Indonesian Journal of Electrical Engineering and Computer Science
Vol. 35, No. 1, July 2024, pp. 593~600
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v35.i1.pp593-600

Harnessing the power of blockchain to strengthen cybersecurity measures: a review

Nidal Turab[1], Hamza Abu Owida[2], Jamal I. Al-Nabulsi[2]
[1]Department of Networks and Cyber Security, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
[2]Department of Medical Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received Feb 13, 2024
Revised Mar 5, 2024
Accepted Mar 25, 2024

Keywords:

Blockchain technology
Internet of things
Proof of stake
Proof of work
Supply chain management

ABSTRACT

As the digital environment continues to evolve with the increasing frequency and complexity of cybersecurity threats, there is growing interest in using blockchain (BC) technology. BC is a technology with desirable properties such as decentralization, integrity, and transparency. The decentralized nature of BC eliminates single points of failure, reducing the vulnerability of critical systems to targeted attacks. The complex and rapidly evolving nature of cyber threats requires an earlier and adaptive approach. This review paper examined several papers collected from official websites. Focusing on using BC technology to improve cybersecurity, the main keywords of the review paper were BC technology, supply chain management, proof of work, and proof of stake. This review paper aims to investigate the security components through a threat assessment that compares the security of BC in different classes and real attack environments. It highlights the potential of BC to strengthen cybersecurity measures, citing unique features. The review paper also points out that there is a lack of focus on addressing security challenges related to computer data and digital systems and calling for a deeper discussion on problem-solving.

Corresponding Author:

Nidal Turab
Department of Networks and Cyber Security, Faculty of Information Technology
Al-Ahliyya Amman University
Amman 19328, Jordan
Email: N.turab@ammanu.edu.jo

1. INTRODUCTION

Blockchain (BC) technology is an emerging technology, it is a distributed ledger technology that makes it possible to record transactions via a network of computers in a safe, transparent, and unchangeable manner. Initially, it was aimed to strengthen cryptocurrencies such as Bitcoin [1]. BC is a decentralized system that has gained more popularity in wide range. Its distributed ledger technology proved its usefulness in supply chain management. In addition to its capability to increase cybersecurity by providing a constant and solid record of every transaction in the supply chain is a significant benefit [2].

The coordination of manufacturers, suppliers, distributors, and retailers is known as supply chain management (SCM), and it involves several issues regarding data security, accountability, traceability, and cost-effectiveness. Due to a lack of transparency and traceability, the complex network of participants and processes frequently makes it challenging to identify fraudulent or illegal activity. As noted by Rossi, G., BC technology uses smart contracts to lower expenses while boosting data security, accountability, transparency, traceability, and transparency. Sophisticated cryptographic algorithms are used to protect data on the BC network, making it difficult for unauthorized parties to access or change data. Supply chain management eventually gains from this increased security since it reduces the possibility of sensitive data breaches or leaks [2]. BC had essential applications in the several areas such as: cryptocurrency, finance (financial services, P2P financial market), internet-of-things (IoT), copyright protection, agricultural sector, and education [3] (as shown in Figure 1).

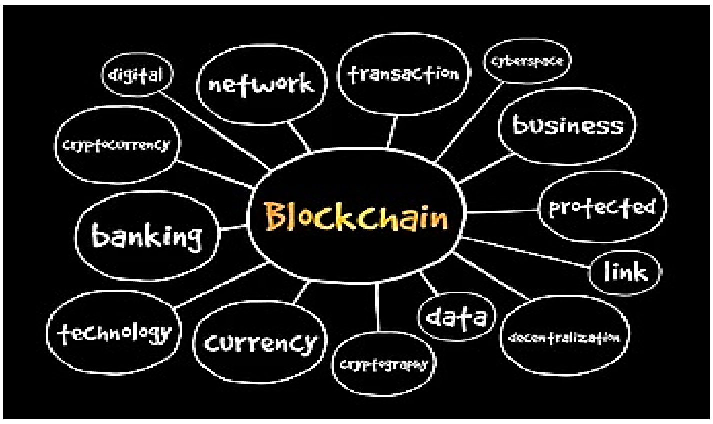

Figure 1. Mind map abstraction of the several types of blockchain applications [3]

Also, they discussed the process of preventing illegal access, attacks, damage, and data breaches from occurring to computer systems, networks, and digital assets. It is known as cybersecurity. The significance of cybersecurity is growing as our dependence on digital technologies increases. Cyber dangers can take many different forms, from malware and simple viruses to experienced hackers, criminal groups, or even nation-states orchestrating complex cyberattacks. Information protection, data integrity and confidentiality, and the availability of digital resources are the three main aims of cybersecurity [3].

Cyber risks evolving along with technology discussed by Sriram *et al*. [2]. To stay ahead of potential threats, cybersecurity is a dynamic field that demands ongoing adaptation to evolving risks and the execution of preventive measures. To build a secure digital environment, people, processes, and technology must work together. BC Technology has the potential to be a reliable cybersecurity tool in the future. This may be achieved by fully understanding this technology and making the most of the resources that are already accessible. Additionally, this technology minimizes human intervention in the cybersecurity process, which removes the risk of human error and so minimizes the likelihood of data breaches.

2. LITERATURE REVIEW

Many papers were collected from official websites. Focusing on using BC technology to improve cybersecurity in different domains, such as supply chain management, proof of work, and proof of stake. Lee and Kang developed a simulation approach for training in cyber operations, supporting with the cybersecurity framework's phases: identify, protect, detect, respond, and recover. Initially, we employ a random number generation algorithm to create two random numbers, treating them as probabilities. Subsequently, these values were input into the Lanchester stochastic model for security, with the threshold adjusted by anomalies detected. The outcomes are organized using a confusion matrix, and reports are generated based on the events, enabling trainees to recognize attempted cyberattacks on the information system. Following visible damage in the target system, trainees become proficient in response and recovery procedures. This has the potential to enhance the capabilities of cybersecurity professionals in defensive cyber operations and improve trainees' skills in managing integrated organizations, making it a valuable addition to training programs [4].

The security of future connected, and autonomous vehicles (CAVs) was discussed by Ahmad *et al.* [5]. Their paper offered a thorough analysis of cybersecurity risks aimed at sensors and problems with multi-modal sensor fusion. Following is a thorough examination of cyberattacks on vehicle-to-vehicle and inter-vehicle communications. Apart from examining conventional cybersecurity risks and their related defenses for CAV systems. Also, the examined contemporary methods like federated learning, blockchain, and machine learning to improve CAV security. Insurance businesses who operate in the cyber insurance sector face several difficulties despite the market's recent rapid rise. These include a lack of automated procedures, a scarcity of data, a rise in false claims from actual policyholders, dishonest attackers impersonating policyholders, and the fact that insurance firms themselves keep a sizable quantity of data, making them targets of cyberattacks. Farao *et al.* [6] presented INCHAIN, an innovative architecture that improves data traceability and transparency by utilizing Blockchain technology. The architecture's core is strengthened by Smart Contracts, which automate cyber insurance operations, and self-sovereign identity, which provides robust identity. The efficiency of INCHAIN's architecture in tackling the issues the cyber insurance sector faces is contrasted with previous research. The strategy efficiently combats fraudulent claims and ensures correct customer identification and verification, which is a significant achievement in the field of cyber insurance. By providing a fresh and useful approach to the complex issue of handling cyber insurance, this study lays a solid basis for further advancements in the area.

Phishing attacks are a serious cybersecurity risk in smart cities where there has been a discernible rise in incidents aimed at the infrastructure of the cities. To detect and prevent phishing attempts in smart cities, the study by Nayomi *et al.* [7] presented a cloud-assisted framework that combined blockchain and machine learning technology. The accuracy of machine learning and artificial intelligence models, successful detection and prevention rates, process efficiency, and cost considerations are all included in valuation measures. The system performs well against phishing assaults in smart cities, as demonstrated by quantitative studies that show recall rates between 0.93 and 0.96, accuracy between 0.92 and 0.95, precision scores between 0.91 and 0.94, and F1 scores between 0.92 and 0.95. Mollah *et al.* [8] presented STarEdgeChain to improve cost-effectiveness, automation, and efficiency in the provision of smart device services. STarEdgeChain is an Internet of Things oriented message distribution solution that considers security and privacy. To address these problems, they suggested using innovative encryption methods and blockchain technology. Regarding this, STarEdgeChain utilized a permissioned blockchain-assisted edge computing technique that permits the fast distribution of single sign crypted messages with specific groups of devices.

Ma *et al.* [9] researched the likelihood of using human intelligent systems (HIS) based on blockchain technology to increase smart city safety. Cryptographic systems like the McEliece Cryptosystem and number theory research unit (NTRU) are used in the analysis. NTRU ensured security in the post-quantum age. It is more realistic for real-time safety applications in smart cities due to its efficiency and reduced key sizes.

The vulnerabilities of cloud computing (CC) were studied by Kanth and Jacob [10], they proposed an enhanced capsule generative adversarial network (ECGAN) with a proof of authority (POA) BC consensus procedure-enhanced intrusion detection (ID) to develop cyber security in CC. During feature selection, the optimal features were extracted using Univariate Ensemble Feature Selection (UEFS).

The utilization of BC in human resource management (HRM) includes well-organized recording of job applicants' records and fraud removal, and improved cyber-security was studied by Adel *et al.* [11]. They created a blockchain-based human resource management system based on smart contracts. The assessment results using the system usability scale (SUS) model revealed an overall success rate of 85% [11]. Safeguarding system integrity and data privacy is of greatest importance before the extensive approval of Vehicular ad-hoc network (VANET) cloud solutions. They were studied by Setia *et al.* [12], they focused on relieving distributed denial of service (DDoS) attacks, proposing a framework. Additionally, it forces machine learning techniques for classification and predictive analytics with an accuracy of 99.59% [12].

Mittal *et al.* [13] created a web-playable serious game centered on blockchain and detailing its features. The sincere game was designed to disseminate pedagogical knowledge related to blockchain, with the specific aim of enriching the understanding of cybersecurity professionals and students. It imparts essential insights into blockchain operations, covering the addition of blocks and fundamental concepts within blockchain technology [13]. A decentralized identifiable distributed ledger technology blockchain (DIDLT-BC) framework was proposed by. The Rabin algorithm produced the digital signature, with both public and private keys established afterward to validate the transactions. The block is then built using the DIDLT model, which includes the block header information, hash code, timestamp, nonce message, and transaction list [14]. A private, safe BC-based approach to communication inside the battlefield of things (BoT) network recommended by Sharma *et al.* [15]. Furthermore, they illustrated the advantages of combining cybersecurity and BC technology when implementing BoT applications [15].

Security risks on BC Technology focused by Guo *et al.* [3], and an analysis of actual BC system vulnerabilities and attacks. Their paper surveyed bugs and Real attacks on BC systems to focus on the importance of BC system security. BC transactions are made by users through exchange platforms, and a private key is stored in a digital wallet. An attack on BC Systems' wallets revealed that users' wallets were tracking digital assets associated with their addresses, user credentials, and other information about their accounts [3]. The role of the BC system focused by Seriam *et al.* [2], in the security of data and making sure no one can alter or drop any data by protecting it from cyber-attack in general. The author focusses on multiple sides: cybersecurity, block chain and smart contract Review the challenges between companies, organization and in general adopting, promotion the block chain technology, which supplies robust storage Strategy when coupled with a smart contract.

The respected concepts related to BC technology were proved by Hussain *et al*. [16] discussed the Proof of Work (PoW). Then, they discussed on Proof of Stake (PoS) the consensus algorithm causes the nodes in the network to be verified. Candidates can confirm new blocks by staking a specific value cryptocurrency amount. The algorithm selects one number of candidates to confirm and get new blocks transaction fees. The selection algorithm uses a combination of a candidate's stake (amount of cryptocurrency held) and other factors such as the age of the coin and randomization to ensure fairness among all nodes in the network.

A hybrid consensus algorithm that combines machine learning (ML) techniques to address the challenges and exposures in blockchain networks was proposed by Venkatesan and Rahayu. The proposed hybrid method power and perfect the proposed consensus protocols' security, trust, and strength. However, they also explored the various ML techniques with hybrid consensus algorithms, such as delegated proof of stake work (DPoSW), proof of stake and work (PoSW), proof of CASBFT (PoCASBFT), delegated byzantine proof of stake (DBPoS) to enhance security [17].

Mahmood *et al.* [18] investigated cybersecurity challenges in BC technology to improve business operations and add more value to business processes. That paper classified various kinds of cybersecurity problems in BC Technology databases, including ScienceDirect, Elsevier, ResearchGate, IEEE, and ABI/INFORM collection (ProQuest). Also, mentioned by dispersed processing. Similar parallel applications have also been covered in several studies. BC technology to support IoT security in smart homes in a decentralized manner using suggested by Giannoutakis *et al*. [19]. The developed mechanism supports several functions related to user and device registration in smart homes. Additionally, offer security-focused tools such as: dynamic and immutable IP blacklisting procedures [19]. Applications of BC Technology in various domains were covered by Casino *et al*. [20]. They examined the state of BC technology today, its uses, and the ways in which certain disruptive features of this technology can revolutionize conventional wisdom. Their review included several reports from grey literature in addition to them to streamline the evaluation and capture the ever-expanding BC domain [20].

Text mining literature analysis of research articles on cybersecurity and BC technology that have been published in significant digital libraries showed by Prakash *et al*. [21]. The automated text mining techniques used in this literature analysis, such as topic modeling and key phrase extraction, help find themes within a large body of literature. The analysis emphasizes how BC technology is multidisciplinary in the cybersecurity space. The results also highlighted the vulnerabilities and cyber threats that arise with the advancement of BC technology [21]. A study involved a thorough analysis of BC Technology methods for integrating BC technology with the Internet of Things are presented by [22].

A variety of BC attack types are compiled and categorized [22]. A framework BC model structure was suggested by Hussein *et al*. [16]. As shown in Figure 2, BC stores data such as time stamps, nonce messages with verification rules, ban logic, and reliable information that has been received. These details support the user's authentication and verification are completed inside the suggested framework [23].

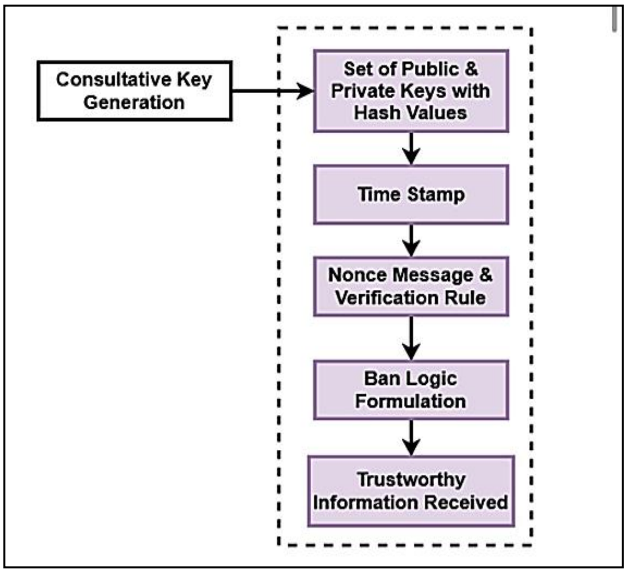
Consultative Key Generation
Set of Public & Private Keys with Hash Values
Time Stamp
Nonce Message & Verification Rule
Ban Logic Formulation
Trustworthy Information Received

Figure 2. The structure of BC [23]

Alkatheiri and Alghamdi [24] proposed a system that used BC to secure healthcare records. The tentative results show that the proposed system had a high security rate of 99.8% and the lowest latency rate of 4.3%. In addition, the consistency of the proposed system was 99.4%. BC Technology design focused on centered approach was proposed by Ragab and Altalbe [25], which can be used to raise the security bar. To address the security flaws in critical infrastructures and create a novel BC that uses deep learning to detect cyberattacks in those infrastructures. The suggested method looks to decide whether network intrusions have occurred. Furthermore, the optimal subset of features is selected using the enhanced chimp optimization-based feature selection (ECOA-FS) technique that has been presented. The use of BC technology and cybersecurity, and a systematic analysis of the most used BC security applications was presented and discussed by Taylor *et al*. [26]. They stated that "IoT is suitable for new BC applications as well as network and machine visualization, public key cryptography, web applications, authentication systems, and secure storage of Personally Identifiable Information (PII).

A secure stochastic energy management framework based on a modified BC technology and using directed acyclic graphs (DAGs) showed by Wang *et al*. [27]. The use of decentralized and transparent BC technology increases network security and reduces risk, thereby preventing financial fraud and reducing total cost of ownership. To address the problems met in traditional BC models mainly due to the complexity of storage and hash address calculation [27]. The properties of BC that are immutable and independent of third parties focused by Bansal *et al.* [28], allowing for the storage of data. Researchers are interested in BC technology, especially in cybersecurity applications for smart grids. Although a lot of work has gone into using BC in smart grids for cybersecurity [28]. The increased use and proliferation of drones that has made the internet of drones a reality put the light on by Ossamah *et al*. [29]. As more industries adopt the use of drones, the question arises of how to secure them. As organizations need to protect and coordinate thousands of drones, the introduction of security mechanisms to ensure the safety of these devices has become necessary [29]. Supplying an enterprise using BC that meets distinct security obstacles, such as malware, eclipse, double-spend attacks, and advanced persistent threats (APT) focused by Fadi and his researchers. Advanced anomaly detection and remediation strategies are needed to address the problems, particularly those that make use of artificial intelligence (AI) technologies federated learning [30], [31]. Table 1 (see Appendix) highlights the important findings of the served papers.

Jonny and Kawar studied the combination of ML and BC for improving cybersecurity in sales commerce. As the sales industry encounters rising threats of cyber-attacks, preserving sensitive financial data and ensuring secure transactions. Their paper depicted a comprehensive analysis of the methods, results, and encountered in integrating ML and BC [32]. Islam *et al*. [33] conduct a reviewed cybersecurity enhancement using blockchain in the heterogeneous network. They surveyed BC based heterogeneous network framework with best performance.

Table 1 showed that the adaptation of BC technology has proven to be highly effective for transaction security. And other security domains. The integration of ML and AI adds more intelligence and attacks detection capability. Yet there is need for more research in adaptation of BC in e-commerce, e-government, real e-state, big data, and cloud computing.

3. CONCLUSION

The summary of the literature review discussed the basic meaning of BC technology, cybersecurity principles, and the role of BC in enhancing and improving cybersecurity. The surveyed paper showed the advantages of combining cybersecurity and BC technology and how BC technology supported IoT security in a decentralized manner. So, the significance of cybersecurity is growing as our dependence on digital technologies increases. Information protection, data integrity, confidentiality, and the availability of digital resources are the three main aims of cybersecurity. Although a lot of work has been done into using BC in smart grids for cybersecurity, there is not a thorough analysis of the topic from an application and technological standpoint. So, a thorough investigation into BC technology for smart grid cybersecurity was conducted to close this gap. Then the review paper talked about industries in general, adopting the use of drones, discussing how to secure them, and exploring the use of BC technology to improve drone cybersecurity. The results of the review papers of combining cybersecurity and BC technology, improving information protection, data integrity, confidentiality, and the availability of cybersecurity. Finally, it sheds light on the gaps that the reviewed papers do not cover. In summary, there is tremendous potential for using BC to improve cybersecurity. Despite its challenges, BC's unique features, such as decentralization, transparency, and automation through smart contracts, make it an attractive technology for strengthening cybersecurity measures. On the other side, the reviewed paper gives less attention to security and issues with computation data, digital systems, and related trust mechanisms and many technical issues are the result of these challenges.

ACKNOWLEDGEMENTS

This work was supported and sponsored by Al-Ahliyya Amman University. The authors would like to express gratitude for their financial support.

APPENDIX

Table 1. Summary of literature presented in this paper

Paper	Findings
[1]	BC handles setting up trust in untrusted systems and offers cyber security benefits. BC technology has proven to be highly effective for transaction security.
[2]	Review of block chain and smart contract and challenges between companies, organization and in general adopting, promotion the block chain technology, which supplies robust storage Strategy when coupled with a smart contract
[3]	An analysis of actual BC system vulnerabilities and attacks.
[4]	A simulation approach for training in cyber operations, supporting with the cybersecurity framework's phases: identify, protect, detect, respond, and recover.
[5]	The security of future CAVs was discussed.
[6]	INCHAIN, an innovative architecture that improves data traceability and transparency by utilizing Blockchain technology.
[7]	A cloud-assisted framework that combined blockchain and machine learning technology. The recall rates between 0.93 and 0.96, accuracy between 0.92 and 0.95, precision scores between 0.91 and 0.94, and F1 scores between 0.92 and 0.95
[8]	STarEdgeChain to improve cost-effectiveness, automation, and efficiency in the provision of smart device services.
[9]	Researched the likelihood of using HIS based on blockchain technology to increase smart city safety. NTRU ensured security in the post-quantum age. It is more realistic for real-time safety applications in smart cities due to its efficiency and reduced key sizes
[10]	An ECGAN with a POA BC consensus procedure-enhanced intrusion detection to develop cyber security in CC. During feature selection, the optimal features were extracted using UEFS
[11]	The utilization of BC in HRM. The assessment results using the SUS model revealed an overall success rate of 85%
[12]	Relieving DDoS attacks, proposing a framework Additionally, it forces machine learning techniques for classification and predictive analytics with an accuracy of 99.59%.
[13]	Improve cybersecurity by offering an unchangeable and tamper-proof record of all supply chain transactions is one of its main advantages.
[14]	A DIDLT-BC framework.
[15]	This study is being done on the advantages of combining cybersecurity and BC technology when implementing BoT applications.
[16]	The algorithm selects one Number of candidates to confirm and get new blocks Transaction fees. The selection algorithm uses a combination of a candidate's stake (amount of cryptocurrency held) and other factors such as the age of the coin and randomization to ensure fairness among all nodes in the network.
[17]	A hybrid consensus algorithm that combines ML techniques to address the challenges and exposures in blockchain networks
[18]	Many applications of BC Technology for security have been explored by researchers. Such BC Technology serves as the safest platform to avoid because it can improve cybersecurity.
[19]	Using BC technology to support IoT security in smart homes in a decentralized manner.
[20]	Examine the state of BC technology today, its uses, and the ways in which certain disruptive features of this technology can revolutionize conventional wisdom.
[21]	A text mining literature analysis of research articles on cybersecurity and BC technology that have been published in significant digital libraries.
[22]	A variety of BC attack types are compiled and categorized
[23]	Details support the user`s authentication and verification are completed inside the suggested framework
[24]	Discussed BC that is a distributed digital ledger that enables end-to-end communication and ensures interaction between untrusted people. The proposed system used BC to record and extract data.
[25]	A novel BC that uses deep learning to detect cyberattacks in those infrastructures. Additionally, the best deep neural network (DNN) combined with a search and rescue (SAR) optimizer is used to identify and categorize intrusions
[26]	It also highlights future directions for BC and cybersecurity research, education, and practice, including BC security in IoT, BC security for AI data, and sidechain security.
[27]	Propose a secure stochastic energy management framework for networked microgrids (NMGs) based on a modified BC approach and using DAGs.
[28]	A thorough investigation into BC technology for smart grid cybersecurity was conducted to close this gap.
[29]	Explored the use of BC technology to improve drone cybersecurity.
[30]	The application of AI-based anomaly detection techniques. And highlighted research trends that could be pursued to use AI to increase the security of BC networks
[31]	Showed the advantages of BC technology for SCM

REFERENCES

[1] A. Malik, V. Parihar, J. Srivastava, K. Purohit, and S. Abidin, "Necessity and role of blockchain technology in the domain of cyber security and data science," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 1487–1493.

[2] V. Sriram *et al.*, "Enhancing cybersecurity through blockchain technology," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2022, pp. 208–224.

[3] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100067, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.

[4] S. Lee and D. Kang, "Designing simulation logic of UAV cyber operation using cyber security framework," *IEEE Access*, vol. 12, pp. 3488–3498, 2024, doi: 10.1109/ACCESS.2023.3349131.

[5] J. Ahmad *et al.*, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *WIREs Data Mining and Knowledge Discovery*, vol. 14, no. 1, Jan. 2024, doi: 10.1002/widm.1515.

[6] A. Farao, G. Paparis, S. Panda, E. Panaousis, A. Zarras, and C. Xenakis, "INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain," *International Journal of Information Security*, vol. 23, no. 1, pp. 347–371, Feb. 2024, doi: 10.1007/s10207-023-00741-8.

[7] B. D. D. Nayomi, S. S. Mallika, T. Sowmya, G. Janardhan, P. Laxmikanth, and M. Bhavsingh, "A cloud-assisted framework utilizing blockchain, machine learning, and artificial intelligence to countermeasure phishing attacks in smart cities," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1s, pp. 313–327, 2023.

[8] M. B. Mollah, M. A. K. Azad, and Y. Zhang, "Secure targeted message dissemination in IoT using blockchain enabled edge computing," Jan. 2024, [Online]. Available: http://arxiv.org/abs/2401.06384.

[9] Y. Ma, S. B. Goyal, A. S. Rajawat, P. Bedi, and S. Yasmeen, "Blockchain-based human intelligent systems for smart city safety," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 2, Feb. 2024, doi: 10.1002/ett.4939.

[10] R. R. Kanth and T. P. Jacob, "Enhanced capsule generative adversarial network with blockchain fostered intrusion detection system for enhancing cyber security in cloud," in *2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, Apr. 2023, pp. 1–6, doi: 10.1109/ICSTSN57873.2023.10151609.

[11] H. Adel, M. ElBakary, K. ElDahshan, and D. Salah, "BC-HRM: a blockchain-based human resource management system utilizing smart contracts," in *Lecture Notes in Networks and Systems*, Springer International Publishing, 2022, pp. 91–105.

[12] H. Setia *et al.*, "Securing the road ahead: machine learning-driven DDoS attack detection in VANET cloud environments," *Cyber Security and Applications*, vol. 2, p. 100037, 2024, doi: 10.1016/j.csa.2024.100037.

[13] A. Mittal, M. P. Gupta, M. Chaturvedi, S. R. Chansarkar, and S. Gupta, "Cybersecurity enhancement through blockchain training (CEBT) – a serious game approach," *International Journal of Information Management Data Insights*, vol. 1, no. 1, p. 100001, Apr. 2021, doi: 10.1016/j.jjimei.2020.100001.

[14] S. Selvarajan, A. Shankar, M. Uddin, A. S. Alqahtani, T. Al-Shehari, and W. Viriyasitavat, "A smart decentralized identifiable distributed ledger technology-based blockchain (DIDLT-BC) model for cloud-IoT security," *Expert Systems*, Jan. 2024, doi: 10.1111/exsy.13544.

[15] G. Sharma, D. K. Sharma, and A. Kumar, "Role of cybersecurity and blockchain in battlefield of things," *Internet Technology Letters*, vol. 6, no. 3, May 2023, doi: 10.1002/itl2.406.

[16] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, p. 30, Nov. 2023, doi: 10.1186/s42400-023-00163-y.

[17] K. Venkatesan and S. B. Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques," *Scientific Reports*, vol. 14, no. 1, p. 1149, Jan. 2024, doi: 10.1038/s41598-024-51578-7.

[18] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity challenges in blockchain technology: a scoping review," *Human Behavior and Emerging Technologies*, vol. 2022, pp. 1–11, Apr. 2022, doi: 10.1155/2022/7384000.

[19] K. M. Giannoutakis *et al.*, "A blockchain solution for enhancing cybersecurity defence of IoT," in *2020 IEEE International Conference on Blockchain (Blockchain)*, Nov. 2020, pp. 490–495, doi: 10.1109/Blockchain50366.2020.00071.

[20] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[21] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: a text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, Nov. 2022, doi: 10.1016/j.jjimei.2022.100112.

[22] M. S. Mahmood and N. B. Al Dabagh, "Blockchain technology and internet of things: review, challenge and security concern," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 1, p. 718, Feb. 2023, doi: 10.11591/ijece.v13i1.pp718-735.

[23] S. Selvarajan and H. Mouratidis, "A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems," *Scientific Reports*, vol. 13, no. 1, p. 7107, May 2023, doi: 10.1038/s41598-023-34354-x.

[24] M. S. Alkatheiri and A. S. Alghamdi, "Blockchain-assisted cybersecurity for the internet of medical things in the healthcare industry," *Electronics*, vol. 12, no. 8, p. 1801, Apr. 2023, doi: 10.3390/electronics12081801.

[25] M. Ragab and A. Altalbe, "A blockchain-based architecture for enabling cybersecurity in the internet-of-critical infrastructures," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1579–1592, 2022, doi: 10.32604/cmc.2022.025828.

[26] 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, May 2020, doi: 10.1016/j.dcan.2019.01.005.

[27] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 7300–7309, Nov. 2019, doi: 10.1109/TIA.2019.2919820.

[28] P. Bansal, R. Panchal, S. Bassi, and A. Kumar, "Blockchain for cybersecurity: a comprehensive survey," in *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, Apr. 2020, pp. 260–265, doi: 10.1109/CSNT48778.2020.9115738.

[29] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, Jun. 2020, pp. 1–9, doi: 10.1109/WF-IoT48130.2020.9221466.

[30] O. Fadi, Z. Karim, E. G. Abdellatif, and B. Mohammed, "A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments," *IEEE Access*, vol. 10, pp. 93168–93186, 2022, doi: 10.1109/ACCESS.2022.3203568.

[31] G. Rossi, “Blockchain technology for enhancing cybersecurity in supply chain management,” *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, vol. 5, no. 2, pp. 1–14, 2022.

[32] R. K. Ray, F. R. Chowdhury, and M. D. R. Hasan, “Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection,” *Journal of Business and Management Studies*, vol. 6, no. 1, pp. 206–214, Feb. 2024.

[33] S. Islam, A. Rahman, M. Ariff Bin Ameedeen, H. Ajra, Z. Binti Ismail, and J. Mohamad Zain, “Blockchain-Enabled Cybersecurity Provision for Scalable Heterogeneous Network: A Comprehensive Survey,” *Computer Modeling in Engineering & Sciences*, vol. 138, no. 1, pp. 43–123, 2024.

BIOGRAPHIES OF AUTHORS

Nidal Turab Ph.D. in computer science Professor at the Networks and Cyber Security Department, Al-Ahliyya Amman University, Jordan. His research interests include WLAN security, computer networks security and cloud computing security, eLearning, and Internet of Things. He can be contacted by this email: n.turab@ammanu.edu.jo.

Hamza Abu Owida Ph.D. in Biomedical Engineering, Assistant Professor at the Medical Engineering Department, Al-Ahliyya Amman University, Jordan. Research interests focused on biomedical sensors, nanotechnology, and tissue engineering. He can be contacted by this email: h.abuowida@ammanu.edu.jo.

Jamal Al-Nabulsi Ph.D. in Biomedical Engineering, Professor at the Medical Engineering Department, Al-Ahliyya Amman University, Jordan. His research interests are biomedical sensors, digital signal processing, and image processing. He can be contacted by this email: j.nabulsi@amm.edu.jo.