Review | Received 26 July 2023; Accepted 16 October 2023; Published 20 October 2023
https://doi.org/10.55092/blockchain20230008

Blockchain from the security perspective: a scoping review

Nazanin Moosavi[1,2] and Hamed Taherdoost[3,*]

[1] Research and Development Department, Hamta Business Corporation, Vancouver, Canada
[2] Q Minded | Quark Minded Technology Inc, Vancouver, Canada
[3] Department of Arts, Communications, and Social Sciences, University Canada West, Vancouver, Canada

* Correspondence author; E-mail: hamed.taherdoost@gmail.com or hamed@hamta.org.

Abstract: Blockchain technology is a prominent that gained a lot of attention from both industrial and research prospectives. Blockchain system is a decentralized and transparent network, which provides a secure platform for transactions. This scoping review aimed to investigate blockchain technology from a security perspective. The motivation for this review stems from the technology's growing importance across industries and the imperative to address security challenges for sustained adoption and success. This review proposes the security analysis of blockchain with the solution for these security issues, besides the blockchain adoption in various sectors as a solution to ensure security. The findings underscore the imperative for further investigation to formulate solutions for security challenges, whether within blockchain networks themselves or when integrating them into other networks. Additionally, considering the existing research gaps in this field, potential research directions for future exploration are recommended for scholars.

Keywords: Blockchain; security; cybersecurity; information security; security solutions; internet of things

1. Introduction

Blockchain technology gained popularity in both academic circles and industries recently. Blockchain is known as a distributed ledger technology that prepares a decentralized database where all the tangible and intangible assets are encoded and encrypted. The most famous blockchain network is Bitcoin which revolutionized the financial market [1]. Bitcoin is a first blockchain technology network, which introduces financial solutions for the long-lived problems in financial markets such as controlling the validation of transactional records without any central authority.

Blockchain structure empowers with mechanisms such as smart contracts and consensus mechanisms. Smart contracts are some predefined programmable rules in a blockchain

network that applies when some condition happens. With smart contracts, there is no need for third-party organizations to guarantee the contracts between participants. A consensus mechanism is used to append new data to the blockchain unanimously and securely which then can solve the user's ownership confirmation and the system integration [2]. Hence, blockchain can prepare a transparent, irreversible, and immutable system by checking multiple nodes in a network redundantly.

These unique features of blockchain make it highly secure compared to the centralized database due to the asymmetrical cryptography process by the set of public and private keys. These keys guarantee the ownership of the transactions and also ensure the non-tamper-provability features of the network. Since the transactions are integrated, confidential, and authorized, the blockchain network is secure [3].

Moreover, due to the transparency of the network, the data is available to all the users not only to the central authority organization. This is an important aspect that eliminates the single point of failure for data transactions since it is spreaded out in all the nodes and the transaction are peer-to-peer and happens with consensus.

Due to the great features and strength of blockchain networks, they can be widely used in diverse sectors and industries beyond financial markets such as the internet of things (IoT) network, health systems, energy sectors, *etc.* It is also expected that blockchain applications will expand in many areas [4–6].

Blockchain is mostly famous for its ability to revolutionize transactions and the financial market, just like what the internet did for information and communication systems. Internet development proposes a lot of exciting applications such as social media, game streaming, *etc* [7]. Blockchain is also known to propose many new services in the future that may encompass all aspects of our lives. Therefore, it is important to have a general overview of blockchain to propose adequate and applicable solutions for academic and industrial purposes.

In this scoping review, we seek the security aspects of the blockchain ecosystem. We categorized the security in blockchain into three main groups to discuss the security solutions and challenges in the literature. To the best of our knowledge, this is the first paper in the literature that discusses security in blockchain ecosystems with these considerations. Indeed, this scoping review concentrates on preparing an extensive knowledge of current researches and opening subjects regarding key security solutions and issues discussed in the researches. Hence, it is proposing future open problems for researchers to work through it.

The rest of the paper is organized as follows: Section 2 outlines blockchain structure and features; Section 3 introduces the method of the scoping review, Section 4 investigates the results and findings, Section 5 outlines a discussion on the results and finally, section 6 concludes the paper.

2. Background

2.1. Blockchain description

Blockchain technology, which is familiar as distributed ledger technology, was first introduced in 2008 by Satoshi Nakamoto It provides a new paradigm called digital currency.

Bitcoin is the first cryptocurrency based on Blockchain network, which is the most famous application of Blockchain technology in recent years.

Blockchain structure consists of a distributed database where all transactional records are stored in a digital ledger. It contains a sequence of blocks and each block has some parts that are outlined in Table 1 [8]. It should be noted that the procedure to append a new block to the blockchain happened by a consensus mechanism. This mechanism replaces the need for authority organizations or third parties to validate or verified transactions. There are many algorithms to reach consensus, but the most widely used approaches are proof of work (PoW), proof of stake (PoS), and proof of Byzantine fault tolerance (PBFT) [9].

Table 1. Block structure.

Sections	Definitions
Block version- 4 bytes	Ordinal number of a block
Merkle tree hash- 32 bytes	Hashing algorithm to create a hash for block data
Previous block hash- 32 bytes	The hash value of all the data in the former block
Timestamp- 4 bytes	The time when the data is created
nBits- 4 bytes	Current hashing target in a compact form
Nonce-4 bytes	Individual hash for each block with random number
Data-32 bytes	Transaction data

2.2. Blockchain generation

Blockchain technology is classified into four generations as follow [10–12].

A. *Blockchain 1.0:* This generation is mainly about the usage of digital cryptocurrencies in the area of the financial market. Bitcoin is the most well-known Blockchain network in this generation.
B. *Blockchain 2.0:* The second-generation proposes the idea behind the programmable codes, which leads to the smart contract terms. Blockchain 2.0 introduces the use of blockchain beyond cryptocurrencies such as cross border transactions, insurance, credits, *etc.*
C. *Blockchain 3.0:* The third generation aimed at introducing blockchain applications in different aspects of people's life such as government, health, art, and industry.
D. *Blockchain 4.0:* The fourth-generation main target is concentrating on real-time applications with focusing on the integration between artificial intelligence (AI) and Blockchain technology.

2.3. Blockchain classification

Blockchain network is classified into two models based on the permission for appending a new block to the block sequence. If any user can append a new block, the blockchain is called permissionless. The most famous permissionless public blockchain is the Bitcoin network. Instead, if only some predefined users can append a new block to the sequence the blockchain is called permissioned. Private and consortium networks belong to this category. Table 2 provides a comparison between different Blockchain categorization [4,13].

Table 2. Comparison between different blockchain classifications.

Category of blockchain	Participant	Consensus protocols	Scalability	Efficiency
Public	Any user	PoW/PoS	High	Low
Private	Predefined	PBFT	Low	High
Consortium	Predefined	PBFT	Low	High

Public blockchains are open to any user and often employ consensus protocols like PoW/PoS, offering high scalability but lower efficiency due to resource-intensive processes. Private blockchains restrict participation to predefined, trusted entities and commonly use consensus protocols like PBFT, emphasizing efficiency and high throughput. Consortium blockchains, also limited to predefined participants, share similar characteristics with private blockchains, prioritizing control and efficiency. This comparison helps elucidate the suitability of each blockchain category for specific use cases, with public blockchains being more open but less efficient, while private and consortium blockchains prioritize control and efficiency but have limited accessibility.

2.4. Blockchain feature

Blockchain technology has some incredible features that make it enjoyable and applicable in various sectors. The description of some blockchain features is given [14].

- *Decentralization*: Blockchain provides a decentralized network, which omits the necessity of central authority organizations' presence to check the proof of the transactions.
- *Privacy*: This feature provides a secure network where the real identities of users are hidden even when they contact each other.
- *Immutability*: This feature guarantee that the information is tamper-proof in the network. Hence, after the transaction happens no one can delete or edit them.
- *Distributed ledger*: Since all users in the blockchain network has one copy of all the transactions, it is distributed.
- *Irreversibility*: When one transaction is stored, it cannot be retraced.
- *Transparency*: Blockchain enables all network participants to verify transactions.

3. Methods

3.1. Study design

A scoping review was performed with to goal of providing an overview of the blockchain security instead of answering focused questions. The presented review method was carried out by defining the following five-step activities.

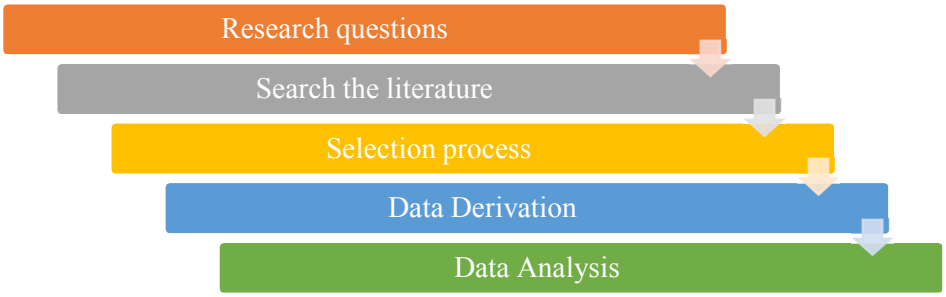

Figure 1. Design of scoping review study.

3.2. Research questions

For this review, we consider some main questions to find a general overview of this topic as follows:

- What are the main topics in blockchain security in the recent researches?
- What are opening problems and issues in blockchain security?
- What is the main area of blockchain usage as a security solution?

3.3. Search the literature

Two main databases, IEEE Xplore and Science Direct were searched and reviewed. Journal publications from 2018 to 2022 are considered the main literature work. After some discussion between the members, some keywords are selected. The final keywords are "Blockchain Security", "Blockchain Cybersecurity" and "Blockchain Information Security". The Boolean operators 'AND' and 'OR' are used in our search procedure. To retake related research papers, we used the following search lines: (Blockchain) AND (Security OR Cybersecurity OR Information Security). 6337 papers were initially considered.

3.4. Selection process

After initially finding the papers, we apply another selection process where the keywords should only appear in the title, abstracts, or keywords on the papers. In this step, 1842 papers were selected. Next, another criterion for inclusion was to have the keywords only in the title. The investigation continued with a total of 170 papers. Then we go through the abstract reading to find more relevant papers. Finally, at this step, 126 papers were selected.

3.5. Data derivation

Data were derived from research papers and categorized into the pre-development paper. The data was mainly extracted by author 1 and then reviewed by author 2. The derived data were grouped and summarized in the table and later exported into more detailed tables and charts.

3.6. Data analysis

Relevant extracted quantified data were summarized. Our main results and approaches is described in the next section. Figure 2 below exhibit a big picture of our strategy used in this paper.

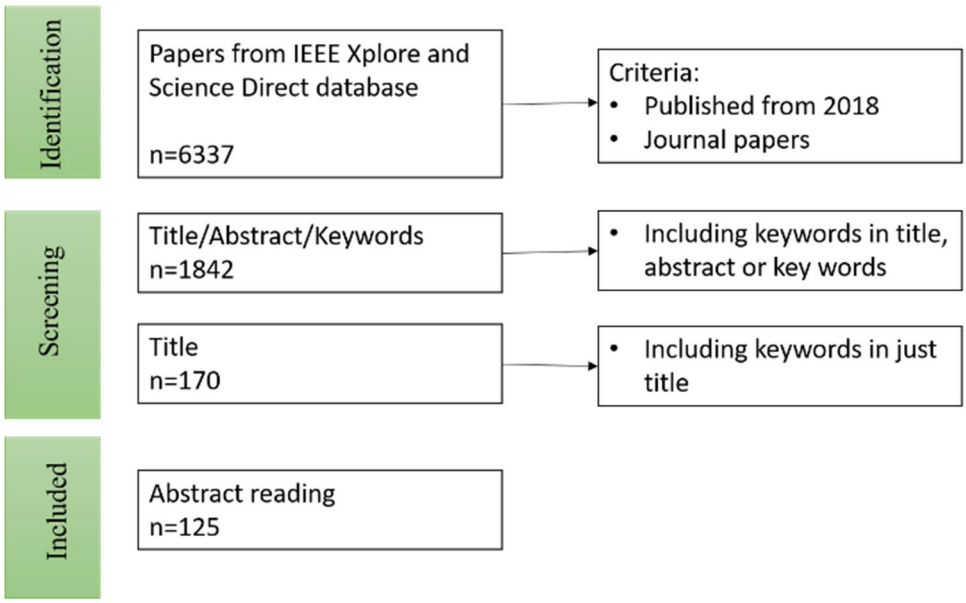

Figure 2. Flow diagram of search method.

4. Results

4.1. Publication year

Papers considered in this scoping review were selected from research studies between 2018 and April 2022 to propose the recent development in the blockchain technology area. Since blockchain technology is a new trend, it has attracted more and more interest in recent years. To show the percentages exactly, 7% of the papers were published in 2018, 10% were published in 2019, 27% were published in 2020, 35% were published in 2021 and 19% were published in 2022. Figure 3 demonstrates the results.

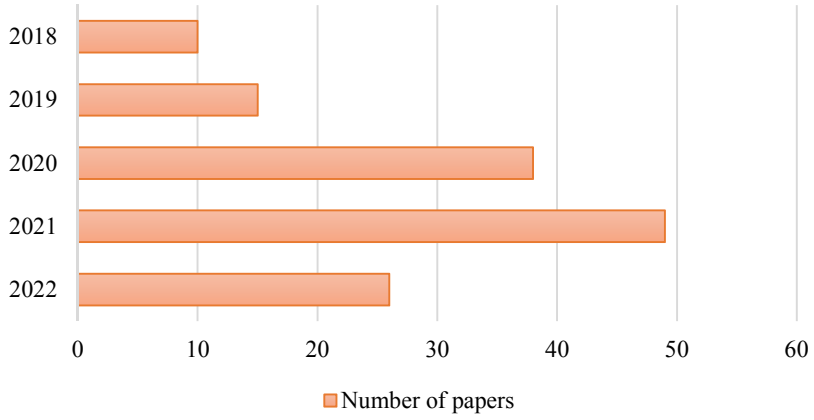

Figure 3. Research papers from each year.

4.2. Paper categorization

By considering the papers, we figured out that papers are categorized into three main groups as demonstrated in Figure 4. In the first category, there are papers that proposed a general review of blockchain security challenges and issues, second category, there are papers that proposed some solutions for blockchain security issues and the majority of papers belong to the third category where blockchain technology application in security in different sectors is proposed. Table *3* represents an overview of these findings, relating the literature references within each category and some descriptions about each reference.

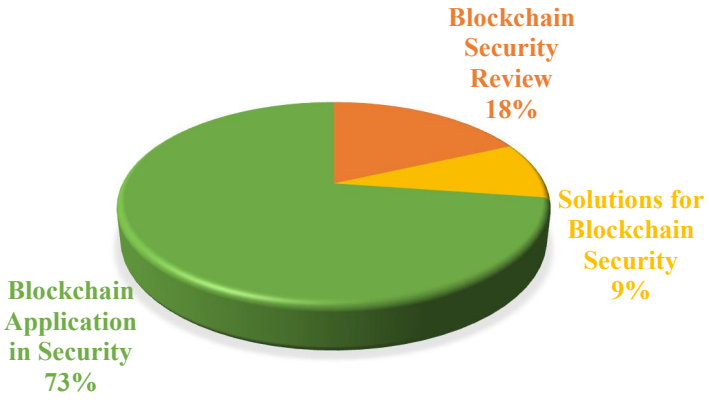

Figure 4. Paper categorization.

Table 3. Categorization of blockchain security.

Ref	Year	Category	Description
[15]	2018	Blockchain application in security	Internet of Things (IoT)
[16]	2018	Blockchain application in security	Smart transportation Electric Vehicle and Charging Pile Management
[17]	2018	Blockchain application in security	IoT
[18]	2018	Solutions for blockchain security problem	General Blockchain
[19]	2018	Blockchain application in security	IoT
[20]	2018	Blockchain application in security	IoT
[21]	2018	Blockchain application in security	IoT
[22]	2018	Blockchain application in security	Smart transportation
[23]	2018	Blockchain security analysis	General Blockchain
[24]	2019	Blockchain application in security	IoT
[25]	2019	Blockchain security analysis	General Blockchain
[26]	2019	Blockchain application in security	Telecommunication Wireless blockchain network
[27]	2019	Blockchain application in security	IoT
[28]	2019	Blockchain application in security	Unmanned aerial network (UAV)
[29]	2019	Solutions for blockchain security problem	General Blockchain
[30]	2019	Blockchain application in security	Smart Industry
[31]	2019	Blockchain application in security	Smart Industry
[32]	2019	Blockchain application in security	IoT

Table 3. *Cont.*

Ref	Year	Category	Description
[33]	2019	Blockchain application in security	IoT
[34]	2019	Blockchain application in security	Smart Industry Smart factory
[35]	2019	Blockchain application in security	Smart health Blockchain + Cloud Computing
[36]	2019	Blockchain application in security	Smart Agriculture
[37]	2019	Blockchain application in security	Smart Transportation
[38]	2020	Blockchain application in security	Smart Home
[39]	2020	Blockchain application in security	Healthcare Cloud Computing + blockchain
[40]	2020	Blockchain application in security	Telecommunication Blockchain + Edge Computing + 5G
[41]	2020	Blockchain application in security	Edge Computing + Blockchain
[42]	2020	Blockchain application in security	IoT UAV
[43]	2020	Blockchain application in security	Industrial IoT
[44]	2020	Blockchain application in security	Smart Transportation Internet of Vehicles
[45]	2020	Blockchain application in security	IoT Smart Agriculture
[46]	2020	Blockchain security analysis	General analysis for blockchain security
[47]	2020	Blockchain security analysis	General analysis for blockchain security
[48]	2020	Blockchain application in security	IoT
[49]	2020	Blockchain application in security	Smart Industry Industry 4.0
[50]	2020	Blockchain security analysis	Smart Grid
[51]	2020	Blockchain security analysis	General Blockchain
[52]	2020	Blockchain application in security	Telecommunication 6G networks
[53]	2020	Blockchain application in security	IoT Software Defined Networking (SDN) + Edge + IoT
[54]	2020	Blockchain application in security	IoT
[55]	2020	Blockchain application in security	IoT Machine Learning + Artificial Intelligence (AI)
[56]	2020	Blockchain application in security	IoT
[57]	2020	Blockchain security analysis	General Blockchain
[58]	2020	Blockchain security analysis	General Blockchain
[59]	2020	Blockchain security analysis	General Blockchain
[60]	2020	Blockchain application in security	Smart Industry Deep learning +Edge Computing
[61]	2020	Blockchain application in security	IoT and Industrial IoT
[62]	2020	Blockchain application in security	Healthcare
[63]	2020	Solutions for blockchain security	General Blockchain
[64]	2020	Blockchain application in security	Healthcare
[65]	2020	Blockchain security analysis	General Blockchain
[66]	2020	Solutions for blockchain security problem	General Blockchain
[67]	2020	Blockchain application in security	Public Sector

Table 3. *Cont.*

Ref	Year	Category	Description
[68]	2020	Blockchain application in security	Task Scheduling Cloud Computing
[69]	2020	Blockchain application in security	IoT Secure authentication model with low latency
[6]	2020	Blockchain application in security	IoT SDN
[70]	2020	Blockchain security analysis	General Blockchain
[71]	2020	Blockchain application in security	Smart Transportation Traffic Light Systems
[72]	2020	Blockchain security analysis	General Blockchain
[73]	2021	Blockchain application in security	IoT
[74]	2021	Solutions for blockchain security problem	IoT
[75]	2021	Blockchain security analysis	Smart Mobility
[76]	2021	Blockchain application in security	Database Cloud Computing
[77]	2021	Blockchain security analysis	General Blockchain
[14]	2021	Blockchain security analysis	General Blockchain
[78]	2021	Blockchain application in security	IoT IoT Platforms
[79]	2021	Solutions for blockchain security problem	Industrial IoT
[80]	2021	Blockchain application in security	IoT
[81]	2021	Blockchain security analysis	General Blockchain
[82]	2021	Blockchain application in security	IoT
[83]	2021	Blockchain application in security	Smart Grid
[84]	2021	Solutions for blockchain security problem	General Blockchain
[85]	2021	Blockchain security analysis	Business
[86]	2021	Blockchain application in security	Telecommunication Wireless Sensor Networks (WSN)
[87]	2021	Blockchain application in security	Internet of Multimedia Things
[88]	2021	Blockchain application in security	Smart grid SDN
[89]	2021	Blockchain security analysis	Decentralized identifiers services
[90]	2021	Blockchain application in security	IoT
[91]	2021	Blockchain application in security	Telecommunication Satellite Network
[92]	2021	Solutions for blockchain security problem	IoT
[93]	2021	Blockchain application in security	Smart Grid
[94]	2021	Blockchain application in security	Healthcare Virtual Reality (VR) + Learning
[95]	2021	Solutions for blockchain security problem	General Blockchain
[96]	2021	Solutions for blockchain security problem	General Blockchain SDN

Table 3. *Cont.*

Ref	Year	Category	Description
[97]	2021	Blockchain application in security	IoT Smart Industry
[98]	2021	Blockchain application in security	Healthcare
[99]	2021	Blockchain application in security	IoT
[100]	2021	Blockchain application in security	Telecommunication Deep Learning + 5G
[101]	2021	Blockchain application in security	Healthcare IoT SDN + Fog Computing
[102]	2021	Blockchain application in security	IoT Smart Agriculture
[103]	2021	Blockchain application in security	Smart energy Internet of Energy
[104]	2021	Blockchain application in security	IoT
[105]	2021	Blockchain application in security	IoT
[106]	2021	Blockchain application in security	Healthcare Big data
[107]	2021	Blockchain security analysis	IoT
[108]	2021	Blockchain application in security	Healthcare
[109]	2021	Blockchain application in security	Cloud server
[110]	2021	Blockchain security analysis	IoT
[111]	2021	Solutions for blockchain security problem	IoT Cloud Computing
[112]	2021	Blockchain security analysis	General Blockchain
[113]	2021	Solutions for blockchain security problem	Smart transportation
[114]	2022	Blockchain application in security	IoT UAV
[115]	2022	Blockchain application in security	IoT Cash Memory
[116]	2022	Blockchain application in security	Fog Computing Security Solution
[117]	2022	Blockchain application in security	IoT Internet of medical things
[118]	2022	Blockchain application in security	IoT Healthcare system
[119]	2022	Blockchain application in security	Healthcare Medical Big Data
[120]	2022	Blockchain application in security	Smart Energy
[121]	2022	Blockchain application in security	Smart energy Smart Grid
[122]	2022	Blockchain application in security	Healthcare
[123]	2022	Blockchain application in security	Smart Transportation
[124]	2022	Blockchain security analysis	General Blockchain
[125]	2022	Blockchain application in security	Healthcare
[126]	2022	Blockchain application in security	Healthcare
[127]	2022	Blockchain application in security	Smart Agriculture
[128]	2022	Blockchain security analysis	General Blockchain

Table 3. *Cont.*

Ref	Year	Category	Description
[129]	2022	Blockchain application in security	IoT SDN + AI
[130]	2022	Blockchain application in security	Healthcare
[131]	2022	Blockchain application in security	Smart City
[132]	2022	Blockchain application in security	Smart Industry
[133]	2022	Solutions for blockchain security problem	General Blockchain
[134]	2022	Blockchain security analysis	General Blockchain
[135]	2022	Blockchain security analysis	General Blockchain
[136]	2022	Solutions for blockchain security problem	Cloud Security
[137]	2022	Blockchain application in security	Industrial IoT Industry 5.0
[138]	2022	Blockchain application in security	Healthcare IoT

4.3. Blockchain security analysis

Most of the research studies in this category provide a review on blockchain security. As an example, the authors in [128] and [59] provided a security analysis for Ethereum blockchain. Ethereum is the second famous blockchain network after Bitcoin and since it is mostly used in smart contract applications; its security analysis has gained attention. Besides ref [46] proposed a survey on security analysis of smart contracts. Rest of the papers around 9% provide a review on security issues of blockchain usage in different sectors and use cases. Ref [107] and [43] worked on the blockchain security analysis in IoT networks. Also the authors in [75], [26] and [50] provided security analysis in smart mobility, wireless blockchain networks and smart grids, respectively. Figure 5 provides a chart to show the results.

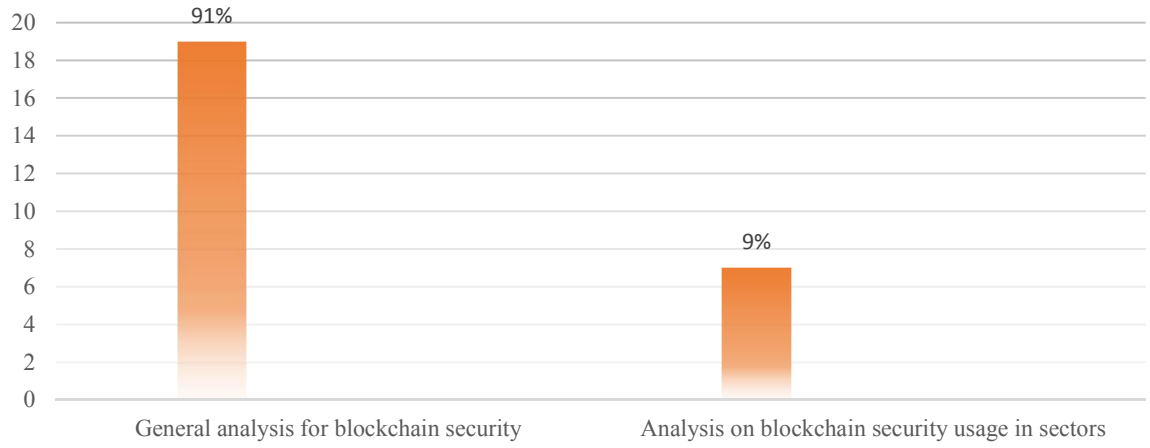

Figure 5. Blockchain security analysis in various sectors.

4.4. Solutions for blockchain security issues

From Figure 6 it is shown that 54% of research studies provide solutions to solve security issues of blockchain technology due to its features, consensus mechanism and its limitations. Authors tried to propose new models to improve the security issues in blockchain systems.

Ref [66] and [18] pointed out a graph-based model to increase the security solutions. Besides new consensus design and new mathematical model are discussed in [63] and [29]. In addition, 46% of papers propose some solutions to solve blockchain security problems when used in different sectors due to the requirements of each use case, the security solutions and problems may vary. Since most of the applications of blockchain are in IoT networks, most of the investigations and researches of providing solution for security problems fall into this category as in ref [92], [79], and [102]. Figure 6 provides a chart to show these findings.

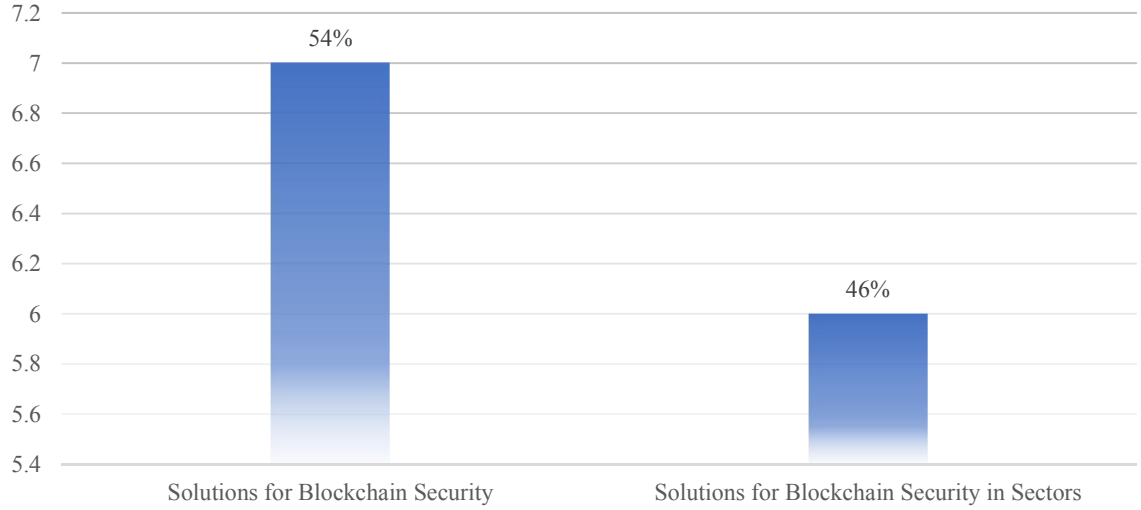

Figure 6. Solutions comparison for blockchain security.

4.5. Blockchain application in security

This group outlines papers whose main research works are proposing a security solution for various sectors with blockchain technology adaptation and implementation. 35% of research articles propose a solution for security problems in the internet of things networks, which can be generally expanded to projects in different areas such as smart health, smart grid, *etc.* Authors in [45] studied the privacy-oriented blockchain-based solutions in the field of smart agriculture in green-based IoT networks plus consensus algorithms and how they are applicable in agriculture systems.

The combination of IoT networks and healthcare systems with blockchain as a security solution provided many use cases in healthcare systems. Blockchain is a hot topic in healthcare and the number of papers considering blockchain in the health industry shows its important effect on these sector security solutions with blockchain is so popular which is 16% of the papers in our literature review. Authors in [118] proposed a secure healthcare system with IoT and Blockchain integration to support remote monitoring of patients with chronic diseases. Ref [138] provided a solution based on fuzzy logic and blockchain technology in Hyperledger blockchain platform to provide private and fast response systems for IoT healthcare systems.

The next category is the blockchain security application in smart industry projects. Ref [49] studied the blockchain solution for autonomous vehicle cyber attacks in industry 4.0 systems. Authors in [137] pointed out solution for industry 5.0, where they propose a way to replace

Merkle tree hash algorithm in the block header, which decreases the proof size and communication consumption. Totally, 8% of the papers propose solution for industrial systems.

The next, energy, and transportation sections have been proposed which are 6% of the papers respectively. Authors in [88] provided blockchain solution to provide privacy assurance and power security in smart grid systems. Ref [103] proposed a solution for the internet of energy by providing Hierarchical key generation as well as a Practical Byzantine Fault Tolerance (PBFT) consensus algorithm with an additional smart contract for energy transfer. In [113], a joint clustering and blockchain scheme for real-time information security transmission is designed to prevent traffic at the crossroads in C-V2X networks.

Furthermore, the integration of blockchain with up-to-date technologies provided interesting security solutions. 10% of the papers propose integration solutions with cloud, fog, and edge computing and 4% with software-defined network (SDN) technology. Researches in [136] proposed a secure sharing method with blockchain technology in a cloud environment to prepare security and integrity of data from images in IoT networks. Authors in [101] pointed out a solution for a wireless body area network with the integration of blockchain, fog computing and SDN to ensure the security, resource limitations and low-latency service challenges of the system. The integration of AI, SDN, and blockchain is another interesting topic where authors in [129] exploited the potential benefits of this integration to propose a new energy-efficient and secure routing protocol in the IoT network.

In addition, the application of blockchain technology with some telecommunication networks such as 5G/6G networks, satellite networks and sensor networks can provide a secure and private connection, which is needed in many use cases. 6% of the papers provide security solutions with telecommunication networks. In [100] the emergence of IoT with 5G network is considered and with the aid of deep learning and blockchain technology, intelligent data analysis operation with security is proposed. 6G network is also considered in [52], where blockchain is used to secure access control and privacy of the resources and the users of the network.

Eventually, 4% of the papers provide blockchain security solutions with unmanned aerial vehicles (UAVs) and drones that can be used in different applications from military and safety services to agriculture and shipping. Figure 7 proposes the pictorial view of these results and Table 4 introduces references for each category analysis.

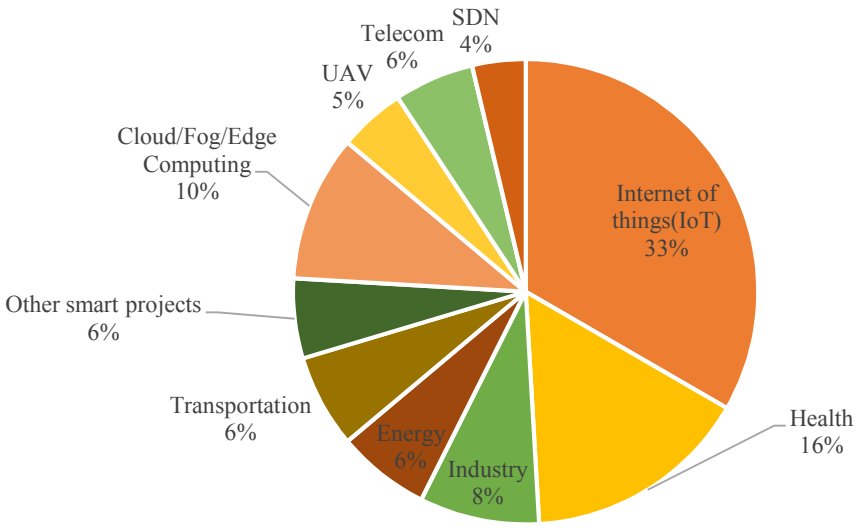

Figure 7. Blockchain application in security.

Table 4. Blockchain as a security solution in different sectors.

Category analysis	References
Internet of things (IoT)	[6,15,17,19–21,24,27,32,33,45,48,53–56,61,69,73,78,80,82, 86,87,90,99–101,104,105,107,110,114,115,117,118,129,138]
Healthcare	[35,39,62,64,94,98,101,106,108,117–119,122,125,126,130, 138]
Industry	[30,31,34,49,60,61,97,132,137]
Energy	[83,88,93,103,120,121,139]
Transportation	[16,22,37,44,71,113,123]
Other Smart projects (Agriculture/city/home)	[36,38,67,69,127,131]
Cloud/Fog/Edge Computing	[39–41,53,68,76,98,109,116,119,136]
Unmanned Arial Vehicle (UAV)	[28,42,69,101,114]
Telecommunication (5G/6G/satellite/sensor network)	[26,40,52,86,91,100]
Software Defined Networking (SDN)	[6,53,96,129]

5. Discussion

The outcomes of this scoping review propose the current researches on blockchain security topics. The study outlines that there should be more in-depth studies to be explored on this subject.

Based on the above analysis most of the research papers belonging to the third category which is providing security solutions for different sectors, are generally proposing solutions and there is no extensive overview of each sector, for example, there are not enough papers about blockchain security solutions for smart home, which is the most mature vertical of IoT and besides its security issues is of high importance. Motivated by this, we suggest that scholars to particularly study blockchain security solutions associated with each industry sector.

Analysis shows that the integration of blockchain with other technologies such as cloud computing or software define networking (SDN) can provide applicable security solutions in

different sectors. Although, since blockchain is a software-based technology, its integration with artificial intelligence (AI) and machine learning can be very applicable. However, there is a lack of research in this area in the literature. Consequently, we encourage future works to investigate on the integration between blockchain technology and artificial intelligence (AI) technology in the security context.

Furthermore, since blockchain technology is new in both research and academia many studies try to use this new trend in their work to address their security challenges. However, blockchain security challenges themselves, which only 10% of research studies consider need to be more investigated to find some strategies to address these issues.

Eventually, it is necessary for more work on suggesting solutions to security challenges for both blockchain technology itself and its adoption in various industries. Indeed, some researchers have explored security issues, but solutions for these security issues have not been fully addressed. We suggest that studies in the field of security issues of blockchain technology must continue to develop. Proposing solutions for these issues is an important research topic in blockchain systems.

This scoping review tries to answer the research questions by providing an extensive review on the newest works on the security aspects of blockchain systems. Besides, we have considered a large number of research studies to help researchers with blockchain security solution decisions. Our categorization and representations of the papers regarded to be useful as reference study for scholars who are working on the blockchain networks in both academic and business sectors.

6. Future directions

In the field of blockchain security, the trajectory of research spans multiple crucial domains. The persistent challenges of scalability and efficacy appear large, particularly in public blockchain networks. To chart future progress, academics can search for innovative solutions aimed at enhancing scalability and transaction throughput while steadfastly preserving the fundamental security attributes of blockchain technology. Simultaneously, the need for privacy and secrecy continues to drive demand for cutting-edge cryptographic methods and privacy-preserving protocols. These developments seek to strengthen the security of sensitive data while preserving the inherent transparency and immutability of blockchain records.

In addition, the evolutionary trajectory of consensus mechanisms arises as an important area of study. Existing proof-of-work and proof-of-stake systems have inherent limitations, necessitating thorough research into novel consensus algorithms. These innovative strategies aim to establish a balance between security, decentralization, and energy efficiency. As decentralized applications (DApps) continue to rise in prominence, the field of smart contract security has become an important focal point. As a result, it is necessary to strengthen the foundations of security audit processes, refine formal verification methodologies, and bolster the arsenal of vulnerability detection tools in order to prevent exploits and vulnerabilities that could compromise the integrity of smart contracts. The emerging terrain of interoperability and cross-chain security commands attention, which is accentuated by the expanding

diversity of blockchain networks. Researchers are tasked with defining the standards and protocols that can enable secure cross-chain communication and seamless asset transfers, thereby ensuring the harmonious and secure interaction between diverse blockchain ecosystems. It is essential to maintain vigilance regarding the ever-changing dynamics of blockchain security in order to guide future advances in this field.

7. Conclusion

This scoping review aims to determine a comprehensive review the latest security topic in blockchain technology and its application to offer some insight into the blockchain adaptation and application in a different environment. Our results reveal that the security subject in blockchain literature is categorized into three main groups. The first one is generally analyzing the blockchain security issues and challenges, the second one is proposing some ideas and solutions to solve the security problems and the third group is blockchain as a security solution adopted in business sectors.

The majority of the research papers are in the third group, which shows the importance of blockchain technology as a security solution in business sectors. Besides, there is a lot of paper that proposes blockchain security solutions integrated with other technologies such as cloud computing, software-defined networking, and telecommunication technologies. However, these research studies are not enough, especially in some popular sectors such as smart homes which propose future implications on this topic. In addition, although blockchain is a promising security solution, it still faces some security issues as well. However, there is a lack of research on this topic.

This scoping review article paper is prepared to be used as a reference for research intended to research on blockchain security and industry sectors to make a better decision on adopting blockchain technology as security solutions. As a result, we encourage future research works to address security subjects in this technology and suggest that research scholars and business sectors work together to reveal better solutions in this area. Furthermore, it proves beneficial to investigate the incorporation of blockchain into nascent industries and emerging technologies such as quantum computing, agriculture, healthcare, supply chain management, renewable energy, and digital identity to bolster security and optimize operational efficiency.

Conflicts of Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors' Contribution

Nazanin Moosavi: Writing – Original Draft, Investigation. Hamed Taherdoost: Conceptualization, Review & Editing, Supervision.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* 2008:21260.

[2] Becker J, Breuker D, Heide T, Holler J, Rauer HP, *et al.* Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. in *the Economics of Information Security and Privacy*. Berlin: Springer, 2013, pp. 135-156.

[3] Attaran M and Gunasekaran A. *Blockchain principles, qualities, and business applications*. Sethi SP, Ed. *SpringerBriefs in Operations Managemen*t. Cham: Springer, 2019, pp. 13-20.

[4] Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* 2018, 88:173-190.

[5] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. *IEEE Access* 2016, 4:2292-2303.

[6] Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, Choo KR. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* 2020, 13(4):625-638.

[7] Gamage H, Weerasinghe H, Dias N. A survey on blockchain technology concepts, applications, and issues. *SN Comput. Sci.* 2020. 1(2):1-15.

[8] Zheng Z, Xie S, Dai H, Chen X, Wang H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* 2018, 14(4):352-375.

[9] Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tut.* 2020, 22(2):1432-1465.

[10] Xu, M, Chen X, Kou G. A systematic review of blockchain. *Financ. Innov.* 2019, 5(1):1-14.

[11] Syed TA, Alzahrani A, Jan S, Siddiqui MS, Nadeem A, *et al.* A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE Access* 2019, 7:176838-176869.

[12] Bhaskar P, Tiwari CK, Joshi A. Blockchain in education management: present and future applications. *Interact. Technol. Smart Educ.* 2020, 18(1):1-17.

[13] Rajasekaran AS, Azees M, Al-Turjman F. A comprehensive survey on blockchain technology. *Sustain. Energy Technol. Assess.* 2022, *52 Pt A*:102039.

[14] Bhutta MN, Khwaja AA, Nadeem A, Ahmad HF, Khan MK, *et al.* A survey on blockchain technology: Evolution, architecture and security. *IEEE Access* 2021, 9:61048-61073.

[15] Banerjee M, Lee J, Choo K. A blockchain future for internet of things security: a position paper. *Digit. Commun. Networks* 2018, 4(3):149-160.

[16] 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.

[17] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* 2018, 82:395-411.

[18] Kotilevets ID, Ivanova IA, Romanov IO, Magomedov SG, Nikonov VV, *et al.* Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. *IFAC-PapersOnLine* 2018, 51(30):693-696.

[19] Kuma NM, Mallick PK. Blockchain technology for security issues and challenges in IoT. *Procedia Comput. Sci.* 2018, 132:1815-1823.

[20] Minoli D, Occhiogrosso B. Blockchain mechanisms for IoT security. *Internet Things* 2018, 1-2:1-13.

[21] Qian Y, Jiang Y, Chen J, Zhang Y, Song J, *et al.* Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* 2018, 72:266-273.

[22] Xu C, Liu H, Li P, Wang P. A remote attestation security model based on privacy-preserving blockchain for V2X. *IEEE Access* 2018, 6:67809-67818.
[23] He D, Choo K, Kumar N, Castiglione A. IEEE access special section editorial: Research challenges and opportunities in security and privacy of blockchain technologies. *IEEE Access* 2018, 6:72033-72036.
[24] Alotaibi B. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. *IEEE Sens. J.* 2019, 19(23):10953-10971.
[25] Mohanta BK, Jena D, Panda SS, Sobhanayak S. Blockchain technology: a survey on applications and security privacy challenges. *Internet Things* 2019, 8:100107.
[26] Cao B, Li M, Zhang L, Li Y, Peng M. How does CSMA/CA affect the performance and security in wireless blockchain networks. *IEEE Trans. Industr. Inform.* 2019, 16(6): 4270-4280.
[27] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. LSB: a lightweight scalable blockchain for IoT security and anonymity. *J. Parallel Distributed Comput.* 2019, 134:180-197.
[28] 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.
[29] Hafid A, Hafid AS, Samih M. New mathematical model to analyze security of sharding-based blockchain protocols. *IEEE Access* 2019, 7:185447-185457.
[30] Kamal M, Tariq M. Light-weight security and blockchain based provenance for advanced metering infrastructure. *IEEE Access* 2019, 7:87345-87356.
[31] Maw A, Adepu S, Mathur A. ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive Mob. Comput.* 2019, 59:101048.
[32] Rathore S, Kwon BW, Park JH. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.* 2019, 143:167-177.
[33] 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.
[34] Wan J, Li J, Imran M, Li D. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans. Ind. Electron.* 2019, 15(6):3652-3660.
[35] 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.
[36] Wu H, Tsai C. An intelligent agriculture network security system based on private blockchains. *J. Commun. Netw.* 2019, 21(5):503-508.
[37] 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.
[38] Arif S, Khan MA, Rehman SU, Kabir MA, Imran M. Investigating smart home security: Is blockchain the answer? *IEEE Access* 2020, 8:117802-117816.
[39] Benil T, Jasper J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Networks* 2020, 178:107344.
[40] Bhat SA, Sofi IB, Chi CY. Edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities. *IEEE Access* 2020, 8:205340-205373.
[41] Bonnah E, Shiguang J. DecChain: A decentralized security approach in Edge Computing based on Blockchain. *Future Gener. Comput. Syst.* 2020, 113:363-379.
[42] Rupa C, Srivastava G, Gadekallu TR, Maddikunta PK, Bhattacharya S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* 2020, 55:102670.
[43] Choo KR, Yan Z, Meng W. Editorial: Blockchain in industrial IoT applications: security and privacy advances, challenges, and opportunities. *IEEE Trans. Ind. Electron.* 2020, 16(6):4119-4121.

[44] 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.
[45] Ferrag MA, 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.
[46] Liu J, Liu Z. A survey on security verification of blockchain smart contracts. *IEEE Access* 2019, 7:77894-77904.
[47] Homoliak I, Venugopalan S, Reijsbergen D, Hum Q, Schumi R, *et al.* The security reference architecture for blockchains: toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Commun. Surv. Tutor.* 2020, 23(1):341-390.
[48] Ge C, Liu Z, Fang L. A blockchain based decentralized data security mechanism for the Internet of Things. *J. Parallel Distributed Comput.* 2020, 141:1-9.
[49] 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.
[50] Alam Khan F, Asif M, Ahmad A, Alharbi MT, Aljuaid H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* 2020, 55:102018.
[51] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* 2020, 107:841-853.
[52] Manogaran G, Rawal BS, Saravanan V, Kumar P, Martínez OS, *et al.* Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Comput. Commun.* 2020, 161:248-256.
[53] Medhane DV, Sangaiah AK, Hossain MS, 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(7):6143-6149.
[54] Mohanta BK, Jena D, Ramasubbareddy S, Daneshmand M, Gandomi AH. Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet Things J.* 2020, 8(2):881-888.
[55] Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* 2020, 11:100227.
[56] Mohanty SN, Ramya KC, Rani SS, Gupta D, Shankar K, *et al.* An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Gener. Comput. Syst.* 2020, 102:1027-1037.
[57] Hafid A, Hafid AS, Samih M. A novel methodology-based joint hypergeometric distribution to analyze the security of sharded blockchains. *IEEE Access* 2020, 8:179389-179399.
[58] Ghosh A, Gupta S, Dua A, Kumar N. Security of cryptocurrencies in blockchain technology: state-of-art, challenges and future prospects. *J. Netw. Comput. Appl.* 2020, 163:102635.
[59] Paavolainen S, Carr C. Security properties of light clients on the ethereum blockchain. *IEEE Access* 2020, 8:124339-124358.
[60] Rathore S, Park JH. A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. *IEEE Trans. Ind. Electron.* 2020, 17(8):5522-5532.
[61] Sengupta J, Ruj S, Bit SD. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* 2020, 149:102481.

[62] Shi SH, He D, Li L, Kumar N, Khan MK, *et al.* Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput Secur* 2020, 97:101966.
[63] Sun G, Dai M, Sun J, Yu H. Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain. *IEEE Internet Things J.* 2020, 8(8):6257-6272.
[64] Tariq N, Qamar A, Asim M, Khan FA. Blockchain and smart healthcare security: a survey. *Procedia Comput. Sci.* 2020, 175:615-620.
[65] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Cho, KR. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* 2020, 6(2):147-156.
[66] Tsoulias K, Palaiokrassas G, Fragkos G, Litke A, Varvarigou TA. A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems. *IEEE Access* 2020, 8:130952-130965.
[67] Warkentin M, Orgeron C. Using the security triad to assess blockchain technology in public sector applications. *Int. J. Inf. Manage.* 2020, 52:102090.
[68] 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.
[69] Yazdinejad A, Parizi RM, Dehghantanha A, Karimipour H, Srivastava G, *et al.* Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE Internet Things J.* 2020, 8(8):6406-6415.
[70] Zaghloul E, Li T, Mutka MW, Ren J. Bitcoin and blockchain: Security and privacy. *IEEE Internet Things J.* 2020, 7(10):10288-10313.
[71] Zeng P, Wang X, Li H, Jiang F, Doss RR. A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology. *IEEE Access* 2020, 8:33644-33657.
[72] Zhang P, Zhou M. Security and trust in blockchains: Architecture, key technologies, and open issues. *IEEE Trans. Comput. Soc. Syst.* 2020, 7(3):790-801.
[73] Abbassi Y, Benlahmer H. IoT and Blockchain combined: for decentralized security. *Procedia Comput. Sci.* 2021, 191:337-342.
[74] El-latif A, Abd-El-Atty B, Mehmood I, Muhammad K, Venegas-Andraca S, *et al.* Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. *Inf. Process. Manag.* 2021, 58(4):102549.
[75] Al Mallah R, López D, Farooq B. Cyber-Security Risk Assessment Framework For Blockchains In Smart Mobility. *IEEE Open J Intell Transp Syst* 2021, 2:294-311.
[76] Awadallah R, Samsudin A. Using blockchain in cloud computing to enhance relational database security. *IEEE Access* 2021, 9:137353-137366.
[77] Bhushan B, Sinha P, Sagayam KM, Onesimu JA. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Comput. Electr. Eng.* 2021, 90:106897.
[78] Brotsis S, Limniotis K, Bendiab G, Kolokotronis N, Shiaeles SN. On the suitability of blockchain platforms for IoT applications: architectures, security, privacy, and performance. *Comput. Networks* 2021, 191:108005.
[79] Cai X, Geng S, Zhang J, Wu D, Cui Z, *et al.* A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things. *IEEE Trans. Industr. Inform.* 2021, 17(11):7650-7658.
[80] Xu LD, Lu Y, Li L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things J.* 2021, 8(13):10452-10473.
[81] Das M, Tao X, Cheng JC. BIM security: a critical review and recommendations using encryption strategy and blockchain. *Autom. Constr.* 2021, 126:103682.

[82] Ferrag MA, 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(24):17236-17260.
[83] Ghiasi MI, Dehghani M, Niknam T, Kavousi-fard A, Siano P, *et al.* 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.
[84] Gimenez-Aguilar M, Fuentes JM, González-Manzano L, Arroyo D. Achieving cybersecurity in blockchain-based systems: A survey. *Future Gener. Comput. Syst.* 2021, 124:91-118.
[85] Gomathi SS, Soni M, Dhiman G, Govindaraj R, Kumar P. A survey on applications and security issues of blockchain technology in business sectors. *Mater. Today: Proc.* 2021.
[86] Hsiao S, Sung W. Employing blockchain technology to strengthen security of wireless sensor networks. *IEEE Access* 2021, 9:72326-72341.
[87] Jan MA, Cai J, Gao X, Khan F, Mastorakis S, *et al.* Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *J. Netw. Comput. Appl.* 2021, 175:102918.
[88] 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(8):5178-5189.
[89] Kim BG, Cho Y, Kim S, Kim H, Woo SS. A security analysis of blockchain-based did services. *IEEE Access* 2021, 9:22894-22913.
[90] Krishna B, Rajkumar P, Velde V. Integration of blockchain technology for security and privacy in internet of things. *Mater. Today: Proc.* 2021.
[91] 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.
[92] Li J, Liu T, Niyato DT, Wang P, Li J, *et al.* Contract-theoretic pricing for security deposits in sharded blockchain with internet of things (IoT). *IEEE Internet Things J.* 2021, 8(12):10052-10070.
[93] Li Q, Li A, Tao W, Cai Y. Interconnected hybrid AC-DC microgrids security enhancement using blockchain technology considering uncertainty. *Int. J. Electr. Power Energy Syst.* 2021, 133:107324.
[94] Lin P, Song Q, Yu FR, 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(21):15749-15761.
[95] Malakhov I, Marin A, Rossi S, Smuseva D. On the use of proof-of-work in permissioned blockchains: security and fairness. *IEEE Access* 2021, 10:1305-1316.
[96] 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.
[97] Pal K. Privacy, Security and policies: a review of problems and solutions with blockchain-based internet of things applications in manufacturing industry. *Procedia Comput. Sci.* 2021, 191:176-183.
[98] Parthiban R, Kumar KS. Effective resource scheduling using hybrid gradient descent cuckoo search algorithm and security enhancement in cloud via blockchain for healthcare 4.0. *Materials Today: Proceedings* 2021, *56 Pt 4*:1802-1808.
[99] Ramamoorthi S, Kumar BK, Sithik MM, Kumar TT, Ragaventhiran J, *et al.* Enhanced security in IOT environment using Blockchain: A survey. *Mater. Today: Proc.* 2021.
[100]Rathore S, Park JH, Chang H. Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. *IEEE Access* 2021, 9:90075-90083.

[101]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(4):760-776.
[102]Ren W, Wan X, Gan P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. *Future Gener. Comput. Syst.* 2021, 117:453-461.
[103]Saha R, Kumar G, Geetha G, Kim TH, Alazab M, *et al.* The blockchain solution for the security of internet of energy and electric vehicle interface. *IEEE Trans. Veh. Technol.* 2021, 70(8):7495-7508.
[104]Šarac M, Pavlović N, Bačanin N, Al-turjman FM, Adamovic SZ. Increasing privacy and security by integrating a blockchain secure interface into an iot device security gateway architecture. *Energy Rep.* 2021, 7:8075-8082.
[105]Shammar EA, Zahary AT, Al-Shargabi AA. A survey of iot and blockchain integration: security perspective. *IEEE Access* 2021, 9:156114-156150.
[106]Sharma P, Borah MD, Namasudra S. Improving security of medical big data by using Blockchain technology. *Comput. Electr. Eng.* 2021, *96 Pt A*:107529.
[107]Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* 2021, 9:13938-13959.
[108]Soni M, Singh DK. Blockchain-based security & privacy for biomedical and healthcare information exchange systems. *Mater. Today: Proc.* 2021.
[109]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.
[110]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.
[111]Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan VK. Enhancing blockchain security in cloud computing with iot environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings* 2021, *37 Pt 2*:2653-2659.
[112]Wang Y, Gou G, Liu C, Cui M, Li Z, *et al.* Survey of security supervision on blockchain from the perspective of technology. *J. Inf. Secur. Appl.* 2021, 60:102859.
[113]Xiao H, Zhang W, Li W, Chronopoulos AT, 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(18):13926-13938.
[114]Abualsauod EH. A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. *Comput. Electr. Eng.* 2022, 99:107847.
[115]Agrawal R, Faujdar N, Kumar P, Kumar A. Security and privacy of blockchain-based single-bit cache memory architecture for IoT systems. *IEEE Access* 2022, 10: 35273-35286.
[116]Alzoubi YI, Al-Ahmad A, Kahtan H. Blockchain technology as a Fog computing security and privacy solution: an overview. *Comput. Commun.* 2022, 182:129-152.
[117]Annane B, Alti A, Lakehal A. Blockchain based context-aware CP-ABE schema for Internet of Medical Things security. *Array* 2022, 14:100150.
[118]Azbeg K, Ouchetto O, Andaloussi SJ. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egypt. Inform. J.* 2022, 23(2): 329-343.
[119]Azzaoui AE, Sharma PK, Park JH. Blockchain-based delegated Quantum Cloud architecture for medical big data security. *J. Netw. Comput. Appl.* 2022, 198:103304.
[120]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.

[121]Esfahani MM. 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.
[122]Foy M, Martyn D, Daly D, Byrne A, Aguneche C, *et al.* Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis. *Procedia Comput. Sci.* 2022, 198:662-669.
[123]Grover J. Security of vehicular ad hoc networks using blockchain: a comprehensive review. *Veh. Commun.* 2022, 34:100458.
[124]Guo H, Yu X. A survey on blockchain technology and its security. *Blockchain: Research and Applications* 2022, 3(2):100067.
[125]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.
[126]Johari R, Kumar V, Gupta K, Vidyarthi DP. BLOSOM: blockchain technology for security of medical records. *ICT Express* 2022, 8(1):56-60.
[127]Kassanuk T, Phasinam K. Design of blockchain based smart agriculture framework to ensure safety and security. *Materials Today: Proceedings* 2022, *51 Pt 8*:2313-2316.
[128]Kushwaha SS, Joshi S, Singh D, Kaur M, Lee H. Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access* 2022, 10:6605-6621.
[129]Latif SA, Wen F, Iwendi C, Wang LF, Mohsin SM, *et al.* AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* 2022, 181:274-283.
[130]Lee Y, Lee H, Hsu C, Kung H, Chiu H. SEMRES-A triple security protected blockchain based medical record exchange structure. *Comput. Methods Programs Biomed.* 2022, 215:106595.
[131]Nisa KU, Alhudhaif A, Qureshi KN, Hadi HJ, Jeon G. Security provision for protecting intelligent sensors and zero touch devices by using blockchain method for the smart cities. *Microprocess. Microsyst.* 2022, 90:104503.
[132]Pan X, Zhong B, Sheng D, Yuan X, Wang Y. Blockchain and deep learning technologies for construction equipment security information management. *Autom. Constr.* 2022, 136:104186.
[133]Sallal MF, Owenson G, Salman D, Adda M. Security and performance evaluation of master node protocol based reputation blockchain in the bitcoin network. *Blockchain: Res. Appl.* 2022, 3(1):100048.
[134]Schlatt V, Guggenberger TM, Schmid J, Urbach N. Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *Int. J. Inf. Manage.* 2022, 68:102470.
[135]Serena L, D'Angelo G, Ferretti S. Security analysis of distributed ledgers and blockchains through agent-based simulation. *Simul. Model. Pract. Theory* 2022, 114:102413.
[136]Singh C, Sunitha CA. Chaotic and Paillier Secure image data sharing based on blockchain and cloud security. *Expert Syst. Appl.* 2022, 198:116874.
[137]Wang J, Chen J, Ren Y, Sharma PK, Alfarraj O, *et al.* Data security storage mechanism based on blockchain industrial Internet of Things. *Comput Ind Eng* 2022, 164:107903.
[138] Zulkifl Z, Khan F, Tahir S, Afzal M, Iqbal W, *et al.* FBASHI: fuzzy and blockchain-based adaptive security for healthcare IoTs. *IEEE Access* 2022, 10:15644-15656.
[139]Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secure Comput.* 2016, 15(5):840-852.