Hindawi
Human Behavior and Emerging Technologies
Volume 2022, Article ID 7384000, 11 pages
https://doi.org/10.1155/2022/7384000

Review Article

Cybersecurity Challenges in Blockchain Technology: A Scoping Review

Samreen Mahmood, Mehmood Chadhar, and Selena Firmin

School of Engineering, Information Technology and Physical Sciences, Federation University, Australia

Correspondence should be addressed to Samreen Mahmood; smahmood@students.federation.edu.au

Received 4 January 2022; Revised 14 February 2022; Accepted 12 March 2022; Published 5 April 2022

Academic Editor: Brandon T. McDaniel

Blockchain technology (BCT) is an emerging technology. Cybersecurity challenges in BCT are being explored to add greater value to business processes and reshape business operations. This scoping review paper was aimed at exploring the current literature's scope and categorizing various types of cybersecurity challenges in BCT. Databases such as Elsevier, ResearchGate, IEEE, ScienceDirect, and ABI/INFORM Collection (ProQuest) were searched using a combination of terms, and after rigorous screening, 51 research studies were found relevant. Data coding was performed following a framework proposed for scoping review. After careful analysis, thirty different types of cybersecurity challenges in BCT were categorized into six standardized classes. Our results show that most of the studies disclose cybersecurity challenges in BCT generally without pointing to any specific industry sector, and to a very little extent, few papers reveal cybersecurity challenges in BCT related to specific industry sectors. Also, prior studies barely investigated the strategies to minimize cybersecurity challenges in BCT. Based on gap identification, future research avenues were proposed for scholars.

1. Introduction

With the advancement of technology, cybersecurity has gained immense importance in research. Cybersecurity issues are growing exponentially across different sectors operating in the business world [1]. Big companies are focusing more on when there will be a cyberattack rather than if there will be an attack [2]. Companies are urging governments to combat cybersecurity attacks [3] as these cybersecurity issues are causing extreme financial losses [4]. A study disclosed that cyberattacks had a severe impact on companies [5], and 61% of small and medium enterprises have suffered cyberattacks [6]. Similarly, another study revealed that cybersecurity risks, like data breaches and disclosure of confidential data, are on the rise due to the increased use of cloud technologies and online applications [7].

One of the critical emerging technologies in recent years is blockchain technology (BCT) [8]. BCT is a distributed database where all assets (tangible or intangible) are digitally encoded. This digital encoding helps easy registering, tracking, and trading through private keys provided on the blockchain [9]. Also, research depicts that blockchain is playing an essential role in achieving decentralized information technology [10]. BCT is considered one of the most significant and emerging technology in the recent computing paradigm ([11][12]). Similarly, another study highlights that BCT is a new and emerging technology that provides additional security to information system applications. At the same time, BCT is facing an increasing number of cyberattack challenges [2]. Blockchain technology is one of the most popular technologies allowing transactions to be more transparent than traditional centralized systems. This technology can help organizations manage and distribute digital data by using mutually distributed ledgers. Literature shows that blockchain technology has four key components. These components include nonlocalization (decentralization), security, auditability [13], and smart execution [14]. This technology initially focuses on sharing and executing digital events among given blockchain.

Furthermore, there are many advantages of using BCT. However, it still has many associated risks [2]. One of the major advantages of using BCT is a decentralized system. A decentralized system works without involving any third party or core administrator [15]. Also, any data entered in the BCT system cannot be altered or deleted which helps in ensuring transparency and immutability [15]. Furthermore, BCT system processing is much faster as compared to traditional systems. BCT system reduces processing time from 3 days to approximately several minutes or even seconds [16].

However, despite these advantages, BCT has many associated risks and disadvantages. BCT systems consume high energy as a substantial amount of computer power is required to keep a real-time ledger and ensure transparency. Also, BCT systems have a significant amount of initial capital costs [16]. Most importantly, the BCT system has a high risk of external cybersecurity threats including 51% attacks, double-spending attacks, and Sybil's attacks [15]. A recent study claims that BCT is prone to multiple cybersecurity attacks [17]. Cyberattack is a critical challenge in all business sectors and is increasing day by day [3]. In other words, without a good understanding of these multiple cybersecurity challenges in BCT, companies cannot adopt BCT successfully. A study reported many different cyberattacks, resulting in system breakdowns like data losses, password hacks, and information stealing through emails [2, 3]. Several cyberattacks have been reported when adopting BCT ([4]; Martin Fleischmann, Bjoern S Ivens, & Bhaskar Krishnamachari, 2020; Martin Fleischmann, Bjoern S. Ivens, & Bhaskar Krishnamachari, 2020; [17, 19, 67]).

Although BCT adoption is increasing due to its unique features, most of the existing literature still reveals concerns about cybersecurity in adopting this system [1, 4, 17]. Also, BCT is still considered a new and emerging area of research in literature. In this regard, we suggest that many questions regarding cybersecurity challenges and their classification in BCT must be addressed so that research scholars and practitioners understand not only cybersecurity challenges in BCT in general but also specifically prioritize the major types of cybersecurity challenges that can be proven too fatal for the BCT system.

Also, as the cybersecurity challenges literature in BCT is rapidly increasing, we found it the right time to grab this novel research opportunity to conduct a scoping review on this topic, identify research gaps through analysis of current research literature, and suggest future implications. More precisely, this scoping review focuses on providing a deeper understanding of current literature and the gaps regarding key cybersecurity challenges reported in BCT literature and then suggesting future opportunities for research scholars working in this area.

This paper is structured as follows: The next section discusses the scoping review methodology used for this research study to ensure rigor and reliability. The following section discloses our analysis and findings based on the review. The last section of the paper discusses results and identifies gaps and future implications.

2. Methodology

In the scoping review methodology, we followed the framework provided by Arksey and O'Malley [20] and Levac et al. [21]. This framework is adopted to ensure the study follows high precision, consistency, and reliability [22]. There are different phases to be followed in a scoping review. However, conducting a scoping review is completely different from traditional systematic literature reviews. The systematic literature review focuses on previous empirical study findings on an already mature topic to answer questions like what is best for this research area, whereas, in a scoping review, the researcher focuses on an emerging topic to report the initial literature size, identify gaps, and propose research agendas accordingly for future implications [23]. As literature states that BCT is an emerging topic [2, 11], a scoping review has been chosen for studying this topic rather than a systematic review methodology. The five-phase scoping review methodology which will be followed for this study is shown in Figure 1.

2.1. Developing a Review Protocol. An extensive review protocol is developed in the first phase and followed throughout the scoping review stages. In scoping review, protocol serves more like a guiding tool than a rigid process and can be modified according to the study fit. This phase involves identifying the research question, search criteria, overall scope of the study, inclusion and exclusion criteria, conceptual framework, data extraction, defining each team member's roles and responsibilities, data analysis methods, and work plans. The research question includes the following: (1) What cybersecurity issues in BCT have been investigated in the current literature? (2) What significant gaps are identified in this current literature? and (3) What are the examples of future implications for cybersecurity challenges in BCT?

The scope of the paper is threefold: (1) to provide an up-to-date literature review of the existing research, contributing to the development of a standard body of knowledge, (2) to report the research gaps identified from the findings based on previous literature, and (3) to reveal future research avenues for research scholars. Furthermore, from a practitioner viewpoint, the paper is of significant value for companies, especially for companies planning to adopt BCT, also for information systems practitioners seeking to implement BCT in their business operations.

2.2. Searching the Literature. Major databases were searched and reviewed for this study to reveal complete literature work. The databases included Elsevier, ResearchGate, IEEE, ScienceDirect, and ABI/INFORM Collection (ProQuest). Citations and publications from these databases were sorted from the years 2017-2022 to identify the most recent literature for inclusion. Final keywords were selected for the review after each team member carried out a pilot test using these databases independently. The frequently used keywords after multiple discussions and test rounds among team members include "Cybersecurity", "Cyber-security", "Cyber security", "Blockchain technology", and "Challenges". There was no time restriction for searching keywords to ensure more literature coverage and selecting accurate keywords. After searching the keywords mentioned above using Boolean operators, 31 papers were acquired

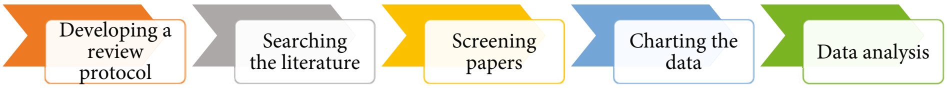

Figure 1: Phases for scoping review methodology [20, 21].

from Elsevier, 48 from ResearchGate, 40 from IEEE, 59 from ScienceDirect, and 27 from ABI/INFORM Collection (ProQuest). Boolean operators AND and OR were used as shown in Figure 2. A total of 202 papers were initially considered.

2.3. Screening Papers. After initially identifying papers for the review, all team members schedule a meeting and applied the inclusion and exclusion criteria on six out of 205 papers for training purposes. The six papers were chosen randomly. This step was done to ensure that all team members have a common understanding of the inclusion and exclusion criteria, and no significant paper has been removed from the review. To continue for further analysis in this phase, each team member ensured that the paper should answer one of the above-stated research questions in phase one. For inclusion and exclusion from the research studies revealed after searching the above keywords, we followed the recommendation provided in the literature [21] as selecting studies after refining is critical for the scoping review study. All 205 research papers were screened by two team members independently. After filtering papers, both members compared and confirmed the results. Then, the third member reviewed these papers and made the final decision. This cross-checking of documents helps in ensuring validity for the review process. During this screening of papers, the whole team met, discussed, and refined the search criteria multiple times. At the above point, after some screening of the studies by each of the authors independently and working in teams, an in-depth analysis of primary studies was carried out after exploring the literature review's relevance; conclusive studies are selected for the research study. This cross-checking of papers among team members helps in adding more reliability to this phase. During the paper screening, we found duplicate research papers. Then, after thorough research and considering limitations, including the availability of papers in the English language, same studies, and topic-based exclusion, research studies were screened as illustrated in Figure 3. Finally, at this step, the investigation continued with a total of 51 papers.

2.4. Charting the Data. A coding sheet was created to extract relevant data from all selected papers in this phase. The coding sheet was created in excel with columns consisting of information about each selected paper. The first simple information sheet includes the name of publication, year of publication, the paper's title, author name, and type of paper. Another core information sheet was developed consisting of research questions, names, and summarised explanations of each of the cybersecurity challenges reported, and ideas for future implications were collected. Then, similar cybersecurity challenges reported in all 51 selected research papers were highlighted with one specific color to make it easier for team members to code and develop themes. A total of 30 cybersecurity challenges were identified from all selected papers. Our main goal is to report all BCT cybersecurity challenges based on the selected papers' current literature. All team members worked together on all selected papers coding and thematic analysis to ensure similar understanding and avoid bias and error in the scoping review process. We adopted a framework at this stage for this review [24]. In this framework, the data is structured by dividing it into themes and significant categories. We used this framework and adopted the main heading proposed by Salvato and Corbetta [24] named as follows: (1) 1st-order data: this includes the descriptive summarised explanation of each of the cybersecurity challenges in BCT reported in the selected papers from the core information sheet developed by team members, (2) 2nd-order themes: this includes the cybersecurity challenges themes in BCT identified from 1st-order data, and (3) aggregated 2nd-order data dimensions: this includes the standardized classification of all 30 cybersecurity challenges themes identified in the 2nd-order data as shown in Figures 4 and 5. A separate third information sheet was developed for this framework to avoid any errors in classifying cybersecurity challenges in BCT. However, all papers were coded independently by each team member, and all disagreements were discussed and reviewed to make a final decision regarding theme development and standardized classification.

2.5. Data Analysis. All team members shared and worked together to develop the coding sheets and perform the thematic analysis. Like other scoping review papers, descriptive standardized classification of similar cybersecurity challenges was conducted under one central theme to depict the nature and scope of the current review. After conducting a rigorous scoping review by following recommendations given by [23], our significant findings are given in the following section of the paper.

3. Findings and Results

3.1. Publication Year. Papers included for the scoping review were published between 2017 and 2022 to inform the trends from the most recent literature. Also, BCT is new, and cybersecurity issues in BCT gained fame recently after organization's interest was found in the adoption and implementation of BCT. To report exact percentage, 6% of papers were published in 2017, 10% of papers were published in 2018, 27% of papers were published in 2019, 22% of papers were published in 2020, and 24% and 12% of papers were published in 2021 and 2022, respectively. A pictorial representation of primary studies found from each year is shown in Figure 6.

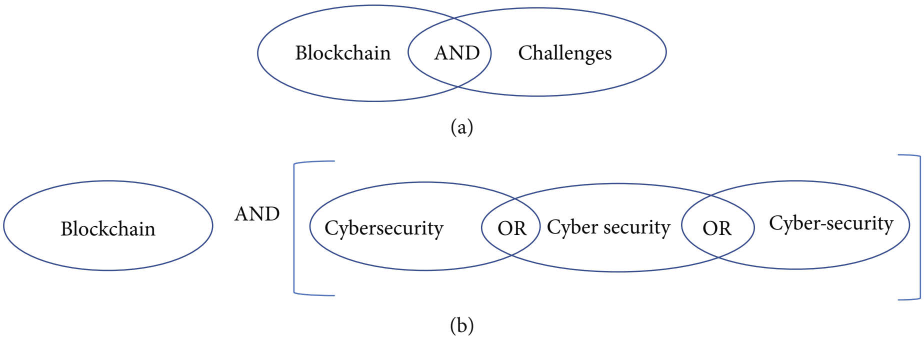

Figure 2: Boolean operators. (a) Both keywords should be present. (b) Any of the first and second keyword or third keyword or fourth keyword should be present.

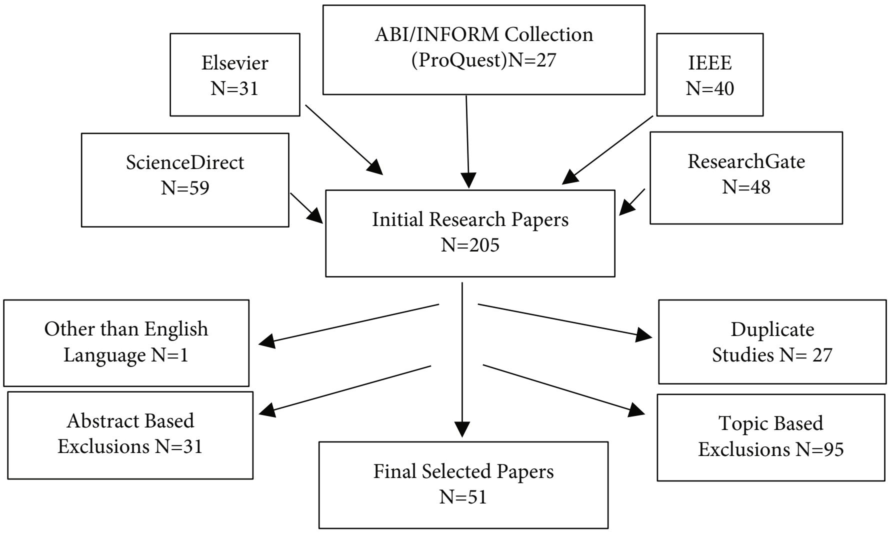
ABI/INFORM Collection (ProQuest)N=27
Elsevier N=31
IEEE N=40
ScienceDirect N=59
ResearchGate N=48
Initial Research Papers N=205
Other than English Language N=1
Duplicate Studies N= 27
Abstract Based Exclusions N=31
Topic Based Exclusions N=95
Final Selected Papers N=51

Figure 3: Paper selection process flowchart.

3.2. Publication Type. The publication type of selected research papers for this review depicts that 84% of the paper sample are included from peer-reviewed journals, whereas 16% of paper samples are from conference proceedings as shown in Figure 7. Based on publication year and publication type, it can be said here that there is a gradual increase in journal papers publications regarding this topic after the year 2017. Hence, it can be predicted that the topic is of interest to practitioners and has potentials for future researchers to work in this emerging research area.

3.3. Nature of Industry Types. Figure 8 depicts the nature of the type of industry in which cybersecurity security challenges in BCT have been explored. It shows that 57% of the sample studies have explored cybersecurity challenges in BCT generally without specifying the nature of industry type, whereas 24% of the studies have focused on healthcare and smart cities. 6% of the studies have chosen to study energy sector, and 8% of the studies have chosen supply chain and energy sectors. Others include oil and gas, accounting and finance, and the agriculture sector. Based on the above facts and figures, it can be predicted here that there is a need for research on cybersecurity challenges in BCT in oil and gas, accounting and finance, agriculture, government, supply chain, and energy sectors. In other words, specialized studies highlighting cybersecurity challenges in BCT focusing on specific industry types are lacking in the literature.

3.4. Cybersecurity Challenges in BCT. A thematic analysis using a framework adapted from Salvato and Cobetta [24] was done. Summarised explanations of each of the cybersecurity challenges were written as 1st-order data, and then, themes for each of these descriptions for cybersecurity challenges in BCT were developed as 2nd-order themes. This was done after careful considerations and repeated independent analysis by each group member, as discussed in Methodology, to ensure the rigor and validity of the review. The final results reveal a total of six standardized cybersecurity attacks, which are reported as the most common and fatal while implementing and adopting BCT depicted named as aggregated 2nd-order dimensions. Figures 4 and 5 show the detailed description of the thematic analysis of cybersecurity challenges in BCT. Table 1 represents an overview of these thematic findings, relating the literature references within each cyberattack category. The left column represents the six standardized classes of cyberattacks in BCT. The middle column shows all themes developed using

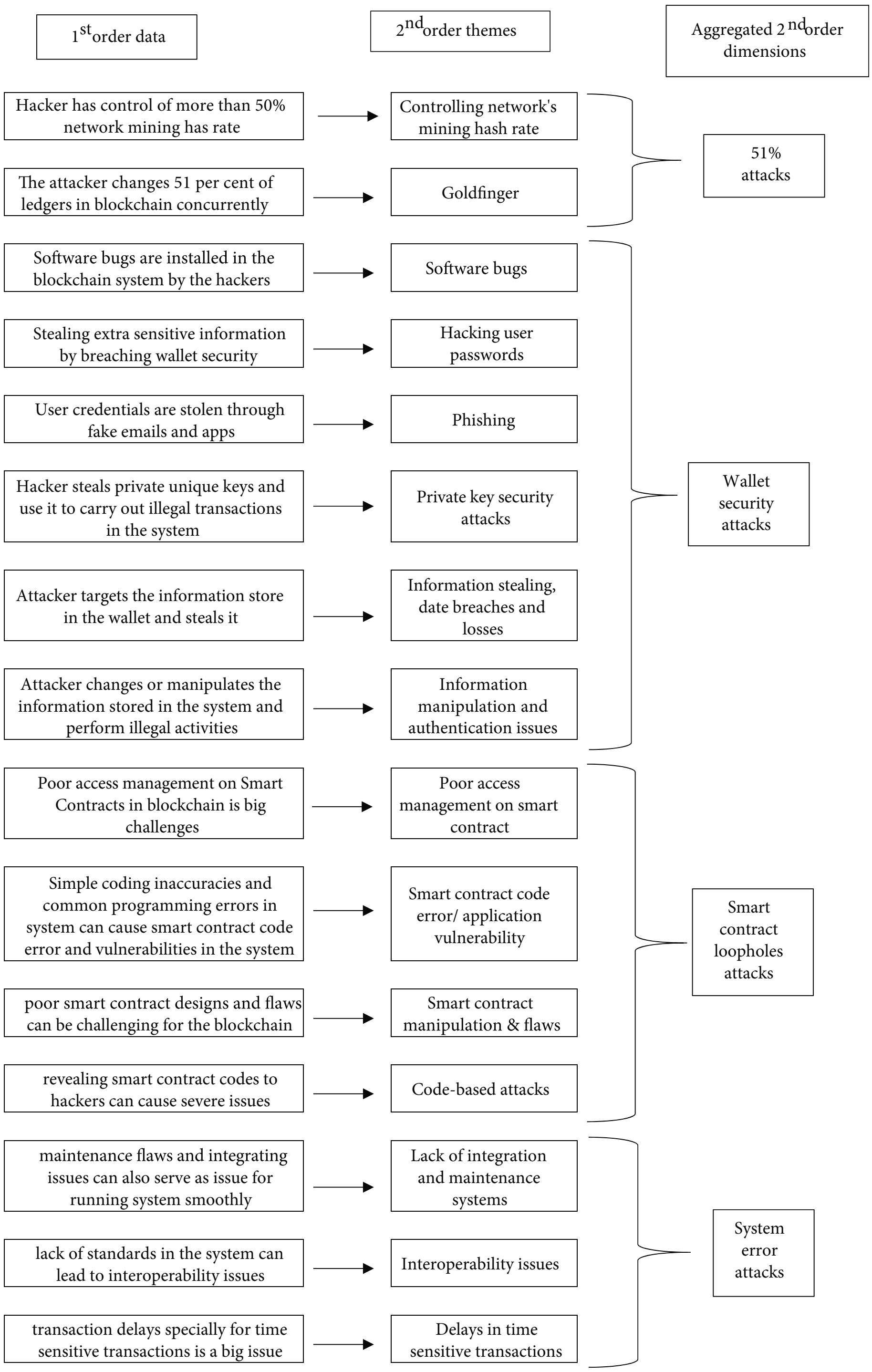
1st order data
2nd order themes
Aggregated 2 nd order dimensions
Hacker has control of more than 50% network mining has rate
Controlling network's mining hash rate
The attacker changes 51 per cent of ledgers in blockchain concurrently
Goldfinger
51% attacks
Software bugs are installed in the blockchain system by the hackers
Software bugs
Stealing extra sensitive information by breaching wallet security
Hacking user passwords
User credentials are stolen through fake emails and apps
Phishing
Hacker steals private unique keys and use it to carry out illegal transactions in the system
Private key security attacks
Wallet security attacks
Attacker targets the information store in the wallet and steals it
Information stealing, date breaches and losses
Attacker changes or manipulates the information stored in the system and perform illegal activities
Information manipulation and authentication issues
Poor access management on Smart Contracts in blockchain is big challenges
Poor access management on smart contract
Simple coding inaccuracies and common programming errors in system can cause smart contract code error and vulnerabilities in the system
Smart contract code error/ application vulnerability
Smart contract loopholes attacks
poor smart contract designs and flaws can be challenging for the blockchain
Smart contract manipulation & flaws
revealing smart contract codes to hackers can cause severe issues
Code-based attacks
maintenance flaws and integrating issues can also serve as issue for running system smoothly
Lack of integration and maintenance systems
lack of standards in the system can lead to interoperability issues
Interoperability issues
System error attacks
transaction delays specially for time sensitive transactions is a big issue
Delays in time sensitive transactions

Figure 4: Thematic analysis for cybersecurity challenges in BCT.

literature descriptions for that cyberattack. The right column shows the literature references for each of the themes and standardized class.

3.5. Nature of Cybersecurity Attacks. 80% of the research studies included in our sample reveal malleability attacks as the most common cybersecurity challenge in BCT. Following this are the wallet security attacks and 51% attacks as the most common cybersecurity challenges in BCT with 33% each, respectively. The other significant cybersecurity attacks reported in BCT in our sample are smart contract loophole attacks, double-spending attacks, and system errors attacks. A pictorial representation of sample studies reporting cybersecurity challenges in BCT for each of the themes is shown in Figure 9.

3.6. Solutions for Cybersecurity Challenges. Our analysis found that only 18% of the sample studies have explored

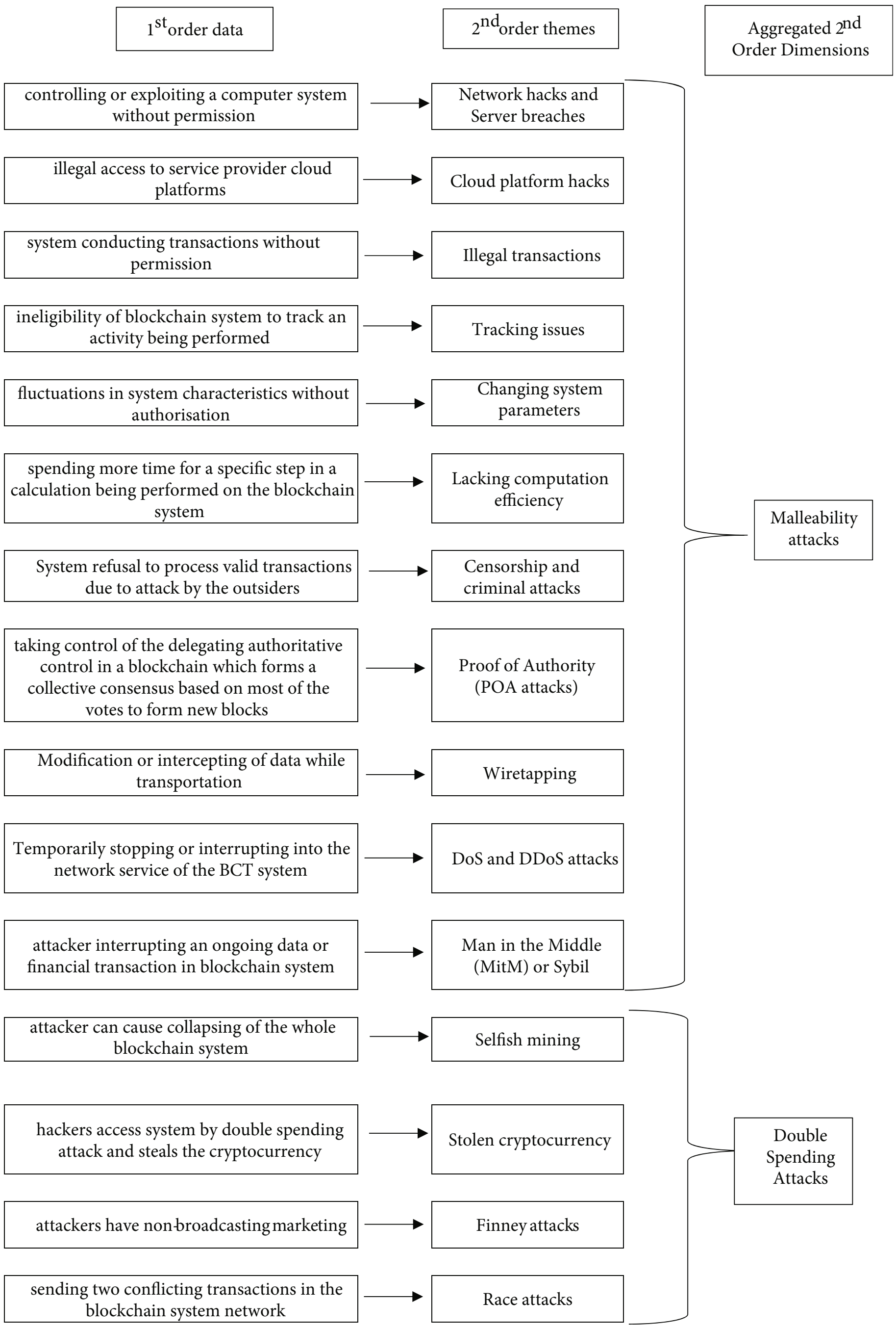
1st order data
2nd order themes
Aggregated 2nd Order Dimensions
controlling or exploiting a computer system without permission
Network hacks and Server breaches
illegal access to service provider cloud platforms
Cloud platform hacks
system conducting transactions without permission
Illegal transactions
ineligibility of blockchain system to track an activity being performed
Tracking issues
fluctuations in system characteristics without authorisation
Changing system parameters
spending more time for a specific step in a calculation being performed on the blockchain system
Lacking computation efficiency
System refusal to process valid transactions due to attack by the outsiders
Censorship and criminal attacks
taking control of the delegating authoritative control in a blockchain which forms a collective consensus based on most of the votes to form new blocks
Proof of Authority (POA attacks)
Modification or intercepting of data while transportation
Wiretapping
Temporarily stopping or interrupting into the network service of the BCT system
DoS and DDoS attacks
attacker interrupting an ongoing data or financial transaction in blockchain system
Man in the Middle (MitM) or Sybil
Malleability attacks
attacker can cause collapsing of the whole blockchain system
Selfish mining
hackers access system by double spending attack and steals the cryptocurrency
Stolen cryptocurrency
attackers have non-broadcasting marketing
Finney attacks
sending two conflicting transactions in the blockchain system network
Race attacks
Double Spending Attacks

Figure 5: Thematic analysis for cybersecurity challenges in BCT.

solutions for various cybersecurity challenges in BCT reported in their research papers, whereas 82% of the sample studies do not provide any solutions for these reported cybersecurity challenges in BCT. The studies reported multiple-signature technique, oyente, smart check, routine audits, automation of blockchain incident response, use of hot wallets and cold wallets, end-to-end product life cycle reviews, regulatory compliance, and blockchain providers selection as few solutions for these above-reported cybersecurity challenges in BCT. However, still, there is a need to explore more practical solutions for these challenges. Based on this finding, it can be said here that there is a need for research studies exploring solutions to these wide ranges of cybersecurity challenges reported in BCT in several research papers.

4. Discussion

The results of this scoping review reveal the current literature on cybersecurity challenges in BCT and highlight the most reported cybersecurity attacks in the BCT. The study's findings reveal that there is still a need for in-depth and extensive research studies to be explored in this area. Most of the research currently reports cybersecurity challenges in

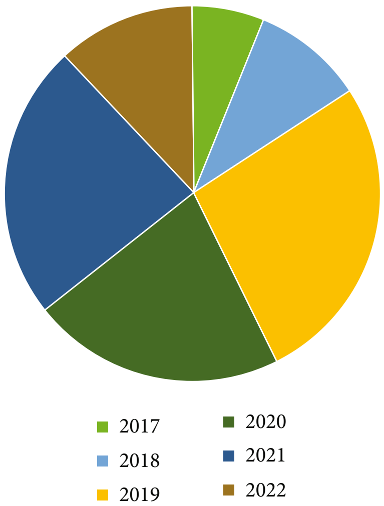

Figure 6: Research paper sample taken from each year.

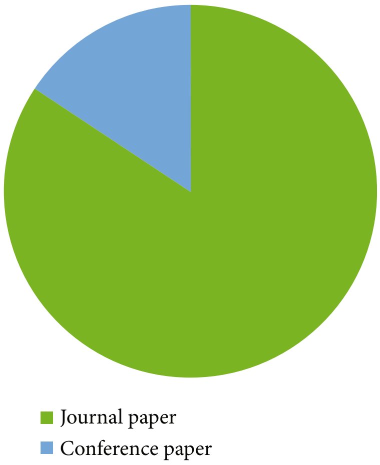

Figure 7: Type of paper publication.

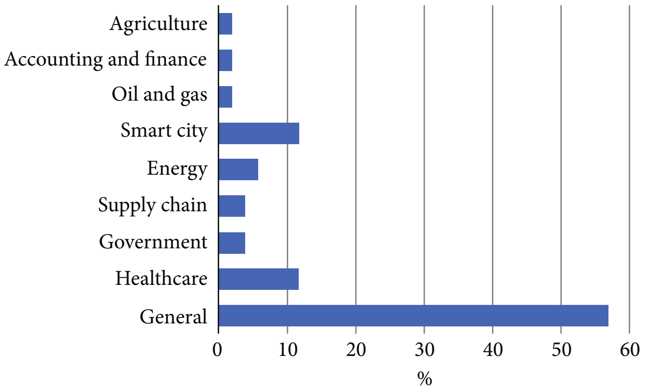

Figure 8: Sector diversity ($N = 51$).

BCT based on conceptual reviews instead of empirical considerations, for example, research studies by Hasanova et al. [19], Abdelwahab et al. [4], Zamani et al. [54], Taylor et al. [1], Vacca et al. [51], and Wylde et al. [53].

Furthermore, based on the above analysis, there are many research gaps in the current literature on cybersecurity challenges in BCT. We will reveal a few significant gaps identified from the results of our current sample. Firstly, based on our analysis, 80% of the sample studies have pointed out malleability attacks as a significant cybersecurity challenge in BCT. Also, the literature points out that malleability attacks are harmful and can hinder a blockchain system's performance [4, 48]. For instance, Accenture [66] reported that a $2.4 million loss could occur due to these malicious attacks. There are no available preventative strategies in place to address this issue. Therefore, we strongly encourage researchers to investigate and design strategies to minimize malicious attacks when adopting and implementing BCT based on empirical studies. This will enrich our collective understanding and knowledge about coping with malicious attacks in BCT. Also, these strategies will be of great benefit for practitioners in various sectors who desire to adopt and implement BCT. Furthermore, analysis reveals that more than 60% of studies reported 51% attacks and wallet security attacks as fatal cybersecurity challenges in BCT adoption. Therefore, it is a timely opportunity for researchers to design strategies exclusively for each of these attacks identified in BCT to help fill the current research gap.

Secondly, there is also a lack of industry focus studies examining the cybersecurity challenges in BCT. Our analysis depicts that half of the current literature sample points out cybersecurity challenges in BCT without specifying any industry. Therefore, knowledge about cybersecurity issues in BCT in specific industry sectors is rather insufficient. Results reveal that only 6% of sample studies focused on agriculture, accounting and finance, and oil and gas sectors. Therefore, we suggest that future studies should exclusively investigate cybersecurity challenges in BCT associated with each industry sector. This will help enrich the current literature by fulfilling this research gap but will also be helpful for practitioners who are searching for cybersecurity challenges in BCT related to their specific industry type.

Finally, there is a need for more research studies providing solutions to these identified cybersecurity challenges in BCT adoption. Indeed, the challenges have been explored by most of the authors. However, solutions for these cybersecurity challenges have not been investigated extensively. We posit the need for more empirical research studies at this stage of knowledge development in the field of cybersecurity challenges in BCT. Proposing solutions for cybersecurity challenges in BCT based on scientific investigations is an interesting research opportunity and significant and relevant in BCT adoption. Novel research studies might help the researchers to develop better solutions for these reported cybersecurity challenges in BCT adoption.

We analysed and interpreted the scoping review with great caution. However, the study has few limitations. Firstly, the study search strategy is only limited to English language papers. After an independent search by each team member, we only found one paper in a language other than

Table 1: Classification of cybersecurity attacks in BCT.

Classification of cybersecurity challenges in BCT	Themes identified	Literature references from sample research studies
Malleability attacks	Network hacks Server breaches Cloud platform hacks Illegal transactions Tracking issues Changing system parameters Lacking computation efficiency Censorship and criminal attacks Proof of authority (POA attacks) Wiretapping Denial of service (DoS attacks) Distributed denial of service (DDoS attacks) Man in the middle (MitM) or Sybil attack	[1–6, 11, 17–19, 25–55]
Double-spending attacks	Selfish mining Stolen cryptocurrency Race attacks	[4, 17–19, 26, 39, 42, 46, 47, 49, 56, 57]
51% attacks	Controlling network's mining hash rate Goldfinger	[4, 17–19, 26, 28, 35, 39, 46–49, 55, 56, 58–60]
Wallet security attacks	Hacking user passwords and software bugs Phishing Private key security attacks Information stealing, date breaches, and losses Information manipulation and authentication issues	[2, 4, 18, 19, 26, 27, 32, 34, 35, 40, 43, 46, 51, 52, 56, 61, 62]
Smart contract loophole attacks	Poor access management on smart contract Smart contract code error/application vulnerability Smart contract manipulation and flaws Code-based attacks	[2, 4, 18, 19, 29–31, 39, 40, 42, 47, 48, 51, 54, 57, 63]
System error attacks	Lack of integration and maintenance systems Interoperability issues Delays in time-sensitive transactions	[1, 5, 6, 26–28, 37, 43, 60, 63–65]

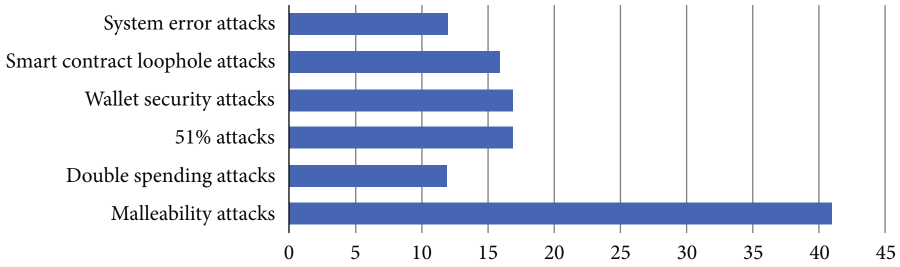

Figure 9: Cybersecurity challenges in BCT reported by sample studies.

English considering our keyword search and databases. Secondly, selection bias can also be a limitation for the current scoping review. Although we searched for papers from different databases which are commonly used, there are still chances that we missed some research papers on this topic published in other databases.

5. Conclusion

The main goal of this scoping review was to determine the size, scope, and gaps in the current literature on cybersecurity challenges in BCT. Our results show that most of the study sample reveals cybersecurity challenges in BCT generally without pointing to any specific industry sector. Few sample papers reveal cybersecurity challenges in BCT related to specific industry sectors to a very small extent. Also, most of the prior literature was conceptual review-based studies and lacked extensive empirical research on this topic. Furthermore, prior studies barely investigated the strategies and solutions to minimize cybersecurity challenges in BCT adoption. The majority of the sample study points out that malleability attacks, 51% attacks, and wallet security attacks are the most common attacks while adopting BCT. However, the literature lacks an answer to what types of strategies can be implemented to avoid malleability attacks, 51% attacks, and wallet security attacks while adopting BCT in an organization.

Based on our findings and gaps identified, we proposed some future implications on this topic. Future research scholars should focus on how and what types of questions to enhance current literature understanding on this topic. The reasons how these six commonly reported cybersecurity attacks revealed in this review could be tackled while adopting BCT should be researched further to minimize the impacts of these challenges while adopting BCT. Overall, it can be recommended based on this review that both research scholars and industry practitioners should work together to understand better and reveal solutions for these cybersecurity challenges identified during BCT adoption. Research questions like the best strategies to avoid cybersecurity challenges concerning one specified industry sector while adopting BCT need more extensive investigation.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[2] H. Lu, K. Huang, M. Azimi, and L. Guo, “Blockchain technology in the oil and gas Industry: a review of applications, opportunities, challenges, and risks,” *IEEE Access*, vol. 7, pp. 41426–41444, 2019.

[3] J. White and C. Daniels, “Continuous cybersecurity management through blockchain technology,” in *Paper presented at the 2019 IEEE Technology & Engineering Management Conference (TEMSCON)*, Atlanta, GA, USA, 2019.

[4] I. Abdelwahab, N. Ramadan, and H. Hefny, “Cybersecurity risks of blockchain technology,” *International Journal of Computer Applications*, vol. 177, no. 42, pp. 8–14, 2020.

[5] F. R. Batubara, J. Ubacht, and M. Janssen, “Challenges of Blockchain Technology Adoption for e-Government: A Systematic Literature Review,” in *Paper presented at the Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, Delft, The Netherlands, 2018.

[6] N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[7] A. Sadiq, M. Anwar, R. A. Butt et al., “A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0.,” *Human behavior and emerging technologies*, vol. 3, no. 5, pp. 854–864, 2021.

[8] E. Mbunge, B. Akinnuwesi, S. G. Fashoto, A. S. Metfula, and P. Mashwama, “A critical review of emerging technologies for tackling COVID-19 pandemic,” *Human behavior and emerging technologies*, vol. 3, no. 1, pp. 25–39, 2021.

[9] K. Francisco and D. Swanson, “The supply chain has no clothes: technology adoption of blockchain for supply chain transparency,” *Logistics MDPI*, vol. 2, no. 1, pp. 2–13, 2018.

[10] S. A. Abeyratne and R. P. Monfared, “Blockchain ready manufacturing supply chain using distributed ledger,” *International Journal of Research in Engineering and Technology*, vol. 5, no. 9, pp. 1–10, 2016.

[11] T. Hewa, M. Ylianttila, and M. Liyanage, “Survey on blockchain based smart contracts: applications, opportunities and challenges,” *Journal of Network and Computer Applications*, vol. 177, article 102857, 2021.

[12] A. Pal, C. K. Tiwari, and N. Haldar, “Blockchain for business management: applications, challenges and potentials,” *The Journal of High Technology Management Research*, vol. 32, no. 2, article 100414, 2021.

[13] J. Steiner and J. Baker, “Blockchain: The Solution for Transparency in Product Supply Chains. Provenance,” 2015, https://www.provenance.org/whitepaper.

[14] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[15] J. Golosova and A. Romanovs, “The advantages and disadvantages of the blockchain technology,” in *Paper presented at the 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, Vilnius, Lithuania, 2018.

[16] W. Song, S. Shi, V. Xu, and G. Gill, “Advantages & disadvantages of blockchain technology,” 2016, https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/.

[17] T. Wang, H. Hua, Z. Wei, and J. Cao, “Challenges of blockchain in new generation energy systems and future outlooks,” *International Journal of Electrical Power & Energy Systems*, vol. 135, article 107499, 2022.

[18] S. Gomathi, M. Soni, G. Dhiman, R. Govindaraj, and P. Kumar, “A survey on applications and security issues of blockchain technology in business sectors,” *Materials Today: Proceedings*, 2021.

[19] H. Hasanova, U. J. Baek, M. G. Shin, K. Cho, and M. S. Kim, “A survey on blockchain cybersecurity vulnerabilities and possible countermeasures,” *International Journal of Network Management*, vol. 29, no. 2, p. 36, 2019.

[20] H. Arksey and L. O'Malley, “Scoping studies: towards a methodological framework,” *International Journal of Social Research Methodology*, vol. 8, no. 1, pp. 19–32, 2005.

[21] D. Levac, H. Colquhoun, and K. K. O'Brien, "Scoping studies: advancing the methodology," *Implementation Science*, vol. 5, no. 1, pp. 1–9, 2010.

[22] G. Pare, M. Tate, D. Johnstone, and S. Kitsiou, "Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews," *European Journal of Information Systems*, vol. 25, no. 6, pp. 493–508, 2016.

[23] G. Paré, M.-C. Trudel, M. Jaana, and S. Kitsiou, "Synthesizing information systems knowledge: a typology of literature reviews," *Information & Management*, vol. 52, no. 2, pp. 183–199, 2015.

[24] C. Salvato and G. Corbetta, "Transitional leadership of advisors as a facilitator of successors' leadership construction," *Family Business Review*, vol. 26, no. 3, pp. 235–255, 2013.

[25] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities," *Information Processing & Management*, vol. 58, no. 4, article 102549, 2021.

[26] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[27] R. Al Nafea and M. A. Almaiah, "Cyber security threats in cloud: literature review," in *Paper presented at the 2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, 2021.

[28] R. Alkadi, N. Alnuaimi, C. Yeun, and A. Shoufan, "Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-art and Open Issues," *Ieee Access*, vol. 10, pp. 14463–14479, 2022.

[29] A. Alkhalifah, A. Ng, M. J. M. Chowdhury, A. S. M. Kayes, and P. A. Watters, "An empirical analysis of blockchain cybersecurity incidents," in *Paper presented at the 2019 IEEE Asia-Pacific conference on computer science and data engineering (CSDE)*, Melbourne, VIC, Australia, 2019.

[30] S. Alonso, J. Basañez, M. Lopez-Coronado, and I. De la Torre Díez, "Proposing new blockchain challenges in eHealth," *Journal of Medical Systems*, vol. 43, no. 3, p. 64, 2019.

[31] M. Andoni, V. Robu, D. Flynn et al., "Blockchain technology in the energy sector: a systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.

[32] S. J. Andriole, "Blockchain, cryptocurrency, and cybersecurity," *IT Professional*, vol. 22, no. 1, pp. 13–16, 2020.

[33] N. Etemadi, Y. Borbon-Galvez, F. Strozzi, and T. Etemadi, "Supply chain disruption risk management with blockchain: a dynamic literature review.," *Information*, vol. 12, no. 2, p. 70, 2021.

[34] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform," *Ieee Access*, vol. 9, pp. 29429–29440, 2021.

[35] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of cryptocurrencies in blockchain technology: state-of-art, challenges and future prospects," *Journal of Network and Computer Applications*, vol. 163, article 102635, 2020.

[36] M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: a survey," *Future Generation Computer Systems.*, vol. 124, pp. 91–118, 2021.

[37] M. K. Hasan, A. Alkhalifah, S. Islam et al., "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9065768, 26 pages, 2022.

[38] Y. Himeur, A. Sayed, A. Alsalemi et al., "Blockchain-based recommender systems: applications, challenges and future opportunities," *Computer Science Review*, vol. 43, article 100439, 2022.

[39] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of Medical Systems*, vol. 43, no. 10, p. 320, 2019.

[40] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[41] S. Latif, Z. Idrees, Z. Huma, and J. Ahmad, "Blockchain technology for the industrial internet of things: a comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, p. e 4337, 2021.

[42] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: a survey on applications and security privacy challenges," *Internet of Things*, vol. 8, article 100107, 2019.

[43] M. Mylrea and S. N. G. Gourisetti, "Blockchain for supply chain cybersecurity, optimization and compliance," in *Paper presented at the 2018 Resilience Week (RWS)*, Denver, CO, USA, 2018.

[44] K. Nam, C. S. Dutt, P. Chathoth, and M. S. Khan, "Blockchain technology for smart city and smart tourism: latest trends and challenges," *Asia Pacific Journal of Tourism Research*, vol. 26, no. 4, 2021.

[45] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini, and A. Skarmeta, "Toward a blockchain-based platform to manage cybersecurity certification of IoT devices," in *Paper presented at the 2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, Granada, Spain, 2019.

[46] J. H. P. Park and J. Hyuk, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, pp. 164–713, 2017.

[47] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[48] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[49] V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, "Attacking the trust machine: developing an information systems research agenda for blockchain cybersecurity," *International Journal of Information Management*, no. article 102470, 2022.

[50] W. Serrano, "The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities," *Journal of Network and Computer Applications*, vol. 175, article 102909, 2021.

[51] A. Vacca, A. Di Sorbo, C. A. Visaggio, and G. Canfora, "A systematic literature review of blockchain and smart contract development: techniques, tools, and open challenges," *Journal of Systems and Software*, vol. 174, article 110891, 2021.

[52] L. Wei, J. Wu, C. Long, and Y. Lin, "The convergence of IoE and blockchain: security challenges," *IT Professional*, vol. 21, no. 5, pp. 26–32, 2019.

[53] V. Wylde, N. Rawindaran, J. Lawrence et al., "Cybersecurity, data privacy and blockchain: a review," *SN Computer Science*, vol. 3, no. 2, pp. 1–12, 2022.

[54] E. Zamani, Y. He, and M. Phillips, "On the security risks of the blockchain," *Journal of Computer Information Systems*, vol. 60, no. 6, pp. 495–506, 2020.

[55] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: a comprehensive survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 3–19, 2021.

[56] F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustainable Cities and Society*, vol. 55, article 102018, 2020.

[57] N. D. Hewett, Sumedha, S. Furuya, F. Jee, and A. H. Alhabib, "Cybersecurity," 2020, https://widgets.weforum.org/blockchain-toolkit/cybersecurity/index.html.

[58] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen et al., "Blockchain for edge of things: applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964–988, 2022.

[59] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, pp. 653–659, 2017.

[60] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: challenges and future perspectives," *Cryptography*, vol. 3, no. 1, p. 3, 2019.

[61] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, 2020.

[62] R. Wang, H. Liu, H. Wang, Q. Yang, and D. Wu, "Distributed security architecture based on blockchain for connected health: architecture, challenges, and approaches," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 30–36, 2019.

[63] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges," *Journal of Cleaner Production*, vol. 260, article 121031, 2020.

[64] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, article 102397, 2021.

[65] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: applications, challenges and research opportunities," *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, article 102067, 2020.

[66] Accenture, "Cybersecurity Statistics," 2020, https://www.vumetric.com/statistics/the-average-cost-of-a-malware-attack-on-a-company-is-2-4-million/.

[67] M. Fleischmann, B. S. Ivens, and B. Krishnamachari, "Blockchain Technology as a Means for Brand Trust Repair–Empirical Evidence from a Digital Transgression," in *Paper presented at the Hawaii International Conference on System Sciences (HICSS)*, USA, 2020b.