Enhancing Cybersecurity through Blockchain Technology: A Review

Preprint · December 2023

DOI: 10.13140/RG.2.2.36577.68969

2 authors, including:

Onyekachi Igbokwe
Bournemouth University
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Enhancing Cybersecurity through Blockchain Technology: A Review

Onyekachi Kingsley Igbokwe
Department of Information Technology.
Bournemouth University.
Bournemouth United Kingdom.
0009-0007-7185-8476

***Abstract*— Blockchain has been described as a major breakthrough in digital security. This paper critically assesses the viability of blockchain in strengthening cybersecurity, focusing on its capacity to ensure data integrity, augment authentication mechanisms and support distributed authority. A blockchain's ledger will provide integrity of data since after recording, no unauthorized person can alter information within it. Blockchain further eliminates problems of duplication of identities and cybercrimes by decentralizing the public critical infrastructure for authentication purposes. The principles behind Blockchain are centred on decentralization as its core values helps address the issue of central pooling of data by spreading it across the network. This makes confidentiality compromised and difficult for one to carry out a cyber-attack.**

However, this paper also critically examines the weaknesses and obstacles of blockchain implementation in cybersecurity. Moreover, the limitations of a blockchain network, including scalability problems and various flaws in smart contract deployment, are also discussed. This review presents an overview of the latest academic literature addressing blockchain in cybersecurity, revealing original uses and future challenges. The synthesis of them can drive a more subtle understanding of blockchain's role in cybersecurity and provide knowledge about future research areas and practical implications for extending blockchain into existing cybersecurity strategies.

Keywords*— *Blockchain, Cybersecurity, Data Integrity, Authentication, Decentralization, Identity Management, Data Transmission, Supply Chain Security, Immutability, Transparency

I. INTRODUCTION

The evolution to the digital age has produced an era where cybersecurity is a requirement rather than a luxury due to massive cyber-attacks that threaten the security of individuals, corporations and even countries. [1]In this unpredictable environment, blockchain technology has emerged as a potential solution, praised for its association with cryptocurrencies and now associated with strengthening cybersecurity defence [2]. Blockchain is decentralized, and the modification of data on it is almost impossible, meaning that using blockchain properties about digital safety as those characteristics can dramatically reinforce existing security infrastructures[3].

Fig. 1. Blockchain: the future of cyber security? (Staff writer, 2020)

This paper critically examines the available literature to dissect the potential usefulness and limitations of blockchain in cybersecurity. In this regard, it looks at how blockchain can change traditional security paradigms by enabling decentralization that reduces the risk of single-point failures often targeted by cyber adversaries in centralized systems [3]. Blockchain's immutability is examined for its part in protecting data integrity, providing an unchanging historical record that acts as a barrier to data alteration and manipulations [4]. The study also examines transparency in blockchain as a source of trust, although it must be noted that this should not compromise privacy issues.

Yet this review recognizes some of the technology's downsides, such as problems with scalability and environmental cost of large network blockchains and underdeveloped regulatory measures [5]-[6]. This paper strives to provide a sustainable view of the role of blockchain in cybersecurity, building on a careful critique of modern research, which will help advance new studies and practical implementation.

II. LITERATURE REVIEW

A. Blockchain Technology Fundamentals

Blockchain technology represents a paradigmatic change in how data is recorded, stored, and maintained. The technology is called Distributed Ledger Technology, which prefers something other than data storage in one central system. Instead, it offers a distributed system of nodes that share responsibility for validating and recording the transactions [7]. The blockchain consists of blocks, each with an encrypted version of its predecessor, time stamp, and relevant transaction data chained one after the other, thus providing security against any unauthorized changes [8]. The resistance to modification, in this case, is not a mere characteristic but rather an inherent element of blockchain architecture that guarantees the authenticity and validity of the data.

The decentralization aspect of blockchain is also crucial since it does away with the requirement for an administrator and hence eliminates risks of single-point failure susceptibility on the part of malicious actors [9]. The distributed consensus

model supports the blockchain networks' security and robustness. Yet, this capability to resist data manipulation does not mean the system can't be monitored. The computation and energy issues surrounding blockchain scaling have elicited several concerns [10].

Although the distributed architecture of blockchain is considered significant for security, it also makes governance and regulatory compliance issues complicated topics of research [11]. Transparency in transactions should balance off privacy concerns because its ledges are inherently open.

Cryptography security, decentralized consensus, and immutability block chains propose a revolutionary model for data management. Nevertheless, the technology, though promising, still has controversies around it, requiring deep critical assessment that is yet to be done to ensure maximum exploitation.

B. Application of Blockchain in Cybersecurity

1) Data Integrity

Data or information integrity must be preserved at all costs when discussing cyber security [12]. This blockchain technology has an indelible record incorporated in its design such that having already been recorded in the blockchain, any information cannot be compromised. Immutability is more than just a deterrent mechanism; it is also an active protector of information integrity highly valued by industries where data sacrosanct cannot be negotiated, like in critical infrastructure and financial systems [13].

In this sense, the cryptographical foundation of blockchain, particularly the use of hashing functions, forms its core. Each of the blocks gets linked together through their hashes, and in effect, this makes it possible to change data within one of the blocks but not throughout the whole network, as this would destroy the overall chain of the mined coins. A change of any records requires all subsequent documents to be practically recomputed and detectable at the speed of light in a distributed scenario [14].

Notwithstanding, the unassailable nature of blockchain's data integrity does have its doubters. The '51% attack' concern is that a user or group who gets the most hashing power can manage their way into changing how a blockchain works [15]. Moreover, blockchain may guarantee the integrity of the data in the ledger. However, data in the ledger are not automatically validated to ensure accuracy; thus, the "garbage-in – garbage out" concept holds [16].

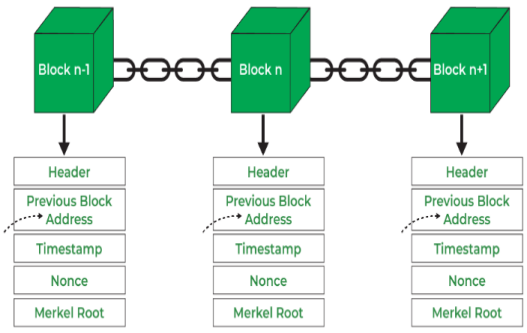

Fig. 2. Blockchain structure diagram. (Swan, 2015)

However, as was pointed out earlier, the academic community believes that blockchain makes a real contribution to ensuring the trustworthiness of the stored data, which is hard to obtain using other ways. Considering this, blockchain's role in data integrity will become a key pillar of further shaping the cyber security policy.

2) Authentication

Blockchain is not restricted to only transaction ledgers; it reinforces authentication measures. DPKI's inclusion into blockchain platforms marks a new era in digital identity management systems. The DPKI employs pre-defined blockchain properties to secure digital identities and reduce theft and fraud incidents [17].

Blockchain's decentralization makes it resilient against attacks since authenticity cannot be compromised by just one point of trust. Instead, it spreads confidence among various nodes that participate in the authentication and verification of personalities. This type of authentication uses some cryptographic methods to ensure that digital identities can be verified without giving third parties access [18].

However, critics of these systems are concerned about scalability matters. These worries arise primarily due to increased transaction speeds, which might result in network congestion, thus impeding authentication [19]. Additionally, although it has proven to be very useful in reducing the risk of identity theft, it should be noted that the original identity verification protocol must remain quite stringent to ensure that only valid identity information is registered in this decentralized system.

Most scholars agree that blockchain can upgrade the authentication processes with a more robust and flexible structure. Nevertheless, this will imply that it should be considered in a way where scalability and the initial verification process are looked into to achieve all the benefits.

3) Decentralized Control

Blockchain technology comes with decentralized control as its distinctive feature, a paradigm shift from the existing centralized data storage models. Using distributed data management over a network of machines reduces the risk of vulnerabilities associated with traditional centralized systems [20]. The decentralization implicitly expands the attack surface and renders it more challenging for unscrupulous agents to compromise the data system's integrity.

However, this characteristic of blockchain transactions removes the need to involve any trusted intermediary that has always been susceptible to attack by bad actors. Blockchain minimizes vulnerability points through the facilitation of direct interaction among various players, eliminating opportunities for individuals to engage in theft and embezzlement [21]. Besides ensuring security in Bitcoin transactions, it promises to facilitate the process of transactions, reducing the cost and time used for mediation.

Nevertheless, decentralization in itself has its problems. These problems include scale-up issues, leading to increased delays with every node and added resources required. Governance within the decentralized networks is even more complicated because different entities must make decisions on many levels to prevent conflict and increase efficiency.

Still, most academics believe that the advantages of distributed control at blockchain, specifically higher security and minimizing intermediates, make it worthwhile [22].

C. *Strengths and Weaknesses of Blockchain in Cybersecurity*

Blockchain technology is often mentioned as being very secure because of its uncentralized aspect. Its adoption of cryptographic hashes and consensus algorithms ensures data integrity and immutability, enhancing security. However, these characteristics significantly cut down the central points of attack, whereby it takes over 50% of nodes to compromise with the system, which needs to be computable.

Moreover, transparency and immutability of the blockchain's ledger lead to greater trust among the users. All transactions are traceable by all network members and, after confirmation, cannot be changed anymore. This transparency is essential for developing trust in digitally mediated interactions, especially when strict audit trails are needed [23].

Blockchain has its weaknesses despite those strengths. However, scalability is still one of the biggest challenges regarding Bitcoin. As more transactions are conducted in the network, so does the size of the blockchain increase, thus resulting in potential performance problems and increased storage demand [24]. Various researchers have criticized the high energy consumption of most of the blockchain proof-of-work consensus systems.

Smart contracts also include code that may pose another potential weakness. Smart contracts can generate and execute secured agreements; however, poorly worded smart contracts can possess loopholes which may be exploited, as proved in several high-profile data breaches [25]. With these vulnerabilities, it becomes evident why smart contracts' codes should undergo thorough testing and audits before deployment.

Although blockchain can potentially disrupt conventional cyber security systems, this potentiality can only be achieved through addressing its weaknesses. Blockchain, if it is helpful for cyber security, has to be assessed, balancing the strong and weak sides [26].

III. DISCUSSION

A. *Innovative Applications of Blockchain in Cybersecurity*

Cybersecurity with a touch of blockchain: A revolutionary approach to the traditional methods of securing different fields from risks and insecurity. However, one case is worth noting — the incorporation of the blockchain platform into the Internet of Things (IoT). The information generated from IoT devices can be archived in a tamper-proof chain of blocks with blockchain, making it difficult to change the records and allowing for reliable communication among devices [27].

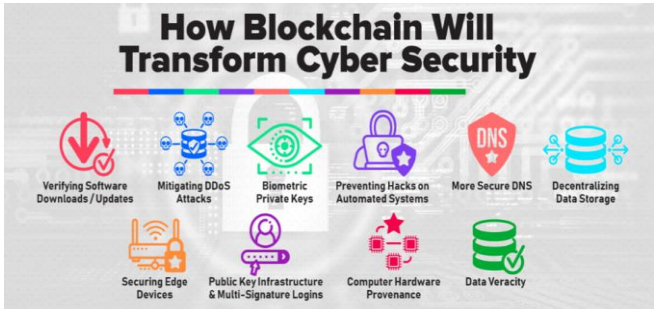

Fig. 3. Blockchain and cybersecurity (Smith, 2022)

Blockchain's immutable ledger about supply chain management affords unparalleled levels of transparency and traceability that are needed to prevent counterfeit products from being introduced into the market. Authentication of provenance and product integrity is crucial for many items where they would be applied – e.g., pharmaceuticals and luxury goods.

Another excellent potential application of blockchain is protecting countries' critical national infrastructure. Since then, cyber-attackers have often attacked infrastructural security on a national level; therefore, another more robust framework for securing all such assets is required. Blockchain is distributive; it may, thus, enable better mechanisms to monitor and control access to vital infrastructures that will reduce the risks of centralized attack, which would paralyse indispensable facilities [28].

In addition, some hindrances are associated with implementing blockchains for cybersecurity purposes. The integration with legacy systems, the need for a proper regulation scheme, and the possible emergence of new types of specific blockchain vulnerabilities require special treatment [29]-[30].

Despite the numerous ways blockchain can be used to improve cyberspace security, various complications arise, such as the maturity of the application in the developing technological environment.

B. *Challenges and Limitations*

While integrating blockchain into cybersecurity promises a lot, it faces numerous challenges that make it hard to employ in most cases. One of the main barriers faced in this regard is regulatory clarity. A sound legal policy on blockchain technology needs to be revised to avoid a climate of ambiguity, which may discourage growth and implementation. Since these are the initial stages of blockchain-specific regulation, organizations might hesitate to allocate a hefty amount towards the technologies without guidance.

The other major obstacle is how to link blockchain to older systems. Most organizations run on legacy systems, which cannot be easily integrated into working with blockchain. It is difficult and expensive as there is significant restructuring in existing infrastructure for blockchain to integrate with these systems [31].

In addition, implementing effective Blockchain-driven cyber protection solutions depends on having a trained labour force. A critical bottleneck is the need for more personnel who are well-versed in blockchain and cybersecurity. Such complex blockchains require knowledge of their theory and

practicality, which current labour needs to improve. (It needs to be improved.

Another area for improvement is that, although scalability, blockchain cannot be expanded. However, with the growth in the size of the blockchain, processing of the transactions may require a sufficient amount of resources, making the system prone to bottleneck.

Finally, although blockchain is safe, it is not immune to all cyber threats. The risks associated with 51 per cent of attacks and smart contract weaknesses, among others, should be factored in to strengthen existing cybersecurity defence systems [32].

Although the blockchain has tremendous cybersecurity potential, some hurdles must be overcome to ensure this dream is achieved.

IV. CONCLUSION

Regarding cybersecurity, blockchain technology evolves as a revolutionary mechanism that guarantees authenticity, data integrity and decentralization. It has become one of the most important means for anti-cyberthreats since it is congruent with essential conditions of safe electronic payments. Although it has tremendous prospects, blockchain has several impediments that hinder its deployment in cybersecurity circumstances.

The size of the blockchain raises scalability concerns because it can result in a performance constraint in conducting various security activities [33]. In other words, the high costs of fuel consumption linked with blockchain, especially using proof of work, are environmentally unsustainable for permanent use in society [34].

Contracting is an Innovative Issue Too: Especially about Security. While it is through these automated contracts that the blockchain becomes useful, their vulnerability presents major security concerns for the system [35]. Therefore, smart contract systems' security should be continually addressed through research.

For blockchain to realize its potential as a cyber security solution these issues must be dealt with. Efforts should concentrate on making scalability stronger, power consumption lower, and sealing the security loophole embedded in smart contracts and other blockchain-centered applications [35].

REFERENCES

[1] D. Kumar, R. K. Singh, R. Mishra, and T. U. Daim, "Roadmap for integrating blockchain with Internet of Things (IoT) for sustainable and secured operations in logistics and supply chains: Decision making framework with case illustration," *Technological Forecasting and Social Change*, vol. 196, p. 122837, 2023, doi: https://doi.org/10.1016/j.techfore.2023.122837.

[2] S. Vasudeva, "Cryptocurrency as an investment or speculation: a bibliometric review study," *Business Analyst Journal*, vol. 44, no. 1, pp. 34-50, 2023, doi: https://doi.org/10.1108/BAJ-07-2022-0008.

[3] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of Blockchain Technology applications for financial services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, p. 100073, 2022, doi: https://doi.org/10.1016/j.tbench.2022.100073.

[4] H. Jamshed, "Survey on Vulnerabilities in Blockchain's Smart Contracts," *Journal of Independent Studies and Research Computing*, vol. 20, no. 2, 2022, doi: DOI: 10.31645/JISRC.22.20.2.2.

[5] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Computers & industrial engineering*, vol. 135, pp. 582-592, 2019, doi: https://doi.org/10.1016/j.cie.2019.06.042.

[6] P. Danese, R. Mocellin, and P. Romano, "Designing blockchain systems to prevent counterfeiting in wine supply chains: a multiple-case study," *International Journal of Operations & Production Management*, vol. 41, no. 13, pp. 1-33, 2021, doi: https://doi.org/10.1108/IJOPM-12-2019-0781.

[7] V. Rakovic, J. Karamachoski, V. Atanasovski, and L. Gavrilovska, "Blockchain paradigm and internet of things," *Wireless Personal Communications*, vol. 106, pp. 219-235, 2019, doi: https://doi.org/10.1109/info.com.2006.231.

[8] A. Kumar *et al.*, "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol. 22, no. 15, p. 5921, 2022, doi: https://doi.org/10.3390/s22155921.

[9] M. Xie, J. Liu, S. Chen, and M. Lin, "A survey on blockchain consensus mechanism: research overview, current advances and future directions," *International Journal of Intelligent Computing and Cybernetics*, vol. 16, no. 2, pp. 314-340, 2023, doi: https://doi.org/10.1108/IJICC-05-2022-0126.

[10] R. Loka, A. M. Parimi, S. Srinivas, and N. M. Kumar, "Leveraging blockchain technology for resilient and robust frequency control in a renewable-based hybrid power system with hydrogen and battery storage integration," Energy Conversion and Management, vol. 283, p. 116888, 2023, doi: https://doi.org/10.1016/j.enconman.2023.116888.

[11] M. Zachariadis, G. Hileman, and S. V. Scott, "Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services," Information and Organization, vol. 29, no. 2, pp. 105-117, 2019, doi: https://doi.org/10.1016/j.infoandorg.2019.03.001

[12] N. Kshetri, "Can blockchain strengthen the internet of things?," IT professional, vol. 19, no. 4, pp. 68-72, 2017, doi: DOI:10.1109/MITP.2017.3051335.

[13] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, 2015: IEEE, pp. 104-121, doi: https:// DOI: 10.1109/SP.2015.14.

[14] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, 2015: IEEE, pp. 104-121, doi: https://DOI: 10.1109/SP.2015.14.

[15] M. Sockin and W. Xiong, "A model of cryptocurrencies," Management Science, 2023, doi: https://doi.org/10.1287/mnsc.2023.4756.

[16] F. Rampone, F. Lecca, P. Giolito, and M. Romano, "Blockchain in the agrifood sector: From storytelling to traceability fact-checking up to new economic models," Economia agro-alimentare/Food Economy, vol. 25, no. 2, pp. 97-114, 2023, doi: DOI:10.3280/ecag2023oa14958.

[17] J. Geng, "Taking Computation to Data: Integrating Privacy-preserving AI techniques and Blockchain Allowing Secure Analysis of Sensitive Data on Premise," 2023, doi: https://doi.org/10.24963/ijcai.2023/741.

[18] P. Mohan, "ENHANCING EDUCATION USING BLOCKCHAIN TECHNOLOGY," doi: https://doi.org/10.1371/journal.pone.0163477.

[19] N. Mansoor, K. F. Antora, P. Deb, T. A. Arman, A. A. Manaf, and M. Zareei, "A Review of Blockchain Approaches for KYC," IEEE Access, 2023, doi: DOI:10.1109/ACCESS.2023.3328536.

[20] A. I. Awad, M. Shokry, A. A. Khalaf, and M. K. Abd-Ellah, "Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach," Computers and Electrical Engineering, vol. 108, p. 108667, 2023, doi: https://doi.org/10.1016/j.compeleceng.2023.108667.

[21] X. Li, Z. Zheng, and H.-N. Dai, "When services computing meets blockchain: Challenges and opportunities," *Journal of Parallel and Distributed Computing*, vol. 150, pp. 1-14, 2021, doi: https://doi.org/10.1016/j.jpdc.2020.12.003.

[22] H. Guo et al., "Decentralized Policy-Hidden Fine-Grained Redaction in Blockchain-Based IoT Systems," Sensors, vol. 23, no. 16, p. 7105, 2023, doi: https://doi.org/10.3390/s23167105.

[23] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by blockchain: Safeguarding internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28-34, 2019, doi: DOI:10.1109/MCE.2019.2892221.

[24] V. K. Mololoth, S. Saguna, and C. Åhlund, "Blockchain and machine° learning for future smart grids: A review," Energies, vol. 16, no. 1, p. 528, 2023, doi: https://doi.org/10.3390/en16010528.

[25] P. Chandra, S. Soni, A. Gupta, P. Kumar, and K. Raj, "THREAT PREVENTION & VULNERABILITY ANALYSIS OF SMART CONTRACTS IN BLOCKCHAIN NETWORKS," doi: DOI:https://doi.org/10.55766/sujst-2023-05-e01234.

[26] T. Navamani, "A review on cryptocurrencies security," Journal of Applied Security Research, vol. 18, no. 1, pp. 49-69, 2023, doi: https://doi.org/10.1080/19361610.2021.1933322.

[27] A. Kuzior and M. Sira, "A bibliometric analysis of blockchain technology research using VOSviewer," Sustainability, vol. 14, no. 13, p. 8206, 2022, doi: https://doi.org/10.3390/su14138206.

[28] R. Saxena, D. Arora, and V. Nagar, "Classifying Transactional Addresses using Supervised Learning Approaches over Ethereum Blockchain," Procedia Computer Science, vol. 218, pp. 2018-2025, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.178.

[29] M. Vishwakarma and N. Kesswani, "A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection," Decision Analytics Journal, vol. 7, p. 100233, 2023, doi: https://doi.org/10.1016/j.dajour.2023.100233.

[30] T. Navamani, "A review on cryptocurrencies security," *Journal of Applied Security Research*, vol. 18, no. 1, pp. 49-69, 2023, doi: https://doi.org/10.1080/19361610.2021.1933322.

[31] R. Saxena, D. Arora, and V. Nagar, "Classifying Transactional Addresses using Supervised Learning Approaches over Ethereum Blockchain," *Procedia Computer Science*, vol. 218, pp. 2018-2025, 2023, doi: DOI:10.1109/ACCESS.2023.3240103.

[32] S. Alam, S. Zardari, and J. Shamsi, "Comprehensive three-phase bibliometric assessment on the blockchain (2012–2020)," *Library Hi Tech*, vol. 41, no. 2, pp. 287-308, 2023, doi: https://doi.org/10.1108/LHT-07-2021-0244.

[33] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," Business & Information Systems Engineering, vol. 62, no. 6, pp. 599-608, 2020. J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," Business & Information Systems Engineering, vol. 62, no. 6, pp. 599-608, 2020, doi: https://doi.org/10.3390/en16031510.

[34]A.-E. Drăgnoiu, M. Platt, Z. Wang, and Z. Zhou, "The more you know: energy labelling enables more sustainable cryptocurrency investments," in 2023 IEEE 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2023: IEEE, pp. 73-78, doi: https://doi.org/10.1016/j.ijinfomgt.2022.102470

[35] V. Malamas, T. K. Dasaklis, V. Arakelian, and G. Chondrokoukis, "A blockchain framework for digitizing securities issuance: the case of green bonds," Journal of Sustainable Finance & Investment, pp. 1-27, 2023, doi: https://doi.org/10.1080/20430795.2023.2275212.