information

Review

Survey of Smart Contract Framework and Its Application

Edi Surya Negara [1,*], Achmad Nizar Hidayanto [2], Ria Andryani [1] and Rezki Syaputra [1]

[1] Computer Science, Universitas Bina Darma, Sumatera Selatan 30111, Indonesia; ria.andryani@binadarma.ac.id (R.A.); r.syaputra@binadarma.ac.id (R.S.)
[2] Computer Science, Universitas Indonesia, Jawa Barat 40111, Indonesia; nizar@cs.ui.ac.id
* Correspondence: e.s.negara@binadarma.ac.aid

Abstract: This article is a literature review on smart contract applications in various domains. The aim is to investigate technological developments and implementation of smart contracts in various domains. For this purpose, the theoretical basis of various papers that have been published in recent years is used as a source of theoretical and implementation studies. Smart contracts are the latest technology that is developing in line with the development of blockchain technology. The literature review that we have carried out explains that smart contracts work automatically, control, or document legally relevant events and actions in accordance with the agreements set forth in the contract agreement. This technology is one of the newest technologies that is expected to provide solutions for trust, security, and transparency in various domains. This literature review was conducted using an exploratory approach. This literature review focuses on reviewing frameworks, methods, and simulations of smart contract implementations in various domains.

Keywords: smart contract; blockchain; e-government; supply chain; cyber security; IoT; symbolic execution

check for updates

Citation: Negara, E.S.; Hidayanto, A.N.; Andryani, R.; Syaputra, R. Survey of Smart Contract Framework and Its Application. *Information* **2021**, *12*, 257. https://doi.org/10.3390/info12070257

Received: 10 May 2021
Accepted: 15 June 2021
Published: 22 June 2021

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

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The adaptation of information systems and information technology to follow social developments is one of the aspects of renewal, change, and the latest technological discoveries in order to meet the needs of information and communication technology in society. Blockchain technology is an example of a technology that continues to be developed according to the needs of society, which is the basis for the development of other technologies such as smart contracts [1]. Smart contract technology is a computerized transaction protocol that independently carries out the terms of the contract and aims to bind an agreement or agreement between several parties [1,2]. Smart contracts are disintermediated and generally transparent, promising commercial efficiency, lowering legal and transaction costs, and anonymous transactions [1]. These various qualities make it one of the most sought-after technologies, one of which is in the financial sector because it reduces the risk of non-payment and fraud, and improves the quality of financial contracts with a certain level of confidence and is independent of the influence of intermediaries [3].

Currently, there have been many advances in the development of technology that supports smart contracts, while there is little understanding regarding their use in various companies. Issues of system security and information technology, trust in data transaction systems, and transparency of data exchange between different organizations are new challenges for organizations. In addition, the decentralization of business processes and work processes of an organization is also an issue in meeting the technological needs of companies that standardize security, trust, and transparency of data transactions. To solve the problem of organizational data transactions, smart contract technology that works on a blockchain basis is proposed as a solution for organizations.

Smart contract is a technology that consists of computer code programs that work consistently to execute these codes where the executed data will be spread across a network

of nodes that do not trust each other, without arbitration from a trusted authority. This is a major advantage in implementing smart contracts in organizations. Contracts support organizations to collaborate and ensure agreed contract clauses and contract information is shared on the blockchain network without the involvement of third parties [4]. However, in its implementation, smart contracts also have several problems, both social technology issues and technical problems, such as: blockchain mechanisms, virtual machines, and smart contract code levels, and disintermediation automation [4]. Zibin Zheng et al. also explained that smart contracts have several advantages, namely: smart contracts can reduce administration and save service costs, improve business process efficiency, and reduce risk [5].

This study presents a literature review of various pre-existing research that discusses various methods, frameworks, and applications of smart contract technology that have been tested and simulated in organizations either as prototypes or implemented in various domains. The contributions of this article are the strengthening of recent theoretical studies and the provision examples of implementing smart contracts in various domains. This article also provides a comprehensive explanation of the methods and frameworks for implementing smart contracts.

This article is divided into several sections; namely, the introductory section describes an outline of the phenomenon, its background, advantages and disadvantages, and the purpose of the article. The second part describes the literature review method which describes the process and stages of the literature study carried out. The third part describes and discusses the framework and application of smart contracts. In the end, the conclusions from the articles and literature reviews that have been carried out are presented.

2. Literature Review Method

This literature exploration study was carried out using a literature review approach [6]. The literature review is one of the most important stages in research activities, where this stage will be a strong foundation for knowing the state of the art of the development of technology and information systems [7]. A literature review on smart contract applications is the basis for tracing the development of blockchain technology, especially for expanding domains in smart contract implementation. In this study, there are four stages of the literature review [6]. Stage 1 is to review the research objectives and protocols. Stage 2 is to conduct a literature search and perform a practical screening of articles on smart contract topics. Stage 3 assesses the quality of the articles and data extraction. Finally, the fourth stage is to analyze the findings.

2.1. Planning Phase

Stage 1, namely, reviewing objectives and protocols, is an important element that must be carried out in the literature review [8]. The review protocol can reduce bias in the research plan [8]. This stage discusses the objectives of the literature review and the design of the literature protocol and criteria, data extraction methods, data analysis, and presentation of the review results.

2.2. Selection Phase

In the second stage of the review, the scientific articles reviewed were sourced from scientific articles in the Google Scholar database from 2015–2020. Scientific articles taken as review material are articles related to the review topic, namely blockchain and smart contracts. The time frame used for searching this article was chosen because it is a relatively new technology. The article search is carried out in various types such as journal papers, conference papers, and white papers. In looking for articles that fit the specified purpose, we use keywords using boolean operators as follows: smart contract + application, smart contract + organization, smart contract + implementation, blockchain + smart contract, application + blockchain, blockchain + enterprise to find papers with constraints and problems, the following keywords are used: problem + blockchain, and problem + smart contract. This pair is used independently in each search. After obtaining the results, the

filtering process is carried out to make sure the articles obtained are the appropriate articles. This filtering process is carried out by removing articles that are not relevant to the topic and studies on smart contracts, duplicates, and articles whose full text we cannot obtain. From this initial process, we obtained 221 papers. See Figure 1 below, which shows the article selection process.

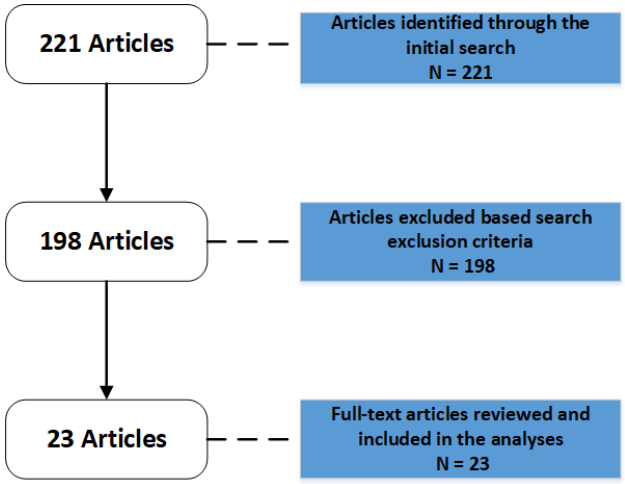

Figure 1. Article Selection Based on Search.

2.3. Exclusion and Inclusion Criteria

In Stage 3, article selection was carried out with exclusion criteria. This stage removes articles that are not suitable or irrelevant to the research topic, removes articles that do not provide complete articles, removes articles that cannot be downloaded or accessed, and removes articles that are not published between 2015–2020. Then, this stage also removes articles unrelated to blockchain technology, or smart contracts. After the exclusion process is carried out, the next step is to select inclusion criteria; namely, journal papers, peer-reviewed conference papers, selecting quality white paper articles, and articles that match the inclusion criteria regarding smart contract applications in an organization.

2.4. Synthesis

The final stage of this review is to extract data or information from articles to be used as material for study, analysis and identification of the implementation of smart contract applications in various domains. At this stage, the extraction is carried out using qualitative techniques. Data analysis continued with literature review study reports.

3. Framework and Application of Smart Contracts

One of the leading blockchain technology products along with the continued development of research and technology commercialization is Bitcoin. The product of this blockchain technology is the pioneer of the development of the cryptocurrency known as blockchain 1.0. This technology is characterized by decentralization, damage resistance, anonymity, and audit capabilities [9]. Bitcoin is a technology based on the blockchain system. However, in its application, Bitcoin has a weakness in writing contracts with complex logic. With Bitcoin, it is not possible to write complex contract logic due to limitations of the Bitcoin scripting language (Bitcoin scripting language only has 256 instructions, 15 of which are currently disabled, and 75 are reserved). Due to these limitations in functionality, Bitcoin can only be considered as a raw prototype smart contract. On the other hand, improvements to smart contracts are continuously being made. One of the other smart contract platforms is Ethereum. Ethereum development was carried out with the aim of covering up the shortcomings of the Bitcoin platform. This development is based on the main idea of running user-defined programs on the blockchain, thus creating expressive custom smart contracts using the Turing-complete programming language [10].

In the development of Ethereum, the Ethereum smart contract code is written in bytecode language based on the stack that runs on the Ethereum Virtual Machine (EVM) [11,12]. The high-level languages used in Ethereum development are Solidity1 and Serpent2 [11]. After that, the program code is compiled into EVM bytecode to run. With complex smart contract logic blockchain technology implemented, currently, Ethereum is the most popular platform for developing smart contracts; then, Ethereum is marked as the developer of blockchain technology which is known as Blockchain 2.0 [13]. As part of Ethereum, Hyperledger Fabric, Corda, and BigchainDB are several platforms that can be used to develop smart contracts [14].

One of the advantages of smart contracts is the implementation of protocols that work by consensus [15,16]. Smart contracts will work by encoding predetermined rules and carry out related operations when the agreed provisions have been fulfilled [17]. Smart contract implementations can be used in a variety of domains including smart assets [18] (e.g., Slock.it3, a German company that uses Ethereum-based smart contracts for leasing, selling, or sharing other transaction activities without the involvement of intermediaries) [18]. In addition, the implementation of smart contracts has been used in the implementation of self-government or autonomous arrangements (for example, digital property management such as ujomusic4, e-voting, and supply chain) [19].

In addition, this smart contract technology is rapidly developing in the form of cryptocurrency. The blockchain technology underlying platforms such as Ethereum and Hyperledger is starting to support various types of smart contracts [20,21]. Smart contracts also have various applications such as services in the financial domain [22], market prediction, utilization of the Internet of Things (IoT), etc. [23]. In the government sector, there are several smart contract frameworks and applications such as e-government, digital rights management, social media platforms, cloud storage, supply chain, smart transportation [23–25].

This article describes several smart contract frameworks and applications developed in several implementation domains such as government services, supply chain management, Internet of Things, software testing, cybersecurity, and geographic information systems.

3.1. eGOV-DAO

One of the blockchain and smart contract applications in the government domain is eGov-DAO. eGov-DAO is a smart contract framework that is used to provide e-government services with a fully automated and efficient system that is integrated so as to provide transparent services [26].

eGov-DAO is a smart contract for real-time e-government services that work to monitor and analyze services provided by the government. This system works with the principles of transparency, accountability, provision. In addition, the most important advantage of this system is the better management of national resources [26]. The system keeps all audit records providing transparency of court proceedings with the parties involved. eGov-DAO is designed to provide convenience to system users so that it does not require maximum user training [26].

The implementation of eGov-DAO can be utilized in government contracts. A government contract is a government agreement with a vendor by recording the agreement in a public contract [26]. There were many weaknesses in the old system, one of which was the inefficient allocation of contracts and deals which required a lot of interaction between institutions and involved a lot of human labor [27]. Apart from that, another weakness is that in providing excellent government services with a simple and comfortable system, the government has provided a lot of human and financial resources, but this is only able to result in a lack of transparency in government administration so that government performance becomes inefficient. Therefore, smart contracts are a solution in increasing transparency and trust, reducing costs and simplifying processes.

The eGov-DAO framework is a blockchain framework which is generic in nature and can be applied to any policy for government contracts. The eGov-DAO framework was developed with the United States Small Business Administration policy in mind [26]. The

first phase of how the framework works is that it provides an explanation of smart contract and blockchain applications in relation to US contracts. After that, it introduces some contract allocation rules required by US policy for the Small Business Administration, then the DAO framework writes all the requirements and regulates the allocation process on the smart contract. eGov-DAO provides definitions of system-related parties and system user activities and builds a model of the main contract process. The last phase of eGov-DAO is validating the rules that have been agreed upon in the smart contract [26].

3.2. Virtual Operation Model

The Virtual Operation Model is one of the technologies with a smart contract framework implemented in the supply chain domain. This experimental technology was constructed with a dynamic approach to assignment and service composition [28]. The Virtual Operating Model also features a rescheduling procedure. The features of the Virtual Operation Model work by combining decision planning and adaptation methodologies that are integrated with dynamic control theory [28]. Another feature of the Virtual Operation Model is the implementation of physical operations modeled in the initiation and delivery of online information services [28].

The implementation of the Virtual Operation Model that works based on blockchain technology provides storage services and uses of information in the supply chain. Services that exist in the Virtual Operation Model include supply chain assignments, sequencing of operations, scheduling that have been adjusted to the communication protocol. All these services work with a special pattern that has been synchronized with the company [28].

The embedded scheduling control methodology characterizes the Virtual Operations Model where blockchain and smart contracts are the main base in the supply chain. Technically, the procedure in virtual operation modeling works by using continuous state variables and discrete control variables. Continuous status variables are used to determine the start time and realization time, and completion of an information service in a smart contract. Meanwhile, discrete control variables are used to define logistics service providers in the supply chain [28].

3.3. Edge Chain

Scalability and security are several aspects that become challenges in developing the Internet of Things (IoT). The weakness of this IoT is that it requires external device intervention in the scalability and security of IoT devices. To solve this problem, Edge computing comes with a promising solution to overcome the weaknesses of cloud computing on a large scale. In order to solve this problem, various studies were carried out and turned blockchain and smart contracts into solutions. Strong security features by applying blockchain technology and smart contracts are solutions in IoT development and Edge computing.

Edge Chain exists as a solution to the scalability and security problems of IoT and Edge computing. Currently, Edge Chain is still only a prototype which is continuously being developed by Jianli Pan et al. on the basis of blockchain and smart contracts [29]. Edge Chain works by integrating the blockchain with a coin system connected to the cloud Edge resource pool, resource usage, and IoT device behavior [29].

The blockchain concept on Edge Chain is implemented in a credit-based resource management system that aims to control all IoT devices from the Edge server. This technology works based on predetermined priority rules. The priority rules include the type and behavior of the application. Meanwhile, the smart contract concept on Edge Chain is used to create rules and policies that each IoT device must implement automatically. Edge Chain works by recording all activities and transactions that occur on IoT devices. This record will be used as a data resource for auditing IoT devices. This Edge Chain technology is one of the solutions in data security for IoT devices with a fairly cheap integration cost [29].

Edge Chain works with an evolutionary and compatible concept. This concept is responsible for some of the advantages of Edge Chain. Edge Chain allows for the evolution of the IoT device paradigm with the old paradigm into a new paradigm that can be automatically installed and updated regularly. This paradigm evolution occurs when audit records that have been carried out before can be compatible to be embedded in new devices. In addition, Edge Chain has the advantage of measuring, monitoring, and controlling the resources of the IoT devices that have been installed. Edge Chain frameworks such as this are achieved through proxies that have worked between old IoT devices and are evolving beyond blockchain technology and installed smart contracts for adoption on new IoT devices. Therefore, with Edge Chain, old IoT devices continue to run transparently with a new paradigm [29].

Through proxies that work between old IoT devices and new IoT devices, old IoT devices do not need to have knowledge of blockchain and smart contracts, but through proxies and new paradigms that have been installed, these devices can still be monitored, managed, and controlled by IoT Edge frameworks, the new one. Even if the device is compromised by hackers, their malicious behavior can be identified, and the damage can be overcome [29].

3.4. Manticore

Manticore is a blockchain-based framework for symbolic execution for binary analysis with a smart contract approach. As one of the symbiotic code testing solutions, Trail of Bits and DARPA Cyber Grand Challenge (CGC) use Manticore technology for code assessment and program analysis. The concept of dynamic symbolic execution is one of Manticore's advantages in analyzing program code by exploring the distance with high-level semantics. The analysis is carried out by exploring each path by taking into account all code with the working principle of dynamic symbolic execution. This procedure is the process of identifying a series of path predicates or providing limits for program testing. In its implementation, the industry has not adopted it much. This is due to the limitations of a flexible and user-friendly tool. In addition, the existing framework is closely related to the traditional execution model, which makes symbolic execution a mere alternative technique, such as the Ethereum platform [30].

The main function of Manticore is as one of the technologies used in program testing with a symbolic execution analysis approach. Manticore can also be used for symbolic execution on alternative execution platforms. In testing program code, Manticore has comparable performance with other standard symbolic execution tools for ordinary binary and an average code coverage of 66% on the basis of the analysis used is smart contracts [30].

In the last decade, there has been much development and interest in research into symbolic execution and there have also been many prominent symbolic execution tools such as KLEE. KLEE is the first and most widely used example of symbolic execution today. Currently, several symbolic execution frameworks are being developed, including: Angr, Triton, binsec, and miasm. This symbolic execution platform is a well-known platform in binary analysis, including the extensive symbolic execution functionality widely used in commercial software auditing [30].

3.5. Smart Contract Online Detection Freamwork against Attacks (SODA)

Smart contracts have become lucrative targets for attackers because they can save a lot of money. Unfortunately, existing offline approaches for discovering vulnerabilities in smart contracts or verifying smart contracts cannot perform the online detection of invading transactions. In addition, existing online approaches only focus on certain attacks and cannot easily be extended to detect other attacks. Plus, developing a new online detection system for smart contracts from scratch is time consuming and requires an in-depth understanding of the blockchain's internals, making it difficult to implement new attack detection mechanisms quickly [31].

The smart contract online detection framework against attacks (SODA) is a new generic online detection framework on all blockchains that supports the Ethereum virtual machine (EVM). SODA differs from existing online approaches in its capabilities, efficiency and compatibility. First, SODA empowers users to easily develop applications to detect various online attacks (i.e., when an attack occurs) by separating information gathering and attack detection with a layered design. At a higher layer, SODA provides a unified interface for developing various attack detection applications, at the lower level, SODA instructs the EVM to gather all the primitive information needed to detect various attacks and build 11 types of structural information for ease of application development. Based on SODA, users can develop new applications in a few lines of code without modifying the EVM. Second, SODA is efficient because it is designed as on-demand information retrieval to reduce additional expenses for information gathering and adopts dynamic linking to eliminate additional expenses from inter-process communication. This design allows users to develop detection applications using any programming language that can generate dynamic link libraries. Third, as more and more blockchains adopt EVM as the smart contract runtime, SODA can easily be migrated to the blockchain without needing to modify the application. From SODA to date, eight detection applications have been developed to detect attacks that exploit major vulnerabilities in smart contracts, and integrate SODA (including all applications) into three popular blockchains: Ethereum, Expanse, and Wanchain. Extensive experimental results show the effectiveness and efficiency of SODA in detection applications [31].

3.6. D-GIS

Blockchain technology enables the creation of a decentralized environment, where cryptographically validated transactions and data are not under the control of any third-party organization. Every transaction that has been completed is recorded in an immutable ledger in a way that is verifiable, secure, transparent and permanent, with a time stamp and other details.

D-GIS is a decentralized application, meaning that nobody has it and everyone can benefit from it. E Leka et al. conducted a study proposing a design methodology for smart contracts to implement a D-GIS project that would allow geologists and engineers to share data and geo-spatial studies in the most efficient way possible [32]. The research focused mainly on several coding approaches related to smart contracts, by looking at the advantages and disadvantages of each of these approaches. Its main purpose is to identify the specific methodology used in the DApp, which will allow it to reach Ethereum's strongest pillar and in turn develop a more secure experience for the end user. The research built a ranking system based on the points (tokens) won by contributing to the community; the bigger the contribution, the greater the user's reputation in the community. When someone casts a vote, the sound is equivalent to their strength in the network. Due to this fact, nothing can manipulate the will of the community for certain decisions it makes [32]. A summary Smart Contract Framework and Its Application can be seen in Table 1.

Table 1. Smart Contract Framework and Its Application.

Article	Year of Publication	Framework	Properties				
			Purpose	**Methods**	**Simulation**	**Domain**	**Status**
[26]	2018	eGov-DAO	eGov-DAO proposes real-time monitoring and analysis of e-government services.	Blockchain technology and decentralized autonomous organization (DAO).	Demonstrating a service that allocates public contracts to specific vendors.	E-Goverment	Prototype (Research still ongoing)
[28]	2019	Virtual Operation Model	Blockchain-oriented dynamic modeling with a Virtual Operation Model that supports the storage and use of information about the supply chain.	Blockchain-oriented dynamic modelling.	Virtual Operation Model demonstrates scheduling control with virtual operation modeling.	Suply Chain	Prototype (Research still ongoing)
[29]	2018	EdgeChain	Edge-IoT, which adopts an evolutionary and backward compatible approach, and supports IoT applications.	Uses a proxy that works between legacy IoT devices and the blockhcain module and smart contracts.	Demonstrating a testing program code with a symbolic execution analysis approach.	Internet of Things	Prototype (Research still ongoing)
[30]	2019	Manticore	Open source dynamic symbolic execution.	Maximizes code coverage in software tests through dynamic symbolic execution.	Demonstrates the ability to find bugs and verify code correctness for commercial kline.	Software Tests	Theoretical description
[31]	2020	SODA	Smart contract online detection framework against attacks protects smart contracts from attacks.	Generic online detection.	There are 8 applications with new detection methods to detect attacks on smart contracts.	Cyber Security	Theoretical description
[32]	2019	D-GIS	Store and share geospatial data.	TxtStreamers to vote on storage reputation and proxy contracts.	A Decentralized Application (DApp).	Geographic Information System	Theoretical description

4. Conclusions

Smart contracts are cutting-edge technologies that continue to develop in terms of frameworks, methods and applications. Smart contract developments are predicted to be able to provide solutions to trust and legality that work automatically on the basis of transparency. Smart contracts are also predicted to develop to solve problems in various domains, such as: e-government, supply chain, Internet of Things, software tests, cyber security, geographic information systems and others. As an initial exploratory study, Table 1 shows some of the frameworks and applications for smart contract development in various domains.

Author Contributions: Writing—original draft, E.S.N.; writing—review & editing, E.S.N.; A.N.H.; R.A.; R.S. All authors have read and agreed to the published version of the manuscript.

Funding: Ministry of Research and Technology/National Research and Innovation Agency for research funding assistance through the Post-Doctoral Research scheme in 2020–2021.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Thank you to the Ministry of Research and Technology/National Research and Innovation Agency for research funding assistance through the Post-Doctoral Research scheme in 2020.

Conflicts of Interest: The authors declare that there is no conflict of interest in this paper.

References

1. Giancaspro, M. Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Comput. Law Secur. Rev.* **2017**, *33*, 825–835. [CrossRef]
2. Hiroki, W.; Fujimura, S.; Nakadaira, A.; Miyazaki, Y.; Akutsu, A.; Kishigami, J. Blockchain contract: Securing a blockchain applied to smart contracts. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–11 January 2016; pp. 467–468.
3. Sanel, H.; Ertem, N. An explorative paper on speculative approaches to smart contracts. *Prague Econ. Pap.* **2020**, *29*, 469–480.
4. Negara, E.S.; Hidyanto, A.N.; Andryani, R.; Erlansyah, D. A survey blockchain and smart contract technology in government agencies. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2021; Volume 1071, p. 012026.
5. Zibin, 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.
6. Chitu, O.; Schabram, K. A guide to conducting a systematic literature review of information systems research. *Sprouts Work Pap. Inf. Syst.* **2010**, *10*, 10–26.
7. Jane, W.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, 13–23.
8. Pearl, B.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. essons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583.
9. Dmitry, E.; Roschin, P. The all-pervasiveness of the blockchain technology. *Procedia Comput. Sci.* **2018**, *123*, 116–121.
10. Shuai, W.; Yuan, Y.; Wang, X.; Li, J.; Qin, R.; Wang, F.-Y. An overview of smart contract: Architecture, applications, and future trends. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018.
11. Everett, H.; Saxena, M.; Rodrigues, N.; Zhu, X.; Daian, P.; Guth, D.; Moore, B. Kevm: A complete formal semantics of the ethereum virtual machine. In Proceedings of the 2018 IEEE 31st Computer Security Foundations Symposium (CSF), Oxford, UK, 9–12 July 2018.
12. Ahmed, K.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016.
13. Imran, B. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*; Packt Publishing Ltd.: Birmingham, UK, 2018.
14. Khaled, S.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. *IEEE Access* **2019**, *7*, 10127–10149.
15. Christian, S.; Waltl, B.; Sillaber, C.; Waltl, B. Life cycle of smart contracts in blockchain ecosystems. *Datenschutz Und Datensicherheit-DuD* **2017**, *41*, 497–500.
16. Massimo, B.; Pompianu, L. An empirical analysis of smart contracts: Platforms, applications, and design patterns. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017.
17. Pierluigi, C. Beyond bitcoin: An early overview on smart contracts. *Int. J. Law Inf. Technol.* **2017**, *25*, 179–195.

18. Steve, O. Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters* **2014**, *1*, 19–21.
19. Natalie, B.; Sandner, P. The blockchain technology in the media sector. In *Media Trust in a Digital World*; Springer: Cham, Switzerland, 2019.
20. Gavin, W. A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
21. Vikram, D.; Metcalf, D.; Hooper, M. The hyperledger project. In *Blockchain Enabled Applications*; Apress: Berkeley, CA, USA, 2017; pp. 139–149.
22. Philip, T.; Brown, R.G.; Yang, D. Blockchain technology in finance. *Computer* **2017**, *50*, 14–17.
23. Yong, Y.; Wang, F.-Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016.
24. Lemuria, C.; Ubacht, J. Blockchain applications in government. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, Delft, The Netherlands, 30 May–1 June 2018.
25. Ioannis, T.; Bechtsis, D.; Kompatsiaris, I. Moving from e-Gov to we-Gov and beyond: A blockchain framework for the digital transformation of cities. In *Smart Cities in the Post-Algorithmic Era*; Edward Elgar Publishing: Cheltenham, UK, 2019.
26. Nour, D.; Shi, W.; Xu, L.; Gao, Z.; Chen, L.; Lu, Y.; Shah, N. eGov-DAO: A better government using blockchain based decentralized autonomous organization. In Proceedings of the 2018 International Conference on eDemocracy & eGovernment (ICEDEG), Ambato, Ecuador, 4–6 April 2018.
27. Mark, D. Does contracting out increase the efficiency of government programs? Evidence from Medicaid HMOs. *J. Public Econ.* **2004**, *88*, 2549–2572.
28. Alexandre, D.; 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.
29. Jianli, P.; 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.
30. Mark, M.; Manzano, F.; Hennenfent, E.; Groce, A.; Grieco, G.; Feist, J.; Brunson, T.; Dinaburg, A. Manticore: A user-friendly symbolic execution framework for binaries and smart contracts. In Proceedings of the 2019 34th IEEE/ACM International Conference on Automated Software, San Diego, CA, USA, 11–15 November 2019.
31. Ting, C.; Cao, R.; Li, T.; Luo, X.; Gu, G.; Zhang, Y.; Liao, Z. A generic online detection framework for smart contracts. In Proceedings of the 27th Network and Distributed System Security Symposium, San Diego, CA, USA, 23–26 February 2020.
32. Leka, E.; Lamani, L.; Selimi, B.; Deçolli, E. Design and implementation of smart contract: A use case for geo-spatial data sharing. In Proceedings of the International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019.