Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Data Privacy and Confidentiality Challenges in Blockchain Technology

Nandini Kale, Tanuja Amnekar
BSc. Computer Application (BSc CA)
Dr. D. Y. Patil ACS College, Pimpri.

Abstract - Blockchain generation has come up as an innovative device for enhancing the transparency, traceability, and accept as true with tiers in deliver chain control. however, in spite of the blessings, information privateness and confidentiality have grown to become out to be predominant demanding situations which might be impeding the adoption technique.

The transparency, immutability, and decentralized nature of blockchain era tend to be in war with the want to maintain confidentiality of sensitive business records which includes pricing, contracts, and provider information. This paper discusses the important thing challenges of records privateness and confidentiality that get up for the duration of the implementation of blockchain era in supply chain control structures.

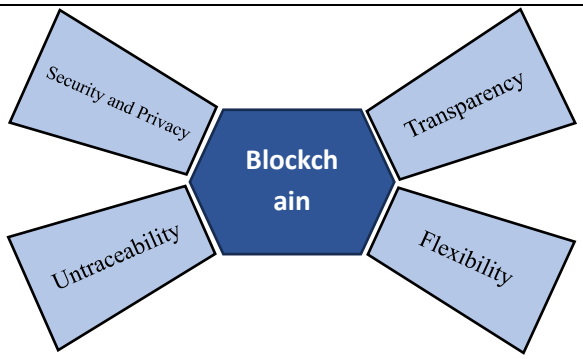
It also opinions the prevailing answers for privacy protection, inclusive of permissioned blockchains, cryptographic equipment, and get admission to control fashions.

every other trouble is the need for a stability among transparency and confidentiality. The fact is that deliver chain members may additionally want to share information selectively, but the existing blockchain era has confined competencies to support such requirements. There had been proposals to apply cryptographic methods consisting of encryption, zero-understanding proofs, and comfy multi-birthday celebration computation to enhance privacy. however, those techniques also upload complexity.

This paper discusses the essential challenges in statistics privateness and confidentiality associated with the adoption of blockchain technology in deliver chain management. It additionally discusses the modern-day nation of the artwork in privateness-keeping solutions and factors out the studies gaps. these challenges want to be addressed with a purpose to build comfortable and trustworthy blockchain-primarily based supply chain systems.

Keywords

Data Privacy, Confidentiality, Blockchain Security, Cryptography, Zero-Knowledge Proofs, Decentralization, Authentication



INTRODUCTION

Blockchain era has emerged as a progressive decentralized ledger machine that enables comfortable, transparent, and tamper-resistant recording of digital transactions without counting on a government. due to its inherent characteristics along with immutability, distributed consensus, and cryptographic safety, blockchain has been broadly followed in numerous domain names including finance, healthcare, deliver chain control, and digital identification systems. those capabilities beautify trust, accountability, and facts integrity among participating entities.

however, the equal transparency and permanence that provide protection advantages additionally introduce extreme worries related to records privacy and confidentiality. In public blockchain networks, transaction records are visible to all contributors, making touchy facts vulnerable to unauthorized analysis, traceability, and identification linkage. once information is recorded at the blockchain, it cannot be altered or removed, which conflicts with privateness regulations and the want for facts manage. As blockchain adoption expands into privateness-essential sectors, those demanding situations emerge as increasingly tremendous.

studying facts privacy and confidentiality in blockchain is necessary to apprehend the trade-offs between transparency and privateness and to perceive effective mechanisms which can shield touchy information at the same time as preserving decentralization. Addressing those demanding situations is crucial for regulatory compliance, consumer consider, and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

secure statistics sharing. furthermore, stepped forward privateness solutions can enhance blockchain scalability, enable broader actual-world packages, and sell ethical information utilization. therefore, this study makes a speciality of studying privateness and confidentiality challenges in blockchain systems and explores capability answers to reinforce comfortable and privateness-maintaining blockchain implementations.

LITERATURE REVIEW

Public Ledger Transparency and privateness alternate-offs Blockchain transparency permits consider and accountability via allowing all members to verify transactions. but studies display that this transparency can compromise user privateness. Meiklejohn et al. proven that transaction analysis can link pseudonymous blockchain addresses to actual-global identities, leading to de-anonymization [1]. Zyskind et al. in addition highlighted that publicly reachable transaction histories reveal touchy facts, creating privateness dangers in blockchain structures [2]. Cryptographic procedures to privacy several cryptographic strategies had been proposed to enhance privacy in blockchain networks. 0-know-how Proofs (ZKPs) permit transaction verification without revealing sensitive data, as proven inside the Zerocash protocol [3]. Ring signatures, utilized in privateness-targeted cryptocurrencies together with Monero, enhance anonymity by means of obscuring the sender's identity [4]. despite the fact that powerful, these techniques often introduce computational overhead and scalability demanding situations. Confidentiality in Permissioned and Permissionless Blockchains Permissionless blockchains offer open participation but restrained privacy controls. In contrast, permissioned blockchains restrict access and offer progressed confidentiality. Androulaki et al. confirmed that Hyperledger material supports non-public facts channels for secure organisation applications [5]. platforms consisting of Corda and Quorum similarly enhance confidentiality by way of sharing transaction data handiest among authorized members [6].

smart Contracts and statistics publicity dangers smart contracts automate blockchain transactions but can disclose touchy information if no longer well designed. Atzei et al. recognized vulnerabilities in clever contracts that may cause information leakage [7]. Luu et al. additionally referred to that publicly performed clever contracts can unintentionally screen non-public statistics thru transaction logs [8].

SYNTHESIS OF LITERATURE

combine and evaluation the findings from the literature review:

- common subject matters: exchange-offs between transparency, decentralization, and privateness.
- techniques used: strengths and applicability of various cryptographic tactics.
- domains of utility: finance, healthcare, supply chain, identification management.
- Convergence: where studies have the same opinion and wherein gaps continue to be.

This synthesis enables construct a coherent photo of the modern-day kingdom of studies, identifying ordinary findings and contrasting conflicting conclusions.

RESULT OF ANALYSIS

Primarily based on your literature synthesis and any additional records you include:

Key findings:

1. Public blockchain's transparency causes inherent privateness vulnerabilities.
2. Permissioned blockchains offer better confidentiality but face consider assumptions.
3. Privateness-enhancing cryptography shows promise however introduces complexity and performance overhead.
4. Smart contracts are capability assets of records leakage if no longer cautiously designed.
5. Technical evaluation: look at various blockchain types and privateness tactics' metrics (such as throughput, scalability, and degree of privacy).

DISCUSSION

Benefits

- Blockchain offers transparent, immutable data storage.
- Cryptographic primitives enable new privacy solutions.
- Unrelated failure factors are reduced by decentralisation.

Restrictions

- Publicly visible transactions put privacy at risk.
- Data security regulations (e.g., GDPR).
- ZKPs and other privacy technologies have a high computational cost. The "proper to be forgotten" may be contested by persistent information.

Unresolved problems.

- Transparency and strong privacy must be balanced.
- Developing scalable privacy solutions without compromising functionality.
- Adherence to regulations in decentralised systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

- Safe authentication and identification systems without the necessary authority.

RECOMMENDATIONS

To cope with information privacy and confidentiality challenges in blockchain structures, several technical and organizational measures can be followed. privacy-improving cryptographic strategies including 0-information Proofs, encryption mechanisms, and cozy multi-birthday celebration computation should be incorporated to limit information exposure even as preserving transaction validity. touchy statistics should be stored off-chain, with only cryptographic hashes recorded at the blockchain to ensure statistics integrity without revealing private facts and important Information. For improved security, blockchain programs should undergo normal protection audits, particularly for clever contracts, to discover vulnerabilities which can cause statistics leakage. comfortable coding practices and formal verification techniques can further reduce the danger of unauthorized get right of entry to exploitation. Authentication mechanisms may be reinforced thru decentralized identification frameworks that allow users to control their credentials without counting on centralized authorities. The adoption of multi-issue authentication and function-based get entry to manage in permissioned blockchain environments can similarly enhance confidentiality and trust. collectively, these hints support the development of secure, privateness-keeping, and scalable blockchain structures suitable for actual-world applications.

CONCLUSION

Blockchain generation offers extensive ability for at ease and obvious virtual systems. however, protective records privateness and confidentiality in blockchain environments remains a powerful undertaking, especially in open public networks. This research has mapped key challenges, compared privateness solutions, and outlined strengths, weaknesses, and open troubles. at the same time as advances in cryptography and permissioned ledgers offer paths ahead, trade-offs among privateness, overall performance, and regulatory compliance persist. Future studies must focus on scalable, privacy-preserving blockchain architectures that strike a balance between openness and secrecy.

REFERENCES

[1] S. Meiklejohn *et al.*, “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,” in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2013.

[2] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” *IEEE Security & Privacy*, vol. 13, no. 6, pp. 14–17, 2015.

[3] E. Ben-Sasson *et al.*, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” in *Proceedings of the IEEE Symposium on Security and Privacy*, 2014.

[4] N. van Saberhagen, “CryptoNote v2.0,” White Paper, 2013.

[5] E. Androulaki *et al.*, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in *Proceedings of the European Conference on Computer Systems (EuroSys)*, 2018.

[6] M. Cachin, “Architecture of the Hyperledger Blockchain Fabric,” IBM Research Report, 2016.

[7] N. Atzei, M. Bartoletti, and T. Cimoli, “A Survey of Attacks on Ethereum Smart Contracts,” in *Principles of Security and Trust (POST)*, 2017.

[8] L. Luu *et al.*, “Making Smart Contracts Smarter,” in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2016.