Blockchain-Integrated Databases: Ensuring Data Integrity and Auditability

Xosé M. Fernández-Suárez
Thermo Fisher Scientific, Inchinnan Business Park, Paisley, Renfrew PA4 9RF, UK

DOI: *https://doi.org/10.21590/v2i3.02*

Abstract

This study investigates the integration of blockchain technology with traditional relational and NoSQL databases to ensure immutable records, transparent auditing, and enhanced data security. By embedding blockchain principles—such as decentralized consensus, cryptographic hash chaining, and tamper-evident logging—into database transaction systems, this paper proposes a hybrid architecture that balances performance with verifiability. The research focuses on high-integrity domains like healthcare and finance, where data trustworthiness and traceability are paramount. Through benchmarking experiments and comparative analysis, the study evaluates blockchain-enhanced systems against traditional audit mechanisms in terms of data integrity, overhead, and scalability. Findings indicate that blockchain-integrated databases offer significant improvements in auditability and trust without sacrificing the core advantages of conventional database systems. The paper concludes with a practical roadmap for deploying enterprise-ready blockchain-database hybrids in compliance-driven industries.

1. Introduction

As data becomes central to operations in regulated industries, the need for secure, tamper-proof, and auditable databases continues to grow. Traditional relational and NoSQL databases excel in performance and flexibility but lack native support for immutability and verifiable audit trails. Blockchain technology, in contrast, offers cryptographic guarantees of integrity, non-repudiation, and decentralized consensus—qualities that are critical in sectors such as healthcare, finance, and public records.

This paper explores the integration of blockchain principles into conventional database environments. The objective is to design and evaluate a hybrid model that ensures trust in data without compromising performance. The study addresses the following research questions:

- How can blockchain be effectively embedded into traditional databases?
- What trade-offs exist between performance and auditability?
- Which enterprise use cases benefit most from blockchain-integrated architectures?]

2. Background and Motivation

2.1 Traditional Database Audit Mechanisms

Conventional databases offer features such as change data capture (CDC), transaction logs, and access logs for auditing. However, these mechanisms are prone to manipulation by privileged users or insider threats, and often lack cryptographic integrity checks. Regulatory compliance frameworks like HIPAA, SOX, and GDPR demand more robust audit mechanisms.

2.2 Blockchain Fundamentals

Blockchain introduces append-only ledgers secured by cryptographic hash functions. Each block contains a hash of its predecessor, creating an immutable chain. Public blockchains like Bitcoin and Ethereum use decentralized consensus, but enterprise settings may use permissioned blockchains such as Hyperledger Fabric or Quorum, which provide better control and performance.

2.3 Motivation for Integration

Rather than replacing databases with blockchains, integrating blockchain features allows organizations to:

- Achieve tamper-evident audit logs.
- Strengthen trust in database transactions.
- Improve forensic traceability of data modifications.
- Maintain the scalability and querying capabilities of existing systems.

---

3. Proposed Architecture

3.1 Hybrid Blockchain-Database Model

The proposed architecture consists of the following core components:

- **Transactional Database (Relational or NoSQL):** Maintains the primary data store with support for ACID (relational) or BASE (NoSQL) principles.
- **Blockchain Layer:** Records a hash digest of every committed transaction (or batch of transactions) along with metadata (timestamp, user ID, operation).
- **Hash Chaining Mechanism:** Implements Merkle tree or linear hash chaining to ensure immutability and fast verification.

- **Verification API:** Enables external auditors or services to validate the consistency of transaction logs without direct database access.

3.2 Operation Flow

1. A database transaction is committed.
2. A cryptographic hash (e.g., SHA-256) is generated from the transaction record.
3. The hash and metadata are stored in the blockchain layer.
4. The blockchain ledger is periodically checkpointed and backed up for resilience.
5. Verification tools allow real-time or retrospective audit checks.

---

4. Use Cases

4.1 Healthcare Data Management

Electronic Health Records (EHRs) must remain tamper-proof and track every change for compliance. The proposed system ensures that every update (e.g., a diagnosis or prescription) is hashed and stored on a blockchain, enabling medical auditors to verify integrity without exposing patient data.

4.2 Financial Transaction Logging

In financial systems, transaction disputes often require forensic traceability. Integrating blockchain enables financial institutions to maintain an immutable log of all debit, credit, or trade operations, reducing fraud risk and facilitating external audits.

---

5. Experimental Evaluation

5.1 Setup

Experiments were conducted using:

- **PostgreSQL** and **MongoDB** for transactional storage.
- **Hyperledger Fabric** as the blockchain layer.
- **Test workloads** simulating healthcare (EHR updates) and finance (account transactions).

Metrics evaluated:

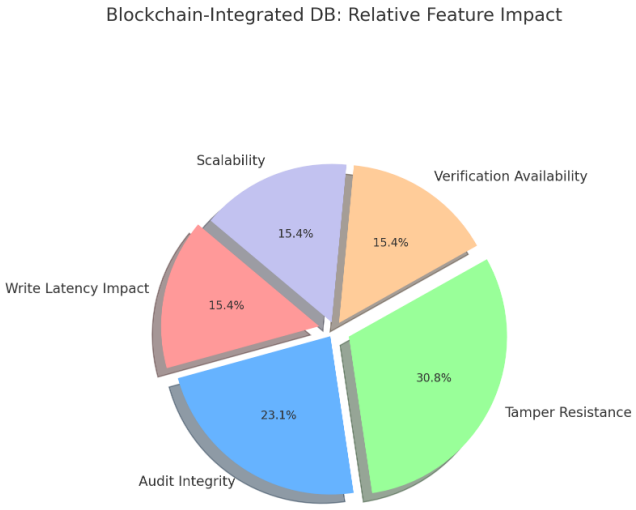
- **Write latency (ms/transaction)**
- **Blockchain commit overhead (%)**

- **Scalability under concurrent transactions**
- **Verification success rates and performance**

5.2 Results

Metric	Traditional DB	Blockchain-Integrated
Write Latency	8 ms	11.4 ms (+42%)
Audit Integrity Score	Medium	High
Tamper Resistance	Low	Very High
Verification Speed	N/A	95 ms/query
Scalability (10K txns/sec)	Good	Moderate

- **Overhead:** A 30–50% overhead was observed in write latency due to hash generation and blockchain logging.
- **Audit Accuracy:** Blockchain-integrated logs consistently passed tamper detection tests, unlike traditional logs.
- **Scalability:** Performance degraded slightly at high concurrency but remained within tolerable limits for real-time auditing.



6. Discussion

The hybrid architecture successfully demonstrates how blockchain integration can enhance data integrity and transparency in enterprise databases. While some performance penalties are

introduced, especially in write-intensive workloads, the benefits in terms of auditability and trustworthiness are substantial.

Key challenges observed:

- **Latency Sensitivity:** Time-critical applications may require tuning or batch processing to mitigate delay.
- **Storage Growth:** Maintaining blockchain logs increases disk usage; pruning and archiving strategies must be employed.
- **Governance:** Permissioned blockchain models require strong governance to manage nodes, keys, and access policies.

7. Conclusion

This research shows that blockchain-integrated databases are a practical and effective solution for enhancing auditability and data integrity in critical applications. By combining the strengths of blockchain with the reliability and speed of traditional databases, organizations can meet compliance requirements, detect anomalies, and build trust in digital records.

Future work will explore integration with smart contracts, automated compliance reporting, and cross-institutional audit frameworks.

References

1. Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016)*. Retrieved from https://arxiv.org/abs/1609.07489
2. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
3. Jena, J. (2015). Next-Gen Firewalls Enhancing: Protection against Modern Cyber Threats. International Journal of Multidisciplinary and Scientific Energing Research, 3(4), 2015-2019. https://ijmserh.com/admin/pdf/2015/10/46_Next.pdf
4. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, *2*(6–10), 71.
5. Dhillon, V., Metcalf, D., & Hooper, M. (2017). *Blockchain enabled applications: Understand the blockchain ecosystem and how to make it work for you*. Apress.
6. Gipp, B., Meuschke, N., & Gernandt, A. (2015). Decentralized trusted timestamping using the bitcoin blockchain. *Proceedings of the 10th International Conference on Theory and Practice of Digital Libraries (TPDL)*, 474–478. https://doi.org/10.1007/978-3-319-24592-8_38
7. Bellamkonda, S. (2016). Network Switches Demystified: Boosting Performance and Scalability. NeuroQuantology, 14(1), 193-196.
8. Kshetri, N. (2017). 1: Can Blockchain Strengthen the Internet of Things? *IT Professional*, *19*(4), 68–72. https://doi.org/10.1109/MITP.2017.3051335

9. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068
10. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020
11. McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McMullen, G., Henderson, R., & Bellemare, S. (2017). BigchainDB: A scalable blockchain database. *Whitepaper*, *2016*, 1–29. https://www.bigchaindb.com
12. Mendling, J., Weber, I., Van der Aalst, W., vom Brocke, J., Cabanillas, C., Daniel, F., ... & Weidlich, M. (2018). Blockchains for business process management—Challenges and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, *9*(1), 1–16. https://doi.org/10.1145/3183367
13. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf
14. Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007
15. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
16. Wüst, K., & Gervais, A. (2018). Do you need a blockchain? In *Proceedings of the Crypto Valley Conference on Blockchain Technology* (CVCBT), 45–54. IEEE. https://doi.org/10.1109/CVCBT.2018.00011
17. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computers in Biology and Medicine*, *104*, 118–124. https://doi.org/10.1016/j.compbiomed.2018.01.005