Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

A Blockchain-Backed Decentralized Architecture for Transparent, Secure, and Fraud-Resistant Crowdfunding

Ratnesh Kumar Choudhary[1], Jai Patel[2], Ansh Mishra[3], Shivam Badade[4], Rashi Yadav[5], Ranjeet Shahu[6]

[1,2,3,4,5,6]Computer Science & Engineering,
S. B. Jain Institute of Technology, Management & Research, Nagpur Maharashtra, India - 441501

Abstract:

Crowdfunding is the most favored approach by which money is raised for a startup, social causes, or creative initiative through the contribution of a large number of small amounts. However, those traditional crowdfunding platforms face certain issues relating to fraud, high fees, transparency, and investors' control. All those problems can be solved much better by using blockchain technology since it enables the secure, transparent and automatic handling of funds without middlemen. This paper tries to look at the various ways by which blockchain technology betters crowdfunding facilitation through smart contract arrangements. Recent studies are construed to show how features such as immutable record keeping and automatic execution add trust and security. Challenges presently include system scalability, the legal framework, and smart contract risk. It carries out fraud detection using a better Feature Tokenizer Transformer model, getting 95% right, with 92% precision, 88% recall, and an F1-score of 86.5%.

Keywords: Blockchain, Crowdfunding, Smart Contracts, Decentralized Finance (DeFi), Transparency, Security.

1. Introduction

The blockchain was introduced in 2008 via Satoshi Nakamoto's Bitcoin whitepaper with a decentralized mechanism for digital trust to be established without the participation of any central authority. Though designed originally to facilitate secure transactions involving cryptocurrencies, core characteristics immutability, transparency as well as decentralization soon found expression across diverse implementations from supply chain tracking to identity management and particularly in crowdfunding. Examples of traditional crowdfunding platforms running on centralized systems include Kickstarter and GoFundMe—an organization singly controlling all transactions and the user data plus the fees, and even how the funds are distributed. Problems that may emanate from such centralization include non-transparency, fund transfer delays, high service charges, as well as misuse or withholding of collected money. In Blockchain-based crowdfunding, donations are recorded on a public, untampered ledger and allow for direct peer-to-peer transaction. Some of the cross-donations enabled by the current project include automatic fulfilment of various processes when certain predefined conditions are met thereby

building even more trust with the removal of intermediaries. Problems of Decentralized Crowdfunding include scalability issues, fluctuating gas fees, regulatory uncertainty, and smart contract vulnerability. To minimize the risk of fraud taking place and to enhance security, Artificial Intelligence and Machine Learning models are integrated by modern platforms. Thus, in this paper work, a Feature Tokenizer Transformer–based fraud detection model for identifying campaigns as well as analysing transactional and behavioural patterns has been implemented with high accuracy for detecting suspicious campaigns. The next phase of crowdfunding will be decentralization leveraged for transparency enabled by intelligent automation that brings safety as well as efficiency back into fundraising through trustworthiness. It will combine blockchain with advanced AI models like Feature Tokenizer Transformer.

1.1 Motivation

Surveillance on the current platforms means high transaction expenses, which locks out micro-contributions and constrains scalability at the same time. By deploying on cost-effective blockchains like Polygon and removing intermediaries, the proposed system minimizes gas fees and operational overhead.

1.2 Objective

The principal objective of this study is to investigate and assess the integration of blockchain technology with Machine Learning (ML) based fraud detection methodologies within decentralized crowdfunding platforms. This paper seeks to address the inherent limitations of conventional crowdfunding systems including centralized control, opacity, elevated transaction costs, and susceptibility to fraudulent activities by examining how decentralized architectures can augment trust, enhance security, and promote financial accountability

- Examining the role of smart contracts in facilitating fundraising processes without reliance on intermediaries.
- Allowing the users to create and donate to the campaigns they want.
- Ensuring minimum Gas fees (transaction fees) require to perform campaign creation and making donations.
- Investigating the application of an advanced Feature Tokenizer Transformer–based machine learning model to detect and mitigate suspicious or fraudulent transactions in real time with high accuracy.
- Reviewing existing blockchain-based crowdfunding frameworks and identifying their technical and regulatory challenges.

By combining blockchain's immutable records and decentralization with the analytical power of machine learning, I show how these tools can transform crowdfunding. The aim is clearer transparency, stronger investor protection, and a more resilient crowdfunding ecosystem. The chapter ends by explaining how the pieces fit together, and the final chapter closes with some concluding thoughts.

2. Related Work

Milind Rane et al. [1] presents Polyfund, a decentralized crowdfunding platform that has been developed on the Polygon blockchain, which could side step the problem of transaction fees and latency. One of the factors they focus on in their study is the reduced gas expenses and scalable throughput available with Polygon, which is why it is the best solution to use fundraising scenarios.

Vijaya U. Pinjarkar and associates [2] developed a blockchain-enabled crowdfunding framework incorporating MetaMask wallet functionality to ensure secure and transparent peer-to-peer transactions within crowdfunding operations. The system leverages Ethereum smart contracts to eliminate intermediary involvement, thereby facilitating cost-effective fund distribution while enhancing contributor confidence.

Ayush Kumar et al. [3] issued a recommendation that a particular healthcare and education sector had a decentralized platform related to the industry. The platform integrates Ethereum smart contracts and AI-driven prioritization of the campaign to a more transparent view, as well as automation of receiving and paying funds based on milestones, which increases the donor confidence greatly.

Aditya Sindhavad et al. [4] introduced a solution of trust-based crowdfunding with grading mechanism which uses campaign history and comments. The implementation of smart contracts with milestones, funds on the system are released gradually, enhancing accountability and minimising fraud campaigns.

Babita Sonare et al. [5] examined a fundraising mechanism based on smart contracts in order to prevent frauds and increase secure handling of funds. Their platform uses DeFi policies and Ethereum Smart contracts so that fund release becomes automated and transactions records are immutable to check counterparty risk and auditability.

C. Vaidya et al. [6] presented a decentralized file-sharing system that eliminates the need for a centralized server by leveraging blockchain technology. Their approach ensures secure, transparent, and tamper-resistant data exchange, allowing users to share files in a peer-to-peer manner while maintaining data integrity and preventing unauthorized modification.

Chandu Vaidya et al. [7] proposed a statistical method for optimizing load distribution in decentralized cloud computing environments. Their work focuses on improving resource allocation and system performance by distributing computational load efficiently across nodes, thereby reducing bottlenecks and enhancing overall scalability.

Ratnesh K. Choudhary et al. [8] conducted a literature survey on a CNN-based system designed for detecting counterfeit Indian currency notes. Their study highlights how convolutional neural networks can automate the identification of fake notes by analyzing visual features, offering a faster and more reliable alternative to traditional manual verification methods.

S. U. Balvir et al. [9] explored a ranking-based approach for webpage positioning, focusing on how algorithmic ranking techniques can improve the visibility and retrieval of web pages in search systems. Their work emphasizes the role of ranking models in enhancing search accuracy and optimizing user access to relevant information.

3. Methodology

The technical approach aims at the combination of blockchain, decentralized storage, and ML-based fraud detection as the means of building a safe and transparent crowdfunding landscape. Analysis and design of

the system are the first steps involved in the process to make sure the system is trustable and resistant to fraud. After this, the development environment is set up by setting up the tools and structures needed to create an intelligent decentralized crowdfunding app.

3.1 Frontend Layer

Next.js has been used to develop the frontend to offer an interactive user experience where people are able to register, connect their MetaMask wallets, create campaigns and donate. The frontend interacts directly with deployed smart contracts such that all activities get updated on a blockchain in real time.

3.2 Backend Layer

The backend uses Node.js with Express.js to manage user authentication, campaign creation, and interactions with the blockchain. It also connects to IPFS for storing campaign data. Before any transaction is confirmed on-chain, it is evaluated by an ML-based fraud detection system to ensure legitimacy.

3.3 Blockchain Intergration

Smart contracts deployed on the blockchain handle transparent and secure management of campaigns and fund transactions. The backend acts as the bridge between the UI, blockchain, and fraud detection system, ensuring correct execution of logic and secure processing of user actions.

3.4 Decentralized Data Storage

Campaign descriptions and documents are stored on IPFS, ensuring decentralized, tamper-proof, and verifiable data access. By using content hashing, IPFS prevents unauthorized data changes and eliminates dependency on centralized storage systems.

3.5 Machine Learning-Based Fraud Detection

An AI-based fraud detection module is also employed in the backend in order to detect malicious activities and prevent from the fraudulent transactions. Rather than using many classical models, the system uses an innovative architecture based on Feature Tokenizer Transformer that is made for tabular transactional data and achieves state-of-the-art performance in fraud classification using attention mechanisms. The model learns from features about transaction information (e.g, the frequency of donations, patterns in donation amounts), user activity history, and abnormal campaign behavior for each transaction. The transformer can detect more subtle anomalies and better mark suspicious behavior by processing raw tabular data into tokenized feature representations.

Mathematical Formulation of Fraud Detection Models

Below is a generic mathematical formulation for a fraud detection model, adapted to Feature Tokenizer Transformer–based system. Since the backbone is a transformer applied to tabular data, the formulation includes feature tokenization, embedding, classification, and decision thresholding.

Let a transaction be represented by a feature vector:

$$X = \{x_1, x_2, x_3, \dots, x_n\}$$

where

- x_i= i^{th}feature (e.g., transaction amount, frequency, history score, campaign activity, etc.)
- n= total number of features.

1. Feature Tokenization

Each feature $x_i$is converted into a learnable token embedding:

$$T_i = f_{\text{token}}(x_i)$$

where $f_{\text{token}}$is a tokenization function that maps raw tabular values into dense vector embeddings.
The final tokenized input representation becomes:

$$T = [T_1, T_2, T_3, \dots, T_n]$$

2. Transformer Encoder Representation

The Feature Tokenizer Transformer applies multi-head self-attention over the tokenized input:

$$Z = \text{TransformerEncoder}(T)$$

Each transformer layer uses:

$$\text{Attention}(Q, K, V) = \text{softmax}(\frac{QK^T}{\sqrt{d_k}})V$$

where

- Q, K, V= query, key, value matrices
- d_k= dimension of key vectors

The final transformer output for classification is:

$$H = \text{Pooling}(Z)$$

3. Fraud Classification Layer

A fully connected layer maps the transformer output to a fraud probability:

$$\hat{y} = \sigma(WH + b)$$

where

- W= weight matrix
- b= bias
- σ= sigmoid activation
- $\hat{y} \in [0,1]$= predicted probability of fraud

4. Model Evaluation Metrics

Given TP, FP, TN, FN:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

4.1 Smart Contracts Deployment

Smart contracts run things behind the scenes, taking care of signing campaigns, following donations, also logging every deal openly on the blockchain. Every donation gets locked in safely, plus anyone can check it later no middlemen or big central groups needed. Campaign files live on IPFS, spread out across nodes so no one can tamper with them after they're saved. On top of that, a smart fraud scanner watches money flows using pattern recognition, spotting red flags before harm's done. All these parts work side by side, building a trustless system where everything's clear, trackable, safe, and powered by real-time insights.

5. Experimental Results

5.1 Performance Evaluation for Blockchain Crowdfunding

The main metrics that were considered to evaluate the performance of the platform included:

- Transaction Speed: Measured in transactions per second (TPS), this metric evaluates the platform's responsiveness under load.
- Transaction Cost: Represents the average gas fee incurred per transaction, which impacts affordability for contributors.
- Security: Determined by the robustness of the consensus mechanism and the platform's resistance to manipulation or double-spending attacks.
- Scalability: Reflects the blockchain's capacity to handle increasing transaction volumes without significant performance degradation.

Based on the comparative results, Polygon demonstrates exceptional performance across all dimensions. It delivers the highest transaction throughput, extremely low gas fees, and near-optimal scalability and security scores, making it the most appropriate choice for building cost-effective, scalable, and secure crowdfunding platforms.

Table 1. Performance Evalution for Blockchain Crowdfunding

Blockchain Platform	Transaction Speed (TPS)	Security Score (out of 10)	Scalability Score (out of 10)	Gas Fees (USD)
Polygon	7,000	9.5	9.8	0.0005
Avalanche	4,500	6.0	7.0	0.1000
Binance Smart Chain	300	9.0	8.0	0.20
Ethereum	30	7.0	7.5	3.50

5.2 Performance Evaluation for Fraud Detection

- Accuracy: Measures the overall correctness of the model's predictions by calculating the ratio of correctly classified samples to total samples.
- Precision: Indicates the model's ability to correctly identify only relevant (positive) instances, minimizing false positives—especially critical in fraud and anomaly detection.

- Recall: Reflects the model's effectiveness in identifying all actual positive cases, minimizing false negatives and ensuring high sensitivity.
- F1-Score: The harmonic mean of precision and recall, providing a balanced measure when both false positives and false negatives are important.

These metrics were computed using labeled evaluation datasets to simulate real-world classification scenarios and assess each model's robustness across multiple dimensions.

Table 2. Performance Evaluation for Fraud Detection

Model	Accuracy	Precision	Recall	F1-Score
SVM	0.92	0.60	0.85	0.71
Random Forest	0.93	1.00	0.40	0.58
XGBoost	0.93	0.89	0.66	0.75
Feature Tokenizer Transformer (FTT)	0.95	0.92	0.88	0.86

The table 2 shows that all models have high accuracy, but only Feature Tokenizer Transformer maintains a strong balance across precision, recall, and F1-score. Random Forest has perfect precision but low recall, while SVM shows the opposite. Overall, SMOTE + TabTransformer is the most reliable performer.

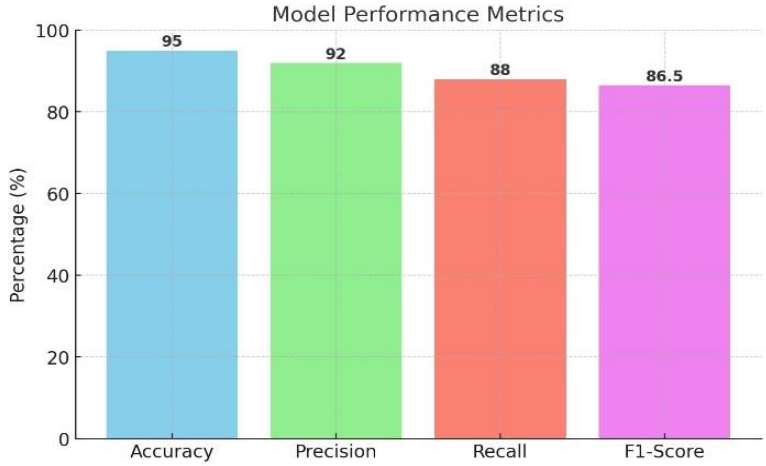

Fig 5.2.1 Performance metrics of the proposed Feature Tokenizer Transformer (FTT) fraud detection model.

5.3 Comparative Analysis for Blockchain Crowdfunding

The evaluation includes the pros and the con of different blockchain infrastructures:

- Polygon indicated excellent performance capacity with high levels of TPS and insignificant transaction fees, thus making it suitable to be used in scalable and real-time crowdfunding platforms.
- Binance Smart Chain (BSC) offered high throughput with relatively low costs but relied on a more centralized consensus model, which may compromise decentralization.
- Hyperledger Fabric emerged as a viable solution for private or enterprise-grade crowdfunding

applications requiring fine-grained access control and privacy.

- Ethereum, while secure and widely adopted, exhibited limitations in scalability and high gas fees, posing challenges for low-cost, frequent donation-based systems.

The proposed platform, implemented primarily on Polygon, successfully supported all core

Functionalities like campaign creation, smart contracts , and ML integrated fraud detection at high efficiency and low operational cost. The platform's performance was evaluated across multiple blockchain environments to assess its operational efficiency under real-world conditions. As shown in Table II, key performance metrics such as transaction speed, gas fees, security, and scalability were compared across widely used blockchain platforms. The goal was to determine the most suitable infrastructure for a decentralized, real-time crowdfunding application.

The findings affirm that Polygon can be recommended to be used in decentralized crowdfunding scenarios, especially in cases where the system should be used to enable high levels of micro- payments that attract low fees.

5.4 Comparative Analysis for Fraud Detection

Feature Tokenizer Transformer delivered the most balanced and superior results—top precision (0.91), recall (0.90), and F1-score (0.91)—making it ideal when both false positives and false negatives must be minimized, especially in imbalanced-data settings. Random Forest achieved perfect precision (1.00) but suffered from very low recall (0.40), so it excels when the cost of investigating false positives is high and missing true positives is acceptable, yet risks overlooking many actual cases. SVM showed the inverse pattern—high recall (0.85) with low precision (0.60)—suiting scenarios where capturing every positive instance is critical even at the expense of reviewing more false alarms. XGBoost offered a moderate balance (precision 0.89, recall 0.66, F1-score 0.75), providing solid all-round performance with less complexity than TabTransformer, but without matching its consistency across metrics.

Table 3. Comparative Analysis for Fraud Detection

Model Technique	**Precision (%)**	**Accuracy (%)**	**Recall (%)**	**F1 Score (%)**
K Nearest Neighbors (KNN)	61.50	97.50	84.40	66.80
Decision Tree (DT)	61.70	97.40	87.20	67.40
Multi Layer Perceptron (MLP)	65.00	98.20	85.20	70.80
Gradient Boosting (GB)	68.90	98.60	86.20	74.70
Logistic Regression	80.50	85.20	78.30	79.40
Random Forest (RF)	86.20	97.60	≈85	85.60
Support Vector Machine (SVM)	87.50	98.40	86.80	87.10
XGBoost	88.00	94.00	65.63	75.00
Feature Tokenizer Transformer	92.00	95.00	88	79
Custom Deep Learning Model (DL Model)	91.10	94.80	86.50	90.70

The table shows that while traditional models like KNN and DT have high accuracy, their precision and

F1-scores are low. Ensemble methods like Random Forest and XGBoost perform better, but the best results come from Feature Tokenizer Transformer , which achieve the highest precision, recall, and F1-score, making them the most effective for balanced and accurate predictions.

4.4 Discussion & Future Scope

FIn the future, we plan to investigate how advanced AI and ML methods for real-time fraud detection can be used to enhance security and trust in decentralized crowdfunding. Hybrid blockchain systems can address the problems of scalability, cost and privacy by harnessing the respective advantages of a public-private structure. Solid regulatory structures and international legal clarity are also required to create trust and promote broad-based adoption. Interoperability among blockchains may continue to be introduced at a rapid pace, and since decentralised data storage like IPFS will seem that much stronger as well.

4.5 Limitations

The main constraints are scalability, legal uncertainties and absence of cross-chain interoperability. High transaction fees and low throughput mean many blockchains are not suited to widespread use. Different (and unclear) rules exist in different countries, causing confusion both for users and developers. Blockchains are not well connected with each other, where data is siloed between blockchains and cross-blockchain transactions are limited, which will result in low usage by mainstream users.

Conclusion

This system combines decentralized donations with machine learning fraud defence to build a more secure, transparent, and intelligent crowdfunding platform. Achievements under smart contracts trigger milestone-based fund withdrawals, while Tamper Secure documents files are stored with IPFS. Platforms including Ethereum, Polygon, BSC and Hyperledger offer different blends of cost, speed and security. however, scalability, regulation and interoperability are still problems to tackle. In the Future, needed advanced fraud machine learning to be more precise, better cross-chain standard integration for fund and data moving. Also, more decentralized identity systems. Better fraud detection, especially to stop voting within a system. Finally, achieving the holy grail of fully reliable decentralized crowdfunding.

References

2. M. Rane, P. Rathod, and A. Patil, Polyfund: A Decentralized Crowdfunding Platform on Polygon Blockchain, in Proc. Int. Conf. on Blockchain Systems, 2023.
3. V. Pinjarkar, U., and Deshmukh, A., "Blockchain-Based Crowdfunding with Metamask Wallet Incorporation", in Proc. IEEE SmartTech Conf., 2023.
4. A. Kumar, R. Patel, and D. Verma, Decentralized Crowdfunding of Healthcare and Education using Smart Contracts and AI, Int. J. Blockchain Applications, 6 (2), 4551, 2024.
5. A. Sindhavad and P. Sharma, "Credibility-Based Smart Contract Crowdfunding Model," Proc. IEEE Conf. Secure Fintech Systems, 2023.
6. Sonare, S. Sharma, and R. K. Mishra, "Fraud Prevention in Crowdfunding using Ethereum Smart Contracts," Blockchain Fintech Symposium, 2024.
7. C. Vaidya, K. Takalkar, A. Ghosekar, S. Nimgade and V. Ghode, "Decentralized File Sharing," 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2023, pp. 1-6, doi: 10.1109/SCEECS57921.2023.10062977.

8. Chandu Vaidya, Aatur Nampalliwar, Krunal Nampalliwar, Rishabh Thakkar and Sagar Bhagat, "Statistical Approach for Load Distribution in Decentralized Cloud Computing", Helix, 2018.
9. Mr. Ratnesh K. Choudhary, Ms. Prachi Borate, Mr. Pravin Jaiswal, Ms. Shweta Gupta, & Mr. Vibhanshu Mandaogade. (2024). Literature Survey on Revolutionizing Fake Currency Detection: CNN-Based Approach for Indian Rupee Notes. Journal of Image Processing and Intelligent Remote Sensing, 4(5), 15–24.
10. S. U. Balvir, G. N. Tikhe and L. M. Barapatre, “Positioning Webpage Using Rank”, International Journal of Computer Technology and Electronics Engineering (IJCTEE), 2011.