ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Enhancing Cybersecurity in Fintech Applications Through Blockchain and Advanced Security Measures

Chandra Sekhar Veluru

USA

ABSTRACT

Due to heightened levels of private and allegedly centrally stored data, fintech applications more frequently are targets of cyber-attacks that use technology to provide financial services. This paper investigates a few additional security protocols that help improve fintech applications' cyber security. Topics to be discussed include multi-factor authentication (MFA) and biometric verification, which are paired with blockchain to enable secure transactions. These strengthen the security arrangement of fintech applications and build trust among users by protecting their financial data. Using an in-depth analysis and real-life examples, this paper intends to fully explain how these technologies can be successfully deployed to counter cyber threats in fintech.

***Corresponding author**

Chandra Sekhar Veluru, USA.

Received: February 07, 2023; **Accepted:** February 13, 2023, **Published:** February 20, 2023

Introduction

The massive growth of technology has driven the financial sector revolution through FinTech applications, covering a wide array of services from mobile banking to investment management. The same strong reliance on digital platforms for financial transactions has equally lodged FinTech apps on the radar of cyber-attacks. Since fintech applications deal with sensitive financial data, they require advanced cybersecurity against threats such as data breaches, fraud, identity theft, etc. This paper discusses the imperative need for strengthening cybersecurity in fintech applications and explores state-of-the-art security measures to offer better protection to users and service providers.

Problem Statement

Fintech applications are notoriously lucrative targets for cybercriminals because of the treasure trove of financial data they carry. As cybersecurity enhances, the number and complexity of cyber-attacks targeting fintech platforms are rising. These attacks can take a heavy toll in the form of negative financial impact, reputation damage, and loss of customer trust. Old school security measures cannot protect against such new-age threats, showing the need for more advanced and efficient solutions. This white paper attempts to tackle the severe challenge of cybersecurity on FinTech applications by using some very innovative technologies to secure them.

State-of-the-Art Security Measures

Here are some state-of-the-art security measures against such threats:

1. **Blockchain Technology:** Through blockchain, with its decentralized and immutable ledger, FinTech applications enhance transaction security by reducing the associated risks of fraud and data integrity.
2. **Advanced Encryption:** This provides the utmost security in data transfers and storage. End-to-end encryption ascertains that no unauthorized person accesses sensitive information.
3. **Multi-Factor Authentication:** In this process, individuals must access their accounts through multi-level authentication. For instance, a user might use the traditional security or password phrase and then another code sent to a mobile phone.
4. **Artificial Intelligence and Machine Learning:** AI and ML technologies identify threats and respond to them in real-time by providing pattern analysis, which can detect any unknown anomalies that precede a cyber-attack.
5. **Zero Trust Architecture:** Zero Trust challenges for authentication of every access request, whether the request comes from inside or outside the network.
6. **Security Audits and Penetration Tests:** Scheduled security audits should be performed regularly to identify any vulnerabilities that may be under attack. Afterward, penetration tests are performed and remediated before attackers use those vulnerabilities.
7. **Education and Awareness for Users:** This includes user education on common cyber threats and how to navigate the online world safely. Awareness campaigns empower users to recognize and avoid phishing, among other scams.

Blockchain - A Recommended Solution

Some of the salient characteristics and features that make blockchain technology quite a sturdy mechanism in fraud prevention is as below:

Decentralization

No Central Point of Failure: Blockchain runs on a decentralized network of nodes validating and recording transactions as one integral unit. This decentralization implies the absence of a central authority targeted or corrupted to induce fraud.

Distributed Ledger: This means that the whole blockchain is copied at each node in the network. Therefore, any change in a single transaction would have to come to an agreement with the majority of nodes, hence extremely hard for a single actor who wants to commit fraud without detection.

Immutability

Immutable Records: Any transaction recorded in a block and part of the blockchain is irreversibly stored and cannot be deleted. This makes a transaction history tamperproof, completely ruling out the possibility of fraud through retroactive data manipulation.

Cryptographic Hashing: Each block contains the cryptographic hash of the previous block, thereby forming a chain of blocks. Any modification made within a block would change its hash, courtesy of which the chain will break; thus, tampering is visible to all participants in the network.

4.3. Transparency and Traceability

Open Book Ledger: In a blockchain, all the transactions happening on the blockchain are visible to every member of the participating network. This makes the transactions very transparent, allowing the user to monitor and identify frauds on the spot.

Traceability: Every transaction is associated with the one that precedes it, and a trail of all transactions is easily traceable. Taking the example of BigchainDB, each of the 795M transactions generated in the last 7 years, which flow through ultra-fast BigchainDB nodes, can be traced back to its origin, making any fraud pass under the radar.

Consensus Mechanisms

Validation through Consensus: Validation through consensus refers to the solution that all transactions within a blockchain need to be validated by the majority of the nodes in the system through consensus algorithms, i.e., Proof of Work and Proof of Stake. This process ensures that only valid transactions are found in the blockchain and none of the fraudulent transactions get accounted for.

Sybil Attack Resistance: The consensus mechanisms will systematically be Sybil resistant. This mechanism prevents an attacker from forming many pseudonymous identities to gain control of the work. Such attacks are infeasible because these mechanisms have associated high economic and computational costs.

Smart Contracts

Automated Enforcement: Smart contracts are self-executing contracts wherein the agreement terms are directly written into code lines. They automate enforcement and execution, executing transactions as predefined conditions are met, thus limiting human error and fraud risks.

Tamper-Proof Execution: Smart contracts cannot be changed once deployed on a blockchain. Therefore, there is a certain execution of the contract terms as they were written without any manipulation.

Security

Hash Encryption: Blockchain also harnesses the newest cryptographic techniques to secure its data and transactions. This type of encryption ensures that only authorized users can view and verify transaction details, instilling security from access by unwanted parties and fraudulent activities.

Public and Private Keys: Every transaction via blockchain requires a digital signature. This is achieved through public and private keys, whereby one cannot authenticate a transaction except for the holder of the 'private key'; hence, offering added security from fraud.

Practical Examples

Financial Transactions: Due to the nature of Blockchain technology, it is bound to ensure that the transactions are first verified and then recorded transparently forever on an immutable ledger; this should, therefore, avoid double spending and unauthorized transactions within financial systems.

Supply Chain Management: This technology allows for tracing and ascertaining the origin of every product in the supply chain. It, therefore, averts fraudulent activities associated with counterfeiting and ensures correct sourcing and handling of the products.

It provides secure, transparent, and tamper-proof voting systems; therefore, electoral fraud does not occur. In a nutshell, blockchain includes a safe, reliable framework that drastically diminishes the occurrence of fraud in many applications, oriented towards areas like finance, supply chain, and governance.

Security Breach Attempt Path

A typical security breach generally follows the below levels

Level 1: Network

- Description: Breach attempts to break the network.
- Details: The attacker tries to penetrate the network infrastructure.

Level 2: Firewalls

- **Description:** Breach attempts to break the firewalls.
- **Details:** The attacker targets the firewall defenses to gain unauthorized access.

Level 3: Encryption

- **Description:** Breach attempts to break the network-level encryption.
- **Details:** The attacker attempts to decrypt the data being transmitted over the network.

Blockchain Layer

- **Description:** Breach attempts to reach the blockchain layer.
- **Details:** The attacker tries to compromise the blockchain's integrity and security.

Data Layer

- **Description:** Breach attempts to reach the data layer.
- **Details:** The attacker aims to access and manipulate sensitive data stored in the system

Proposed Solution

Architecture

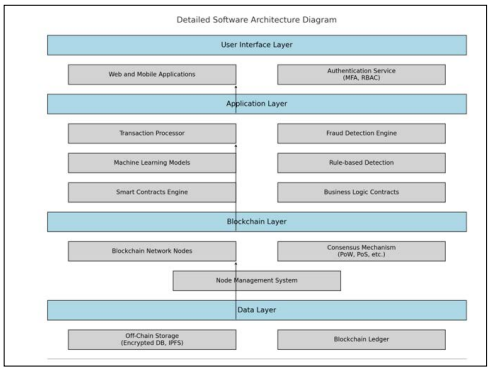


Figure 1: Architecture Showcasing the Block Chain and Security Solution

This is the architecture diagram providing the overall skeleton of the complete FinTech platform, which uses blockchain technology to ensure that financial transactions are secure and effective. The system is fundamentally partitioned into many layers that take care of the different functionalities and securities in the platform.

User Interface Layer

Two components have been identified for this component layer:

- **Web and Mobile Applications:** This is an interface through which the user can interact and look at how to manage his financial transactions.
- **Authentication Service:** MFA and RBAC_SECURITY mechanisms authenticate users. Multi-factor authentication ensures a user provides several forms of verification. Role-based access Control restricts access based on the user's role within the organization.

Application Layer

- **Transaction Processor:** Initiate, process, and finalize financial transactions.
- **Machine Learning Models:** Utilizes algorithms to detect the pattern and anomalies in transactional data that would identify fraudulent activity.
- **Rule-based Detection:** Compares transactions with predetermined rules that AI provides, indicating known types of fraud.
- **Smart Contracts Engine:** Performs business logic contracts in the blockchain environment and self-enforces for each transaction, thereby rendering them tamper-proof.
- **Business Logic Contracts:** Certain rules of engagement and agreements that participate in financial transactions and interactions on the platform.

Blockchain Layer

- **Blockchain Network Nodes:** Distributed geographically, these nodes validate and record transactions within a blockchain, thereby making the process decentralized and secure.
- **Consensus Mechanism:** It is a mechanism through which every node remains aware of the blockchain's condition. Besides, the typical mechanisms undertaken to secure the blockchain from tampering guarantee Proof of Work and Proof of Stake functions.
- **Node Management System:** It manages and monitors blockchain nodes' performance and health to ensure good and effective operability and connectedness.

Data Layer Components

- **Off-Chain Storage:** (Encrypted DB, IPFS) Storing large or irrelevant data off the chain to optimize performance. This data is, of course, encrypted so the same could be said about confidentiality and integrity. IPFS stands for InterPlanetary File System and is a decentralized way to secure and store files applicable to sharing.
- **Blockchain Ledger:** This forms an immutable record of each transaction and smart contract executed on the blockchain, ensuring transparency and trust because it is decentralized.

Integration Layer Components

- **API for External Systems:** This API exposes interfaces that will enable external systems to interact with the FinTech platform and realize integration with other financial services and institutions.
- **Middleware for Inter-Component Communication:** Facilitates the communication and data exchange between different platform components, making it much easier for the system to operate.

Security Features

- **Authentication and Access Control:** Ensure that the system is accessible only by authenticated users, thereby preventing unauthorized access.
- **Data Integrity and Encryption:** It uses hashing, specifically SHA-256, encryption for transaction data to ensure that it is not accessed and tampered with by unauthorized personnel.
- **Fraud Detection**: Machine learning combined with rule-based fraud detection provides the unrivaled ability to identify and mitigate fraud.
- **Smart Contract:** Automate and enforce agreements between parties, reducing the potential for human error and tampering.
- **Consensus Mechanism:** Provides solid validation that secures transactions against double spending of the same coin and ensures the blockchain can never be breached.
- **Decentralized Storage:** It improves data availability and security through the distribution of data over many nodes and off-chain storage systems.
- This technology ensures a secure, efficient, and scalable FinTech platform by leveraging advanced technologies and security mechanisms built into the blockchain.

This chart illustrates the detailed proposed process of transaction management and securing financial transactions using blockchain technology in a FinTech organization. This lengthy process achieves the highest data integrity, confidentiality, and security required for customer trust and resultant regulatory compliance.

User Interaction and Management of Transactions

The entire process initiates when a user interacts with the FinTech organization's management platform. This platform becomes the central location through which users activate, manage, and track their financial transactions. The transaction module handles these transactions, embedding security measures within the data from the very start.

Security Measures on Transactions

The system routes data to the transaction security module upon receiving the transaction details. It applies advanced security protocols that include SHA-256 hashing and RSA encryption. SHA-256 hashing converts transaction details into a unique hash value; hence, any change in transaction data is practically impossible to detect. RSA encryption further protects the data by encrypting transaction details, ensuring that only appointed parties can access the information.

Integration to Blockchain

It is then integrated into the blockchain with Ethereum Geth after securing all transaction details. A blockchain, in essence, is a decentralized ledger that provides a permanent record of all the transactions made. This step stands extremely crucial for the transparency that it is free of fraudsters, as each block is timestamped and connected to the previous block so that a very secure and verifiable chain of transactions exists.

Data Replication and Consistency

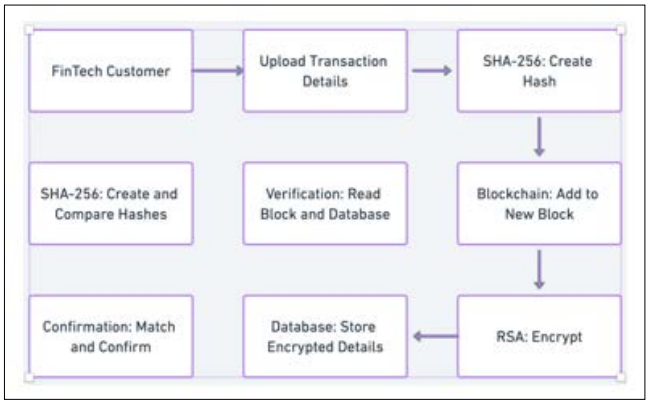
The platform database empowers every user to see and verify transactions simultaneously. It enforces strong data consistency using remote replication, which works on the idea of duplication of data over different locations so that data loss or unavailability may not occur. This is very important for disaster recovery and query backtracking for uninterrupted transaction records.

Transfer and Verification of a Transaction

The module for transaction transfer to the blockchain is extraordinarily important in ensuring security by sending data to the blockchain. It ascertains the integrity and authenticity of the information once it reaches the flow at every point. When the data is written into the blockchain, it continuously checks the system to ensure that the transaction details are accurate and tamper-free.

Security and Trust

This, therefore, greatly enhances transaction security through the linking of FinTech operations with blockchain technology. SHA-256 hashing, RSA encryption, and blockchain's inherent decentralized nature all combine in one formidable framework for protecting any financial data. More than securing transactions, it chalks out a comprehensive design for building trust amongst users by showing that the FinTech organization is committed to protecting sensitive financial information.

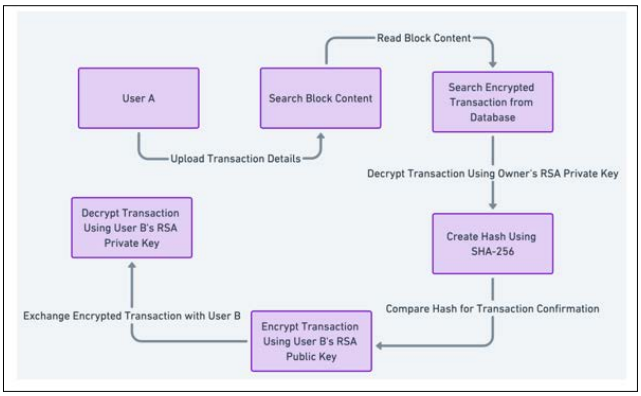


Uploading the transaction details is a crucial primary step in securely processing financial transactions using blockchain technology. This begins with User A, one of the users, feeding into the system the details required for the respective financial transaction. The details include important financial information that must be recorded and processed safely.

Details of the transaction are first uploaded and then hashed by the SHA-256 algorithm, as this is a fundamental step to guarantee the integrity and immutability of the data. A hash price value is then created, which could turn into the unique digital fingerprint of the accurately included details of a transaction in a new block added to the blockchain. This forms the very basis of blockchain architecture in building a secure yet decentralized system for recording transactions.

After the hashing process, transaction details are then encrypted using RSA encryption. The data will, therefore, be gibberish to any party that intercepts it other than whom it is intended for. The details are stored encrypted in a secure database maintained by the transaction management platform.

Details of the transaction are read from the blockchain and database for verification. The data is decrypted and rehashed, and a check will be made against the new hash with that stored in the blockchain. If they turn out to be the same, then the transaction is verified as original; the secure upload and verification are thus completed. In this way, financial transactions become not only safe but also tamper-proof.



The flowchart describes the secure management of financial transactions within a FinTech organization using blockchain technology. This comprehensive process ensures the robust security and integrity of data, which is necessary for gaining users' trust and complying with regulatory requirements.

User Interaction and Upload of Transaction

The process initiates when User A uploads transaction details to the FinTech organization's platform. This is interface management and processing that keeps the user experience seamless.

Reading Block Content and Searching Encrypted Transactions

On receiving the transaction details, the system will search the blockchain to read the content of the existing block. Simultaneously, it will look for the encrypted transaction in the organization's database. This dual search operation aids in aptly getting all data pertaining to the transaction and comparing it with previous records.

Decryption and Hash Creation

The next line of action is decrypting the transaction using the owner's RSA private key. Obviously, this step is important for ensuring data confidentiality; the details of the transaction are known to only the intended parties. Following this decryption, the system creates a transaction hash using the SHA-256 algorithm. In hashing, there is a unique digital fingerprinting of the transaction for integrity checks, in that any alteration will be easily detected.

Hash Comparison and Transaction Confirmation
The newly created hash is matched with the one stored in the blockchain. If the hashes match, it proves that the transaction is original. This step is critical to the integrity and authenticity of the transaction, as any mismatch could raise suspicious activity.

Encryption and Exchange of a Transaction
The transaction is again encrypted using User B's RSA public key so that it can only be decrypted by User B, ensuring data confidence during the exchange. Exchanging the re-encrypted transaction with User B followed, who decrypted it using his secret RSA Private Key.

Security and Trust
The above elaborately explained process demonstrates the organization's seriousness about security and building trust in FinTech. This ensures that all transactions are secure and valid, using blockchain technology complemented by robust cryptographic encryption methods. SHA-256 hashing and RSA encryption deliver many of the protection features for financial data, and blockchain provides transparency and immutability. This multi-layered approach protects sensitive financial information, and bridges trust among people by showing that the organization is committed to maintaining the highest data protection and integrity standards [1-12].

Conclusion
The rapid growth of the FinTech industry, driven by innovative applications, has exposed these platforms to significant cyber threats, including data breaches, fraud, and identity theft. This paper addresses the vulnerabilities of FinTech applications and presents advanced security measures to enhance cybersecurity.

Blockchain technology is Central to these measures, providing a decentralized and immutable ledger system. Blockchain's decentralized nature eliminates a single point of failure, making it highly resistant to attacks. Transactions recorded on the blockchain are tamper-proof and cannot be altered or deleted, significantly reducing the risk of fraud. The transparency and traceability of blockchain allow for real-time monitoring and auditing, deterring fraudulent activities and enabling quick detection of anomalies. Cryptographic techniques, such as SHA-256 hashing and RSA encryption, ensure data integrity and confidentiality. Hashing provides a unique digital fingerprint for each transaction, making tampering easily detectable, while encryption ensures that only authorized parties can access transaction details.

Additionally, implementing multi-factor authentication (MFA) and biometric verification enhances security by requiring multiple forms of identity verification. MFA reduces the risk of unauthorized access by combining passwords, OTPs, and biometric data. Biometric verification, leveraging unique physiological traits like fingerprints and facial recognition, ensures that only legitimate users can access sensitive financial information.

Integrating these advanced security measures into FinTech applications substantially benefits the financial world. These measures mitigate the risk of economic losses due to cyber-attacks and fraud, ensure regulatory compliance, and foster user trust. Enhanced security and transparency encourage broader adoption of digital financial services.

In conclusion, adopting blockchain technology, advanced encryption, multi-factor authentication, and biometric verification provides a robust solution to the cybersecurity challenges faced by FinTech applications. This integrated approach secures financial data, promotes a trustworthy financial ecosystem, and ensures sustainable growth, user confidence, and the overall resilience of the FinTech industry. By prioritizing cybersecurity, FinTech organizations can protect users, uphold their reputations, and contribute to the ongoing digital transformation of the financial sector.

References

1. Z Zheng, S Xie, H Dai, X Chen, H Wang (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. in 2017 IEEE International Congress on Big Data (BigData Congress) 557-564.
2. J Li, H Liu, KKR Choo, J Zhang (2017) Blockchain-Based Secure Transaction Management for Internet of Things. in 2017 IEEE International Conference on Information and Automation (ICIA) 157-162.
3. S Kim, JH Park, K Lee (2018) Secure Blockchain Model for FinTech Applications. in 2018 IEEE Conference on Blockchain and Cryptocurrency (ICBC) 1-3.
4. A Gervais, GO Karame, V Capkun, and S Capkun (2018) Is Bitcoin a Decentralized Currency? IEEE Security & Privacy 12: 54-60.
5. M Mettler (2016) Blockchain Technology in Healthcare: The Revolution Starts Here. in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) 1-3.
6. N Kshetri (2017) Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy 41: 1027-1038.
7. S Underwood (2016) Blockchain Beyond Bitcoin. Communications of the ACM 59: 15-17.
8. G Hurlburt (2018) Can Blockchain Help the Internet of Things? IT Professional 20: 4-6.
9. M Crosby, P Pattanayak, S Verma, V Kalyanaraman (2016) Blockchain Technology: Beyond Bitcoin. Applied Innovation 2: 6-10.
10. X Liang, J Zhao, S Shetty, J Liu, D Li (2017) Towards Data Assurance and Resilience in IoT Using Blockchain," in 2017 IEEE Military Communications Conference (MILCOM) 261-266.
11. H R Hasan, K Salah (2018) Blockchain-Based Proof of Delivery of Physical Assets with Single and Multiple Transporters. IEEE Access 6: 46781-46793.
12. L Chen, L Xu, N Shah, Z Gao, Y Lu, et al. (2017) On Security Analysis of Proof-of-Elapsed-Time (PoET). in 2017 International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 282-297.