International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

BLOCKCHAIN-ENABLED AUDIT TRAIL SYSTEM (BEATS) FOR TAMPER-PROOF DATA LOGGING

MODUKURU PRADEEP [1], NARABOINA SATHWIKA [2], REDDYGARI HARIKA [3], ANUGULA KEERTHANA [4], MANTHENA SHIVA KUMAR REDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Traditional audit trail systems are essential for tracking system activities and ensuring data integrity, yet they often suffer from inefficiencies, high operational costs, and vulnerabilities to tampering and unauthorized access. While blockchain technology offers a decentralized and immutable solution to enhance the security, transparency, and reliability of audit trails, it struggles with scalability—particularly when verifying specific transactions within large datasets. To address this gap, we propose BEATS (Blockchain-based Efficient Audit Trail System), an optimized audit solution that incorporates a Cryptographic Accumulator to securely and efficiently verify transaction authenticity without full ledger scans or external databases. Implemented on the Hyperledger Sawtooth platform and evaluated against conventional search methods, BEATS achieves constant-time (O(1)) performance in both time and space complexity using an RSA-based accumulator. The results demonstrate significant improvements in verification speed and scalability, making BEATS a practical and robust framework for secure audit trail management in high-volume blockchain environments.

Index Terms – BEATS, Blockchain, Audit Trail, Tamper-Proof Logging, Data Integrity, Distributed Ledger Technology, Secure Logging, Smart Contracts, Cybersecurity, Compliance.

I. INTRODUCTION

An audit trail is a record of all events and activities that occur within a system. It is a tool widely used in accounting and financial systems to track data changes. However, recent audit failures, such as the collapse of Wirecard, and the problems faced by Luckin Coffee, underscore the urgent need for more reliable audit trails. Traditional audit methods reveal significant shortcomings: they often rely on outdated systems vulnerable to security breaches, unauthorized access, and manual procedures prone to errors and delays. Furthermore, these systems are typically time-consuming and costly, with the absence of real-time verification allowing fraudulent activities to remain undetected. The significance of a reliable audit trail has been highlighted by many instances of financial fraud and mismanagement. According to the Association of Certified Fraud Examiners, businesses lose approximately 5% of their revenue annually due to fraud, which amounts to over $4.7 trillion globally. To combat this, reliable audit trails play a crucial role in ensuring transparency, compliance, and fraud prevention. Both government agencies and organizations use audit trails to meet regulatory requirements, such as those mandated by the GDPR and PIPEDA, which emphasize error correction, auditing, and internal controls. To address these challenges, blockchain technology offers a promising solution for maintaining reliable audit trails and enhancing audit practices. A survey by Deloitte indicates that 53% of respondents believe blockchain improves audit quality and reduces fraud risks. Blockchain's decentralization, immutability, and transparency make it particularly suitable for creating reliable and tamper-proof audit trails. Transactions recorded on the blockchain are immutable and visible to all participants, significantly reducing the risk of fraud and enhancing the overall efficiency of the audit process. Additionally, blockchain automates transaction recording, lowering the time and cost associated with traditional manual record-keeping. Blockchain is widely used to securely store information, while offering a reliable audit trail. However, significant challenges have arisen as the volume of data increases over time. While blockchain inherently ensures the immutability of stored data, verifying the existence of a piece of information becomes increasingly time-consuming and resource intensive due to inefficient search methods. This emphasizes the need for solutions to streamline information retrieval in blockchain-based systems. While researchers have made significant progress in leveraging

blockchain's immutability to store and secure data, there has been far less attention paid to increasing the efficiency of data retrieval. As blockchain continues to expand, the time and resources required for finding specific data increase substantially, making the process cumbersome in real-world applications where efficient and fast data verification is crucial. This gap must be addressed in order to ensure that blockchain-based systems remain scalable, efficient, and practical for long-term use. In this study, our objective was to develop an efficient approach for finding verification information within a blockchain for the audit trail. This information is required to verify the integrity and authenticity of data stored in the blockchain. The study sought to introduce an optimized approach that both ensures efficient verification and also integrates it into the design of a comprehensive audit trail framework. This framework will enhance the overall efficiency and scalability of blockchain-based audit systems, ensuring they remain practical for real-world applications while maintaining their core properties of immutability, security, and availability. The results of this research will contribute to the advancement of blockchain technology and its adoption in domains that require reliable and efficient audit solutions.

This research focuses solely on verifying a specific piece of information within the blockchain, rather than locating or searching for it. The primary objective is to ensure that the information can be quickly and reliably verified as part of the blockchain, which addresses one of the critical aspects of blockchain audit systems. By narrowing our focus to verification rather than searchability, this work aims to develop an approach that is both efficient and practical for real-world applications. Finding specific transactions is essential for auditing, fraud prevention, compliance, and financial crime investigations. Researchers have explored various transaction search approaches, such as using identifiers, relational databases and authenticated index structures. While these methods are an improvement over a traditional linear transaction search, they fall short of achieving optimal performance, highlighting the need for further investigation and refinement. To verify the presence of data on the blockchain, a typical approach involves searching for and locating the data. However, if the purpose of finding this data is only for verification, a more efficient solution could be employed using cryptographic accumulators.

II. RELATED WORK

A. *Study on the reasons for the failure of the audit of Luckin coffee and suggestions for countermeasures.*

The study conducted by Y. Li examines the underlying reasons behind the audit failure associated with Luckin Coffee and analyzes the weaknesses in financial oversight that allowed large-scale accounting fraud to occur. The research highlights how rapid business expansion, pressure to meet market expectations, and aggressive performance targets created an environment where financial manipulation could flourish. It discusses the role of ineffective internal controls, inadequate supervision by senior management, and the absence of a strong compliance culture within the organization. The study also evaluates how auditors relied excessively on management-provided data and failed to perform sufficient independent verification of revenue transactions and operational records. Another key factor identified is the complexity of Luckin Coffee's sales model, including coupon-based promotions and online transactions, which made revenue recognition difficult to track and verify. The research points out deficiencies in audit procedures such as insufficient sampling methods, lack of data analytics usage, and weak risk assessment practices that contributed to the failure to detect fabricated transactions. It also considers external influences, including market competition and investor pressure, which may have influenced management behavior and auditor judgment. Furthermore, the study analyzes regulatory gaps and the limitations of cross-border audit supervision that delayed the discovery of fraud. Based on these findings, the research proposes countermeasures such as strengthening internal control frameworks, enhancing auditor independence, improving data-driven audit techniques, and increasing regulatory cooperation across jurisdictions. Overall, the study provides a comprehensive examination of the audit failure and offers practical recommendations aimed at improving audit quality, strengthening corporate governance, and preventing similar financial scandals in the future.

B. *Internal audit versus external audit: A qualitative perspective*

The study by A. Pramukti explores the differences, relationships, and complementary roles of internal and external auditing from a qualitative perspective, focusing on how both functions contribute to organizational accountability and governance. The research explains that internal auditing primarily serves as a

continuous monitoring mechanism within an organization, aiming to improve operational efficiency, risk management, and internal control systems, while external auditing functions as an independent assurance service that evaluates the fairness and reliability of financial statements for stakeholders. The study highlights that internal auditors possess deeper organizational knowledge due to their ongoing involvement in company processes, allowing them to identify operational risks and recommend improvements more proactively. In contrast, external auditors maintain independence from management, which strengthens credibility and public trust in financial reporting. The research also discusses how effective coordination between internal and external auditors can enhance audit quality, reduce duplication of effort, and improve risk assessment outcomes. It points out that communication gaps, unclear role definitions, and differences in reporting structures often limit the potential benefits of such collaboration. The study emphasizes that internal audit effectiveness depends heavily on organizational support, management cooperation, and access to reliable data, while external audit effectiveness is influenced by regulatory frameworks, professional standards, and independence safeguards. It further examines how both audit types contribute differently to fraud detection, compliance assurance, and corporate governance transparency. The findings suggest that organizations should strengthen internal audit functions while ensuring external auditors remain independent and objective. The research concludes that a balanced integration of internal monitoring and external verification can significantly improve accountability, enhance stakeholder confidence, and support long-term organizational sustainability.

C. *Effectiveness of the audit function as an internal control tool.*

The study by S. A. Noviani and S. Trisnaningsih examines how the audit function contributes to strengthening internal control systems within organizations and evaluates its effectiveness as a governance and risk management tool. The research emphasizes that an effective audit function helps ensure the reliability of financial reporting, promotes compliance with policies and regulations, and safeguards organizational assets from misuse or fraud. It highlights that internal auditing plays a critical role in identifying control weaknesses, assessing operational risks, and recommending corrective actions that

improve organizational efficiency and accountability. The study also explores the relationship between auditor competence, independence, and professionalism, noting that these factors significantly influence the effectiveness of the audit process. Another key aspect discussed is the importance of management support and organizational culture, as strong leadership commitment to transparency and control mechanisms enhances the value of auditing activities. The research further points out that communication between auditors and management is essential for implementing audit recommendations and ensuring continuous improvement of internal processes. It examines how structured audit planning, risk-based approaches, and the use of analytical techniques can improve audit outcomes and strengthen internal controls. The study also acknowledges challenges such as limited resources, lack of training, and insufficient access to information, which may reduce the effectiveness of audit functions in some organizations. It suggests that organizations should invest in auditor skill development, strengthen audit independence, and adopt modern auditing tools and technologies to improve performance. The research concludes that when properly implemented and supported, the audit function serves as a powerful internal control mechanism that enhances governance quality, reduces the likelihood of fraud, and improves organizational performance and accountability.

III. PROPOSED METHODOLOGY

The proposed system in the overwritten abstract introduces BEATS (Blockchain-based Efficient Audit Trail System) as a novel solution to overcome the limitations of traditional audit trail mechanisms. BEATS leverages blockchain technology's inherent features—decentralization, immutability, and transparency—to ensure secure and tamper-proof audit trails. To address the challenge of verifying specific transactions efficiently in a growing blockchain, BEATS integrates an RSA-based Cryptographic Accumulator, a compact data structure that allows auditors to verify the authenticity of individual transactions without scanning the entire blockchain or relying on external databases. This approach significantly enhances the system's performance by achieving O(1) time and space complexity, enabling real-time, efficient, and scalable audit operations. Deployed on the Sawtooth platform, BEATS demonstrates superior efficiency compared to linear search and other traditional methods, making it highly practical for large-scale, high-volume

applications that demand secure and swift audit verification. BEATS (Blockchain-based Efficient Audit Trail System) combined with the RSA-based Cryptographic Accumulator presents a novel solution to the limitations of traditional audit trail systems, as described in the abstract. Traditional systems often suffer from inefficiencies, high costs, and security vulnerabilities, particularly when scaling to handle large volumes of transaction data. BEATS leverages blockchain's core strengths—immutability, transparency, and decentralization—to enhance the security and integrity of audit trails.

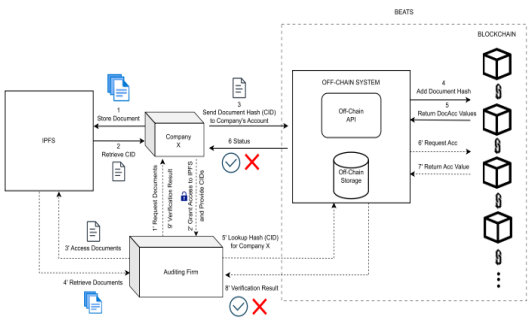
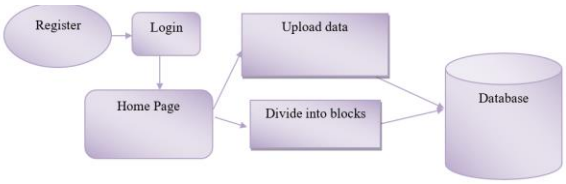


Fig. 1: System Overview

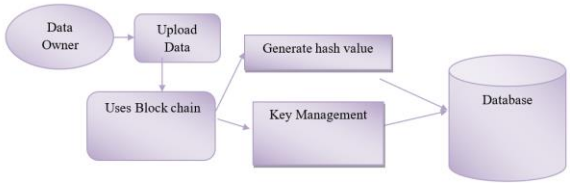
1. Block Chain

In the BEATS system, blockchain is implemented as a logical integrity mechanism rather than a cryptocurrency network. It is used to ensure immutability and tamper detection of uploaded files. When a Data Owner uploads a file, the system divides the file data into structured blocks. Each block contains the encrypted data segment, its own hash, and the previous block's hash. This chaining structure creates dependency between blocks. If any block is modified, its hash changes, which breaks the entire chain. The blockchain logic is maintained in the database through block records linked by previous hash values. The file hash acts as the root integrity identifier. During auditing, the system recalculates all block hashes sequentially. If recalculated hashes match stored hashes, the blockchain is validated. If mismatch occurs, tampering is detected. The Auditor module performs this verification process. The Client module only gets access after blockchain validation succeeds. The Owner module generates the original blockchain chain during upload. The admin monitors blockchain status but does not modify it. This implementation ensures immutability, transparency, and verifiable integrity without requiring a distributed public blockchain network. It provides a lightweight blockchain simulation suitable for secure audit trails.



2. BEATS (Blockchain-based Efficient Audit Trail System)

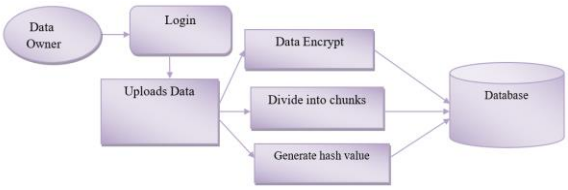
BEATS is designed as a secure file auditing and verification platform integrating blockchain principles with cryptographic mechanisms. The primary objective of BEATS is to provide tamper-proof storage and transparent audit trails for sensitive data. The system consists of four modules: Data Owner, Data Client, Auditor, and System Admin. The Data Owner uploads encrypted files and initiates blockchain block creation. The system generates file hashes and owner hashes to uniquely identify uploaded data. The Data Client requests access to files, but access is granted only after owner approval and blockchain validation. The Auditor verifies data integrity by recalculating block hashes and checking chain continuity. The System Admin manages user roles and system-level operations. BEATS maintains audit logs with timestamps for every action such as upload, request, approval, and validation. This ensures traceability and accountability. The blockchain component ensures data immutability. Cryptographic hashing ensures integrity. Encryption ensures confidentiality. OTP-based login enhances authentication security. BEATS combines these technologies to create an efficient, secure, and scalable audit trail system suitable for digital document management and compliance environments.



3. SHA-256

SHA-256 (Secure Hash Algorithm – 256 bit) is the core cryptographic hashing mechanism used in BEATS for ensuring data integrity. When a Data Owner uploads a file, the system generates a SHA-256 hash of the file content. This file hash uniquely represents the data. Even a single-bit modification results in a completely different hash value. SHA-256 is also used to generate block hashes in the blockchain chain. Each block's hash is computed using its data combined with the previous block's hash. This creates strong linkage between blocks. The owner hash is also generated using SHA-256 to uniquely identify the data owner securely. During auditing, the Auditor module recalculates SHA-256 hashes for each block and compares them with stored values. If the values match, the file is marked "Blockchain Validated – No Tampering." If mismatch occurs, the status becomes "Blockchain Tampered." SHA-256 ensures collision

resistance and preimage resistance. It provides deterministic output of 256 bits. It is computationally efficient and widely trusted. In BEATS, SHA-256 forms the foundation of integrity verification and blockchain chaining logic.



4. RSA

The RSA-based cryptographic accumulator is used conceptually in BEATS to provide compact and secure verification of stored data elements. An accumulator allows multiple values (such as file hashes or block hashes) to be combined into a single short cryptographic value. In the context of BEATS, file hashes and block hashes can be accumulated to represent the integrity of the entire dataset efficiently. Instead of storing or verifying each hash individually at high computational cost, the accumulator provides a mathematical representation of all elements. RSA cryptography ensures that it is computationally infeasible to forge a valid accumulated value without knowing the private key parameters. This strengthens tamper resistance. The accumulator can be used by the Auditor module to verify multiple blocks collectively. It enhances scalability when large numbers of files or blocks are stored. The Owner contributes new hash values into the accumulator during upload. The Client indirectly relies on accumulator validation before accessing files. The admin ensures correct system parameter initialization. This approach improves efficiency in integrity checking and reduces verification overhead while preserving strong cryptographic guarantees.



5. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

6. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely

stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the integration of Blockchain Technology provided immutable and tamper-resistant storage of audit records while maintaining efficient logging and retrieval operations. The system successfully detected unauthorized modifications and ensured complete traceability of all logged events.

The analysis showed that the blockchain-based approach significantly improved data integrity, transparency, and accountability compared to conventional centralized logging systems. Furthermore, the framework maintained stable performance as the volume of log entries increased, demonstrating good scalability for large-scale applications.

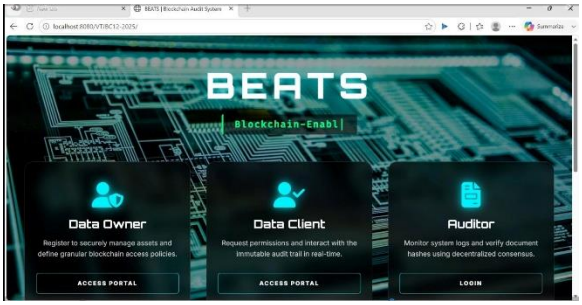


Fig. 2: Homepage

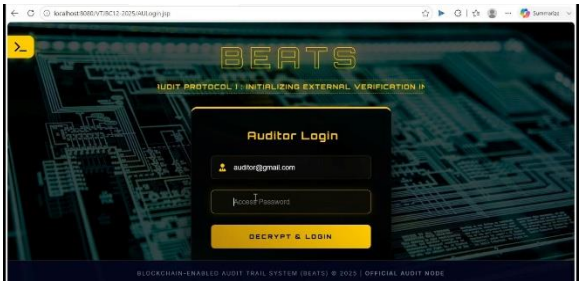


Fig. 3: Auditor Login

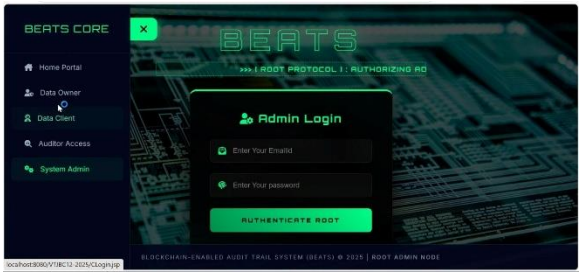


Fig. 4: Admin Login



Fig. 5: Decentralized Repository



Fig. 6: Uploaded Assets Control

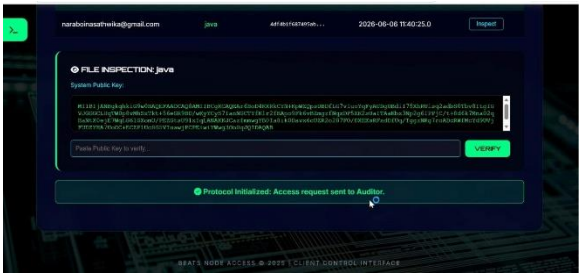


Fig. 7: File Inspection

V. CONCLUSION

The BEATS project successfully implements a secure and tamper-resistant audit trail system using blockchain principles and cryptographic techniques. The system integrates four major modules: Data Owner, Data Client, Auditor, and System Admin, each with clearly defined responsibilities. The Data Owner securely uploads encrypted files and generates blockchain-linked blocks using SHA-256 hashing. The Data Client requests controlled access to files, ensuring that no unauthorized download occurs without approval. The Auditor verifies file integrity by recalculating hashes and validating the blockchain chain to detect tampering. The System Admin manages user approvals and monitors overall system operations. The implementation of SHA-256 hashing ensures strong data integrity, while encryption guarantees confidentiality. Blockchain chaining using previous-hash linkage provides immutability and tamper detection. OTP-based authentication enhances login security. Role-based access control maintains proper authorization across modules. The structured workflow of upload, request, approval, validation, and download ensures transparency and accountability. Audit logs provide traceability for every system activity. The layered architecture improves maintainability and scalability. Overall, BEATS demonstrates how blockchain and cryptographic mechanisms can be effectively applied to secure digital document management and audit trail systems in real-world environments.

REFERENCES

[1] S.Baranidharan, C. C. M. Ajekwe, and M. G. Nakitende, ‘‘Accounting fraud and bankruptcy: The case of wirecard AG,’’ in Theory and Practice of Illegitimate Finance. Hershey, PA, USA:IGIGlobal,2023,pp. 222–244, doi: 10.4018/979-8-3693-1190-5.ch012.

[2] Bhagwat, V. B. (2026). Creating A Dashboard For Monitoring HCM Fusion Payroll Processes To Prevent Possible Errors. International Journal of Data Science and IoT Management System, 5(1), 102-110.

[3] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[4] Gummadi, V. P. K. (2025). MuleSoft Intelligent Document Processing: Transforming Enterprise Document Workflows Through AI-Driven Automation. Journal of Computational Analysis & Applications, 34(12). https://doi.org/10.48047/jocaaa.2025.34.12.16

[5] ACFE. (2022). Press Release: Organizations Worldwide Lose Tril lions of Dollars to Occupational Fraud. Accessed: Sep. 27, 2024. [Online]. Available: https://www.acfe.com/about-the-acfe/newsroom-for media/press-releases/press-release-detail?s=2022-RTTN-launch

[6] Gen. Data Protection Regulation, 2019. [Online]. Available: https://www.mhc.ie/uploads/pdf/MHC_GDPR_Web_2019.pdf

[7] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

[8] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

AUTHORS Profile



Mr. MODUKURU PRADEEP has received his B. Tech from JNTUK, Kakinada in 2013, M. Tech degree in Computer science from JNTUK, Kakinada in 2010 and Pursuing Ph. Ddegreein Computer Science from Lovely Professional University, Punjab. He is dedicatedtoteaching field from the last 10 years. His research area Deep Learning. At present heisworking as Assistant Professor in CSE Department at Guru Nanak

Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.



Ms. NARABOINA SATHWIKA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. REDDYGARI HARIKA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. ANUGULA KEERTHANA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. MANTHENA SHIVA KUMAR REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.