information

Review

Smart Contracts in Blockchain Technology: A Critical Review

Hamed Taherdoost

Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B, Canada; hamed.taherdoost@gmail.com; Tel.: +1-236-889-5359

Abstract: By utilizing smart contracts, which are essentially scripts that are anchored in a decentralized manner on blockchains or other similar infrastructures, it is possible to make the execution of predetermined procedures visible to the outside world. The programmability of previously unrealized assets, such as money, and the automation of previously manual business logic are both made possible by smart contracts. This revelation inspired us to analyze smart contracts in blockchain technologies written in English between 2012 and 2022. The scope of research is limited to the journal. Reviews, conferences, book chapters, theses, monographs, and interview-based works, and also articles in the press, are eliminated. This review comprises 252 articles over the last ten years with "Blockchain", "block-chain", "smart contracts", and "smart contracts" as keywords. This paper discusses smart contracts' present status and significance in blockchain technology. The gaps and challenges in the relevant literature have also been discussed, particularly emphasizing the limitations. Based on these findings, several research problems and prospective research routes for future study that will likely be valuable to academics and professionals are identified.

Keywords: smart contracts; blockchain; technology

Citation: Taherdoost, H. Smart Contracts in Blockchain Technology: A Critical Review. *Information* **2023**, *14*, 117. https://doi.org/10.3390/info14020117

Academic Editors: Soumya Banerjee and Samia Bouzefrane

Received: 7 December 2022
Revised: 31 January 2023
Accepted: 10 February 2023
Published: 13 February 2023

1. Introduction

The blockchain has been around for over a decade as a proven technology for recording transactions in a decentralized, peer-to-peer network using a distributed database [1,2]. It is considered a distributed computing paradigm that solves the confidence in a single entity problem. Therefore, several nodes work together in a blockchain network to securely and reliably maintain a distributed ledger of all past transactions. Satoshi Nakamoto launched Bitcoin in 2008 [3], which was the first suggested cryptocurrency to present the blockchain as a distributed infrastructure platform. It made it possible for anyone to send and receive bitcoins, a kind of cryptocurrency, without needing to depend on any central authority. Other blockchain-based systems have also been suggested for usage with the coin, including Hyperledger Fabric [4] and Ethereum [5]. The usage of smart contracts is possible, unlike with Bitcoin. With smart contracts, blockchain technology may go beyond conventional contracts by automatically carrying out the terms of agreements between two or more people in a decentralized setting once the necessary circumstances have been satisfied [6].

As blockchain has developed, smart contracts have become more popular [7,8]. A smart contract is a piece of cutting-edge technology that may be used in a blockchain ecosystem to mechanically negotiate, carry out, and enforce the conditions of a legally binding agreement [9]. Reduced risk, lower service, and lower administration costs, and enhanced business process efficiency are some of the benefits of smart contracts over standard contracts [10]. More crucially, smart contracts may build confidence between parties in no-trust contracting contexts [11]. In this respect, it will revolutionize established ways of doing business [12].

Distributed ledger technology (blockchain) and smart contracts have many potential uses outside of the financial sector, including in insurance claims processing, supply chain management, and IP enforcement. The use of smart contracts and blockchain applications

among businesses shows no signs of slowing down. Blockchain applications, however, must be carefully crafted and rigorously tested to meet stringent security, scalability, and performance standards. This is particularly the case when the non-standard software life cycles used in the development of smart contracts are considered, which makes it difficult to update or fix flaws in deployed apps by releasing an updated version of the program [13]. Smart contract creation is very different from more conventional forms of software engineering, and as such has its own unique set of difficulties [14,15]. For example, developers must guarantee code safety for smart contracts because of the immutability of blockchain and the sensitive nature of digital information often managed, and they must pay close attention to gas consumption because the implementation of smart contracts in blockchain platforms, the same as Ethereum, is applied through the gas mechanism [16]. The product lifecycle and software development process of smart contracts and blockchain-based apps should consider the unique limits and features demanded by blockchain technology. It is necessary to identify and investigate all of these shifts in software products and processes to build a complete body of knowledge based on blockchain software engineering.

Despite the growing interest in smart contracts and the research proposals made to address some of these problems, the solutions that have been put forth are not yet unified. For this reason, it is important to determine whether software engineering methods, methodologies, best practices, and testing strategies have been tailored to accommodate the unique aspects of blockchain-based decentralized application development [17]. Smart contracts have been the topic of several literature assessments, surveys, and reviews. Macrinici et al. [7] categorized 64 papers on smart contracts and concluded that the topics of discussion included smart contract scaling, and the security, privacy, and programmability of blockchains. Ante [18] summarized and analyzed the present state of the literature on smart contracts and identified intellectual structures and new trends. The study by Hewa et al. [19] looked at some of the important uses for smart contracts that have previously been successful. They emphasized the smart contracts built on blockchain's future potential from the standpoint of these applications. A technical and practical analysis of blockchain-enabled smart contracts was provided by Khan et al. [20]. They pointed out several difficulties and unresolved problems that need attention in the next research. This paper conducts a critical literature review of the blockchain and smart contracts' advancement, issues, and direction to fill this void and gain a clearer picture of the research efforts that have been made to enhance the execution, reliability, and security of this type of application. Furthermore, the aim is to pinpoint potential future research areas and unresolved concerns. The specific study questions are as follows:

- Research question 1 (RQ1): What is the present condition of the field of study?
- Research question 2 (RQ2): How significant are smart contracts in blockchain technology?
- Research question 3 (RQ3): What challenges do smart contracts in the blockchain often encounter?
- Research question 4 (RQ4): In what ways will smart contracts in the blockchain develop in the near future?

Here is how the current study is set up: Section 2 describes in full the research process used to find, filter, and select the literature. The third section reviews the literature on smart contracts in the blockchain, outlining the most cited works and analyzing their significance, as well as emphasizing some of the challenges that have been identified in this field. The section concludes with a consideration of upcoming trends. Finally, conclusions are discussed in the report's last section.

2. Background of the Study

Over the last decade, blockchain technology has emerged as a popular academic pursuit. A smart contract is a collection of tamper-resistant, self-executing, and self-verifying algorithms. Integrating blockchain technology into a smart contract makes it possible to complete a transaction in near real time at a lower cost and with a higher

level of security. The background of the blockchain and smart contracts is covered in the following sections:

2.1. Blockchain

The blockchain is described as the underlying technology of Bitcoin and other cryptocurrencies—a shared digital ledger or a continuously updated record of all transactions [21]. Blockchain may be considered both an economic and technological breakthrough [22]. It provides a solution to any issue requiring a trustworthy ledger in a decentralized setting where not all participants, whether human or computer, can be trusted completely [23]. The blockchain is a collection of cryptographic techniques and protocols used by a network of nodes that cooperate to accomplish the safe recording of data inside a distributed database that consists of encrypted blocks encapsulating the data [24].

There have been three major milestones in the evolution of blockchain technology so far: the use of digital money in the 1.0 stage, the use of smart contracts in the 2.0 stage, and the creation of programmable blockchains in the 3.0 stage [25]. In its present phase of development, blockchain is mostly employed for small-scale local applications; there are very few industry- or ecosystem-level uses for it. Nevertheless, the distinctive characteristics of blockchain have begun to extend across several sectors [26].

2.2. Smart Contracts

Smart contracts are a significant development in blockchain [27]. Smart contracts were first proposed in the 1990s as a digital transaction protocol to carry out the terms of an agreement [28]. Smart contracts are simply containers of code that encapsulate and replicate the terms of real-world contracts in the digital domain. Contracts are fundamentally a legally binding agreement between two or more parties, with each party committed to fulfilling its commitments. Importantly, the agreement must be enforceable by law, often via a centralized legal body (organization). Nevertheless, smart contracts replace trusted third parties or mediators between contracting parties. They make use of this with the assistance of code execution that is automatically disseminated and checked by network nodes in a decentralized blockchain. In addition, they allow transactions between untrusted parties without the necessity for direct contact between the parties, reliance on third parties, and intermediary commission costs [29].

Compared to conventional contracts, smart contracts offer the benefits of reducing transaction risk, reducing administration and service costs, and enhancing the efficiency of corporate processes, since they are often placed on and secured by blockchain [12]. Smart contracts are projected to give a superior solution to the present transaction mechanism in a variety of businesses in this regard.

3. Research Methodology

3.1. Planning the Review

The purpose of this research synthesis was to determine where smart contracts stand in the blockchain industry at the current time. This inquiry was carried out with the utmost seriousness by carefully reading all of the current applicable literature. The review process involves the use of structured research questions, databases, and procedures for identifying and assessing information. To provide a transparent evaluation of smart contracts in blockchain technology, certain features of the suggested reporting items for critical reviews were chosen. The overall strategy consists of the following major steps:

- Examining the present condition of the field.
- Recognizing the significance of the review.
- Determining the challenges and future directions of the field.
- An overview of the investigation's findings.

3.2. Research Strategy

A comprehensive evaluation of the literature requires an inclusive viewpoint. To maximize the chances of discovering highly relevant papers, an adequate selection of databases were selected before the search. During the review, the Scopus sources were checked.

3.3. Search Criteria

To guarantee that the material given here is exhaustive, relevant databases were thoroughly searched. However, not all classic literary works were incorporated into the search parameters for several reasons. Perhaps the search term was not included in the abstract, or the article had a very distinctive title. To accomplish the objective, a comprehensive literature search was conducted. Thus far, around 774 Scopus results have been evaluated (9 November 2022). Approximately 252 were considered to be relevant (Figure 1). The study domain and research questions influenced the search string creation. By searching "Blockchain" or "Block chain" AND "Smart contracts" or "Smart contract", the relevant material was located and obtained.

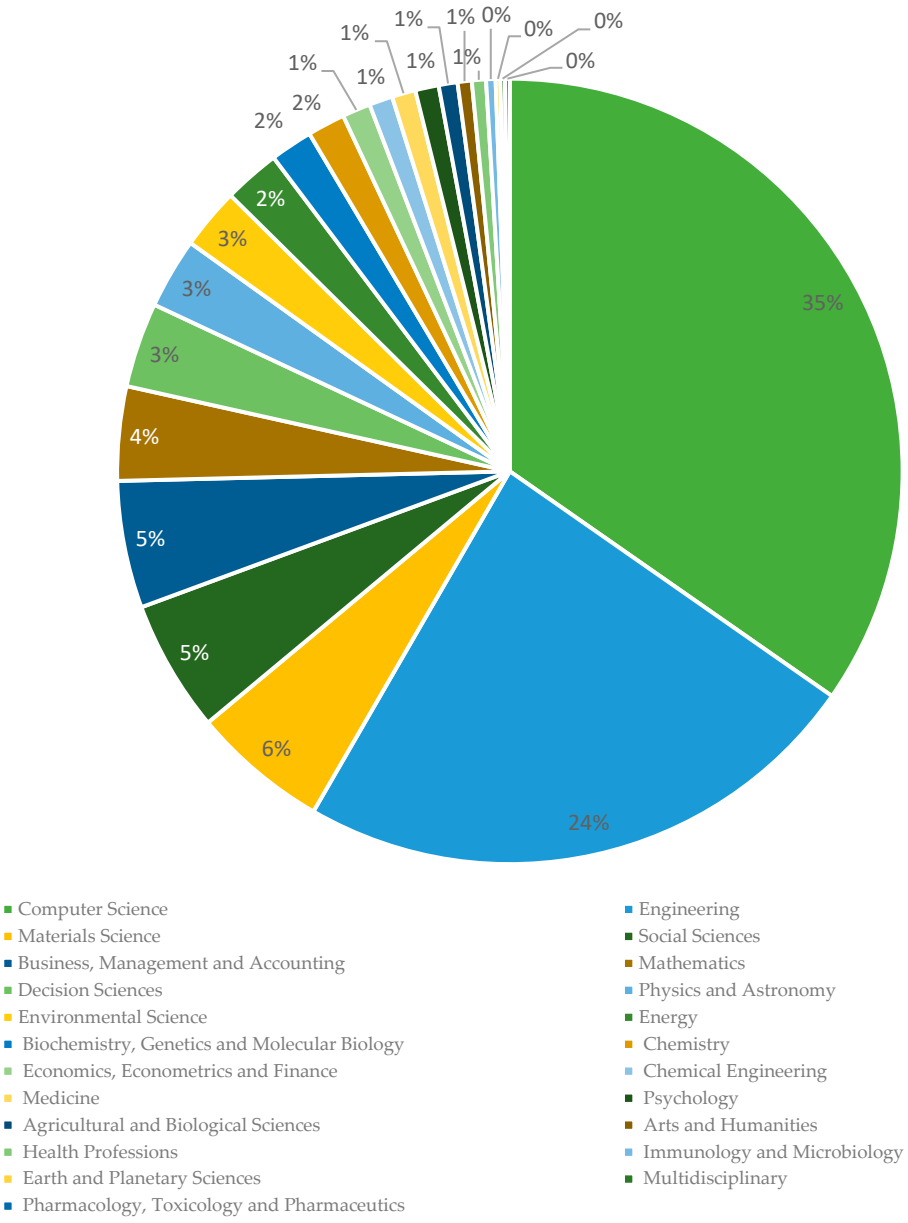

Figure 1. The number of articles on the topic published between 2012 and 2022.

- Inclusion Criteria (IC).
  1. Research may be released anytime between 2012 and 2022.
  2. The scope of research is limited to the journal.
  3. "Blockchain", "block-chain", "smart contracts", and "smart contracts" are the keywords.
- Exclusion Criteria (EC).
  1. Articles not written in English
  2. The exclusion of reviews, conferences, book chapters, theses, monographs, and interview-based works.
  3. Articles in the press are eliminated.

4. Results and Discussion

Below are the findings from responding to the research queries specified in the aforementioned critical review. This section presents blockchain technology and smart contracts and discusses the technology's foundations, variants, development teams, platforms, and consensus mechanisms. There is further discussion of the value of utilizing smart contracts in blockchain later in the review.

4.1. Selection Results

Out of the 774 items provided by this search, 522 were screened. There are 252 articles in this critical review. The articles in the press fulfilled the criterion for inclusion, but they were not considered for the 2012–2022 series. The list of selected papers with explanations of the overall categorization results is provided below.

RQ1: What is the present condition of the field of study?

This methodical investigation looks at the gathered descriptive information on the various articles published each year, the publication source, and the yearly average amount of citations that research papers obtain. This critical review's analysis of smart contracts in blockchain research publications published between 2012 and 2022 comes to a close. There are most publications on this topic in the IEEE Access journal (27 articles).

Figure 1 shows the number of articles generated per subject area from 2012 to 2022. Computer science (179 articles) and engineering are the primary topic areas (122 articles). Other subjects include Materials Science (29 articles), Social Sciences (28 articles), Business, Management, and Accounting (27 articles), Mathematics (20 articles), Decision Sciences (18 articles), Physics and Astronomy (15 articles), Environmental Science (13 articles), and Energy (12 articles), etc. Approximately 35% of research is in the field of computer science, specific to blockchain and smart contracts. This is the basis of blockchain and smart contracts. The next category is engineering (about 24%), which can, usefully, include all of these subjects.

Figure 2 displays the number of papers created each year between 2012 and 2022. There is no content available from 2012 to 2015. The year 2016 saw the publication of one article, while 2017 had no publications. Clearly, between 2018 and 2022, the number of articles increased. There were 12 articles published in 2018, 27 papers published in 2019, 52 papers in 2020, 86 papers in 2021, and 74 papers in 2022. The number of publications published has dramatically increased during the last ten years. This department reflects an interdisciplinary approach to the subject of smart contracts. There is a notable lack of research output in economics, which suggests that the discipline draws most of its basic research from engineering and legal scholars.

The percentage of authors by nationality is presented in Figure 3. China has the most authors. India and the United States follow. This may suggest that the scientists of these crowded countries are working together, i.e., co-authoring numerous publications.

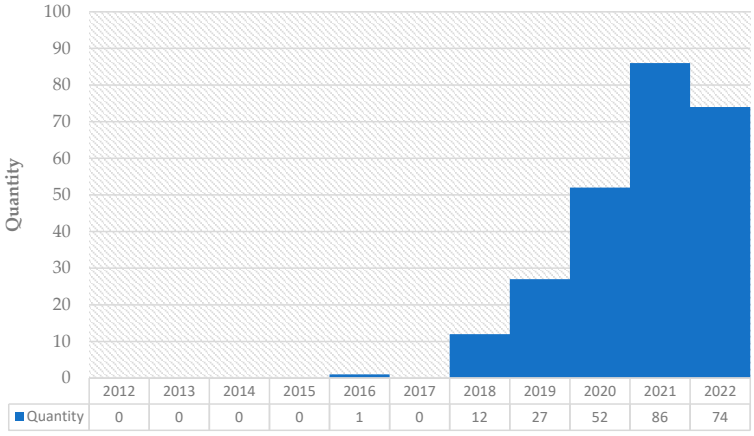

Figure 2. The yearly number of articles released between 2012 and 2022.

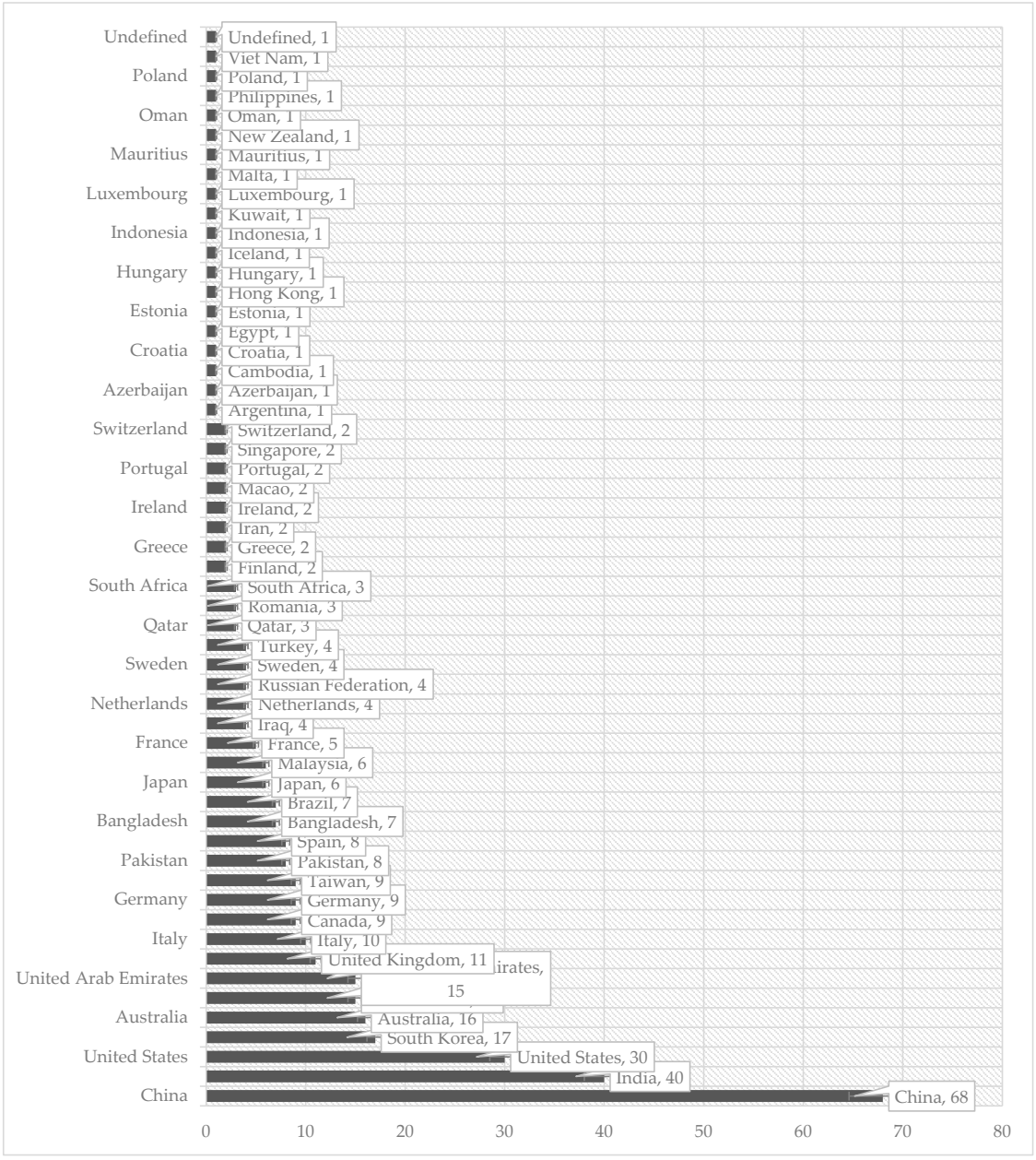

Figure 3. Distribution of authors by country.

RQ2: How significant are smart contracts in blockchain technology?

The name "smart contract" is deceptive since it implies a legally enforceable agreement, while, in reality, it is only stupid computer code. To put it accurately, Ethereum's creator said, "I quite regret choosing the phrase 'smart contracts'. Maybe I should have gone with a more dry and technical name, like 'persistent scripts'" [5]. Different levels of smart contracts' efficacy as legally enforceable contracts are distinguishable: A "smart contract" is described as "computer code that does not represent any legal contract but merely executes a predefined logic" in one definition, and as "a program with a predefined logic based on legal structures that are expected to act in a particular way" in another.

For the first time, blockchain technology provided an appropriate distributed infrastructure for the use of smart contracts by facilitating the safe p2p transfer of value across the internet between non-confidential parties. When the conditions are satisfied, the blockchain will run the code without anybody or anything being able to stop it. Since the underlying code can be seen by everyone with access to the blockchain, there is no longer a requirement to trust your counterparty. Due to the usage of a unified contract, there is no need for a third party to read the terms and conditions, and transactions may be processed instantly. Moreover, digital signatures reveal without a doubt the origin of the transactions that activated the smart contract.

Despite the numerous advantages and possibilities that smart contracts provide, they are not without their share of difficulties and threats. There is no way for a smart contract to initiate itself. It sleeps until a transaction occurs in which one of its tasks is invoked. As a result, smart contracts are never independent; something else (a transaction, for example) must occur for them to take effect. There is a problem with smart contract use cases that involves events and processing data that do not occur immediately on the blockchain. A smart contract's response to a blockchain transaction is instantaneous since the whole process takes place on-chain. However, if the necessary information, for instance, involves a guest checking out of a hotel room (off-chain), the script cannot automatically get these data. While the blockchain itself may be relied upon, the information transferred there may not be trusted by the parties to a smart contract. This is referred to as the "oracle issue" because it affects all people, programs, and devices that take part in these activities.

Since all nodes in a network need to keep a copy of the blockchain (and any attached computer code), the technique is inefficient in theory. Smart contracts on public blockchains are performed worldwide, at each node in the blockchain on each iteration. Because computing is a predictable process, it is likely that a global code rollout is not required [30]. The storing of all data by all network members also introduces the problem of data security. The stored data cannot be quickly erased, which goes against the provisions of laws such as the "right to be forgotten" [31,32].

In their simplest form, smart contracts are just blockchain-based computer programs that are activated when certain criteria are satisfied. Common applications include automating the execution of agreements so that all parties involved know the result without delay or third-party participation. They may also automate a process by causing one action to lead to another automatically.

Coded "when . . . then . . . " and "if" expressions on a blockchain are what make smart contracts tick. If, and only if, certain requirements are validated and satisfied, the activities are carried out via a network of computers. These measures may include transferring monies to the correct accounts, registering a vehicle, notifying relevant persons, or issuing a citation. Following this, the blockchain is updated to reflect the successful completion of the transaction. This implies that after the transaction is finalized, no changes can be made, and only those who have been given access to the data may see them.

To ensure that all parties are satisfied with the agreement's conclusion, a smart contract may include as many conditions as are required. Participants must agree on the representation of data and transactions on the blockchain, the "if/when . . . then . . . " rules that apply to transactions, the exceptions to those rules, and a structure for resolving disputes to set the terms. A developer may then code the smart contract, albeit a growing number of

blockchain-using businesses also provide web interfaces, templates, and other online tools to make smart contract construction more manageable.

4.2. Smart Contracts' Platforms

Expert blockchain developers are needed to help clients in identifying the optimal blockchain platform and method for developing and deploying smart contracts to their organization's needs. Different blockchain systems allow for the development and deployment of smart contracts (e.g., Ethereum, Hyperledger Fabric, NEM, STELLAR, Waves, and Corda). Because of its restricted scripting language and emphasis on security over programmability, Bitcoin was rarely mentioned when smart contracts were addressed. Bitcoin networks cannot support complex smart contracts. Furthermore, basic contracts that may be carried out on Bitcoin are often difficult to draft and expensive to carry out. For creating smart contracts, several platforms provide unique capabilities such as security levels, contract code execution, and contract programming languages. Some platforms enable the creation of smart contracts using high-level programming languages. Table 1 compiles a summary of the advantages and disadvantages of various platforms.

Table 1. Various platforms of smart contracts: pros and cons.

Platform	Advantages	Disadvantages
Ethereum	Access to various resources Clear rules for developers Solidity's own smart contract programming language Ethereum token standard Free setup	Many smart contracts are hackable due to poor-quality coding Costlier than other platforms Security problems with Ethereum code. Overloaded network
Hyperledger Fabric	Enabling plug-in components Dependable performance Allowing multi-language contract coding. Membership with permission Free and open-source	No token system
NEM	Outstanding performance Scalability Platform-independent programming language Simple to use	NEM employs non-blockchain coding, making it less decentralized. Less accessible tools Fewer developers than other platforms
STELLAR	Excellent performance Simple platform Highly respected in the business Cheaper than Ethereum	Unsuitable for sophisticated smart contract development
Waves	Suitable for crowd sales Token creation requires minimal basic knowledge	Non-versatile platform Still has a rather small user base
Corda	Long-term privacy protection Support for regulatory and supervisory nodes A wide range of industrial compatibilities Possibility of realistic contractual enforcement Support for various consensus mechanisms	Only verified by trustworthy notaries There is no native cryptocurrency

4.3. The Advantages of Smart Contracts

- Savings

Through the use of smart contracts, the time and money often spent waiting for and paying middlemen to process transactions is eliminated. The method presented by Khatoon [33] utilizes blockchain to establish a healthcare ecosystem. Through this study, many medical system stakeholders would be assisted in providing improved healthcare services while reducing costs.

- Security

The blockchain's encrypted transaction records are almost hack-proof. Additionally, with a distributed ledger, hackers will need to modify the whole chain to change a single entry. Pan et al. [34], by developing an EdgeChain model, indicated the security advantages of smart contracts and blockchain with fair cost.

- Confidence and openness

There is no need to worry that information has been changed for nefarious purposes since there is no middleman and participants exchange encrypted records of transactions. Nugent et al. [35] demonstrated that blockchain-based smart contracts provide an innovative technical solution to the issue of data tampering by supplying an immutable record of experimental history and serving as trusted administrators.

- Accuracy, efficiency, and rapidity

As soon as a condition is satisfied, the contract is instantly executed. There is no paperwork to handle and no time wasted correcting mistakes that often occur from manually filling out documentation due to the digital and automated nature of smart contracts. Griggs et al. [36] developed a system where the sensors interact with a smart device that executes smart contracts and logs all occurrences on a private blockchain on the Ethereum platform. Sending alerts to patients and medical experts, while keeping a secure record of who started these actions, would enable real-time patient monitoring. The top cited papers from 2012–2022 are shown in Table 2.

Table 2. Most cited articles between 2012 and 2022.

Goal	Approach	Results	Year	Cited by	Reference
Smart contract-based healthcare blockchain system for automated remote monitoring of patients	Using an Ethereum-based private blockchain to connect sensors to a smart device that calls smart contracts and records all occurrences on the blockchain.	Real-time patient care and secure record management	2018	404	[36]
Smart contracts enabled by blockchain: architecture, applications, and future trends	Introducing blockchain-enabled smart contracts' operation mechanism and popular platforms and proposing a smart contract research framework.	Many conventional sectors, such as IoT, management, finance, etc., are anticipated to be transformed by smart contracts.	2019	375	[37]
Is the technology mature for blockchain and smart contracts in insurance?	Supporting players participating in the decision-making process about whether or not to use blockchain.	Insurance businesses can investigate it by gaining the necessary skills and establishing prototype solutions.	2018	237	[38]
Reengineering the supply chain with blockchain technology: a case of a smart contract-based tracking system	A possible use case of business process disintermediation through a hypothetical, shared information ledger via the illustrated architecture of an integrated process.	The suggested blockchain-based approach to monitor and automate supply chain processes may be an excellent starting point for future studies on supply chain performance.	2019	215	[39]

Table 2. *Cont.*

Goal	Approach	Results	Year	Cited by	Reference
Blockchain-based dynamic modeling of the design and execution of smart contracts in the supply chain	Developing and evaluating a novel model for smart contract design in the supply chain with different logistical service providers.	The modeling complex can build and regulate supply chain smart contracts.	2020	213	[40]
Enhancing clinical trial data transparency via blockchain smart contracts	Smart contracts—code and data stored at a blockchain address and cryptographically authenticated by the network.	Blockchain smart contracts function as trustworthy administrators and give an immutable trial history, solving the data tampering issue.	2016	152	[35]
Using smart contracts and blockchain to confront deepfake videos	Blockchain-based solution for digital video authenticity that provides safe and verified traceability to the original creator or source.	The solution is based on the idea that material may be genuine and authentic if it can be reliably linked to a reliable or trustworthy source.	2019	131	[41]
Design and administration of a distributed hybrid energy system using smart contracts and blockchain technology	A peer-to-peer energy information exchange in the real-time market as a hierarchical framework for managing energy demand side + a case study based on Singapore.	With successful participant interactions, the power consumption of the overall energy system closely matches renewable resource production.	2019	129	[42]
EdgeChain: a framework and prototype for edge-IoT based on smart contracts and blockchain	"EdgeChain", an edge-IoT architecture built on the blockchain and smart contracts.	The findings indicate that incorporating blockchain and smart contracts into EdgeChain is affordable and secure.	2019	128	[34]
A system for healthcare administration based on blockchain-based smart contracts	Blockchain technology is being used in multiple workflows in the healthcare industry to improve data management.	This effort would help healthcare stakeholders optimize costs and improve quality.	2020	125	[33]

4.4. Applications

Smart contracts have many potential applications in industries including healthcare, supply chains, energy, etc. The development of smart contracts may automate procedures in many types of sectors. They offer the data accessibility necessary to provide a service when requested. Table 3 offers a concentration of the top 50 cited publications, arranged from top to bottom by citation. This is according to the paper's main focus areas, which include Healthcare, Potential Study, Supply Chain, Transparency, Authenticity, Privacy, and Security, Energy, Rights and Data Sharing, and Construction Payment.

Table 3. A summary of the major uses of the top 50 cited publications.

Articles	Healthcare	Potential Study	Supply Chain	Transparency, Authenticity, Privacy, and Security	Energy	Rights and Data Sharing	Construction Payment	Cited by
[36]	✓							404
[37]		✓						375
[38]		✓						237

Table 3. *Cont.*

Articles	Healthcare	Potential Study	Supply Chain	Transparency, Authenticity, Privacy, and Security	Energy	Rights and Data Sharing	Construction Payment	Cited by
[39]			✓					215
[40]			✓					213
[35]				✓				152
[41]				✓				131
[42]					✓			129
[34]		✓						128
[33]	✓							125
[43]				✓				113
[44]		✓						108
[45]				✓				74
[46]				✓				67
[47]				✓				65
[48]			✓					63
[49]				✓				63
[50]		✓						60
[51]	✓							59
[52]				✓				54
[53]				✓				53
[20]		✓						52
[54]		✓		✓				51
[55]		✓						47
[56]		✓						44
[57]				✓				44
[58]				✓				43
[59]					✓			43
[60]					✓			43
[61]				✓				41
[62]				✓				41
[63]						✓		41
[64]		✓		✓				40
[65]				✓				38
[66]				✓				37
[67]		✓		✓				36
[68]		✓						33
[69]	✓		✓					32
[70]		✓						31
[71]			✓					31
[72]		✓						31
[73]		✓						29

Table 3. *Cont.*

Articles	Healthcare	Potential Study	Supply Chain	Transparency, Authenticity, Privacy, and Security	Energy	Rights and Data Sharing	Construction Payment	Cited by
[74]	✓			✓				28
[75]							✓	27
[76]				✓		✓		26
[77]		✓						26
[78]		✓		✓				25
[79]		✓						23
[80]		✓		✓				23
[81]						✓		23

RQ3: What challenges do smart contracts in the blockchain often encounter?

Since smart contracts are implemented in the blockchain system, and the blockchain itself may be thought of as a distributed database, the blockchain has the added benefit of being a distributed system that can guarantee the integrity of any data stored in it. However, there are still several obstacles preventing smart contract technology from being widely used.

4.5. Challenges

I. Processing

Mainstream blockchain systems lack robust data processing capabilities and efficient smart contract execution. Mainstream blockchain systems such as Hyperledger and Ethereum may be seen as distributed databases; as a consequence, every node shares the data of the whole blockchain, resulting in a platform with no more data-processing power than a single node. Smart contract code is performed sequentially, which reduces the blockchain's data processing capability. Smart contracts struggle to expand storage because of this. Every block in the blockchain has a predetermined amount of storage space, and its size cannot be increased. If a mistake has already been made in a block data record, the only way to fix it is to attach the right record to the end of the chain. This approach aids the system's decentralization but drastically restricts block storage's scalability. As the volume of blockchain data continues to grow in tandem with the number of transactions, the time has come to provide truly scalable storage for smart contracts.

II. Acceptance

There are still many myths about the technology despite the buzz around smart contracts and blockchains in both the public and consortium spheres. There have been numerous exaggerated use cases and overblown expectations. Even with appropriate use cases, convincing consumers and stakeholders to adopt new technology may be challenging. This could lead to increased development expenses and a poor return on investment. In reality, implementing some of the described use cases using conventional databases is more effective. Therefore, individuals interested in creating smart contract solutions should consider the cost of development, as well as what can and cannot be done.

III. Immutability

There is a lack of sophisticated contract development language and efficient vulnerability detection and processing techniques [82]. Once Ethereum smart contracts have been implemented, they cannot be altered, making it very difficult to find a solution to the security issue in smart contracts. After a smart contract has been integrated into a blockchain, there is no straightforward way to fix any bugs that may have been introduced during the development process. As a result, a process for updating and terminating the

contract status must be developed. In contrast, this approach runs against Ethereum's guiding concept that "code is law", and even if it is built, it faces significant challenges in being accepted by every node in the network. A new blockchain is created if certain nodes are not validated. One of the difficulties with smart contracts is that they provide a security risk such as this.

IV. Integrity

Even though all nodes in a network execute predetermined software to carry out the terms of a smart contract, the data used by such contracts are under the control of other parties and hence not entirely reliable. Access to information stored in a smart contract or blockchain is often restricted. Instead, they utilize third-party wallet applications that put users' personal information at risk.

V. Usability

In contrast to conventional contracts, smart contracts are not adaptable with exceptions such as bugs since they are logic-based computer programs with a limited amount of interaction. They also do not enable individuals to discuss and make changes based on subsequently approved revisions. Allowing common consumers to directly handle their data is problematic because of the P2P nature of blockchains, and when using cryptocurrency, the exchange rate might be unpredictable.

VI. Security

One of the primary issues of any blockchain system and associated process is security. In reality, many vulnerabilities are caused by scripting language misunderstandings [37]. Wang et al. [37] classified smart contract semantic vulnerabilities as transaction-ordering reliance, call stack depth, time-stamp dependence, re-entry attacks, and mishandled exceptions.

A smart contract system has low maintainability and several potential security flaws. Smart contracts pose substantial, unseen risks since their code is difficult to maintain once they have been implemented. There is no method to patch a security issue in a smart contract in the chain unless the contract code is updated and redeployed, which wastes time and space. Because of the immutable nature of the blockchain, smart contracts are almost impossible to alter. The creation of new smart contract languages and the upgrading of current ones should be carefully considered to increase the security of smart contracts. Additionally, before utilizing certain blockchain platforms, one should be aware of their mechanisms and weaknesses since the sorts of attacks differ from one platform to the next.

VII. Legal issues

Lawyers can address the issue of regulation in detail if smart contracts are well-stated. However, it is also debatable whether smart contracts need any kind of regulation (direct or indirect). It is ultimately just computer code. Regulating smart contracts in light of their particular uses, dangers, and ramifications could make more sense. According to most studies, smart contracts will not replace the law per se, but they may serve as particular, legally enforceable contracts. Therefore, it is crucial to comprehend if smart contract technology can or cannot serve as a substitute for the law. The research by Marino and Juels [83] serves as a foundation for the ongoing development of a technological smart contract system that is based on contract law and allows parties to modify or annul smart contracts under predetermined circumstances. The phrase "smart contract" may suggest that research should not be entirely focused on contract law.

VIII. Privacy

Public smart contracts' pseudonymity may not always imply a guarantee of privacy. They specifically do not ensure unlinkability, which is essential for both fungibility and privacy [84]. Integrating an additional data protection component is one method to safeguard privacy. Since the use of encryption methods often results in an increased processing load on the system, future research and development of privacy-preserving strategies will concentrate on lightweight solutions.

RQ4: In what ways will smart contracts in the blockchain develop in the near future?

The security performance of smart contracts has improved overall. Numerous aspects, including cryptography, consensus algorithms, and smart contracts, have an impact on the security performance of smart contracts. Smart contracts' security issues cannot be effectively addressed by focusing on just one component of them. Blockchain security issues have not been completely resolved by the current research. Therefore, from a global viewpoint, taking into account several levels and multiple influencing elements would be crucial for creating the safest and most ideal blockchain security protection system.

Smart contract verification on a large scale and the standardization of verification methods and tools, and tools for formally checking Ethereum bytecode and smart contract source code are still in their infancy and have few practical uses at the moment. There are a lot of ways out there, but many of them can only identify one kind of vulnerability or a small number of vulnerabilities and take a lot of effort. Due to the overlap in the vulnerabilities detected by some technologies and differences in the vulnerabilities detectable by others, vulnerability identification in contracts is a particularly complicated and uncomfortable problem. To boost detection efficiency and reduce detection costs, formal verification of smart contracts must go in the direction of scale and the unification of vulnerability security validation and monitoring technologies.

To deal with the difficulties of quantum computing, cryptographic security technology has been developed. The blockchain system relies on cryptography, which was thought to be unbreakable when it was first developed. However, cryptography is not without its flaws, and there is always the chance that it may be cracked. The quantum computing Shor algorithm, developed in 1994, offers a significant danger to encryption techniques such as DES and hence poses a threat to the security of blockchain. Because it relies on cryptography, blockchain technology will lose its primary benefits if and when its underlying security is compromised. As a result, blockchain research and development will focus on creating reliable cryptographic security technologies to counteract the threats posed by quantum computers, and harmonization and interoperability between conventional legal norms and digitally executed contracts. The current stage of smart contracts is when they work along with conventional contracts. Further work will have to be carried out to improve smart contracts' grasp of the law, set up review criteria for smart contracts, cut down on mistakes, and bring smart contracts up to par with legal review requirements. However, to prevent thorny accountability issues in the future, it is also required to enhance current laws to specify the different scenarios of smart contracts and the specific meaning communicated by the parties to the transaction. These two variables achieve the purpose of better coordinating and integrating smart contracts and traditional regulations.

4.6. Potential Developments

The following sections explore the potential of incorporating more computer science theory into smart contracts. Theories and works of significance in computer science are explored in light of their relevance to smart contracts:

- Data science smart contracts

Data science may use smart contracts as a scalable method. Performance constraints, failure concerns, and security threats are particularly present when managing a large amount of data in a centralized design. Smart contracts play a crucial role in data science in several ways. Trustworthy data-sharing procedures, decentralized trust, data integrity, and access control are all areas where blockchain-based smart contracts have proven useful in the field of data science. For large data, Abdullah et al. [85] presented authentication methods related to blockchain. The limits of Kerberos authentication were explored, along with how the blockchain may overcome them. To assist data analytics in the Internet of Things, Xu et al. [86] proposed the Sapphire smart-contract-based storage system to regulate access to massive data sets.

- Artificial intelligence

Smart contracts may be enhanced in several ways by using artificial intelligence (AI). Smart contracts can be validated using certain forms of AI, while other forms of AI can be included in the contracts themselves [44]. In addition, Tensor and other deep learning principles are finding new uses in blockchain-based smart contracts. In the research by Sun and Gu [87], a technique for identifying blockchain-based smart contracts' vulnerabilities is proposed. The machine learning method with great performance and speed enables speedy detection. As long as the model's threshold is adjusted, it may function as a quick prefilter for conventional symbolic analysis techniques to increase accuracy even further. Another branch of AI, cognitive computing, attempts to recreate the mental processes of humans in a digital environment. When it comes to optimizing the performance of blockchain-based smart contracts, AI's role as a utility service is crucial. The application of AI for smart contract verification was introduced by Marwala et al. [88]. They highlighted the significant ways in which AI may be used in the setting of blockchain-based smart contracts, such as enhancing security, scalability, etc. They also emphasized how formal verification based on AI may be used to judge smart contracts.

Cognitive computing is a cutting-edge area of AI study that implements human-like thought processes into the digital sphere. When compared to traditional AI methods, cognitive computing's superior accuracy is a direct result of its incorporation of human cognitive processes and execution constraints. The service values in many cognitive computing use cases will be enhanced by blockchain-based smart contracts. From the standpoint of cognitive computing, the most important aspects of blockchain-based smart contracts are their data openness, decentralized access control capacity, and decentralized trust. The potential for cognitive computing in the medical field was the subject of a survey by Daniel et al. [89]. They stressed the need of adhering to regulatory standards while using blockchain technology in healthcare.

In sync with the decentralization potential of the blockchain, federated learning is a distributed and collaborative method of education [90]. In a federated learning setup, the raw data are not uploaded and used as training datasets. Data access management and federated learning are only two of the many uses for blockchain technology, which may also be used for other types of sensitive data that are widely dispersed, such as healthcare data. Smart contracts and federated learning provide a unique opportunity for academic inquiry. An industrial Internet of Things privacy preservation strategy based on blockchain technology and federated learning was presented by Lu et al. [91]. To reduce time spent processing data and maximize the use of available computer power, the authors included federated learning in the consensus. Data privacy needs are highlighted, and unresolved concerns related to the limited computer infrastructure are examined.

- Game theory

To analyze the dynamics between players, game theorists use several mathematical methods. Game theory and smart contracts are two areas where researchers are beginning to dig deeper. The usefulness of smart contracts extends to a wide variety of contexts. The game theory of integrated smart contract casinos was studied by Piasecki [92]. The author investigated the possibility that a well-off attacker may exploit the system by buying more computing resources. To protect the Proof-of-Work blockchain from this specific kind of assault, the author offered several suggestions.

5. Conclusions

The decentralization, auto-enforcing ability, and verifiability characteristics of smart contracts enable their encoded business rules to be executed in a peer-to-peer network, where each node is "equal" and none has any special authority without the involvement of a trusted authority or a central server. Thus, smart contracts are expected to revolutionize many traditional industries, such as finance, healthcare, energy, etc. Not only are they commonplace in business and commerce, but they also play an important role in many

other spheres of human interaction. This insight led us to conduct a thorough evaluation of blockchain-based smart contracts published between 2012 and 2022. The purpose of this study is to analyze the current state of smart contracts in the blockchain, their applications, and the potentially revolutionary effects of their unique characteristics. Constraints and their ripple effects in other domains have been noted, as have the difficulties and omissions in the literature on the issue. There are a total of 252 publications in this area that were considered for this review. Smart contract technology is promising, but it is still in its infancy, so there are a lot of kinks to work out such as the lack of strong data processing capacity and effective smart contract management by mainstream blockchain systems, the absence of a sophisticated contract development language and effective vulnerability scanning and processing technique, the low maintainability, several potential security vulnerabilities of smart contracts, etc. Future developments in domains such as data science, AI, and game theory that can be integrated into smart contracts in blockchain systems have been considered and demonstrated.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Vieira, G.; Zhang, J. Peer-to-peer energy trading in a microgrid leveraged by smart contracts. *Renew. Sustain. Energy Rev.* **2021**, *143*, 110900. [CrossRef]
2. Taherdoost, H.A. Critical Review of Blockchain Acceptance Models—Blockchain Technology Adoption Frameworks and Applications. *Computers* **2022**, *11*, 24. [CrossRef]
3. Nakamoto, S.; Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 1 December 2022).
4. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–15.
5. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 2-1.
6. Sklaroff, J.M. Smart contracts and the cost of inflexibility. *Univ. Pa. Law Rev.* **2017**, *166*, 263.
7. Macrinici, D.; Cartofeanu, C.; Gao, S. Smart contract applications within blockchain technology: A systematic mapping study. *Telemat. Inform.* **2018**, *35*, 2337–2354. [CrossRef]
8. Madanchian, M.; Taherdoost, H. The Impact of Digital Transformation Development on Organizational Change. In *Driving Transformative Change in E-Business through Applied Intelligence and Emerging Technologies*; IGI Global: Hershey, PA, USA, 2022; pp. 1–24.
9. Rouhani, S.; Deters, R. Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access* **2019**, *7*, 50759–50779. [CrossRef]
10. Feng, T.; Yu, X.; Chai, Y.; Liu, Y. Smart contract model for complex reality transaction. *Int. J. Crowd Sci.* **2019**, *3*, 184–197. [CrossRef]
11. Eenmaa-Dimitrieva, H.; Schmidt-Kessen, M.J. Creating markets in no-trust environments: The law and economics of smart contracts. *Comput. Law Secur. Rev.* **2019**, *35*, 69–88. [CrossRef]
12. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
13. Destefanis, G.; Marchesi, M.; Ortu, M.; Tonelli, R.; Bracciali, A.; Hierons, R. Smart contracts vulnerabilities: A call for blockchain software engineering? In Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 20 March 2018; pp. 19–25.
14. Marchesi, L.; Marchesi, M.; Destefanis, G.; Barabino, G.; Tigano, D. Design patterns for gas optimization in ethereum. In Proceedings of the 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), London, ON, Canada, 18 February 2020; pp. 9–15.
15. Taherdoost, H. An Overview of Trends in Information Systems: Emerging Technologies that Transform the Information Technology Industry. *Cloud Comput. Data Sci.* **2023**, *4*, 1–16. [CrossRef]
16. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.-B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart contract development: Challenges and opportunities. *IEEE Trans. Softw. Eng.* **2019**, *47*, 2084–2106. [CrossRef]
17. Chakraborty, P.; Shahriyar, R.; Iqbal, A.; Bosu, A. Understanding the software development practices of blockchain projects: A survey. In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement; Computing Machinery: New York, NY, USA, 2018; pp. 1–10.
18. Ante, L. Smart contracts on the blockchain–A bibliometric analysis and review. *Telemat. Inform.* **2021**, *57*, 101519. [CrossRef]

19. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
20. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef] [PubMed]
21. Davidson, S.; De Filippi, P.; Potts, J. Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. 2016. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995 (accessed on 1 December 2022).
22. Liebenau, J.; Elaluf-Calderwood, S. Blockchain Innovation beyond Bitcoin and Banking. 2016. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2749890 (accessed on 1 December 2022).
23. Sharma, P.; Jindal, R.; Borah, M.D. Blockchain-based decentralized architecture for cloud storage system. *J. Inf. Secur. Appl.* **2021**, *62*, 102970. [CrossRef]
24. Chen, Y.; Zhang, Y.; Zhou, B. Research on the risk of block chain technology in Internet finance supported by wireless network. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 71. [CrossRef]
25. Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The revolution of blockchain: State-of-the-art and research challenges. *Arch. Comput. Methods Eng.* **2021**, *28*, 1497–1515. [CrossRef]
26. Perera, S.; Nanayakkara, S.; Rodrigo, M.; Senaratne, S.; Weinand, R. Blockchain technology: Is it hype or real in the construction industry? *J. Ind. Inf. Integr.* **2020**, *17*, 100125. [CrossRef]
27. Ream, J.; Chu, Y.; Schatsky, D. Upgrading blockchains: Smart contract use cases in industry. *Retrieved Dec.* **2016**, *12*, 2017.
28. Szabo, N. The idea of smart contracts. *Nick Szabo's Pap. Concise Tutor.* **1997**, *6*, 199.
29. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
30. Greenspan, G. Smart Contracts: The Good, the Bad and the Lazy. 2015. Available online: https://www.multichain.com/blog/2015/11/smart-contracts-good-bad-lazy/ (accessed on 1 December 2022).
31. Finck, M. Blockchains and data protection in the European Union. *Eur. Data Prot. L. Rev.* **2018**, *4*, 17. [CrossRef]
32. Politou, E.; Casino, F.; Alepis, E.; Patsakis, C. Blockchain mutability: Challenges and proposed solutions. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1972–1986. [CrossRef]
33. Khatoon, A. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. [CrossRef]
34. Pan, J.; Wang, J.; Hester, A.; Alqerm, I.; Liu, Y.; Zhao, Y. EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. *IEEE Internet Things J.* **2018**, *6*, 4719–4732. [CrossRef]
35. Nugent, T.; Upton, D.; Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* **2016**, *5*, 2541. [CrossRef]
36. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 1–7. [CrossRef]
37. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.-Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
38. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
39. Chang, S.E.; Chen, Y.-C.; Lu, M.-F. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technol. Forecast. Soc. Change* **2019**, *144*, 1–11. [CrossRef]
40. Dolgui, A.; Ivanov, D.; Potryasaev, S.; Sokolov, B.; Ivanova, M.; Werner, F. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *Int. J. Prod. Res.* **2020**, *58*, 2184–2199. [CrossRef]
41. Hasan, H.R.; Salah, K. Combating deepfake videos using blockchain and smart contracts. *IEEE Access* **2019**, *7*, 41596–41606. [CrossRef]
42. Li, Y.; Yang, W.; He, P.; Chen, C.; Wang, X. Design and management of a distributed hybrid energy system through smart contract and blockchain. *Appl. Energy* **2019**, *248*, 390–405. [CrossRef]
43. Hasan, H.R.; Salah, K. Proof of delivery of digital assets using blockchain and smart contracts. *IEEE Access* **2018**, *6*, 65439–65448. [CrossRef]
44. Governatori, G.; Idelberger, F.; Milosevic, Z.; Riveret, R.; Sartor, G.; Xu, X. On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artif. Intell. Law* **2018**, *26*, 377–409. [CrossRef]
45. Sultana, T.; Almogren, A.; Akbar, M.; Zuair, M.; Ullah, I.; Javaid, N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Appl. Sci.* **2020**, *10*, 488. [CrossRef]
46. Wang, H.; Qin, H.; Zhao, M.; Wei, X.; Shen, H.; Susilo, W. Blockchain-based fair payment smart contract for public cloud storage auditing. *Inf. Sci.* **2020**, *519*, 348–362. [CrossRef]
47. Ramezan, G.; Leung, C. A blockchain-based contractual routing protocol for the internet of things using smart contracts. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 4029591. [CrossRef]
48. De Giovanni, P. Blockchain and smart contracts in supply chain management: A game theoretic model. *Int. J. Prod. Econ.* **2020**, *228*, 107855. [CrossRef]
49. Yuan, R.; Xia, Y.-B.; Chen, H.-B.; Zang, B.-Y.; Xie, J. Shadoweth: Private smart contract on public blockchain. *J. Comput. Sci. Technol.* **2018**, *33*, 542–556. [CrossRef]
50. Abou El Houda, Z.; Hafid, A.S.; Khoukhi, L. Cochain-SC: An intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract. *IEEE Access* **2019**, *7*, 98893–98907. [CrossRef]
51. Sharma, A.; Tomar, R.; Chilamkurti, N.; Kim, B.-G. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics* **2020**, *9*, 1609. [CrossRef]

52. Liu, H.; Zhang, Y.; Zheng, S.; Li, Y. Electric vehicle power trading mechanism based on blockchain and smart contract in V2G network. *IEEE Access* **2019**, *7*, 160546–160558. [CrossRef]
53. Huang, X.; Ye, D.; Yu, R.; Shu, L. Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 426–441. [CrossRef]
54. Bodó, B.; Gervais, D.; Quintais, J.P. Blockchain and smart contracts: The missing link in copyright licensing? *Int. J. Law Inf. Technol.* **2018**, *26*, 311–336. [CrossRef]
55. Oliva, G.A.; Hassan, A.E.; Jiang, Z.M.J. An exploratory study of smart contracts in the Ethereum blockchain platform. *Empir. Softw. Eng.* **2020**, *25*, 1864–1904. [CrossRef]
56. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. A Distributed framework for detecting DDoS attacks in smart contract—Based Blockchain—IoT Systems by leveraging Fog computing. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4112. [CrossRef]
57. Xiong, W.; Xiong, L. Smart contract based data trading mode using blockchain and machine learning. *IEEE Access* **2019**, *7*, 102331–102344. [CrossRef]
58. Zhang, L.; Zhang, Z.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Research on a covert communication model realized by using smart contracts in blockchain environment. *IEEE Syst. J.* **2021**, *16*, 2822–2833.
59. Chen, C.; Xiao, T.; Qiu, T.; Lv, N.; Pei, Q. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4122–4133. [CrossRef]
60. Seven, S.; Yao, G.; Soran, A.; Onen, A.; Muyeen, S. Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts. *IEEE Access* **2020**, *8*, 175713–175726. [CrossRef]
61. Hamledari, H.; Fischer, M. Role of blockchain-enabled smart contracts in automating construction progress payments. *J. Leg. Aff. Disput. Resolut. Eng. Constr.* **2021**, *13*, 04520038. [CrossRef]
62. Xuan, S.; Zheng, L.; Chung, I.; Wang, W.; Man, D.; Du, X.; Yang, W.; Guizani, M. An incentive mechanism for data sharing based on blockchain with smart contracts. *Comput. Electr. Eng.* **2020**, *83*, 106587. [CrossRef]
63. Panescu, A.-T.; Manta, V. Smart contracts for research data rights management over the ethereum blockchain network. *Sci. Technol. Libr.* **2018**, *37*, 235–245. [CrossRef]
64. Rozario, A.M.; Thomas, C. Reengineering the audit with blockchain and smart contracts. *J. Emerg. Technol. Account.* **2019**, *16*, 21–35. [CrossRef]
65. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart contract-based blockchain-envisioned authentication scheme for smart farming. *IEEE Internet Things J.* **2021**, *8*, 10792–10806. [CrossRef]
66. Fan, K.; Bao, Z.; Liu, M.; Vasilakos, A.V.; Shi, W. Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Gener. Comput. Syst.* **2020**, *110*, 665–674. [CrossRef]
67. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.B. Blockchain and smart contract for IoT enabled smart agriculture. *PeerJ Comput. Sci.* **2021**, *7*, e407. [CrossRef]
68. Liu, X.; Muhammad, K.; Lloret, J.; Chen, Y.-W.; Yuan, S.-M. Elastic and cost-effective data carrier architecture for smart contract in blockchain. *Future Gener. Comput. Syst.* **2019**, *100*, 590–599. [CrossRef]
69. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access* **2021**, *9*, 37397–37409. [CrossRef]
70. Vacca, A.; Di Sorbo, A.; Visaggio, C.A.; Canfora, G. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *J. Syst. Softw.* **2021**, *174*, 110891. [CrossRef]
71. Philipp, R.; Prause, G.; Gerlitz, L. Blockchain and smart contracts for entrepreneurial collaboration in maritime supply chains. *Transp. Telecommun.* **2019**, *20*, 365–378. [CrossRef]
72. Wang, S.; Huang, C.; Li, J.; Yuan, Y.; Wang, F.-Y. Decentralized construction of knowledge graphs for deep recommender systems based on blockchain-powered smart contracts. *IEEE Access* **2019**, *7*, 136951–136961. [CrossRef]
73. Unal, D.; Hammoudeh, M.; Kiraz, M.S. Policy specification and verification for blockchain and smart contracts in 5G networks. *ICT Express* **2020**, *6*, 43–47. [CrossRef]
74. Omar, I.A.; Jayaraman, R.; Salah, K.; Simsekler, M.C.E.; Yaqoob, I.; Ellahham, S. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Med. Res. Methodol.* **2020**, *20*, 224. [CrossRef]
75. Hamledari, H.; Fischer, M. Construction payment automation using blockchain-enabled smart contracts and robotic reality capture technologies. *Autom. Constr.* **2021**, *132*, 103926. [CrossRef]
76. Singh, S.K.; Salim, M.M.; Cho, M.; Cha, J.; Pan, Y.; Park, J.H. Smart contract-based pool hopping attack prevention for blockchain networks. *Symmetry* **2019**, *11*, 941. [CrossRef]
77. Daniel, F.; Guida, L. A service-oriented perspective on blockchain smart contracts. *IEEE Internet Comput.* **2019**, *23*, 46–53. [CrossRef]
78. Patil, A.S.; Hamza, R.; Hassan, A.; Jiang, N.; Yan, H.; Li, J. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Comput. Secur.* **2020**, *97*, 101958. [CrossRef]
79. Bhardwaj, A.; Shah, S.B.H.; Shankar, A.; Alazab, M.; Kumar, M.; Gadekallu, T.R. Penetration testing framework for smart contract blockchain. *Peer Peer Netw. Appl.* **2021**, *14*, 2635–2650. [CrossRef]
80. Debe, M.; Salah, K.; Rehman, M.H.U.; Svetinovic, D. Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access* **2020**, *8*, 20118–20128. [CrossRef]
81. Goldenfein, J.; Leiter, A. Legal engineering on the blockchain:'Smart contracts' as legal conduct. *Law Crit.* **2018**, *29*, 141–149. [CrossRef]

82. Wang, Y.; He, J.; Zhu, N.; Yi, Y.; Zhang, Q.; Song, H.; Xue, R. Security enhancement technologies for smart contracts in the blockchain: A survey. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4341. [CrossRef]
83. Marino, B.; Juels, A. Setting standards for altering and undoing smart contracts. In *Rule Technologies. Research, Tools, and Applications*; Springer: Cham, Switzerland, 2016; pp. 151–166.
84. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference; Association for Computing Machinery: New York, NY, USA, 2013; pp. 127–140.
85. Abdullah, N.; Hakansson, A.; Moradian, E. Blockchain based approach to enhance big data authentication in distributed environment. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017; pp. 887–892.
86. Xu, Q.; Aung, K.M.M.; Zhu, Y.; Yong, K.L. A blockchain-based storage system for data analytics in the internet of things. In *New Advances in the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 119–138.
87. Sun, Y.; Gu, L. Attention-based machine learning model for smart contract vulnerability detection. *J. Phys. Conf. Series* **2021**, *1820*, 012004. [CrossRef]
88. Marwala, T.; Xing, B. Blockchain and artificial intelligence. *arXiv* **2018**, arXiv:1802.04451.
89. Daniel, J.; Sargolzaei, A.; Abdelghani, M.; Sargolzaei, S.; Amaba, B. Blockchain technology, cognitive computing, and healthcare innovations. *J. Adv. Inf. Technol* **2017**, *8*, 194–198. [CrossRef]
90. Nguyen, D.C.; Ding, M.; Pham, Q.-V.; Pathirana, P.N.; Le, L.B.; Seneviratne, A.; Li, J.; Niyato, D.; Poor, H.V. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet Things J.* **2021**, *8*, 12806–12825. [CrossRef]
91. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
92. Piasecki, P.J. Gaming self-contained provably fair smart contract casinos. *Ledger* **2016**, *1*, 99–110. [CrossRef]