

Review

# Blockchain Technology Application in Security: A Systematic Review

Nazanin Moosavi <sup>1</sup> and Hamed Taherdoost <sup>2,3,\*</sup> 

<sup>1</sup> Research and Development Department, Hamta Business Corporation, Vancouver, BC V6E 1C9, Canada; nazanin@hamta.ca

<sup>2</sup> Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada

<sup>3</sup> Q Minded Quark Minded Technology Inc., Vancouver, BC V6E 1C9, Canada

\* Correspondence: hamed.taherdoost@gmail.com or hamed@hamta.org

**Abstract:** Blockchain technology is a promising technology that attracts popularity among researchers. However, it was first introduced with digital currencies, particularly Bitcoin, but nowadays, it is also known as one of the most frequently used techniques for securing networks. This systematic review research identifies studies that use blockchain for their security challenges. In addition, different fields in blockchain usage, blockchain categorization type, consensus mechanism, smart contract usage, and integration with other software-based algorithms are also investigated. Our results maintain that the Internet of Things (IoT) is the main field in which blockchain provides security.

**Keywords:** blockchain technology; blockchain security solutions; Internet of Things (IoT); healthcare; consensus mechanisms; smart contracts

## 1. Introduction



**Citation:** Moosavi, N.; Taherdoost, H. Blockchain Technology Application in Security: A Systematic Review.

*Blockchains* **2023**, *1*, 58–72. <https://doi.org/10.3390/blockchains1020005>

Academic Editors: Keke Gai and Liehuang Zhu

Received: 23 August 2023

Revised: 20 October 2023

Accepted: 27 October 2023

Published: 29 October 2023



**Copyright:** © 2023 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/>).

Blockchain technology is a novel idea that was first introduced by Satoshi Nakamoto with the invention of the Bitcoin [1]. Bitcoin is a digital currency that has revolutionized financial trading. Blockchain is a distributed Hyperledger technology with many intrinsic features, including security, decentralization, transparency, immutability, and provenance [2–4]. These features create unique blockchain applications beyond the financial market.

Blockchain is categorized into three types: public, private, and consortium. Public blockchains are permissionless blockchains where every user can enter the network, compared to the private network, where only authorized users by one organization can access the network. A consortium blockchain is a combination of public and private where there is more than one organization in the network. The best selection of blockchain categorization type according to various requirements and conditions of different use cases is very important [5,6].

Consensus mechanisms are a feature that provides a fair and decentralized network. The main goal of the consensus algorithm is to reach consensus without the need for a central authority or third parties, which makes the blockchain decentralized [7]. There are different techniques for reaching consensus, such as proof of work (PoW), which is the most famous algorithm and is used in the Bitcoin network, Practical Byzantine Fault Tolerance (PBFT), and proof of authority (PoA). Each algorithm has its own features, specific time, and energy consumption. Consequently, choosing the right consensus algorithm depends on the specific needs of the project's applications.

Nowadays, blockchain is widely used in a variety of areas such as the Internet of Things (IoT), healthcare, energy market, and industrial projects to provide solutions for their security attacks and challenges, and there is an increasing trend of using blockchain to provide security frameworks in different fields [8–12].

This systematic review focuses on recent research that applied blockchain as their security framework and concerns their categorization type, consensus algorithms, usage of smart contracts, and integration with other technologies. We deeply investigate this area and use our insight to propose future research for scholars and academics interested in working in this field.

### 1.1. Related Articles

To the best of our knowledge of blockchain application in security, very few systematic reviews deeply consider this topic from different aspects, as we have in our work.

Authors in [13] provide a systematic review of blockchain cybersecurity. They highlight the potential application of blockchain as security in different fields, such as IoT, networks, and data storage. This article covers subjects from cryptography to IoT technology security and data storage security, whereas issues, challenges, and future research topics are also recognized. However, this study has no analysis for categorization types, consensus algorithms, smart contract usage, or integration with other technologies.

Article [14] systematically reviewed security solutions in Industry 4.0. They investigated security schemes for autonomous vehicles (AVs) and explored how blockchain can overcome AV cyberattacks. They do not have an exploration of other fields or any analysis of blockchain structure.

Some papers survey blockchain security, such as [15–17], which focus on blockchain applications in IoT and provide an overview to enhance IoT security and improve privacy, or [18], which provides tutorials for green IoT-based agriculture challenges and blockchain solutions. However, they need a general overview of blockchain security applications in various use cases.

All the mentioned works try to answer questions about the security application of blockchain technology. However, they need to provide specific and deep analysis in the blockchain security field to improve security solution performance. It is noticed that since blockchain is still in its infancy and has a short history, it is necessary to investigate a new review of recent works specifically in the scope of blockchain and security solutions to orient research.

### 1.2. Research Goals and Motivation

The main motivation for this study is to analyze research works on blockchain applications in security for different use cases and to summarize recent efforts in these fields. To be more focused, we have provided a list of the research questions to be answered in this study as follows:

- What prominent domains employ blockchain security applications and their specific use cases?
- What are the prevailing consensus mechanisms in use?
- What influences the selection of blockchain types?
- How do smart contracts bolster blockchain security?
- Which software-based technologies are integrated with blockchain to enhance security?

### 1.3. Contributions

We systematically review blockchain technology security applications from 2018 to April 2022. Our study contributes to a detailed understanding of blockchain applications in different fields and industries. Our key contributions are as follows:

- We selected 54 articles relating to blockchain applications in security solutions.
- We organized a complete data analysis within selected articles to propose their research idea and considerations in blockchain security applications.
- We offered a meta-analysis concerning mechanisms in which blockchain technology is used to overcome security challenges.
- We proposed future research and topics for further investigation around security topics in blockchain applications.

#### 1.4. Paper Outline

The remainder of this paper is written as follows: Section 2 discusses the systematic review methodology, Section 3 outlines the key findings of the review, Section 4 presents a discussion of the main results of our work and future research, and, finally, Section 5 concludes this survey by presenting a summary of the contributions.

### 2. Methodology

This section explains the procedure used to select the articles for a systematic review. We plan to proceed with selecting papers and organizing and presenting parts of the review iteratively to have a complete evaluation for the systematic review.

#### 2.1. Primary Selection

Primary selection was conducted using the following keywords that are mostly related to our research questions:

“Blockchain” AND (“Security” OR “Cybersecurity” OR “Information Security”)

The search engine was the IEEE Xplore and the Elsevier database was used. Only peer-reviewed and journal papers from 2018 to April 2022 were selected. 6337 papers were selected in this stage. Then, we applied another selection processes where the keywords should only appear in the papers’ titles, abstracts, or keywords. In this step, 1842 papers were selected. Next, we searched to have the keywords only in the title. The selection process continued with a total of 170 papers. Then, inclusion/exclusion criteria were applied to filter the results.

#### 2.2. Inclusion and Exclusion Criteria

Studies considered in our systematic review should propose a security solution with blockchain technology. Papers that worked on security aspects of blockchain or papers that have solutions to blockchain security issues are separate from the topic of our study. Table 1 provides the key inclusion/exclusion criteria.

**Table 1.** Inclusion/Exclusion Criteria.

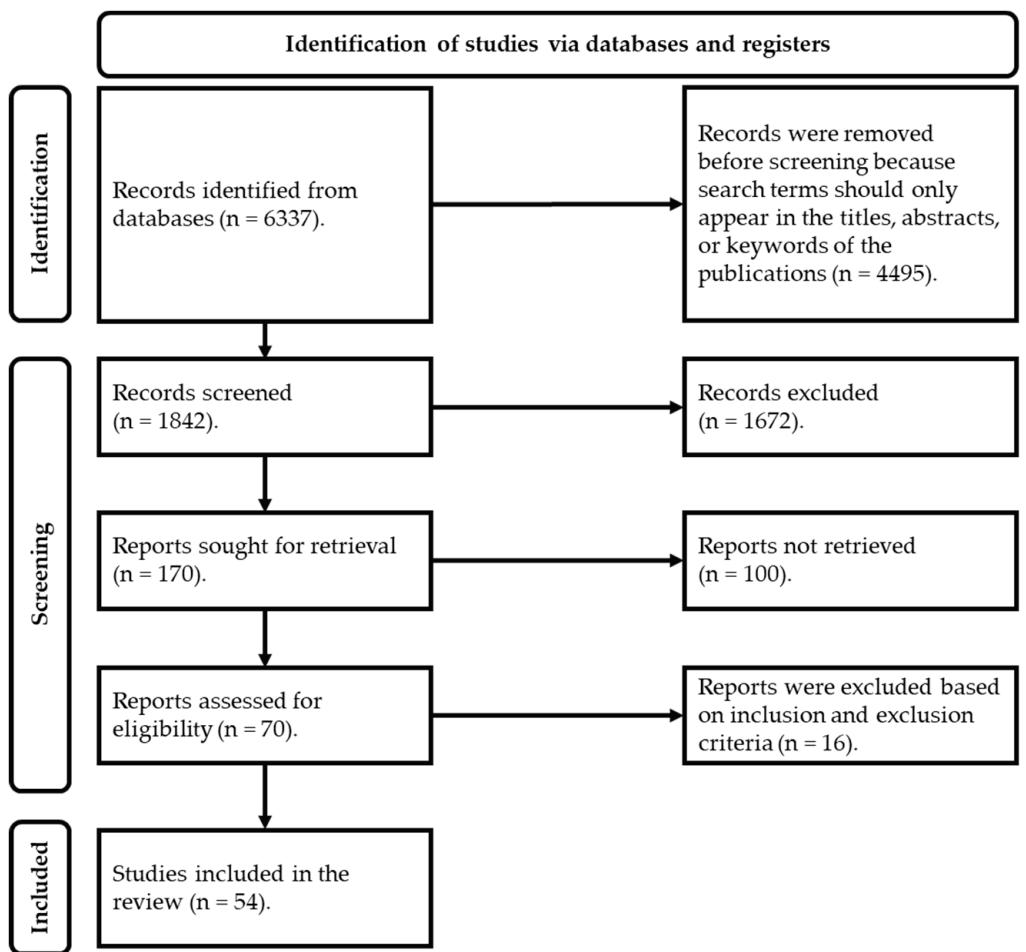
Criteria for Inclusion	Criteria for Exclusion
Papers must propose a security solution with blockchain. Papers must propose some information, including their used blockchain architecture.	Review or survey articles that give a general specific idea about blockchain as a security solution. Papers with no information on research questions. Papers analyzing security topics in blockchain technology. Paper giving solutions for security concerns in the blockchain.

#### 2.3. Selection Results

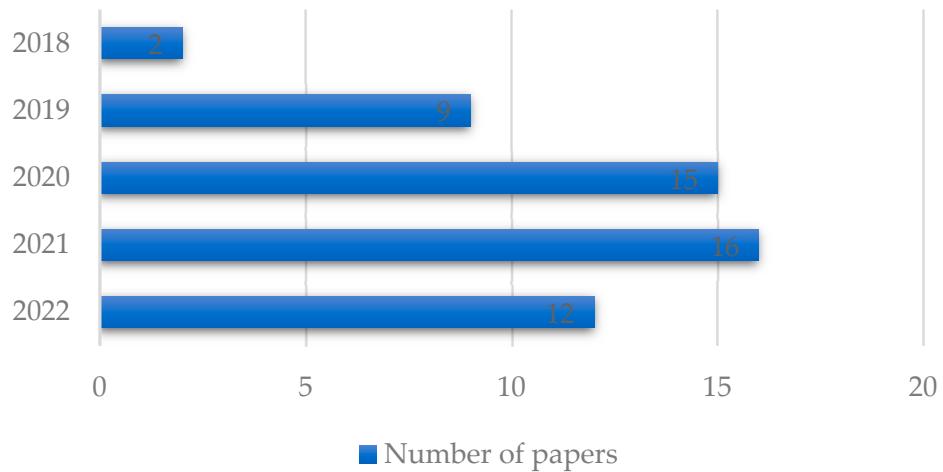
After applying the inclusion/exclusion criteria to the articles, 70 papers remained for further reading. The 70 papers were fully read, with the inclusion/exclusion criteria applied again. Finally, 54 papers are included in this systematic review (Figure 1).

#### 2.4. Publication Year

Figure 2 shows the number of publications each year. It is obvious from the figure that blockchain is an upward trend, and, each year, the number of papers is increasing. Also, the number of papers published in the first month of 2022 is more than half of the total papers published in 2021, which shows the interest in this topic in recent years.



**Figure 1.** PRISMA flowchart for selecting included papers.



**Figure 2.** Publication year.

### 3. Findings

All the selected papers have been fully read and the related data about the field of the blockchain usage application, the category type, consensus algorithms, usage of smart contracts, and the integration with other technologies are fully investigated and given in Table 2.

**Table 2.** The main findings of the study.

Ref	Data	Application Field	Category Type	Consensus Algorithm	Smart Contract	Integration with Other Tech
[19]	Blockchain ensures data privacy and confidentiality and manages resources against untrusted users.	IoT (healthcare)	Private	Time-dependent Consensus Algorithm	Yes	SDN/Fog computing
[20]	A lightweight blockchain is designed to enable the IoT domain to deploy its blockchain network on its IoT devices on the Hyperledger Fabric blockchain platform.	IoT	Consortium (HLF)	PBFT	Yes	-
[21]	A security framework as a distributed blockchain-based Platform-as-a-Service (PaaS) model is implemented to ensure data confidentiality, detect a security attack, and authorize its identification.	IoT	Not specified	Not specified	No	Edge/Cloud computing/SDN
[22]	Blockchains secure WSN transmissions, IoT communications, and mobile databases.	IoT (Wireless Sensor Networks)	Public (HLF)	PoW	No	AI
[23]	Ethereum platform is used to authenticate and authorize IoT devices with smart contracts deployed as business logic.	IoT (real-time monitoring)	Private or Consortium (Ethereum)	Not specified	Yes	-
[24]	In smart city use cases, a secure, low-latency blockchain framework is used for drone authentication.	IoT (smart city) UAV	Public	Delegated PoS	No	Drone/UAV
[25]	Providing P2P communication ensures the security of access control for IoT devices and guarantees data privacy.	IoT	Public and private	Customized Consensus Algorithm	Yes	SDN
[26]	A fuzzy logic with blockchain technology is designed to reach Authentication, Authorization, and Audit Logs (AAA) in IoT systems.	IoT (healthcare)	Consortium (HLF)	PBFT	Yes	-
[27]	Secure orchestration is developed in 5G-IoT using blockchain solutions.	5G-IoT	Private	PBFT	Yes	Deep learning/Fog/Edge computing/SDN
[28]	Blockchain is combined with a re-encryption proxy to ensure security criteria, such as confidentiality, integrity, privacy, and access control using smart contracts Ethereum to accelerate data storage.	IoT (healthcare)	Private or Consortium (Ethereum)	Proof of authority (PoA)	Yes	-

**Table 2.** *Cont.*

Ref	Data	Application Field	Category Type	Consensus Algorithm	Smart Contract	Integration with Other Tech
[29]	Blockchain provides a security architecture for UAVs to help decrease security risks.	IoT (UAV)	Public (Ethereum)	PoW	No	Machine learning
[30]	Blockchain proposes a solution for robust authentication of identity and privacy of healthcare data.	IoT (healthcare)	Not specified	Not specified	Yes	Fog computing
[31]	A new routing protocol on blockchain integrated with SDN is presented to mitigate security and energy consumption.	IoT (cyber-physical systems)	Private and public	PoW	Yes	AI/SDN
[32]	Blockchain technology solution with advanced scripts of Solidity and embedded programming is proposed.	IoT (wireless body area network)	Private	Not specified	Yes	-
[33]	A storage mechanism based on blockchain is proposed to ensure security without third-party authority.	IoT	Public	PoW	Yes	-
[34]	A lightweight, scalable blockchain is proposed for IoT requirements and security issues.	IoT	Public	Time-based Consensus Algorithm	No	-
[35]	An efficient, lightweight, integrated blockchain (ELIB) is designed to meet the security needs of blockchain.	IoT (smart home)	Public	Time-dependent Consensus Algorithm	No	-
[36]	The blockchain solution is proposed to secure the storage system for IoT device location information to aid in sharing services.	IoT	Private Public Consortium	PBFT	Yes	-
[37]	Blockchain is used to decrease a single point of failure in the system.	IoT	Private (Ethereum)	Not specified	Yes	SDN/Fog/Edge
[38]	A secure sharing protocol with blockchain technology for electronic health records is implemented.	Healthcare	Consortium (Ethereum)	PoA	Yes	-
[39]	Blockchain is used to enhance the security of the task-offloading system.	Healthcare	Not specified	PBFT	No	Reinforcement learning/Edge computing/VR
[40]	The proposed blockchain provides a decentralized solution to avoid failure and provide tamper-proof healthcare ledgers.	Healthcare	Public	PoW	No	-

**Table 2.** Cont.

Ref	Data	Application Field	Category Type	Consensus Algorithm	Smart Contract	Integration with Other Tech
[41]	A triple encryption authentication architecture using blockchain is developed to secure the sharing of personal data.	Healthcare	Private	PoA	No	-
[42]	Data storage and data transmission are secured with blockchain technology.	IoT (healthcare)	Not specified	Not specified	No	Cloud computing
[43]	Medical data processing is secured with blockchain.	Healthcare	Consortium	PBFT	No	Cloud computing
[44]	The blockchain solution is proposed for the secure management of medical big data.	Healthcare	Public (Ethereum)	PoW	Yes	-
[45]	Blockchain framework used to secure patients' medical data.	Healthcare	Public	PoW	No	-
[46]	A new verification scheme with blockchain is designed to detect corruption in data in cloud servers.	Healthcare	Private	PoW	No	Cloud computing
[47]	A distributed network with blockchain is introduced to reshape the traditional industrial IoT architecture.	IoT (industrial)	Private	PoW	No	Edge computing
[48]	Blockchain provides decentralized and secure control for cyber-physical systems in the industry.	IoT (industrial)	Private (Ethereum)	PoW	Yes	Edge computing
[49]	Operational data records in industrial systems are secured with blockchain.	Industry	Private	PoA	Yes	-
[50]	Transactions in energy trading systems are secure and private with blockchain technology.	Energy	Private	PoW	Yes	-
[51]	Blockchain provides a charging framework for electric taxis to handle charging disconnections and trust challenges among charging stations.	Energy	Consortium	PBFT	Yes	SDN
[52]	Fault identification and secure and reliable store measurement data in smart grids are developed with blockchain.	Energy	Private	PBFT	Yes	-

**Table 2.** Cont.

Ref	Data	Application Field	Category Type	Consensus Algorithm	Smart Contract	Integration with Other Tech
[53]	Blockchain is used to provide an electricity market framework for energy transactions.	Energy	Public	Not specified	No	-
[51]	Blockchain is used to provide an energy trading framework that is designed for secure and optimal trading of AC microgrids.	Energy	Public	Not specified	No	-
[54]	Enhancing the security of smart microgrids using blockchain.	Energy	Private/Consortium	PoA	No	Deep learning
[55]	The vehicle trust management system is designed with blockchain to evaluate message sources.	Transportation	Public	PoW	No	-
[56]	A decentralized, secure model and authentication mechanisms for a lightning network with smart contracts are provided.	Energy	Private	PoA	Yes	-
[57]	The digital signature technique of blockchain ensures reliability and integrity.	Transportation	Consortium	PoW	Yes	-
[58]	A secure and distributed model for intelligent traffic light systems is proposed.	Transportation	Not specified	PBFT	Yes	Edge computing
[59]	A trust management system with blockchain is introduced for the internet of vehicle systems.	Transportation	Consortium (HLF)	PBFT	No	Fog/Edge computing
[60]	Blockchain guarantees agriculture information preservation and accuracy.	IoT (agriculture)	Private	Not specified	Yes	-
[61]	Smart home security is fulfilled using blockchain.	Smart home	Consortium	PoW	No	-
[62]	Cloud relational database is secured with blockchain-based systems.	Cloud computing Database	Not specified	PBFT	No	Cloud computing
[63]	Blockchain is used to maintain the privacy of sensitive data.	Cloud server	Private (HLF)	Not specified	No	Cloud computing
[64]	Blockchain warrants the security of image data.	Cloud Image data sharing	Not specified	Not specified	Yes	Cloud computing

**Table 2.** Cont.

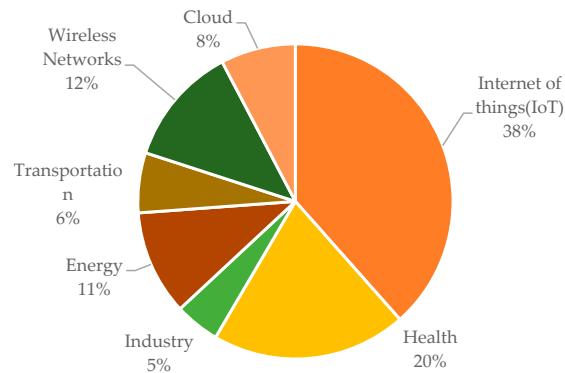
Ref	Data	Application Field	Category Type	Consensus Algorithm	Smart Contract	Integration with Other Tech
[65]	A fully decentralized approach by eliminating the third party in the network is designed using blockchain.	Edge computing	Consortium	Not specified	No	Edge computing
[66]	Blockchain provides a secure architecture for secure cloud schedulers.	Cloud computing	Public	Proof-of-schedule	No	Cloud computing
[67]	Proposing a solution to improve security and privacy in UAVs.	IoT (UAV)	Public	Not specified	Yes	Cloud computing
[68]	Compromised UAVs are detected based on trust policies with blockchain.	UAV	Consortium (HLF)	Not specified	No	--
[69]	Data transmission security in satellite networks is enhanced with blockchain.	Satellite network	Public	Context-based Consensus Algorithm	No	-
[70]	Security issues due to heterogeneous standard integration and access delegations in 6G are mitigated via blockchain.	6G	Not specified	Not specified	No	Machine learning/SDN
[71]	Blockchain provides a security mechanism that creates a trust-based filtration to decrease malicious traffic.	IoT/SDN	Consortium	Not specified	No	SDN

Figure 3 shows the percentage of different fields of blockchain usage as a security solution in various works. Of all the studies, 38% concern IoT security. ‘Health’ is the second most common with 20%. Generally, healthcare has also gained much attention from blockchain research and security. ‘Wireless Networks’, including wireless sensor networks, satellite communications, UAVs, 5G, and 6G networks, are next, attracting 12% of the research. ‘Energy’ with 11% and ‘Transportation’ with 6% follow. The next is the ‘Cloud’ with 8%, and the last is solutions for ‘Industry’ with a portion of 5%.

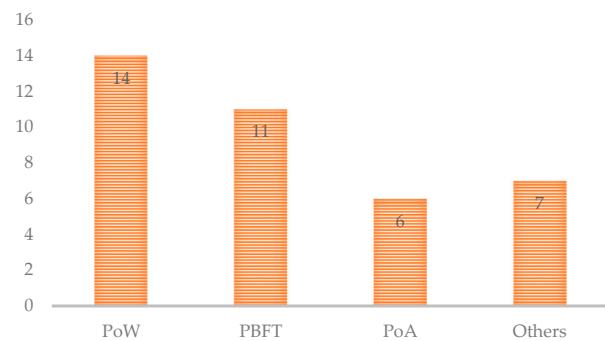
The next results focus on the most consensus algorithm used in the research (Figure 4). Some information about their consensus algorithm was provided in 38 papers, and others do not mention their consensus mechanism. Proof of work (PoW) is the consensus algorithm widely used in Bitcoin and other blockchain networks. Our results show that it is also widely used in blockchain security applications. However, it needs much computational power, and its algorithm is more popular. The next one is the PBFT algorithm, mostly used in private and consortium blockchains and needs less computational power than PoW. Proof of authority appeared the third most and is an algorithm mostly used in permissioned blockchains. It provides many advantages such as speeding up the consensus process, so it does not need huge computing, and data storage is also accelerated. Some novel consensus algorithms are based on time or capacity and are used based on the requirements in each use case.

The next result concerns the blockchain categorization types used in studies (Figure 5). The percentage of different blockchain types is 38% for private, 35% for public, and 27% for the consortium, a combination of public and private. The results show that researchers

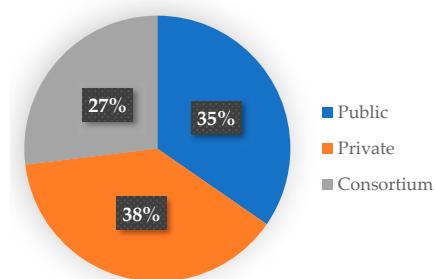
are still working on the specification of each type, and there should be more work to fully understand each type and its usage in different use cases.



**Figure 3.** Blockchain application fields.



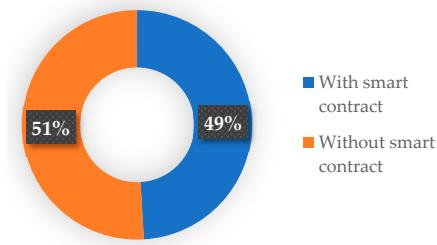
**Figure 4.** Consensus Algorithms.



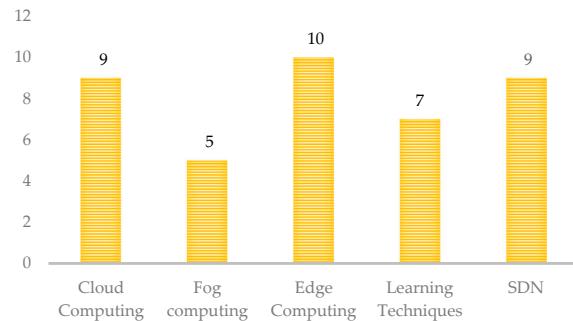
**Figure 5.** Blockchain categorization type.

In this systematic review, we focused on the usage of smart contracts to answer the question of how many papers used smart contracts in their blockchain security solutions (Figure 6). The results show that almost half of the papers used smart contracts in their solutions, and other blockchain security solutions focus on the other features of the blockchain to provide security.

Ultimately, we focus on integrating blockchain and other technologies, which results in better security solutions (Figure 7). Around half of the papers used other technologies integrated with blockchain to provide solutions. Cloud, fog, and edge computing are the most common technologies to be used with blockchain. Since blockchain is a software-based technology, its integration with these cloud-based technologies and software-defined networking (SDN) can provide applicable security solutions with better resource allocation, low-delay services, and data storage. Although artificial intelligence and machine learning techniques are technology trends these days, some of the papers proposed solutions with the integration of blockchain and learning techniques.



**Figure 6.** Smart contract usage.



**Figure 7.** Integration with other technologies.

#### 4. Discussion

The main goal of this paper is to provide a systematic review of practical applications of blockchain usage as a security solution with an in-depth analysis of their blockchain architectures. Hence, the selected papers are investigated based on this goal. One of the important notes about blockchain solutions to be applied is the use of some well-established, ready-to-use, and open-source platforms such as Ethereum and Hyperledger Fabric (HLF). Ethereum is a decentralized peer-to-peer blockchain platform that executes application codes called smart contracts securely. Paper [23] uses its decentralized authentication technique for IoT devices in the Ethereum platform with a smart contract that is automatically run in the Ethereum. Authors [38] provide a secure sharing protocol with blockchain technology for electronic health records written into smart contracts using solidity language and run on the Ethereum blockchain. HLF platform supports multiple blockchain ledgers, and only some verified users can store the data in the corresponding blockchain ledgers. Paper [20] provides a lightweight blockchain with HLF for IoT networks. Some of the most practical and implement-ready blockchain solutions were those implemented on Ethereum or HLF platforms.

Next, we are focusing on providing rigid solutions for each research question.

- What prominent domains employ blockchain security applications and their specific use cases?
  - IoT: IoT networks are in the first stage of blockchain application usage in security. The most use cases of blockchain security solutions for IoT networks are for authentication and authorization of devices [24,26] and for providing a secure network for data confidentiality [28,30].
  - Healthcare: blockchain is mostly used to guarantee the privacy of personal healthcare data storage and management [38,43].
  - Wireless network: securing data transmission [69] and user authentication are the most common blockchain usage in wireless networks [24].
  - Energy: securing energy trading in energy markets [50,51] and enhancing the security of smart grids [54] is accomplished with blockchain networks.
- What are the prevailing consensus mechanisms in use?

From the results, it is obvious that PoW is still the favorite consensus algorithm among researchers. Although PoW is the most powerful computing algorithm, since it is simpler

to deploy and more mature, it is widely used in different use cases. However, for some use cases, such as IoT networks, the PoW mechanism is not a good idea since IoT devices have limitations in computing power. Based on the above studies, only four IoT articles use PoW, and others use PBFT [20,26,27] or some context-based consensus mechanisms [25,34]. The Proof of Authority (PoA) algorithm aims to set up an authorized node to build all the other blocks to reduce the building block time [41]. It is faster and highly secure compared to PoW; consequently, it is preferred to be used in some networks [28,38].

#### C. What influences the selection of blockchain types?

There is no popular type within considered articles in our systematic review. It can be concluded that authors select blockchain types by considering their requirements and users' permission to access networks before researchers select their appropriate type. For example, [18,19,25,26] latency is an important subject in [17,24]. Hence, the authors use private and consortium blockchains instead of public, where the process in public is slower than in others. Additionally, in [27], the power consumption problem is so important that the authors decided to use two kinds of nodes, full and light, with different responsibilities to decrease the power consumed in each node. Hence, the choice of private blockchain is meaningful.

#### D. How do smart contracts bolster blockchain security?

Smart contracts are rules that run automatically when some conditions happen. Due to its function, the authors decided to use it to ensure the automatic implementation of some logic in their framework. For example, authors in [28] used smart contracts as a rule for controlling access in the network, and authors in [56] use it for authentication or authorization of devices.

#### E. Which software-based technologies are integrated with blockchain to enhance security?

Blockchain is a software-based technology. Hence, its integration with other software-based technologies can provide remarkable solutions. Based on our systematic review, many articles integrate blockchain with computing techniques. Edge computing is most common, along with cloud and fog computing. Researchers in [62] integrated cloud computing with blockchain to secure data storage and detect and prevent erroneous cloud relational database manipulation. In [27], authors proposed a security blockchain solution for edge nodes since edge computing in the edge nodes is very vulnerable to attacks, and a blockchain solution can secure this communication. Learning techniques and software-defined networking (SDN) are the next steps. In [25], researchers provide integration of SDN and blockchain to balance security and minimize energy consumption for IoT applications.

#### *Future Research*

One of the main drawbacks of using blockchain technology in different systems is increasing latency and power consumption. This causes many problems, especially in IoT networks, where the power computation of devices is so low. Some techniques to overcome these problems include using consensus techniques designed to speed up the process with less computing power, such as PoA [28,54,56]. In addition, some papers use different techniques to overcome these issues. Authors in [19] provide blockchain sharding techniques to reduce latency, and researchers in [26] try to increase the block sizes to reduce latency. Hence, potential future research should focus on working on new techniques to decrease latency and power consumption to make blockchain usage applicable in different situations.

As noted in the first section, several studies use Ethereum and Hyperledger platforms to propose security solutions for their problems [20,23,38]. Potential future research can provide a review study on using these platforms for security solutions with their strengths and weaknesses.

## 5. Conclusions

This systematic review has comprehensively reviewed available studies on blockchain applications for security solutions. Research studies report that blockchain applications can bring possible security solutions for different use cases such as IoT, healthcare, industry, energy, etc. In addition, there is an analysis of blockchain categorization type (public, private, consortium), various consensus algorithms (PoW, PBFT, PoA), usage of blockchain open platforms such as Ethereum and Hyperledger Fabric, and blockchain integration with other software-based technologies. Moreover, future research potential is also given to scholars searching for new fields.

This systematic review is proposed as a reference for researchers working on blockchain security applications to better decide on adopting blockchain technology as a security solution. As a result, we encourage future research to address security subjects in this technology and suggest that research scholars and business sectors work together to propose movable security solutions in this field.

**Author Contributions:** Conceptualization, N.M.; methodology, H.T.; validation, H.T.; formal analysis, H.T. and N.M.; resources, N.M.; writing—original draft preparation, N.M. and H.T.; writing—review and editing, N.M.; visualization, N.M.; supervision, H.T. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** Author Nazanin Moosavi was employed by the company Hamta Business Corporation. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## References

1. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, *21260*. [[CrossRef](#)]
2. Niranjanamurthy, M.; Nithya, B.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Clust. Comput.* **2019**, *22*, 14743–14757. [[CrossRef](#)]
3. Amirifard, M.; Taherdoost, H. Employment of Blockchain Technology in the Field of Renewable Energy. In Proceedings of the International Conference Interdisciplinarity in Engineering, Târgu Mureş, Romania, 6–7 October 2022; Springer: Berlin/Heidelberg, Germany, 2022.
4. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain meets cloud computing: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [[CrossRef](#)]
5. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
6. Taherdoost, H. Blockchain technology and artificial intelligence together: A critical review on applications. *Appl. Sci.* **2022**, *12*, 12948. [[CrossRef](#)]
7. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. [[CrossRef](#)]
8. Gai, K.; Wu, Y.; Zhu, L.; Zhang, Z.; Qiu, M. Differential privacy-based blockchain for industrial internet-of-things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4156–4165. [[CrossRef](#)]
9. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [[CrossRef](#)]
10. Taherdoost, H. A critical review of blockchain acceptance models—Blockchain technology adoption frameworks and applications. *Computers* **2022**, *11*, 24. [[CrossRef](#)]
11. Gai, K.; She, Y.; Zhu, L.; Choo, K.-K.R.; Wan, Z. A blockchain-based access control scheme for zero trust cross-organizational data sharing. *ACM Trans. Internet Technol.* **2023**, *23*, 1–25. [[CrossRef](#)]
12. Taherdoost, H. Smart Contracts in Blockchain Technology: A Critical Review. *Information* **2023**, *14*, 117. [[CrossRef](#)]
13. Taylor, P.J.; Dargahi, T.; Dehghanianha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [[CrossRef](#)]
14. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717. [[CrossRef](#)]
15. Da Xu, L.; Lu, Y.; Li, L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473.
16. Ferrag, M.A.; Shu, L. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet Things J.* **2021**, *8*, 17236–17260. [[CrossRef](#)]

17. Shammar, E.A.; Zahary, A.T.; Al-Shargabi, A.A. A Survey of IoT and Blockchain Integration: Security Perspective. *IEEE Access* **2021**, *9*, 156114–156150. [[CrossRef](#)]
18. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [[CrossRef](#)]
19. Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2021**, *27*, 760–776. [[CrossRef](#)]
20. Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain. *IEEE Access* **2021**, *9*, 36868–36878. [[CrossRef](#)]
21. Medhane, D.V.; Sangaiah, A.K.; Hossain, M.S.; Muhammad, G.; Wang, J. Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach. *IEEE Internet Things J.* **2020**, *7*, 6143–6149. [[CrossRef](#)]
22. Hsiao, S.-J.; Sung, W.-T. Employing blockchain technology to strengthen security of wireless sensor networks. *IEEE Access* **2021**, *9*, 72326–72341. [[CrossRef](#)]
23. Mohanta, B.K.; Jena, D.; RamasubbaReddy, S.; Daneshmand, M.; Gandomi, A.H. Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet Things J.* **2020**, *8*, 881–888. [[CrossRef](#)]
24. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [[CrossRef](#)]
25. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.-K.R. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [[CrossRef](#)]
26. Zulkifl, Z.; Khan, F.; Tahir, S.; Afzal, M.; Iqbal, W.; Rehman, A.; Saeed, S.; Almuhaideb, A.M. FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs. *IEEE Access* **2022**, *10*, 15644–15656. [[CrossRef](#)]
27. Rathore, S.; Park, J.H.; Chang, H. Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. *IEEE Access* **2021**, *9*, 90075–90083. [[CrossRef](#)]
28. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egypt. Inform. J.* **2022**, *23*, 329–343. [[CrossRef](#)]
29. Abualsaoud, E.H. A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. *Comput. Electr. Eng.* **2022**, *99*, 107847. [[CrossRef](#)]
30. Annane, B.; Alti, A.; Lakehal, A. Blockchain based context-aware CP-ABE schema for Internet of Medical Things security. *Array* **2022**, *14*, 100150. [[CrossRef](#)]
31. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-li, F.W.; Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2022**, *181*, 274–283. [[CrossRef](#)]
32. Krishna, B.; Rajkumar, P.; Velde, V. Integration of blockchain technology for security and privacy in internet of things. *Mater. Today Proc.* **2021**. [[CrossRef](#)]
33. Ge, C.; Liu, Z.; Fang, L. A blockchain based decentralized data security mechanism for the Internet of Things. *J. Parallel Distrib. Comput.* **2020**, *141*, 1–9. [[CrossRef](#)]
34. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [[CrossRef](#)]
35. Mohanty, S.N.; Ramya, K.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.; Khanna, A. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Gener. Comput. Syst.* **2020**, *102*, 1027–1037. [[CrossRef](#)]
36. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT information sharing security mechanism based on blockchain technology. *Future Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [[CrossRef](#)]
37. Rathore, S.; Kwon, B.W.; Park, J.H. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.* **2019**, *143*, 167–177. [[CrossRef](#)]
38. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access* **2019**, *7*, 136704–136719. [[CrossRef](#)]
39. Lin, P.; Song, Q.; Yu, F.R.; Wang, D.; Guo, L. Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning. *IEEE Internet Things J.* **2021**, *8*, 15749–15761. [[CrossRef](#)]
40. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* **2022**, *164*, 152–167. [[CrossRef](#)]
41. Lee, Y.-L.; Lee, H.-A.; Hsu, C.-Y.; Kung, H.-H.; Chiu, H.-W. SEMRES-A triple security protected blockchain based medical record exchange structure. *Comput. Methods Programs Biomed.* **2022**, *215*, 106595. [[CrossRef](#)]
42. Parthiban, R.; Kumar, K.S. Effective resource scheduling using hybrid gradient descent cuckoo search algorithm and security enhancement in cloud via blockchain for healthcare 4.0. *Mater. Today Proc.* **2021**, *56*, 1802–1808. [[CrossRef](#)]
43. Azzaoui, A.E.; Sharma, P.K.; Park, J.H. Blockchain-based delegated Quantum Cloud architecture for medical big data security. *J. Netw. Comput. Appl.* **2022**, *198*, 103304. [[CrossRef](#)]
44. Sharma, P.; Borah, M.D.; Namasudra, S. Improving security of medical big data by using Blockchain technology. *Comput. Electr. Eng.* **2021**, *96*, 107529. [[CrossRef](#)]
45. Johari, R.; Kumar, V.; Gupta, K.; Vidyarthi, D.P. BLOSM: BLOckchain technology for Security of Medical records. *ICT Express* **2022**, *8*, 56–60. [[CrossRef](#)]

46. Benil, T.; Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Netw.* **2020**, *178*, 107344. [[CrossRef](#)]
47. Wan, J.; Li, J.; Imran, M.; Li, D. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3652–3660. [[CrossRef](#)]
48. Rathore, S.; Park, J.H. A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5522–5532. [[CrossRef](#)]
49. Maw, A.; Adepu, S.; Mathur, A. ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive Mob. Comput.* **2019**, *59*, 101048. [[CrossRef](#)]
50. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [[CrossRef](#)]
51. Kaur, K.; Kaddoum, G.; Zeadally, S. Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5178–5189. [[CrossRef](#)]
52. Bhattacharya, P.; Ghafouri, M.; Soeanu, A.; Kassouf, M.; Debbabi, M. Security enhancement of time synchronization and fault identification in WAMS using a two-layer blockchain framework. *Appl. Energy* **2022**, *315*, 118955. [[CrossRef](#)]
53. Esfahani, M.M. A hierarchical blockchain-based electricity market framework for energy transactions in a security-constrained cluster of microgrids. *Int. J. Electr. Power Energy Syst.* **2022**, *139*, 108011. [[CrossRef](#)]
54. Ghiasi, M.; Dehghani, M.; Niknam, T.; Kavousi-Fard, A.; Siano, P.; Alhelou, H.H. Cyber-attack detection and cyber-security enhancement in smart dc-microgrid based on blockchain technology and hilbert huang transform. *IEEE Access* **2021**, *9*, 29429–29440. [[CrossRef](#)]
55. Xiao, H.; Zhang, W.; Li, W.; Chronopoulos, A.T.; Zhang, Z. Joint Clustering and Blockchain for Real-Time Information Security Transmission at the Crossroads in C-V2X Networks. *IEEE Internet Things J.* **2021**, *8*, 13926–13938. [[CrossRef](#)]
56. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [[CrossRef](#)]
57. Zhang, X.; Chen, X. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access* **2019**, *7*, 58241–58254. [[CrossRef](#)]
58. Zeng, P.; Wang, X.; Li, H.; Jiang, F.; Doss, R. A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology. *IEEE Access* **2020**, *8*, 33644–33657. [[CrossRef](#)]
59. Cinque, M.; Esposito, C.; Russo, S.; Tamburis, O. Blockchain-empowered decentralised trust management for the Internet of Vehicles security. *Comput. Electr. Eng.* **2020**, *86*, 106722. [[CrossRef](#)]
60. Wu, H.-T.; Tsai, C.-W. An intelligent agriculture network security system based on private blockchains. *J. Commun. Netw.* **2019**, *21*, 503–508. [[CrossRef](#)]
61. Arif, S.; Khan, M.A.; Rehman, S.U.; Kabir, M.A.; Imran, M. Investigating smart home security: Is blockchain the answer? *IEEE Access* **2020**, *8*, 117802–117816. [[CrossRef](#)]
62. Awadallah, R.; Samsudin, A. Using Blockchain in Cloud Computing to Enhance Relational Database Security. *IEEE Access* **2021**, *9*, 137353–137366. [[CrossRef](#)]
63. Sowmiya, B.; Poovammal, E.; Ramana, K.; Singh, S.; Yoon, B. Linear Elliptical Curve Digital Signature (LECDs) With Blockchain Approach for Enhanced Security on Cloud Server. *IEEE Access* **2021**, *9*, 138245–138253. [[CrossRef](#)]
64. Singh, C.E.J.; Sunitha, C.A. Chaotic and Paillier Secure Image Data Sharing Based On Blockchain and Cloud Security. *Expert Syst. Appl.* **2022**, *198*, 116874. [[CrossRef](#)]
65. Bonnah, E.; Shiguang, J. DecChain: A decentralized security approach in Edge Computing based on Blockchain. *Future Gener. Comput. Syst.* **2020**, *113*, 363–379. [[CrossRef](#)]
66. Wilczyński, A.; Kołodziej, J. Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology. *Simul. Model. Pract. Theory* **2020**, *99*, 102038. [[CrossRef](#)]
67. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [[CrossRef](#)]
68. García-Magariño, I.; Lacuesta, R.; Rajarajan, M.; Lloret, J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Netw.* **2019**, *86*, 72–82. [[CrossRef](#)]
69. Li, C.; Sun, X.; Zhang, Z. Effective Methods and Performance Analysis of a Satellite Network Security Mechanism Based on Blockchain Technology. *IEEE Access* **2021**, *9*, 113558–113565. [[CrossRef](#)]
70. Manogaran, G.; Rawal, B.S.; Saravanan, V.; Kumar, P.M.; Martínez, O.S.; Crespo, R.G.; Montenegro-Marín, C.E.; Krishnamoorthy, S. Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Comput. Commun.* **2020**, *161*, 248–256. [[CrossRef](#)]
71. Meng, W.; Li, W.; Zhou, J. Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration. *Inf. Fusion* **2021**, *70*, 60–71. [[CrossRef](#)]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.