University of Dammam to practice transformational leadership style from the point of view of the faculty members," *J. Soc. Sci.*, vol. 5, no. 1, pp. 56–79, 2016, Accessed: Oct. 21, 2021. [Online]. Available: http://centreofexcellence.net/J/JSS/JSS Mainpage.htm.

[330] D. Gharakhani and M. Mousakhani, "Knowledge management capabilities and SMEs' organizational performance," *J. Chinese Entrep.*, vol. 4, no. 1, pp. 35–49, Feb. 2012, doi: 10.1108/17561391211200920.

[331] T. Cho, "Knowledge management capabilities and organizational performance: an investigation into the effects of knowledge infrastructure and processes on organizational performance," 2011, Accessed: Oct. 21, 2021. [Online]. Available: https://www.ideals.illinois.edu/handle/2142/24182.

[332] J. S. Denford, "Building knowledge: developing a knowledge-based dynamic capabilities typology," *J. Knowl. Manag.*, vol. 17, no. 2, pp. 175–194, Mar. 2013, doi: 10.1108/13673271311315150.

[333] T. A. Smith, "Knowledge Management and its Capabilities Linked to the Business Strategy for Organizational Effectiveness," Nova Southeastern University, 2006.

[334] P. Kushwaha and M. K. Rao, "Integrative role of KM infrastructure and KM strategy to enhance individual competence: Conceptualizing knowledge process enablement," *VINE*, vol. 45, no. 3, pp. 376–396, Aug. 2015, doi: 10.1108/VINE-02-2014-0014.

[335] R. Masa'deh and R. Masa'deh, "The Role of Knowledge Management Infrastructure in Enhancing Job Satisfaction at Aqaba Five Star Hotels in Jordan," *Commun. Netw.*, vol. 8, no. 4, pp. 219–240, Sep. 2016, doi: 10.4236/CN.2016.84021.

[336] Y. J. Yeh, S. Q. Lai, and C. T. Ho, "Knowledge management enablers: a case study," *Ind. Manag. & Data Syst.*, vol. 106, no. 6, pp. 793–810, 2006, doi: 10.1108/02635570610671489.

[337] B. S. Sandhawalia and D. Dalcher, "Developing knowledge management capabilities: a structured approach," *J. Knowl. Manag.*, vol. 15, no. 2, pp. 313–328, Apr. 2011, doi: 10.1108/13673271111119718.

[338] R. O. Shannak, B. Y. Obeidat, and R. M. Masadeh, "Culture and the Implementation Process of Strategic Decisions in Jordan," *J. Manag. Res.*, vol. 4, no. 4, pp. 257–281, Sep.

2012, doi: 10.5296/JMR.V4I4.2160.

[339] J. B. Barney and M. H. Hansen, “Trustworthiness as a Source of Competitive Advantage,” *Manag. J. , Winter*, vol. 15, pp. 175–190, 1994.

[340] O. E. Williamson, “Markets and Hierarchies: Some Elementary Considerations,” *Source Am. Econ. Rev.*, vol. 63, no. 2, pp. 316–325, 1973.

[341] O. E. Williamson, *The Economic Intstitutions of Capitalism*. Simon and Schuster, 1985.

[342] R. Dore, “Goodwill and the Spirit of Market Capitalism,” *Source Br. J. Sociol.*, vol. 34, no. 4, pp. 459–482, 1983.

[343] M. Law Review, “Michigan Law Review Michigan Law Review The New Social Contract: An Inquiry into Modern Contractual The New Social Contract: An Inquiry into Modern Contractual Relations Relations Michigan Law Review,” Accessed: Oct. 21, 2021. [Online]. Available: https://repository.law.umich.edu/mlrhttps://repository.law.umich.edu/mlr/vol79/iss4/28.

[344] A. Zaheer and N. Venkatraman, “Relational Governance as an Interorganizational Strategy: An Empirical Test of the Role of Trust in Economic Exchange,” *Manag. J.*, vol. 16, no. 5, pp. 373–392, 1995.

[345] Y.-P. Lin *et al.*, “Blockchain: The Evolutionary Next Step for ICT E-Agriculture,” *Environments*, vol. 4, no. 3, p. 50, Jul. 2017, doi: 10.3390/environments4030050.

[346] K. Biswas, V. Muthukkumarasamy, and W. L. Tan, “Blockchain based Wine Supply Chain Traceability System,” 2017.

[347] W. (Derek) Du, S. L. Pan, D. E. Leidner, and W. Ying, “Affordances, experimentation and actualization of FinTech: A blockchain implementation study,” *J. Strateg. Inf. Syst.*, vol. 28, no. 1, pp. 50–65, Mar. 2019, doi: 10.1016/J.JSIS.2018.10.002.

[348] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” *2016 13th Int. Conf. Serv. Syst. Serv. Manag. ICSSSM 2016*, Aug. 2016, doi: 10.1109/ICSSSM.2016.7538424.

[349] . S. A. A., “BLOCKCHAIN READY MANUFACTURING SUPPLY CHAIN USING DISTRIBUTED LEDGER,” *Int. J. Res. Eng. Technol.*, vol. 05, no. 09, pp. 1–10, Sep. 2016, doi: 10.15623/IJRET.2016.0509001.

[350] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, “Blockchain-based traceability in Agri-Food supply chain management: A practical implementation,” in *2018 {IoT} {Vertical} and {Topical} {Summit} on {Agriculture} - {Tuscany} ({IOT} {Tuscany})*, May 2018, pp. 1–4, doi: 10.1109/IOT-TUSCANY.2018.8373021.

[351] D. A. Almajali and M. Al-Lozi, “Reviewing the Literature of The associations among Knowledge Management, Knowledge Management Infrastructure, and Job Satisfaction,” *J. Bus. Manag.*, vol. 7, no. 1, pp. 1–15, 2019, doi: 10.25255/jbm.2019.7.1.1.15.

[352] G. Zhao *et al.*, “Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions,” *Comput. Ind.*, vol. 109, pp. 83–99, Aug. 2019, doi: 10.1016/j.compind.2019.04.002.

[353] Z. Zhao, F. Meng, Y. He, and Z. Gu, “The Influence of Corporate Social Responsibility on Competitive Advantage with Multiple Mediations from Social Capital and Dynamic Capabilities,” *Sustain. 2019, Vol. 11, Page 218*, vol. 11, no. 1, p. 218, Jan. 2019, doi: 10.3390/SU11010218.

[354] A. M. Pettigrew, “LONGITUDINAL FIELD RESEARCH ON CHANGE: THEORY AND PRACTICE*,” *Organ. Sci.*, vol. 1, no. 3, 1990, Accessed: Oct. 21, 2021. [Online]. Available: https://about.jstor.org/terms.

[355] R. A. Burgelman, “A Process Model of Internal Corporate Venturing in the Diversified Major Firm,” *Quarterly*, vol. 28, no. 2, pp. 223–244, 1983.

[356] S. G. Harris and R. I. Sutton, “Functions of Parting Ceremonies in Dying Organizations,” *Source Acad. Manag. J.*, vol. 29, no. 1, pp. 5–30, 1986, Accessed: Oct. 21, 2021. [Online]. Available: https://about.jstor.org/terms.

[357] R. I. Sutton and A. L. Callahan, “The Stigma of Bankruptcy: Spoiled Organizational Image and Its Management,” *Source Acad. Manag. J.*, vol. 30, no. 3, pp. 405–436, 1987, Accessed: Oct. 21, 2021. [Online]. Available: https://www.jstor.org/stable/256007.

[358] D. Leonard-Barton, “A Dual Methodology for Case Studies: Synergistic Use of a Longitudinal Single Site with Replicated Multiple Sites,” *Organ. Sci.*, vol. 1, no. 3, pp. 248–266, 1990, Accessed: Oct. 21, 2021. [Online]. Available: https://about.jstor.org/terms.

[359] J. Saldaña, *The Coding Manual for Qualitative Researchers*. Sage Publications Ltd, 2015.

[360] V. G. Venkatesh, K. Kang, B. Wang, R. Y. Zhong, and A. Zhang, “System architecture for blockchain based transparency of supply chain social sustainability,” *Robot. Comput. Integr. Manuf.*, vol. 63, p. 101896, Jun. 2020, doi: 10.1016/j.rcim.2019.101896.

[361] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, “BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS,” p. 15, 2016.

[362] F. Hawlitschek, B. Notheisen, and T. Teubner, “The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy,” *Electron. Commer. Res. Appl.*, vol. 29, pp. 50–63, 2018, doi: 10.1016/j.elerap.2018.03.005.

[363] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, “Untrusted Business Process Monitoring and Execution Using Blockchain,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9850 LNCS, pp. 329–347, 2016, doi: 10.1007/978-3-319-45348-4_19.

[364] S. Fosso Wamba, J. R. Kala Kamdjoug, R. Epie Bawack, and J. G. Keogh, “Bitcoin, Blockchain and Fintech: a systematic review and case studies in the supply chain,” *Prod. Plan. Control*, vol. 31, no. 2–3, pp. 115–142, 2020, doi: 10.1080/09537287.2019.1631460.

[365] A. Ramachandran and D. M. Kantarcioglu, “Using Blockchain and smart contracts for secure data provenance management,” *arXiv1709.10000 [cs]*, Sep. 2017, Accessed: Feb. 11, 2020. [Online]. Available: http://arxiv.org/abs/1709.10000.