International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
SJIF (2024): 6.623

Blockchain for Secure Digital Payments - Preventing Payment Fraud

Yadiki Bhavashya Chandra

Department of Computer Science & Engineering, Nitte Meenakshi Institute of Technology, Bangalore-560019, Karnataka, India

Abstract: ***Digital payments have grown exponentially but face risks such as fraud, account takeover, and unauthorized transactions. This paper explores how blockchain technology, with its decentralized ledger, cryptographic integrity, and smart contracts, can secure digital payments and prevent fraud. We propose a permissioned blockchain architecture for payment systems, integrating identity management, escrow-based smart contracts, and audit-ready transaction logs. Illustrative simulations compare fraud-risk indices, transaction confirmation time, and per-transaction cost across traditional payment gateways and blockchain systems. The results indicate that blockchain can reduce fraud exposure while maintaining near real-time settlement. Challenges such as scalability, privacy, and regulatory compliance are also discussed. This study highlights blockchain's potential as a preventive, secure mechanism for digital payments and sets the stage for future research integrating zero-knowledge proofs and federated learning.***

Keywords: Blockchain, Digital Payments, Fraud Prevention, Smart Contracts, Payment Security

1. Introduction

- The rapid growth of digital payments globally and in India has increased both convenience and the risk of fraud.
- Common fraud types include phishing, double spending, fake refunds, and chargebacks.
- Traditional payment systems rely on post-transaction review, which is often reactive.
- Blockchain provides immutable ledgers, decentralized validation, and smart contracts, enabling proactive fraud prevention.

2. Literature Survey

- Prior research explores blockchain in financial systems, emphasizing secure, auditable transactions.
- Public blockchains (Ethereum, Bitcoin) provide openness but may face scalability and privacy issues.
- Permissioned blockchains (Hyperledger Fabric) are more suitable for banking/payment networks due to controlled access and fast consensus.
- Existing studies show blockchain reduces fraud but have gaps in integrating with real-time digital payment systems.

3. Problem Definition

- Digital payment systems are vulnerable to various frauds.
- Traditional systems rely on reactive fraud detection.
- Objective: Design a blockchain-based payment system that prevents fraud proactively while maintaining efficiency and compliance.

4. Methodology / Approach

Proposed Permissioned Blockchain Architecture:

1. **Identity Management (MSP/DID):** Ensures verified user and merchant identities.
2. **Payment Gateway Layer:** Interfaces with apps/merchants, collects signatures, applies device binding.
3. **Consensus / Orderers (BFT):** Provides deterministic finality for transactions.
4. **Smart Contracts:**
   - Escrow & automatic release upon delivery verification
   - Refunds/chargeback management
   - Spend control/velocity limits
5. **Private Channels & Off-chain Analytics:** Protect sensitive data; compute risk scores off-chain.
6. **Regulatory/Audit Node:** Provides read-only access for compliance.

Transaction Flow:

User initiates payment → smart contract verification → block confirmation → ledger update → receipt issued.

Table 1: Fraud Types vs Blockchain Controls

Fraud Type	Typical Attack	Blockchain/Smart-Contract Countermeasure
Double Spending	Replay or ledger rewrite	Immutable ledger; BFT consensus
Account Takeover	Stolen credentials	Device binding, multi-signature
Merchant Collusion	Fake refunds	Escrow, multi-party approval, audit trails
Friendly Fraud	Disputed transactions	On-chain evidence, programmable dispute
MITM / Relay Attack	Transaction tampering	End-to-end signatures, encrypted channels

Illustrative Simulation Metrics:

- Fraud-Risk Index (0–100)
- Median Transaction Confirmation Time (s)
- Cost per Transaction (USD cents)

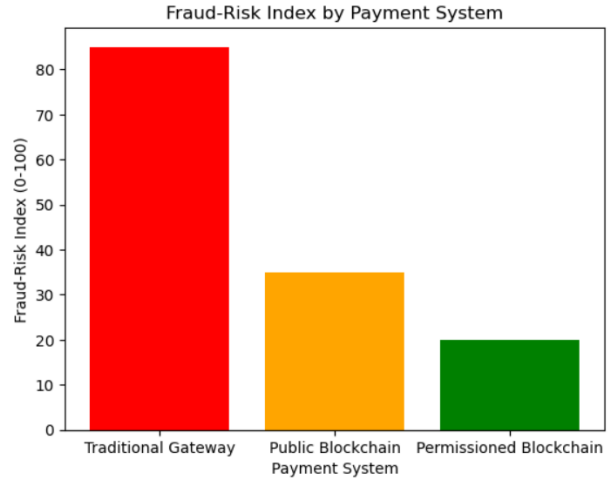

Figure 1: Fraud-Risk Index

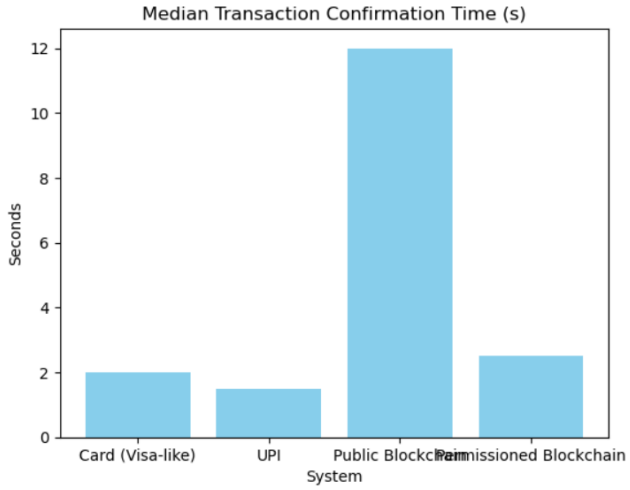

Figure 2: Confirmation Time

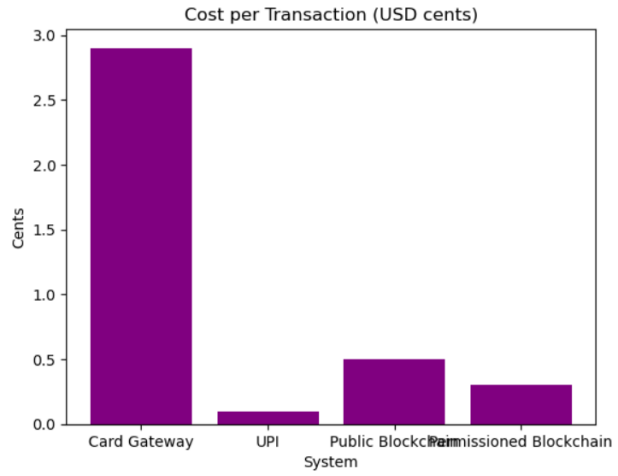

Figure 3: Cost per Transaction

5. Results & Discussion

- Fraud-risk index: Traditional 85, Public Blockchain 35, Permissioned Blockchain 20
- Median confirmation time: Card ~2s, UPI ~1.5s, Public Blockchain 12s, Permissioned Blockchain 2.5s
- Cost per transaction: Card 2.9¢, UPI 0.1¢, Public Blockchain 0.5¢, Permissioned Blockchain 0.3¢
- Permissioned blockchain shows strong fraud prevention while maintaining near real-time performance.
- Challenges include scalability, privacy concerns, and regulatory alignment.

6. Conclusion

- Blockchain prevents digital payment fraud proactively.
- Permissioned networks provide security, compliance, and near real-time settlement.
- Smart contracts automate escrow, refunds, and spend control.

7. Future Scope

- Integrating blockchain with CBDCs and banking systems.
- Use of zero-knowledge proofs for enhanced privacy.
- Federated learning models for fraud prediction.
- Expansion to cross-border payment networks.

References

[1] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” Proceedings of the Thirteenth EuroSys Conference (EuroSys ’18), ACM, 2018. [Online]. Available: arXiv:1801.10228
[2] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper),” Ethereum Project, Version 2025-02-04, 2025.
[3] Bank for International Settlements, “BIS Survey on Central Bank Digital Currencies,” BIS Papers, No. 159, 2025. [Online]. Available: https://www.bis.org
[4] EY, “The Digital Payments Ecosystem of India,” EY Report, 2025. [Online]. Available: https://www.ey.com
[5] PwC India, “Indian Payments Handbook 2024–2029,” PwC India Report, 2024. [Online]. Available: https://www.pwc.in