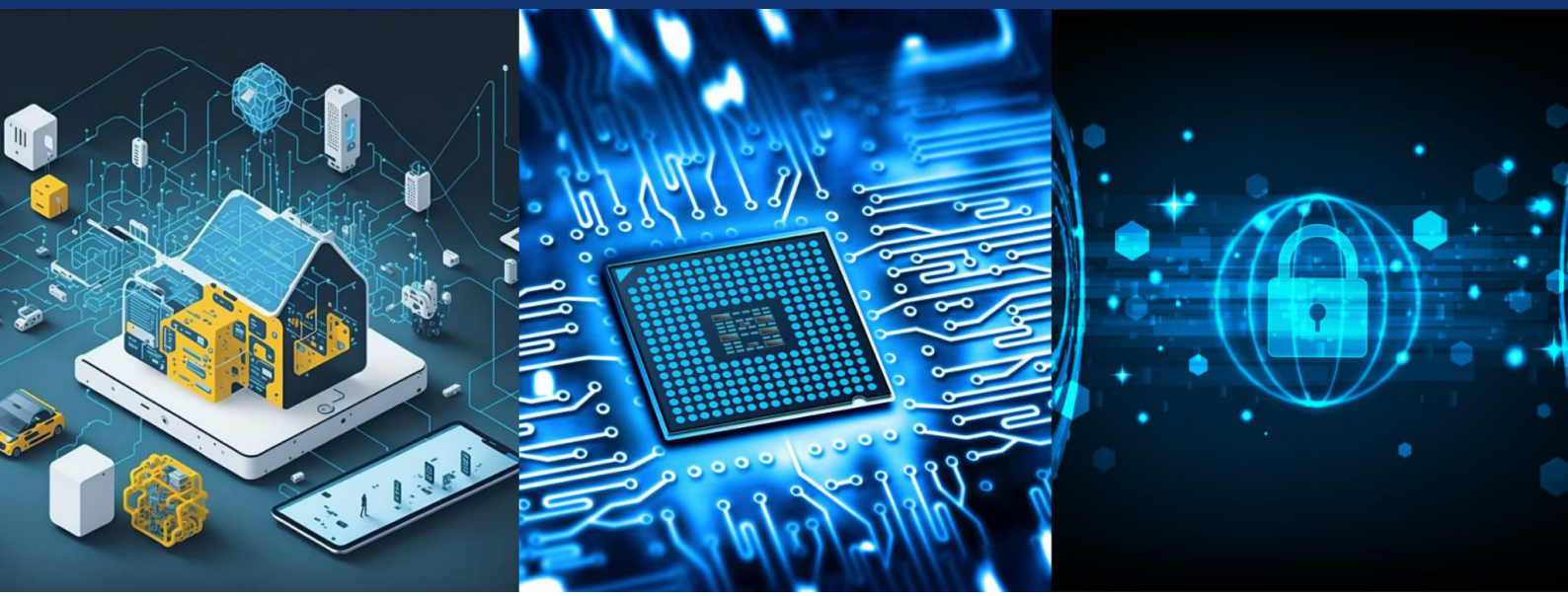
IJIRCCE

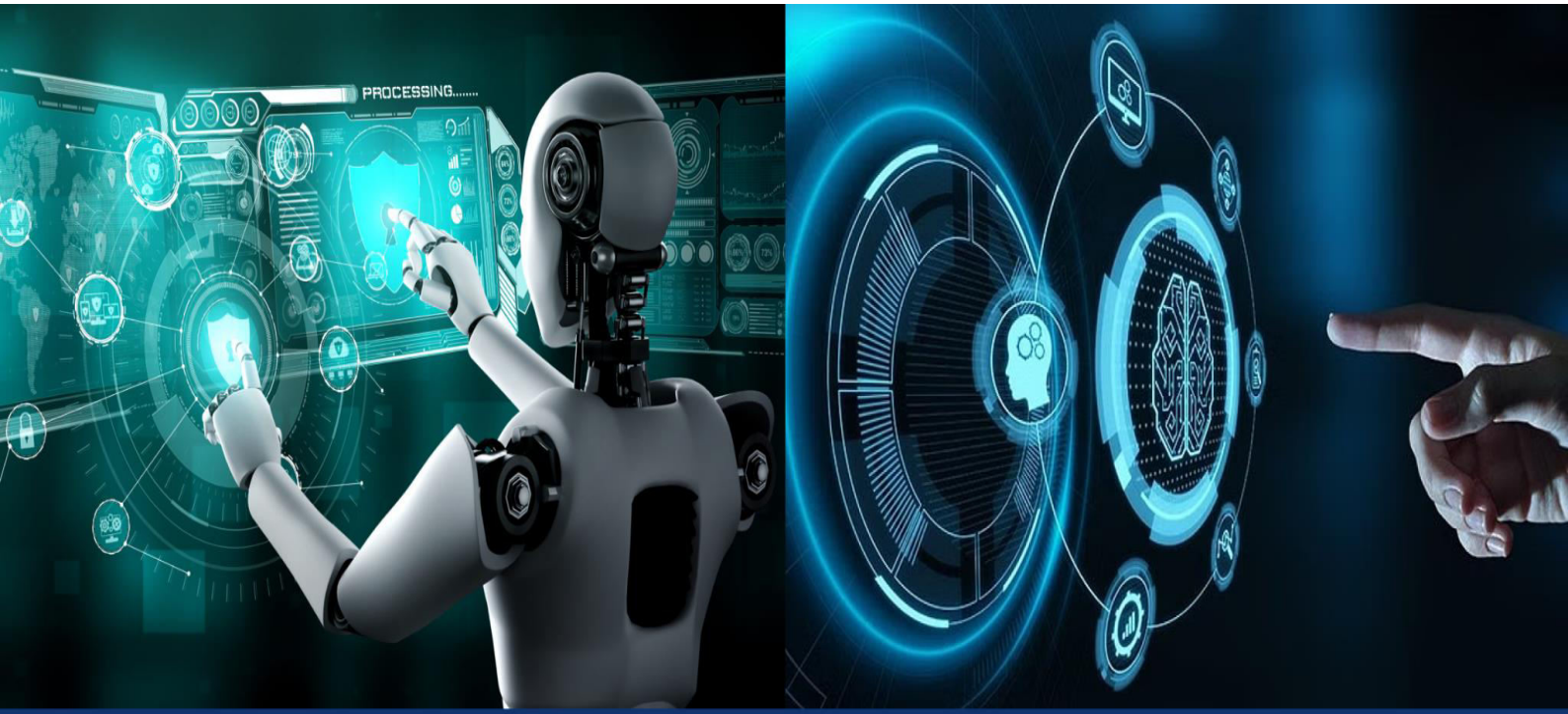
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

ChainSecure: Blockchain Based Secure Transaction and Anti Money Laundering System

Buddhapriya Meghana[1], Chandapur Ganesh[2], K. Sunitha[3], Dr V. Subbaramaiah[4], Dr K. Rajitha[5]

Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India[1, 2]

Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India[3, 4, 5]

ABSTRACT: ChainSecure is a blockchain-based system designed to provide secure, transparent, and reliable digital transactions. It uses smart contracts to execute and record transactions on an immutable ledger, ensuring data integrity and preventing tampering. The system integrates KYC verification to allow only authorized users and an AML module to detect and prevent suspicious activities through rule-based monitoring and automated actions. MetaMask is used for secure wallet-based authentication and transaction signing, eliminating the need for traditional login methods. The platform also includes user and admin dashboards for easy interaction, monitoring, and management of transactions, KYC processes, and AML rules. Additionally, the system maintains audit logs and real-time notifications to enhance traceability and user awareness. By combining frontend, backend, and blockchain technologies, ChainSecure provides a secure, efficient, and scalable solution for modern financial systems while ensuring transparency, compliance, and fraud prevention. It demonstrates the practical application of blockchain technology in building secure and trustworthy financial platforms.

KEYWORDS: Blockchain; Secure Transactions; Decentralized Finance; Anti-Money Laundering (AML); Digital Financial Operations; Digital Finance.

I. INTRODUCTION

The rapid growth of digital financial systems has made transactions faster and more convenient, but it has also increased the risk of fraud, identity theft, and money laundering. Traditional systems rely on centralized databases, which are vulnerable to data breaches, manipulation, and lack of transparency. This creates a need for a more secure and reliable system to handle financial transactions.

Blockchain technology offers a solution by providing a decentralized and immutable ledger where all transactions are recorded securely. In this project, ChainSecure uses blockchain to ensure transparency and prevent data tampering. Smart contracts are used to automate transaction execution, while MetaMask enables secure wallet-based authentication.

In addition, the system integrates KYC (Know Your Customer) for user verification and AML (Anti-Money Laundering) to monitor and detect suspicious activities. These features help in preventing fraud and ensuring compliance. Overall, the project aims to provide a secure, transparent, and efficient platform for digital financial operations.

II. RELATED WORK

A. Blockchain-Based Financial Transaction Systems

Blockchain-based financial systems have gained importance due to their decentralized and secure nature. These systems record transactions on a distributed ledger, ensuring transparency and preventing data tampering. They reduce the need for intermediaries and improve trust in digital transactions. However, many existing systems face challenges related to scalability and real-time processing.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. Smart Contracts for Secure Transactions

Smart contracts are widely used to automate financial transactions in a secure and reliable manner. They execute predefined conditions without human intervention, reducing errors and fraud. Many research works highlight their role in ensuring trust and efficiency in blockchain-based applications. However, improper design of smart contracts can lead to vulnerabilities and security risks.

C. Anti-Money Laundering (AML) Detection in Financial Systems

AML systems are used to detect suspicious financial activities and prevent fraud. Traditional AML approaches use rule-based or machine learning techniques to analyze transaction patterns. While these systems improve fraud detection, they often require high computational resources and may not work efficiently in real-time scenarios. Integrating AML with blockchain can enhance transparency and monitoring.

III. PROPOSED SYSTEM

The proposed system, ChainSecure, is a blockchain-based platform designed to provide secure and transparent financial transactions. It integrates KYC verification to ensure that only authorized users can access the system and AML mechanisms to detect and prevent suspicious activities. Transactions are executed using smart contracts and stored on an immutable blockchain ledger. The system also includes user and admin modules for efficient management, monitoring, and control, ensuring a safe and reliable financial environment.

A. System Architecture

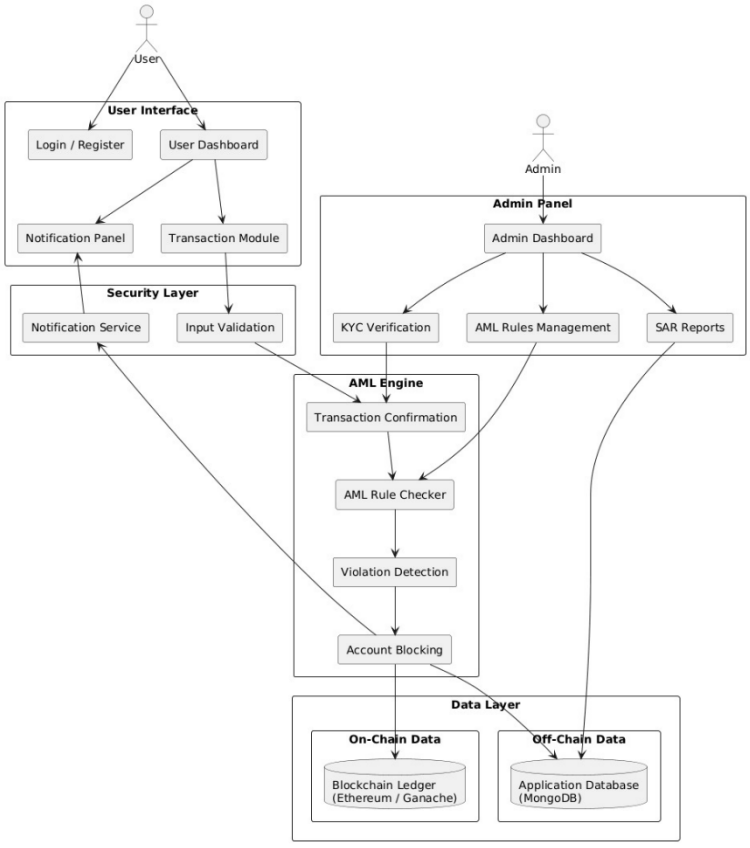


Figure 1: System architecture of Chainsecure: Blockchain Based Secure Transaction and Anti Money Laundering System.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This Figure 1 represents the overall architecture of the ChainSecure system, showing how different components interact to ensure secure transactions. The system mainly consists of the User Interface, Admin Panel, Security Layer, AML Engine, and Data Layer.

At the top, the User interacts with the system through the user interface, which includes login/register and user dashboard. From the dashboard, users can perform transactions and view notifications. The Admin manages the system through the admin panel, where they handle KYC verification, manage AML rules, and monitor suspicious activity reports (SAR).

The Security Layer ensures safe operation by validating user inputs and sending notifications. The AML Engine is the core component that processes transactions, checks them using AML rules, detects violations, and blocks accounts if suspicious activity is found. Finally, the Data Layer stores information, where blockchain (on-chain) stores transaction records and the database (off-chain) stores user and application data. This overall flow ensures that the system is secure, transparent, and efficient.

B. Process Flow Diagram

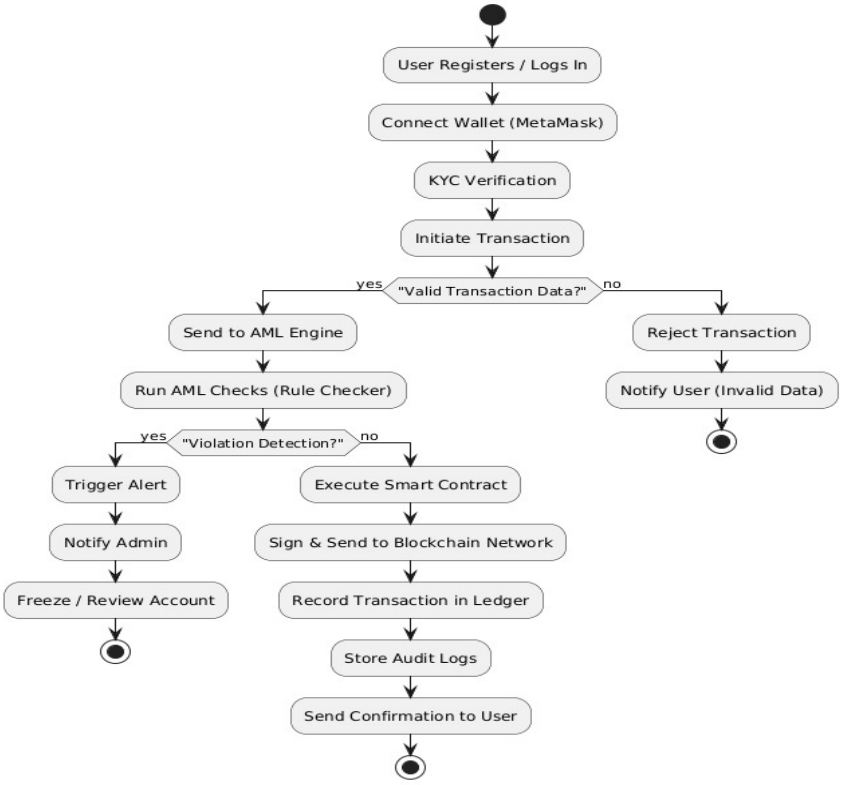


Figure 2: Process Flow Diagram of Chainsecure: Blockchain Based Secure Transaction and Anti Money Laundering System.

This Figure 2 represents the working flow of the ChainSecure system from user action to transaction completion. The process starts when the user registers or logs in and connects their wallet using MetaMask. After completing KYC verification, the user initiates a transaction, which is first checked for valid input data.
If the transaction data is invalid, it is rejected and the user is notified. If valid, the transaction is sent to the AML engine where rule checks are performed. If any violation is detected, an alert is triggered, the admin is notified, and the user account may be frozen or reviewed.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

If no violation is found, the transaction is executed using a smart contract, signed, and sent to the blockchain network. The transaction is then recorded in the ledger, audit logs are stored, and a confirmation is sent to the user. This flow ensures secure, verified, and transparent transaction processing.

IV. IMPLEMENTATION

The ChainSecure system is implemented by integrating multiple components to provide secure and transparent financial transactions. The system follows a modular approach where the frontend, backend, blockchain, and database work together to ensure smooth operation. Users interact with the system through a web interface, while the backend processes requests and communicates with the blockchain. Smart contracts handle transaction execution, and the AML module ensures fraud detection. This integrated implementation provides a secure, reliable, and efficient system.

A. Frontend Implementation

The frontend is designed to provide an easy and user-friendly interface for users and administrators. It is developed using Next.js (React) for building dynamic UI and Tailwind CSS for responsive design. It allows users to register, login, connect their wallet, perform transactions, and submit KYC details. Admins can monitor users, verify KYC, and manage AML rules through the dashboard. The frontend communicates with the backend using APIs and integrates with blockchain using Ethers.js for smooth interaction.

B. Backend Implementation

The backend handles the core logic of the system, including user authentication, KYC verification, AML processing, and API management. It is developed using Node.js and Express.js, which provide a scalable and efficient server environment. It validates user inputs, processes transactions, and communicates with the blockchain network. The backend also manages notifications and ensures secure data handling using JWT authentication and other security mechanisms.

C. Blockchain Implementation

Blockchain is used to execute and store transactions securely using smart contracts. It is implemented using Ethereum blockchain and Solidity for smart contract development. Each transaction is recorded on an immutable ledger, ensuring transparency and data integrity. The system uses Ganache for local blockchain testing and MetaMask for wallet-based authentication and transaction signing.

D. Database Implementation

The database is used to store user information, KYC details, AML logs, and application data. The system uses MongoDB as a NoSQL database for efficient data storage and retrieval. While transaction data is stored on the blockchain, other system-related data is stored off-chain in the database. This ensures faster access and better performance while maintaining security.

E. Limitations of Existing Systems

Existing systems have several limitations such as lack of transparency, dependency on centralized control, and vulnerability to fraud and data breaches. Many AML solutions are complex and may not provide real-time detection, while some blockchain systems face issues like scalability and high cost. These challenges highlight the need for a more integrated and efficient solution.

V. FORMULAS

A. Transaction Velocity Detection

This formula is Used to detect unusually frequent transactions in a short time window.

timeWindow = timeWindowMinutes * 60 * 1000

timeWindowStart = currentTime - timeWindow

transactionCount = count(transactions where timestamp >= timeWindowStart) + 1

B. Behavioral Deviation Analysis

This formula is Used to Detects abnormal transaction amounts compared to user history.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

avgAmount = Σ(last 20 transactions) / min(20, total_transactions)
deviationPercentage = (currentAmount / avgAmount) × 100

C. Round Number Pattern Detection

This formula helps detect transactions that contain round number amounts, often used in structured financial activity.
isRoundNumber = (amount === Math.floor(amount)) AND (amount ≥ 10)
roundTxCount = count(round transactions in last 24 hours)

VI. ALGORITHMS

A. ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA is used in the system to verify the authenticity of transactions. It ensures that only the actual owner of the wallet can authorize a transaction using their private key. The corresponding public key is used to validate the signature, providing security and preventing unauthorized access.

Input: Transaction Message *M*, User Private Key *K_priv*, Public Key *K_pub*

Output: Valid or Invalid Transaction Authorization

```
function ECDSA_VERIFY(M, K_priv, K_pub)
    if wallet is not connected then
        request user to connect MetaMask wallet
    end if

    Compute message hash H ← SHA256(M)
    Generate digital signature (r, s) using K_priv
    Send signature (r, s) and message M for verification
    Verify signature using K_pub

    if signature is valid then
        return Transaction Authorized
    else
        return Transaction Rejected
    end if
end function
```

B. SHA (Secure Hash Algorithm)

SHA-256 is used to maintain the integrity of transaction data. It converts input data into a fixed-length hash value, making it impossible to alter the data without changing the hash. This ensures that any tampering with transaction data can be easily detected.

Input: Transaction Data *T*

Output: Hash Value *H_hex*

```
function SHA_HASH(T)
    if T is not a string then
        convert T to serialized string format
    end if

    Compute SHA-256 hash H ← SHA256(T)
    Encode H as hexadecimal string H_hex
    Store transaction T in application database
    Anchor H_hex in blockchain ledger for integrity verification

    return H_hex
end function
```

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. RESULTS AND DISCUSSION

A. Home Page of ChainSecure

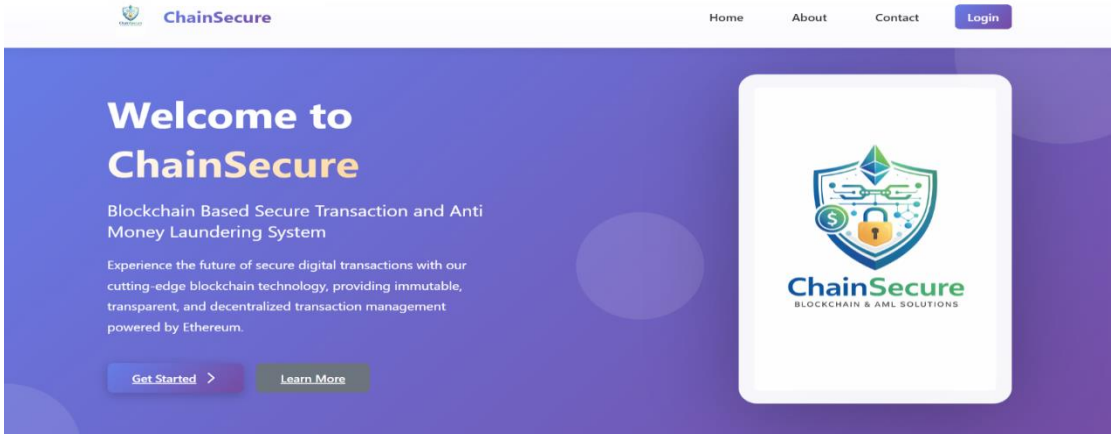


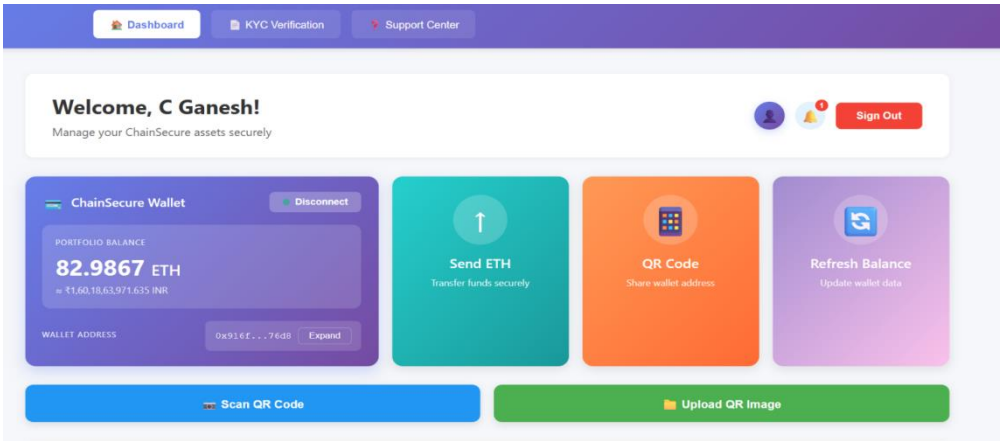
Figure 3: Home page of ChainSecure: Blockchain Based Secure Transaction and Anti Money Laundering System

This Figure 3 shows the home page of the ChainSecure system. It introduces the project and its purpose of providing secure blockchain-based transactions. The page includes navigation options, a brief description, and buttons like “Get Started” and “Learn More” for user interaction

B. User Dashboard

This Figure 4 shows the user dashboard of the ChainSecure system. It displays wallet details such as balance and wallet address, and provides options like sending ETH, generating QR code, and refreshing balance. Users can perform transactions and manage their wallet securely through this interface Laundering

Figure 4: User Dashboard of Chainsecure: Blockchain Based Secure Transaction and Anti Money



C. Admin Dashboard

This Figure 5 shows the overview section of the admin dashboard in the ChainSecure system. It displays key information such as total users, active users, and recent transaction activity. The admin can use this panel to monitor the system, track user activity, and manage different modules like users, AML rules, KYC, and reports. This helps in efficient system control and monitoring.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404110

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

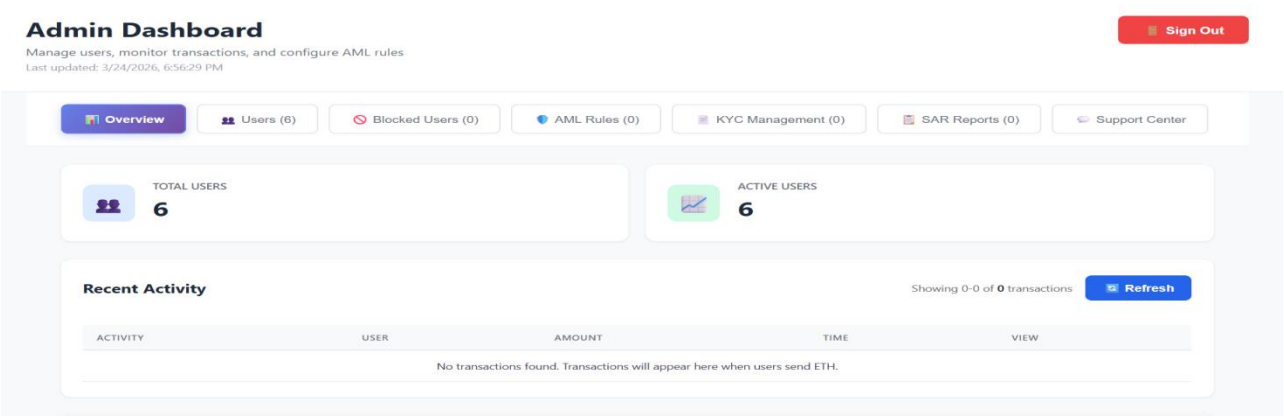


Figure 5: Admin Dashboard of Chainsecure: Blockchain Based Secure Transaction and Anti Money Laundering System.

D. Ganache Transaction Details

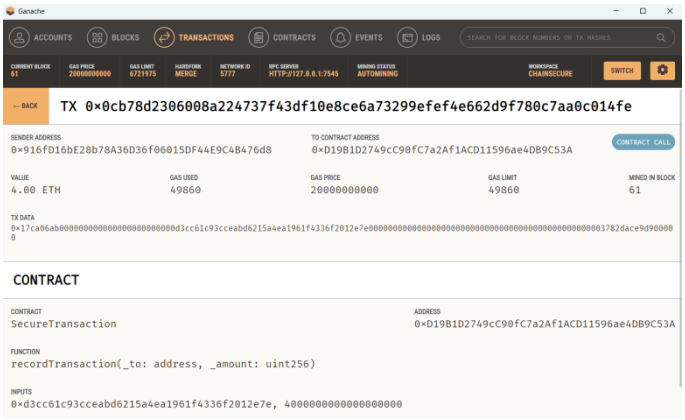


Figure 6: Ganache Transaction Details

This Figure 6 shows the transaction details in the Ganache blockchain environment. It displays important information such as sender address, contract address, transaction value, gas used, and block number. The transaction is executed through a smart contract function, and all details are recorded on the blockchain. This helps in verifying that the transaction is successfully processed and stored securely in the system.

VIII. CONCLUSION AND FUTURE SCOPE

A. CONCLUSION

The ChainSecure system successfully demonstrates a secure, transparent, and efficient platform for digital financial transactions using blockchain technology. It ensures data integrity through an immutable ledger, making transactions tamper-proof and trustworthy. The integration of KYC verification restricts system access to authenticated users, reducing identity-related risks. The AML module enhances security by monitoring transactions, detecting suspicious activities, and preventing fraud through automated actions such as account blocking. Smart contracts enable automated and reliable transaction execution without intermediaries, improving efficiency and reducing errors. Additionally, user and admin dashboards provide easy interaction, monitoring, and management of system activities. Overall, the system effectively combines blockchain and security mechanisms to deliver a reliable and fraud-resistant financial solution.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. FUTURE SCOPE

The ChainSecure system can be further enhanced by integrating advanced technologies and expanding its capabilities for real-world applications. Machine learning and AI techniques can be incorporated to improve AML detection accuracy and identify complex fraud patterns. The system can be deployed on public blockchain networks like Ethereum mainnet to increase scalability and usability. Additional features such as mobile application support, multi-currency transactions, and cross-chain interoperability can make the system more flexible and widely accessible. Real-time analytics dashboards can be added to provide better insights into system performance and transaction behavior. Security can be further strengthened using advanced techniques such as multi-factor authentication, biometric verification, and zero-knowledge proofs. These improvements will make the system more scalable, secure, and suitable for large-scale financial environments.

REFERENCES

1. V. Femiak and K. Košťál, "Zero-Knowledge Proofs in Anti-Money Laundering Multiparty Computation," 2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Pisa, Italy, 2025, pp. 1-3. DOI: 10.1109/ICBC64466.2025.11114560
2. Constantinides, Theodoros & Cartlidge, John. (2025). zkMixer: A Configurable Zero-Knowledge Mixer with Anti-Money Laundering Consensus Protocols. 111-120 DOI: 10.1109/DAPPS65174.2025.00022
3. Muntean, Otilia & Pungila, Ciprian. (2025). Unmasking Blockchain Fraud: A Review of Aml Challenges and Regulatory Shortcomings. 000051-000056 DOI: 10.1109/SACI66288.2025.11030173
4. J. Song, S. Zhang, P. Zhang, J. Park, Y. Gu and G. Yu, "Illicit Social Accounts? Anti-Money Laundering for Transactional Blockchains," in IEEE Transactions on Information Forensics and Security, vol. 20, pp. 391-404, 2025, DOI: 10.1109/TIFS.2024.3518068
5. Z. Li, R. Yao, D. Yang, Y. Zhang, H. Mao and Y. Yuan, "BELFAL: A Blockchain based Ensemble Learning Framework for Anti-money Laundering in Crypto-Currency Markets," 2024 IEEE 30th International Conference on Parallel and Distributed Systems (ICPADS), Belgrade, Serbia, 2024, pp. 520-527, DOI: 10.1109/ICPADS63350.2024.00074
6. M. F. A. Al Sohan, A. Nahar, R. Al Mamun Rudro, M. H. Uddin, M. J. A. Aurnob and K. Nur, "AMLChain: An Automated Blockchain Model Architecture For Anti Money Laundering in Banking Industry," 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET, Sydney, Australia, 2024, pp. 1-6, DOI: 10.1109/ICECET61485.2024.10698295
7. J. R. de Oliveira and A. G. Leal, "An Anti-Money Laundering Approach for the Brazilian Smart Contract/Digital Currency (DREX) Platform," 2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Berlin, Germany, 2024, pp. 1-4. DOI: 10.1109/BRAINS63024.2024.10732715
8. B, Divya & P, Thara & S., Kavitha & Ancy, Alvin & R, Preethi & D, Dhanalakshmi. (2024). An Effective Anti-Money Laundering System Using Block Chain Technology. 209-214 DOI: 10.1109/ICSSEECC61126.2024.10649485
9. T. Masitoh and Y. Yunanto, "Analysis of Implementation of Anti-Money Laundering Mechanisms in Blockchain-Based Smart Contracts under Indonesian Regulation," International Journal of Social Science and Human Research, vol. 7, no. 9, 2024, pp. 7027-7032. DOI: 10.47191/ijsshr/v7-i09-35
10. O. S. Owolabi, E. Hinneh, P. C. Uche, N. T. Adeniken, J. A. Ohaegbulem, S. Attakorah, O. G. Emi-Johnson, C. S. Belolisa and H. Nwariaku, "Blockchain-Based System for Secure and Efficient Cross-Border Remittances: A Potential Alternative to SWIFT," Journal of Software Engineering and Applications, vol. 17, 2024, pp. 664-712. DOI:10.4236/jsea.2024.178036
11. E. Pappa, P. Georgitseas and G. Tantis, "Exploring the Role of Blockchain Technology in Anti-Money Laundering," Journal of Legal, Ethical and Regulatory Issues, vol. 27, no. S3, 2024, pp. 1-10. DOI: 1544-0044-27-S3-015
12. K. Koo, M. Park and B. Yoon, "A Suspicious Financial Transaction Detection Model Using Autoencoder and Risk-Based Approach," IEEE Access, vol. 12, 2024, pp. 68926–68939. DOI: 10.1109/ACCESS.2024.3399824
13. V. Nakonechnyi, S. Toliupa, V. Saiko, V. Lutsenko, G. S. N. Ghno and A. K. Hussain, "Blockchain Implementation in the Protection System of Banking System During Online Banking Operations," 2024 35th Conference of Open Innovations Association (FRUCT), Tampere, Finland, 2024, pp. 492-500.DOI: 10.23919/FRUCT61870.2024.10516404
14. C. R. Lakireddy, Princi, K. Pal, M. K. Singh and A. S. Verma, "The Blockchain Paradigm: Revolutionizing Banking Systems with E-KYC Integration," 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN), Greater Noida, India, 2024, pp. 525-530. DOI: 10.1109/EmergIN63207.2024.10961377

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

15. K. Singh and S. M. Hiremath, "Blockchain-Based Smart Contracts for Secure and Efficient Financial Transactions in Digital Banking," Proceedings of TEMSCON-ASPAC (IEEE TEMSCON-ASPAC), 2023, pp.1-5. DOI: 10.1109/TEMSCON-ASPAC59527.2023.10531368
16. Raj, A. Kumar, V. Sharma, S. Rani and A. K. Shanu, "Enhancing Security Feature in Financial Transactions using Multichain Based Blockchain Technology," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp.16, DOI: 10.1109/ICIEM59379.2023.10166589
17. Aashima, I. Chandrasekeran, A. Rana, S. Naredla, W. K. Ibrahim and M. Bader Alazzam, "Blockchain Technology for Secured Transactions in Banking," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, 660, DOI: 10.1109/ICACITE57410.2023.10182668 India, 2023, pp. 655
18. Y. Yu, J. Wu, D. Lin and Q. Fu, "Money Laundering Detection on Ethereum: Applying Traditional Approaches to New Scene," Proceedings of the 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS), vol. –, 2023, pp. 1759–1766. DOI: 10.1109/ICPADS60453.2023.00244
19. V. C. Achebe, O. Ilori and N. J. Isibor, "Next-Generation AML Compliance: Leveraging Blockchain Innovations to Disrupt Money Laundering Networks," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 4, no. 2, 2023, pp. 741–753. DOI: 10.54660/.IJMRGE.2023.4.2.741-753
20. Ž. Bjelajac and B. M. Bajac, "Blockchain Technology and Money Laundering," Pravo — Teorija i Praksa, vol. 39, no. 2, 2022, pp. 21–38. DOI:10.5937/ptp2202021B

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details