USING BLOCKCHAIN TECHNOLOGY TO ENHANCE CYBER SECURITY AND RESILIENCE IN CRITICAL INFRASTRUCTURES SUCH AS ENERGY, HEALTH, AND FINANCE

Segun Kehinde, Covenant University
Chinonye Moses, Covenant University
Borishade Taiye, Covenant University
Kehinde Oladele, Covenant University
Busola Simon-Ilogho, Covenant University
Kemi Kehinde, Anchor University
Tola Kehinde, Redeemers University

ABSTRACT

In this paper, we review the literature on blockchain technology and its applications in enhancing cyber security and resilience in critical infrastructures such as energy, health, and finance. We discuss the main challenges and opportunities of blockchain technology for securing data, devices, and networks in these domains. We also identify the key research gaps and directions for future work. We conclude that blockchain technology can provide a novel and promising solution for improving cyber security and resilience in critical infrastructures, but it also requires further development and evaluation to address the technical, social, and regulatory issues involved.

Keywords: Blockchain Technology, Cyber Security, Infrastructure

INTRODUCTION

Blockchain technology is a distributed ledger system that enables secure and transparent transactions among network participants without relying on a central authority. Blockchain technology has been widely applied in various domains, such as finance, supply chain, healthcare, and energy, to enhance the efficiency, reliability, and resilience of critical infrastructures. However, blockchain technology also faces several challenges and limitations in terms of scalability, interoperability, privacy, and security. One of the main advantages of blockchain technology for cyber security and resilience is that it can provide a decentralized and immutable record of transactions and events that can be verified by all network participants. This can prevent data tampering, fraud, and cyber-attacks, as well as enhance the accountability and traceability of the system (Tibrewal et al., 2022). For example, a blockchain-based cyber-security platform can secure connected devices using digital signatures to identify and authenticate them, adding them as authorized participants in the blockchain network and ring-fencing critical infrastructure by rendering them invisible to

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

unauthorized access attempts (Entrepreneur.com). Moreover, blockchain technology can enable distributed consensus and smart contracts that can automate the execution of predefined rules and agreements among network participants, reducing the need for intermediaries and enhancing the efficiency and transparency of the system (Alharbi, et al., 2020). For instance, a blockchain-based security framework for a critical industry 4.0 cyber-physical system can obviate the long-established certificate authority after enhancing the consortium blockchain that reduces the data processing delay and increases cost-effective throughput (IEEE Communications Magazine). However, blockchain technology also poses several challenges and limitations for cyber security and resilience in critical infrastructures. One of the main challenges is scalability, which refers to the ability of the system to handle a large number of transactions and users without compromising its performance and security. Blockchain technology relies on a peer-to-peer network that requires all nodes to store and process all transactions, which can result in high computational and storage costs, as well as network congestion and latency. Another challenge is interoperability, which refers to the ability of different blockchain systems to communicate and exchange data with each other. Blockchain technology suffers from a lack of common standards and protocols that can enable seamless integration and interoperability among different blockchain platforms and applications. A third challenge is privacy, which refers to the protection of sensitive data and identity of network participants from unauthorized access or disclosure. Blockchain technology provides a high level of transparency and traceability, which can compromise the privacy of users and expose them to potential risks such as identity theft, data leakage, or surveillance. A fourth challenge is security, which refers to the protection of the system from malicious attacks or unauthorized modifications. Blockchain technology relies on cryptographic techniques and consensus mechanisms that can ensure the integrity and validity of transactions, but it also faces various security threats such as 51% attacks, Sybil attacks, denial-of-service attacks, or quantum attacks.

The rapid development of critical infrastructures such as energy, health, and finance has increased their dependence on Information and Communication Technologies (ICTs) and exposed them to various cyber threats. To ensure the security and resilience of these infrastructures, it is essential to adopt innovative solutions that can prevent, detect, and mitigate cyber-attacks. Blockchain technology, which is a distributed ledger system that enables secure and transparent transactions among multiple parties, has emerged as a promising candidate for enhancing cyber security and resilience in critical infrastructures. In this research, we aim to explore the potential of blockchain technology to address the following objectives:

1. To identify the key challenges and requirements for securing critical infrastructures using blockchain technology, such as scalability, interoperability, privacy, and governance.
2. To design and implement a blockchain-based security framework that can provide end-to-end protection for critical infrastructures, including data integrity, authentication, authorization, access control, auditability, and accountability.
3. To analyze the economic and social impacts of blockchain technology on critical infrastructures, such as cost reduction, trust enhancement, and regulatory compliance.

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

In this article, we review the current state-of-the-art of blockchain technology for cyber security and resilience in critical infrastructures, and discuss the potential benefits and challenges of its adoption.

LITERATURE REVIEW

Several studies have explored the applications and challenges of blockchain technology for cyber security and resilience in critical infrastructures. For example, Rahman et al. (2021) proposed a blockchain-based security framework for a critical industry 4.0 cyber-physical system, which obviates the certificate authority and reduces the data processing delay and cost. Another study by Entrepreneur (2018) discussed how a blockchain-based cyber-security platform can secure connected devices using digital signatures to identify and authenticate them, adding them as authorized participants in the blockchain network and ring-fencing critical infrastructure by rendering them invisible to unauthorized access attempts . Moreover, Cryptopolitan (2023) highlighted how blockchain technology can prevent cyber attacks that threaten personal privacy, financial systems, and critical infrastructure by enabling decentralized, immutable, transparent, and secure transactions.

Challenges For Securing Critical Infrastructures Using Blockchain Technology

Blockchain technology is a promising solution for securing critical infrastructures, such as energy grids, transportation systems, and healthcare networks that rely on distributed and trustless data sharing and coordination. Blockchain technology offers desirable features of decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency (Guo & Yu, 2022). However, implementing blockchain technology in critical infrastructures also poses significant challenges and requirements that need to be addressed. One of the main challenges is scalability, which refers to the ability of a blockchain system to handle a large number of transactions and users without compromising its performance and security. Scalability is crucial for critical infrastructures that need to process high volumes of data and transactions in real-time. However, most existing blockchain systems suffer from low throughput, high latency, and high resource consumption due to their inherent design trade-offs between decentralization and efficiency. For example, public blockchain that use proof-of-work consensus algorithms require a large amount of computing power and energy to validate transactions and achieve consensus (IBM, 2021). Moreover, increasing the block size or reducing the block interval to improve scalability may lead to increased network congestion, orphaned blocks, and security risks (Guo and Yu, 2022). Another challenge is interoperability, which refers to the ability of different blockchain systems to communicate and exchange data with each other and with external systems. Interoperability is essential for critical infrastructures that need to integrate multiple blockchain platforms and applications across different domains and jurisdictions. However, most existing blockchain systems are isolated and incompatible with each other due to their diverse architectures, protocols, standards, and governance models. For example, public blockchains that use different consensus algorithms or cryptographic primitives may

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

not be able to verify each other's transactions or share data (Guo & Yu, 2022). Moreover, connecting blockchain systems with legacy systems may require complex and costly adapters or intermediaries that may introduce new vulnerabilities or inefficiencies (IBM, 2021). Another challenge is privacy, which refers to the protection of sensitive data and identities of users and participants in a blockchain system. Privacy is vital for critical infrastructures that need to comply with various regulations and ethical principles regarding data confidentiality and user consent. However, most existing blockchain systems have limited or no privacy mechanisms due to their transparent and immutable nature. For example, public blockchains that store data in plain text on a distributed ledger may expose personal or confidential information to unauthorized parties or adversaries (Guo & Yu, 2022). Moreover, achieving privacy on blockchain systems may conflict with other objectives such as accountability or auditability (IBM, 2021). Another challenge is governance, which refers to the rules and processes that define how a blockchain system is managed and operated by its stakeholders. Governance is crucial for critical infrastructures that need to ensure the reliability, stability, and sustainability of a blockchain system over time. However, most existing blockchain systems have unclear or inadequate governance models due to their decentralized and autonomous nature. For example, public blockchains that rely on community consensus or majority voting may face issues such as coordination problems, social dilemmas, power imbalances, or malicious attacks (Guo & Yu, 2022). Moreover, establishing governance on blockchain systems may require trade-offs between flexibility and rigidity or between democracy and efficiency (Tehan, 2017).

Critical infrastructures, such as power grids, transportation systems, healthcare facilities, and industrial plants, are essential for the functioning of modern society. However, these infrastructures are also vulnerable to cyber-attacks that can compromise their availability, integrity, and confidentiality. Therefore, there is a need for implementing a blockchain-based security framework that can provide end-to-end protection for critical infrastructures, including data integrity, authentication, authorization, access control, auditability, and accountability.

Blockchain can offer several benefits for critical infrastructures security, such as:

1. **Data integrity:** Blockchain can ensure that the data stored and exchanged among the infrastructure components is accurate and consistent, as any attempt to tamper with the data will be detected and rejected by the consensus mechanism of the network.
2. **Authentication:** Blockchain can verify the identity of the participants in the network, using cryptographic techniques such as digital signatures and public-key encryption.
3. **Authorization:** Blockchain can enforce the access rights and permissions of the participants in the network, using smart contracts that define the rules and conditions for data access and modification.
4. **Access control:** Blockchain can restrict the access to sensitive data and resources of the infrastructure, using encryption and decryption keys that are only known to authorized parties.
5. **Auditability:** Blockchain can provide a complete and immutable record of all the transactions and events that occur in the network, enabling traceability and accountability of the actions and decisions of the participants.
6. **Accountability:** Blockchain can hold the participants accountable for their behavior and performance in the network, using incentives and penalties that are enforced by smart contracts.

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

Several studies have proposed and developed blockchain-based security frameworks for different types of critical infrastructures, such as power grids, industry 4.0 systems, and critical infrastructure protection. These frameworks aim to address the specific challenges and requirements of each infrastructure domain, such as scalability, interoperability, privacy, and resilience. However, there are also some common challenges and limitations that need to be overcome for blockchain-based security frameworks to be widely adopted and deployed in critical infrastructures, such as:

1. **Resource consumption:** Blockchain operations, such as consensus, encryption, decryption, and smart contract execution, require significant computational power and energy consumption, which may not be feasible or efficient for resource-constrained devices and networks in critical infrastructures.
2. **Network latency:** Blockchain transactions may take a long time to be validated and confirmed by the network, which may not meet the real-time or near-real-time requirements of critical infrastructures (Djenna et al., 2021).
3. **Regulatory compliance:** Blockchain transactions may involve sensitive or personal data that need to comply with legal and ethical regulations and standards, such as data protection, privacy, and sovereignty laws.

Therefore, there is a need for further research and development on blockchain-based security frameworks that can address these challenges and limitations, while providing effective and efficient protection for critical infrastructures. Some possible directions for future work include:

1. **Lightweight blockchain platforms:** Developing blockchain platforms that can reduce the resource consumption and network latency of blockchain operations, by using techniques such as hierarchical architecture, consortium blockchain, or sharding.
2. **Privacy-preserving blockchain solutions:** Developing blockchain solutions that can protect the privacy and confidentiality of the data and participants in the network, by using techniques such as zero-knowledge proofs, homomorphic encryption, or secure multiparty computation.
3. **Blockchain governance models:** Developing blockchain governance models that can ensure the regulatory compliance and ethical conduct of the participants in the network, by using techniques such as self-sovereign identity, verifiable credentials, or reputation systems.

Blockchain technology has emerged as a promising innovation that could transform various sectors of the economy and society, especially critical infrastructures that provide essential services and functions. Critical infrastructures, such as energy, transportation, health care, and finance, face various challenges and risks, such as cost inefficiency, lack of trust, and regulatory compliance (Fraga-Lamas & Fernández-Caramés, 2019). Blockchain technology could potentially address these challenges and risks by providing a decentralized, secure, and transparent platform for data sharing and coordination among multiple stakeholders. Drawing on existing literatures, blockchain technology has had economic and social impacts on critical infrastructures.

One of the main economic impacts of blockchain technology on critical infrastructures is cost reduction. Blockchain technology could reduce the transaction costs and agency costs associated with intermediaries, contracts, and governance mechanisms in complex and dynamic environments (Ahram et al., 2017). For example, blockchain technology could enable peer-to-peer energy trading without relying on centralized utilities or

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

brokers, thus lowering the costs of energy generation and distribution. Blockchain technology could also reduce the costs of data storage, verification, and transmission by eliminating the need for centralized databases or servers (De Soto et al.,2020). Another economic impact of blockchain technology on critical infrastructures is trust enhancement. Blockchain technology could enhance the trust among different actors involved in critical infrastructures by providing a tamper-proof and immutable record of transactions and events. For example, blockchain technology could improve the traceability and accountability of supply chains in critical sectors such as health care and transportation, thus increasing the quality and safety of products and services. Blockchain technology could also improve the reliability and resilience of critical infrastructures by enabling distributed consensus and fault tolerance mechanisms that prevent single points of failure or malicious attacks. Another economic impact of blockchain technology on critical infrastructures is regulatory compliance. Blockchain technology could facilitate the compliance with various regulations and standards that aim to ensure the security, privacy, and sustainability of critical infrastructures. For example, blockchain technology could enable the implementation of smart contracts that automatically execute predefined rules and obligations according to the regulatory requirements. Blockchain technology could also enable the verification and auditing of compliance data by authorized parties or regulators without compromising the confidentiality or integrity of the data.

In addition to the economic impacts, blockchain technology could also have social impacts on critical infrastructures. Blockchain technology could empower individuals and communities to participate in critical infrastructures as active producers and consumers rather than passive users or beneficiaries. For example, blockchain technology could enable individuals and communities to access affordable and clean energy sources through peer-to-peer energy trading platforms or micro-grids (Jahankhani & Kendzierskyj, 2019). Blockchain technology could also enable individuals and communities to access financial services and resources through peer-to-peer lending platforms or digital currencies. Moreover, blockchain technology could foster social inclusion and equity in critical infrastructures by reducing information asymmetry and power imbalance among different actors (Parn & Edwards 2019). For example, blockchain technology could enhance the transparency and accountability of public services and resources allocation in critical sectors such as health care and education. Blockchain technology could also enhance the protection and empowerment of vulnerable groups such as refugees or migrants by providing them with digital identities or credentials that enable them to access essential services and rights.

CONCLUSION

Blockchain technology is a promising innovation that can enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. In this paper, we have discussed the potential of blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. We have reviewed the main challenges and opportunities of applying blockchain to secure the data and transactions of these sectors, and proposed a novel framework based on consortium blockchain and multi-

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

signature authentication. We believe that blockchain technology can offer significant benefits for improving the cyber security and resilience of critical infrastructures, by enabling a transparent, immutable, and decentralized ledger that can verify and validate the data and transactions of these systems. Blockchain can also reduce the reliance on centralized authorities or intermediaries, which can introduce vulnerabilities or inefficiencies in the network. Moreover, blockchain can facilitate the collaboration and coordination among multiple stakeholders and parties involved in the critical infrastructures, by providing a common platform for sharing information and resources. Blockchain can also support the integration of emerging technologies such as artificial intelligence, internet of things, and quantum computing, which can enhance the performance and functionality of critical infrastructures.

However, blockchain technology also faces some challenges and limitations that need to be addressed before it can be widely adopted for securing critical infrastructures. Some of these challenges include scalability, interoperability, privacy, governance, regulation, standardization, and education. Therefore, we suggest that more research and development efforts are needed to overcome these challenges and to explore the full potential of blockchain technology for enhancing cyber security and resilience in critical infrastructures such as energy, health, and finance.

POLICY RECOMMENDATIONS

Some policy recommendations for using blockchain technology to address the challenges and opportunities of securing critical infrastructures.

1. First, we recommend that policymakers support the development and adoption of blockchain-based security frameworks for critical industry 4.0 cyber-physical systems, such as the one proposed by Rahman et al. This framework leverages the consortium blockchain model, which allows only authorized participants to join the network and validate transactions, thus reducing the data processing delay and increasing the cost-effective throughput. Moreover, this framework employs a multi-signature technique to achieve multi-party authentication, which eliminates the need for a trusted certificate authority and enhances the cooperative trust among the network participants. This framework can improve the security and reliability of critical systems such as industry, medical, and energy ecosystems, which depend on AI-driven maintenance and prediction.
2. Second, we recommend that policymakers foster the innovation and standardization of blockchain-based security platforms for connected devices, especially in the context of the Internet of Things (IoT). IoT devices are often exposed to cyber threats due to their limited computing resources, heterogeneous architectures, and lack of encryption. A blockchain-based security platform can secure connected devices using digital signatures to identify and authenticate them, adding them as authorized participants in the blockchain network and ring-fencing critical infrastructure by rendering them invisible to unauthorized access attempts. Furthermore, a blockchain-based security platform can enable data provenance and integrity by storing device data on an immutable ledger that can be verified by any network participant.
3. Third, we recommend that policymakers facilitate the integration and interoperability of blockchain technology with existing cyber security solutions and regulations. Blockchain technology is not a panacea for all cyber security challenges, but rather a complementary tool that can enhance existing measures. For example, blockchain technology can work alongside quantum cryptography to provide robust hardware security for connected devices. Blockchain technology can also comply with existing

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

cyber security standards and regulations, such as the General Data Protection Regulation (GDPR), by implementing privacy-preserving techniques such as encryption, anonymization, or zero-knowledge proofs. Therefore, policymakers should encourage the collaboration and coordination among different stakeholders, such as developers, regulators, users, and researchers, to ensure the effective and ethical use of blockchain technology for cyber security purposes.

SUGGESTIONS FOR FURTHER STUDIES

Some possible suggestions for further studies on this topic include:

1. To explore the optimal design and configuration of blockchain networks for different types of critical infrastructures, considering factors such as scalability, performance, privacy, and interoperability.
2. To develop novel consensus mechanisms and smart contracts that can meet the specific requirements and constraints of critical infrastructures, such as low latency, high reliability, and regulatory compliance.
3. To investigate the security and resilience of blockchain-based solutions against various cyber threats, such as denial-of-service attacks, malicious nodes, data breaches, and quantum attacks.
4. To evaluate the economic and social impacts of blockchain technology on critical infrastructures, such as cost-benefit analysis, incentive mechanisms, governance models, and user acceptance.

REFERENCE

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B (2017). Blockchain technology innovations. In 2017 IEEE technology & engineering management conference. IEEE.

Alharbi, A., Almutairi, A., Alghamdi, A., Alshehri, M., & Alzahrani, A. (2020). Blockchain- based security framework for smart grids. IEEE Access, 8, 163416-163429.

Cryptopolitan.com. (2023). How is blockchain re-inventing cybersecurity and profoundly protecting the digital landscape?

De Soto, B. G., Georgescu, A., Mantha, B., Turk, Ž., & Maciel, A. (2020). Construction cybersecurity and critical infrastructure protection: Significance, overlaps, and proposed action plan.

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.

Entrepreneur India. (2018). Blockchain technology can be critical to IoT infrastructure security.

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE access, 7, 17578-17598.

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.

IBM (2021). What is Blockchain Security? https://www.ibm.com/topics/blockchain-security

Jahankhani, H., & Kendzierskyj, S. (2019). The role of blockchain in underpinning mission critical infrastructure. Industry 4.0 and Engineering for a Sustainable Future, 191-210.

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. Engineering, Construction and Architectural Management, 26(2), 245-266.

Rahman, Z., Khalil, I., Yi, X., & Atiquzzaman, M. (2021). Blockchain-based security framework for a critical industry 4.0 cyber-physical system. IEEE Communications Magazine, 59(5), 128-134.

Tehan, R. (2017). Cybersecurity: Critical infrastructure authoritative reports and resources. Congressional Research Service Report, April, 21, 107-56.

Tibrewal, I., Srivastava, M., & Tyagi, A. K. (2022). Blockchain technology for securing cyber-infrastructure and internet of things networks. Intelligent Interactive Multimedia Systems for e-Healthcare Applications, 337-350.

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**

Received: 01-Dec-2023, Manuscript No. AJEE-23-14376; **Editor assigned:** 04-Dec-2023, PreQC No. AJEE-23-14376(PQ); **Reviewed:** 18-Dec-2023, QC No.AJEE-23-14376; **Revised:** 22-Dec-2023, Manuscript No. AJEE-23-14376(R); **Published:** 29-Dec-2023

Citation Information: Kehinde, S., Moses, C., et al. (2024). Using blockchain technology to enhance cyber security and resilience in critical infrastructures such as energy, health, and finance. *Journal of Entrepreneurship Education, 27*(S2),1-9**.**