Computer Science and Information Technologies
Vol. 6, No. 2, July 2025, pp. 214∼224
ISSN: 2722-3221, DOI: 10.11591/csit.v6i2.pp214-224

Blockchain technology for optimizing security and privacy in distributed systems

Wisnu Uriawan, Adryan Putra Pratama, Shafwan Mursyid
Department of Informatics, Faculty of Science and Technology, UIN Sunan Gunung Djati, Bandung, Indonesia

Article Info

Article history:

Received Jul 21, 2023
Revised May 9, 2025
Accepted May 23, 2025

Keywords:

Blockchain
Distributed systems
Privacy
Security
Technology

ABSTRACT

Blockchain technology is increasingly recognized as an effective solution for addressing security and privacy challenges in distributed systems. Blockchain ensures information security by validating data and defending against cyber threats, while guaranteeing data integrity through transaction validation and reliable storage. The research involves a literature study, problem identification, analysis of blockchain security and privacy, model development, testing, and analysis of trial results. Furthermore, blockchain enables user anonymity and fosters transparency by utilizing a distributed network, reducing the risk of fraudulent activities. Its decentralized nature ensures high reliability and accessibility, even in node failures. Blockchain enhances security and privacy by offering features like data immutability, provenance, and reduced reliance on trust. It decentralizes data storage, making tampering or deletion extremely challenging, and ensures the invalidation of subsequent blocks upon any changes. Blockchain finds applications in various domains, including supply chains, finance, healthcare, and government, enabling enhanced security by tracking data origin and ownership. Despite scalability and security challenges, the potential benefits of reduced costs, increased efficiency, and improved transparency position blockchain as a promising technology for the future. In summary, blockchain technology provides secure transaction recording and data storage, thus enhancing security, privacy, and the integrity of sensitive information in distributed systems.

Corresponding Author:

Shafwan Mursyid
Department of Informatics, Faculty of Science and Technology, UIN Sunan Gunung Djati
Bandung, Indonesia
Email: shafwanmursyid88@gmail.com

1. INTRODUCTION

Distributed systems have been used in various fields, including finance, healthcare, automobile, risk management, internet of things (IoT), and public and social services. While distributed systems offer many benefits, they also have potential drawbacks when it comes to security and privacy. One of the potential drawbacks of using distributed systems is centralized control, which can lead to a single point of failure or attack [1]. The central authority controlling the system is compromised, the entire system can be compromised as well, another potential drawback of using distributed systems is the lack of transparency and immutability of data. Unlike blockchain systems, distributed systems may not have the same level of transparency and immutability, which can lead to potential security and privacy concerns [2], that data can be easily altered or deleted, which can decrease the reliability of the data. Data leaks are also a potential drawback of using

distributed systems.

Distributed systems can have privacy concerns due to the potential for data leaks or unauthorized access to data [2], that sensitive data may be exposed to unauthorized parties, which can lead to potential security and privacy concerns. Finally, the lack of trust is another potential drawback of using distributed systems. Distributed systems may not have the same level of trust as blockchain systems, which can lead to potential security and privacy concerns [3]. This means that users may not be able to trust the system to protect their data and privacy. Overall, while distributed systems offer many benefits, they also have potential drawbacks when it comes to security and privacy. These drawbacks include centralized control, lack of transparency and immutability of data, data leaks, and lack of trust. Blockchain technology can help address some of these potential drawbacks by providing decentralization and distributed data management, preserving data privacy, increasing the reliability and transparency of data, using smart contracts, and combining blockchain and artificial intelligence (AI) technologies.

Security and privacy are two important aspects of distributed systems. Blockchain technology has the ability to increase security and privacy in distributed systems because every transaction is protected with strong cryptographic keys and user identities are encrypted so that they can only be accessed with proper authorization. In addition, blockchain technology also allows each user to verify each transaction and avoid fraud or detrimental actions. However, while blockchain technology has the potential to improve security and privacy in distributed systems, its implementation also requires a good understanding of the technology and how to optimize it. Apart from that, blockchain technology also has several challenges such as scalability and high transaction fees. Therefore, there is a need for further research and development in the implementation of blockchain technology in distributed systems [4]. Blockchain technology has gained significant attention in recent years as a secure and decentralized system for storing and sharing information. Its unique features, such as immutability, transparency, and decentralization, have made it an attractive solution for a variety of use cases, including finance, supply chain management, and healthcare [5]. Blockchain technology has emerged as a promising solution for enhancing security and privacy in distributed systems. With its decentralized and immutable nature, blockchain provides a secure and trustworthy mechanism for storing and exchanging information [6].

2. RESEARCH METHOD

This research describes various stages to achieve the results that will prove that blockchain privacy and security that able to improve the services.

2.1. Problem identification

The initial phase of this research involves identifying the security and privacy challenges faced by distributed systems. These challenges may include data breaches, unauthorized access, and lack of transparency. By closely examining these issues, we aim to gain a deeper understanding of the specific obstacles that hinder the security and privacy of distributed systems. This step also entails defining the objectives and research questions that will guide our investigation and form the basis for our methodology.

2.2. Literature review

To establish a foundation for this research, it conduct an extensive review of existing literature on blockchain technology and its applications in optimizing security and privacy in distributed systems. These literature review will encompass a wide range of sources, including academic papers, industry reports, and case studies. By thoroughly examining the body of knowledge in this field, we can identify relevant studies, frameworks, and approaches that have addressed similar security and privacy challenges. This review will serve as the basis for developing our methodology and providing a comprehensive understanding of the current state of research in this domain.

2.3. Results and analysis

In this phase, present and analyze the findings obtained from our research, which may include both theoretical analysis and empirical studies. By integrating blockchain technology into distributed systems, the purpose is to evaluate its impact on the security and privacy aspects. We assess the improvements achieved, such as enhanced data protection, increased transparency, and stronger access controls. Moreover, identifying any limitations or trade-offs encountered during the implementation of blockchain technology and discussing

their implications. Through rigorous analysis, we will provide insights into the effectiveness of blockchain technology in optimizing security and privacy in distributed systems.

2.4. Conclusion

In the final phase of this research, we will summarize the key findings derived from our study. We will emphasize the benefits of integrating blockchain technology as a means to optimize security and privacy in distributed systems. The conclusions drawn from our analysis will be presented, highlighting the implications and potential impact of this research on the field. We will provide recommendations for practitioners, researchers, and policymakers based on our findings, aiming to guide future endeavors and foster the adoption of blockchain technology for improved security and privacy in distributed systems.

2.5. Future work

Identifying potential areas for future research and development is crucial for advancing the field of blockchain technology for security and privacy in distributed systems [7], [8]. In this phase, we will outline the opportunities for further investigation and propose innovative approaches, methodologies, or technologies that can enhance security and privacy in distributed systems. We will also highlight any research gaps or unresolved issues that require further exploration. By delineating future work, we aim to inspire researchers and practitioners to delve deeper into this field and contribute to its growth.

3. RESULTS AND DISCUSSION

In this section, we provide the results of the research and give a comprehensive discussion (contribution). The discussion shows opportunities for future work or further research.

3.1. Result

Blockchain has become an increasingly popular topic in recent years due to its ability to provide innovative security and privacy solutions. This research discusses the ability of blockchain technology to optimize security and privacy in distributed systems. Firstly, blockchain offers strong information security by validating data in linked blocks. This ensures that data is difficult to branch or edit without the approval of all nodes in the network. Therefore, blockchain technology can help protect sensitive information from cyber attacks or hacking. This is especially important for companies and organizations that need protection against ever-increasing cyber-attacks.

Secondly, the blockchain also ensures data integrity by validating each new transaction before it is entered into the network. This makes the data cannot be edited without the consent of all nodes in the network, thereby ensuring that the data stored is accurate and reliable. Data integrity is an important factor in many businesses and organizations, especially when there are financial transactions being carried out. The next, blockchain enables anonymity for users by storing their identity in the form of a digital address that cannot be traced back to their original identity [9]. This makes blockchain technology suitable for applications that require privacy such as online payments or fund transfers. This provides privacy protection for users without compromising security. Blockchain makes data and transactions transparent because data is stored in a distributed network and can be accessed by anyone with access to the network. This helps reduce the risk of abuse or fraud, thereby ensuring that the data and transactions stored are accurate and reliable. This transparency gives confidence to users that their data will be processed correctly and transactions will be carried out honestly and fairly. Blockchain has high reliability because data is stored in a distributed network. If one of the nodes is damaged, data can still be accessed through other nodes. This ensures that data remains available and accessible even if there is an interruption at one of the nodes in the network. This reliability is very important in distributed systems that require high accessibility.

Blockchain technology is a revolutionary solution for enhancing security and privacy in distributed systems. By utilizing its unique features, organizations can mitigate various vulnerabilities and safeguard sensitive information. One significant advantage of blockchain is its ability to maintain data immutability. Through cryptographic linking of blocks, the integrity of data becomes practically unalterable, providing assurance against unauthorized modifications. Additionally, blockchain's distributed consensus mechanism strengthens security by eliminating the dependence on a single controlling entity. This decentralization prevents fraudulent activities and ensures the overall system's reliability. Moreover, blockchain systems employ robust authentication measures, guaranteeing the verification of user identities and thwarting unauthorized access attempts.

Furthermore, privacy concerns can be addressed using blockchain technology. By encrypting data, only authorized individuals possess the decryption keys, granting them exclusive access. This capability is particularly crucial for sensitive information such as medical records or financial details, where maintaining privacy is truly important. Real-world applications of blockchain technology illustrate its potential in optimizing security and privacy in various sectors. For instance, in supply chain management, blockchain enables traceability, ensuring the authenticity and origin of goods while combating counterfeiting [10].

In healthcare, blockchain-based systems securely store patient records, protecting sensitive data and facilitating efficient access for healthcare providers. Financial services have also leveraged blockchain technology to create innovative products and services. Smart contracts, powered by blockchain, enable automated and transparent financial transactions, enhancing efficiency and security. As blockchain technology continues to advance, we can anticipate further groundbreaking applications that capitalize on its ability to optimize security and privacy in distributed systems. Its potential to transform industries and protect valuable data is undoubtedly a compelling prospect for the future.

Blockchain technology famous in various fields, including: finance, healthcare, automobile, risk management, IoT, and public and social services [11], [12]. Blockchain technology offers enhanced reliability and efficiency, it is crucial to acknowledge the security, privacy concerns, and challenges associated with this cutting-edge technology. A comprehensive survey encompassing technical and application perspectives has yet to be undertaken. However, in a recent survey paper, the authors aim to bridge this gap by conducting an extensive examination of blockchain technology. Exploring various aspects, such as its structure, different consensus algorithms, the challenges and opportunities related to data security, and privacy in blockchains. Additionally, the authors provide insights into potential future trends and advancements that the blockchain technology may adopt in the coming years [12], [13].

Blockchain technology has revolutionized the concept of trust by offering a decentralized and distributed data management solution that ensures security, privacy, and data integrity without relying on intermediaries. However, it is important to acknowledge the existing technological difficulties and limitations associated with blockchain. In a systematic comparative study, researchers have examined the current applications of blockchain in cyber-security. The paper assesses the advantages that blockchain brings to the field of cyber-security and provides a comprehensive overview of recent studies and blockchain applications in various cyber-security domains. By addressing security challenges, the paper identifies and thoroughly investigates four key security issues related to blockchain through extensive research and analysis of existing work [13].

A survey paper highlights the potential of blockchain technology as a solution for enhancing security in electronic health record (EHR) systems. However, the use of blockchain as a public database poses potential privacy challenges for raw or encrypted data stored in the public ledger, as sensitive information may be at risk of exposure during statistical attacks. To address this, data in the ledger can be stored in an encrypted format using various cryptographic techniques, thereby safeguarding data privacy. Additionally, users can adopt pseudo-anonymity measures to protect their real identities while engaging with the system [1].

The growing interest in Central Bank Digital Currencies (CBDCs) has emphasized the importance of implementing suitable security technologies to protect the privacy of CBDCs users. While the architecture of the CBDCs system shares connections with legacy payment systems and public blockchain systems, the security and privacy challenges of CBDCs differ significantly from existing systems due to their focus on auditable privacy. A survey paper provides a comprehensive classification of security and privacy issues in CBDCs systems across key areas such as identity, transactions, consensus, and auditability. Additionally, the paper highlights research gaps arising from the unique characteristics of CBDCs, including challenges related to authorized audit risk and cross-border payments [14].

Smart environments encompass a wide range of interconnected devices and computing units aimed at enhancing human life. As data generation within these environments continues to surge, the need for efficient data management becomes crucial. To address this, many enterprises are turning to blockchain technology as a viable solution. Blockchain, functioning as a distributed transaction ledger, offers data reliability and transparency. However, blockchain technology encounters inherent security challenges such as denial of service (DoS), eclipse and double spending attacks, as well as advanced persistent threat (APT) and malware risks. To tackle these challenges, advanced anomaly detection and mitigation approaches, particularly those utilizing AI techniques such as: machine learning, deep learning, and federated learning. The combined utilization of AI and blockchain technology enables accurate anomaly detection within blockchain networks.

In a survey paper, the authors delve into the obstacles faced by blockchain deployment in smart

environments. Furthermore, they explore the potential of AI-based anomaly detection techniques as a solution to security issues in such environments. Their proposed framework emphasizes the integration of AI-based anomaly detection methods to effectively address security concerns [15]. Blockchain technology offers many advantages in optimizing security and privacy in distributed systems. This can help protect sensitive information from cyber attacks, ensure data integrity, provide anonymity for users, ensure transparency and trust, and high reliability in accessing data. By leveraging blockchain technology, organizations and companies can improve security and privacy in their distributed systems, thereby strengthening their position in the market. This proves that blockchain is a technology that can increase the security and privacy of distributed systems. Apart from that, blockchain technology also ensures data integrity by validating each new transaction before it is entered into the network. Thus, the data stored in the blockchain is very difficult to edit without the consent of all nodes in the network [13].

In a distributed system using traditional technology, data stored at each node in the network can be falsified or altered by irresponsible parties, causing data inaccuracies and affecting the integrity of the system as a whole. Apart from that, anonymity is another important feature in blockchain technology. By storing users' identities in the form of digital addresses that cannot be traced back to their original identities, blockchain technology enables better privacy for users. This makes blockchain technology suitable for applications that require privacy such as online payments or fund transfers. In traditional systems, online transactions can be tracked and monitored by certain parties, thereby increasing the risk of disclosing personal information. However, by using the blockchain, users can maintain their anonymity while making online transactions. In addition to maintaining security and privacy, blockchain technology can also increase transparency in distributed systems.

The data and transactions stored on the blockchain are accessible to anyone with access to the network. This helps reduce the risk of abuse or fraud, thereby ensuring that the data and transactions stored are accurate and reliable. In a distributed system that uses traditional technology, data and transactions may not be accessible to all parties involved, increasing the risk of abuse or fraud. However, using the blockchain, each new transaction must be verified by all nodes in the network before being included in the block, thus ensuring that the data and transactions stored are accurate and trustworthy. Then, reliability is another feature of blockchain technology that makes it ideal for use in distributed systems. Because data is stored in a distributed network, if one node is damaged, data can still be accessed through other nodes. This ensures that data remains available and accessible even if there is an interruption at one of the nodes in the network.

Blockchain technology has various features that make it an effective solution for increasing security and privacy in distributed systems. In this research, the authors have discussed information security, data integrity, anonymity, transparency, and reliability as key features of blockchain technology that can help improve security and privacy in distributed systems. Therefore, blockchain technology can be used as an effective solution to fix vulnerabilities of scattered systems that are often vulnerable to cyber attacks or hacks. Blockchain also offers solutions to improve security and privacy in distributed systems. For example, in a distributed system using traditional technology, data stored at each node in the network can be accessed by anyone who has access to that node. This increases the risk of disclosure of sensitive data and information leakage [16]. However, using a blockchain, data is stored in linked blocks that validate each other, making it more difficult for data to be stolen or edited without the consent of all nodes in the network. Thus, blockchain technology can help improve security and privacy in distributed systems.

The Figure 1 shows every layer in the blockchain system has security review to pass down the data from one to another. The data has to be passed this security review to be able to move onto the next layer of the system. With that kind of security system, blockchain has proven that not only the secured data on the input nor the output, but it has done so many times before it can pass onto the next layer. Blockchain technology uses several cryptographic techniques to ensure data privacy and security like cryptography, hashing, digital signatures, zero-knowledge proofs, and secure multi-party computation. Cryptography is used in blockchain technology to secure transactions and data. Blockchain technology uses cryptographic algorithms such as SHA-256 and Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure the authenticity and integrity of data. Hashing is a technique used in blockchain technology to create a unique digital fingerprint of data. Blockchain technology uses hashing algorithms such as SHA-256 to create a unique hash for each block in the chain. Hashing is used to ensure that data is not duplicated or altered. The use of hashing in blockchain technology ensures that data is secure and cannot be tampered with. Digital signatures are a technique used in blockchain technology to ensure the authenticity of transactions. Blockchain technology uses digital signature algorithms such as ECDSA to ensure that transactions are signed by the correct parties [15], [17], [18].

Digital signatures are used to ensure that transactions are not tampered with and that they are executed as intended. Zero-knowledge proofs are a cryptographic technique used in blockchain technology to prove the authenticity of data without revealing the data itself. Zero-knowledge proofs are used to enhance privacy and security in blockchain transactions. Zero-knowledge proofs ensure that data is secure and cannot be accessed by unauthorized parties. Secure multi-party computation is a cryptographic technique used in blockchain technology to enable multiple parties to compute a function on their inputs without revealing their inputs to each other [19].

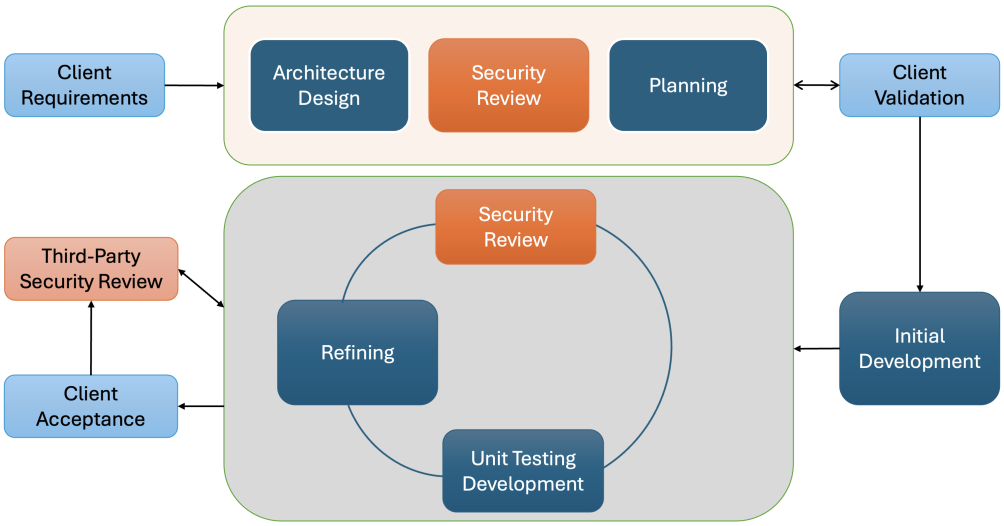

Figure 1. Blockchain structure

Secure multi-party computation is used to enhance privacy and security in blockchain transactions. Secure multi-party computation ensures that data is secure and cannot be accessed by unauthorized parties. In summary, blockchain technology uses several cryptographic techniques such as cryptography, hashing, digital signatures, zero-knowledge proofs, and secure multi-party computation to ensure data privacy and security. These techniques ensure the authenticity, integrity, and confidentiality of data in blockchain transactions. The use of these cryptographic techniques ensures that data is secure and cannot be tampered with or accessed by unauthorized parties.

3.2. Discussion

In 2018, Walmart already collaborated with IBM to develop a supply chain management system that used blockchain technology to track the origin of its food products and improve food safety [20]. This system, which relied on IBM's Hyperledger Fabric blockchain, aimed to create a transparent and secure record of each product's journey from the farm to the store. The blockchain-based system helped Walmart to enhance food traceability, reduce the time it takes to identify the source of contaminated food, and improve food safety by quickly detecting potential issues. Additionally, the system provided greater transparency and accountability in the supply chain by allowing all parties involved to access the same information about each product's journey. Moreover, the smart contract capabilities of the system enabled Walmart to automate certain aspects of the supply chain, such as payment processing and compliance with food safety regulations, resulting in a reduced risk of fraud and errors. By using blockchain technology, Walmart could improve security and privacy in its supply chain management system, as the decentralized and immutable nature of the blockchain ensured a secure record of all transactions while keeping sensitive information private and only accessible by authorized parties. This case study highlights the potential of blockchain technology to optimize security and privacy in supply chain management and other industries by offering a transparent and secure record of all transactions, allowing automation of specific processes, and improving traceability and accountability [21].

Case study that blockchain already used to public services to secure data of a nation. In Estonia, is known for its innovative use of technology, and one of its most notable implementations is its blockchain-based

national identity system, called e-Residency. The system, which was launched in 2014, enables individuals to apply for a digital ID card, which can be used to access a range of government and private sector services online [22]. The e-Residency system is built on the blockchain and uses cryptographic protocols to secure users' identities and personal data. The system also provides a secure and transparent record of all transactions, which enables individuals to track who has accessed their data and for what purpose. The system's decentralized architecture means that users have control over their data and can choose who has access to it, which enhances privacy and security. The e-Residency system has been a success in Estonia, with over 70,000 people from 150 countries having applied for an e-Residency card. The system has also inspired other countries to explore the use of blockchain technology in their national identity systems. This case study demonstrates the potential of blockchain technology to optimize security and privacy in national identity systems, by providing a secure and transparent record of all transactions, enabling individuals to control their data, and enhancing privacy and security.

The high potential on those idea that didn't use blockchain technology before if it used the blockchain technology, for example the voting system. A blockchain-based voting system would enable individuals to cast their votes electronically in a secure and transparent manner. The system would use a distributed ledger technology to record and verify every vote, ensuring that the results are accurate and tamper-proof. To use this system, voters would need to have a digital wallet that is connected to the blockchain. When a voter casts their vote, the transaction would be recorded on the blockchain as a new block, which would include the voter's identity and their choice. Each block would be linked to the previous block, creating an immutable and transparent chain of data. Once the voting period is over, the results would be calculated by counting the number of votes for each candidate or option. As the blockchain is decentralized, this process can be done in real-time by anyone with access to the blockchain. The use of blockchain technology in voting systems has several advantages. First, it eliminates the need for a central authority to oversee the voting process, reducing the risk of fraud or manipulation. Second, it ensures the privacy of the voters, as their identities are kept anonymous on the blockchain. Finally, it provides greater transparency and accountability, as the results are publicly available and cannot be altered [23], [24].

However, there are also challenges in implementing a blockchain-based voting system, such as ensuring the security of the digital wallets, preventing double voting, and ensuring that everyone has access to the technology. Despite these challenges, blockchain-based voting systems have the potential to revolutionize the way we vote by providing a secure and transparent alternative to traditional voting methods. Blockchain technology holds immense promise for enhancing security and privacy in distributed systems. Nonetheless, it is crucial to address existing technological hurdles and limitations associated with blockchain. To bolster the security and privacy of blockchain systems, the following measures can be undertaken. Firstly, a comprehensive survey encompassing both technical and applications perspectives can be conducted. This survey would delve into the intricate structure of blockchain technology, including various consensus algorithms, while exploring the challenges and opportunities it presents in terms of data security and privacy [16], [23].

Conducting a comprehensive comparison of blockchain applications in the realm of cyber-security can shed light on the benefits that blockchain has brought to this domain. This comparison would evaluate recent studies and highlight various blockchain applications in cyber-security is related fields. By conducting such an analysis, it becomes possible to address the security challenges prevalent in cyber-security and propose effective solutions to mitigate them [13]. This can help identify potential security challenges of blockchain and propose solutions to address them. To ensure the preservation of data privacy, it is crucial to consider the actual deployment of the system. By employing various cryptographic techniques, such as encryption, data can be stored in the ledger in an encrypted form. This approach significantly enhances data privacy, safeguarding sensitive information from unauthorized access or exposure [1].

In addition, users have the ability to safeguard their real identities through a concept known as pseudo-anonymity. This means that while participating in transactions or interactions within system, users can maintain a level of anonymity, protecting their true identities. To further strengthen the system's resilience and reliability, the introduction of smart contracts is recommended. These contracts are self-executing and contain predefined terms and conditions written directly into the code, ensuring automated and trustworthy agreements between parties involved [1]. Decentralization and distributed data management are fundamental aspects of blockchain technology. By adopting a decentralized approach, blockchain redefines trust by eliminating the need for intermediaries or third parties. This ensures enhanced security, privacy, and data integrity within the system. Through its distributed nature, blockchain provides a robust framework where data is shared across multiple

nodes, ensuring transparency and reliability without relying on a central authority or single point of control. This decentralized and distributed data management solution revolutionizes traditional trust models, offering a new paradigm for secure and private transactions [13], there is no central authority controlling the system, which can reduce the risk of a single point of failure or attack. Combining blockchain and AI, Blockchain, and AI technologies can be combined to enhance security and privacy in smart environments [2], [24], [25].

The AI-based techniques can be used to detect anomalies within blockchain networks with high accuracy, which can help address security issues in smart environments. To enhance the security capabilities of blockchain-based systems, a decentralized selective ring-based access control mechanism can be implemented. This mechanism allows for fine-grained control over data access by utilizing a ring-based structure. In addition, device authentication and patient records anonymity algorithms can be integrated to further strengthen security of system. By employing these measures, blockchain-based systems can ensure that only authorized entities have access to sensitive data, enhancing the overall security and protecting the privacy of individuals' information [3]. Overall, these measures can help improve the security and privacy of blockchain systems. By conducting comprehensive surveys, comparing blockchain applications in cyber-security, preserving data privacy, using decentralization and distributed data management, combining blockchain and AI technologies, and introducing selective ring-based access control mechanisms, blockchain technology can be made more secure and private.

Blockchain technology has the potential to optimize security and privacy in distributed systems, there are also potential drawbacks to its use. One of the drawbacks is scalability, which refers to its ability to handle a large number of transactions. As the number of transactions increases, the blockchain may become slower and less efficient. Another drawback is energy consumption, as blockchain technology requires a significant amount of energy to operate, which can be a concern for sustainability and environmental impact [13]. Privacy concerns are also a potential drawback of using blockchain technology. While blockchain technology can provide greater transparency and immutability of data, it can also have privacy concerns due to the public nature of the ledger. Sensitive data may be exposed under statistical attacks, and users may need to protect their real identities in the sense of pseudo-anonymity [3], [26], [27].

To tackle this issue, data stored in the ledger can be encrypted using various cryptographic techniques, ensuring its confidentiality and protecting sensitive information. Moreover, users can adopt pseudo-anonymity measures to safeguard their real identities and maintain privacy. Additionally, the introduction of smart contracts can enhance system robustness. These self-executing contracts contain predefined terms and conditions written in code, enabling automated and secure transactions between parties. By implementing these measures, blockchain systems can achieve greater security, privacy, and efficiency in data management and transaction processing [3]. Security challenges are another potential drawback of using blockchain technology.

Blockchain technology can face inherent security challenges such as DoS, eclipse, and double spending attacks, as well as APT and malware [1], [14]. These challenges can be addressed through advanced anomaly detection and mitigation approaches, but they still pose a potential risk. Finally, the lack of regulation is another potential drawback of using blockchain technology. Blockchain technology is still a relatively new and unregulated technology, which can lead to uncertainty and potential risks for users and businesses [13]. Blockchain technology has the potential to optimize security and privacy in distributed systems, there are also potential drawbacks to its use. These include scalability, energy consumption, privacy concerns, security challenges, and lack of regulation. Further research and development can help address these potential drawbacks and optimize the use of blockchain technology in distributed systems.

4. CONCLUSION

Blockchain technology is a distributed ledger technology that enhances security and privacy in distributed systems. It achieves this through several key features, including: i) data immutability is ensured by decentralizing data storage making it extremely difficult to tamper with or delete information. The interlinking of blocks through cryptographic hashes ensures that any changes to one block would render all subsequent blocks invalid. ii) Blockchain provides data provenance allowing the tracking of data origin and ownership. This feature enhances data security and privacy, such as in tracking the authenticity of food products to prevent counterfeiting or contamination. iii) Blockchain convinces parties by offering transparent and immutable data. All participants are able to independently verify the authenticity of data without relying on a third party, which enhances security in transactions. These features make blockchain applicable in various sectors, such as supply

chains, where it can track the movement of goods, ensuring their authenticity and safety. However, the potential advantages of blockchain, including reduced costs, increased efficiency, and improved transparency, make it an appealing technology for the future. However, there are still certain technological difficulties and restrictions with blockchain that need to be addressed. A comprehensive survey on technical and applications perspective can be conducted to identify potential security and privacy issues and propose solutions to address them. Blockchain technology can help address potential drawbacks of using distributed systems, such as centralized control, lack of transparency and immutability of data, data leaks, and lack of trust. Further research and development can help address potential drawbacks of using blockchain technology, such as scalability, energy consumption, privacy concerns, security challenges, and lack of regulation. By preserving data privacy, using decentralization and distributed data management, introducing smart contracts and selective ring-based access control mechanisms, combining blockchain and AI technologies, blockchain technology can be made more secure and private.

ACKNOWLEDGMENTS

The author's wishes to acknowledge the Informatics Department, Faculty of Science and Technology, UIN Sunan Gunung Djati Bandung which partially supports this research work.

FUNDING INFORMATION

The author confirmed that no funding was involved during the research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Wisnu Uriawan	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Adryan Putra Pratama		✓	✓			✓	✓	✓		✓	✓			
Shafwan Mursyid			✓	✓		✓	✓			✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

The authors whose names are listed immediately below certify that they have no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

This research, unrelated to animal use. However, has complied with all the relevant national regulations and institutional policies for the care and use of animals.

DATA AVAILABILITY

This research is not using a specific data or dataset. However, we provided all the references that are needed for this research work in the references section.

REFERENCES

[1] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey," *Computers & Security*, vol. 97, Oct. 2020, doi: 10.1016/j.cose.2020.101966.

[2] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[3] R. Kumar, "A survey on the security and privacy of blockchain systems," *International Journal of Scientific Research in Engineering and Management*, vol. 6, no. 1, 2022, doi: 10.55041/ijsrem11514.

[4] A. Argani and W. Taraka, "Utilization of blockchain technology to optimize certificate security in higher education (in bahasa: *pemanfaatan teknologi blockchain untuk mengoptimalkan keamanan sertifikat pada perguruan tinggi*)," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 1, no. 1, pp. 10–21, 2020, doi: 10.34306/abdi.v1i1.121.

[5] M. Pilkington, "Blockchain technology: principles and applications," *Research Handbook on Digital Transformations*, Edward Elgar Publishing, 2016, pp. 225–253, doi:10.4337/9781784717766.00019.

[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[7] F. Sun, "A survey of consensus algorithms in crypto," *Medium*. 2018. [Online]. Available: https://medium.com/@sunflora98/a-survey-of-consensus-algorithms-in-crypto-e2e954dc9218

[8] M. Kim and T. Suh, "Eavesdropping vulnerability and countermeasure in infrared communication for IoT devices," *Sensors*, vol. 21, no. 24, 2021, doi: 10.3390/s21248207.

[9] S. Salim, N. Moustafa, and B. Turnbull, "Privacy preservation of Internet of Things-integrated social networks: a survey and future challenges," *International Journal of Web Information Systems*, 2025, doi: 10.1108/IJWIS-04-2024-0120.

[10] M. H. Abidi, H. Alkhalefah, U. Umer, and M. K. Mohammed, "Blockchain-based secure information sharing for supply chain management: optimization assisted data sanitization process," *International Journal of Intelligent Systems*, vol. 36, pp. 260-290, 2021, doi: 10.1002/int.22299.

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[12] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Mathematical Foundations of Computing*, vol. 1, no. 2, pp. 121–147, 2018, doi: 10.1109/ICSSE.2019.8823094.

[13] E. M. Abou-Nassar, A. M. Iliyasu, P. Elkafrawy, O.- Y. Song, A. K. Bashir, A. A. A. El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223-1112338, 2020, doi: 10.1109/ACCESS.2020.2999468.

[14] Y. Lee, B. Son, S. Park, J. Lee, and H. Jang, "A survey on security and privacy in blockchain-based central bank digital currencies," *Journal of Internet Services and Information Security*, vol. 11, no. 3, pp. 16–29, 2021, doi: 10.22667/JISIS.2021.08.31.016.

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

[16] N. Fahmi, D. E. Hastasakti, D. Zaspiagi, and R. K. Saputra, "A comparison of blockchain application and security issues from bitcoin to cybersecurity," *Blockchain Frontier Technology*, vol. 3, no. 1, pp. 81–88, 2022, doi: 10.34306/bfront.v3i1.231.

[17] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, 2023, doi: 10.3390/electronics12030546.

[18] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[19] I. Abrar, and J. A. Sheikh, "Current trends of blockchain technology: architecture, applications, challenges, and opportunities," *Discover Internet of Things*, Springer, vol. 4, pp. 7, 2024, doi: 10.1007/s43926-024-00058-5.

[20] B. Tan, J. Yan, S. Chen, and X. Liu, "The impact of blockchain on food supply chain: the case of walmart," *Smart Blockchain*, pp. 167–177, 2018, doi: 10.1007/978-3-030-05764-0_18.

[21] S. Ranjan, A. Negi, H. Jain, B. Pal, and H. Agrawal, "Network system design using hyperledger fabric: permissioned blockchain framework," *2019 Twelfth International Conference on Contemporary Computing (IC3)*, Noida, India, 2019, pp. 1-6, doi: 10.1109/IC3.2019.8844940.

[22] S. Rojnic, "Blockchain technology is making its way into public services: the examples from georgia and estonia," *HeinOnline*, 2022. [Online]. Available: https://heinonline.org/HOL/LandingPage?handle=hein.journals/amslawf14&div=26&id=&page=

[23] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-based e-voting system," *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[24] K. Salah, M. H. ur Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: review and open research challenges," *IEEE Access* vol. 7, pp. 10127-10149, 2019, doi:10.1109/ACCESS.2018.2890507.

[25] T. N. Dinh and M. T. Thai, "AI and blockchain: a disruptive integration," *Computer*, IEEE, vol. 51, no. 9, pp. 48-53, 2018, doi: 10.1109/MC.2018.3620971.

[26] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, no. 20, 2021, doi: 10.3390/app11209372.

[27] E. Tam, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: a conceptual framework for public management," *Government Information Quarterly, Elsevier*, vol. 39, no. 1, 2022, doi: 10.1016/j.giq.2021.101625.

BIOGRAPHIES OF AUTHORS

Wisnu Uriawan is of Indonesian origin and has a Ph.D. in Informatics and Mathematics from INSA Lyon, France. He works as a Lecturer in the Department of Informatics at the Faculty of Science and Technology of UIN Sunan Gunung Djati, Bandung, Indonesia. Currently, he is focusing on blockchain technology. His research area is in blockchain technology, artificial intelligence, expert systems, decision support systems, software engineering, and information systems. He can be contacted at email: wisnu_u@uinsgd.ac.id.

Adryan Putra Pratama is a 2025 graduate of Universitas Islam Negeri Sunan Gunung Djati Bandung in Indonesia, majoring in Informatics. His research focuses on the development and efficiency of future technologies, including blockchain, artificial intelligence, and other emerging innovations. He can be contacted at email: adry.pprtm@gmail.com.

Shafwan Mursyid is pursuing his Bachelor's in Department of Informatics at the Faculty of Science and Technology, Universitas Islam Negeri Sunan Gunung Djati Bandung, Indonesia. His main research focuses on blockchain optimization for privacy and security in distributed systems. His research interests include distributed systems, blockchain technology, and artificial intelligence. He can be contacted at email: shafwanmursyid88@gmail.com.