Divaneth, D.R., Mapa, M.M.I.S., Konara, G. and Samarakoon, W.K.U.R.M.K.P.K., 2024. Enhancing data security in smart buildings leveraging blockchain technology. In: Sandanayake, Y.G., Waidyasekara, K.G.A.S., Ranadewa, K.A.T.O. and Chandanie, H. (eds). *Proceedings of the 12th World Construction Symposium*, 9-10 August 2024, Sri Lanka. pp. 435-445. DOI: https://doi.org/10.31705/WCS.2024.34. Available from: https://ciobwcs.com/papers/

ENHANCING DATA SECURITY IN SMART BUILDINGS LEVERAGING BLOCKCHAIN TECHNOLOGY

D. Rashmitha Divaneth[1], M.M.I.S. Mapa[2], Gayani Konara[3], and W.K.U.R.M.K.P.K. Samarakoon[4]

ABSTRACT

This article investigates the use of blockchain technology to improve data security in smart buildings, addressing the growing vulnerabilities caused by the interdependence of IoT devices. The paper thoroughly examines the existing issues and limitations of traditional security solutions in smart buildings. Through a comprehensive literature review and qualitative analysis, this research identifies decentralisation, cryptographic mechanisms, transparency, and distributed ledger technology as core features of blockchain that can significantly improve data security and confidentiality in smart buildings. This paper qualitatively assesses the importance of the identified blockchain features which enhance data security in the context of smart buildings aiming to create a secured system environment that enhances data security and prevents unauthorised access. The methodology employs a qualitative approach, including semi-structured interviews with industry experts and data analysis, to validate the effectiveness of the identified blockchain features. According to the findings, blockchain not only improves data transaction security yet nurtures a resilient infrastructure to meet the changing demands of smart building management. The study contributes to academic literature and provides practical insights for professionals looking to adopt blockchain-based security solutions in smart buildings, with implications for legislation and future research paths.

Keywords: *Blockchain Technology; Data Security; Internet of Things; Smart Buildings.*

1. INTRODUCTION

As digitisation progresses, smart buildings have emerged as integral components of the Internet of Things (IoT) revolution, blending sophisticated technologies such as sensors, automation, and data analytics within a cyber-physical-social system to enhance efficiency, comfort, and management (Brad & Murar, 2014). These buildings transform traditional architectures into responsive, interconnected hubs that employ extensive IoT

[1] Undergraduate, Department of Building Economic, University of Moratuwa, Sri Lanka, dilanikaneshapalan@gmail.com
[2] Lecturer, Department of Facilities Management, University of Moratuwa, Sri Lanka, isuru.mapa@uom.lk
[3] Lecturer, Ritsumeikan University, Japan, gy_kaushi@yahoo.com
[4] Lecturer, Department of Facilities Management, University of Moratuwa, Sri Lanka, samarakoonk@uom.lk

devices to optimise various functions. However, this increased connectivity and reliance on networked systems introduce potential security vulnerabilities.

The integration of numerous IoT devices in smart buildings heightens risks such as unauthorised access, data breaches, and other cyber threats that could compromise sensitive information. Such vulnerabilities may lead to significant financial losses, privacy invasions, and even physical harm (Nawari & Ravindran, 2019). Traditional security measures such as encryption protocols and firewalls often fall short due to their centralised nature, which creates single points of failure and exposes systems to sophisticated cybercriminals (Alshahrani, 2021). Amidst these challenges, blockchain technology emerges as a promising solution to bolster data security in smart buildings. Originally developed for digital currencies such as Bitcoin, blockchain offers a decentralised and irreversible ledger system that can significantly secure data transactions and storage (Nehe & Jain, 2019). Its key features are decentralisation, cryptographic hashing, and consensus-based validation for a robust framework for secure, transparent management of building operations and data.

Blockchain ensures tamper-proof records and enhances data integrity by distributing data across a network, thus eliminating single points of failure, and reducing susceptibility to cyberattacks. Its cryptographic protocols enable secure, peer-to-peer transactions and data exchanges, minimising the risks associated with centralised data storage systems. The transparency and immutability of blockchain increase trust and accountability in digital interactions within smart buildings (Ramachandran & Kantarcioglu, 2017). Equipped with blockchain, smart buildings can leverage automated smart contracts to facilitate secure and efficient property management tasks, access control, and energy transactions. These contracts execute automatically based on pre-set rules and conditions, ensuring only authorised entities and devices can operate within the network, thereby bolstering security (Nanayakkara et al., 2021).

However, implementing Blockchain in smart buildings presents challenges such as scalability, interoperability with existing systems, and the energy consumption of blockchain operations, particularly those using proof-of-work consensus mechanisms (Krishnamurthi & Shree, 2021). These challenges necessitate collaborative efforts between blockchain developers, cybersecurity experts, and building management professionals to design solutions that are both effective and sustainable.

This research addresses the vulnerability of IoT-based smart buildings to cyberattacks due to their interconnectedness and the insufficiency of traditional security measures. The main objectives are to review literature on smart buildings, data security, and blockchain technology, and to identify key blockchain characteristics that enhance data security in smart buildings through expert opinions. The study aims to provide valuable insights for researchers and industry professionals on which blockchain features should be prioritised for developing secure systems in smart buildings. Additionally, it seeks to inform policymakers about blockchain's capabilities, promoting its integration into smart building infrastructures to enhance data security. Through analysis and application of blockchain technology, this paper seeks to demonstrate how the convergence of smart building technology and blockchain can lead to more secure, efficient, and user-centric building environments.

2. LITERATURE REVIEW

2.1 DATA SECURITY

Data security involves safeguarding digital data from unauthorised access, corruption, or theft at every phase of its lifecycle. This includes a range of protective measures aimed at maintaining the confidentiality, integrity, and availability of data (Tellenbach et al., 2019). The scope of data security covers a broad spectrum of information protection activities. These activities include protecting physical hardware and storage devices, implementing administrative controls, setting access restrictions, and integrating logical security mechanisms within software applications (Yang et al., 2020). Additionally, organisational policies and procedures are vital in strengthening the overall framework of information security (Yang et al., 2020).

The CIA Triad, comprising confidentiality, integrity, and availability, significantly shapes the criteria for data security. Anand et al. (2020) describe how these three fundamental properties, encapsulated by the CIA Triad, have historically provided the foundation for defining the parameters of data security. Data confidentiality ensures that information is only accessible to those who are allowed to view it, preventing unlawful disclosure. Data integrity is concerned with ensuring that data is accurate and reliable and that it has not been tampered with. Finally, data availability ensures that authorised users may access information when it is required, allowing for smooth and ongoing access.

2.2 DATA SECURITY IN SMART BUILDINGS

The necessity for robust data security in smart buildings is underscored by their reliance on interconnected systems to perform essential operations. The integration of new protocols complicates security frameworks, necessitating comprehensive measures to protect these environments (Ciholas et al., 2019). In contemporary smart buildings, the widespread use of IoT devices and wireless technologies introduces new vulnerabilities to cyber threats. These buildings generate and process extensive data volumes to enhance efficiency but raise concerns regarding data privacy and the potential for unauthorised access or misuse of sensitive information (Ciholas et al., 2019). Additionally, the challenge of managing vast data collections in smart cities can lead to compromised privacy if not properly governed (Li et al., 2016). Moreover, research by Harper et al. (2022) highlights a significant gap in residents' understanding of data collection practices in smart buildings, impacting their privacy. This lack of awareness underscores the urgent need for clearer policies and regulations to protect the privacy of building occupants (Harper et al., 2022).

2.3 BLOCKCHAIN TECHNOLOGY (BCT)

Blockchain technology has revolutionised various industries by offering a decentralised, transparent, and secure method for recording transactions and managing data. Initially developed for Bitcoin, its foundational principles rely on consensus mechanisms and cryptographic techniques to ensure data confidentiality and integrity without a central authority (Nanayakkara et al., 2021; Perera et al., 2020). Beyond cryptocurrencies, blockchain has significant applications in fields such as smart contracts, financial services, healthcare, and education, demonstrating its transformative potential (Beck et al., 2017).

Blockchain's influence extends to sectors such as supply chain management, healthcare, and voting systems, where it provides a secure framework that enhances transparency and promotes innovation (Krichen et al., 2022). However, as blockchain technology evolves, it faces challenges such as scalability, transaction latency, and energy consumption, particularly with Proof of Work processes (Krichen et al., 2022). Ongoing development of alternative consensus mechanisms such as Proof of Stake highlights the technology's adaptability and commitment to overcoming these limitations, supporting sustainable growth and continued innovation across various fields.

2.4 CURRENT APPLICATION OF BLOCKCHAIN TECHNOLOGY

Blockchain technology has evolved beyond Bitcoin, significantly impacting various industries. In finance, it enhances transparency and efficiency in international transactions, reducing costs and boosting security (Krichen et al., 2022). Its influence extends to supply chain management, increasing traceability, reducing fraud, and ensuring product authenticity (Zhu et al., 2020). In the legal and corporate sectors, Blockchain deploys smart contracts to automate processes and streamline operations (Nanayakkara et al., 2021).

Beyond cryptocurrencies, Blockchain transforms financial services by enabling real-time transaction processing and improving fraud protection. For instance, it streamlines financial processes and lowers costs through smart contracts (Polyviou et al., 2019). In healthcare, Blockchain enhances the management of Electronic Health Records (EHRs), protects data and patient privacy, and expedites insurance claims and fraud detection (Angraal et al., 2017). In the industrial sector, blockchain supports Industry 4.0 and the Industrial IoT, improving data quality and security across complex networks. Logistics benefit from real-time tracking and administration of goods and materials (Alladi et al., 2019). Blockchain's adaptability and decentralised nature make it a powerful tool for modernising operations across various fields, promising a future where it is integral to global business and governance strategies.

2.5 BLOCKCHAIN TECHNOLOGY IN THE CONTEXT OF SMART BUILDINGS

Extensive research has explored blockchain's application in smart buildings, particularly its effectiveness in managing smart grid operations, as noted by studies by Alladi et al. (2019). This technology significantly enhances security and privacy through smart contract services in IoT-enabled urban environments, supporting activities such as secure e-voting systems which bolster the security framework of smart cities (Rahman et al., 2020). Blockchain also protects data integrity by preventing unauthorised access or modifications to crucial information systems, overseeing access control, surveillance, and environmental monitoring (Li et al., 2019). Moreover, it streamlines and automates transactions within smart buildings, reducing administrative costs and ensuring the timely execution of maintenance contracts, thereby improving operational efficiency (Nanayakkara et al., 2021). These diverse applications highlight Blockchain's role in transforming urban infrastructure through the integration of advanced technologies in smart buildings.

2.6 FEATURES OF BLOCKCHAIN TECHNOLOGY IN THE CONTEXT OF SMART BUILDINGS

Blockchain technology is revolutionising data management across various industries with its decentralised architecture, enhancing security and efficiency in smart buildings. Key features include:

I. Decentralisation: Distributes data across a network, reducing dependency on central authorities and mitigating risks of centralised system failures (Khalid et al., 2023; Mingxiao et al., 2017).

II. Cryptographic Mechanisms: Employs advanced encryption and hashing to secure data, enhancing confidentiality and preventing data breaches (Ahubele & Musa, 2022; Raikwar et al., 2019).

III. Consensus Mechanisms: Facilitates agreement among network nodes to validate transactions, ensuring data accuracy and trust (Kassab, 2021).

IV. Transparency: Provides clear, verifiable records of transactions while maintaining user privacy, which enhances trust and compliance (Afanasyev et al., 2020).

V. Distributed Ledger: Maintains data consistency and availability even if some nodes are compromised (Karaarslan & Konacakli, 2020).

VI. Immutability: Prevents data alteration after recording, providing a strong defence against tampering and enhancing transaction reliability (Ratta et al., 2021).

VII. Interoperability: Interoperability in blockchain enhances data security by enabling secure data exchange across blockchain systems, protecting data integrity and reducing security breaches through decentralisation (Khalid et al., 2023).

These features underscore Blockchain's potential to enhance security protocols and operational efficiency in smart building environments, supporting data management systems against a variety of threats and failures.

3. RESEARCH METHODOLOGY

To enhance data security in smart buildings using Blockchain technology, characteristics of Blockchain technology which aid in enhancing data security were identified based on existing literature. Qualitative research tools are used to extensively study and understand human experiences and social phenomena, capturing expressive aspects that quantitative methods may miss (Busetto et al., 2020).

Initially, a comprehensive review of the literature was carried out to understand the key concepts, such as Blockchain technology, smart buildings, and data security. A comprehensive analysis of some sub-elements, such as features and the evolution of Blockchain technology, was adequately addressed in this piece of work.

To gather data for the analysis, semi-structured interviews were conducted with four industry experts specialising in data security within the information technology sector, guided by a structured interview protocol. The aim was to collect expert opinions on each Blockchain characteristic identified in the literature and to pinpoint the most significant features of blockchain technology that could enhance data security in the context of smart buildings by conducting a thematic analysis. Interviews were conducted with four interviewees, selected for their expertise in the data security sector and their managerial

or higher roles. The number of interviews was limited to four due to the extreme scarcity of experts in the data security sector who are knowledgeable about Blockchain technology in Sri Lanka (refer to Table 1).

Table 1: Interviewee profile

Respondent	Profession	Designation	Expertise	Experience in the industry
I01	Managed Security Services	Analyst	Information Security/Blockchain	4 years
I02	Information Security	Engineer	Information Security	5 years
I03	Information Security	Engineer	Information Security	5 years
I04	Cloud Technologies	Project Manager	Data security/Blockchain	8 years

4. RESEARCH FINDINGS AND RESULTS

4.1 THEMATIC ANALYSIS

Information derived from the expert interviews with data security experts allowed for the classification of each variable identified through literature. The interview guideline was developed based on the characteristics of Blockchain identified as related to enhancing data security in smart buildings. The questions were structured to obtain the interviewees' opinions on the importance of each identified characteristic in enhancing data security within the context of smart buildings. The interviewees rated the importance of each variable as Highly Important, Moderately Important, and Less/Not Important. A thematic analysis was then conducted, treating these identified characteristics as themes.

Table 2 represents the opinions of the interviewees regarding the importance of each blockchain technology characteristic to enhance data security in smart buildings (Interviewees are denoted as IO1, IO2, IO3 and IO4).

Table 2: Importance of blockchain technology characteristics

Themes	I01	I02	I03	I04
Decentralisation	✔	✔	✔	✔
Cryptography Mechanisms	✔	✔	✔	✔
Transparency	✔	✔	✔	✔
Distributed Ledger Technology	✔	✔	✔	✔
Immutability	○	○	✕	✔
Consensus Mechanisms	○	✔	○	○
Interoperability	○	✕	✕	✕

Highly Important ✔ Moderately Important ○ Not /Less Important ✕

4.2 RESULTS AND DISCUSSION

The opinions of each interviewee on the importance of the identified blockchain characteristics are summarised in Table 2.

Decentralisation is unanimously recognised by interviewees as a pivotal feature for enhancing security in smart buildings. As I01 and I02 emphasize, decentralisation distributes control across the network, thus increasing robustness and reliability ("... *decentralisation is a critical feature of Blockchain to increase system security and stability," I01; "...decentralisation in smart buildings is extremely important,"* I02). This view is also supported by literature indicating that decentralisation minimises vulnerabilities and dependency on central authorities (Khalid et al., 2023; Mingxiao et al., 2017; Nawari & Ravindran, 2019).

Cryptography is vital for ensuring the security of data within smart building systems, as acknowledged by all interviewees. Techniques such as encryption help maintain the confidentiality, integrity, and authenticity of transactions, making cryptographic mechanisms indispensable ("...*cryptography in my opinion contributes greatly to security*," I02). The literature reinforces this perspective, highlighting the role of cryptographic algorithms in developing secure systems and the foundation they provide for preserving data security (Leng et al., 2022; Ahubele & Musa, 2022; Raikwar et al., 2019; Zhang et al., 2020).

Transparency is heralded for its role in enhancing data security and trustworthiness within systems, particularly when balanced with privacy. Interviewees argue that transparency fosters accountability and trust while protecting sensitive information ("...*transparency offered by blockchain makes the system a lot more trustworthy and secure*," I04). The literature suggests that transparency can improve data security and trustworthiness by developing accountability, although it raises privacy concerns (Afanasyev et al., 2020; Lu et al., 2021).

DLT is recognised for its significant impact on enhancing data security by distributing the ledger across a network, effectively reducing unauthorised access and data tampering ("...*blockchain's distributed ledger feature is a game-changer for data security in smart buildings*," I04). Literature corroborates the efficacy of DLT in syncing across the network and minimising data tampering threats, underscoring its crucial role in protecting against cyberattacks (Karaarslan & Konacakli, 2020; Lyu et al., 2023).

Immutability is valued for its role in maintaining a tamper-resistant record of transactions, crucial for data integrity and trust. It is considered a sub-feature of the distributed nature of blockchain that enhances security by reducing data tampering ("*The immutability characteristic of Blockchain technology significantly impacts the security of data*," I04). This characteristic aligns with the consensus that immutability ensures data remains unchanged and secure. These insights highlight immutability as a sub-feature in the distributed nature of Blockchain, maintaining a tamper-resistant record of transactions, crucial for data integrity and trust.

Consensus mechanisms are highlighted for their critical role in validating transactions, indirectly contributing to data security. They are essential for maintaining the integrity and reliability of the network, as they validate and secure transactions across Blockchain systems ("...*consensus mechanism plays a crucial role in preserving the integrity and reliability of the network*," I03). Literature supports this by showing how consensus

mechanisms, such as Proof of Work and Proof of Stake, are pivotal in ensuring data privacy and network security (Kassab, 2021; Wei et al., 2021; Yassein et al., 2019). These viewpoints identify consensus mechanisms as an indirect contribution of consensus procedures to improved data security in smart buildings.

Interoperability is discussed with varied opinions on its direct impact on data security. It is recognised for enhancing the functionality and quality of Blockchain technologies, facilitating wider adoption, though not necessarily boosting data security directly ("*...it's more of a feature that enhances the quality of what Blockchain offers*," I04). The literature notes interoperability's importance for Blockchain development and acceptance yet points to potential security vulnerabilities (Domingo-Ferrer et al., 2022).

The findings indicate that decentralisation, cryptographic mechanisms, transparency, and distributed ledger characteristics were identified as the most important factors for enhancing data security in smart buildings by four interviewees. These insights underscore immutability as a sub-feature inherent in the distributed nature of Blockchain, maintaining a tamper-resistant record of transactions essential for data integrity and trust. Consensus mechanisms were identified as a characteristic indirectly contributing to improved data security in smart buildings, while interoperability was considered a characteristic that does not have a direct impact on enhancing data security in smart buildings.

5. CONCLUSIONS

This research focuses on a complete exploration of the applicability of Blockchain technology in enhancing data security within the context of smart buildings, motivated by the significant vulnerabilities presented by modern interconnected systems. The study thoroughly identified and analysed various characteristics of Blockchain that could be leveraged to fortify the security frameworks of smart buildings, effectively countering the cyber threats that these advanced infrastructures face. Among these characteristics, industry experts emphasised decentralisation, cryptographic techniques, transparency, and distributed ledger technology as important for establishing a robust defence against the variety of security challenges frequently encountered today.

Decentralisation emerged as a prominent feature, crucial for mitigating risks associated with centralised data control, which often leads to single points of failure. By dispersing data across a network, blockchain reduces the impact of cyber-attacks and enhances system resilience. Cryptographic mechanisms protect sensitive information from unauthorised access with robust encryption. This not only secures data transactions yet maintains confidentiality within smart buildings. Transparency, another significant attribute of Blockchain, fosters trust and accountability in transactions. Blockchain enables traceable and verifiable record-keeping, crucial in environments where data integrity and auditability are key. Its immutable nature ensures that records cannot be altered without consensus, preventing tampering and enhancing reliability. Distributed ledger technology supports this by maintaining data consistency and availability, ensuring system functionality even if parts of the network are compromised.

The integration of these Blockchain characteristics into smart building management not only secures data transactions yet introduces efficiency in operations through automated processes such as smart contracts, which execute tasks based on predefined rules and agreements without human intervention. This automation potential, coupled with

enhanced security features, points towards a transformative shift in how building management systems operate, making them more secure, efficient, and user-centric.

In conclusion, the application of Blockchain in smart buildings presents a promising avenue to address the complex security and operational challenges posed by the digital era. By adopting Blockchain, stakeholders in the smart building sector can ensure a more secure, transparent, and efficient management system, thereby safeguarding both data and infrastructure. Future research should continue to explore and refine Blockchain applications in this field, focusing on scalability, energy efficiency, and integration with existing technologies, to fully realise its potential in enhancing smart building environment.

This study is limited by the possibility of response bias due to how data collection was conducted. Since the technology itself is very new, different respondents might have different views and understandings, leading to varied responses. The limitations of such methods can be overpowered in future studies by taking more stringent and varied data collection methods that would take measures to reduce response bias, along with increasing the levels of awareness and education regarding Blockchain technology, ensuring a more informed and consistent set of responses from participants.

6. REFERENCES

Afanasyev, V. Y., Lyubimova, N. G., Ukolov, V. F., & Shayakhmetov, S. R. (2020). Impact of blockchain technology for modification of the supply chain management in energy markets. *International Journal of Supply Chain Management*, *9*(3), 757-762. https://download.garuda.kemdikbud.go.id/article.php?article=1730561&val=13549&title=impact%20of%20blockchain%20technology%20for%20modification%20of%20the%20supply%20chain%20management%20in%20energy%20markets

Ahubele, B. O., & Musa, M. O. (2022). Towards a scalable and secure blockchain based on post-quantum cryptography. *International Journal of Advanced Research in Computer and Communication Engineering*, *11*(7). https://doi.org/10.17148/ijarcce.2022.11703

Alladi, T., Chamola, V., Parizi, R. M., & Choo, K. R. (2019). Blockchain applications for Industry 4.0 and industrial IoT: A review. *IEEE Access*, *7*, 176935–176951. https://doi.org/10.1109/access.2019.2956748

Alshahrani, M. M. (2021). Secure multifactor remote access user authentication framework for IoT networks. *Computers, Materials & Continua*, *68*(3), 3235–3254. https://doi.org/10.32604/cmc.2021.015310

Anand, P., Singh, Y., Selwal, A. K., Alazab, M., Tanwar, S., & Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges. *IEEE Access*, *8*, 168825–168853. https://doi.org/10.1109/access.2020.3022842

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology. *Circulation. Cardiovascular Quality and Outcomes*, *10*(9). https://doi.org/10.1161/circoutcomes.117.003800

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering*, *59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*, *2*(1). https://doi.org/10.1186/s42466-020-00059-z

Ciholas, P., Lennie, A., Sadigova, P., & Such, J. M. (2019, January 17). *The Security of Smart Buildings: a Systematic Literature Review*. arXiv.org. http://arxiv.org/abs/1901.05837

Domingo-Ferrer, J., Blanco-Justicia, A., Manjon, J., & Sanchez, D. (2022). Secure and privacy-preserving federated learning via co-utility. *IEEE Internet of Things Journal*, *9*(5), 3988–4000. https://doi.org/10.1109/jiot.2021.3102155

Harper, S., Mehrnezhad, M., & Mace, J. (2022). User privacy concerns in commercial smart buildings1. *Journal of Computer Security*, *30*(3), 465–497. https://doi.org/10.3233/jcs-210035

Karaarslan, E., & Konacaklı, E. (2020). Data storage in the decentralized world: Blockchain and derivatives. *User Privacy Concerns in Commercial Smart Buildings*, 37–69. https://doi.org/10.26650/b/et06.2020.011.03

Kassab, M. (2021, September 20-24). *Exploring non-functional requirements for blockchain-oriented systems*. 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), Notre Dame. https://doi.org/10.1109/rew53955.2021.00040

Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., Ullah, S. S., & Nayab, N. (2023). A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access*, *11*, 10995–11015. https://doi.org/10.1109/access.2023.3240237

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors*, *22*(14), 5274. https://doi.org/10.3390/s22145274

Krishnamurthi, R., & Shree, T. (2021). A brief analysis of blockchain algorithms and its challenges. In *IGI Global eBooks* (pp. 23–39). https://doi.org/10.4018/978-1-7998-5351-0.ch002

Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2022). Blockchain security: A survey of techniques and research directions. *IEEE Transactions on Services Computing*, *15*(4), 2490–2510. https://doi.org/10.1109/tsc.2020.3038641

Li, Y., Dai, W., Ming, Z., & Qiu, M. (2016). Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, *65*(5), 1339–1350. https://doi.org/10.1109/tc.2015.2470247

Lu, Y., Liu, Z., Wang, S., Li, Z., Liu, W., & Chen, X. (2021). Temporal index scheme of hyperledger fabric system in IoT. *Wireless Communications and Mobile Computing*, *2021*, 1–15. https://doi.org/10.1155/2021/9945530

Lyu, Z., Cheng, C., Lv, H., & Song, H. (2024). Blockchain based intelligent resource management in distributed digital twins cloud. *IEEE Network*, *1*. https://doi.org/10.1109/mnet.2023.3326099

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October 5-8). *A review on consensus algorithm of blockchain*. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff. https://doi.org/10.1109/smc.2017.8123011

Nanayakkara, S., Perera, S., Senaratne, S., Weerasuriya, G. T., & Bandara, H. M. N. D. (2021). Blockchain and smart contracts: A solution for payment issues in construction supply chains. *Informatics*, *8*(2), 36. https://doi.org/10.3390/informatics8020036

Nawari, N. O., & Ravindran, S. (2019). Blockchain and the built environment: Potentials and limitations. *Journal of Building Engineering*, *25*, 100832. https://doi.org/10.1016/j.jobe.2019.100832

Nehe, M., & Jain, S. A. (2019, March 8-9). *A survey on data security using blockchain: Merits, demerits and applications*. 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), Nagercoil. DOI: 10.1109/ICRAECC43874.2019.8995064

Perera, S., Nanayakkara, S., Rodrigo, M., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration*, *17*, 100125. https://doi.org/10.1016/j.jii.2020.100125

Polyviou, A., Velanas, P., & Soldatos, J. (2019). Blockchain technology: Financial sector applications beyond cryptocurrencies. *Proceedings*, *28*(1). https://doi.org/10.3390/proceedings2019028007

Rahman, A., Nasir, M. K., Rahman, Z., Mosavi, A., S, S., & Minaei-Bidgoli, B. (2020). DistBlockBuilding: A distributed blockchain-based SDN-IoT network for smart building management. *IEEE Access*, *8*, 140008–140018. https://doi.org/10.1109/access.2020.3012435

Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SOK of used cryptography in blockchain. *IEEE Access*, *7*, 148550–148575. https://doi.org/10.1109/access.2019.2946983

Ramachandran, A., & Kantarcioglu, M. (2017, September 28). *Using Blockchain and smart contracts for secure data provenance management*. arXiv. https://arxiv.org/abs/1709.10000

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *Journal of Food Quality*, *2021*, 1–20. https://doi.org/10.1155/2021/7608296

Tellenbach, B., Rennhard, M., Schweizer, R. (2019). Security of data science and data science for security. In M. Braschler, T. Stadelmann, & K. Stockinger (Eds.) *Applied Data Science*. (pp. 265-288). Springer. https://doi.org/10.1007/978-3-030-11821-1_15

Wei, Y., Liang, L., Zhou, B., & Feng, X. (2021, June 4-7). *A modified blockchain DPoS consensus algorithm based on anomaly detection and reward-punishment*. 2021 13th International Conference on Communication Software and Networks (ICCSN), Chongqing. https://doi.org/10.1109/iccsn52437.2021.9463634

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723–131740. https://doi.org/10.1109/access.2020.3009876

Yassein, M. B., Shatnawi, F., Rawashdeh, S., & Mardin, W. (2019, November 3-7). *Blockchain technology: Characteristics, security and privacy; issues and solutions*. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi. https://doi.org/10.1109/aiccsa47632.2019.9035216

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 1–34. https://doi.org/10.1145/3316481

Zhu, L., Zheng, B., Shen, M., Gao, F., Li, H., & Shi, K. (2020). Data security and privacy in bitcoin system: A survey. *Journal of Computer Science and Technology/Journal of Computer Science and Technology*, *35*(4), 843–862. https://doi.org/10.1007/s11390-020-9638-7