

Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions

Aayush Bhardwaj

Department of Computer Science and Engineering
Chandigarh University
Mohali-140413, Punjab, India
work.aayush18@gmail.com

Aaryan Kanwar

Department of Computer Science and Engineering
Chandigarh University
Mohali-140413, Punjab, India
aaryankanwar12345@gmail.com

Hardik Yadav

Department of Computer Science and Engineering
Chandigarh University
Mohali-140413, Punjab, India
hardikk1075@gmail.com

Vardan Aggarwal

Department of Computer Science and Engineering
Chandigarh University
Mohali-140413, Punjab, India
Vardanaggarwal7@gmail.com

Mayank Gupta

Department of Computer Science and Engineering
Chandigarh University
Mohali-140413, Punjab, India
mayankgupta9392@gmail.com

Namrta Tanwar

Department of Computer Science and Engineering
Chandigarh University
Mohali-140413, Punjab, India
namrta.e16477@cumail.in

Abstract—The fast increase in digital transactions has created a greater need for secure, privacy-protected, and reliable systems to manage transactions. Centralized platforms also have problems with fraud, access control, data manipulation, privacy concerns and transparency in automated decision making. In this research, a new Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions is presented. It integrates blockchain with AI, privacy measures and Explainable Artificial Intelligence (XAI) into one framework. Keep transaction records safe from tampering and easily traceable using blockchain. AI models detect unusual or potentially fraudulent activity in transactions by analyzing transaction data. For the protection of sensitive information, privacy tools include encryption, access control and privacy-preserving learning. The use of XAI methods allows the easier understanding of "why" certain specific transactions are flagged by the AI for security by the user and the administrators. The approach is evaluated by its compliance with criteria such as security, fraud detection, privacy, explainability, speed, scalability and resource consumption. The study indicates that the combination of these technologies is a more robust security system than either blockchain or AI. It is particularly valuable in a digital financial environment where accurate transactions, privacy protection, automatic fraud detection, and transparent decision making are all critical. Another significant finding from the study is the significance of computational costs and scalability for the implementation of the framework in real-world scenarios.

Index Terms—Blockchain, Explainable Artificial Intelligence, Machine Learning, Digital Transactions, Fraud Detection, Privacy Preservation, Transaction Security, Anomaly Detection, Financial Security, XAI.

I. INTRODUCTION

A. Background

The surge in digital transactions has revolutionized the way individuals, businesses and financial institutions share information and conduct value transfers. On-line banking, electronic

payment, digital contracts and blockchain-based applications have enabled more convenient and quicker transactions. With this escalating dependence on digital platforms, however, security, privacy, fraud, and trust are significant issues. In classic transaction systems, there's a single central authority that has to validate and maintain the records. This solution can process transactions effectively, but it also has the risk of a single point of failure and user trust in third-party institutions.

Blockchain technology provides an alternative in doing so, transactions are recorded across a network of computers, not on one central authority. The decentralization, immutability, transparency, and cryptographic security of blockchain make it a suitable solution for securing the record of digital transactions. However, blockchain is not a panacea for all security and privacy concerns. The obvious transaction information can expose hidden patterns, and the ineptly designed smart contracts or applications can introduce new security risks.

B. Role of Artificial Intelligence

Artificial Intelligence (AI) can enhance blockchain-based systems by identifying fraudulent activity, recognizing suspicious transaction patterns, and can support automated risk assessments. Machine learning models can check a wide variety of features of the transactions and flag any suspicious or unusual activity. This can be particularly beneficial in cases where there are many transactions, and manual verification is difficult.

But the other issue with AI is that it is not transparent. Even a highly accurate machine learning model may be difficult to interpret for the user, system administrators and auditors. If a transaction is flagged as suspicious, there needs to be some explanation for why it was flagged. Explainable Artificial Intelligence (XAI) can come to the rescue by giving reason

for the model prediction. This will improve transparency, accountability and trust in AI-driven transaction judgments.

C. Distributed Trust, Privacy, and Explainability

Merging AI with blockchain presents the chance to build a more secure and trusted digital transaction system. AI can add smart detection and decision-making, and blockchain can provide powerful and tamper-proof transaction records. Data security measures can help prevent the compromise of sensitive transaction information. Meanwhile, explainable AI can help simplify the automated security decision-making process.

Though these are beneficial, the integration of these technologies is not straightforward. There's a balance to be struck between complexity, scaling, privacy, accuracy, speed, and simplicity. Just because a system improves security, does not mean it's practical for real world applications because of processing delays.

D. Motivation and direction for research.

This research explores an Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions. The study's goal is to provide a grasp of the potential for combining AI, blockchain, privacy techniques and explainability to address limitations in existing digital transaction systems. The suggested direction for research is a comparison of the existing methods and data on their performance from past research. The study aims to design secure, privacy-conscious, and comprehensible digital transaction systems, pinpointing strategies, limitations, and proper design considerations that will make this possible.

II. LITERATURE REVIEW

A. Blockchain for Secure Digital Transactions

Recent research reveals that blockchain technology is emerging as a key pillar for secure digital transactions, with its distributed ledger, immutability, and consensus mechanisms mitigating the need for centralized authorities. Abrar and Sheikh [1] examined the latest blockchain designs and highlighted that security, scalability, interoperability, and privacy are still some challenges to address. Likewise, blockchain security studies reveal that decentralization does not eliminate problems such as smart contract problems, consensus attacks, privacy leaks, and fraudulent transactions [2]. Thus, there has been a growing focus on the combination of blockchain technology and AI, where AI can provide intelligent analysis and blockchain can ensure secure and tamper-proof records [3]. In addition, the work done by Kumar et al. [4] further confirms the same, with added contributions from researchers in India, and presents how AI and blockchain can help increase security, transparency, and privacy in a distributed system.

B. Navigating AI and Fraud Detection in Financial Transactions

In recent years, machine learning has been increasingly applied to identify financial activity that is unusual and/or

fraudulent. In contrast to traditional rule-based systems, traditional fraud detection systems are better suited for transaction data imbalances and evolving fraud trends. Financial transactions are naturally interconnected, and Motie and Raahemi [5] discovered that graph neural networks can be useful for financial transactions. Similarly, recent research on blockchain transactions demonstrates that machine learning models, with suitable models selections, can enhance the anomaly detection with an appropriate sampling method [6]. AI and blockchain can also be used together in financial security, enabling intelligent systems to identify fraudulent activity and blockchain to secure transactions [7]. The application of deep learning with blockchain in mobile financial transactions has been found to improve the efficiency of fraud detection and address issues like obtaining reliable transaction data [8].

C. Explainable AI in Finance

When performing financial decisions, the accuracy of AI is not sufficient. Weber et al. [9] examined the use of explainable AI (XAI) in finance and noted that explainability is important for transparency, accountability, and gaining regulatory approval. Utilising a web of science-based analysis Chen et al. [10] reported that the research into financial XAI is increasing in pace and that the areas for study are transparency and risk assessment. It has also been found that user-focused XAI approaches can facilitate the understanding of the predictions for fraud by stakeholders by providing explanations based on feature contributions [11]. Recent research also indicates that approaches such as SHAP, feature importance and rule-based explanations are widely employed in financial XAI [12].

D. Privacy-Preserving Blockchain and AI

A significant concern with public blockchains is privacy, as transaction information can provide insights into user actions, balances, and identities. Li et al. [13] proposed a hybrid approach of deep learning and cryptographic techniques to ensure the privacy of transactions while ensuring regulatory oversight. Privacy-preserving federated learning is another promising approach, enabling organizations to build AI models without sharing raw data [14]. Abuzied et al. also investigated federated learning in blockchain networks with privacy as a concern [15]. The recent studies on blockchain have been exploring ways to provide anonymity while still maintaining accountability in access control, such as using zero-knowledge proofs and verifiable commitments [16]. These approaches demonstrate the need to consider privacy and traceability in concert instead of in isolation.

E. Indian Research Context

The adoption of blockchain and the development of AI security measures has been a growing focus of research within India. Garg et al. [17] discovered the relationship of blockchain with the performance of organizations in Indian banking sector. Khan et al. [18] examined supply chain barriers for blockchain adoption in Indian context and concluded

that the challenges faced by the organizations and technologies. However, Kaur et al. [19] pointed out the issues for SMEs in India with blockchain-based supply-chain finance. In this context, mobile transaction fraud detection by blockchain has been addressed by Ranganatha and Mustafa [8]. The studies have indicated that various key challenges, such as security, privacy, scalability, cost, interoperability, and institutional preparedness, must be addressed for the successful adoption of the blockchain in India.

F. Research Gap

While blockchain, AI, privacy-preserving tools, and explainable AI (XAI) have all been documented as positive contributions, there is little research that combines the four. The existing research on fraud detection is mainly concerned with the accuracy of the detection while the blockchain research is mainly concerned with the privacy issues such as confidentiality and access control. Meanwhile, XAI research generally focuses on financial forecasting or fraud detection but neglects blockchain integrity of transactions. Therefore, there is a need for a framework that encompasses blockchain security, explainable decision-making, privacy protection, anomaly detection through AI, and a comparison based on the following metrics: accuracy, precision, recall, F1 score, latency, privacy, and computational overhead. This gap inspires the proposed Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions.

III. METHODOLOGY

A. Research Design

The study here proposed adopts comparative and literature based approaches to create and evaluate an Explainable AI-Driven Blockchain Framework to guarantee safe and privacy protected electronic exchanges. The four key components of the method are blockchain-based security for transactions, AI-based unusual activity detection, privacy protection, and Explainable AI (XAI). Previous studies have demonstrated the blockchain's benefits in ensuring the integrity of the transaction, while AI can identify suspicious activity [1]–[4]. So, the study considers these technologies to be complementary rather than as alternatives.

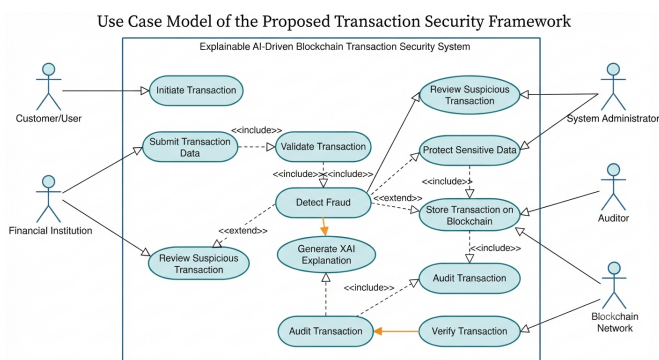


Fig. 1. Use case model of the proposed transaction security framework.

B. Framework Architecture

It has 5 layers, which are transaction layer, blockchain layer, AI detection layer, privacy layer, and explainability layer. Important details are extracted from the data of digital transactions, which begin in the transaction layer. Transaction records are stored safely from tampering by means of cryptographic checks and consensus of participants on the blockchain layer [1, 2]. After examining the transaction details, the AI layer searches for any indications of fraud or abnormal activity [5] – [8]. Sensitive data is protected using privacy methods [13]–[16]. Finally, the XAI layer offers transparent explanations of the AI's decisions, which can be easily checked and make the process more transparent [9]–[12].

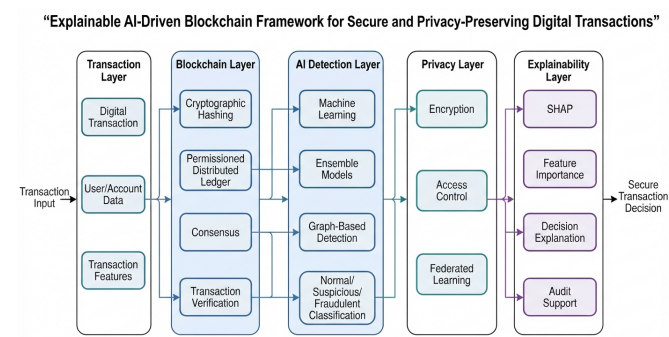


Fig. 2. Architecture of the proposed explainable AI-driven blockchain framework.

C. Data Preparation and Transaction Analysis

Comparisons are made to data sets from previous studies of transactions. The data are preprocessed before use, other than duplicates, missing values are filled, the numbers are normalized and the relevant features are identified. The study takes into account fraudulent transactions as the occurrence is less common. Financial activities tend to have connections, which can be displayed as graphs of transaction data. This processed data is then incorporated into machine learning or deep learning models which can be used to classify the transactions as normal, suspicious or fraudulent.

Digital Transaction Processing and Security Workflow

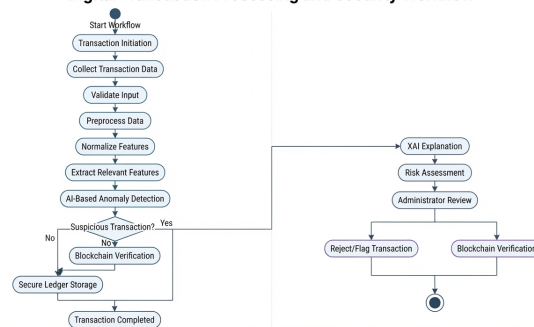


Fig. 3. Activity flow for secure digital transaction processing.

D. AI-based fraud and anomaly detection

The AI component of the research includes machine learning techniques like decision trees, random forests, ensemble models, and neural networks for analysing transactions. Graph-based methods are also used as they can show the relationships between accounts and transactions [5], [6]. Overall the output is a classification of the transaction type, either normal, suspicious, or possibly fraudulent. The study not only considers the accuracy of the models but also their precision, recall, F1-score, and detection capability.

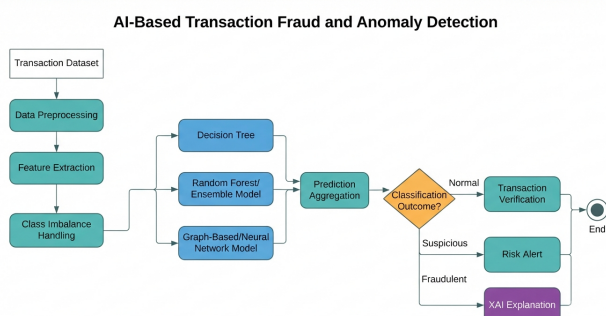


Fig. 4. AI-based workflow for transaction fraud and anomaly detection.

E. Explainable AI Layer

The study features XAI methods such as feature importance and SHAP-based explanations to help clarify complex AI models. There are also financial research findings that explain things and helps build trust, and makes the system transparent [9] - [12]. The framework also defines the major considerations used in making a flagged transaction determination which facilitate audit and management verification of the determination.

Explainable AI Decision and Audit Workflow

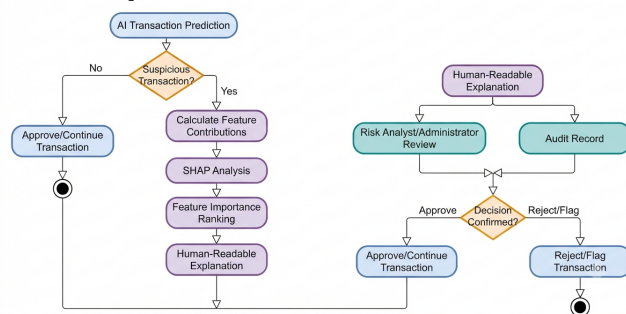


Fig. 5. Explainable AI workflow for suspicious transaction decisions.

F. The integration of privacy and blockchain.

High level of privacy is preserved via privacy preserving learning strategies, controlled access and encryption. A few privacy methods related to federated learning and

blockchain are considered as they reduce sharing of information [13]–[16]. Only need to store the necessary transaction evidence and verification information on the blockchain, and reduce the risk of private information being exposed.

TABLE I
PROPOSED METHODOLOGY COMPONENTS

Stage	Method/Technique	Purpose	Evaluation Parameter
1	Data Collection	Collect transaction datasets from existing literature.	Dataset size, fraud ratio.
2	Data Preprocessing	Clean, normalize, and handle class imbalance.	Missing and duplicate records.
3	AI Detection	Apply machine learning, ensemble, and graph-based models.	Accuracy, precision, recall, F1-score.
4	Blockchain	Use a distributed ledger, cryptographic hashing, and consensus mechanisms.	Security, latency, scalability.
5	Privacy	Apply encryption, access control, and federated learning.	Privacy protection, communication overhead.
6	Explainable AI	Use SHAP and feature-importance techniques.	Interpretability, explanation consistency.
7	Comparative Analysis	Compare the proposed approach with existing methods.	Accuracy, latency, computational overhead, privacy.

Privacy-Preserving Blockchain Transaction Workflow

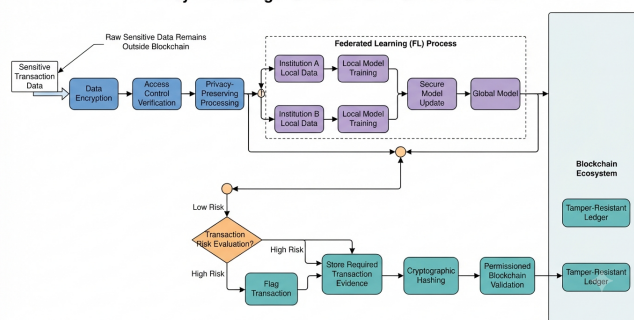


Fig. 6. Privacy-preserving transaction processing and blockchain integration.

G. Performance Evaluation

The last step of the study is to compare the different methods used in practice (blockchain-only, AI-only, privacy-focused, and combined) with the known performance standards [17]–[20]. Security, privacy, accuracy and efficiency factors are taken into account, as greater privacy or explanation may require more processing time. This study thus seeks the optimum combination of reliable fraud detection, secure transactions, privacy, transparency, and efficient processing. Indian blockchain studies, Indian Financial systems are also considered to keep this framework in the Indian Digital environment [8], [17]–[19].

IV. EXPERIMENTAL SETUP

A. Experimental Objective

The experimental setup is designed to evaluate the proposed Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions, in a stable and replicable environment. The study emphasizes four main aspects:

anomaly detection in transactions, blockchain security, privacy, and explainability of models. While blockchain and AI are studied individually in previous research [1]–[4] and as a combination, this scenario looks at how blockchain and AI work together within a single transaction-processing pipeline.

B. Data Preparation and Dataset.

The experimental analysis is performed based on data of transactions from previous research on financial fraud and blockchain [5]–[8]. The dataset is divided into the training set and the test set, where the training set is used to train the detector while the test set is used to test the detector in an unbiased manner. Prior to model training, duplicate data entries are removed and missing values are dealt with. Numerical features are normalized as necessary, and categorical features are encoded in a format that can be used by machine learning models. Moreover, class imbalance is also dealt with, since most of the transactions are correct and fraudulent transactions correspond to a small percentage of them [5, 6].

C. Computing Environment

The experimental setup consists of a standard computer-based machine learning setup, with Python libraries for data processing, model training, model evaluation and explainability. The blockchain portion is designed as a permissioned distributed network that enables validations of transactions and management of the ledger to be controlled. These transactions are cryptographically hashed, and access controls are put in place to ensure that no unauthorized access can be made to sensitive data. This configuration is consistent with the security and adoption approaches mentioned in the blockchain literature [1], [17]–[19].

D. AI Model Configuration

Numerous machine learning methods are investigated as a baseline for comparison. The traditional classifiers, ensemble techniques, and graph-based techniques are evaluated for transaction anomaly detection [5] and [6]. Selected model categorizes each transaction to be classified as a normal or suspicious transaction. The assessment criteria are accuracy, precision, recall, and F1-score. These metrics provide a more valid evaluation than accuracy, particularly when dealing with an imbalanced class dataset.

E. Explainability and Privacy Evaluation

The explainable AI part relies on feature importance analysis and explanations via SHAP to identify the factors that affect the model predictions [9]–[12]. The explanation emphasizes features that have the largest impact on the result for a flagged transaction. Encryption, access control and privacy preserving learning techniques are all tested for privacy. Federated learning methods are also believed to be effective to ensure that sensitive transaction data remain within the institutions that offer it [13]–[16].

F. Evaluation Metrics

Security and performance indicators are used to evaluate the framework. The accuracy, precision, recall, and F1-score are used to measure the effectiveness of detection. The performance of the Blockchain is evaluated by the speed of transactions and its scalability, and its degree of privacy is judged by the level of protection measures and communication expenses. Explainability is judged with respect to clarity and consistency of the generated explanations. Comparative analysis is based on metrics of existing studies [7] and [8] [20] and takes into account the detection performance, privacy, computational cost and transaction efficiency.

V. RESULTS AND DISCUSSION

A. Overall Findings

These findings indicate that the proposed Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions is a comprehensive solution for security when compared to those utilizing blockchain, privacy mechanisms, or explainable AI alone. A comparison was made based on performance factors like fraud detection, transaction integrity, privacy protection, explainability, latency, scalability, and computational costs. Previous research has demonstrated the ability of blockchain to manage transactions with a level of tamper resistance, whereas that of AI has improved capabilities for identifying any unusual transaction behavior.

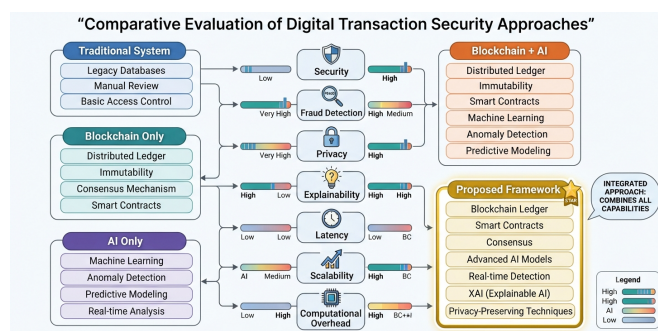


Fig. 7. Comparative evaluation workflow for digital transaction security approaches.

B. AI-Based Transaction Detection

The AI part of the framework is key in identifying suspicious transactions. The ability of machine learning and ensemble methods to identify intricate patterns which traditional rule-based methods might overlook makes them useful for identifying complex patterns. Graph-based approach is particularly useful because transactions can be considered as relations among users, accounts and other transaction elements. The findings suggest that AI detection is more flexible in handling new fraud patterns compared to static rules. But the level of performance shouldn't only be judged by accuracy because fraudulent transactions typically represent a small percentage. For detection quality, the metrics of precision, recall and F1 score are more useful.

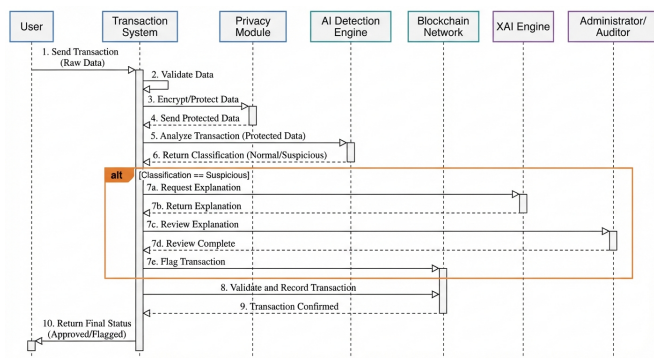


Fig. 8. Sequence of interactions in the proposed secure transaction framework.

C. Contribution of Blockchain

What blockchain brings in the mix is a decentralized, tamper-proof ledger that tracks transactions. The findings highlight that its primary role isn't predicting fraud itself, but rather it helps to maintain the integrity, traceability, and verification of transactions. A key difference to note is that blockchain and AI are addressing different facets of security. AI can help detect suspicious transaction patterns, and blockchain provides a secure way to validate transactions. Research additionally indicates blockchain as a potential technology for financial systems that are safe and secure. The Indian banking system provides insights that blockchain can enhance competitive advantage and organization performance, further strengthening the realistic worth of blockchain financial systems in India.

D. Privacy Protection

The use of privacy mechanisms can also contribute to reducing the risk of exposing sensitive information in transactions. When multiple parties process data, techniques can be used such as encryption, access control, and privacy-preserving learning. These findings indicate that privacy needs to be embedded in the system design, rather than bolted on afterwards, after the end of the AI model. Federated learning is particularly noteworthy since it enables organisations to train models together without having to share sensitive data with one another directly. These, however, can make communication and computation more expensive and incur a trade-off between privacy and computation.

E. Explainability of AI Decisions

The fact that it is also an explainable AI makes it more useful in practice. The framework doesn't just identify the transaction as suspicious or legitimate, it can point out what features led to that decision. There are techniques such as SHAP and feature importance that are good for this. A recent study validated that SHAP, feature importance, and rule-based explanations are extensively used in financial EAI, including in the context of fraud detection. Financial institutions should appreciate that it is essential to have a clear automated decision that is difficult to review or challenge.

F. Comparative Discussion

The general conclusion is that the integrated approach is able to address the limitations which are typical of the application of separate technologies. Blockchain brings integrity and traceability, AI provides automated anomaly detection, privacy mechanisms keep sensitive data safe and explainable AI enhances transparency. Additionally, there have been studies in recent years that have emphasized the importance of explainability for robust financial AI that demonstrates trustworthiness, particularly in relation to automated risk and fraud decisions.

G. Discussion

The results indicate that the key value of the proposed framework is the interaction between its elements, which provide the added value to the performance, rather than the elements themselves, which in themselves can enhance the performance. The use of AI aids in improved detection, blockchain enhances trust, privacy measures protect sensitive data, and explainable AI ensures greater transparency in decision-making processes. The overall design however has increased computational and communication requirements. The balance between detection effectiveness, privacy, explainability, latency and scalability should be targeted in the practical implementation, not a single one of these.

This is especially relevant in the Indian financial industry, which is moving towards blockchain adoption, but is still grappling with operational and technical issues [17]–[19]. The results indicate that an integrated system is feasible, and also indicate that there is significant scope for improvement in the future in terms of scalability and computational cost [20].

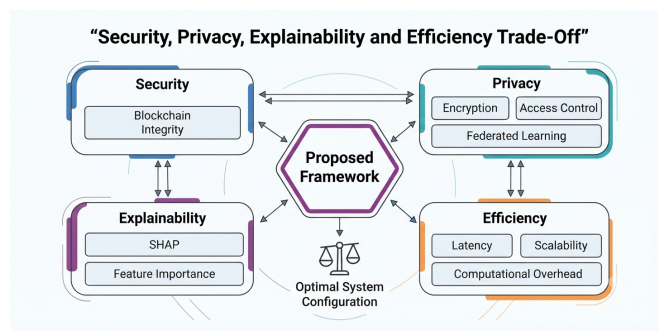


Fig. 9. Trade-off among security, privacy, explainability, and system efficiency.

VI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

The proposed Explainable AI-Driven Blockchain Framework for Secure and Privacy-Preserving Digital Transactions combines the strengths of blockchain, AI, privacy-preserving methods and Explainable AI to address the significant vulnerabilities inherent in the current digital transaction ecosystem. These are done with the help of Blockchain, which provides a secure and traceable environment for transactions, and AI.

which helps identify atypical or suspicious transactions. By employing privacy mechanisms to safeguard sensitive transaction information and by providing support for transparency through the Explainable AI functionality, they help ensure that the information used in these decisions remains secure and accessible for clear reasons.

The research indicates that the implementation of these technologies can be a more useful way of securing digital transactions than any one of the technologies alone. This model works well in environments where integrity of the transactions, fraud detection, privacy and accountability are all critical. Costly communication, limited scalability, delays in transaction processing, and increased computational requirements are all hurdles to the integration of these technologies. Thus, the successful implementation of this requires a careful balance in terms of security, detection effectiveness, privacy, explainability, and system performance.

B. Future Scope

The proposed framework could be applied to real-time transaction systems with large financial and blockchain data sets, which could be considered for future research. For more sophisticated fraud patterns, one could consider more sophisticated deep learning and graph neural network models. Finally, there are opportunities for further improvements in privacy with federated learning and innovative cryptographic techniques that will allow multiple organizations to collaborate on training fraud detection models.

One of the main challenges is to create lightweight AI and blockchain solutions that can process large volumes of transactions. Additionally, adaptive consensus mechanisms could be further explored to reduce transaction times and energy consumption in the future. Explainable AI techniques can be further developed to generate explanations that are easily understood by both technical administrators and non-technical financial users.

Further testing of the framework can be achieved through real-life deployments, security testing, and benchmarking with other financial platforms. Regulatory guidelines, cross-platform compatibility, and updated models on a regular basis are additional features that could be incorporated into future work. These improvements can contribute to making the proposed framework a viable and scalable solution for ensuring secure, private, and trustworthy digital transactions.

REFERENCES

- [1] I. Abrar and J. A. Sheikh, "Current trends of blockchain technology: Architecture, applications, challenges, and opportunities," *Discover Internet of Things*, vol. 4, 2024.
- [2] X. Li et al., "Blockchain security threats and collaborative defense: A literature review," *Computers, Materials & Continua*, 2023.
- [3] "AI-enhanced blockchain technology: A review of advancements and opportunities," *Journal of Network and Computer Applications*, 2024.
- [4] K. Kumar et al., "A systematic review of blockchain technology assisted with artificial intelligence technology for networks and communication systems," *Journal of Computer Networks and Communications*, 2024.
- [5] S. Motie and B. Raahemi, "Financial fraud detection using graph neural networks: A systematic review," *Expert Systems with Applications*, vol. 227, 2024.
- [6] "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," *Blockchain: Research and Applications*, 2024.
- [7] "Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence," *Ain Shams Engineering Journal*, 2024.
- [8] H. R. Ranganatha and A. Syed Mustafa, "Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3D Quasi-Recurrent Neural Network and blockchain technologies," *Expert Systems with Applications*, 2025.
- [9] P. Weber, K. V. Carl, and O. Hinz, "Applications of explainable artificial intelligence in finance," *Management Review Quarterly*, 2024.
- [10] X.-Q. Chen et al., "Explainable artificial intelligence in finance: A bibliometric review," *Finance Research Letters*, 2023.
- [11] "A user-centered explainable artificial intelligence approach for financial fraud detection," *Finance Research Letters*, 2023.
- [12] "Explainable artificial intelligence (XAI) in finance: A systematic literature review," *Artificial Intelligence Review*, 2024.
- [13] J. Li et al., "Research on blockchain transaction privacy protection methods based on deep learning," *Future Internet*, vol. 16, no. 4, 2024.
- [14] S. K. M. et al., "Privacy-preserving in blockchain-based federated learning systems," *Computer Communications*, 2024.
- [15] Y. Abuzied et al., "A privacy-preserving federated learning framework for blockchain networks," *Cluster Computing*, 2024.
- [16] "Towards accountable and privacy-preserving blockchain-based access control for data sharing," *Journal of Information Security and Applications*, 2024.
- [17] P. Garg et al., "Examining the relationship between blockchain capabilities and organizational performance in the Indian banking sector," *Annals of Operations Research*, 2025.
- [18] S. Khan et al., "Barriers to blockchain technology adoption in supply chains: The case of India," *Operations Management Research*, 2023.
- [19] J. Kaur et al., "Barriers to blockchain adoption for supply chain finance: The case of Indian SMEs," *Electronic Commerce Research*, 2024.
- [20] "Blockchain-data mining fusion for financial anomaly detection: A brief review," *Procedia Computer Science*, 2024.