Archives available at journals.mriindia.com

International Journal of Advanced Scientific Research and Engineering Trends

ISSN: 2456-0774

Volume 10 Issue 03, 2026

Next-Generation Fraud Detection System Using AI And Blockchain for Real-Time Monitoring and Payment Integrity

[1]Rashmi Vilas Deshpande, [2]Dr. Ankita Karale, [3]Dr. Balkrishna K. Patil, [4]Dr. Naresh Thoutam

[1]Student, Computer Department, Sandip Institute of Technology and Research Centre, Nashik, India
[2,3,4] Dr. Computer Department, Sandip Institute of Technology and Research Centre, Nashik, India
Email: [1]rashmideshpande321@gmail.com, [2]ankita.karale@sitrc.org, [3]balkrishnapatileng@gmail.com, [4]naresh.thoutam@sitrc.org

Peer Review Information

Submission: 10 Feb 2026

Revision: 26 Feb 2026

Acceptance: 11 March 2026

Keywords

Fraud Detection, Artificial Intelligence, Explainable AI, Blockchain, Real-Time Monitoring, Payment Security, Transaction Analysis, Audit Trail, System Dashboard, Risk Assessment

Abstract

The increasing use of digital payment platforms has led to a rapid rise in financial frauds, making traditional detection systems less effective against modern attack patterns. To address this issue, this work presents a system that combines Artificial Intelligence, Explainable AI, and Blockchain into a single framework for secure and transparent fraud detection. The system is designed to analyze transactions in real time, identify suspicious activities, and maintain a tamper-proof record of decisions. The proposed system processes each transaction through an AI-based analysis module that generates a risk score. Based on this score, transactions are either approved or flagged for review. Along with the prediction, an explainability layer provides clear reasons behind each decision, improving system transparency. To ensure trust and auditability, all important transaction evidence is stored securely, with its integrity protected through blockchain-based hashing. The system also includes an interactive dashboard that allows users to monitor transaction activity, view analytics, and understand system behavior visually. Screens such as live analytics, transaction flow visualization, and performance metrics help in better understanding and managing fraud detection processes. Overall, the system focuses on delivering a practical, user-friendly, and secure solution that not only detects fraud but also builds trust through transparency and verifiable records.

Introduction

Digital payment systems have become a major part of everyday life, allowing users to perform transactions quickly and conveniently through online platforms, mobile applications, and banking services. While this shift has improved efficiency, it has also increased the risk of financial fraud and cyber threats. With a large number of transactions happening every second, even a small percentage of fraudulent activities can lead to serious financial losses and reduced trust in digital systems. [9]

Traditional fraud detection methods were mostly based on predefined rules, such as transaction limits or location-based checks. These systems were simple and fast but lacked the ability to adapt to new and evolving fraud patterns. As attackers started using more advanced techniques, including identity manipulation and intelligent transaction behavior, these rule-based systems became less effective. This created a need for systems that can learn from data and identify complex patterns automatically. [12]

Machine learning approaches improved fraud detection by analyzing transaction data and identifying unusual patterns. However, many of these models work as black boxes, making it difficult to understand why a transaction is flagged as fraudulent. This lack of transparency reduces trust among users, auditors, and regulatory bodies. At the same time, the storage of fraud-related data in traditional databases raises concerns about data tampering and reliability during audits.[1]

Another important challenge is the imbalance in transaction data, where fraudulent cases are very rare compared to normal transactions. This makes it difficult for models to detect fraud accurately without missing critical cases. In addition, real-time processing is essential, as fraud detection must happen before a transaction is completed. Delays in decision-making can either allow fraud to occur or affect user experience.[5]

To overcome these challenges, the proposed system combines Artificial Intelligence for detection, Explainable AI for transparency, and Blockchain for secure and tamper-proof record keeping. The system is designed to analyze transactions in real time, generate understandable explanations, and store evidence in a way that cannot be altered. It also provides visual interfaces and dashboards that help users and analysts monitor system performance and transaction behavior effectively.

Overall, the need for a system that is accurate, transparent, secure, and user-friendly forms the foundation of this work. The proposed solution aims to meet these requirements by integrating multiple technologies into a single, cohesive framework. [3]

Objectives Of the System

The main objective of this system is to design a secure, intelligent, and transparent fraud detection framework that can operate in real-time while ensuring data integrity and user trust. The system integrates multiple technologies to address the limitations of traditional approaches and provide a complete end-to-end solution.

The specific objectives of the system are as follows:

- To develop an intelligent fraud detection mechanism

The system aims to analyze transaction data using AI models to identify suspicious patterns and detect fraudulent activities with high effectiveness, even in highly imbalanced datasets.

- To provide explainable decision outputs

The system includes an explainability layer that generates clear and understandable reasons for each fraud prediction, helping users and analysts understand why a transaction is flagged.

- To ensure data integrity using blockchain

All important transaction evidence is securely stored and linked with blockchain-based hashing, ensuring that the data cannot be altered or tampered with during audits or investigations.

- To support real-time transaction processing

The system is designed to process transactions instantly, allowing fraud detection decisions to be made before transaction completion, without affecting system performance.

- To implement a structured dispute resolution workflow

The system supports a transparent process where disputed transactions can be tracked and verified using stored evidence and blockchain records.

- To provide an interactive monitoring interface

A user-friendly dashboard is included to visualize transaction activity, system performance, and fraud detection insights, enabling better monitoring and decision-making.

- To maintain system reliability over time

The system incorporates mechanisms to monitor changes in transaction patterns and maintain consistent performance as fraud strategies evolve.

Overall, these objectives ensure that the system is not only focused on detecting fraud but also on providing transparency, security, and usability in practical environments.

System Overview

The proposed system provides a complete and integrated solution for fraud detection and transaction monitoring by combining Artificial Intelligence, Explainable AI, and Blockchain into a unified workflow. The system is designed to handle transactions in real time, analyze their behavior, generate explanations, and securely store evidence for future verification. [10]

At a high level, the system begins with capturing transaction data from users through a digital payment interface. Each transaction is validated to ensure correctness before being passed to the core analysis module. The AI-based detection engine evaluates the transaction using learned patterns and assigns a risk score. Based on this score, the system determines whether the transaction is normal or suspicious.[8]

After the decision is made, the system generates an explanation using an explainable AI layer.

This step provides clear reasoning behind the classification, such as unusual transaction amount, new device usage, or abnormal location. These explanations help users and analysts understand system behavior and increase trust in the decision-making process.

To ensure security and transparency, the system creates an evidence record for each transaction. This record includes transaction details, prediction results, and explanation data. Instead of storing all data directly on the blockchain, the system stores it off-chain and records a cryptographic hash on the blockchain. This approach ensures that the data remains tamper-proof while maintaining system efficiency. [13]

The system also provides a monitoring interface where users can view transaction summaries, analytics, and fraud detection results. The dashboard presents information in a visual format, making it easier to understand system activity and identify suspicious patterns quickly. Additionally, the system supports a structured dispute process, allowing users to verify decisions using stored evidence and blockchain records. [17]

Overall, the system operates as a continuous pipeline where each component contributes to detection, explanation, and verification. The integration of these modules ensures that the system is not only effective in detecting fraud but also transparent, secure, and user-friendly for practical deployment.

System Architecture

The system architecture follows a layered and modular design where each component performs a specific role in the fraud detection pipeline. All layers work together to ensure real-time processing, accurate detection, transparent decision-making, and secure evidence storage.

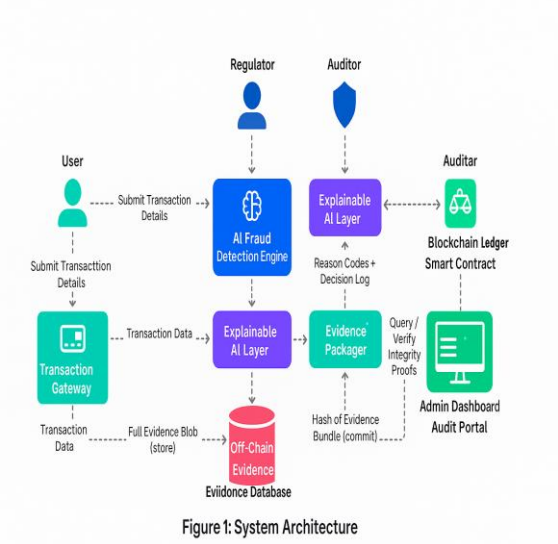

Figure 1: System Architecture

The architecture is structured into multiple functional layers, each responsible for a key operation in the system.

User and Transaction Layer

This layer acts as the entry point of the system. It captures transaction requests from users through digital payment interfaces. Basic validation checks are performed here, such as verifying input format, ensuring required fields are present, and filtering duplicate or invalid requests. Only valid transactions are forwarded to the next stage.

This layer ensures that the system starts with clean and reliable data, reducing the chances of processing errors in later stages.

AI Fraud Detection Layer

The core processing of the system happens in this layer. The validated transaction data is analyzed using machine learning models that are trained to detect fraudulent patterns. The model evaluates multiple attributes of a transaction and generates a risk score.

Based on this score, the system classifies the transaction as either legitimate or suspicious. The design focuses on maintaining high detection capability while operating within real-time constraints.

This layer is responsible for the intelligence of the system, enabling it to identify complex and evolving fraud patterns.

Explainable AI Layer

Once a prediction is made, the explainable AI layer generates human-readable explanations for the decision. Instead of providing only a result, the system highlights the key factors that influenced the outcome.

For example, the system may indicate that a transaction is suspicious due to unusual location, high transaction amount, or new device usage. These explanations help users and analysts understand system behavior and improve trust in automated decisions.

This layer plays an important role in transparency and regulatory compliance.

Evidence Management Layer

In this layer, all important outputs related to a transaction are combined into a structured evidence record. This includes transaction details, prediction results, explanation data, and model-related information.

The evidence is stored securely in off-chain storage systems. This approach allows efficient data handling while maintaining accessibility for verification and audits.

This layer ensures that every decision is backed

by complete and structured information.

Blockchain Layer
The blockchain layer is responsible for maintaining data integrity. Instead of storing full transaction data, the system generates a cryptographic hash of the evidence record and stores it on the blockchain.
This ensures that any future modification in the data can be detected by comparing hash values. The use of blockchain provides immutability, transparency, and trust, which are critical for audit and dispute resolution processes.
This layer strengthens the reliability of the entire system.

Monitoring and Dashboard Layer
The final layer provides an interface for users, analysts, and auditors. It displays transaction details, fraud alerts, system analytics, and verification results in a visual format.
Users can monitor system activity, review flagged transactions, and understand decisions through graphical representations. This improves usability and allows quick identification of suspicious patterns.
This layer connects the technical system with real-world users, making the solution practical and accessible.
Overall, the system architecture ensures smooth interaction between all components. Each layer contributes to a specific function, but together they form a complete pipeline that delivers accurate, transparent, and secure fraud detection in real time.

Methodology
The system follows a structured workflow where each transaction is processed through multiple stages, ensuring that fraud detection, explanation, and verification are performed in a coordinated manner. The workflow is designed to maintain accuracy while meeting real-time processing requirements.

Transaction Processing Flow
The workflow begins when a transaction is initiated by a user through a digital payment interface. The system captures the transaction data and performs initial validation to ensure that all required information is present and correctly formatted.
After validation, the transaction moves to the AI-based analysis stage, where relevant features are extracted and evaluated. The model computes a risk score based on learned patterns from historical data. This score determines whether the transaction is normal or suspicious.
Once the prediction is made, the system generates an explanation using the explainable AI module. This explanation identifies the key factors that influenced the decision, making the output understandable to users and analysts.

Evidence Generation and Storage
After classification and explanation, the system creates an evidence record for the transaction. This record includes transaction details, risk score, and explanation output. The evidence is structured in a way that it can be easily retrieved and verified.
The complete evidence record is stored in an off-chain storage system, ensuring efficient data handling. At the same time, a cryptographic hash of this evidence is generated and stored on the blockchain. This ensures that the stored data remains secure and cannot be altered without detection.

Decision and Response Handling
Based on the risk score, the system makes a final decision. If the transaction is classified as legitimate, it is allowed to proceed. If it is identified as suspicious, it is either blocked or flagged for further review.
The decision, along with its explanation, is returned to the user or system interface. This ensures that every action taken by the system is transparent and justified.

Dispute Resolution Workflow
In cases where a user challenges a decision, the system supports a structured dispute process. The dispute moves through different stages such as initiation, review, and resolution.
During this process, the system retrieves the stored evidence and verifies it using the blockchain hash. This ensures that the data used for decision-making is authentic and has not been modified. This workflow improves accountability and builds trust among users and regulators.

End-to-End Workflow Summary
The complete workflow can be summarized as follows:

1. Transaction input is received
2. Validation checks are performed
3. AI model evaluates transaction and generates risk score
4. Explainable AI provides reasoning for the decision
5. Evidence record is created and stored
6. Blockchain hash is generated and recorded
7. Final decision is returned
8. Dispute handling is supported if required

Overall, the methodology ensures that all system

components work together in a continuous flow. The integration of detection, explanation, and verification within a single workflow makes the system efficient, transparent, and reliable for real-world usage.

System Implementation

The system implementation focuses on how the designed framework is translated into a working application with interactive user interfaces and functional modules. This section highlights the practical realization of the system using visual screens and explains how different components operate together during execution.

Figure 2: Dashboard Overview Interface

This screen shows the main dashboard of the system where overall transaction activity is displayed. It provides a summary of key metrics such as total transactions, flagged fraud cases, and system status.

The dashboard acts as the central control panel, allowing users to monitor system performance and quickly understand the current state of fraud detection.

Figure 3: Transaction Monitoring Screen

This interface displays a list of transactions processed by the system. Each transaction includes relevant details such as amount, status, and risk classification.

It helps analysts track individual transactions and identify suspicious activities in real time, making it an essential part of operational monitoring.

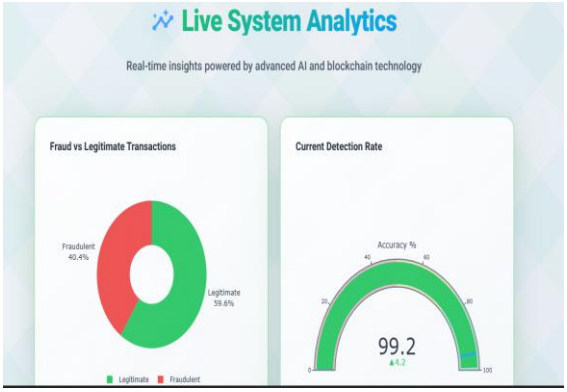

Figure 4: Fraud Detection Result Screen

This screen presents the outcome of the fraud detection process. It clearly shows whether a transaction is classified as legitimate or fraudulent.

The result is displayed along with risk indicators, helping users quickly understand the system's decision.

Figure 5: Explainable AI Output Screen

This interface provides detailed explanations for the system's decision. It highlights the key factors that contributed to the fraud classification, such as unusual behavior or abnormal transaction patterns.

This screen is important for transparency, as it allows users to understand why a particular decision was made.

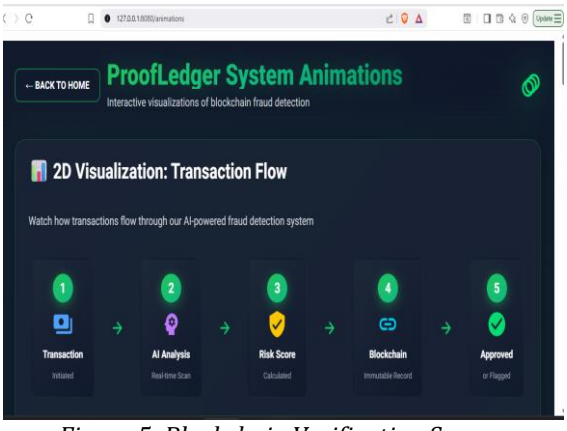

Figure 5: Blockchain Verification Screen

This screen demonstrates how transaction evidence is verified using blockchain. It shows the stored hash values and validation results.
The verification process confirms that the transaction data has not been altered, ensuring trust and integrity in the system.

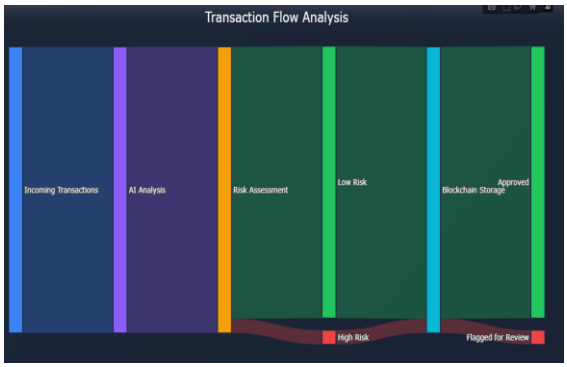

Figure 7: Transaction Flow Visualization

This interface visually represents the flow of transactions through different stages of the system, from input to final decision. It helps users understand how data moves within the system and how different modules interact during processing.

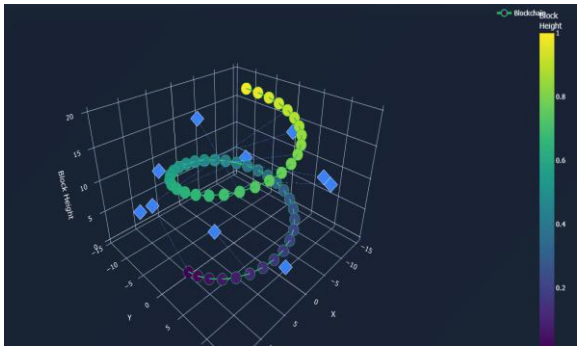

Figure 8: System Analytics and Performance Screen

This screen displays analytical insights such as trends, patterns, and system performance indicators.
It allows users to evaluate how the system is performing over time and identify any unusual patterns in transaction behavior.
The implementation demonstrates that the system is not only functional but also user-friendly. Each interface is designed to present complex information in a simple and understandable way. The combination of real-time monitoring, explainability, and blockchain verification ensures that the system is practical for real-world deployment.

Discussion

The implemented system demonstrates a practical approach to fraud detection by combining multiple technologies into a single workflow. Unlike traditional systems that focus only on detection, this framework extends its capability to explanation, verification, and user interaction. This makes the system more suitable for real-world applications where trust and transparency are equally important as accuracy.
One of the key strengths of the system is its ability to present results in a clear and understandable manner. Through the dashboard and explanation screens, users can easily interpret why a transaction is marked as suspicious. This reduces confusion and builds confidence in automated decision-making. The use of visual interfaces further improves usability, allowing even non-technical users to understand system behavior without difficulty.
The integration of blockchain adds another important dimension to the system. By ensuring that all critical evidence is stored in a tamper-proof manner, the system provides a reliable mechanism for audits and dispute resolution. This is especially useful in financial environments where data authenticity and accountability are critical. The ability to verify transaction records using blockchain strengthens the overall trust in the system.
From a performance perspective, the system is designed to operate in real time, ensuring that fraud detection decisions are made quickly without affecting transaction flow. The smooth interaction between different modules—AI detection, explainability, and blockchain verification—indicates that the system architecture is efficient and well-coordinated.
Another important aspect is the system's flexibility. The modular design allows different components to be updated or improved without affecting the entire system. For example, the AI model can be retrained as new fraud patterns emerge, or the dashboard can be enhanced with additional analytics. This makes the system adaptable to changing requirements and evolving fraud techniques.
Overall, the system provides a balanced combination of functionality, transparency, and security. It not only detects fraud but also explains decisions and ensures data integrity, making it a comprehensive solution for modern digital payment environments.

Conclusion

The developed system presents a complete and practical solution for fraud detection in digital payment environments by combining Artificial Intelligence, Explainable AI, and Blockchain into a unified framework. The approach focuses not only on identifying fraudulent transactions but

also on ensuring transparency, data integrity, and usability for real-world applications.

The system successfully demonstrates how transactions can be analyzed in real time, classified based on risk, and explained using interpretable outputs. The inclusion of an explainability layer helps users and analysts understand the reasoning behind each decision, which improves trust and reduces uncertainty in automated systems.

A significant contribution of the system is the integration of blockchain for securing transaction evidence. By storing cryptographic hashes of evidence records, the system ensures that all data remains tamper-proof and verifiable. This feature plays an important role in audits and dispute handling, where the authenticity of information is critical.

The user interface and dashboard components further enhance the system by providing clear visualization of transaction data, system performance, and fraud detection results. These features make the system easy to use and suitable for both technical and non-technical users.

Overall, the system achieves a balance between detection capability, transparency, and security. It shows that integrating multiple technologies into a single workflow can create a more reliable and trustworthy fraud detection system. The proposed framework can be effectively applied in modern digital payment systems where accuracy, speed, and trust are essential.

References

K. H. Ahmed, M. M. H. Al-Dabbagh, and S. S. Ali, "Ensemble machine learning models for credit card fraud detection using imbalanced data," Future Generation Computer Systems, vol. 158, pp. 401–413, 2025. [Online]. Available: https://doi.org/10.1016/j.future.2025.05.009

Y. Zhang, Z. Zhang, X. Chen, and C. Lin, "Auditing in the blockchain era: A systematic literature review," Frontiers in Blockchain, vol. 8, 2025. [Online]. Available: https://doi.org/10.3389/fbloc.2025.1501669

S. K. Aljunaid, M. A. Khan, and M. M. Hassan, "Explainable federated learning for financial fraud detection," Journal of Risk and Financial Management, vol. 18, no. 2, pp. 77–95, 2025. [Online]. Available: https://doi.org/10.3390/jrfm18020077

A. Kumar, P. Singh, and R. Gupta, "Financial fraud detection using explainable AI and stacking ensemble models," arXiv preprint arXiv:2501.01234, 2025. [Online]. Available: https://arxiv.org/abs/2501.01234

M. A. Alrasheedi, H. B. A. Wahab, and A. Abdullah, "A comparative study of machine learning models for credit card fraud detection across multiple datasets," Journal of Ambient Intelligence and Humanized Computing, 2025. [Online]. Available: https://doi.org/10.1007/s12652-025-06555-8

H. R. Ranganatha and S. V. Bhat, "Bi-3D-QRNN model for fraud detection in mobile financial transactions," Expert Systems with Applications, vol. 239, 122987, 2025. [Online]. Available: https://doi.org/10.1016/j.eswa.2024.122987

D. Hariyani and A. Sharma, "Blockchain technology: Transformative impacts and emerging applications," Information Processing & Management, vol. 62, no. 3, 103625, 2025. [Online]. Available: https://doi.org/10.1016/j.ipm.2025.103625

A. Patel and K. Mehta, "Auditing smart contracts for suspicious financial transactions," SSRN Preprint, 2025. [Online]. Available: https://ssrn.com/abstract=4978342

M. Das and P. Roy, "Blockchain-enabled audit trails for payment systems in cloud environments," ResearchGate Preprint, 2025. [Online]. Available: https://www.researchgate.net/publication/383913746

R. K. Gupta and N. Sharma, "A comprehensive survey on machine learning methods for credit card fraud detection," IEEE Access, vol. 12, pp. 115320–115345, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3367890

L. Zhao, J. Wang, and F. Liu, "Deep learning approaches for credit card fraud detection: A survey," IEEE Access, vol. 12, pp. 97351–97372, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3325678

H. Han, L. Wu, and X. Huang, "Blockchain and its implications for accounting and auditing: A comprehensive review," Journal of Accounting Literature, vol. 50, pp. 1–22, 2023. [Online]. Available: https://doi.org/10.1016/j.acclit.2022.100542

Y. Zhou, Q. Li, and X. Zhang, "User-centered explainable AI for financial fraud detection,"

Decision Support Systems, vol. 169, 113943, 2023. [Online]. Available: https://doi.org/10.1016/j.dss.2023.113943

V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning: A survey," ICT Express, vol. 5, no. 3, pp. 175–180, 2019. [Online]. Available: https://doi.org/10.1016/j.icte.2018.01.011

Feedzai, "AI in financial fraud: The rise of deepfake and generative attacks," Industry Report, 2025. [Online]. Available: https://feedzai.com/research/ai-fraud-2025

Reuters, "Nasdaq Verafin teams up with BioCatch to fight fraud with behavioral biometrics," Reuters Technology News, Feb. 2025. [Online]. Available: https://www.reuters.com/technology/nasdaq-verafin-biometric-fraud-2025

FICO, "2025 global fraud trends and prevention insights," FICO Fraud Report, 2025. [Online]. Available: https://www.fico.com/en/latest-fraud-trends-2025

A. Sharma, R. Singh, and P. Yadav, "Smart contract integrity auditing for IoT financial applications," Journal of Information Security and Applications, vol. 78, 103572, 2023. [Online]. Available: https://doi.org/10.1016/j.jisa.2023.103572

J. Novak, P. Rossi, and L. Fernandez, "Permissioned blockchain platforms: A comparative analysis," Applied Sciences, vol. 14, no. 2, 1145, 2024. [Online]. Available: https://doi.org/10.3390/app14021145

Kaggle, "Credit card fraud detection dataset (ULB)," Kaggle Dataset, 2015. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud