International Journal of Research in Engineering and Management Sciences (IJREMS)
E-ISSN: 3107-7439

Research Article
VOL.: 1, Issue: 1, June 2025

Data Privacy in the Age of Blockchain: Balancing Transparency and Confidentiality in Financial Transactions

***[1]P. Nethrasri**

*[*1]Department of Computer Science and Engineering,*
Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana, India
Email: nethra.srip27@gmail.com
Orcid ID: https://orcid.org/0009-0006-6171-1238

ABSTRACT:

Organizations must adopt improved cyber security methods that defend against cyber threats because Advanced Persistent Threats have exhibited rising sophistication in their operations. APT infiltrates organizations through extended targeted system intrusions to access secrets or break infrastructure while defying conventional sign-based security measures. The paper examines the operation of Artificial Intelligence technologies for APT detection and defense. The research develops an APT detection system in real time using machine learning and deep learning simultaneously for detecting anomalous activity and predictive modeling. The detection accuracy of AI systems increases substantially due to neural networks that show better results than normal traditional models. Standard cyber security infrastructure and false alarm management present main barriers to the deployment of this artificial intelligence system. The study focuses on Advanced Persistent Threats together with Artificial Intelligence and its linked techniques such as Anomaly Detection, Intrusion Detection Systems, and Real-time Response and Machine Learning and its subset Deep Learning.

Keywords: Regulatory Compliance, Cryptographic Techniques, Immutable Records, Data Encryption, Tokenization, Blockchain Auditing, Privacy-Preserving Blockchain, Distributed Ledger Technology (DLT), Financial Privacy

Received Date: 5 June 2025**; Accepted Date:** 15 June 2025**; Published Date:** 20 June 2025.

I. Introduction

Blockchain technology has already demonstrated itself as a ground-breaking technology in the financial sector, and it holds the possibility of a decentralized open ledger, transparent, and unchangeable platform on which financial transactions can be carried out (Vangala et al., 2020). It has brought a revolution in the financial systems by enabling the cryptocurrencies and smart contracts and changing the way financial transactions are being conducted (Alam, 2024). It is what blockchain promise is that it can introduce transparency, reduction of fraud and enhancement of security to the financial operations and make the environment more credible to the parties (Eljazzar et al., 2018). Decentralization is a major characteristic,
whereby the authorized user can transact using the internet without involving third parties (Kaur et al.,

2022). All the registered users can trace and observe the transaction and copy all the transactions, and it is transparent (Kaur et al., 2022). The copies of the transaction details are saved in decentralized computers or nodes in the blockchain without any supervision central body (Kaur et al., 2022). Each node gets an opportunity to audit and confirm the transactions in the blockchain, and any changes have to be accepted by consensus, which enhances the integrity and security of the information (Vangala et al., 2020). It is a distributed ledger technology (which is facilitated by cryptographic methods) that enables Data and security consistency across the members of a network (Vangala et al., 2020). The single point of failure that is present in the traditional system would not be maintained in this new system, there can be a multi-point of authority with multiple nodes and when a node fails, all the nodes connected to it would be redirected to another node as long as there is no disconnection in the network (Aldweesh, 2025).

Background of the Study

The emergence of the blockchain technology that was spearheaded by the creation of Bitcoin in 2008 has caused a paradigmat shift in data management and transactions systems across different industries (Wright, 2008). Blockchain architecture, namely the use of a distributed registry, means that each participant approximately has the same copy of the transaction history, which enhances a previously unknown degree of transparency (Eljazzar et al., 2018). This emerging transparency leads to trust and accountability because any data alteration will be observed by every network participant (Vangala et al., 2020). This distributed ledger technology extends the traditional centralized databases as it eliminates the single point of failure and control, thus, making the system more resilient and secure (Feng et al., 2018). What is blockchain technology? It is \\\"consensus algorithms and digital signatures\\\" all about, which, in combination, offer integrity and immutability of the data stored on the chain (Wang et al., 2022). The employed cryptographic mechanisms, i.e., hashing, also provide the blockchain with the property of manipulation resistance, i.e., once a block was appended to the chain, it cannot be altered or removed (Vangala et al., 2020).

Justification

The financial sphere and blockchain technology find themselves in a peculiar paradox, and the balancing between openness and privacy has to be performed carefully (Wei et al., 2024). Even though the transparency of blockchain can eliminate fraud and establish trust, it poses a possible privacy threat of individuals and organizations (Hassan et al., 2020). The immutable nature of blockchain that ensures resilience to manipulation and guarantees data integrity conflicts with the growing popularity of data protection and privacy regulations, such as the General Data Protection Regulation (Vangala et al., 2020; Zieglmeier et al., 2023). There is a need to determine how to harness the benefits of blockchain without having to reveal delicate financial details (Masluk & Gofman, 2018). The risk of data breaches is growing at tremendous rates and becoming more sophisticated, and the trade-offs between transparency and confidentiality in the application of blockchain must be identified and appropriately resolved (Satybaldy & Nowostawski, 2020). However, the regulatory landscape is also getting increasingly complicated, thus introducing another layer of complexity where a company attempts to deploy a blockchain and adhere to privacy laws (Zieglmeier & Daiqui, 2021).

Objectives of the Study

1. To learn the implication of blockchain technology with regard to privacy of data involved in a financial transaction.
2. To ascertain the trade off between transparency and confidentiality in block chain based financial system.
3. To analyse the privacy-enhancing technologies and strategies, applied to blockchain networks.
4. To determine the regulatory risk that blockchain faces in terms of data privacy compliance.
5. To suggest the solutions to reach the balance of transparency and confidentiality in the blockchainsystems.

Literature Review

The introduction of the blockchain technology to the financial services sector opens the possibilities of the future with the never-before- seen

effectiveness of transactions and safety of the information, yet, simultaneously, introduces the series of the rather complicated challenges concerning the privacy of the user data. The very characteristics of blockchain as the technology with the distributed ledger system provide the environment of transparency unparalleled in the history of business: all transactions can be stored forever and, at least theoretically, monitored by a vast number of participants (Zieglmeier et al., 2023). Even though this transparency is essential to guarantee the integrity of transaction validation and prevent frauds, it creates a paradox as it is contrary to the necessity to keep sensitive personal and financial information safe (Satybaldy & Nowostawski, 2020). Such contradictory demands are inherent and identifiable qualities of blockchains, and they need novel solutions (Vangala et al., 2020). Some of the characteristics of the blockchain technology include decentralization, anonymity and auditability (Vangala et al., 2020). The technology is not vulnerable to a central point of control and distributes the data across a large number of nodes, which reduces the likelihood of failure at a single point and censorship (Vangala et al., 2020). The block chain has a timestamp and a cryptographic hash of the previous block, which provides an auditable history of all the transactions (Vangala et al., 2020). It also hides users and protects their personal data using cryptographic instruments and pseudonymous addresses (Silva & Santos,2022).

Material and Methodology

The method of the study of the present paper is qualitative since it provides an overview of the existing literature, case studies, and theories on the issue of blockchain technology and data privacy. The principal data sources include academic articles, reportages in the industry press, and regulatory documents. The paper also examines real-world applications, such as cryptocurrency transactions and decentralized finance (DeFi) to get an understanding of how the issue of privacy is addressed today.

Result and discussion

It is both the strength and weakness of blockchain because of its decentralized and transparent structure. With public blockchains (i.e. Bitcoin), privacy features are limited and therefore the data relating to transactions is fully disclosed to all the individuals on the network. This lack of confidentiality is absolutely devastating in financial dealings because sharing of personal or financial sensitive data can lead to fraud and theft. One of the possible solutions to this issue is privacy-enhancing technologies, namely, zero-knowledge proofs, which allow verifying the transactions without revealing the data. Also, cryptographic solutions, such as ring signatures and confidential transactions have been proposed as potential means of achieving privacy without affecting the integrity and transparency of the blockchain.

However, as the blockchain technology evolves, the regulatory requirements evolve as well. Data protection laws such as GDPR allow individuals to manage their personal data and this presents certain issues to blockchain systems which are meant to be transparent and unchangeable. How blockchain platforms can conform to these regulations without losing the defining qualities of the systems is an urgent issue that needs to be resolved.

Study Limitations

This reliance on existing publications suggests a list of restrictions, in particular, concerning the rapidly evolving ecosystem of blockchain technology and privacy-enhancing mechanisms in it (Dasaklis et al., 2021). Being not an original empirical study, limitation of this study is in a conclusion which can be made because the literature utilized might be restricted in its completeness and up-to-date nature (Tse et al., 2024). The sphere of blockchain is rapidly developing, meaning that the new approaches to privacy might be invented after the termination of the research and a part of the findings would be outdated or incomplete (Furtado et al., 2020). It is also encouraged by the absence of real-life experimentation and data registration, which reduces the chances to demonstrate the sound theoretical concepts and the effectiveness of diverse privacy solutions in diverse conditions (Maragno et al., 2021). In addition, the fact that the research depends on secondary sources opens up the prospect of biasing since the selection and interpretation of the already existing research is

restricted to the opinions and interests of the first authors (Abdul, 2024).

The elaboration of hybrid blockchain models is the next research activity that should be undertaken since it can be characterized as a golden middle between the privacy of permissioned blockchains and the transparency of public blockchains (Shanmugam et al., 2023). These hybrid models can be set to a specific use-case and can be tailored considering the

Future Scope

accessibility and data visibility (Periyasamy et al., 2024). It can be particularly useful when it is necessary to exchange sensitive information between few participants that are allowed to view it, yet must possess certain degree of transparency and traceability to external parties (Pandl et al., 2020). In the set of potential

Conclusion

Blockchain can revolutionize the financial sector since it is more open and safer. However, the element of privacy on the transactions carried out on the side of finances is a huge challenge. The new privacy-enhancing technologies such as zero-knowledge proofs and cryptography provide the path to alleviating those concerns without affecting the transparency that is the major asset of blockchain.

Having found the equilibrium between transparency and confidentiality, blockchain will be able to evolve further and accept the demands of the modern financial system and adhere to privacy regulations. The future of blockchain in financial transactions is worked out in the development of the potent privacy-preserving technologies that would not impact the soundness of the blockchain transparency paradigm.

References

1. Alam, S. T. (2024). The convergence of artificial intelligence, blockchain and fintech in energy, oil and gas trading: Increasing efficiency, transparency and automations. World Journal of Advanced Research and Reviews, 22(2), 2064. https://doi.org/10.30574/wjarr.2024.22.2.1625
2. Aldweesh, A. (2025). Blockchain-Based Secure Firmware Updates for Electric Vehicle Charging Stations in Web of Things Environments. World Electric Vehicle Journal, 16(4), 226. https://doi.org/10.3390/wevj16040226
3. Eljazzar, M. M., Amr, M., Kassem, S., & Ezzat, M. (2018). Merging supply chain and blockchain technologies. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1804.04149
4. Kaur, A., Singh, G., Kukreja, V., Sharma, S., Singh, S., & Yoon, B. (2022). Adaptation of IoT with Blockchain in Food Supply Chain Management: An Analysis-Based Review in Development, Benefits and Potential Applications. Sensors, 22(21), 8174. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/s22218174
5. Vangala, A., Das, A. K., Kumar, N., & Alazab, M. (2020). Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective. IEEE Sensors Journal, 21(16), 17591. https://doi.org/10.1109/jsen.2020.3012294
6. Chang, H., & Lund, B. (2025). Bringing AI and Blockchain Synergy into Cyber Threat Intelligence Cycle. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5191276
7. Pandl, K. D., Thiebes, S., Schmidt- Kraepelin, M., & Sunyaev, A. (2020). On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2001.11017
8. Periyasamy, A., Deepankumar, E., Kokila, D., & Nanda Kumar, N. (2024). Blockchain Technology in Modern Agriculture: Exploring Techniques and Applications for Enhancing Transparency, Efficiency, and Traceability in Current Agricultural Systems.
9. Shanmugam, L., Tillu, R., & Jangoan, S. (2023). Privacy-Preserving AI/ML Application Architectures: Techniques, Trade-offs, and Case Studies. Journal of Knowledge Learning and Science Technology, 2(2), 398. https://doi.org/10.60087/jklst.vol2.n2.p420

10. Abdul, S. S. M. (2024). Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance. Blockchains, 2(3), 265. https://doi.org/10.3390/blockchains2030013
11. Dasaklis, T. K., Casino, F., & Patsakis, C. (2021). SoK: Blockchain Solutions for Forensics. In Security informatics and law enforcement (p. 21). Springer International Publishing. https://doi.org/10.1007/978-3-030-69460-9_2
12. Furtado, F. R., Silva, J. V. e, Cappellari, M. J., Castilhos, C. H. M., Rodrigues, V. F., Costa, C. A. da, & Righi, R. da R. (2020). Towards characterising architecture and performance in blockchain: a survey. International Journal of Blockchains and Cryptocurrencies, 1(2), 121. https://doi.org/10.1504/ijbc.2020.109002
13. Maragno, G., Gastaldi, L., Tangi, L., & Benedetti, M. (2021). Blockchain applications within the public sector: evidence from an international census. 479. https://doi.org/10.1145/3463677.3463699
14. Tse, W. K., Dai, X., Lee, Y. M., & Lu, D. (2024). User Acceptance of Blockchain Technology in Financial Applications: Information Security, Technology Awareness and Privacy Aspects. Blockchains, 2(3), 299. https://doi.org/10.3390/blockchains2030014
15. Satybaldy, A., & Nowostawski, M. (2020). Review of Techniques for Privacy- Preserving Blockchain Systems. https://doi.org/10.1145/3384943.3409416
16. Silva, J. O. D. da, & Santos, D. R. dos. (2022). Study of Blockchain Application in the Logistics Industry. Theoretical Economics Letters, 12(2), 321. https://doi.org/10.4236/tel.2022.122017
17. Zieglmeier, V., Daiqui, G. L., & Pretschner, A. (2023). Decentralized Inverse Transparency with Blockchain. Deleted Journal, 2(3), 1. https://doi.org/10.1145/3592624
18. Hassan, M. U., Rehmani, M. H., & Chen, J. (2020). Differential privacy in blockchain technology: A futuristic approach. Journal of Parallel and Distributed Computing, 145, 50. https://doi.org/10.1016/j.jpdc.2020.06.003
19. Masluk, A., & Gofman, M. (2018). Protecting Personal Data with Blockchain
20. Wei, Z., Fang, J., Hong, Z., Zhou, Y., Ma, S., Zhang, J., Liang, C., Zhao, G., & Tang, H. (2024). Privacy Protection Method for Blockchain Transactions Based on the Stealth Address and the Note Mechanism. Applied Sciences, 14(4), 1642. https://doi.org/10.3390/app14041642
21. Zieglmeier, V., & Daiqui, G. L. (2021). GDPR-Compliant Use of Blockchain for Secure Usage Logs. Evaluation and Assessment in Software Engineering, 313. https://doi.org/10.1145/3463274.3463349
22. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45. https://doi.org/10.1016/j.jnca.2018.10.020
23. Wang, W.-S., Yu, Y., & Du, L. (2022). Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Scientific Reports, 12(1). https://doi.org/10.1038/s41598-022-12412-0
24. Wright, D. C. S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. SSRN ElectronicJournal. https://doi.org/10.2139/ssrn.344080