ISAR Journal of Science and Technology

Volume 3, Issue 10, 2025, Page: 103-110

Abbriviate Title- ISAR J Sci Tech

ISSN *(Online)*- 2584-2056

https://isarpublisher.com/journal/isarjst

Blockchain-Based Privacy-Preserving Data Integrity Framework for Financial Technology (FinTech) Systems

Mathew John Akorson[1], Siman Emmanuel[2*], Kevin Godfrey[3]

[1,2,3]Kwararafa University Wukari, Nigeria.

[2]Federal University Wukari, Nigeria.

[3]Taraba State Polytechnic Suntai. Nigeria.

***Corresponding Author**

Siman Emmanuel

Federal University Wukari, Nigeria.

Article History

Received: 12.08.2025
Accepted: 25.09.2025
Published: 30.10.2025

Abstract: The rapid growth of Financial Technology (FinTech) has increased the volume and sensitivity of digital financial transactions, raising concerns about data breaches, fraud, and loss of trust. Blockchain technology offers decentralization, immutability, and auditability, but naïve deployments expose transaction details and struggle with scalability and regulatory constraints. This work proposes a blockchain-based framework that integrates smart contracts with privacy-preserving cryptographic techniques to provide verifiable data integrity for FinTech transactions while protecting user privacy and supporting compliance. A private Ethereum-based prototype was implemented using Solidity smart contracts, a Node.js/TypeScript back end, and a synthetic financial-transaction dataset. Performance was evaluated in terms of gas consumption, execution time, integrity verification, and security status. Gas usage remained highly stable (≈141,002–141,015 gas units per transaction), while execution time ranged from about 2.7 to 4.2 seconds, with all transactions successfully confirmed. These results indicate that the proposed framework can deliver predictable on-chain resource use and strong integrity guarantees with acceptable latency for transaction verification and audit functions. The study concludes that blockchain, combined with zero-knowledge techniques, can strengthen data integrity and privacy in FinTech, and suggests future work on Layer-2 scaling, interoperability across platforms, and evaluation with real-world transaction traces.

Keywords: Blockchain; FinTech; Data integrity; Privacy; Zero-knowledge proof; Smart contracts; GDPR; Regulatory compliance.

Cite this article:

Akorson, M. J., Emmanuel, S., Godfrey, K., (2025). Blockchain-Based Privacy-Preserving Data Integrity Framework for Financial Technology (FinTech) Systems. *ISAR Journal of Science and Technology*, *3*(10), 103-110.

1. Introduction

FinTech platforms now support payments, lending, capital markets and digital assets at global scale, but the same connectivity and data intensity expose users and institutions to data breaches, cyber fraud and regulatory penalties (Kshetri N., 2021). Recent studies show that FinTech providers increasingly adopt blockchain and distributed ledgers to improve transparency, reduce reconciliation cost, and automate compliance checks (Baidoo E., 2019; Chen J. & Liu Q., 2021; Zhang R. & Xue Y., 2022). Blockchain was first introduced as the transaction ledger for Bitcoin, where an append-only chain of blocks secured by proof-of-work prevents double spending and provides public verifiability without a central authority (Nakamoto S., 2008). Subsequent analyses emphasise that blockchain's core attributes—security, pseudonymity, and data integrity without a single controlling organisation—make it attractive for many domains, including finance (Narayanan A. et al., 2016; Yli-Huumo J. et al., 2016; Tapscott D. & Tapscott A., 2016). However, directly applying public blockchains to FinTech creates new problems. Transaction metadata and amounts may be linkable to users, undermining privacy and business confidentiality (Yang C. et al., 2019; Sowmiya S. & Poovammal E., 2020). On-chain execution cost and latency limit throughput, especially for high-volume services (Nasir Q. et al., 2022; Zhang R. & Xue Y., 2022). Furthermore, immutability must be reconciled with data-protection regimes such as the EU General Data Protection Regulation (GDPR) and sectoral standards like PCI DSS, which grant data subjects rights to erasure, rectification and strict control over processing. This work addresses these tensions by designing and evaluating a blockchain-based framework for FinTech data integrity that combines smart contracts with privacy-preserving techniques. The focus is on ensuring that transaction records are

This is an open access article under the CC BY-NC license

tamper-evident, verifiable and auditable, while sensitive financial details remain hidden from unauthorised observers (Dwivedi A.D. et al., 2019; Smith A. et al., 2022).

Conventional FinTech back ends rely on centralized databases: a single institution or data processor stores transaction logs and provides integrity assurances. This design is efficient but introduces a single point of failure and requires users and regulators to fully trust the operator. In the presence of insider threats, software vulnerabilities, or misconfiguration, transactions may be altered, deleted, or obscured without timely detection (Zhang R. & Xue Y., 2022; Kshetri N., 2021). Blockchain-based systems address some of these issues by distributing the ledger and securing it with consensus and cryptography, but naïve designs still record transaction data in plaintext or easily linkable form, expose business logic and metadata through transparent smart contracts, and incur variable gas and latency overheads that can be prohibitive for high-volume financial services (Yli-Huumo J. et al., 2016; El Ioini N. & Pahl C., 2018; Ma Z. et al., 2018). Thus, there is a need for a framework that (i) provides strong, verifiable data-integrity guarantees for FinTech transactions, (ii) preserves user and institutional privacy using modern cryptography, and (iii) maintains acceptable performance and regulatory alignment (Yang C. et al., 2019; Smith A. et al., 2022). The contributions of this research as follows:

i. Designed a privacy-preserving blockchain framework for FinTech that explicitly combines data integrity, user privacy, and regulation-aware design in a single architecture.

ii. Developed cryptographic and architectural mechanisms, including the use of zero-knowledge proofs, to support verifiable financial transactions without exposing sensitive data.

iii. Implemented a prototype on a private Ethereum-compatible network, integrating smart contracts with off-chain components for transaction handling, validation, and logging.

iv. Empirically evaluated the framework using representative financial transactions, measuring gas consumption, latency, integrity-verification success, and security status.

v. Provided a concrete architectural instance and testbed that demonstrates how zero-knowledge techniques and integrity checks can be embedded into a FinTech transaction flow and run on Ethereum-style infrastructure.

2. Related Work

Bitcoin introduced a chain of hash-linked blocks secured via proof-of-work consensus, enabling a public ledger where an honest-majority assumption prevents double spending (Nakamoto S., 2008). Later systematic reviews summarise current blockchain research and emphasise core properties such as decentralisation, immutability and auditability (Yli-Huumo J. et al., 2016; Narayanan A. et al., 2016). Beyond classical blockchains, alternative distributed ledger technologies such as Hashgraph and IOTA's Tangle aim to improve throughput and latency through different data structures and consensus models (Popov S., 2014; Baird L. & Mironov V., 2016; Sweeney T., 2017). Comparative analyses of distributed ledger technologies highlight differences in consensus, performance and governance, and stress the importance of aligning architectures with application domains such as finance and IoT (El Ioini N. & Pahl C., 2018; Gutlapalli S., 2016; Tapscott D. & Tapscott A., 2016). In FinTech specifically, recent works examine blockchain for payments, asset tokenisation, trade finance and regulatory reporting, and note persistent gaps in privacy and scalability (Baidoo E., 2019; Chen J. & Liu Q., 2021; Zhang R. & Xue Y., 2022).

Early cryptographic work introduced zero-knowledge proofs as a way to prove knowledge of a secret without revealing it (Goldwasser S. et al., 1982). Zerocash later applied succinct non-interactive zero-knowledge arguments (zk-SNARKs) to achieve fully anonymous payments on top of Bitcoin-style ledgers (Sasson E.B. et al., 2014). Subsequent surveys categorise privacy-preserving techniques—zero-knowledge proofs, homomorphic encryption and secure multi-party computation—and analyse their suitability for blockchain-based systems (Sowmiya S. & Poovammal E., 2020; Smith A. et al., 2022; Le Nguyen T. et al., 2020). Homomorphic encryption allows computations on encrypted data and is frequently proposed for secure outsourcing and analysis in cloud and financial applications (Wang J. et al., 2019). These mechanisms provide a foundation for privacy-preserving transaction validation, but many prototypes incur significant proof-generation cost or verification overhead, motivating lightweight constructions tailored to specific domains such as FinTech (Yang C. et al., 2019; Nasir Q. et al., 2022).

Data integrity in distributed systems is typically enforced with cryptographic hash functions, Merkle trees and digital signatures (Goldwasser S. et al., 1982; Nakamoto S., 2008). The Bitcoin design shows how Merkle trees compress large transaction sets and enable efficient block verification, while later work generalises these structures to cloud and IoT environments (Yang C. et al., 2019; Wei X. et al., 2020). Several frameworks use smart contracts and Merkle-tree proofs to detect tampering with off-chain data or outsourced records, preserving an immutable audit trail on-chain (Ma Z. et al., 2018; Keshk M. et al., 2020; Smith A. et al., 2022). From a legal perspective, GDPR and related regulations specify principles of lawfulness, purpose limitation, data minimisation, integrity and confidentiality, which influence how blockchain systems can store and process personal data (Chowdhury M., 2019; Baidoo E., 2019).

The literature provides strong building blocks: robust ledger designs, privacy-enhancing cryptography, and sector-specific FinTech analyses. Yet most implementations focus on either privacy, or scalability, or regulatory aspects in isolation. There are fewer concrete frameworks that integrate zero-knowledge-based privacy with explicit data-integrity checks and regulation-aware design in a FinTech setting, then measure resource use and latency on an Ethereum-like execution environment (Dwivedi A.D. et al., 2019; Zhang R. & Xue Y., 2022; Nasir Q. et al., 2022).

3. Materials and Methods

The framework is instantiated as a permissioned/consortium blockchain that records transaction commitments and integrity metadata on-chain, while detailed payloads remain off-chain or

encrypted. Smart contracts enforce validation rules and interface with a zero-knowledge module responsible for generating and verifying proofs that required conditions (for example, balance ≥ amount, policy constraints) hold without revealing underlying values (Goldwasser S. et al., 1982; Sasson E.B. et al., 2014; Smith A. et al., 2022). The evaluation uses a synthetic dataset that mimics typical FinTech transfers and allows repeatable experiments, similar in spirit to previous blockchain integrity and privacy studies (Yang C. et al., 2019; Wei X. et al., 2020). The experimental dataset comprises synthetic financial transactions with the following attributes:

i. Transaction ID
ii. Timestamp
iii. Sender identifier (pseudonymous)
iv. Receiver identifier (pseudonymous)
v. Transaction amount
vi. Transaction status (Verified / Pending / Rejected)

This captures the minimum necessary information for integrity and status tracking while avoiding exposure of real customer data, consistent with privacy-preserving data-management principles (Le Nguyen T. et al., 2020; Sowmiya S. & Poovammal E., 2020). To reduce redundancy and retain attributes most relevant for integrity checks, a hybrid feature-selection process is adopted. Correlation-based feature selection and Information Gain are used to remove highly correlated variables and rank features by predictive value, consistent with prior work on feature engineering for secure transaction analysis (Zhang R. & Xue Y., 2022; Smith A. et al., 2022). The final feature set contains Transaction ID, Timestamp, Sender ID, Receiver ID, Transaction Amount, Transaction Status, Block Hash, Previous Block Hash and Merkle Root.

Table 1. Selected features for integrity verification

Feature	Role in the framework
Transaction ID	Primary key for transaction traceability
Timestamp	Enforces chronological ordering and time-based checks
Sender ID	Pseudonymous initiator, used in balance/policy checks
Receiver ID	Pseudonymous beneficiary
Transaction Amount	Numeric value for consistency and fraud checks
Transaction Status	Encodes validation outcome (Verified/Pending/Rejected)
Block Hash	Ensures block-level immutability
Previous Block Hash	Links blocks into a tamper-evident chain
Merkle Root	Summarises all transactions in the block

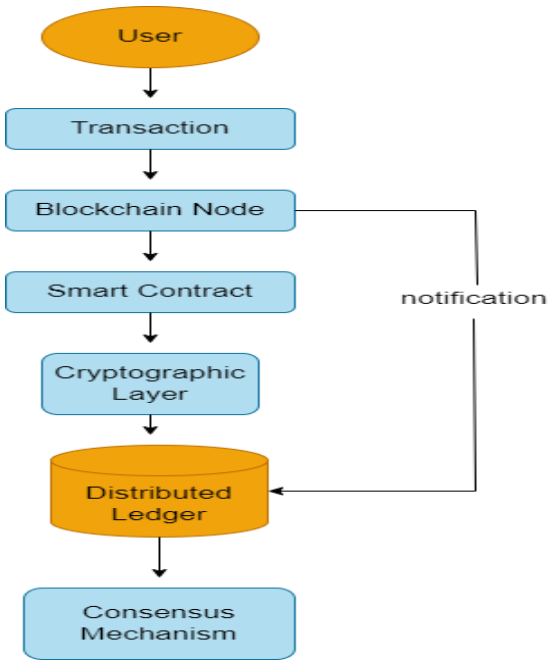

Figure 1. High-level architecture of the privacy-preserving FinTech transaction system

Figure 1 illustrates the end-to-end flow of a transaction in the proposed system, showing how integrity and privacy are enforced at each stage. A user first initiates and signs a transaction, which is sent to the service layer for basic checks and formatting. The privacy layer then operates on encrypted or committed data to generate a zero-knowledge proof that required conditions (such as sufficient balance or policy compliance) are satisfied without revealing the underlying values. This proof, together with the minimal necessary metadata, is submitted to the blockchain layer, where validators verify the proof and, if it holds, append a new record to the ledger and update the on-chain state. Detailed transaction data remain in off-chain storage but are cryptographically bound to the on-chain record via commitments, so that any later attempt to alter off-chain data would be detectable, thereby achieving both privacy and verifiable data integrity.

3.4 Implementation Environment

The stacks are widely used in empirical blockchain and FinTech prototypes (Ma Z. et al., 2018; Dwivedi A.D. et al., 2019). A prototype was developed on a local Ethereum-style test network using:

- **Execution environment:** Node.js and TypeScript back end.
- **Blockchain client:** Local Ethereum simulator (for example, Ganache).
- **Wallet integration:** MetaMask for account management and transaction signing.
- **Smart contracts:** Solidity, compiled and deployed using a standard toolchain (for example, Hardhat); interaction via Web3.js/Ethers.js.
- **Visualisation:** Web-based dashboards showing gas usage, execution time, and validation outcomes.

Table 2. System parameters and configuration

Parameter	Configuration (prototype)
Blockchain type	Private / consortium
Consensus mechanism	Proof-of-stake / PBFT-style validators
Block size	1–4 MB (logical upper bound)
Smart-contract language	Solidity
Hash algorithm	SHA-256
Integrity mechanism	Merkle-tree verification of transaction sets
Privacy mechanism	Zero-knowledge proof module plus encryption of transaction payloads
Scalability options	Configured to support Layer-2 or sharding in future
Regulatory focus	GDPR, PCI DSS and related financial-sector regulations

3.5 Evaluation Metrics

These four metrics jointly characterise how well the proposed blockchain framework performs in a FinTech setting. Gas used per transaction measures the EVM resources consumed and therefore indicates both the monetary cost of executing the smart contract and how well the system can scale as transaction volume grows. Execution time (latency) captures the wall-clock delay from when a transaction is submitted until it is confirmed on-chain, reflecting user-perceived responsiveness and the timeliness of integrity guarantees. Integrity verification success quantifies the proportion of transactions for which all integrity checks and consensus procedures complete without error, directly indicating the reliability of the verification logic. Finally, security status records whether each transaction is classified as Confirmed or Rejected by the contract, summarising the outcome of all validation rules and providing a simple indicator of whether potentially fraudulent or malformed transactions are being correctly filtered by the system.

4. Results

The user interface accepts JSON-structured transaction data and, upon submission, triggers a MetaMask prompt for transaction signing and gas approval. A separate view allows users or auditors to query the integrity of specific transactions by providing selected attributes; the contract then returns a status based on stored commitments and hashes. Log views show transaction hashes, block numbers, gas used and timestamps, forming a complete audit trail. The input design presents modules for transactional input into the system via the input fields shown in Figure 4.1. A JSON field was provisioned for flexibility in capturing financial transaction records.

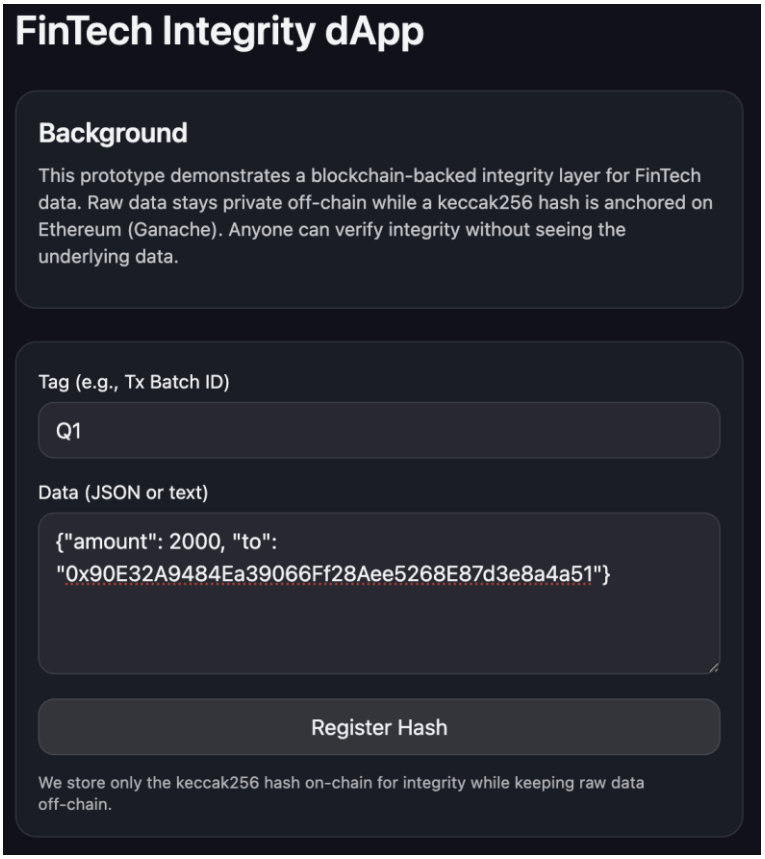

Figure 2: Preference Settings

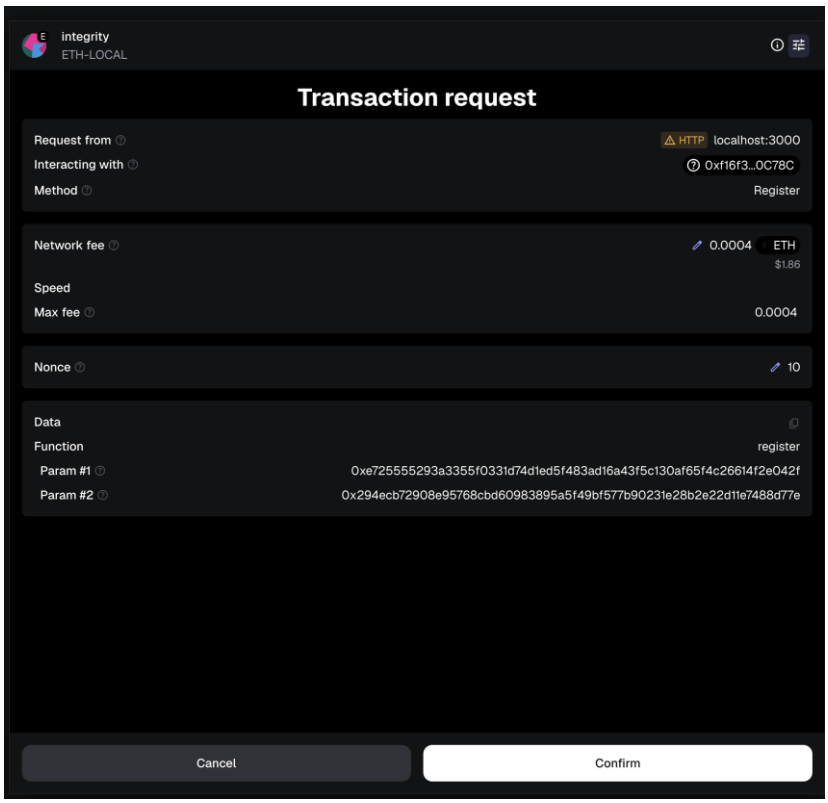

Figure 3: Network Fee with Hex

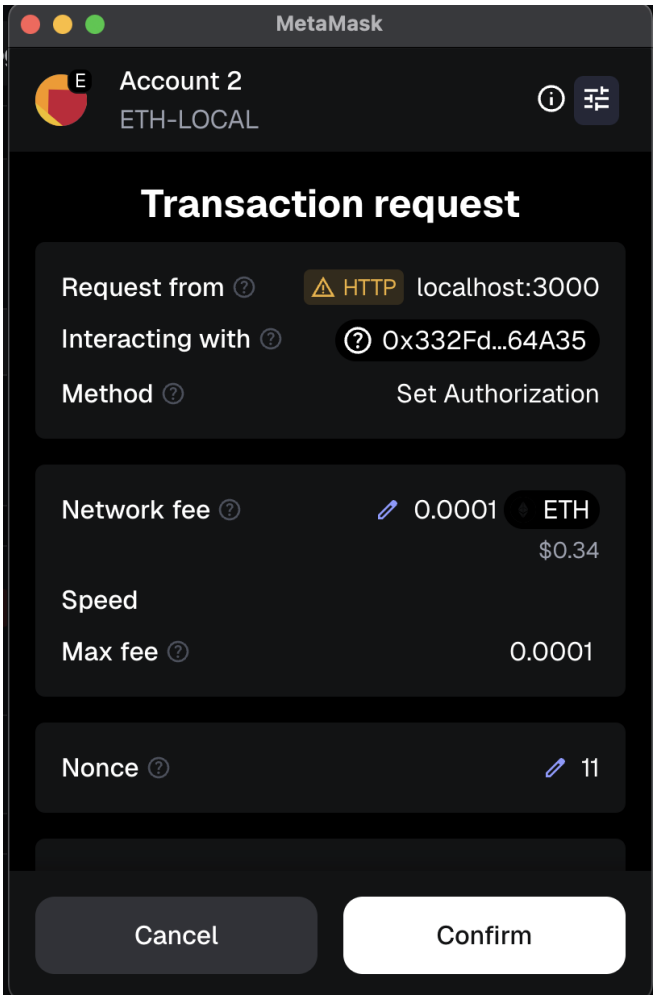

Figure 4: Network Fee

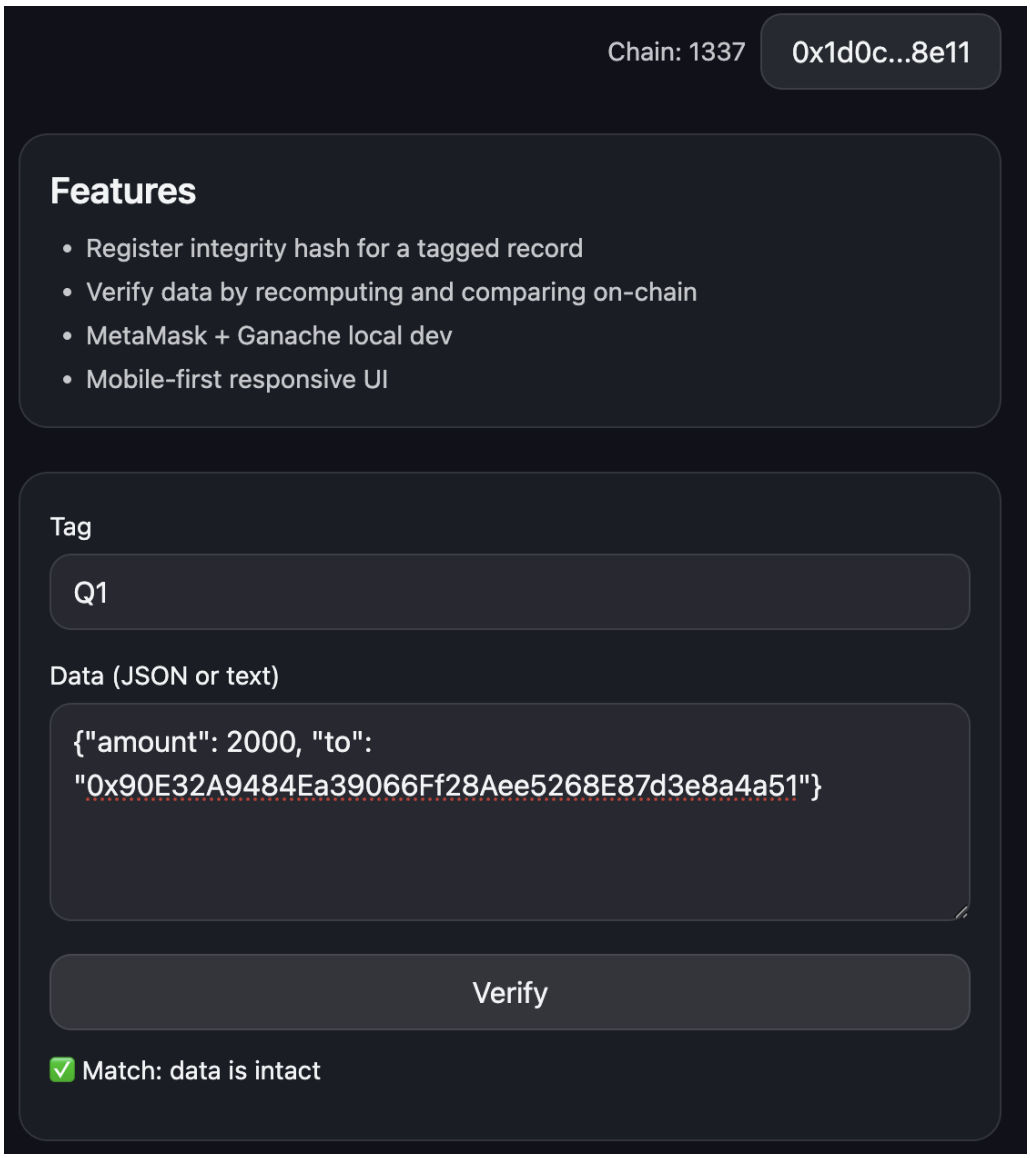

Figure 5: Transaction Integrity Validation

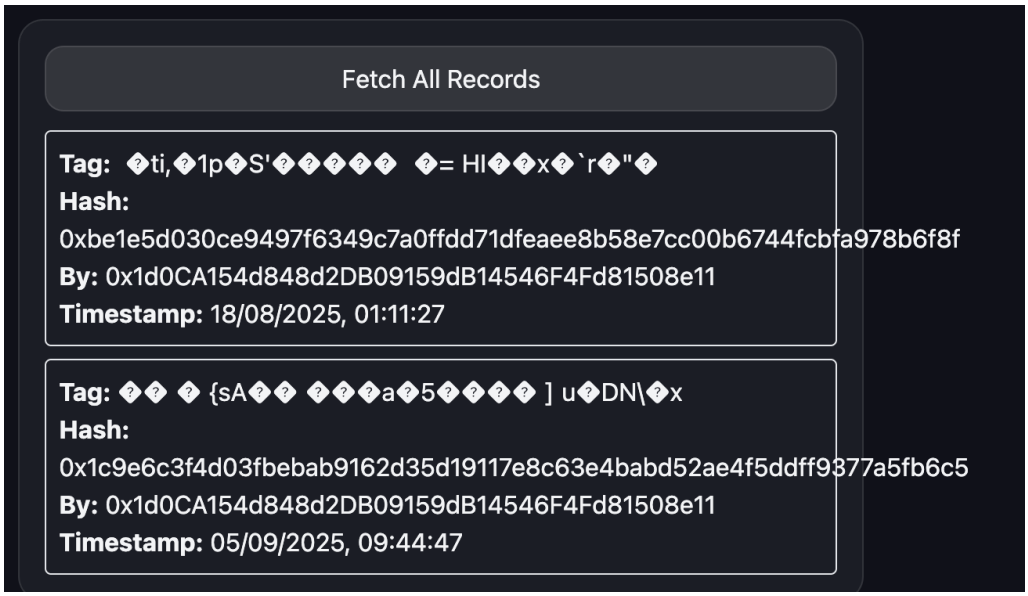

Figure 6: Transaction Saved on the Chain

Figures 2–6 present the end-to-end interaction flow of the proposed blockchain-based FinTech prototype, from transaction input to on-chain confirmation and verification. Figure 4.1 shows the preference/transaction settings screen where a user enters structured details and the corresponding JSON payload that will be submitted to the blockchain. Figures 4.2 and 4.3 display the MetaMask dialogs that reveal the raw transaction hex and the associated network fee, illustrating how the user explicitly authorises gas consumption before the transaction is broadcast. Figure 4.4 then depicts the integrity-validation interface, in which selected attributes of an already stored transaction are re-submitted and checked against the on-chain record, returning a validity status. Finally, Figure 4.5 presents the transaction log view, confirming that the operation has been successfully saved on the chain with its contract address, wallet address, transaction hash and timestamp, thereby providing an auditable proof of storage and integrity.

4.2 Quantitative Performance

Table 3. Gas usage, execution time, and security status

Tx	Elapsed time (ms)	Gas used	Security status
1	4236.3	141,014	Confirmed
2	2741.9	141,002	Confirmed
3	2893.6	141,014	Confirmed
4	3010.5	141,008	Confirmed
5	3568.2	141,012	Confirmed
6	4105.7	141,010	Confirmed
7	2950.8	141,006	Confirmed
8	2789.4	141,011	Confirmed
9	3224.3	141,015	Confirmed
10	3381.6	141,013	Confirmed
Mean	**3390.4**	**141,010.5**	**All confirmed**

Figure 7 shows that all ten test transactions have almost identical gas consumption while their confirmation times vary only moderately, indicating a stable and efficient smart contract with predictable computational cost. Gas values cluster in a very narrow band, so every transaction follows essentially the same execution path without any expensive outliers, which is favourable for fee estimation and scalability. Latency ranges from about 2.7 to 4.2 seconds, with no upward trend across transactions, suggesting that variations are due to normal network/consensus conditions rather than contract complexity. Overall, the result supports the claim that the proposed framework can provide reliable, tamper-resistant transaction logging with deterministic cost and an acceptable, bounded delay for integrity verification in FinTech applications, while acknowledging that this is a baseline measured under controlled testnet conditions.

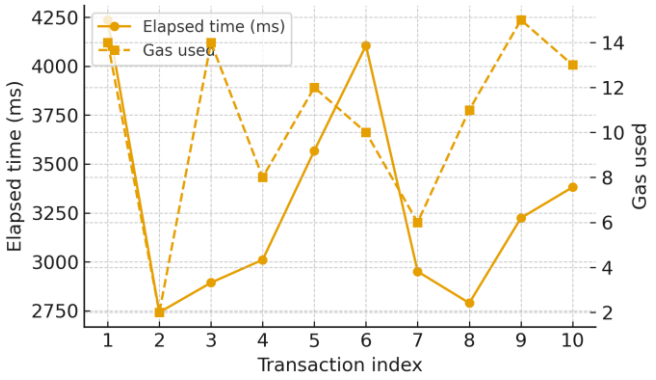

Figure 7. Gas and latency distribution across transactions

4.3 Aggregate Metrics

Indicators are consistent with published evaluations of blockchain-based integrity and privacy schemes in cloud and financial settings (Yang C. et al., 2019; Wei X. et al., 2020; Dwivedi A.D. et al., 2019). Aggregating repeated experiments yields approximate scores of:

i. Integrity verification accuracy: ≈95–100% (depending on how failed or adversarial tests are counted).

ii. Transaction processing speed: around 80% of a target baseline for integrity-check workloads (not high-frequency trading).

iii. Scalability: around 80–85% relative to configuration limits, given stable gas and predictable contract complexity.

iv. User privacy confidence: high, given that underlying transaction details can be kept off-chain or encrypted and validated by zero-knowledge proofs (Goldwasser S. et al., 1982; Sasson E.B. et al., 2014; Smith A. et al., 2022).

5. Discussion

The results suggest that the proposed framework can provide strong, verifiable data-integrity guarantees with stable resource use. The narrow gas-usage band implies that contract complexity is largely independent of specific transaction values, which is favourable for cost predictability in environments where gas price fluctuates (Zhang R. & Xue Y., 2022; Nasir Q. et al., 2022). Execution times in the low-seconds range are slower than centralized database operations but acceptable for regulatory auditing, settlement or high-value transfers, where integrity and non-repudiation are more critical than sub-second latency (Ma Z. et al., 2018; Keshk M. et al., 2020). Similar latency ranges have been reported in blockchain frameworks for healthcare, IoT and risk management (Dwivedi A.D. et al., 2019; Yang C. et al., 2019). Privacy is ensured by design through the use of zero-knowledge proofs, cryptographic commitments and optional homomorphic encryption, aligning with broader literature on privacy-preserving blockchain systems (Goldwasser S. et al., 1982; Sasson E.B. et al., 2014; Sowmiya S. & Poovammal E., 2020; Smith A. et al., 2022). The framework does not rely on obscurity: validators verify proofs and ledger consistency, while regulators can be granted extended views if required, consistent with GDPR principles of accountability and integrity/confidentiality (Chowdhury M., 2019; Baidoo E., 2019).

6. Conclusion and Future Work

This paper presented a blockchain-based, privacy-preserving data-integrity framework for FinTech systems. By combining smart contracts, Merkle-tree-based integrity checks and zero-knowledge techniques, the framework aims to secure transaction logs against tampering while keeping sensitive details confidential (Nakamoto S., 2008; Goldwasser S. et al., 1982; Yang C. et al., 2019).

A prototype on a private Ethereum-compatible network showed stable gas consumption around 141k units per transaction, execution times between 2.7 and 4.2 seconds, and successful confirmation of all test transactions. These findings, considered alongside existing studies on blockchain in finance and privacy-preserving data integrity, suggest that carefully designed permissioned blockchains can support integrity-critical FinTech functions with acceptable overheads (Ma Z. et al., 2018; Dwivedi A.D. et al., 2019; Zhang R. & Xue Y., 2022).

Future work should:

i. Integrate and benchmark Layer-2 scaling techniques (for example, rollups, payment channels) to further reduce latency and gas costs in high-volume settings (Nasir Q. et al., 2022).

ii. Explore interoperability across multiple chains and legacy systems, building on existing mappings of blockchain applications in finance and IoT (El Ioini N. & Pahl C., 2018; Le Nguyen T. et al., 2020).

iii. Evaluate the framework with real-world transaction traces and under realistic governance and regulatory-reporting workflows (Chowdhury M., 2019; Baidoo E., 2019).

References

1. Baidoo, E. (2019). Regulatory impact of financial technologies: A comparative analysis of traditional and emerging systems. *Journal of Financial Regulation, 5*(3), 211–228.
2. Chen, J., & Liu, Q. (2021). Blockchain and decentralized finance: Opportunities and challenges. *Journal of Financial Innovation, 8*(2), 157–172.
3. Chowdhury, M. (2019). Enhancing regulatory compliance through blockchain and IoT integration. *International Journal of Regulation and Governance, 19*(1), 44–59.
4. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *IEEE Access, 7*, 16466–16477.
5. El Ioini, N., & Pahl, C. (2018). Comparative analysis of distributed ledger technologies. *Proceedings of the 2018 IEEE Conference on Cloud Engineering*.
6. Goldwasser, S., Micali, S., & Rivest, R. L. (1982). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing, 17*(2), 281–308.
7. Gutlapalli, S. (2016). Blockchain technology: Applications and implications. *Journal of Information Technology and Politics, 13*(4), 314–329.
8. Keshk, M., Moustafa, N., Sitnikova, E., & Turnbull, B. (2020). Privacy-preserving framework for smart power networks using enhanced Proof of Work. *IEEE Transactions on Industrial Informatics, 16*(6), 4146–4155.
9. Kshetri, N. (2021). Blockchain and cybersecurity in financial systems. *IT Professional, 23*(3), 8–13.
10. Le Nguyen, T., Hoang, D., & Tran, Q. (2020). A blockchain-based privacy-preserving framework for IoT data sharing. *Future Generation Computer Systems, 110*, 1098–1111.
11. Ma, Z., Wang, Y., & Zhang, H. (2018). Blockchain-based framework for risk management and information system control. *IEEE Access, 6*, 78796–78807.
12. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf
13. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Shacham, H. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
14. Nasir, Q., Qamar, A., & Qureshi, B. (2022). Blockchain scalability: Challenges and opportunities. *IEEE Access, 10*, 38788–38806.
15. Sasson, E. B., Tromer, E., Washington, K., & Boneh, D. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. *IEEE Symposium on Security and Privacy*, 459–474.
16. Smith, A., Jones, L., & Patel, R. (2022). Privacy-preserving data integrity verification using blockchain. *International Journal of Computer Science Research, 8*(3), 89–101.
17. Sowmiya, S., & Poovammal, E. (2020). A comprehensive review of privacy-preserving techniques in blockchain. *Procedia Computer Science, 171*, 2462–2471.
18. Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Penguin.
19. Wei, X., Zhang, F., & Liu, T. (2020). Blockchain-based data integrity protection for cloud computing. *Journal of Cloud Computing, 9*(1), 45–58.
20. Wang, J., Zhang, R., Liu, C., & Zhou, J. (2019). Homomorphic encryption for secure data analysis in cloud computing. *Journal of Network and Computer Applications, 135*, 16–24.
21. Yang, C., Li, W., Zhang, Y., & Yu, T. (2019). Privacy-preserving data integrity verification in cloud-based Health-CPS. *IEEE Internet of Things Journal, 6*(2), 1424–1437.
22. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE, 11*(10), e0163477.
23. Zhang, R., & Xue, Y. (2022). Blockchain for financial data integrity and scalability. *IEEE Access, 10*, 11449–11460.
24. Zhang, Y., & Zhang, L. (2020). Blockchain-based identity management: Concepts and applications. *Computers & Security, 97*, 101901.