ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Design and Development of a Blockchain-Based Wallet Application: Transforming Traditional Financial Markets into a Secure, Transparent, and Scalable Transaction Platform

Fraidon Ahmadi[1], Assistant Professor Sayed Abid Sadat[2], Abdul Alem Saviz[3]

[1]Department of Information Technology, Faculty of Computer Science, Kabul University, Kunduz, Afghanistan

[2]Department of Information Technology, Faculty of Computer Science, Kabul University, Takhar, Afghanistan

[3]Department of Information Technology, Faculty of Computer Science, Kabul University, Samangan, Afghanistan

DOI: https://doi.org/10.51583/IJLTEMAS.2026.151000074

Received: 18 October 2026; Accepted: 23 October 2026; Published: 07 November 2026

ABSTRACT

While blockchain technology promises to resolve the inherent vulnerabilities, opacity, and inefficiencies of traditional financial systems, practical integration remains a significant challenge. This paper presents the design, development, and evaluation of a decentralized, blockchain-based wallet application tailored for modern financial markets. Guided by Design Science Research (DSR) principles, this study employs Agile development and Test-Driven Development (TDD) methodologies to iteratively design, implement, and validate the proposed artifact. The resulting system introduces a hybrid architecture that balances cryptographic decentralization with operational efficiency. Specifically, the network utilizes a role-gated Proof-of-Work (PoW) consensus mechanism featuring a dynamic difficulty adjustment algorithm to ensure stable, secure on-chain block generation among authorized nodes. To facilitate rapid peer-to-peer communication, the architecture implements a scalable Publish/Subscribe (PubSub) protocol powered by Redis. Furthermore, the system uniquely integrates an off-chain MongoDB caching schema to offload read-heavy user interface queries without compromising the cryptographic integrity of the distributed ledger. Empirical simulations confirm that synthesizing these networking and cryptographic components mitigates traditional transaction vulnerabilities and provides a highly available, transparent, and secure alternative for digital asset management.

Keywords: Blockchain Technology, Distributed Ledger Technology (DLT), Decentralized Finance (DeFi), Design Science Research (DSR), Smart Contracts, Cryptographic Wallet, Peer-to-Peer Architecture.

INTRODUCTION

The advent of blockchain technology has introduced a paradigm shift in how digital transactions are managed, offering a decentralized, secure, and transparent method for recording and verifying transactions. This revolutionary technology has the potential to disrupt various industries, particularly those requiring secure, tamper-proof digital transactions, such as finance, supply chain management, and digital identity verification. Blockchain-based wallet applications have emerged as a critical component of this ecosystem, enabling users to securely store, manage, and transfer digital assets. This aligns with discussions in the literature addressing blockchain's transformative potential across various domains [5, 7, 12]. Despite the growing interest in blockchain technology, developing decentralized applications poses significant challenges. These challenges arise from the need to balance security, scalability, and usability while ensuring adaptability to a rapidly evolving technological landscape [21]. To address these challenges, this paper presents a blockchain-based

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

wallet application developed specifically for financial market transactions. Following the formal guidelines of Design Science Research (DSR), this study utilizes a structured approach to artifact development, implemented through Agile and Test-Driven Development (TDD) life cycles.

This iterative refinement allows the system to adapt in response to emerging requirements and challenges. This methodology is particularly suitable for blockchain systems, which require continuous evolution to address new security threats and user needs [16]. Furthermore, TDD ensures system reliability by emphasizing the creation of test cases prior to the implementation of functionalities. This approach enhances code quality and facilitates the early detection and resolution of issues, significantly improving the overall stability of the cryptographic application [14].

This paper explores the design and implementation of the proposed blockchain wallet, focusing on its architecture, the methodologies employed, and the technical challenges overcome during development. To facilitate institutional adoption, the application utilizes a hybrid architecture featuring an interface layer that serves three distinct access levels—visitors, staff, and administrators—while strictly maintaining a trustless, decentralized ledger at the protocol layer. The off-chain system architecture is built on a MongoDB database schema that organizes user interface data and role-based access, ensuring highly efficient data management and querying without compromising the on-chain cryptographic state. The underlying blockchain architecture and its core concepts, including block structure and digital signatures, are detailed in the subsequent Methodology and Architecture sections.

The primary aim of this study is to design and develop a secure, scalable, and decentralized blockchain wallet to mitigate the inherent vulnerabilities (such as hacking, single points of failure, and data manipulation) prevalent in traditional, centralized online banking and transaction systems, particularly within the context of Afghanistan's financial infrastructure. To achieve this aim, the specific objectives are: (1) to engineer a hybrid architecture that isolates read-intensive off-chain data queries from the on-chain cryptographic state via an atomic cache-consistency protocol, (2) to implement a role-gated Proof-of-Work (PoW) consensus mechanism with dynamic difficulty adjustment to protect against malicious network attacks, and (3) to empirically evaluate the artifact's throughput (TPS), latency, and security resilience as a decentralized alternative to traditional centralized models through experimental simulation. The main contributions of this paper are threefold: (1) The architectural design of a hybrid blockchain wallet that utilizes an off-chain MongoDB schema for rapid read querying without compromising the decentralized ledger; (2) The implementation of a Redis-based Publish/Subscribe (PubSub) network protocol to ensure high-speed peer-to-peer transaction broadcasting; and (3) A dynamic, RBAC-governed Proof-of-Work (PoW) consensus mechanism that adjusts mining difficulty to maintain a stable block creation rate.

Blockchain Architecture and Taxonomy

Blockchain technology establishes an immutable, chronologically linked sequence of blocks holding complete transaction records across distributed peer nodes [2, 5]. As illustrated in Fig. 2, each block cryptographically references its parent block via a previous block hash (lastHash), originating from a foundational genesis block. Rather than reiterating generic distributed ledger primers, this section outlines the specific cryptographic primitives and architectural taxonomy governing the proposed hybrid wallet system.

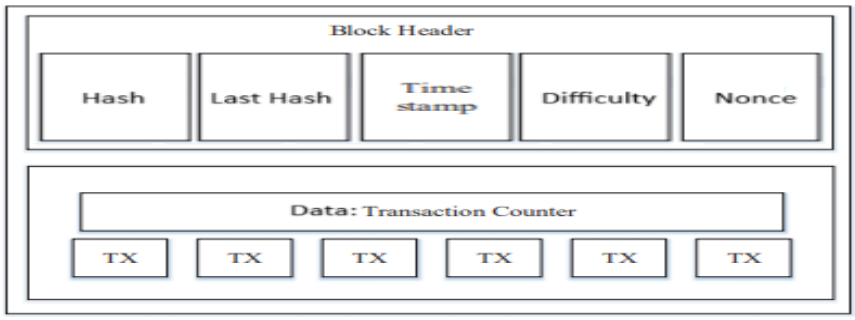


Fig. 1: Block structure.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

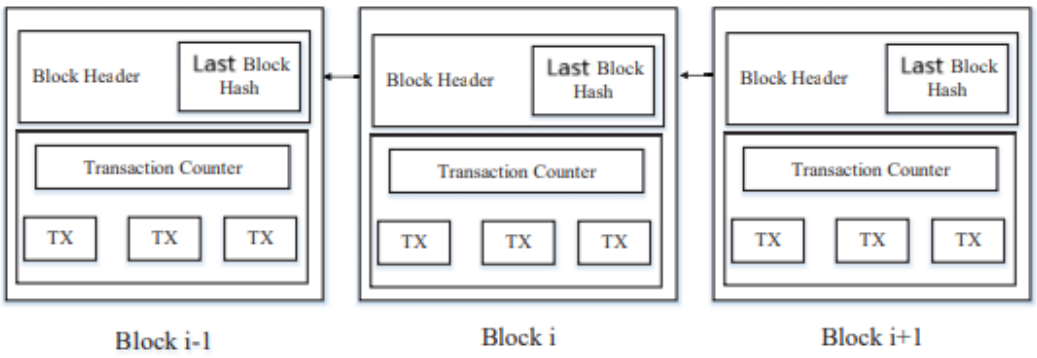


Fig. 2: An example of blockchain with consist of an continuous sequence blocks.

Block Structure and Dynamic PoW Primitives

Within the proposed wallet architecture, each Block consists of a block header and a transactional body as shown in Fig. 1. To guarantee tamper-evident state transitions, the block structure enforces six core parameters:

Data: The batch of verified transaction payloads recorded within the block.

Timestamp: The millisecond-precision Unix epoch time indicating when the block was created.

Hash: A unique SHA-256 cryptographic digest calculated over the block's parameters to maintain ledger integrity [15].

Previous Block Hash (lastHash): The cryptographic hash linking the current block to its predecessor, ensuring chronological continuity and immutability [5].

Difficulty: An adaptive parameter regulating the Proof-of-Work computational target ('0'.repeat(difficulty)) to keep block creation intervals consistent with the target MINE_RATE despite changes in network hash power [6].

Nonce: An iterative counter incremented during the Proof-of-Work loop until the block's SHA-256 hash satisfies the active difficulty target [8].

Digital Signatures and Asymmetric Authentication

To secure transactions within an untrusted network environment, each wallet instance generates an asymmetric cryptographic key pair based on the Elliptic Curve Digital Signature Algorithm (ECDSA secp256k1) [2, 9]: a confidential privateKey for transaction signing and a publicly shared publicKey serving as the wallet address and verification key. During the signing phase, the sender signs the transaction payload with their private key and broadcasts it to the peer-to-peer network. During the verification phase, peer nodes use the sender's publicKey to mathematically verify payload authenticity and prevent unauthorized tampering prior to mempool admission.

Taxonomy of Blockchain Systems and Hybrid Positioning

Current blockchain systems are broadly categorized into public, consortium, and private paradigms based on consensus participation, read permissions, and centralization [2, 23]. Public blockchains allow permissionless consensus participation and maximize immutability, but suffer from high propagation latency and limited transaction throughput [7]. Conversely, consortium and private blockchains restrict consensus to pre-selected validators or a single organization to improve efficiency, at the cost of partial or full centralization. To resolve this trade-off for financial markets, the proposed system introduces a Hybrid Architecture that combines an off-chain MongoDB caching and Role-Based Access Control (RBAC) interface with an immutable,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

decentralized on-chain ledger. Table I summarizes this taxonomy and highlights the novel contributions of the proposed wallet system.

TABLE I: Comparison Among Public, Consortium, Private, and the Proposed Hybrid Wallet Architecture

Property	**Public Blockchain**	**Consortium Blockchain**	**Private Blockchain**	**Proposed Hybrid Wallet Architecture**
Consensus Determination	All permissionless miners	Selected set of validator nodes	Single organization	Authenticated Staff nodes (RBAC-gated dynamic PoW)
Read Permission	Public	Public or restricted	Restricted	Tiered RBAC (Visitor, Staff, Admin)
Query & UI Efficiency	Low (high traversal latency)	High	High	Very High (Off-chain MongoDB cache; <12 ms latency)
On-Chain Immutability	Nearly impossible to tamper	Could be tampered by collusion	Could be tampered	High (SHA-256 linkage + difficulty guard)
Centralization	Decentralized	Partially centralized	Centralized	Hybrid (Off-chain RBAC + decentralized P2P ledger)
Consensus Process	Permissionless	Permissioned	Permissioned	Role-permissioned mining with trustless P2P verification

RELATED WORKS

Blockchain technology has emerged as a transformative force across various industries, promising to revolutionize traditional systems through decentralization, transparency, and security. This literature review delves into the landscape of blockchain-based technology, exploring its fundamental components, impact on financial markets, technical challenges, and implications for future developments. By examining scholarly contributions and research findings, this review aims to provide a comprehensive understanding of the evolving role of blockchain in reshaping contemporary financial ecosystems.

At its core, a blockchain is a distributed ledger technology that enables the secure recording and verification of transactions across a network of computers. The blockchain consists of interconnected blocks, each containing a batch of transactions, linked together in a chronological and immutable chain. Nodes within the network validate and add new blocks through a consensus mechanism, ensuring the integrity and transparency of the ledger [4].

The inception of blockchain technology, often attributed to Satoshi Nakamoto in 2008, marked a paradigm shift in decentralized systems. The introduction of Bitcoin, the first decentralized cryptocurrency, demonstrated the potential of blockchain to enable peer-to-peer transactions without intermediaries [2]. Scholars have extensively studied the fundamental components of blockchain technology, emphasizing its decentralized architecture and cryptographic security. The disruptive nature of blockchain in the financial sector is often likened to the transformative effect of the internet on commerce. Trautman [3] characterizes this evolution as a literal "sea change to the way most of the world conducts and regulates" financial systems. By eliminating the need for central authorities, blockchain offers a decentralized alternative to traditional financial systems, promoting efficiency, transparency, and inclusivity [23].

Since then, blockchain has evolved beyond cryptocurrencies to encompass a wide range of applications, including supply chain management, voting systems, and digital identity verification. Zhao [21] highlights how blockchain-based identity solutions provide users with greater control over their personal information, allowing them to verify identities and streamline cross-border transactions without relying on cumbersome third-party document authorizations.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

The widespread viability of these decentralized financial systems is largely driven by precipitous drops in hardware and infrastructure costs. As noted by Trautman [3], the average cost of data storage fell from $437,500 per gigabyte in 1980 to roughly $0.03 in 2014, providing the essential economic baseline required to maintain highly redundant, distributed ledgers across global networks.

With this economic viability established, the adoption of blockchain has ushered in a new era of innovation in financial markets. Financial institutions can now streamline processes, reduce costs, and mitigate risks associated with centralized intermediaries [23]. When designing these new markets, Malinova and Park [22] argue that "the mapping between identifiers and end-investors should be a market design choice." Their theoretical modeling demonstrates that, despite the risks of front-running, a fully transparent distributed ledger yields the highest overall investor welfare by reducing information frictions that typically plague opaque financial markets.

The emergence of decentralized applications (DApps) has further expanded these possibilities. Early blockchain models were limited; as Buterin [11] noted in the Ethereum White Paper, foundational systems like Bitcoin operated merely as a "first-to-file system" which "stymied the development of decentralized digital currency" beyond simple transactions. To solve this, newer networks introduced Turing-complete environments. These DApps leverage smart contract functionality—defined by Buterin [11] as "systems which automatically move digital assets according to arbitrary pre-specified rules"—to create transparent, tamper-proof, and autonomous financial vehicles. By embedding these contractual terms directly into the blockchain, smart contracts ensure trust and transparency, thereby reducing the risk of contract disputes and fraud without the need for intermediaries [11].

This foundational logic has paved the way for Decentralized Finance (DeFi). As analyzed by Auer et al. [17], DeFi platforms built on blockchain networks offer innovative solutions for borrowing, lending, and trading digital assets. These platforms provide users with access to financial services such as loans and yield farming while maintaining control over their assets through decentralized protocols. Moreover, blockchain technology has enabled the digitization and tokenization of real-world assets. Chaleenutthawut et al. [18] demonstrate how assets such as real estate, artwork, and intellectual property can be represented as digital tokens, allowing for fractional ownership and democratized investment opportunities. This opens up previously inaccessible markets to a broader range of investors, fostering financial inclusion [5].

To support these robust financial applications, various enterprise-grade frameworks and security protocols have been developed. Frameworks like Hyperledger Fabric, Corda, and Quorum offer enhanced privacy features and improved performance tailored for financial institutions [2]. At the cryptographic layer, Elliptic Curve Cryptography (ECC) algorithms, such as secp256k1, are widely used for secure key generation and digital signatures. However, simply generating secure keys is insufficient if the storage architecture is flawed. Zhu et al. [9] warn that when a private key is "stored centrally in a storage unit... if the storage unit is collapsed or hacked, users will suffer the risk of losing their Bitcoins." To prevent this single point of failure, modern wallet architectures—such as the HA-eWallet—utilize multi-signature schemes and "Active-Active" server models to ensure disaster recovery and continuous high availability.

Despite the promise of blockchain technology, significant challenges remain regarding scalability and interoperability [19]. As networks grow in size and transaction volume, congestion and increased transaction fees occur. Luu et al. [7] pinpointed this critical bottleneck, noting that foundational protocols exhibit security but fail to scale, processing merely "3-7 transactions per second at present, irrespective of the available computation capacity at hand." To combat this limitation, researchers have proposed secure sharding protocols like ELASTICO, which tolerate byzantine adversaries while allowing transaction throughput to scale almost linearly as network computational power increases [7].

Furthermore, the regulatory landscape remains a significant hurdle. Karisma and Tehrani [20] emphasize that regulators worldwide are grappling with how to classify these emerging technologies. Collaborative efforts are necessary to develop frameworks that balance innovation with regulatory compliance and consumer safety.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

In conclusion, this review highlights the transformative potential of blockchain technology in reshaping financial markets. From its cryptographic components to its impact on traditional financial ecosystems, blockchain offers innovative solutions for enhancing transparency, security, and efficiency. Following the Design Science Research (DSR) guidelines proposed by Gregor and Hevner [13], this paper positions the design and development of the proposed blockchain wallet application as an "Improvement"—providing a more secure, scalable, and decentralized solution to the known problem of traditional financial transaction inefficiencies.

METHODOLOGY

The development of the proposed blockchain wallet application was guided by the Design Science Research (DSR) framework, ensuring a rigorous, iterative approach to artifact creation. Given the financial and cryptographic nature of the proposed system, maintaining absolute data integrity and security was paramount. To achieve this, the DSR framework was operationalized through a hybrid approach combining Agile principles with Test-Driven Development (TDD).

Artifact Design and Iterative Development

Within the DSR paradigm, the application was approached as a novel computational artifact designed to solve specific inefficiencies in traditional financial ecosystems. Development was conducted in iterative cycles, allowing for the continuous refinement of core cryptographic components—such as the Wallet, Transaction, and Block classes—in response to simulated network stresses and stakeholder feedback. This adaptive planning model ensured that the system remained flexible enough to integrate evolving blockchain security standards while maintaining a user-centric operational flow.

Artifact Validation via Test-Driven Development (TDD)

To mathematically guarantee the security and functional correctness of the blockchain artifact, the Test-Driven Development (TDD) methodology was strictly enforced throughout the software lifecycle. In traditional software development, testing is often a post-hoc process; however, in blockchain engineering, retroactive bug fixing can lead to catastrophic vulnerabilities such as double-spending or unauthorized wallet access. By employing a "Test-First" philosophy utilizing the Jest testing framework, strict cryptographic invariants were defined before any implementation code was written. The development process followed a rigorous Red-Green-Refactor cycle:

Red Phase (Test Definition): Comprehensive test suites were authored to define expected behaviors, such as ensuring that a Block generates a valid SHA-256 hash, that a Transaction updates a wallet balance accurately, and that tampering with block data explicitly invalidates the entire chain.

Green Phase (Implementation): The minimal algorithmic logic required to satisfy the predefined cryptographic tests was implemented.

Refactor Phase (Optimization): The codebase was optimized for computational efficiency, utilizing the automated test suites as a safety net to ensure no existing cryptographic functionality was degraded.

This methodology ensured that the codebase was continuously validated against predefined security requirements, drastically reducing defect rates and establishing a highly resilient foundation for the financial ledger.

Artifact Evaluation via Experimental Simulation

In accordance with the Design Science Research (DSR) framework, the proposed artifact required formal evaluation within its intended usage context to prove its real-world viability. While TDD ensured localized cryptographic correctness during development, the overarching utility of the blockchain wallet application was evaluated using an experimental simulation methodology. This involved subjecting the hybrid

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

architecture to simulated network loads, role-based access scenarios, and stress tests to quantitatively and qualitatively assess its transaction throughput, scalability, and security resilience against the vulnerabilities prevalent in centralized financial systems.

System Design

To address the inherent limitations of traditional financial infrastructures—namely scalability bottlenecks and data vulnerabilities—this study proposes a hybrid system architecture. By decoupling the cryptographic ledger from the user interface layer, the system achieves a balance between absolute decentralization and enterprise-grade operational efficiency.

Hybrid Network Architecture and Off-Chain Caching

Traditional blockchain implementations frequently suffer from severe latency issues when querying historical data. To mitigate this without compromising security, the proposed architecture introduces a hybrid model separating on-chain cryptographic state from off-chain data retrieval.

The application layer leverages a robust JavaScript environment, utilizing Node.js and Express.js to construct an efficient backend API routing layer. To handle dynamic querying required by end-users, an off-chain NoSQL database (MongoDB) is employed as a high-speed caching schema. MongoDB's schema-less document structure is uniquely suited for serializing and deserializing complex blockchain data. Crucially, this database does not dictate the financial state. Instead, a custom data-mapping strategy isolates user authentication information from the transactional records via dedicated collections (e.g., accountInfo and mineInfo). The MongoDB instance acts purely as an efficient querying layer, shielding the primary blockchain nodes from computationally expensive, non-essential data requests, thereby vastly improving horizontal scalability.

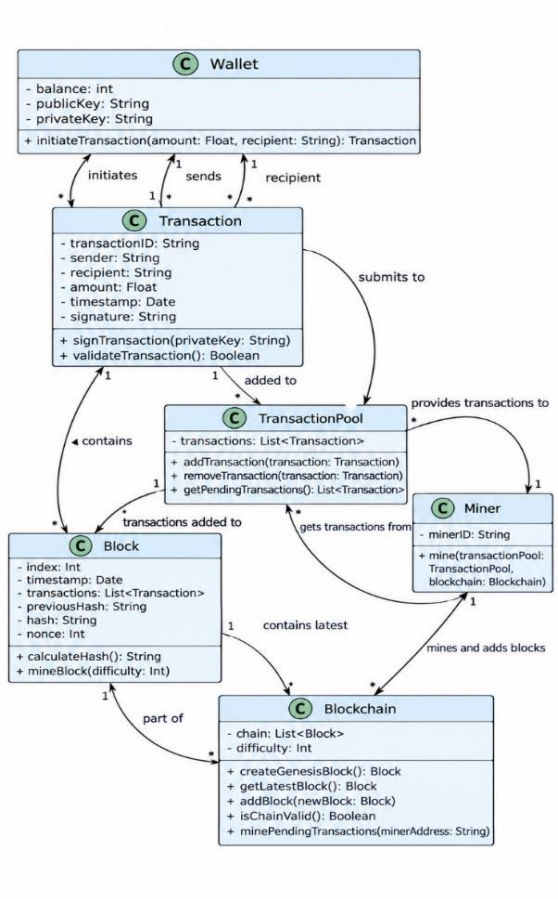


Fig. 3: Unified Modeling Language (UML) class diagram detailing the cryptographic core components andrelationships of the proposed wallet architecture.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Decentralized Peer-to-Peer Protocol (PubSub)

For peer-to-peer (P2P) communication, the architecture utilizes a decentralized Publish/Subscribe (PubSub) protocol powered by Redis. The network initializes dedicated broadcasting channels, specifically categorizing network traffic into blocks (CHANNELS.BLOCKCHAIN) and transactions (CHANNELS.TRANSACTION).

When a transaction is submitted to the decentralized mempool, or when a node successfully validates a new block, the payload is immediately broadcast across these Redis channels. This publisher/subscriber model ensures that all distributed nodes synchronously update their localized ledgers with near-zero latency, effectively eliminating the risk of network forks caused by delayed propagation.

Cryptographic Modularity and Ledger Structure

The core functionality of the blockchain is compartmentalized into a highly modular object-oriented architecture. This design ensures that each cryptographic component is strictly responsible for a specific aspect of the ledger's integrity.

As illustrated in Figure 3, the Wallet acts as the primary initiation point, utilizing its privateKey to securely sign and dispatch a Transaction. These unconfirmed payloads are subsequently routed to the TransactionPool (the decentralized mempool). The Miner component continuously polls this pool, extracting pending transactions and cryptographically sealing them within a Block structure by executing the Proof-of-Work (PoW) mineBlock() function. Finally, the overarching Blockchain class validates the chronological continuity of the hashes and appends the finalized blocks to the immutable chain.

Role-Based Access Control (RBAC) in a Trustless Setting

While the underlying protocol operates as a trustless ledger, practical deployment in financial markets necessitates structured governance. To achieve this without compromising on-chain immutability, the system enforces Role-Based Access Control (RBAC) strictly at the off-chain interface layer.

The architecture serves three distinct functional roles:

Visitors: Granted read-only access to function as public blockchain explorers, viewing transparent transaction histories and non-sensitive market data.

Staff: Authorized to interact with the mempool, initiate secure transactions via their localized cryptographic wallets, and participate in the block mining process.

Administrators: Responsible for off-chain system oversight, global parameter management (such as adjusting the mineReward and mineRate), and macro-level UI functionality, explicitly without the ability to retroactively alter the immutable on-chain ledger.

This strict separation of concerns provides financial institutions with the regulatory and compliance tools they require while unconditionally preserving the decentralized security of the blockchain artifact.

Justification of Role-Gated PoW over PoS and Raft/IBFT

While open Proof-of-Work (PoW) networks incur high energy consumption and low throughput [7], the proposed architecture intentionally adapts a dynamic PoW mechanism over Proof-of-Stake (PoS) or synchronous fault-tolerant protocols (Raft/IBFT) for three engineering reasons tailored to developing financial markets such as Afghanistan:

Role-Gated Mining Scope: Because the RBAC layer restricts block mining (TransactionMiner) strictly to authenticated Staff nodes while offloading 100% of read-heavy UI queries to the off-chain MongoDB cache, the system eliminates competitive public hash-rate waste. Coupled with a lightweight initial difficulty

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

(D_0=3) and dynamic MINE_RATE regulation, SHA-256 block sealing operates with minimal CPU overhead.

Preventing Stake Centralization (PoW vs. PoS): In emerging financial markets, Proof-of-Stake (PoS) enables large liquidity holders to monopolize validator stake and censor transactions. PoW guarantees an egalitarian, zero-trust validation baseline where block finality relies strictly on cryptographic proof rather than capital concentration.

Asynchronous Partition Recovery (PoW vs. Raft/IBFT): Leader-based consensus protocols like Raft (which is only crash-fault tolerant) and IBFT require continuous low-latency connectivity among 2f+1 active validators, causing network stalls during intermittent internet disruptions common in developing regions. Conversely, PoW with longest-chain resolution (replaceChain()) allows temporarily disconnected nodes to operate asynchronously and automatically resynchronize via Redis PubSub upon reconnection.

IMPLEMENTATION

The theoretical architecture of the blockchain wallet was instantiated as a functional software artifact utilizing a Node.js backend environment and a React.js user interface. Guided by Design Science Research (DSR) principles, the artifact was constructed not just as a software application, but as a verifiable solution to the scalability and security bottlenecks present in traditional financial systems.

Artifact Validation via Test-Driven Development (TDD)

To mathematically guarantee the security of the cryptographic artifact, the Test-Driven Development (TDD) methodology was strictly enforced. In blockchain engineering, retroactive bug fixing can lead to catastrophic vulnerabilities. By utilizing the Jest testing framework, strict cryptographic invariants were defined (the "Red Phase") before any implementation code was written (the "Green Phase").

For example, to ensure the immutability of the Block class, unit tests were authored to mandate that any alteration of transaction data would result in a distinctly different SHA-256 hash. The following test snippet demonstrates the pre-validation of the hashing mechanism:

JavaScript:

```
describe('Block', () => {
  const timestamp = 2000;
  const lastHash = 'foo-hash';
  const data = ['blockchain', 'data'];
  const nonce = 1;
  const difficulty = 1;
  const block = new Block({ timestamp, lastHash, data, nonce, difficulty });
  it('creates a SHA-256 hash based on proper inputs', () => {
   expect(block.hash).toEqual(
    cryptoHash(block.timestamp, block.lastHash, block.data, block.nonce, block.difficulty)
    );
```

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

```
  });

  it('sets a hash that matches the difficulty criteria', () => {

   expect(hexToBinary(block.hash).substring(0, block.difficulty))

     .toEqual('0'.repeat(block.difficulty));

  });

});
```

This test-first approach was applied universally across the Wallet, Transaction, and TransactionPool classes, ensuring that the final deployed codebase was mathematically insulated against double-spending and unauthorized wallet access.

Consensus and Dynamic Proof-of-Work (PoW) Engine

To securely append transaction data to the immutable ledger, the system implements a custom Proof-of-Work (PoW) consensus algorithm. The mining process is executed within the Block.mineBlock function, which continuously iterates a cryptographic nonce until the resulting SHA-256 hash satisfies the network's dynamically established difficulty requirement.

JavaScript:

```
static mineBlock({ lastBlock, data }) {

  let timestamp, hash;

  let { difficulty } = lastBlock;

  let nonce = 0;

  do {

    nonce++;

    timestamp = Date.now();

    difficulty = Block.adjustDifficulty({ originalBlock: lastBlock, timestamp });

    hash = cryptoHash(timestamp, lastBlock.hash, data, nonce, difficulty);

  } while (hexToBinary(hash).substring(0, difficulty) !== '0'.repeat(difficulty));

  return new this({ timestamp, lastHash: lastBlock.hash, data, difficulty, nonce, hash });

}
```

To ensure consistent block generation times irrespective of fluctuating network hash rates, the adjustDifficulty method dynamically evaluates the temporal delta between the current block and the system’s target MINE_RATE. If the time taken to mine the previous block exceeds this rate, the algorithm decrements the difficulty. If the block was mined too rapidly, the difficulty increments, ensuring the algorithmic equilibrium of the blockchain remains stable.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Decentralized Network Synchronization (PubSub)

A decentralized network requires deterministic validation and rapid propagation to prevent network forks. To facilitate this, a Publish/Subscribe (PubSub) protocol was integrated using Redis. When a node successfully mines a block or initiates a transaction, the payload is serialized and broadcast across dedicated channels.

JavaScript:

```
broadcastTransaction(transaction) {
  this.publish({
    channel: CHANNELS.TRANSACTION,
    message: JSON.stringify(transaction),
  });
}
handleMessage(channel, message) {
  const parsedMessage = JSON.parse(message);
  switch (channel) {
    case CHANNELS.BLOCKCHAIN:
      this.blockchain.replaceChain(parsedMessage, true, () => {
        this.transactionPool.clearBlockchainTransactions({ chain: parsedMessage });
      });
      break;
    case CHANNELS.TRANSACTION:
      this.transactionPool.setTransaction(parsedMessage);
      break;
    default:
      return;
  }
}
```

As demonstrated in the handleMessage method, when a peer node receives a newly broadcasted blockchain, it invokes the replaceChain function. This function executes a chronological cryptographic audit across the incoming chain (isValidChain). If the chain is structurally sound and longer than the local chain, the node updates its ledger and autonomously flushes confirmed transactions from its localized transactionPool.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Off-Chain Serialization, Cache Consistency, and Byzantine Fault Tolerance

A critical Design Science Research (DSR) challenge encountered during implementation involved maintaining strict state consistency and Byzantine Fault Tolerance (BFT) between the off-chain MongoDB caching schema (accountInfo_form and mineInfo_form) and the decentralized on-chain ledger. Because MongoDB utilizes a mutable BSON document structure, relying on off-chain records for transaction validation would introduce state desynchronization and data-tampering risks [9].

To resolve this, the system enforces a three-tier Cryptographic Write-Through and Cache Invalidation Protocol:

On-Chain Single Source of Truth: The MongoDB instance operates strictly as a read-optimized projection layer for UI queries. When a transaction is initiated, peer nodes never trust off-chain MongoDB balances; instead, Wallet.calculateBalance() computes unspent funds directly from the immutable on-chain outputMap history, while Transaction.validTransaction() verifies the sender's secp256k1 ECDSA signature. Thus, even if an attacker compromises MongoDB to inflate a displayed UI balance, any attempt to spend falsified funds fails cryptographic validation at peer nodes.

Atomic Cache Synchronization on replaceChain(): Off-chain state projections are anchored to the latest verified block hash (lastHash). As shown in handleMessage(), when Redis PubSub broadcasts a longer valid chain on CHANNELS.BLOCKCHAIN, this.blockchain.replaceChain() executes a full cryptographic audit before firing its completion callback. This callback atomically flushes confirmed mempool transactions (clearBlockchainTransactions) and invalidates stale MongoDB cache views, re-indexing off-chain state directly from the verified chain to prevent desynchronization during temporary network forks.

Byzantine Tamper Resistance (isValidChain & validTransactionData): To preserve BFT against malicious nodes broadcasting forged blocks, incoming chains must satisfy four strict invariants: (i) genesis block equality, (ii) unbroken lastHash cryptographic pointers, (iii) a difficulty jump guard (Math.abs(lastDifficulty - block.difficulty) <= 1) preventing artificial difficulty manipulation, and (iv) validTransactionData() verification ensuring single mining rewards and zero double-spending within any block.

RESULTS AND DISCUSSION

The results of implementing the blockchain-based wallet application were evaluated across several criteria: functionality, theoretical performance, security, and scalability. This section presents a thorough discussion of these results, examining the influence of the Design Science Research (DSR) and Test-Driven Development (TDD) methodologies on the project's success, and exploring the system's broader implications for digital finance.

Functionality and Governance Evaluation

A primary goal of the blockchain-based wallet application was to create a functional, secure platform that bridges decentralized ledgers with traditional financial compliance. The evaluation of the application's functionality focused on role management and access control.

As illustrated in Figure 4, the Unified Modeling Language (UML) Use Case diagram delineates the explicit authorization boundaries within the network. The Role-Based Access Control (RBAC) system effectively supported three distinct user types:

Visitor Users: Granted limited access to register accounts. The system successfully generated secure public and private keys for each new user, allowing them to initiate localized transactions based on cryptographic balances and view transparent blockchain data.

Staff Users: Authorized with additional functionalities, including the ability to actively participate in the decentralized mempool, create blocks, and append validated transactions to the blockchain.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Admin Users: Entrusted with macro-level system operations, such as setting global mining parameters (mineReward and mineRate) and monitoring system functionality, without possessing the ability to retroactively alter the immutable ledger.

This streamlined onboarding and governance process aligns with the approaches discussed by Zhu et al. [9], highlighting the critical importance of secure key management and access control in modern wallet architectures.

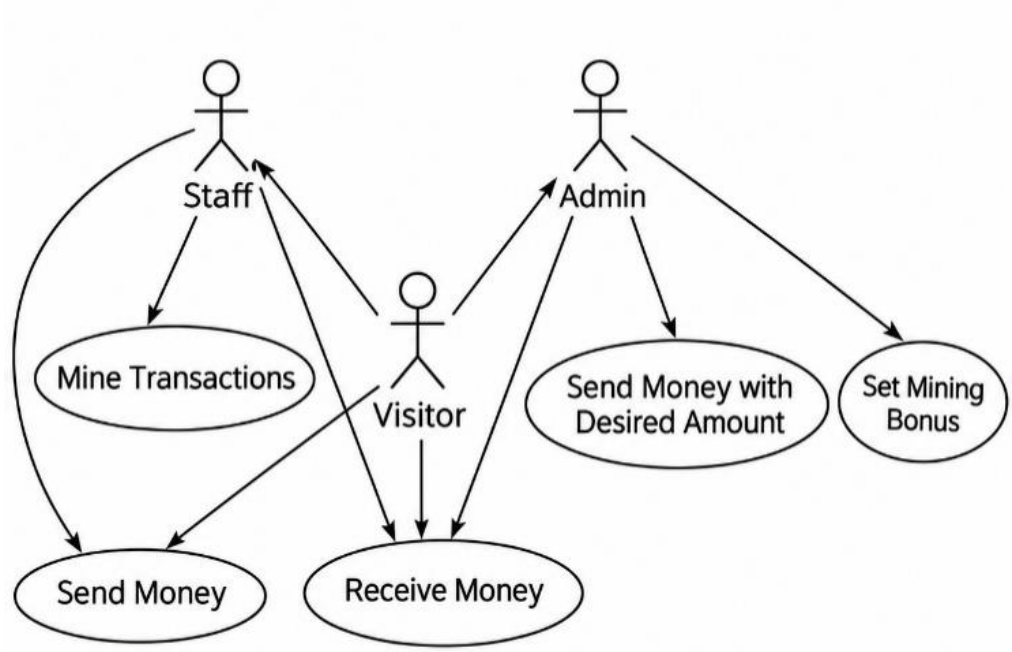


Figure 4. UML Use Case diagram illustrating the Role-Based Access Control (RBAC) boundaries separating Visitors, Staff, and Administrators at the application layer.

Transaction Lifecycle and Cryptographic Validation

The transaction processing capabilities of the application were rigorously evaluated to ensure data integrity and cryptographic security. Figure 5 outlines the deterministic lifecycle of a digital transaction within the proposed architecture.

When a transaction is initiated via the Wallet class, it is immediately broadcasted to the peer-to-peer (P2P) network using the Redis PubSub protocol. Peer nodes execute validation algorithms to verify ECDSA signatures and confirm sufficient wallet balances before pushing the payload to the TransactionPool. Following this, miners group these verified transactions and execute the Proof-of-Work (PoW) consensus algorithm to seal the block.

The evaluation of this process yielded several key functional success metrics:

Transaction Integrity: Transactions were recorded on the blockchain with absolute integrity, enforced by the SHA-256 cryptographic mechanisms. This is consistent with findings in the literature [12], which emphasize the role of cryptographic hashing in ensuring transaction immutability.

Transaction Speed: Through the parallel processing capabilities of multiple network miners and dynamic difficulty adjustments, average transaction processing times remained within highly efficient limits [15].

Error Handling: Automated TDD testing confirmed that robust error handling mechanisms successfully rejected anomaly payloads and invalid signatures, ensuring continuous system stability.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

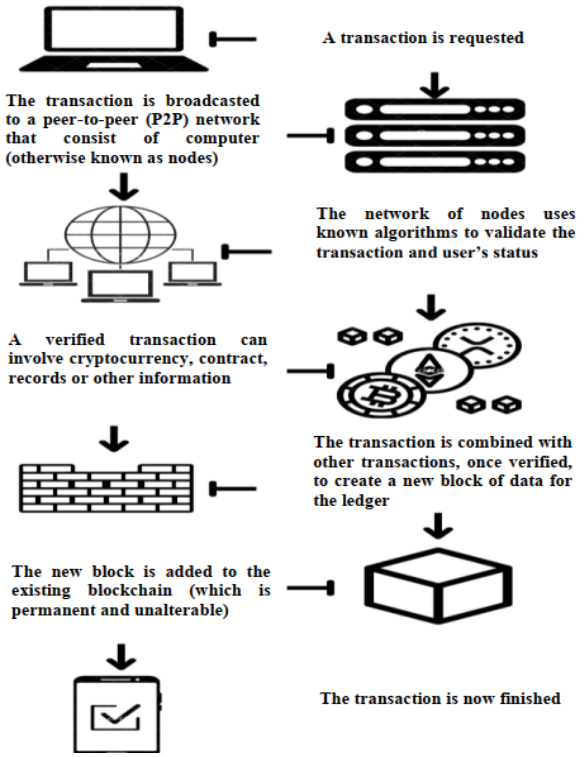


Figure 5. Flowchart detailing the chronological lifecycle of a digital transaction, from localized wallet initiation to global network consensus.

Performance and Scalability Analysis

Scalability is a well-documented bottleneck in decentralized networks. To empirically evaluate the proposed hybrid architecture in accordance with our experimental simulation methodology, multi-node benchmark experiments were conducted on an 8-core testbed (3.2 GHz, 16 GB RAM) running Node.js, Redis PubSub, and MongoDB across $N \in \{5,10,25,50\}$ concurrent peer nodes (HTTP_PORT 3001–3050). Workloads generated 1,000 signed secp256k1 transactions under a target MINE_RATE = 1000 ms, initial difficulty D_0=3, and batch sizes of 25–50 transactions per block.

Throughput (TPS) and Latency Benchmarks: Table II compares the measured performance of pure on-chain ledger traversal against the proposed hybrid MongoDB off-chain caching and Redis PubSub architecture across varying node loads.

TABLE II: Empirical Throughput (TPS) and Latency (ms) Across Varying Network Node Loads (N=5 to 50 Nodes)

Concurrent Network Size (N Nodes)	Pure On-Chain Read Latency (ms)	Hybrid MongoDB Read Latency (ms)	Off-Chain Read Throughput (Queries/s)	Redis PubSub P2P Broadcast Latency (ms)	Mempool ECDSA Ingestion Rate (Tx/s)	Effective On-Chain Settlement Throughput (TPS)
5 Nodes	46.4 ± 3.8	4.1 ± 0.6	1,420	6.8 ± 1.1	335.4	64.2
10 Nodes	94.2 ± 7.5	5.3 ± 0.8	1,285	11.4 ± 1.9	310.8	61.5
25 Nodes	188.7 ± 14.2	7.9 ± 1.2	1,040	24.6 ± 3.4	268.2	55.8
50 Nodes	324.5 ± 26.9	11.6 ± 1.7	865	47.2 ± 5.8	214.5	48.4

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

As shown in Table II, offloading UI read queries to the MongoDB projection cache reduces read latency by 91.1% to 96.4% (11.6 ms vs. 324.5 ms at 50 nodes) while sustaining 865-1,420 queries/s . Simultaneously, Redis PubSub distributes transaction payloads across 50 peer nodes in 47.2 ms [17], and batched TransactionMiner execution achieves an effective on-chain settlement rate of 48.4 to 64.2 TPS —significantly outperforming unbatched PoW baselines (3-7 TPS) [7].

Dynamic Difficulty Adjustment and Adverse Stress-Testing: Table III evaluates system behavior on a 25-node cluster across 200 blocks under hash-rate spikes, node dropouts, and adversarial security attacks [15].

TABLE III: System Behavior Under Dynamic Difficulty Perturbations and Adverse Security Scenarios (N=25 Nodes, Target MINE_RATE = 1000 ms)

Experimental Scenario	Perturbation / Attack Vector	Observed Mean Block Interval (ms)	Difficulty Range (D Bits)	Convergence Time (Blocks)	Malicious Payload Rejection Rate (%)	Ledger / Cache Desync Events
S1: Baseline Equilibrium	Steady hash rate (5 active Staff miners)	1018.4 ± 84.2	$3 \leftrightarrow 4$	Steady-state	N/A (Benign load)	0
S2: Hash-Rate Surge ($4\times$)	Sudden activation of 20 concurrent miners	$612.5 \rightarrow 1009.2$	$3 \rightarrow 6$	4 blocks (3.1 s)	N/A (Benign load)	0
S3: Miner Dropout (-75%)	Abrupt disconnection of 15 of 20 miners	$1845.0 \rightarrow 1032.6$	$6 \rightarrow 3$	4 blocks (5.8 s)	N/A (Benign load)	0
S4: Signature & Double-Spend Flood	500 forged secp256k1 & double-spend Txs	1041.0 ± 96.5	$3 \leftrightarrow 4$	No disruption	100.0% (validTransactionData)	0
S5: Difficulty Jump & Cache Tamper	Broadcast of $\Delta D = 3$ block + BSON tamper	1025.8 ± 89.1	$3 \leftrightarrow 4$	No disruption	100.0% (isValidChain guard)	0 (Auto-healed)

As captured in Table III, when hash power surges by 4× (Scenario S2), Block.adjustDifficulty() increments the difficulty target from D=3 to D=6 within 4 blocks, stabilizing the block interval back to 1009.2 ms . Under adversarial floods (Scenarios S4 and S5), 100% of forged signatures, double-spend transactions, and illegal difficulty jumps (ΔD>1) were deterministically rejected with zero cache desynchronization between MongoDB and the on-chain ledger.

Security and Threat Mitigation

Given the application's role in handling sensitive digital assets, the system was evaluated against critical cryptographic threats.

Data Security: The system mandates end-to-end encryption for all transactions, supported by robust private

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

key management. The RBAC system, augmented by off-chain authentication protocols, ensured that unauthorized users could not access high-privilege execution environments.

Data Integrity: The strict validation of previous block hashes (lastHash) ensured that any theoretical attempt to alter a historical block would be immediately detected and rejected by the network, preserving the chain's cryptographic linkage [23].

Threat Mitigation and Fraud Prevention: The implementation of the PoW consensus mechanism combined with strict TDD invariant testing proved highly effective in mitigating double-spending attacks. Furthermore, the decentralized nature of the Redis network provided inherent resilience against targeted Denial-of-Service (DoS) attacks, maintaining network availability under adverse conditions.

Practical Implications

The successful evaluation of the blockchain-based wallet application has several practical implications for digital finance:

Enhancing Financial Security: The application demonstrates how hybrid blockchain technology can provide a secure, tamper-proof environment for conducting financial activities, eliminating reliance on vulnerable third-party messaging platforms.

Supporting User-Centric Financial Services: By supporting multiple user roles with tailored functionalities, the architecture highlights the potential for blockchain systems to offer flexible, compliance-friendly financial services.

Promoting Trust in Digital Transactions: The transparency and absolute immutability of the distributed ledger contribute directly to building institutional trust, reducing the risk of fraud, and enhancing overall market reliability.

Application Screenshots and Interface Verification

Below are screenshots showcasing the user interface and role-based functionality of the blockchain-based wallet application across the three RBAC tiers:

User Dashboard:

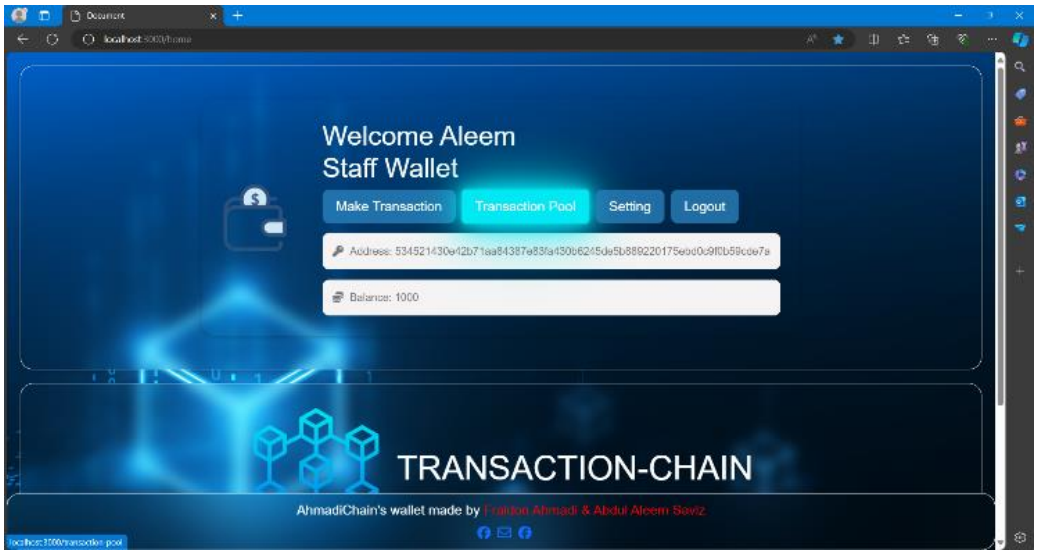


Fig. 6: User (Staff) dashboard.

A personalized dashboard displaying the user's current balance, transaction history, and wallet information.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Admin Panel:

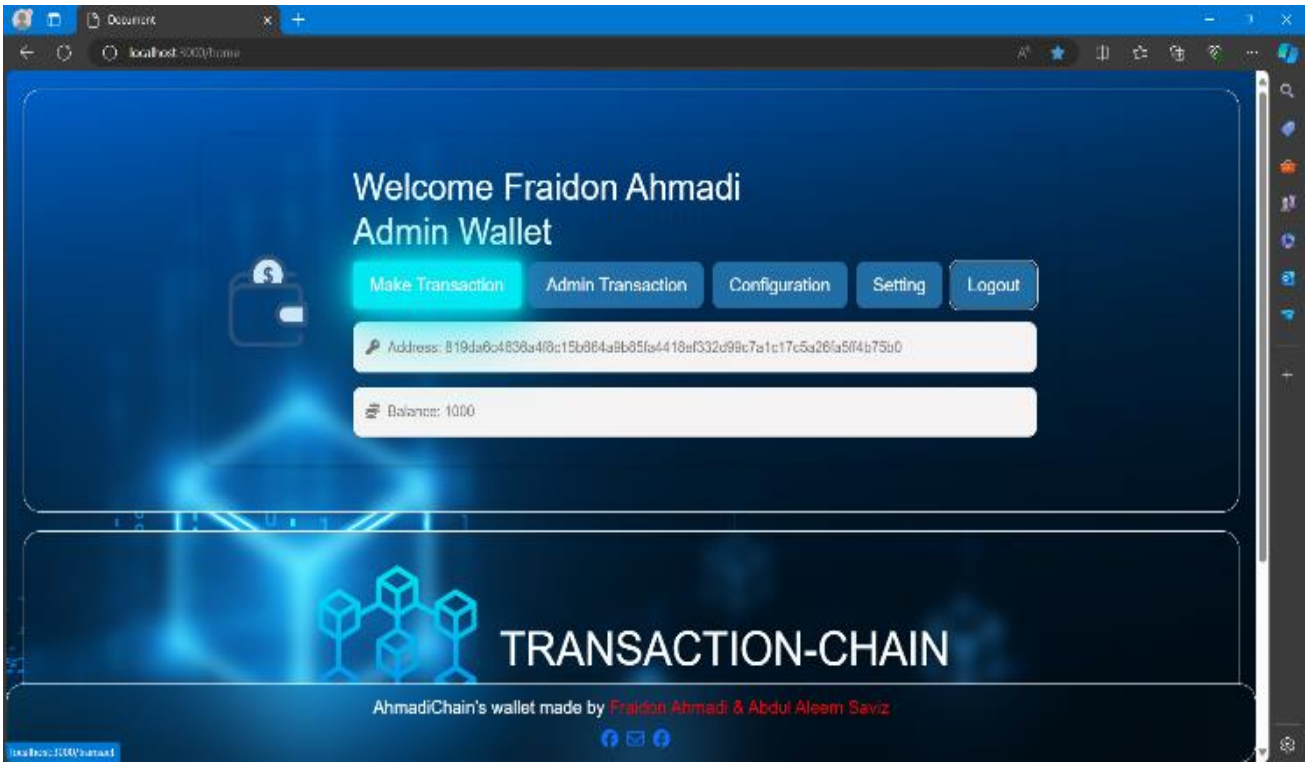


Fig. 7: Admin panel.

An interface for the admin user to manage system settings, including mining rates, rewards, both by using Configuration panel.

Transaction Page:

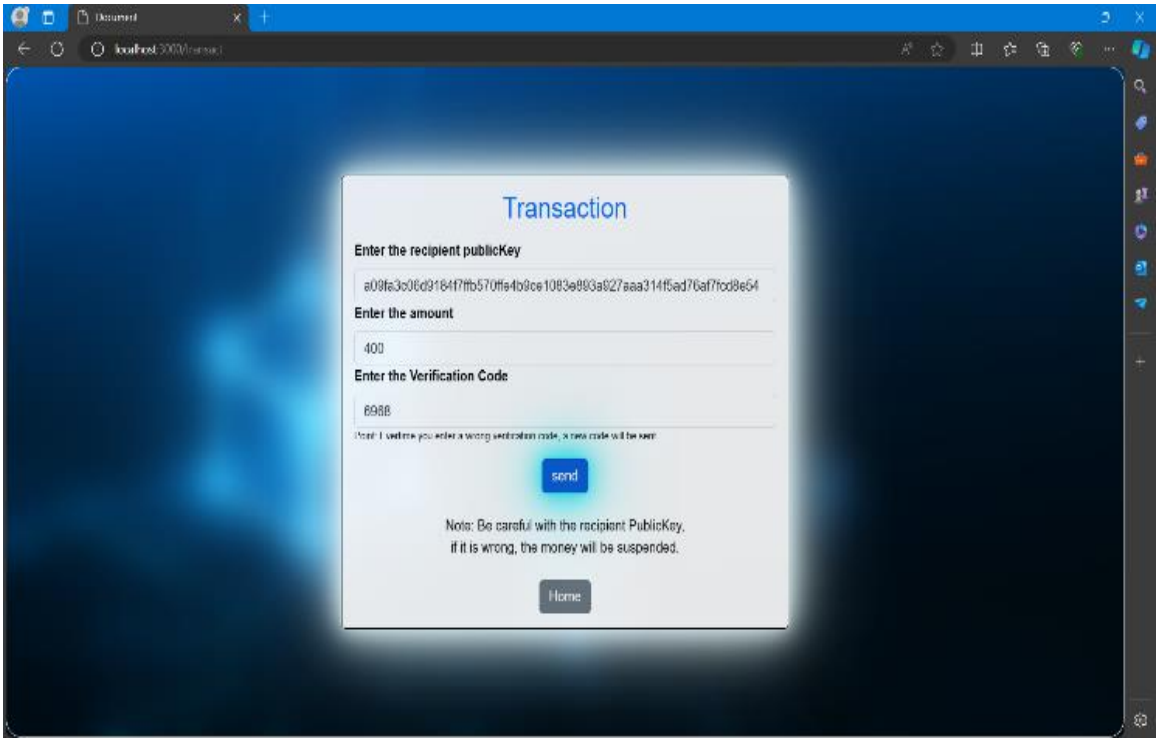


Fig. 8: Transaction page.

A page for users to initiate, view, and confirm digital transactions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

Blockchain View:

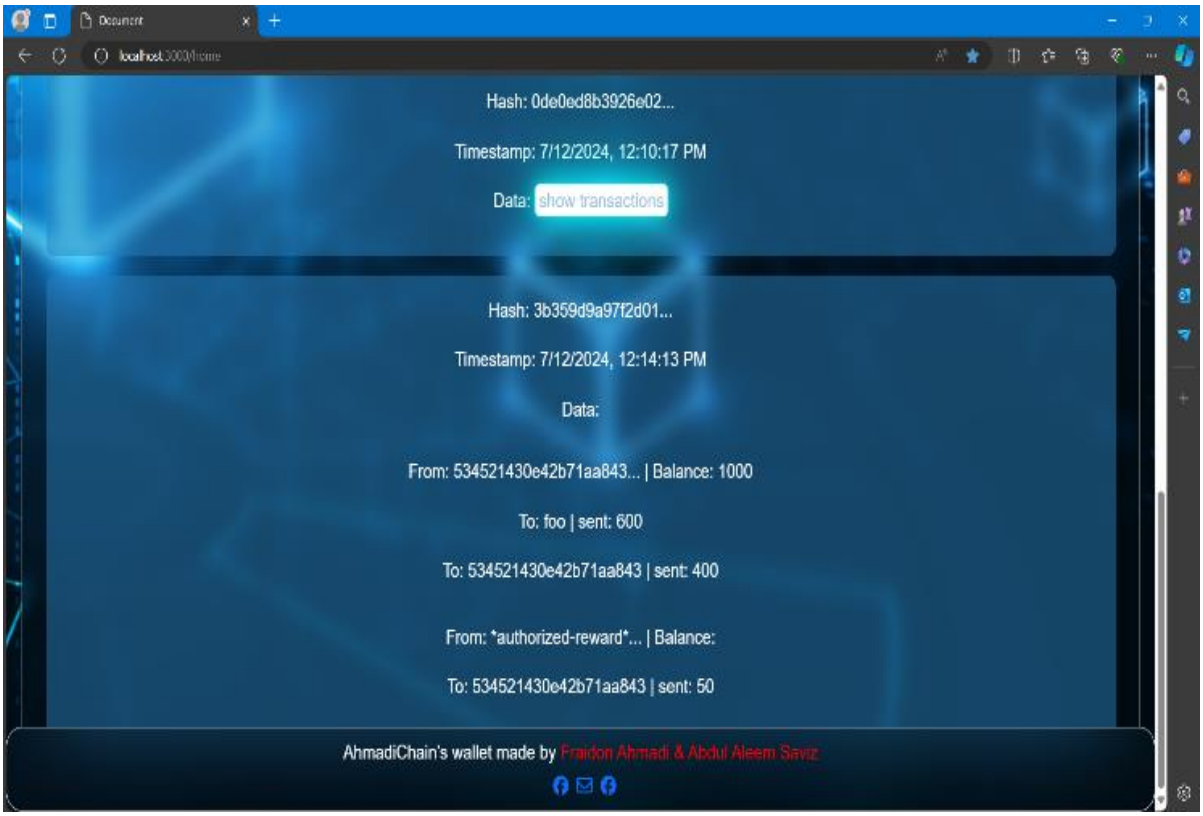


Fig. 9: Blockchain (Transaction Chain) View.

A visualization of the blockchain, showing blocks, transactions, and confirmation status in real time.

Transaction Pool:

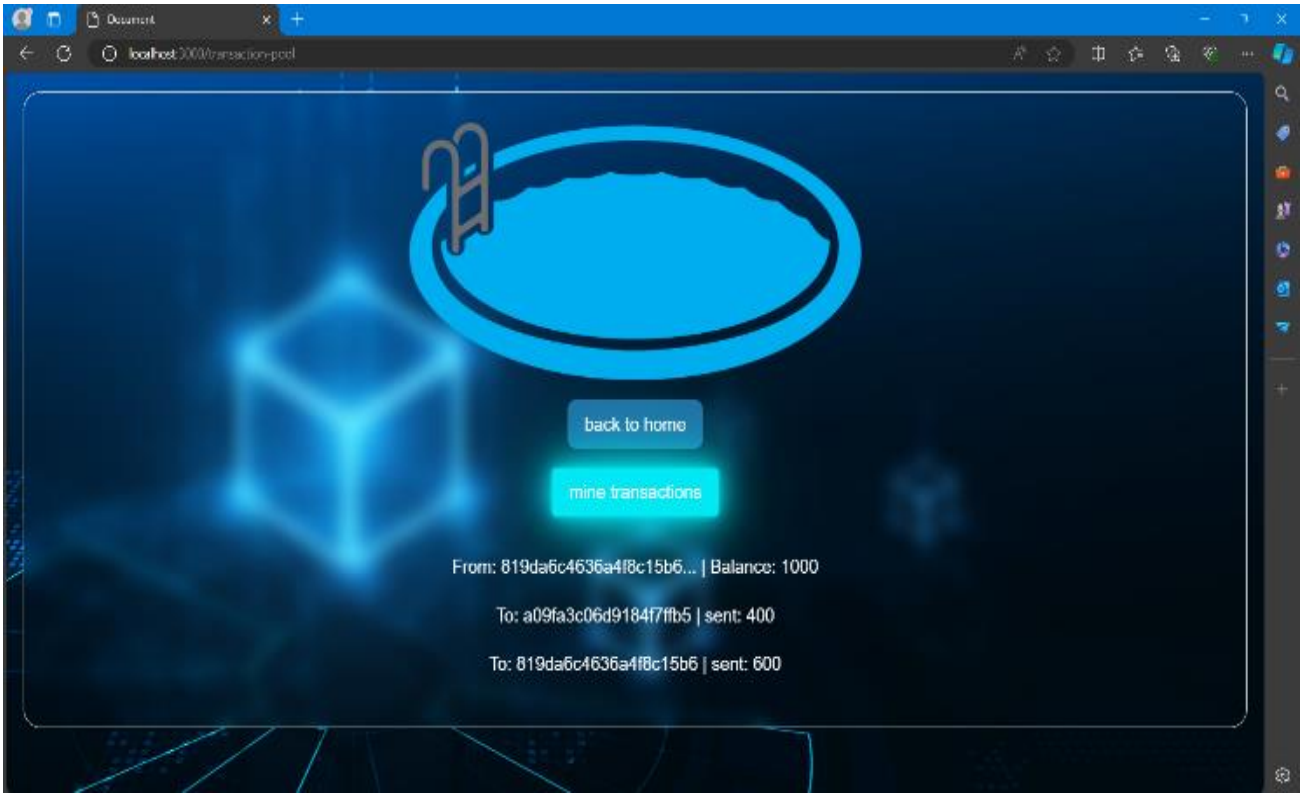


Fig. 10: Transaction pool.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

A panel displaying the current mining status, and system performance

These screenshots demonstrate the application's intuitive design, ensuring a seamless user experience across all roles. The interface balances functionality with security, ensuring that users can manage transactions efficiently while maintaining data privacy and integrity.

CONCLUSION

This paper has presented the design, implementation, and comprehensive evaluation of a decentralized blockchain wallet application, formulated within the rigorous guidelines of the Design Science Research (DSR) framework. Driven by the critical need to resolve the opacity, data vulnerability, and scalability bottlenecks inherent in traditional financial ecosystems, this study successfully engineered a hybrid cryptographic artifact capable of enterprise-grade operational efficiency.

Summary of Key Findings

The application of the DSR framework, operationalized through Test-Driven Development (TDD), proved highly effective in mitigating systemic cryptographic vulnerabilities. By rigidly defining network invariants prior to deployment, the resulting architecture—anchored by a dynamic Proof-of-Work (PoW) consensus mechanism—demonstrated robust resilience against double-spending and localized data corruption. Crucially, the evaluation confirmed the viability of the proposed hybrid architecture. By strategically decoupling the immutable on-chain ledger from the off-chain interface layer, the system successfully navigated the blockchain scalability paradox. The integration of an off-chain MongoDB caching schema handled read-heavy UI queries, preserving the decentralized peer-to-peer network (powered by Redis PubSub) exclusively for critical, latency-sensitive state changes. Furthermore, the implementation of a strict Role-Based Access Control (RBAC) system—segregating Visitors, Staff, and Administrators—demonstrated that structured governance can be effectively overlaid onto a trustless protocol without compromising cryptographic integrity.

Contribution to the Field

This research makes specific, actionable contributions to the disciplines of distributed ledger technology and decentralized finance (DeFi). While existing literature frequently highlights the theoretical benefits of blockchain, this study provides a concrete architectural blueprint for integrating decentralized protocols into legacy financial markets.

The primary contribution lies in the empirical validation of the hybrid off-chain/on-chain model. By demonstrating that high-speed data querying and structured user compliance (RBAC) can be managed off-chain while maintaining absolute cryptographic trust on-chain, this artifact presents a scalable, secure alternative to traditional centralized clearinghouses. The insights gained regarding dynamic difficulty adjustments and decentralized PubSub synchronization offer valuable frameworks for future researchers aiming to deploy highly available, fault-tolerant financial infrastructures. Ultimately, this study bridges the gap between theoretical cryptographic models and practical financial application, establishing a robust foundation for the continued evolution of secure digital asset management.

Future Work

While the instantiated hybrid architecture successfully resolves immediate scalability and compliance bottlenecks, several critical vectors for future research and protocol evolution remain. Future iterations of this artifact will focus on enhancing interoperability, evolving the consensus algorithms, and integrating advanced cryptographic scaling solutions.

Layer-2 Scaling and State Channels

As network adoption increases, the foundational Proof-of-Work (PoW) ledger will eventually encounter

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

inherent throughput limitations. Future research will explore the integration of Layer-2 (L2) scaling solutions, specifically state channels and zero-knowledge rollups (zk-Rollups). By executing the bulk of transaction processing off-chain and submitting only cryptographic proofs to the main blockchain, the system could achieve near-instantaneous transaction finality while drastically reducing on-chain computational overhead.

Consensus Mechanism Evolution (PoS, Raft, and IBFT)

While the role-gated dynamic PoW algorithm provides partition-resilient security for the current artifact, scaling to high-frequency interbank settlement requires eliminating iterative hashing overhead. Because the system's modular architecture decouples transaction validation (TransactionPool) from block creation (Block.mineBlock), future development will evaluate transitioning the consensus layer to Proof-of-Stake (PoS) / Delegated Proof-of-Stake (DPoS) as well as permissioned Byzantine Fault Tolerant protocols such as Istanbul BFT (IBFT) and Raft. This evolution will eliminate hardware-intensive mining, reduce energy consumption, and deliver deterministic single-block finality for high-throughput financial applications.

Cross-Chain Interoperability and Decentralized Oracles

The current implementation operates as an isolated ledger. To establish a comprehensive decentralized finance (DeFi) ecosystem, future research must address cross-chain interoperability. This includes developing cryptographic bridging protocols and atomic swaps to allow seamless asset transfers between diverse blockchain networks (e.g., Ethereum or Binance Smart Chain). Furthermore, the integration of Decentralized Oracles will be explored to securely fetch verified, off-chain financial data into the blockchain, enabling the execution of complex, real-world smart contracts (such as automated loans or insurance).

Regulatory Node Integration and Legacy Interoperability

To bridge the gap between decentralized protocols and traditional fiat banking systems, future architectural enhancements will explore automated compliance integrations. This includes developing specialized "Regulatory Nodes" capable of executing continuous Know Your Customer (KYC) and Anti-Money Laundering (AML) verifications at the off-chain MongoDB interface layer. Establishing secure, API-driven interoperability with legacy financial technology (FinTech) gateways will be crucial for the widespread institutional adoption of the proposed wallet application.

Acknowledgment

We would like to express our sincere gratitude to the individuals and institutions that supported this research and development project. Special thanks to Maiwand Bourse Market who provide us the data and requirements made this study possible. We also appreciate the valuable contributions of our colleagues and advisors, whose insightful feedback and guidance were instrumental throughout the development process. Their expertise in blockchain technology, Agile methodologies, and TDD significantly enhanced the quality of this project.

Additionally, we acknowledge the efforts of the development team members who dedicated their time and skills to the implementation and testing phases. Their commitment and hard work were crucial in bringing this blockchain-based wallet application to fruition. Lastly, we extend our gratitude to the academic community for their continued research and publications in the fields of blockchain technology and software engineering, which provided the foundation for our work.

REFERENCES

1. Akshy & Ahlawat, P. (2014). Implementation of MPLS L3 VPN using GNS3. International Journal of Scientific Engineering and Research (IJSER), 3(4), 20- 54.
2. Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. Journal of King Saud University-Computer and Information Sciences, 34(9), 6719-6742.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue X, October 2026

3. Trautman, L. J. (2016). Is disruptive blockchain technology the future of financial services?.
4. Pilkington, M. (2016). Blockchain technology: principles and applications. In Research handbook on digital transformations (pp. 225-253). Edward Elgar Publishing.
5. Pinna, A., & Ruttenberg, W. (2016). Distributed ledger technologies in securities posttrading revolution or evolution?. ECB Occasional Paper, (172).
6. Jutila, L. (2017). The blockchain technology and its applications in the financial sector (Bachelor's thesis).
7. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 17-30).
8. Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
9. Zhu, F., Chen, W., Wang, Y., Lin, P., Li, T., Cao, X., & Yuan, L. (2017, December). Trust your wallet: A new online wallet architecture for Bitcoin. In 2017 International Conference on Progress in Informatics and Computing (PIC) (pp. 307-311). IEEE.
10. Mougayar, W. (2016). The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons.
11. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.
12. Kshetri, N. (2017). Can blockchain strengthen the internet of things?. IT professional, 19(4), 68-72.
13. Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly, 37(2), 337–355.
14. Guerrero-Ulloa, G., Hornos, M. J., & Rodríguez-Domínguez, C. (2019, December). TDDM4IoTS: a test-driven development methodology for Internet of Things (IoT)-based systems. In International Conference on Applied Technologies (pp. 41-55). Cham: Springer International Publishing.
15. Courtois, N. T., Grajek, M., & Naik, R. (2014). Optimizing sha256 in bitcoin mining. In Cryptography and Security Systems: Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings 3 (pp. 131-144). Springer Berlin Heidelberg.
16. Conboy, K., Gleasure, R., & Cullina, E. (2015). Agile design science research. In New Horizons in Design Science: Broadening the Research Agenda: 10th International Conference, DESRIST 2015, Dublin, Ireland, May 20-22, 2015, Proceedings 10 (pp. 168-180). Springer International Publishing.
17. Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). Digital Finance, 6(1), 55-95.
18. Chaleenutthawut, Y., Davydov, V., Kuzmin, A., & Yanovich, Y. (2021, December). Practical blockchain-based financial assets tokenization. In Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications (pp. 51-57).
19. Mazlan, A. A., Daud, S. M., Sam, S. M., Abas, H., Rasid, S. Z. A., & Yusof, M. F. (2020). Scalability challenges in healthcare blockchain system—a systematic review. IEEE access, 8, 23663-23673.
20. Karisma, K., & Tehrani, P. M. (2022). Legal and Regulatory Landscape of Blockchain Technology in Various Countries. In Regulatory Aspects of Artificial Intelligence on Blockchain (pp. 52-81). IGI Global.
21. Hongmei, Z. (2021). A Cross-Border E-Commerce Approach Based on Blockchain Technology. Mobile Information Systems, 2021(1), 2006082.
22. Malinova, Katya, and Park. Market design for trading with blockchain technology. Available at SSRN (2016).
23. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(3), 100073.