International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Secured Banking System using Blockchain Technology

Mr. Muhammad Owais A [1], Pavithra M [2], Meghana S [3], Musaib Fayaz Bhat [4]
1, Assistant Professor, Dept. of Computer Science & Engineering, ACS college of Engineering, Bangalore, India
2,3,4,5, Dept. of Computer Science & Engineering, ACS college of Engineering, Bangalore, India
1, owais88258117661@gmail.com , 2, manipavithra20@gmail.com, 3, meghanasnc@gmail.com, 4, musaibfayaz94@gmail.com

Abstract- **In the rapidly evolving digital banking landscape, ensuring robust security while maintaining seamless user experience is paramount. This project, "Mobile Banking Security: A Futuristic Improved Security System," aims to enhance mobile banking security by integrating multi-factor authentication (MFA), encrypting sensitive data, and implementing fraud detection algorithms to safeguard users against unauthorized access and financial threats. The system also focuses on efficient bank account management by enabling users to create and manage different account types with real-time balance updates for deposits and withdrawals. Additionally, an automated interest calculation mechanism is developed using Celery scheduled tasks to ensure accurate monthly interest updates. A comprehensive transaction monitoring and reporting feature allows users to track their financial activities with customizable filters and data visualization options. By combining advanced security measures with user-friendly banking functionalities, this system offers a secure, efficient, and futuristic approach to mobile banking.**

Keywords - Blockchain, Transaction Security, Smart Contracts Decentralization, Consensus Mechanisms, Transparency.

I. INTRODUCTION

Faster transactions, greater accessibility, and better customer service are all made possible by the explosive expansion of digital banking, which has completely changed how financial institutions function. Data breaches, fraud, identity theft, and system vulnerabilities resulting from centralized infrastructures are only a few of the serious security issues brought about by this digital development. Sensitive financial data can be compromised by a single point of failure in traditional banking systems, which mostly rely on centralized databases. A more robust and transparent security architecture is desperately needed to protect the integrity of financial activities as cyberattacks become increasingly sophisticated. By utilizing decentralization, cryptographic protection, and unchangeable data storage, blockchain technology has become a viable way to overcome these security constraints. Because there are no dysfunctional systems or singular points of attack. However, there is already analytics software that selects community members based solely on transaction records because all bit currency transactions are public and available to everyone. Blockchain implementation, which consists of two types of records transactions and blocks is the most crucial component. Each block has a timestamp, and the safe hash method provides a link to a previous block. Several algorithms, such as SHA for hash formation, mining for a valid hash, smart contract for system policy, and consensus for certifying the current blockchain on all peer- to-peer nodes, are executed when transaction data is saved in the blockchain system.

By incorporating cutting-edge cryptographic techniques and decentralized technologies, the proposed financial system seeks to improve overall security. Secure data storage and dependable data access are important aspects of this activity. In order to prevent this, the system uses keyword-based hashing, Shamir's Secret Sharing mechanism, and content-based encryption approaches to protect sensitive financial data. This project's main goal is to build and create a blockchain-based financial infrastructure that is safe, transparent, and effective. The system improves trust, transaction integrity, and operational transparency by utilizing blockchain's decentralized, immutable, and distributed features. The main goal is to protect customer-to-bank interactions by making sure that all financial transactions are precisely documented and impervious to unauthorized changes.

- By incorporating blockchain technology to guard against fraud, data manipulation, and illegal access, the proposed financial system's main goal is to greatly improve security.
- The method removes the single point of failure that is commonly present in conventional centralized banking infrastructures by encrypting sensitive data and dispersing it around a decentralized network.
- It is very difficult for attackers to change or compromise important financial data because of this decentralized design. Improving the openness of banking activities is another important goal.
- An unchangeable ledger that documents each financial transaction is visible to authorized users of the system. Stakeholders can independently check actions without disclosing private user information because these records are permanently maintained and cannot be altered.
- Customers, financial institutions, and regulatory agencies all gain more trust as a result of this degree of openness.
- Enhancing data dependability is also essential to the system's objectives.
- The platform makes sure that once data is entered to the ledger, it stays correct, consistent, and unchangeable by utilizing blockchain's consensus algorithms and cryptographic validation techniques.
- Automating critical processes like loan processing, payments, and compliance verification is made possible in large part by smart contracts.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

- Automation makes banking more seamless and economical for both institutions and consumers by reducing errors, speeding up transaction processing, and lowering operating expenses.

This platform is built on a distributed ledger, which records each transaction in a shareable, verifiable, and fraud-proof way. By doing this, the chances of data manipulation, internal breaches, and foreign cyber threats are greatly reduced. Additionally, the system uses smart contracts to automate a number of crucial financial functions. Efficiency and accountability can be increased by automating procedures including loan approvals, regular payments, fund settlements, and compliance checks. The application employs robust cryptographic techniques, such as digital signatures and asymmetric key pairs, to safeguard user identification and financial data, guaranteeing safe authentication and stringent user privacy. All things considered, our work shows how blockchain- driven decentralized ledger technology, bolstered by clever automation and strong encryption, can completely transform security and dependability in contemporary state contemporary financial system.

Fig.1. Features included in Banking System

Transparency and Auditability: Real-time transaction auditing will be made possible by the system, providing banks and regulatory bodies with transparent, unchangeable records for monitoring and compliance.

Performance and Scalability: To handle numerous concurrent transactions while maintaining low latency and optimal performance, the architecture will take scalability into consideration.

Exclusions: The project excludes the creation of speculative financial instruments or cryptocurrency-based banking features. Fiat currency transactions and conventional banking operations continue to be the main focus.

Regulatory Compliance: The system will be built to adhere to current financial regulations, including data protection laws, AML (Anti-Money Laundering), and KYC (Know Your Customer).

II. Literature Survey

Secure banking systems using blockchain technology have been widely studied to enhance transaction security, transparency, and efficiency. Several researchers have explored different approaches to integrate blockchain into banking systems.

Karthikeyan et al. [1] explored blockchain as a decentralized ledger to enhance banking security. The study emphasized key features such as immutability, transparency, and tamper-proof records, which help in preventing fraudulent activities. The authors also discussed the use of smart contracts to automate compliance processes and reduce human errors. However, the study highlighted scalability challenges when dealing with high-volume banking transactions.

Sharma and Gupta [2] focused on integrating blockchain technology into core banking operations to eliminate single points of failure. Their work highlighted the importance of cryptographic hashing and distributed consensus mechanisms in securing transactions. Additionally, the authors analysed the potential of blockchain to streamline Know Your Customer (KYC) processes, thereby reducing redundancy across multiple banking institutions.

Mehta et al. [3] proposed a blockchain-based secure banking framework using a permissioned blockchain model for interbank settlements. The system ensured data privacy through role-based access control while maintaining transparency and auditability. The authors demonstrated through a prototype that their approach reduced transaction latency and improved fraud detection compared to traditional centralized banking systems.

Thomas and Reddy [4] examined the role of blockchain in enhancing security against cyberattacks in digital banking. The study discussed advanced mechanisms such as multi-signature authentication, real-time monitoring, and decentralized identity management. The authors concluded that integrating blockchain with artificial intelligence-based anomaly detection can significantly reduce phishing and man-in-the-middle attacks.

III. Problem Statements

Statement **-** Traditional banking systems are vulnerable to security threats, data breaches, and internal fraud due to centralized architecture. There is a pressing need for a secure, decentralized system that ensures transparency, integrity, and efficiency in banking operations.

Explanation **-** Conventional banking systems mainly rely on centralized architectures, in which customer data, transactions, and other banking operations are managed by a single organization or centralized server. This model makes the system extremely susceptible to security risks like cyberattacks, data breaches, and internal fraud because it establishes a single point of failure even though it permits control and coordination. Sensitive financial data can be accessed without authorization by hackers who target central

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

servers, and malicious insiders can alter data or transactions covertly. Furthermore, centralized systems frequently lack complete transparency, which makes it challenging to quickly identify the source of mistakes or fraudulent activity. A decentralized solution that disperses data among several secure nodes, like blockchain technology, is therefore becoming more and more necessary. These systems guarantee data integrity and transparency by collectively verifying transactions and recording them in an unchangeable ledger. It becomes very difficult for attackers or insiders to change records or manipulate data covertly because no single party controls the entire system. Additionally, automation via cryptographic verification and smart contracts improves operational security and efficiency, providing a strong substitute for conventional banking infrastructure.

Motivation:

- To switch from centralized to decentralized banking transactions.
- To develop a single platform that uses blockchain authentication to grant users access to all bank accounts.
- To remove any reliance on tangible items that are necessary for banking transactions.
- We observe that data recovery from various attacks is automatically provided by the decentralized architecture.
- A multi-user system prototype for controlling access to datasets kept in amazing cloud environments is presented by the Al system.
- Cloud storage necessitates secure information sharing, just like other unreliable environments.
- Without requiring the provider to make an investment, our method offers access control over data stored in the cloud.
- Making the transition from centralized to decentralized financial transactions.
- To create a single platform that allows users to access all bank accounts using blockchain authentication.
- To eliminate the need for physical goods in order to conduct bank transactions.

We note that the decentralized architecture automatically provides data recovery from various attacks. As Ilya Sukhodolski put it. The Al system presents a multi-user system prototype for managing access to datasets stored in amazing cloud environments. Like other unstable environments, cloud storage requires secure information sharing. Our approach provides access control over data stored in the cloud without requiring the provider to invest.
We observe that data recovery from various attacks is automatically provided by the decentralized architecture. As stated by Ilya Sukhodolski. A multi-user system prototype for controlling access to datasets kept in amazing cloud environments is presented by the Al system. Cloud storage necessitates secure information sharing, just like other unreliable environments. Without requiring the provider to make an investment, our method offers access control over data stored in the cloud.

IV. METHODOLOGY

This design methodology, characterized by its architectural and concept-driven nature, represents a robust framework for developing complex, regulatory-compliant distributed systems, such as a banking solution built on blockchain technology. The entire process follows a structured, top-down, modular decomposition approach, ensuring the system is built on solid, logically separated foundations.

Phase 1: Foundational Architectural Selection The initial and most critical step involved defining the core problem space and making a fundamental architectural choice. Core **Challenge Definition:** The methodology started by clearly identifying the inherent tension between blockchain's decentralization and immutability and the non-negotiable requirements of banking—specifically, strict access control and regulatory rigor (e.g., KYC, AML). Architectural **Choice:** This challenge directly led to the selection of a Permissioned Blockchain Model as the foundational architecture. This choice is concept-driven, as it allows for the integration of: Immutability and Transparency (from blockchain) Identifiable Participants, Role-Based Access Control (RBAC), and Governance (required by banking regulation).

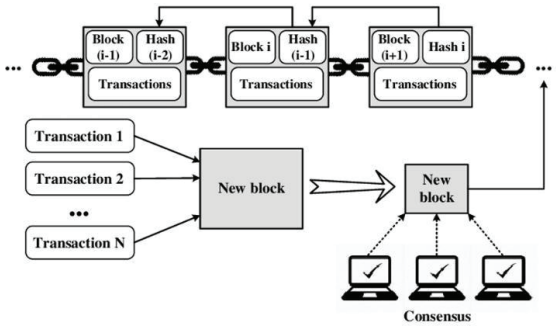

Fig.2.Work Flow of BCT in banking system

Phase 2: Layered Decomposition and Modularity Following the architectural selection, the system is broken down into specialized, manageable components using layered decomposition. This modularity is key to maintainability, security, and parallel development. The responsibilities were logically separated into distinct architectural layers, including:
Ledger/Data Layer: Responsible for the secure, immutable storage of all transaction records. This layer guarantees data integrity and traceability.
Consensus Layer: Manages the agreement mechanism among participating nodes, ensuring that all validated transactions are uniformly added to the ledger, thereby preventing double-spending and unauthorized state changes.
Smart Contracts Layer: The core logic execution environment where business rules, including crucial regulatory checks, are codified. Identity and Access Management (IAM) Layer: Governs the identity verification and authorization levels for all participants and nodes within the permissioned network.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Phase 3: Design and Functional Specification - Novelty During this stage, the focus was on adding novel design components that improve the system above a traditional blockchain-based implementation. The goal was to incorporate elements that offer both technological progress and regulatory dependability in a regulated financial setting.

The incorporation of Compliance - Embedded Smart Contracts, in which regulatory policies are explicitly encoded into the contract logic, is a key innovation of the suggested design. Rules like transaction thresholds, user permissions, and permitted counterparties are automatically validated at the time of execution rather than being checked externally or after transactions take place. This eliminates delays and minimizes inconsistencies linked to compliance by guaranteeing that all network operations are intrinsically compliant with regulations.

The makes use of the blockchain's built-in transparency while abiding by the privacy rules of the permissioned architecture. Strict Functional Conditions: At this stage, these additional elements needed to be precisely and thoroughly described. This guarantees that the new features are both technically sound and fully compliant with all regulatory requirements. This is essential for operational integrity and regulatory acceptance because it allows flexibility, transparency, and traceability across all operational workflows. The system is safe, well-designed, decentralized, and unchangeable because to this thorough, three-phase process.

V. RESULT

The project's outcomes show that blockchain technology may be successfully used to create a decentralized, transparent, and safe banking system. Several long-standing issues with traditional banking systems are successfully mitigated by the implemented solution, including the dependence on human verification procedures, the dangers associated with centralized databases, and the absence of end-to-end transaction visibility. Key financial processes, including loan approvals, transaction validation, and client verification, are carried out automatically through the integration of smart contracts, cutting down on processing time and greatly decreasing human error.

Consensus techniques and cryptographic identity management, which cooperate to guarantee that each transaction is verified, unchangeable, and permanently recorded, were used to validate the platform's security and dependability. Sensitive financial data cannot be accessed or altered by unauthorized parties thanks to these security measures, which also preserve excellent data integrity. Performance reviews demonstrate gains in auditability, compliance monitoring, and overall operating efficiency under actual usage situations, underscoring the system's resilience.

Practically speaking, the suggested blockchain-enabled banking model is ideal for contemporary financial ecosystems looking to improve regulatory alignment, security, and trust. Digital identity verification, loan and asset management, retail and corporate banking, and cross- border payment processing are just a few of the areas in which the system can be successfully used. Additionally, its extensible and modular architecture facilitates smooth interaction with current banking infrastructure while providing the flexibility required to adjust to new financial technologies and changing market demands. Overall, the project's findings demonstrate that a blockchain- powered banking system can provide an alternative to traditional financial platforms that is more safe, responsible, and prepared for the future.

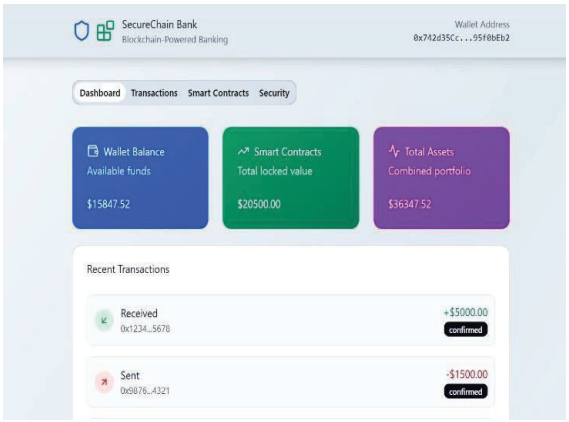

Fig.3. Dashboard of Secured Banking System

The project successfully validates the concept of a hybrid financial system, combining the efficiency of DLT with the control mandated by global regulators. One of the main economic drivers for future adoption is its potential to unlock billions in cost savings through back-office automation.

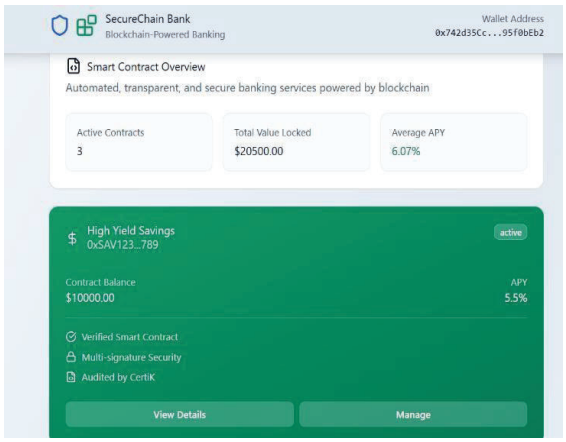

Fig.4. Usage of Smart Contract

The outcomes of the suggested system provide crucial information on how blockchain technology can change the operational framework and security of contemporary financial settings. A significant change from conventional manual workflows to rule-driven, self-executing operations is demonstrated by the effective automation of key activities through smart contracts. In addition to minimizing operational delays, this shift lessens reliance on human intervention, which is frequently the cause of mistakes and irregularities in traditional banking systems. The results support the idea that financial services dependability and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

consistency are much improved by directly integrating preset logic into the transaction layer. The enhancements in data security and integrity further show how blockchain technology might solve persistent flaws in centralized financial systems.

The system successfully removes single points of failure and lowers the likelihood of unauthorized tampering by dispersing data across a network of nodes and safeguarding it with cryptographic techniques. This is especially important in a time when financial institution cyberattacks are become more common and sophisticated. Performance testing's resilience indicates that blockchain's consensus- driven validation may offer a solid basis for delicate financial operations. When assessing the efficacy of the suggested blockchain-based financial system, transparency and regulatory alignment become crucial factors. Regulators, auditors, and authorized stakeholders may confirm financial activities with total clarity thanks to the platform's immutable ledger and real-time auditability. Compared to traditional systems, where oversight frequently relies on delayed, disjointed, or manually produced reports, this represents a substantial improvement. The system improves regulatory compliance, speeds up dispute resolution, and builds institutional confidence by providing ongoing visibility into transaction histories.

The architecture's potential for wider applicability outside of the banking industry is further highlighted by its scalability and versatility. The system's modular and interoperable design allows it to easily integrate with the current financial infrastructure while still being adaptable enough to take into account new features and regulatory upgrades. It may easily expand into industries including corporate finance, international payment networks, and retail services. Because of its scalability, the solution is positioned as a long-term, sustainable strategy that may change in tandem with improvements in global compliance requirements and financial technologies.

Nonetheless, the conversation also takes into account a number of useful factors for practical implementation. Organizational preparedness, regulatory permissions, and interoperability issues must all be carefully considered for effective deployment. To fully adopt blockchain-driven operations, financial institutions might need to train staff, update legacy workflows, and restructure important procedures. There may be brief operational challenges while moving from centralized to decentralized systems, particularly when integrating with current tools and data repositories. Notwithstanding these difficulties, the examination as a whole show that blockchain-enabled banking provides a considerably more safe, transparent, and forward-thinking substitute for conventional financial structures. Its integrated auditability, improved data security, and automation features offer a convincing method to update the financial ecosystem while promoting increased efficiency and confidence.

REFERENCES

[1] Casino. F., Dasaklis, T. K., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open Issues. Telematics and Informatics, 36, 55–81.

[2] Mylrea M., & Gourisetti, S. N. G. (2020). Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Opportunities. IEEE Transactions on Engineering Management, 67(3), 939–948.

[3] Xu. X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2020). A Taxonomy of Blockchain-Based Systems for Architecture Design IEEE Transactions on Software Engineering, 46(3), 477–498.

[4] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2021). Blockchain Technology Overview. NIST Special Publication 800-215.

[5] Christidis, K., & Devetsikiotis, M. (2021). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 8, 211071–211084.

[6] Zyskind, G., Nathan, O., & Pentland, A. (2020). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security & Privacy, 18(4).

[7] Dubey, R., Gunasekaran, A., Childe, S. J., & Wamba, S. (2021). Blockchain Technology Adoption, Architecture, and Sustainability Impact in Supply Chains.

[8] Al-Jaroodi, J., & Mohamed, N. (2020). Blockchain in Industries: A Survey. IEEE Access, 7, 36500–36515.

[9] Sharma, P., & Mehrotra, D. (2022). Blockchain Technology in Banking Sector: Opportunities and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering.