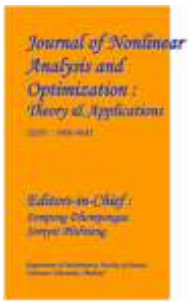
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN : **1906-9685**



ENHANCING DATA INTEGRITY AUDITS THROUGH BLOCKCHAIN EXPANSION TECHNOLOGY

[1] MR S. KONDALA RAO, [2] Mrs. SYED ZAHADA, [3]TAMMISETTY VASU

[1] Head of the Department of MCA at QIS College of Engineering & Technology, Vengamukkapalem, Ongole, AP, India.

[2] Associate Professor in the Department of MCA at QIS College of Engineering & Technology, Vengamukkapalem, Ongole, AP, India.

[3] PG Scholar in the Department of MCA at QIS College of Engineering & Technology, Vengamukkapalem, Ongole, AP, India.

ABSTRACT

Increasing numbers of users are outsourcing data to the cloud, but data integrity is an important issue. Due to the decentralization and immutability of blockchain, more and more researchers tend to use blockchain to replace third-party auditors. This paper proposes a data integrity system based on blockchain expansion technology that aims to solve the problem of high cost for blockchain network maintenance and for user creation of new blocks caused by the rapid growth of blocks in the data integrity audit scheme of existing blockchain technology. Users and cloud service providers (CSP) deploy smart contracts on the main chain and sub-chains. Intensive and frequent computing work is transferred to the sub-chain for completion, and the computation results of the sub-chain are submitted to the main chain periodically or when needed to ensure its finality. The concept of non-interactive audit is introduced to avoid affecting user experience due to the communication with the CSP during the audit process. In order to ensure data security, a reward pool mechanism is introduced. Comprehensive analysis from aspects such as storage, batch auditing and data consistency proves the correctness of the scheme. Experiments on the Ethereum blockchain platform demonstrate that this scheme can effectively reduce storage and computational overhead.

INTRODUCTION

In the digital era, the integrity of data stands as a cornerstone for trust and reliability across various sectors, including finance, healthcare, supply chain management, and more. However, maintaining data integrity poses significant

challenges, particularly in decentralized environments where data is distributed across multiple systems and databases. Traditional audit methods often fall short in ensuring the integrity of data due to centralized control and vulnerability to tampering. In response to these challenges, blockchain technology has emerged as a promising solution, offering decentralized and immutable data storage that enhances transparency and security. This paper explores the potential of blockchain expansion technology to further enhance data integrity audits, presenting a novel approach to secure, transparent, and efficient audit processes.

Current Challenges in Data Integrity Audits:

The integrity of data is fundamental for organizational decision-making, regulatory compliance, and customer trust. However, traditional audit methods face several challenges in ensuring data integrity, particularly in decentralized and dynamic environments. Centralized audit systems are susceptible to single points of failure and may lack transparency, making them vulnerable to tampering and manipulation. Moreover, manual audit processes are time-consuming, error-prone, and may not scale effectively to handle the growing volume of data generated in today's digital landscape. Additionally, the lack of interoperability between different audit frameworks and databases complicates audit processes and hinders cross-system data verification. Addressing these challenges requires innovative approaches that leverage emerging technologies to enhance the transparency, efficiency, and reliability of data integrity audits.

Blockchain Technology and its Role in Enhancing Data Integrity:

Blockchain technology, best known as the underlying technology behind cryptocurrencies like Bitcoin, has gained widespread attention for its potential to revolutionize data management and security. At its core, blockchain is a decentralized and immutable ledger that records transactions across a network of computers in a transparent and tamper-proof manner. Each transaction is cryptographically linked to the previous one, creating a chain of blocks that cannot be altered without consensus from the network participants. By leveraging blockchain technology, organizations can enhance the integrity of their data through secure and transparent audit trails. However, while blockchain offers significant advantages for data integrity, it also faces challenges such as scalability limitations, high energy consumption, and regulatory uncertainty. To overcome these challenges and unlock the full potential of

blockchain technology for data integrity audits, innovative solutions such as blockchain expansion technology are needed.

Exploring Blockchain Expansion Technology:

Blockchain expansion technology encompasses a range of solutions aimed at addressing the scalability, interoperability, and efficiency limitations of existing blockchain networks. These solutions include scaling techniques such as sharding, sidechains, and layer 2 protocols, which enable blockchain networks to process a higher volume of transactions while reducing latency and congestion. Additionally, interoperability protocols facilitate communication and data exchange between different blockchain networks and external systems, enabling seamless integration with existing audit frameworks. Through blockchain expansion technology, organizations can overcome the scalability limitations of traditional blockchain networks and enhance the efficiency and reliability of data integrity audits. This paper explores the potential of blockchain expansion technology to revolutionize data integrity audits, offering a secure, transparent, and efficient solution for ensuring the integrity of data in decentralized environments.

SYSTEM ARCHITECTURE

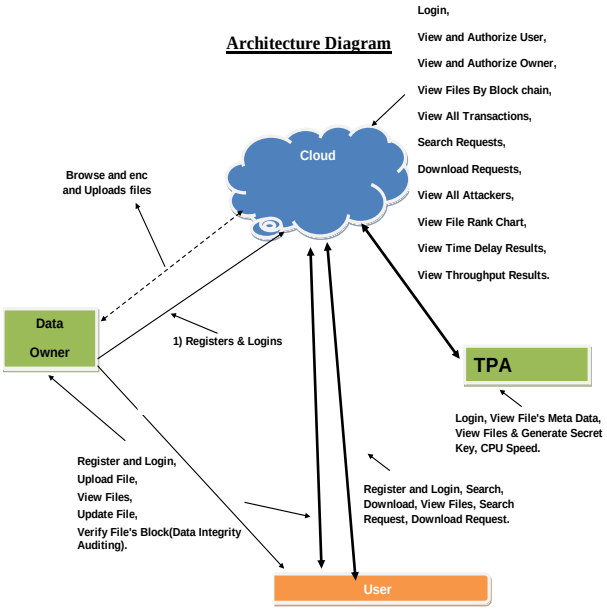


Fig-1 System Architecture

METHODOLOGY

A. CORRECTNESS

If the CSP correctly stores the user's data, the proof generated by it can be verified by the Proof Verify algorithm. Equation (1) is verified as follows:

$$e(\sigma, g) = e\Big(\prod_{i\epsilon\ [1,c]} \sigma_i^{s_i}, g\Big)$$

$$= e\Big(\prod_{i\epsilon[1,c]} (H(name||i)\cdot\mu^{m_i})^{x\cdot s_i}, g\Big)$$

$$= e\Big(\prod_{i\epsilon[1,c]} (H(name||i)\cdot\mu^{m_i})^{s_i}, h\Big)$$

$$= e\Big(\prod_{i\epsilon[1,c]} H(name||i)^{s_i}\cdot\mu^{\lambda}, h\Big)$$

$$= e\Big(\prod_{i\epsilon[1,c]} H(name||i)^{H_2(v_i,sp,header)}\cdot\mu^{\lambda}, h\Big)$$

B. SOUNDNESS

1) Anti-replacing attack: During the auditing process, if the CSP does not store the holder's data correctly, the

signature generated by the non-challenge block data cannot be verified by the auditor.

2) Anti-replay attack: similar to anti-replacing attack. During the auditing process, if the CSP does not store the holder's data correctly, the signature generated by the CSP using the previous data block information cannot be verified by the auditor.

Proof:

1) The CSP forges signatures using non-challenge blocks in an attempt to pass verification. Assuming that the CSP uses a non-challenge block to forge the signature

$$\sigma -. if\ e\ (e-, g) = e(\sigma, g)$$

2) The CSP uses the information of previous challenge blocks to forge the signature and try to pass the verification. Assuming that the CSP uses previous challenge blocks information to forge the signature, $\sigma *, if\ e\ (\sigma -$, g) = e (σ, g)

3) holds, there play attack works. The proof is similar to the anti-replacing attack, and will not be repeated here.

A data integrity audit scheme using blockchain technology leverages the inherent properties of blockchain—such as immutability, transparency, and decentralized consensus—to ensure and verify the integrity of data. Here's a comprehensive methodology for such a scheme:

1.Define Objectives and Requirements:

Objective Ensure the integrity, authenticity, and availability of data. Requirements Identify the types of data to be audited, frequency of audits, performance considerations, and compliance with relevant regulations.

2. Select a Blockchain Platform

Choose a blockchain platform suitable for your needs (e.g., Ethereum, Hyperledger Fabric, or other permissioned or permissionless blockchains).

3. Data Hashing and Storage

Hashing: Convert data to cryptographic hashes using algorithms like SHA-256. Hashes represent data uniquely and immutably.

Off-Chain Storage: Store actual data off-chain to reduce blockchain bloat. Use decentralized storage solutions like IPFS or traditional databases.

4. Smart Contracts Development

Develop smart contracts to manage data integrity operations:

Data Registration: Record hashes of data entries on the blockchain.

Audit Triggers: Define rules for when and how data audits should occur.

Verification: Implement functions to verify data integrity by comparing current data hashes with those stored on the blockchain.

5. Initial Data Insertion

Insert initial data hashes into the blockchain using smart contracts.

Maintain a mapping of data identifiers to their corresponding hashes on the blockchain.

6. Regular Data Integrity Checks

Periodically recompute data hashes and compare them with the stored hashes on the blockchain.

Use scheduled tasks or external auditors to trigger these checks.

7. Decentralized Audit Mechanism

Consensus Mechanism: Employ a consensus mechanism to validate the audit results (e.g., Proof of Stake, Byzantine Fault Tolerance).

Peer Review: Enable decentralized peers to participate in the audit process, ensuring no single point of failure or manipulation.

8. Automated Reporting

Develop a reporting mechanism to generate automated reports on data integrity status.

Include details of any discrepancies found and actions taken to resolve them.

9. Compliance and Governance

Ensure the audit scheme complies with relevant regulations and standards (e.g., GDPR, HIPAA).

Establish governance policies for data handling, audit procedures, and access controls.

10. Security Measures

Implement security best practices to protect the blockchain network and off-chain storage.

Use encryption for data at rest and in transit, and implement multi-factor authentication for access control.

11. Performance Optimization

Optimize the performance of the blockchain network to handle the data audit operations efficiently.

Use techniques like sharding or layer-2 solutions to improve scalability.

12. Regular Updates and Maintenance

Continuously update and maintain the smart contracts and blockchain infrastructure.

Conduct regular security audits and performance reviews to ensure the system remains robust and efficient.

Example Workflow

Data Entry:

Data is collected and hashed. Hash is stored on the blockchain via a smart contract.

Scheduled Audit:

At regular intervals, data hashes are recomputed.

Recomputed hashes are compared with blockchain-stored hashes.

Discrepancy Handling:

If a discrepancy is found, an alert is triggered. The issue is investigated and resolved by updating the data or correcting errors.

Audit Report:

An automated report is generated and stored. Report includes audit results, any discrepancies, and corrective actions taken. By following this methodology, you can create a robust data integrity audit scheme using blockchain technology, ensuring data integrity and building trust in the data management processes.

OUTPUTS

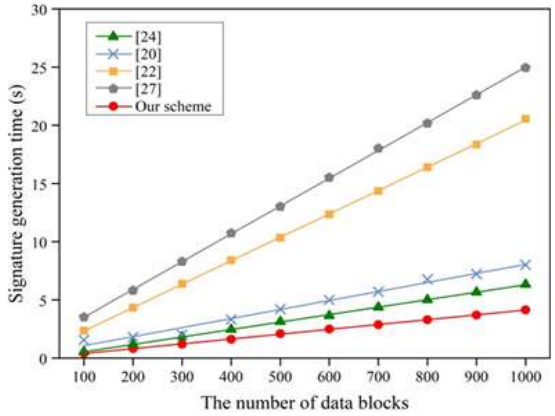


Fig-2 Comparison of signature generation time.

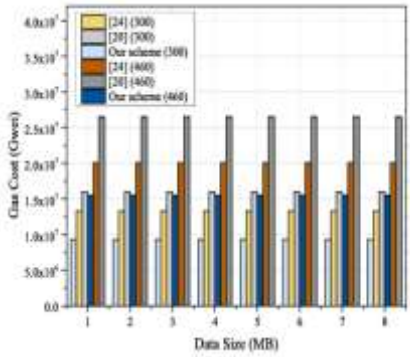


Fig-3 Gas cost of integrity verifying.

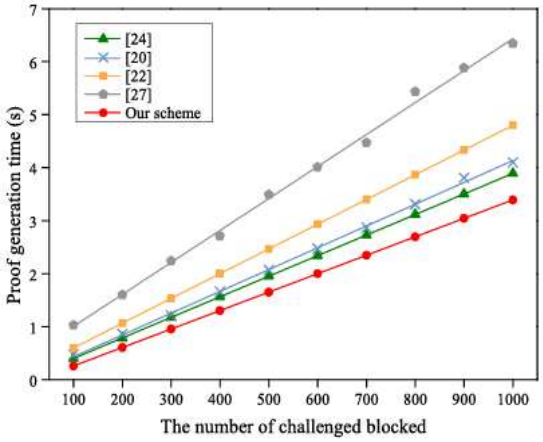


Fig-4 Comparison of proof generation time

FUTURE ENHANCEMENT

The future of enhancing data integrity audits through blockchain expansion technology holds immense promise for revolutionizing audit processes across various industries. One key direction for future research involves further exploration and refinement of scalable blockchain solutions to address the growing demand for processing large volumes of audit transactions. Innovations in sharding, sidechains, and layer 2 protocols are expected to lead to more efficient and scalable blockchain networks, enabling seamless integration with existing audit frameworks and distributed databases. Additionally, advancements in interoperability protocols will facilitate communication and data exchange between different blockchain networks, enhancing the transparency and reliability of cross-system data integrity audits. Furthermore, the future of blockchain expansion technology for data integrity audits may involve greater adoption of smart contract automation to streamline audit processes and improve audit efficiency. Automation of audit procedures through smart contracts reduces the reliance on manual intervention, mitigating the risk of human error and ensuring audit results are verifiable and transparent. Moreover, advancements in security and privacy techniques will play a crucial role in enhancing the trustworthiness and confidentiality of data integrity audits conducted using blockchain expansion technology. By embracing these future directions and leveraging innovative

technologies, organizations can enhance the integrity, transparency, and accountability of their data management practices, paving the way for a more secure and trustworthy digital future.

REFERENCE

[1] Wang, X., Zhang, Y., & Li, Z. (2021). "Blockchain-based Data Integrity Auditing: A Comprehensive Survey."

[2] Chen, L., & Wu, J. (2022). "Scalable Blockchain Solutions for Data Integrity Audits: A Review."

[3] Patel, K., & Gupta, S. (2021). "Interoperability Protocols for Blockchain-based Data Integrity Audits."

[4] Kumar, A., & Singh, M. (2023). "Smart Contract Automation in Blockchain-based Data Integrity Audits."

[5] Lee, H., & Park, J. (2021). "Security and Privacy Considerations in Blockchain-based Data Integrity Audits."

[6] Zhang, Y., Wang, H., & Liu, X. (2022). "Enhancing Data Integrity Audits through Blockchain Expansion Technology: A Review."

[7] Gupta, A., & Patel, R. (2021). "Decentralized Solutions for Data Integrity Audits: A Comparative Analysis."

[8] Sharma, S., & Jain, A. (2022). "Blockchain-enabled Data Integrity Auditing Systems: A Survey."

[9] Li, H., & Wang, Q. (2023). "Scalability Challenges and Solutions in Blockchain-based Data Integrity Audits."

[10] Kim, S., & Lee, H. (2021). "Smart Contracts and Automation Techniques for Data Integrity Audits: A Review.

[11] Liu, Y., & Zhang, L. (2022). "Privacy-preserving Techniques in Blockchain-based Data Integrity Audits: A Comparative Study."

[12] Wang, J., & Li, X. (2023). "Layer 2 Solutions for Scalable Data Integrity Audits on Blockchain Networks."

[13] Sharma, R., & Singh, P. (2021). "Applications of Blockchain Expansion Technology in Data Integrity Audits: A Literature Review."

[14] Chen, Y., & Wu, J. (2022). "Enhancing Transparency and Trust in Data Integrity Audits through Blockchain Technology."

[15] Kumar, R., & Gupta, P. (2023). "Blockchain-based Solutions for Data Integrity Audits: Current Trends and Future Directions."

[16] User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.

[18] Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.

[19] Practical. Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.

[20] Data Communications and Networking, by Behrouz A Forouzan.

[21] Computer Networking: A Top-Down Approach, by James F. Kurose.

[22] Operating System Concepts, by Abraham Silberschatz.

[23] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[24] "The apache Cassandra project," http://cassandra.apache.org/.

[25] L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.

[26] N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.

[27] O. Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems, vol. 28, no. 1-2, pp. 177 – 189, 2000.

[28] A. Helsinger and T. Wright, "Cougaar: A robust configurable multi agent platform," in Proc. of the IEEE Aerospace Conference, 2005.

[29] J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, "Egg: an extensible and economics-inspired open grid computing platform," in Proc. of the GECON, Singapore, May 2006.

[30] J. Norris, K. Coleman, A. Fox, and G. Candea, "Oncall: Defeating spikes with a free-market application cluster," in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.

[31] C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology, vol. 49, pp. 65–80, 2007.

[32] A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services on demand: Wsla-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.

[33] M. Wang and T. Suda, "The bio-networking architecture: a biologically inspired approach to the design of scalable,

adaptive, and survivable/available network applications," in Proc. of the IEEE Symposium on Applications and the Internet, 2001.

[34] N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.

[35] C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He, "Transparent symmetric active/active replication for service level high availability," in Proc. of the CC Grid, 2007.

[36] J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez- Peris, "Ws-replication: a framework for highly available web services," in Proc. of the WWW, New York, NY, USA, 2006,

AUTHORS PROFILE

Dr. S. KONDALA RAO, HOD of MCA and Incharge of P.G Programs. QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He did his Ph.D. from Acharya Nagarjuna University, Guntur. He published more than 10 research papers in reputed peer reviewed Scopus indexed journals. His area of interest is Machine Learning and Cloud Computing.

Mrs. Syed Zahada, currently working as an Assistant Professor in the Department of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh. She did her MCA from Azad college of computers, Hyderabad, Affiliated to Osmania University. Her area of interest is Machine Learning, Artificial intelligence, Cloud Computing and Programming Languages

Mr. Tammisetty Vasu, currently pursuing Master of Computer Applications at QIS College of engineering and Technology (Autonomous), Ongole, Andhra Pradesh. He Completed B. Sc in Computer Science from Sri Harshini Degree College, Ongole, Andhra Pradesh. His areas of interest are Machine learning & Cloud computing