10.48047/jocaaa.2021.29.01.21

Improving Banking Transaction Integrity Through Decentralized Audit Trails

Adarsh Naidu
Independent Researcher, USA
Email : adarshnaidu2910@gmail.com

Abstract

Ensuring the integrity of banking transactions is essential for maintaining trust, regulatory compliance, and operational reliability in modern financial systems. Conventional banking infrastructures rely on centralized audit mechanisms that, while efficient, remain vulnerable to insider manipulation, single points of failure, and limited transparency. As transaction volumes increase and regulatory scrutiny intensifies, these limitations pose significant challenges to reliable auditability and long-term data integrity. This paper proposes a decentralized audit trail framework designed to enhance transaction integrity without disrupting existing banking operations. The proposed approach introduces a permissioned distributed ledger that records cryptographic representations of transaction events generated by centralized core banking systems. By decoupling transaction execution from audit assurance, the framework preserves system performance and data confidentiality while enabling immutable and independently verifiable audit records. The methodology emphasizes practical deploy ability, privacy preservation, and regulatory alignment, making it suitable for integration within legacy banking environments. The paper discusses the system architecture, audit record generation process, and integrity verification mechanism, demonstrating how selective decentralization can strengthen trust and accountability in banking transaction auditing.

Index Terms : Banking systems, transaction integrity, decentralized audit trails, distributed ledger technology, blockchain, financial auditing, data integrity, regulatory compliance.

I. Introduction

The integrity of banking transactions is fundamental to the reliability of financial systems, directly influencing customer trust, regulatory compliance, and institutional accountability. Modern banking environments process enormous volumes of digital transactions across heterogeneous platforms, relying on centralized core banking systems to ensure correctness and availability. Alongside transaction execution, audit mechanisms play a critical role in validating transaction authenticity, detecting fraudulent activity, and supporting regulatory oversight. However, in most existing architectures, audit trails are maintained within centralized databases controlled by the same entities responsible for transaction processing, creating inherent structural limitations.

Centralized audit systems are susceptible to several well-documented risks, including insider manipulation, unauthorized data alteration, and single points of failure. While access controls and security policies mitigate these risks to some extent, they do not eliminate the fundamental issue

10.48047/jocaaa.2021.29.01.21

of trust concentration. In scenarios involving internal fraud, system compromise, or post-incident investigations, the credibility of audit records can be questioned if those records are not independently verifiable. As regulatory requirements increasingly emphasize transparency, traceability, and long-term data integrity, these limitations pose significant challenges for financial institutions.

Recent advances in distributed ledger technologies have demonstrated strong potential for ensuring immutability, tamper resistance, and decentralized trust. Consequently, substantial research efforts have explored the application of blockchain and related technologies within financial systems, particularly in areas such as digital payments, interbank settlement, and asset tokenization. While these approaches highlight the advantages of decentralization, they often require fundamental changes to transaction execution models and introduce concerns related to scalability, privacy, and regulatory acceptance. As a result, their direct applicability to traditional banking infrastructures remains limited.

Despite the growing body of work on blockchain-based financial systems, comparatively little attention has been given to the use of decentralized ledgers as dedicated audit mechanisms for conventional banking operations. Transaction auditing represents a distinct problem domain with unique requirements, including strict confidentiality, minimal performance overhead, and compatibility with legacy systems. Addressing audit integrity independently from transaction execution offers an opportunity to leverage the benefits of decentralization while avoiding many of the challenges associated with fully decentralized banking models.

This paper addresses this gap by proposing a decentralized audit trail framework specifically designed to enhance transaction integrity in centralized banking systems. The proposed approach introduces a permissioned distributed ledger that operates as a parallel audit layer, recording cryptographic representations of transaction events after execution. By decoupling audit assurance from transaction processing, the framework preserves existing operational workflows while enabling immutable and independently verifiable audit records. The design prioritizes privacy preservation, regulatory alignment, and practical deployability within real-world banking environments.

II. Related Work

Ensuring transaction integrity and auditability in banking systems has been extensively studied through centralized auditing frameworks, cryptographic logging mechanisms, and, more recently, distributed ledger technologies. Traditional banking audit systems rely on centralized databases combined with access control, transaction logs, and reconciliation procedures to support compliance and fraud detection [1], [2]. While these systems are operationally efficient, prior studies have identified structural vulnerabilities arising from centralized control, including susceptibility to insider attacks, unauthorized data modification, and limited transparency during forensic investigations [3], [4].

To mitigate these risks, several works have proposed cryptographic techniques to secure audit logs, including hash chaining, secure timestamping, and digitally signed transaction records [5]–[7].

10.48047/jocaaa.2021.29.01.21

These approaches enhance tamper detection and non-repudiation but continue to depend on centralized storage infrastructures, thereby limiting independent verifiability. As noted in [8], the effectiveness of such mechanisms ultimately relies on trust in the managing institution, which may be insufficient in adversarial or regulatory dispute scenarios.

The emergence of blockchain and distributed ledger technologies has prompted significant research into decentralized trust mechanisms. Early foundational work demonstrated how consensus-based ledgers could ensure immutability and fault tolerance without centralized authority [9], [10]. Subsequent studies explored blockchain adoption in financial domains such as cryptocurrency systems, interbank settlement, and cross-border payments [11]–[13]. These systems highlight the potential of decentralization but often require transaction execution to occur directly on the ledger, introducing scalability, latency, and privacy challenges [14], [15].

Permissioned blockchain platforms were later proposed to address enterprise and regulatory requirements by restricting participation and employing efficient consensus protocols [16], [17]. Research has examined their use in financial reporting, compliance automation, and shared data repositories among trusted organizations [18], [19]. Although these approaches demonstrate improved feasibility for regulated environments, they typically emphasize transaction processing or data sharing rather than audit integrity as a primary objective.

A smaller body of literature has investigated blockchain-based audit and logging systems. Studies such as [20] and [21] suggest that decentralized audit trails can enhance accountability and tamper resistance by distributing trust across multiple stakeholders. However, many of these proposals either lack integration with existing banking infrastructures or replicate sensitive transaction data across ledger nodes, raising confidentiality and compliance concerns [22], [23]. Furthermore, some approaches introduce tight coupling between operational systems and distributed ledgers, increasing deployment complexity and performance overhead.

In contrast, recent research has begun to emphasize selective and modular use of distributed ledgers for specific assurance functions rather than full system decentralization [24]–[26]. These studies argue that decoupling integrity verification from transaction execution can provide strong trust guarantees while preserving operational efficiency. Building on this direction, the present work focuses explicitly on transaction audit integrity in centralized banking systems. By introducing a parallel, privacy-preserving decentralized audit layer, the proposed framework addresses limitations identified in prior work while aligning with practical deployment and regulatory constraints [27]–[30].

III. System Model and Problem Formulation

Modern banking systems operate through centralized core infrastructures responsible for executing, recording, and managing financial transactions. These systems are optimized for performance, availability, and consistency, and they typically rely on centralized databases to store transaction records and associated audit logs. While such architectures are effective for real-time transaction processing, they inherently concentrate trust and control within a single administrative

10.48047/jocaaa.2021.29.01.21

domain. As a result, the integrity of transaction records and audit logs is ultimately dependent on internal security controls and governance mechanisms.

In the considered system model, transactions are executed within a centralized core banking system that maintains authoritative transaction state. Audit records are generated internally and stored in centralized repositories for compliance, reconciliation, and forensic analysis. Although access controls and logging mechanisms are employed, the audit infrastructure remains vulnerable to insider manipulation, delayed detection of unauthorized modifications, and challenges in establishing independent verifiability during regulatory or legal investigations. These limitations motivate the need for an enhanced audit assurance mechanism that does not rely solely on centralized trust.

The problem addressed in this work is the absence of an immutable and independently verifiable audit trail for banking transactions that can operate alongside existing systems without disrupting transaction execution. Specifically, the challenge lies in ensuring that once a transaction is executed, its recorded state cannot be altered without detection, even by privileged internal entities. At the same time, any proposed solution must preserve transaction confidentiality, comply with regulatory requirements, and avoid introducing performance bottlenecks in high-throughput banking environments.

To formally define the problem, let a banking transaction be represented by a set of attributes including identifiers, participants, monetary values, and timestamps, all maintained within the centralized system. An audit mechanism is required to produce a verifiable representation of this transaction state such that any subsequent modification to the original record can be detected with high confidence. This audit mechanism must be tamper-evident, resistant to single points of failure, and accessible for verification by authorized auditors or regulators without exposing sensitive transaction details.

The system model assumes the existence of multiple trusted but independent entities, such as internal audit departments and regulatory bodies, that can participate in maintaining a shared audit infrastructure. These entities do not execute transactions but are responsible for validating and preserving audit records. By distributing audit responsibility across multiple stakeholders, the model reduces reliance on unilateral trust while maintaining clear operational boundaries between transaction processing and audit assurance.

Under this model, the core requirement is to design an audit framework that cryptographically binds transaction execution to an immutable external record while remaining operationally decoupled from the transaction processing system. Addressing this requirement forms the basis for the methodology presented in the following section, which introduces a decentralized audit trail architecture tailored for centralized banking environments.

IV. Methodology

A. Methodological Framework

10.48047/jocaaa.2021.29.01.21

The methodology proposed in this work is grounded in a system-oriented research approach aimed at improving transaction integrity in banking environments through decentralized audit mechanisms. The primary objective is not to redesign banking transaction execution but to enhance post-transaction accountability and trustworthiness. This distinction is critical in regulated financial systems, where replacing core banking infrastructure is neither practical nor desirable. Instead, the methodology introduces a decentralized audit layer that operates in parallel with existing systems while remaining cryptographically linked to them.

The research framework focuses on modeling how transactional events generated within centralized banking systems can be securely reflected in a decentralized audit structure. This approach ensures that the integrity of transaction records can be independently verified without interfering with operational workflows. The methodology is therefore aligned with real-world banking constraints, including performance requirements, regulatory compliance, and data confidentiality.

B. System Architecture and Audit Integration

The proposed system architecture consists of a centralized transaction execution environment coupled with a permissioned decentralized ledger dedicated exclusively to audit logging. Transactions continue to be processed within the core banking system using conventional mechanisms. Upon successful execution, each transaction triggers the generation of a corresponding audit event. This audit event captures essential metadata related to the transaction while excluding sensitive customer or financial details.

The decentralized audit ledger is maintained by a set of authorized participants, such as internal compliance units, audit departments, and optionally regulatory observers. A permissioned model is adopted to ensure controlled participation, accountability, and adherence to regulatory requirements. The separation between transaction execution and audit recording ensures that the decentralized component does not introduce latency into real-time banking operations, a critical factor for high-throughput financial systems.

C. Audit Record Generation and Ledger Commitment

Each audit record generated by the system contains a cryptographic hash derived from the transaction state at the time of execution, along with a timestamp and a digital signature generated by the originating system. The use of cryptographic hashing ensures that even minor modifications to transaction data can be detected during verification. Digital signatures provide non-repudiation, allowing the source of each audit record to be authenticated.

Once generated, the audit record is broadcast to the decentralized ledger network, where participating nodes validate its structure and authenticity. Validation is performed using a Byzantine Fault Tolerant consensus mechanism, which is well suited for permissioned environments where participants are known but not necessarily fully trusted. After consensus is achieved, the audit record is immutably appended to the ledger. From this point onward, the audit entry becomes tamper-evident and permanently verifiable.

10.48047/jocaaa.2021.29.01.21

D. Transaction Integrity Verification Mechanism

Transaction integrity verification is achieved by comparing the cryptographic representation stored on the decentralized ledger with the corresponding transaction record retrieved from the centralized system. During an audit, the transaction data is rehashed using the same cryptographic function employed during audit record generation. A match between the recomputed hash and the ledger-stored hash confirms that the transaction has remained unaltered since execution.

This verification process can be conducted at any point in time, including long after the transaction has occurred. Importantly, the process does not require direct access to the decentralized ledger by the transaction execution system, thereby reducing the risk of coordinated manipulation. The independence of the audit layer strengthens the credibility of audit outcomes and supports both internal and external compliance assessments.

E. Performance and Practical Considerations

The methodology explicitly considers performance and scalability constraints inherent to banking systems. Since audit records are generated only after transaction completion and are processed asynchronously, the proposed approach avoids introducing delays into transactional workflows. The decentralized ledger is used solely for audit purposes, significantly reducing data volume and consensus overhead compared to systems that attempt to process transactions directly on a blockchain.

Scalability is addressed through the use of lightweight audit records and efficient consensus protocols optimized for enterprise environments. By limiting ledger participation to authorized entities and restricting stored data to cryptographic summaries, the system remains feasible even under high transaction volumes. These design decisions collectively ensure that the proposed methodology is not only theoretically sound but also practically deployable within existing banking infrastructures.

F. Methodological Significance

The methodological significance of this approach lies in its ability to provide strong integrity guarantees without disrupting established banking operations. By decoupling audit assurance from transaction execution and leveraging decentralized ledger properties selectively, the methodology demonstrates how trust, transparency, and accountability can be enhanced in a controlled and regulation-compliant manner. This positions decentralized audit trails as a practical enhancement to banking systems rather than a disruptive technological replacement.

V. Novelty and Research Contribution

10.48047/jocaaa.2021.29.01.21

The primary novelty of this work lies in its conceptualization of decentralized ledger technology as an independent audit assurance mechanism rather than as a replacement for centralized banking transaction systems. While existing research predominantly explores blockchain-based solutions for transaction execution, settlement, or interbank payment processing, this study shifts the focus toward post-transaction integrity verification within conventional banking infrastructures. This reframing addresses a critical gap in the literature, as transaction integrity and audit reliability remain central concerns for financial institutions operating under strict regulatory oversight.

A distinguishing contribution of the proposed approach is the introduction of a decoupled decentralized audit layer that operates in parallel with the core banking system. Unlike tightly integrated blockchain architectures that require transaction logic to be embedded within distributed ledgers, the proposed methodology preserves existing operational workflows while enhancing trust guarantees. This architectural separation allows institutions to adopt decentralized audit capabilities incrementally, reducing deployment risk and lowering barriers to adoption in legacy environments.

Another novel aspect of this research is its privacy-preserving audit design. Rather than replicating transactional data across distributed nodes, the system records cryptographic representations of transaction states. This design choice ensures that audit transparency does not come at the expense of customer confidentiality or regulatory compliance. By enabling integrity verification through cryptographic comparison alone, the proposed framework demonstrates how decentralized auditability can coexist with stringent data protection requirements.

The work further contributes a regulator-aware audit model in which supervisory entities can participate as passive ledger observers. This capability introduces a new paradigm for regulatory oversight, enabling independent verification of transaction integrity without requiring direct access to internal banking databases. Such an approach supports continuous auditing and enhances institutional accountability while maintaining clear boundaries between operational control and supervisory functions.

Collectively, these contributions distinguish the proposed framework from existing blockchain-based banking solutions by prioritizing practicality, audit integrity, and regulatory alignment. The research demonstrates that meaningful integrity guarantees can be achieved through selective decentralization, offering a viable pathway for strengthening trust in banking systems without introducing disruptive architectural changes. As such, this work provides both conceptual and practical advancements in the application of decentralized technologies for financial audit assurance.

VI. Discussion and Analysis

The proposed decentralized audit trail framework introduces a structural shift in how transaction integrity is assured within centralized banking systems. Rather than treating decentralization as a replacement for transaction processing, the framework selectively applies distributed ledger

10.48047/jocaaa.2021.29.01.21

principles to the audit domain. This design choice significantly influences system performance, security guarantees, and deploy ability, and therefore warrants detailed discussion.

From a performance perspective, the decoupling of audit assurance from transaction execution plays a critical role in maintaining operational efficiency. Since transactions are finalized within the core banking system before audit records are generated, the proposed approach avoids introducing latency into time-sensitive transaction workflows. Audit events are processed asynchronously and contain only cryptographic summaries rather than full transaction data, reducing both data volume and consensus overhead. As a result, the framework is well suited to high-throughput banking environments where transaction processing delays are unacceptable.

In terms of security and integrity, the framework strengthens audit reliability by eliminating single points of control over audit records. Once an audit event is committed to the decentralized ledger, it becomes computationally infeasible to modify without detection. This property is particularly valuable in scenarios involving insider threats, where privileged users may have the ability to alter centralized logs. By distributing audit record maintenance across multiple independent participants, the system ensures that transaction integrity can be verified even if the centralized infrastructure is compromised.

Privacy and regulatory compliance are central considerations in banking system design, and the proposed framework explicitly addresses these constraints. The decision to store only cryptographic hashes and metadata on the decentralized ledger ensures that sensitive transaction details remain within the bank's internal systems. This minimizes data exposure while still enabling strong integrity verification. Furthermore, the use of a permissioned ledger allows institutions to define clear governance rules regarding participation, access rights, and audit responsibilities, aligning the framework with existing regulatory and compliance requirements.

The inclusion of regulator or external auditor nodes as passive participants represents an important step toward continuous and transparent auditing. Unlike traditional audit models that rely on periodic reporting and retrospective analysis, the proposed approach enables near-real-time verification of transaction integrity. This capability has the potential to reduce audit delays, improve regulatory confidence, and lower the cost of compliance by automating integrity verification processes.

Despite these advantages, certain limitations and challenges must be acknowledged. The framework assumes the availability of multiple trusted entities willing to participate in maintaining the decentralized audit ledger, which may not always be feasible in smaller institutions. Additionally, while the framework minimizes performance overhead, the scalability of the audit ledger remains dependent on the chosen consensus mechanism and network configuration. These factors highlight the importance of careful system design and governance planning during deployment.

.

10.48047/jocaaa.2021.29.01.21

Aspect	Centralized Audit	Blockchain-based Transactions	Proposed Decentralized Audit Trail
Transaction Execution	Centralized	Decentralized	Centralized
Audit Storage	Centralized DB	On-chain	Permissioned ledger
Data Exposure	Full records	Full/partial	Cryptographic hashes only
Tamper Resistance	Limited	High	High
Regulatory Fit	High	Medium	High

Table 1: Comparison of Audit Approaches

A. Evaluation and Results

This section evaluates the proposed decentralized audit trail framework in terms of integrity assurance, operational overhead, and scalability feasibility under realistic banking constraints. Because the framework is designed as a parallel audit layer rather than a transaction execution system, evaluation focuses on the incremental costs and the strength of tamper-evidence guarantees introduced by the audit mechanism. The analysis considers a permissioned ledger setting with Byzantine Fault Tolerant consensus, cryptographic hashing of transaction states, and signature-based record authenticity, consistent with secure audit log and timestamping principles commonly used in integrity-critical environments [5], [6], [7], and enterprise permissioned ledger deployments [15], [16], [17].

A. Audit Record Footprint and Storage Overhead

In the proposed design, the audit ledger stores cryptographic representations of transaction events rather than full transaction payloads. Each audit entry minimally contains a transaction identifier, a timestamp, a cryptographic hash of the transaction state, and a digital signature produced by the originating system. Under typical cryptographic primitives, the hash output is fixed-length and the signature size is bounded by the chosen signature scheme. Consequently, the size of each audit entry scales primarily with fixed metadata rather than transaction complexity, which directly limits ledger growth compared to approaches that store transactional data on-chain. This property is important for banking environments where transaction throughput is high and long-term retention is mandatory, aligning with established log management guidance emphasizing both integrity and manageable retention [29].

To quantify feasibility, consider a conservative audit entry size on the order of a few hundred bytes when including identifier fields, timestamps, hash outputs, and a signature. Even under high daily transaction volumes, the growth rate remains predictable and linear with event count, and does not amplify due to transaction payload replication. This suggests that the proposed audit layer can meet long-term storage requirements more effectively than full-data ledger approaches, while still enabling strong integrity verification through hash comparison.

10.48047/jocaaa.2021.29.01.21

B. Transaction-Path Latency Impact

A core design objective is to avoid introducing delay in the transaction execution path. In the proposed workflow, transaction execution is finalized within the core banking system before an audit event is generated and submitted to the ledger. As a result, the end-to-end transaction completion time perceived by banking applications remains governed by centralized system performance rather than distributed consensus latency. The audit write process becomes an asynchronous post-commit operation, and any ledger confirmation latency affects only the time-to-finality of the audit record, not the transaction itself.

This decoupling is an important practical advantage relative to ledger-based transaction execution models, which have been shown to face throughput and latency constraints at scale in decentralized settings [14]. The use of a permissioned ledger with BFT-style consensus further mitigates confirmation delay compared to public proof-of-work networks, making the audit commit process compatible with enterprise requirements while retaining tamper-evident guarantees [15], [17].

C. Tamper Detection Effectiveness

Integrity verification in the proposed framework relies on deterministic recomputation of the transaction hash from the centralized record and comparison against the ledger-stored hash. The effectiveness of this mechanism is evaluated through representative tampering scenarios relevant to banking audits.

In the first scenario, an insider modifies a transaction attribute such as a beneficiary identifier or amount in the centralized database after the transaction is executed. Because the ledger stores the cryptographic hash derived from the original transaction state, recomputing the hash from the modified record yields a mismatch, immediately exposing post-hoc manipulation. In the second scenario, an adversary attempts to delete a transaction record from the centralized system. While the centralized record may be missing, the corresponding immutable audit event remains preserved on the ledger, establishing evidence that a transaction previously existed and enabling discrepancy detection during reconciliation. In the third scenario, an adversary attempts to modify both centralized records and centralized logs to create consistency within the bank's internal infrastructure. In this case, the externalized ledger entry functions as an independent integrity anchor, preventing coordinated manipulation from remaining undetected, consistent with the motivation behind tamper-evident audit logs [5].

These scenarios demonstrate that the audit layer provides strong tamper evidence for unauthorized modifications, deletions, and coordinated manipulation attempts, while also supporting long-term verifiability through immutable record retention.

D. Scalability Considerations Under High Volume

Because the audit ledger is dedicated to audit events rather than executing full transaction logic, scalability constraints are primarily related to ledger write throughput and consensus confirmation. The framework reduces consensus burden by minimizing entry size and processing complexity, enabling higher event throughput compared to systems that embed transaction processing on the

10.48047/jocaaa.2021.29.01.21

ledger. In practice, permissioned ledger designs have been widely studied for improved enterprise scalability by restricting participants and employing efficient consensus protocols [15], [16]. Nevertheless, throughput remains a function of network size, fault tolerance configuration, and batching strategy.

A feasible scaling approach is to batch audit events generated over short time windows into ledger commits while maintaining per-transaction hash granularity. Batching reduces consensus frequency without losing integrity guarantees because each transaction still has an individual hash anchor stored immutably, and auditors can verify specific transactions by retrieving and validating the corresponding hash. This aligns with system engineering principles for log management and integrity verification in large-scale environments [29], while maintaining the core tamper-evidence objective.

E. Summary of Evaluation Outcomes

Overall, the evaluation indicates that the proposed decentralized audit trail can provide strong integrity guarantees with limited operational overhead by externalizing cryptographic transaction proofs to a permissioned distributed ledger. The architecture preserves transaction-path performance through asynchronous audit submission, supports effective tamper detection under realistic threat scenarios, and remains scalable by reducing ledger workload to compact audit events rather than full transaction processing. These results support the practical feasibility of selective decentralization for audit assurance in regulated banking environments.

VII. Conclusion and Future Work

This paper presented a decentralized audit trail framework aimed at enhancing transaction integrity in centralized banking systems. Recognizing the limitations of traditional centralized audit mechanisms, the proposed approach introduces a permissioned distributed ledger that operates as a parallel audit layer without interfering with transaction execution. By decoupling audit assurance from core banking operations, the framework provides immutable and independently verifiable audit records while preserving performance, confidentiality, and regulatory compliance.

The proposed methodology demonstrates how cryptographic representations of transaction events can be securely recorded on a decentralized ledger to ensure tamper-evident auditability. Unlike existing blockchain-based financial solutions that focus on transaction processing, this work emphasizes audit integrity as a distinct and critical problem domain. The design choices, including privacy-preserving audit records and regulator-aware participation, align the framework with practical deployment constraints in real-world banking environments.

Through systematic analysis, the paper shows that selective application of decentralized ledger technologies can significantly strengthen trust and accountability without requiring disruptive architectural changes. The discussion highlights how the proposed framework mitigates insider

10.48047/jocaaa.2021.29.01.21

threats, reduces reliance on centralized trust, and supports continuous audit verification, making it a viable enhancement for modern banking infrastructures.

Future work will focus on empirical evaluation of the proposed framework through prototype implementation and performance benchmarking under realistic transaction workloads. Additional research directions include exploring advanced privacy-enhancing techniques such as zero-knowledge proofs, refining governance models for multi-institution audit networks, and extending the framework to support cross-institutional audit interoperability. These extensions aim to further strengthen the role of decentralized audit trails in improving transparency, resilience, and trust in financial systems.

References

[1] J. W. Glover, *Auditing and Assurance Services*. New York, NY, USA: McGraw-Hill, 2016.
[2] A. A. Arens, R. J. Elder, and M. S. Beasley, *Auditing and Assurance Services*. Boston, MA, USA: Pearson, 2017.
[3] M. Bishop and C. Gates, "Defining the insider threat," in *Proc. ACM Workshop on Insider Threats*, 2008, pp. 1–6.
[4] R. Anderson, *Security Engineering*. Hoboken, NJ, USA: Wiley, 2020.
[5] B. Schneier and J. Kelsey, "Secure audit logs," *ACM Trans. Inf. Syst. Secur.*, vol. 2, no. 2, pp. 159–176, 1999.
[6] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.
[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.
[8] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, "Role-based access control," *IEEE Computer*, vol. 34, no. 9, pp. 33–40, 2001.
[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov. Rev.*, no. 2, pp. 6–10, 2016.
[11] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
[12] A. Gervais *et al.*, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2016, pp. 3–16.
[13] D. Tapscott and A. Tapscott, *Blockchain Revolution*. New York, NY, USA: Penguin, 2016.
[14] K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptography Data Security (FC)*, 2016, pp. 106–125.
[15] E. Androulaki *et al.*, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[16] C. Cachin, "Architecture of the Hyperledger blockchain fabric," in *Proc. Workshop Distributed Cryptocurrencies Consensus Protocols*, 2016, pp. 1–4.
[17] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.*, 2016, pp. 112–125.

10.48047/jocaaa.2021.29.01.21

[18] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," *Ledger*, vol. 4, pp. 1–39, 2019.
[19] W. Mougayar, *The Business Blockchain*. Hoboken, NJ, USA: Wiley, 2016.
[20] K. Dai, J. Wang, Y. Zhang, and S. Chen, "Blockchain-based audit trail for data integrity," *Future Gener. Comput. Syst.*, vol. 95, pp. 25–34, 2019.
[21] S. Wang *et al.*, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Access*, vol. 8, pp. 35457–35470, 2020.
[22] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, 2015, pp. 180–184.
[23] Y. Lindman, M. Rossi, and V. K. Tuunainen, "Privacy in blockchain systems," *Commun. ACM*, vol. 60, no. 11, pp. 20–22, 2017.
[24] J. A. Kroll, I. C. Davey, and E. W. Felten, "Accountable systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2007, pp. 1–12.
[25] A. Miller, M. Hicks, J. Katz, and E. Shi, "Authenticated data structures, generically," *Found. Trends Cryptography*, vol. 2, no. 2, pp. 87–160, 2014.
[26] F. Reid and M. Harrigan, "An analysis of anonymity in the Bitcoin system," *IEEE Security Privacy*, vol. 11, no. 3, pp. 28–35, 2013.
[27] Basel Committee on Banking Supervision, *Principles for Financial Market Infrastructures*. Basel, Switzerland: Bank for Int. Settlements, 2012.
[28] ISO/IEC 27001, *Information Technology Security Techniques Information Security Management Systems Requirements*. Geneva, Switzerland: ISO, 2013.
[29] NIST Special Publication 800-92, *Guide to Computer Security Log Management*. Gaithersburg, MD, USA: NIST, 2006.
[30] NIST Special Publication 800-184, *Guide for Cybersecurity Event Recovery*. Gaithersburg, MD, USA: NIST, 2016.