

# Privacy-Enhanced Blockchain Transaction Analysis with Advance Analytics for Enhanced Bitcoin Security

K. Sri Navya, J. Deekshitha, B. Jahnavi, Mr. G. Prasad

Department of Information Technology  
ACE Engineering College, Hyderabad, India

**Abstract:** *This project offers a sophisticated framework for increasing Bitcoin security through the combination of Privacy-Enhanced Blockchain Transaction Analysis (PEBTA) with state-of-the-art analytics. Bitcoin, even as it has been designed as decentralized, is vulnerable to fraud, money laundering, and invasion of privacy. This study offers an approach of consolidating real-time monitoring of data, machine learning algorithms (such as Random Forest), graph analysis, and clustering to detect anomalies. The model utilizes privacy-preserving technologies such as Isekai to ensure user anonymity. Also designed is a risk scoring system to indicate suspicious transactions, enhancing surveillance without compromising privacy.*

**Keywords:** Blockchain Security, Privacy-Enhancing Technologies (PET), Bitcoin Analysis, Machine Learning, Risk Assessment, Transaction Anomaly Detection, Real-Time Analytics, Graph Analysis

## I. INTRODUCTION

The widespread use of Bitcoin and other cryptocurrencies has transformed the world of finance, providing decentralized peer-to-peer transfers without the need for using conventional financial institutions. But this increased use has been accompanied by rising concerns over security and privacy. Bitcoin, even though it has been made secure with its underlying technology of blockchain, is still vulnerable to a range of cyberattacks, fraud, and privacy breaches. The absence of any regulatory system and the anonymity of Bitcoin transactions have made it difficult to ensure the authenticity and security of users' interactions and have therefore become a target of choice for bad actors.

To mitigate these issues, Privacy-Enhanced Blockchain Transaction Analysis (PEBTA) can be combined with powerful analytics to enhance the security of Bitcoin transactions. PEBTA seeks to track blockchain transactions in a way that preserves user privacy and does not allow unauthorized parties to access sensitive information. This approach guarantees that although transactions can be monitored for fraud and suspicious behavior, privacy for users is preserved, in consonance with the decentralized nature of Bitcoin. Furthermore, using cutting-edge analytical tools like machine learning and anomaly detection can offer real-time surveillance, allowing for the detection of patterns or anomalies that can signal possible security issues.

The combination of PEBTA with next-generation analytics is an innovative method of improving the security of Bitcoin. By integrating machine learning techniques, anomaly detection mechanisms, and real-time transaction analysis, this system proposes to counter the growing security threats in the world of cryptocurrencies. The solution not only raises the security and integrity levels of Bitcoin transactions but also the confidence in blockchain technology as a whole. Through the use of sophisticated analytics to identify fraud, block hacking attempts, and detect potential vulnerabilities, this methodology enhances Bitcoin's security while maintaining user anonymity—a key function in the blockchain environment.



## II. LITERATURE SURVEY

**Kumar, R. et al. (2023)** proposed "An integrated framework for enhancing security and privacy in IoT-based business intelligence applications". This research proposes a secure and lightweight encryption-based framework for safeguarding sensitive IoT data in Business Intelligence (BI) applications. The framework offers a combination of privacy-preserving solutions, secure data sending protocols, and access control mechanisms. Real-time threat detection is also a critical feature of the framework. But it is essentially intended for IoT environments and not for blockchain-exclusive security issues or anonymizing financial transactional networks like Bitcoin.

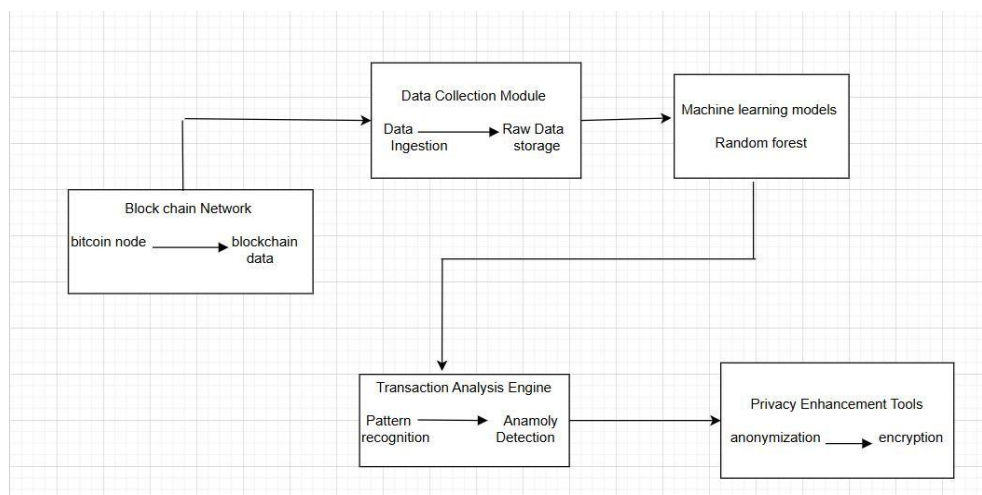
**Ghani, M. A. N. U. et al. (2024)** in their paper titled "Toward robust and privacy-enhanced facial recognition: A decentralized blockchain-based approach with GANs and deep learning", introduced a privacy-sensitive facial recognition framework. The study replaces centralized storage with blockchain-based facial data decentralization and enhances privacy through the use of Generative Adversarial Networks (GANs) for synthetic training data generation. Deep learning ensures identification accuracy and smart contracts ensure secure access controls. Despite a strong emphasis on privacy and decentralization, the system revolves around biometric security and fails to provide solutions for transactional behavior or financial networks.

**Bhaladhare, P. et al. (2022)** proposed "PMNBARL: Enhancing Efficiency of Privacy Management in Digital Networks with Blockchain and Adaptive Reinforcement Learning". They integrated blockchain technology and reinforcement learning to dynamically handle user privacy policies. The system records privacy actions on-chain for openness and adjusts policy behavior based on user interaction patterns. Though this model promotes improved adaptive privacy control, it does not have real-time financial risk analysis and threat detection features required for secure blockchain transaction analysis within cryptocurrency platforms.

## III. PROPOSED METHODOLOGY

### ARCHITECTURE

The proposed system includes four primary modules that enhance the security of Bitcoin transactions without sacrificing anonymity. The data gathering module initially retrieves up-to-date blockchain information from various Bitcoin nodes using secure APIs. Secondly, the preprocessing module tidies, normalizes, and anonymizes data by implementing privacy-preserving methodologies like Isekai encryption and anonymization. Random Forest, graph analytics, and clustering are used by the core analysis engine to detect anomalies and unusual transaction trends. Finally, a risk-scoring model monitors transaction activity and detects high-risk addresses in order to enable timely alerts and complete reporting. The end to-end solution delivers precise, private, and scalable blockchain transaction monitoring.



**Fig 1: Architecture of the proposed system**



**Blockchain Network** provides transaction data.

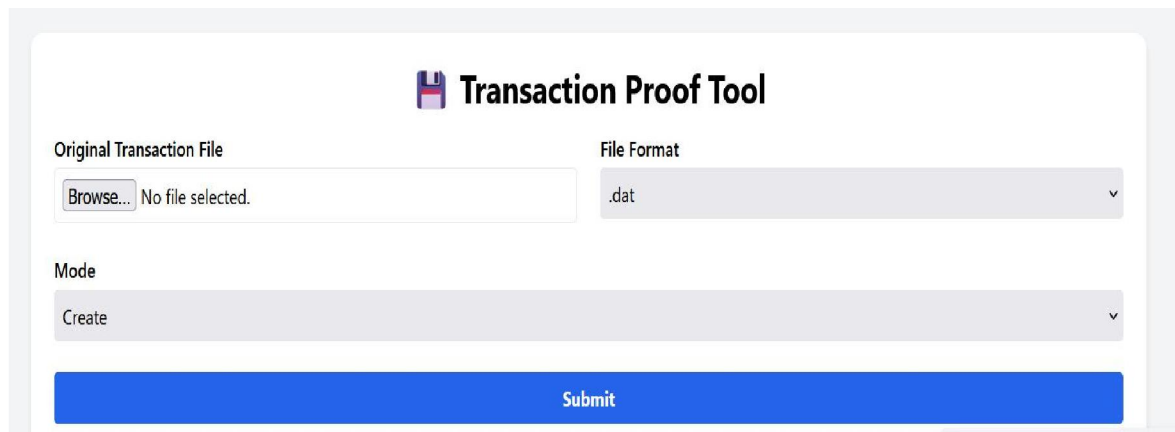
**Data Collection Module** ingests and stores this data securely.

**The Machine Learning Model (Random Forest)** is trained and applied to detect suspicious patterns.

**The Transaction Analysis Engine** further processes the data for deeper insight into anomalies and behavioral patterns. Finally, **Privacy Enhancement Tools** ensure that all analysis is performed in a privacy-preserving and secure manner

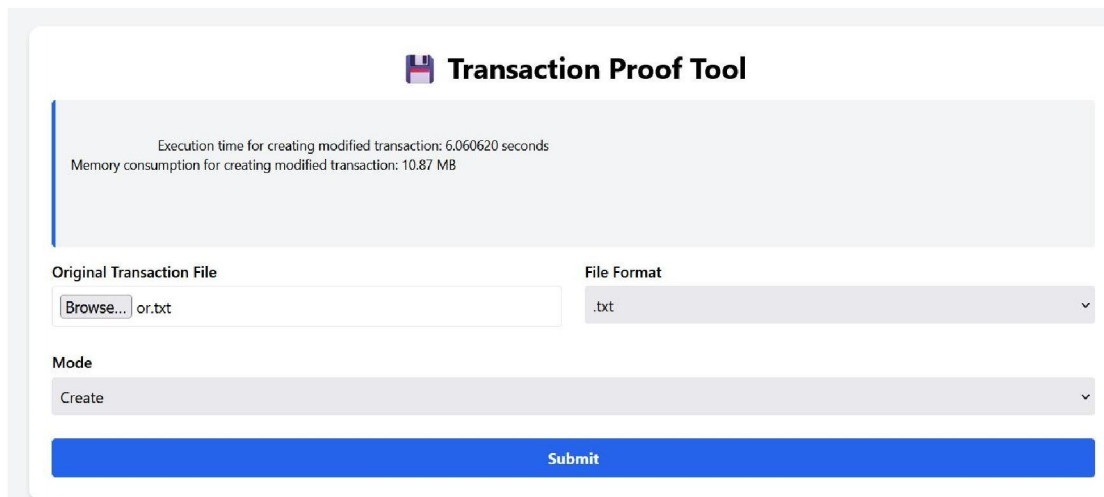
## IV. EXPERIMENTAL RESULTS

### 4.1 OUTPUT SCREENS



The screenshot shows the 'Transaction Proof Tool' interface. It features a title bar with a floppy disk icon and the text 'Transaction Proof Tool'. Below the title bar, there are two input fields: 'Original Transaction File' with a 'Browse...' button and the text 'No file selected.', and 'File Format' with a dropdown menu showing '.dat'. Below these fields, there is a 'Mode' dropdown menu showing 'Create'. At the bottom of the form is a large blue 'Submit' button.

FIG.1 HOME PAGE



The screenshot shows the 'Transaction Proof Tool' interface during the 'Creating Transaction' process. It features a title bar with a floppy disk icon and the text 'Transaction Proof Tool'. Below the title bar, there is a large light blue box containing the text: 'Execution time for creating modified transaction: 6.060620 seconds' and 'Memory consumption for creating modified transaction: 10.87 MB'. Below this box, there are two input fields: 'Original Transaction File' with a 'Browse...' button and the text 'or.txt', and 'File Format' with a dropdown menu showing '.txt'. Below these fields, there is a 'Mode' dropdown menu showing 'Create'. At the bottom of the form is a large blue 'Submit' button.

FIG.2 CREATING TRANSACTION



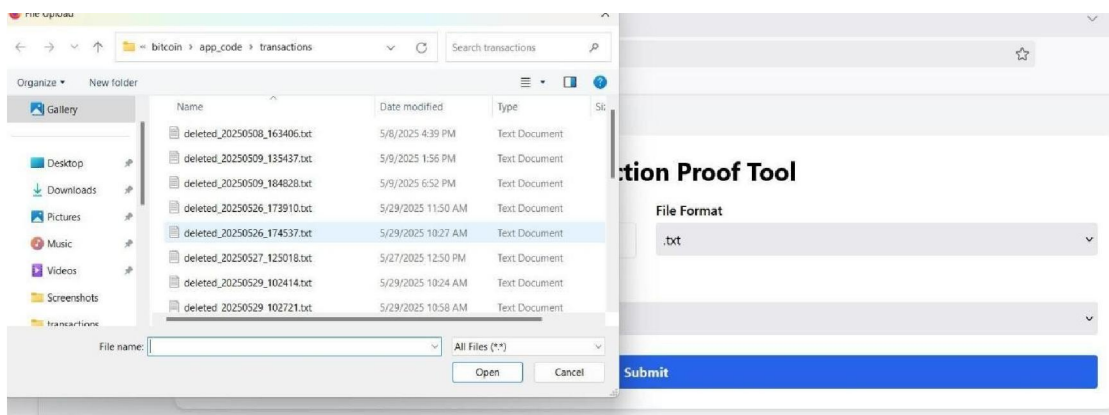


FIG.3 UPLOADING FILE

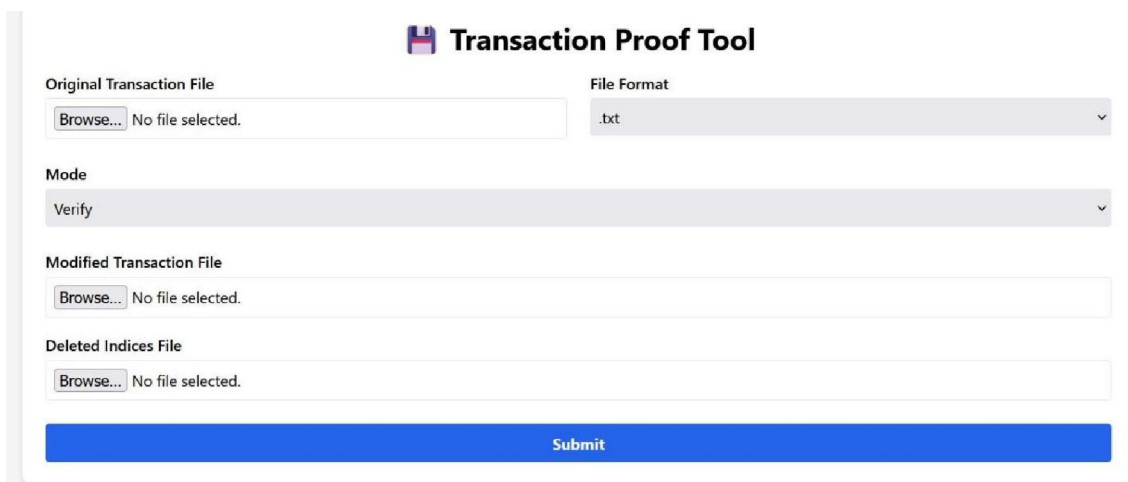


FIG.4 VERIFYING TRANSACTION

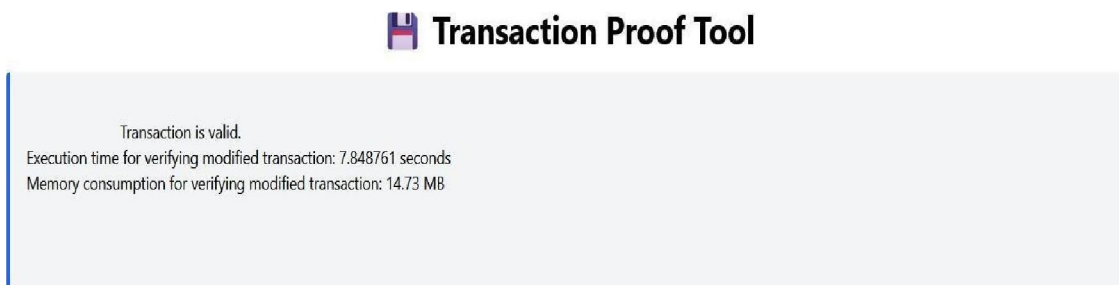


FIG.5 VALID TRANSACTION



## Transaction Proof Tool

Transaction is invalid.  
Execution time for verifying modified transaction: 8.156751 seconds  
Memory consumption for verifying modified transaction: 14.75 MB

FIG .6 INVALID TRANSACTION

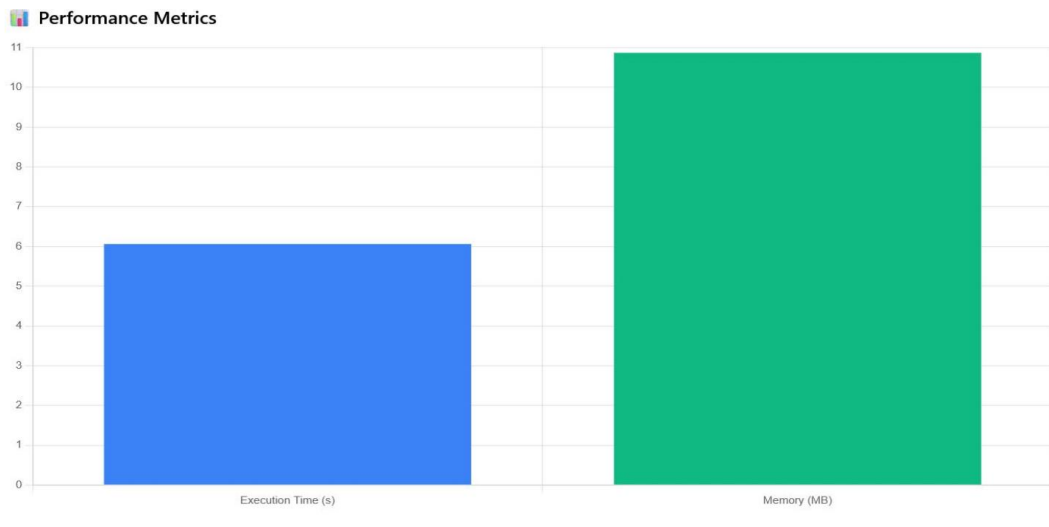


FIG .7 PERFORMANCE METRICS

## IV. CONCLUSION

The system is very efficient in strengthening the security and privacy of the Bitcoin transactions by combining cutting-edge analytics with privacy-preserving technologies. By making use of machine learning-based algorithms such as Random Forest, along with graph-based analysis and clustering methods, the system is able to efficiently detect suspicious patterns and possible fraud in the blockchain. Through the use of such tools as Isekai and differential privacy, anonymity of the user is preserved without impacting the depth or precision of the analysis. Moreover, through the inclusion of a risk scoring model, proactive surveillance and real-time alarm generation are possible. In all, this framework proves an equal and scalable solution that balances the dual requirement of privacy and security in cryptocurrency environments and is thus useful to financial institutions, regulatory agencies, and forensic examiners..

## REFERENCES

- [1]. N.Lu,Y.Chang,W.ShiandK.-K.R.Choo,"CoinLayering:AnEfficientCoinMixing Scheme for Large Scale Bitcoin Transactions," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1974-1987, 1 May-June 2022, doi: 10.1109/TDSC.2020.3043366.
- [2]. A Sajjad et al., "What Motivates Bitcoin Miners to Practice Bitcoin Mining: An Assessment Based on Behavioral Reasoning Theory," in IEEE Transactions on Engineering Management, vol. 71, pp. 8209-8222, 2024, doi: 10.1109/TEM.2023.3335662.
- [3]. M. Monem et al., "An Industry-4.0-Compliant Sustainable Bitcoin Model Through Optimized Transaction Selection and Sustainable Block Integration," in IEEE TransactionsonIndustrial Informatics, vol.18,no.12,pp.9162-9172, Dec. 2022,doi: 10.1109/TII.2022.3159673.



- [4]. M. M. Islam and H. P. IN, "A Privacy-Preserving Transparent Central Bank Digital CurrencySystemBasedonConsortiumBlockchainandUnspentTransactionOutputs," in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2372-2386, 1 July- Aug. 2023, doi: 10.1109/TSC.2022.3226120.
- [5]. X. Wang et al., "ESS: An Efficient Storage Scheme for Improving the Scalability of BitcoinNetwork,"inIEEETransactionsonNetworkandServiceManagement,vol.19, no. 2, pp. 1191-1202, June 2022, doi: 10.1109/TNSM.2021.3127187.
- [6]. K. Tarmissi et al., "Mitigating Security Threats of Bitcoin Network by Reducing Message Broadcasts During Transaction Dissemination," 2022 14th International ConferenceonComputationalIntelligenceand CommunicationNetworks(CICN),Al- Khobar, Saudi Arabia, 2022, pp. 772-777, doi: 10.1109/CICN56167.2022.10008238.
- [7]. D. Liu et al., "Analysis and Reflection on the Situation of Industrial Information Security RansomwareAttacks," 2023 8thInternational Conferenceon Data Sciencein Cyberspace (DSC), Hefei, China, 2023, pp. 354-358, doi: 10.1109/DSC59305.2023.00057.
- [8]. K. Gargetal., "ASurveyonBlockchainforBitcoinandItsFuturePerspectives,"2022 3rdInternationalConferenceonComputing,AnalyticsandNetworks(ICAN),Rajpura, Punjab, India, 2022, pp. 1-6, doi: 10.1109/ICAN56228.2022.10007225.
- [9]. S.NassarandT.Yaacoub,"WhyBitcoinissooriginal,andwhyitscopiesaredoomed to fail?," 2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), Victoria, Seychelles, 2024, pp. 1-5, doi: 10.1109/ACDSA59508.2024.10467994.
- [10]. P.Lavanyaet al., "Internet ofThings enabledBlockLevel Security MechanismtoBig Data Environment using Cipher Security Policies," 2022 International Conference on AdvancesinComputing,Communicationand AppliedInformatics(ACCAI),Chennai, India, 2022, pp. 1-6, doi: 10.1109/ACCAI53970.2022.9752603.
- [11]. A Vikram et al., "Blockchain Technology and its Impact on Future of Internet of Things (IoT) and Cyber Security," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 2022, pp. 444-447, doi: 10.1109/ICECA55336.2022.10009621.
- [12]. F.PituandN.C.Gaitan,"Surveyofsecurity,performance,andprofitabilityofMonero: a browser-based cryptocurrency," 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Tenerife, Canary Islands, Spain, 2023, pp. 1-5, doi: 10.1109/ICECCME57830.2023.10253316.
- [13]. F.BarbàraandC.Schifanella,"BxTB:cross-chainexchangesofbitcoinsforallBitcoin wrappedtokens,"2022FourthInternationalConferenceonBlockchainComputingand Applications (BCCA), San Antonio, TX, USA, 2022, pp. 143-150, doi: 10.1109/BCCA55292.2022.9922019.
- [14]. A Mosaif et al., "Blockchain-Based System for Security and Privacy of Students' Health Records," 2023 International Conference on Digital Age & Technological Advances for Sustainable Development (ICDATA), Casablanca, Morocco, 2023, pp. 36-40, doi: 10.1109/ICDATA58816.2023.00016.
- [15]. T. Kowalski et al., "Bitcoin: Cryptographic Algorithms, Security Vulnerabilities and Mitigations,"2022IEEE InternationalConference onElectroInformationTechnology (eIT), Mankato, MN, USA,2022, pp.544-549, doi:10.1109/eIT53891.2022.9814066.

