International Transactions on Education Technology (ITEE)
Vol. 2 No. 1 November 2023

p-ISSN: 2963-6078
e-ISSN: 2963-1947

Implementation of Blockchain Technology as the Latest Solution to Improve Data Security and Integrity

M. Adhit Dwi Yuda[1], Sri Watini[2]

[1] Informatics Engineering, University of Raharja, Indonesia
[2] Early Childhood Education Teacher Education, Universitas Panca Sakti Bekasi, Indonesia

E-mail address: adhit@raharja.info, srie.watini@gmail.com

Author Notification
October, 01 2023
Final Revised
October, 15 2023
Published
November, 01 2023

To cite this document:
Yuda, M.A.D., Watini, S. (2023). Implementation of Blockchain Technology as the Latest Solution to Improve Data Security and Integrity. International Transactions on Education Technology (ITEE), 2(1) 71-82

Abstract

Blockchain technology represents an innovative solution for enhancing data security across various sectors. This research aims to examine the potential and challenges of blockchain technology in data security. The methodology employed involves a comprehensive literature review of up-to-date and relevant sources discussing the concepts, characteristics, types, and applications of blockchain technology, as well as the data security aspects associated with it. The findings of this study reveal that blockchain technology offers several advantages in data security, such as transparency, decentralization, immutability, and cryptography. However, it also confronts several obstacles, including scalability, interoperability, privacy, and regulatory concerns. This research offers recommendations and implications for addressing these challenges, such as the development of appropriate protocols and standards, fostering collaboration among stakeholders, and raising public awareness about the benefits and risks of blockchain technology. It is anticipated that this research will contribute to the development and future implementation of blockchain technology in data security.

Keywords: Blockchain technology, data security, enterprises literature review, potential and challenges, strategies and implications

1. Introduction

Data is a critical asset for individuals, organizations, and nations in the current digital era. Data serves various purposes, such as education, healthcare, finance, governance, and more [1]. However, data is also susceptible to security threats, such as theft, manipulation, or destruction by unauthorized parties. According to a report by IBM Security, the average cost of global data breaches in 2020 reached $3.86 million per incident. Therefore, there is a need for solutions to protect data from these threats [2].

One promising solution for data security is blockchain technology. Blockchain technology allows for the distributed recording and storage of data in a peer-to-peer network without the need for a central authority [3],[4]. This technology possesses unique characteristics, such as transparency, decentralization, immutability, and cryptography, which can enhance data security against both external and internal attacks [5]. Blockchain technology has been applied across various sectors, including finance, healthcare, education, and governance, to address existing data security issues[6].

However, blockchain technology also faces several challenges in data security, such as scalability, interoperability, privacy, and regulation. Scalability relates to the technology's ability to handle a large volume of transactions quickly [7]. Interoperability pertains to the technology's capability to communicate and collaborate with other systems. Privacy concerns the protection of users' identities and personal information within blockchain technology. Regulation concerns the legal framework and policies governing the use of blockchain technology [8][9].

This research aims to assess the potential and challenges of blockchain technology in data security. The methodology employed involves a literature review of up-to-date and relevant sources discussing the concepts, characteristics, types, and applications of blockchain technology, as well as the data security aspects related to this technology. This research utilizes a qualitative approach with content analysis techniques to identify, classify, and synthesize information from selected literature sources [10]. The research does not employ specific variables or hypotheses but instead focuses on gaining an in-depth understanding of the research topic [11].

The research findings indicate that blockchain technology offers several advantages in data security, including transparency, decentralization, immutability, and cryptography . However, it also faces challenges such as scalability, interoperability, privacy, and regulation. The research provides recommendations and implications for addressing these challenges, such as the development of appropriate protocols and standards, enhancing collaboration among stakeholders, and raising public awareness of the benefits and risks of blockchain technology. This research is expected to contribute to the development and future implementation of blockchain technology in data security.

This scientific journal consists of five main sections: introduction, literature review, discussion, conclusion, and recommendations. The introduction explains the background, problem, objectives, methodology, results, and structure of the scientific journal [12]. The literature review presents a theoretical and empirical overview of blockchain technology and data security. The discussion delves into the potential and challenges of blockchain technology in data security based on the literature review findings. The conclusion summarizes the main findings, implications, and research contributions [13]. The recommendations offer suggestions for further research and practices related to blockchain technology and data security [14].

2. Research Method

This research employs a literature review method with a qualitative approach to examine the potential and challenges of blockchain technology in data security [15]. The literature review method is suitable for exploring and integrating information from various sources related to the research topic. The qualitative approach is appropriate for comprehending and interpreting the meaning of this information [16].

The data utilized in this study consists of literature sources related to blockchain technology and data security [17]. The data collected for this research are sourced from various mediums, such as academic journals, books, reports, articles, blogs, and websites. The data analyzed in this study encompass the concepts, characteristics, types, and applications of blockchain technology, as well as the data security aspects associated with this technology. The data selected for this research adhere to the criteria of relevance, currency, validity, and reliability [18].

The collected data are subsequently analyzed using content analysis techniques. Content analysis is a technique used to identify, classify, and synthesize information from literature sources [19]. The data analysis steps undertaken in this research are as follows:

1. **Coding**: Assigning codes or labels to each piece of information found in the literature sources based on the research topic or subtopics.
2. **Categorization**: Grouping pieces of information with the same codes or labels into specific categories based on similarities or differences in meaning.
3. **Theming**: Identifying main themes or sub themes within each category of information based on the relationships or patterns among these pieces of information.
4. **Visualization**: Creating visual representations of the identified themes or sub themes in the form of tables, graphs, diagrams, or concept maps to facilitate the presentation and comprehension of the data analysis results.
5. **Interpretation**: Providing interpretations or explanations of the meaning and implications of the identified themes or sub themes based on relevant theories or prior research relevant to the research topic.

2.1 Literature Review

Blockchain technology is one of the technologies that offers a solution to enhance data security across various sectors [20]. This literature review will delve into the concepts, characteristics, types, and applications of blockchain technology, along with previous studies related to blockchain technology and data security [21].

In theoretical terms, blockchain technology can be defined as a system that enables the distributed recording and storage of data within a peer-to-peer network, eliminating the need for a central authority. It was initially introduced by Satoshi Nakamoto in 2008 as the foundation for the digital currency Bitcoin. This technology possesses several unique characteristics:

1. **Transparency**: All transactions within the blockchain network are visible to all participants, promoting accountability and trust among users.
2. **Decentralization**: There is no single entity that controls or regulates the blockchain network, reducing the risk of manipulation or corruption by unauthorized parties.
3. **Immutability**: Once data is recorded on the blockchain network, it cannot be altered or deleted by anyone, ensuring data integrity and authenticity.
4. **Cryptography**: Data recorded on the blockchain network is protected using cryptographic techniques such as encryption, decryption, hashing, and digital signatures, guaranteeing data confidentiality and authentication.

Based on its operational mode, blockchain technology can be categorized into three main types:

1. **Public Blockchain**: An open blockchain network accessible to anyone interested in joining and participating. Examples include Bitcoin, Ethereum, and Litecoin.
2. **Private Blockchain**: A closed blockchain network accessible only to select members who have received permission. Examples include Hyperledger Fabric, Corda, and Quorum.
3. **Consortium Blockchain**: A semi-closed blockchain network accessible only to a group of organizations that have agreed to collaborate. Examples include Ripple, Stellar, and EWF.

In terms of its applications, blockchain technology can serve various purposes, such as:

1. **Finance**: Facilitating fast, cost-effective, and secure financial transactions without the need for intermediaries like banks or other financial institutions. Examples include digital currencies, cross-border money transfers, and online payments.
2. **Healthcare**: Storing and sharing sensitive healthcare data such as medical records, test results, prescriptions, and more in a protected and verifiable manner. Examples include MedRec, Healthureum, and Medicalchain.
3. **Education**: Managing and verifying educational data, such as diplomas, certificates, transcripts, and more, easily and reliably. Examples include Blockcerts, ODEM, and BitDegree.
4. **Governance**: Enhancing the efficiency and transparency of public services such as elections, licensing, taxes, and more in a fair and accountable manner. Examples include Agora, Voatz, and GovCoin.

Empirically, numerous studies have been conducted to assess the potential and challenges of blockchain technology in data security. Here is a summary of some of these studies:

Researcher	Title	Destination	Methods	Results
Zheng et al.	Blockchain challenges and opportunities: A survey	Identify the challenges and opportunities of blockchain technology in technical, social, economic, and political aspects	Literature study from 41 sources related to blockchain technology	Found that the main challenges of blockchain technology are scalability, interoperability, privacy, and regulation; while the main opportunities are the development of innovative applications in various sectors
Yli-Huumo et al.	Where is current research on blockchain technology? A systematic review	Examine current trends and research focuses on blockchain technology	Literature study from 41 sources related to blockchain technology	Finds that most research on blockchain technology focuses on the technical and financial aspects; while the social and

				organizational aspects have received less attention.
Al Ansari et al.	Blockchain for government services – use cases, security benefits, and challenges	Examining the use of blockchain technology for public services in the government sector	Case studies from four countries that have implemented blockchain technology for public services, namely Estonia, Dubai, the UK, and Singapore.	It found that blockchain technology can improve the security of government data from cyberattacks; however, it also faces challenges such as infrastructure readiness, regulatory compliance, and public participation.

3. Findings

Based on the results of the data analysis that has been carried out using content analysis techniques [22], four main themes can be found relating to the potential and challenges of blockchain technology in data security, namely:

- **Transparency**: this theme relates to the ability of blockchain technology to provide clear and open information about all transactions taking place on the blockchain network.
- **Decentralization**: this theme relates to the ability of blockchain technology to eliminate the role of a central authority in controlling or regulating a blockchain network.
- **Immutability**: this theme relates to the ability of blockchain technology to maintain the integrity and authenticity of data that has been recorded on the blockchain network.
- **Cryptography**: this theme deals with the ability of blockchain technology to protect the confidentiality and authentication of data recorded on the blockchain network.

From each of these main themes, several more specific sub themes can be derived, namely:

Theme	Subtheme	Description
Transparency	Accountability	The ability of blockchain technology to increase accountability and trust between users.
Transparency	Participation	The ability of blockchain technology to increase engagement and collaboration between users.
Decentralization	Efficiency	The ability of blockchain technology to reduce transaction costs and time.
Decentralization	Autonomy	The ability of blockchain technology to give users freedom and independence.
Immutability	Integrity	The ability of blockchain technology to maintain data consistency and conformity.
Immutability	Authenticity	The ability of blockchain technology to maintain data correctness and accuracy.
Cryptography	Confidentiality	The ability of blockchain technology to maintain privacy and data protection.
Cryptography	Authentication	The ability of blockchain technology to maintain identity and verify data.

3.1 Problem

Based on the results of the data analysis that has been conducted using content analysis techniques, four main themes related to the potential and challenges of blockchain technology in data security can be found. However, there are still some aspects that need to be understood more deeply to explore the full impact and potential of blockchain technology in the context of data security [23]. Therefore, the following are some of the issues that can be used as the basis for further research:

1. How can blockchain technology effectively increase accountability and trust between data users, and how will it impact sectors such as finance, healthcare, and logistics?
2. To what extent can blockchain technology reduce the cost and time of data transactions, and what are the economic implications of using this technology in terms of efficiency and productivity?
3. How can scalability challenges in blockchain technology be overcome to ensure its ability to handle large and fast transaction amounts across multiple industries?

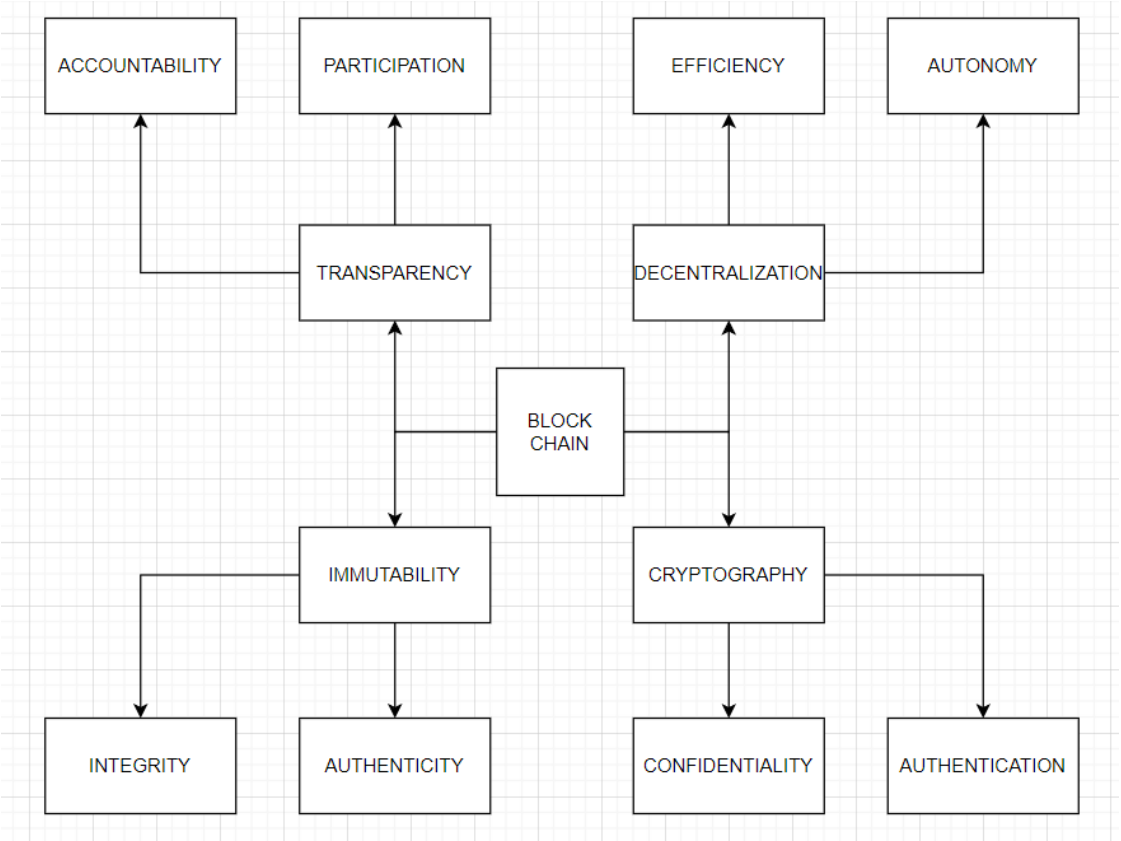
4. How can blockchain technology interact with other systems more efficiently and securely, especially in terms of interoperability with conventional technologies?
5. How can data user privacy be properly safeguarded in the context of blockchain technology, and how can appropriate regulations be implemented to protect individual privacy rights?
6. How can consistent regulations be established at the global level to address the issue of incompatibilities or inconsistencies between countries' regulations on the use of blockchain technology?
7. What are the implications of blockchain technology for cybersecurity and countering possible cyber threats in the blockchain ecosystem?
8. How can blockchain technology affect data ownership and control structures in different sectors, and what impact will it have on sustainability and decision-making?
9. How can the adoption of blockchain technology be scaled up across various sectors, including education, energy, and government, to maximize its potential to improve data security?
10. Are there ethical risks associated with using blockchain technology in data security, and how can we mitigate those risks?

3.2 Research Implementation

The following is a visualization of the themes and subthemes found from the data

p-ISSN: 2963-6078
e-ISSN: 2963-1947

analysis:



Picture 1. Concept map

From the concept map above, it can be seen that each theme and subtheme has a relationship that affects each other. This shows that the potential and challenges of blockchain technology in data security cannot be separated from the unique characteristics of the technology.

The potential of blockchain technology in data security is as follows:

- Blockchain technology can increase accountability and trust between data users, because all transactions that occur on the blockchain network can be seen and verified by all network members. This is in accordance with the opinion of Zheng et al. which states that the transparency of blockchain technology can increase accountability and trust between users. .
- Blockchain technology can increase engagement and collaboration between data users, because all members of the blockchain network can participate and contribute to the process of recording and storing data. This is in accordance with the opinion of Yli-Huumo et al. which states that decentralization of blockchain technology can increase participation and collaboration between users.
- Blockchain technology can reduce the cost and time of data transactions, because it does not require an intermediary or central authority in the data transaction process. This is in accordance with the opinion of Alansari et al. which states that decentralization of blockchain technology can reduce the cost and time of data transactions.
- Blockchain technology can provide freedom and independence to data users, because they can control and manage their own data without interference from other parties. This is in accordance with the opinion of Zheng et al. which states that the decentralization of blockchain technology can provide autonomy to users.

- Blockchain technology can maintain data consistency and conformity, because data that has been recorded on the blockchain network cannot be changed or deleted by anyone. This is in accordance with the opinion of Yli-Huumo et al. which states that the immutability of blockchain technology can maintain data integrity.
- Blockchain technology can maintain the truth and accuracy of data, because the data recorded on the blockchain network is equipped with mathematical evidence that guarantees the authenticity of the data. This is in accordance with the opinion of Alansari et al. which states that the immutability of blockchain technology can maintain data authenticity.
- Blockchain technology can maintain data privacy and protection, because the data recorded on the blockchain network is protected by cryptographic techniques, such as encryption, decryption, hashes, and digital signatures. This is in accordance with the opinion of Zheng et al. which states that blockchain technology cryptography can maintain data confidentiality.
- Blockchain technology can maintain data identity and verification, because the data recorded on the blockchain network is equipped with a digital signature that shows who made the data transaction. This is in accordance with the opinion of Yli-Huumo et al. which states that blockchain technology cryptography can maintain data authentication.

The challenges of blockchain technology in data security are as follows:

- Blockchain technology faces the problem of scalability, which is the ability to handle a large number of transactions quickly. This is due to the limitations of block size, block generation frequency, and network consensus that affect the capacity and speed of transactions on the blockchain network. This is in accordance with the opinion of Zheng et al. who stated that scalability is one of the main challenges of blockchain technology.
- Blockchain technology faces the problem of interoperability, which is the ability to communicate and collaborate with other systems. This is due to the lack of standards or protocols governing interactions between different types or generations of blockchain technology, as well as between blockchain technology and conventional systems. This is in accordance with the opinion of Yli-Huumo et al. who stated that interoperability is one of the main challenges of blockchain technology.
- Blockchain technology faces privacy issues, namely the protection of the identity and personal information of users. This is due to the paradox between transparency and confidentiality offered by blockchain technology. On the other hand, the confidentiality of blockchain technology can pose privacy issues for users, as they cannot know or control who can access or use their data. This is in accordance with the opinion of Alansari et al. who stated that privacy is one of the main challenges of blockchain technology.
- Blockchain technology faces regulatory issues, namely the regularity of laws and policies governing the use of blockchain technology. This is caused by discrepancies

- or inconsistencies between regulations that apply in various countries or regions related to blockchain technology, especially in terms of taxation, consumer protection, anti-money laundering, and anti-terrorism. This is in accordance with the opinion of Zheng et al. which states that regulation is one of the main challenges of blockchain technology.

From the results and discussion above, it can be concluded that blockchain technology has great potential in data security in various sectors, but it also faces several challenges that need to be overcome. This research provides suggestions and implications for addressing these challenges in the next section.

4. Conclusion

This research has identified that blockchain technology holds significant potential for enhancing data security across various sectors but also faces several challenges that need to be addressed. The study reveals that the potential of blockchain technology in data security is associated with its unique characteristics, including transparency, decentralization, immutability, and cryptography. Conversely, the challenges faced by blockchain technology in data security are related to aspects that require improvement or development within the technology, such as scalability, interoperability, privacy, and regulation. The research concludes that blockchain technology can provide a solution for enhancing data security across various sectors if these challenges can be overcome with appropriate strategies.

The findings of this study have implications for blockchain technology developers, users, and regulators in the context of data security. Specifically, the research contributes to blockchain technology developers by encouraging the development of protocols and standards that align with the data security needs and challenges across various sectors. For blockchain technology users, the findings promote increased engagement and collaboration in data recording and storage processes and raise awareness and responsibility regarding their own data. For blockchain technology regulators, the research offers insights into creating fair and flexible regulations that can accommodate the evolution and implementation of blockchain technology in data security.

This research makes a contribution to the field of computer science and informatics, particularly in the areas of blockchain technology and data security. It provides a comprehensive and in-depth literature review on the potential and challenges of blockchain technology in data security. The research introduces innovation in the form of concept maps that visualize themes and subthemes related to the potential and challenges of blockchain technology in data security. Lastly, the study offers relevant and up-to-date recommendations and implications for the future development and implementation of blockchain technology in data security.

References

[1] M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, and Z. Irani, “A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors,” *Int J Inf Manage*, vol. 50, pp. 302–309, 2020, doi: 10.1016/j.ijinfomgt.2019.08.012.

[2] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, “A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities,” *IEEE Access*, vol. 9, pp. 12730–12749, 2021, doi: 10.1109/ACCESS.2021.3050241.

[3] H. Tabrizchi and M. Kuchaki Rafsanjani, *A survey on security challenges in cloud computing: issues, threats, and solutions*, vol. 76, no. 12. 2020. doi: 10.1007/s11227-020-03213-1.

[4] Wahyu Sejati and Vivi Melinda, "Education on the Use of Iot Technology for Energy Audit and Management Within the Context of Conservation and Efficiency," *International Transactions on Education Technology (ITEE)*, vol. 1, no. 2, pp. 138–143, 2023, doi: 10.34306/itee.v1i2.324.

[5] Amitkumar Dudhat and Ardi, "Application of Information Technology to Education in the Age of the Fourth Industrial Revolution," *International Transactions on Education Technology (ITEE)*, vol. 1, no. 2, pp. 131–137, 2023, doi: 10.34306/itee.v1i2.319.

[6] C. Malesios, D. De, A. Moursellas, P. K. Dey, and K. Evangelinos, "Sustainability performance analysis of small and medium sized enterprises: Criteria, methods and framework," *Socioecon Plann Sci*, vol. 75, 2021, doi: 10.1016/j.seps.2020.100993.

[7] M. Cooper and Q. T. K. Nguyen, "Multinational enterprises and corporate tax planning: A review of literature and suggestions for a future research agenda," *International Business Review*, vol. 29, no. 3, 2020, doi: 10.1016/j.ibusrev.2020.101692.

[8] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[9] Suryari Purnama and Cicilia Sriliasta, "Independent Learning and Blended Learning Information System Student," *International Transactions on Education Technology (ITEE)*, vol. 1, no. 2, pp. 144–150, 2023, doi: 10.34306/itee.v1i2.327.

[10] M. K. Lim, Y. Li, C. Wang, and M. L. Tseng, "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Comput Ind Eng*, vol. 154, 2021, doi: 10.1016/j.cie.2021.107133.

[11] B. Harney and H. Alkhalaf, "A quarter-century review of HRM in small and medium-sized enterprises: Capturing what we know, exploring where we need to go," *Hum Resour Manage*, vol. 60, no. 1, pp. 5–29, 2021, doi: 10.1002/hrm.22010.

[12] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "applied sciences IoT Privacy and Security : Challenges and Solutions," *Mdpi*, pp. 1–17, 2020.

[13] S. K. N. Gamage, E. M. S. Ekanayake, G. A. K. N. J. Abeyrathne, R. P. I. R. Prasanna, J. M. S. B. Jayasundara, and P. S. K. Rajapakshe, "A review of global challenges and survival strategies of small and medium enterprises (SMEs)," *Economies*, vol. 8, no. 4, 2020, doi: 10.3390/ECONOMIES8040079.

[14] Q. Li *et al.*, "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," *IEEE Trans Knowl Data Eng*, vol. 35, no. 4, pp. 3347–3366, 2023, doi: 10.1109/TKDE.2021.3124599.

[15] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *Int J Healthc Manag*, vol. 15, no. 1, pp. 70–83, 2022, doi: 10.1080/20479700.2020.1843887.

[16] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–20, 2020, doi: 10.3390/s20133625.

[17] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach," *IEEE Internet Things J*, vol. 7, no. 8, pp. 7751–7763, 2020, doi: 10.1109/JIOT.2020.2991401.

[18] N. Deepa *et al.*, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Generation Computer Systems*, vol. 131, pp. 209–226, 2022, doi: 10.1016/j.future.2022.01.017.

[19] C. Troncoso *et al.*, "Decentralized Privacy-Preserving Proximity Tracing," no. May, pp. 1–46, 2020, [Online]. Available: http://arxiv.org/abs/2005.12273

[20] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," *IEEE Internet Things J*, vol. 8, no. 6, pp. 4004–4022, 2021, doi: 10.1109/JIOT.2020.3015432.

[21] S. Bakhtiari, R. Breunig, L. Magnani, and J. Zhang, "Financial Constraints and Small and Medium Enterprises: A Review*," *Economic Record*, vol. 96, no. 315, pp. 506–523, 2020, doi: 10.1111/1475-4932.12560.

[22] F. Bartolacci, A. Caputo, and M. Soverchia, "Sustainability and financial performance of small and medium sized enterprises: A bibliometric and systematic literature review," *Bus Strategy Environ*, vol. 29, no. 3, pp. 1297–1309, 2020, doi: 10.1002/bse.2434.

[23] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "Iot-based big data secure management in the fog over a 6G wireless network," *IEEE Internet Things J*, vol. 8, no. 7, pp. 5164–5171, 2021, doi: 10.1109/JIOT.2020.3033131.