**ORIGINAL ARTICLE**
Electrica 2026; 26: 1-13

# Securing Blockchain Loyalty Programs with Artificial Intelligence–Driven Fraud Detection

**Can İşcan[1], Muhammet Furkan Özara[1], Ahmet Erkan Çelik[1], Muhammed Ali Aydın[2], Akhan Akbulut[1,3]**

[1]Private practice
[2]Department of Computer Engineering, İstanbul Üniversitesi-Cerrahpaşa Faculty of Engineering, İstanbul, Türkiye
[3]Department of Computer Engineering, İstanbul Kültür University Faculty of Engineering, İstanbul, Türkiye

**Cite this article as:** C. İşcan, M. F. Özara, A. E. Çelik, M. A. Aydın and A. Akbulut, "Securing blockchain loyalty programs with artificial intelligence–driven fraud detection," *Electrica*, 26, 0189, 2026. doi: 10.5152/electrica.2026.25189.

## WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *Fraud is a major problem in customer loyalty programs, and traditional databases are often insufficient to detect fraudulent activities.*
- *Blockchain technology provides transparency and immutability, which improve security and prevent manipulation of records.*

**Corresponding author:**
Akhan Akbulut

**E-mail:**
a.akbulut@iku.edu.tr

**Received:** September 9, 2025
**Revision Requested:** October 16, 2025
**Last Revision Received:** March 4, 2026
**Accepted:** May 5, 2026
**Publication Date:** November 3, 2026

**DOI:** 10.5152/electrica.2026.25189

Content of this journal is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

## ABSTRACT

Blockchain technology offers enhanced security and transparency, making it a more reliable foundation for loyalty programs compared to traditional relational databases. Its decentralized nature ensures tamper-resistant records, which is crucial for fraud detection in financial systems. Recent reports reveal a financial loss of $1 billion annually due to fraudulent activities in loyalty platforms, and the blockchain's transparency and immutability make it an ideal solution for minimizing this issue. This paper presents an innovative approach that combines blockchain technology with artificial intelligence (AI)-driven fraud detection models to enhance the security of loyalty platforms. The approach includes real-time detection and rejection of fraudulent transactions prior to being committed to the immutable blockchain ledger, utilizing a meticulously created synthetic dataset to train a variety of machine learning models. A total of 100 000 user wallets, campaigns, and market items were generated to develop effective detection models, simulating real-world transaction patterns. Afterwards, various fraud scenarios, including new user abuse, employee fraud, and account theft, were injected into the Ethereum network with randomness to mimic the complexity of real-world situations. Using Blockscout explorer for data extraction, multiple models, including Random Forest, XGBoost, and a 3-layer neural network, were trained. The artificial neural network achieved the highest performance, with a receiver operating characteristic area under the curve score of 0.9942. The method allows for real-time fraud detection and seamless retraining as real user data accumulates, demonstrating its scalability and potential to prevent fraud in blockchain-based systems. By incorporating blockchain technology with AI-driven fraud detection methods, this innovative solution improves the security of loyalty platforms.

***Index Terms*—**Blockchain, ethereum, fraud detection, loyalty program, neural networks

## I. INTRODUCTION

Loyalty programs serve as a strategic asset within customer relationship management (CRM), significantly contributing to customer retention and the promotion of brand loyalty [1].As competition intensifies and customer expectations evolve, businesses require effective strategies to develop long-term relationships and enhance brand loyalty. Loyalty programs function as mechanisms that incentivize repeat engagement by providing rewards, discounts, and exclusive offers. Loyal customers receive special prizes, while companies benefit from deeper engagement and increased sales. As a result of this mutually beneficial situation, loyalty programs are becoming more increasingly popular. In 2023, the loyalty management market was worth $11.31 billion and is expected to quadruple by the end of 2032 [2].These programs offer value to both customers and companies by facilitating the collection of important data regarding purchasing behaviors, preferences, personalized offers and engagement trends. Loyalty programs enable CRM systems to transcend mere transactional interactions, fostering personalized customer experiences and enhancing emotional connections. Integrating these programs into CRM systems enables businesses to enhance their understanding of customer needs, forecast future behaviors, and optimize marketing strategies effectively. Loyalty programs are essential components of an effective

**WHAT DOES THIS STUDY ADD TO THIS TOPIC?**

- *This study introduces a blockchain-based loyalty platform combined with artificial intelligence models to detect fraud, using synthetic data to simulate real-world scenarios.*
- *The proposed system successfully stopped 52% of fraudulent transactions before completion while maintaining a very low false-positive rate.*
- *A three-layer artificial neural network achieved outstanding performance (receiver operating characteristic area under the curve = 0.9975), outperforming other machine learning models in real-time fraud detection.*

CRM strategy, as they strengthen customer retention, enhance brand loyalty, and offer valuable insights to increase customer lifetime value. However, as loyalty programs gain more attention, fraudulent individuals are also targeting these highly vulnerable services. According to a report published by Ernst & Young, recent estimates indicate an annual financial loss of $1 billion occurring in loyalty programs due to fraudulent activities [3]. As a consequence of this problem, utilizing more secure data storage systems and robust fraud detection mechanisms in contemporary loyalty programs has become a necessity.

Blockchain technology provides a transformative solution for loyalty programs, providing clear advantages compared to traditional relational databases. In contrast to centralized relational databases, which are vulnerable to data manipulation and typically necessitate significant administrative effort for transaction validation, blockchain's decentralized and immutable ledger provides enhanced transparency and security [4]. This transparency enables all stakeholders, including businesses and customers, to access verifiable records of loyalty transactions, thereby fostering trust and mitigating fraud, which is a significant issue in loyalty programs. Blockchain facilitates real-time, peer-to-peer transaction processing, eliminating the necessity for intermediaries, thereby decreasing operational costs and expediting the reward process. Smart contracts on blockchain technology enhance the automation of loyalty transactions, facilitating seamless and conditional reward distributions while reducing the need for manual oversight. These capabilities render blockchain a more efficient and secure basis for loyalty programs, improving both user experience and program integrity.

This study presents a novel method for improving the security and efficiency of loyalty programs by integrating blockchain technology with artificial intelligence (AI)-based fraud detection mechanisms. This research utilizes blockchain's transparency and smart contract automation, in conjunction with advanced machine learning (ML) models, to tackle the ongoing issues of fraud in loyalty platforms. The contribution of the research is threefold following as:

- This study presents a synthetic data generation method designed for training ML models in the context of loyalty program fraud scenarios. The study creates a comprehensive dataset by simulating real-world behaviors and integrating various fraud cases, facilitating precise and flexible fraud detection.
- This study establishes a tailored private Ethereum blockchain utilizing proof of authority (PoA) consensus, specifically designed for loyalty program transactions. This blockchain framework facilitates automated, transparent, and tamper-resistant record-keeping, thereby minimizing administrative overhead and decreasing transaction processing time.
- This study assesses and contrasts various ML models, such as Random Forest, XGBoost, and a neural network, in the context of fraud detection within the blockchain ecosystem. The findings indicate the neural network's enhanced performance, attaining elevated receiver operating characteristic (ROC) area under the curve (AUC) scores, thereby illustrating its applicability for real-time fraud detection in loyalty platforms.

The remaining sections are organized as follows. Section 2 reviews related work on blockchain applications in loyalty programs and fraud detection. Section 3 describes the methodology, detailing the blockchain framework, smart contracts, and AI models used for fraud detection. Section 4 presents the experimental results and discussion, comparing model performances and analyzing their effectiveness in detecting fraud. Finally, Section 5 concludes the paper, summarizing key findings and suggesting directions for future research.

### A. Related Work

The growing integration of blockchain technology in loyalty programs and fraud detection systems has drawn considerable interest from researchers. The decentralized and tamper-resistant architecture of blockchain provides a secure framework for handling loyalty rewards, while its transparency and immutability give improved protection against fraudulent actions. Recent research has investigated many uses of blockchain, analyzing its function in establishing safe loyalty ecosystems, executing fraud-resistant incentive systems, and incorporating ML models for automated fraud detection. This section examines recent developments and pertinent research in blockchain-based loyalty programs and fraud mitigation techniques. Anudeep et al. [5] propose a blockchain-based approach for loyalty programs designed to improve security and transparency in retail marketing. The authors develop and execute a system that employs blockchain's immutable ledger to monitor consumer transactions and incentives, therefore mitigating fraud and enhancing trust among players. The model illustrates how blockchain may optimize loyalty

programs by offering a safe and transparent framework for administering consumer rewards.

Another study [6] tackles the issue of detecting fraudulent activities in blockchain transactions by utilizing ML techniques. The authors offer a methodology that combines blockchain's intrinsic transparency and immutability with sophisticated ML algorithms to successfully detect and prevent fraud. The study illustrates the possibility for real-time fraud detection in blockchain systems by studying transaction patterns and utilizing algorithms such as Random Forest, XGBoost, and neural networks, hence improving security and trust in decentralized apps. The study by Bogdanović et al. [7] examines a blockchain-based loyalty program designed for smart city applications. The authors suggest a cooperative loyalty program that allows consumers to accumulate loyalty points throughout a smart city viaconventional purchases and engagement in diverse collaborative activities. The research underscores the capability of blockchain to establish a cohesive and transparent loyalty system that promotes community involvement and improves customer experiences.

Pranto et al.'s research [8]presents an innovative methodology that integrates blockchain technology with ML to identify fraud in financial transactions. The authors suggest a privacy-preserving approach in which businesses collaborate by exchanging data on a blockchain, facilitating the progressive enhancement of ML models for fraud detection. An adaptive incentive mechanism is implemented to promote participation, and the system is evaluated for efficiency under various conditions, attaining high accuracy in identifying fraudulent activity.

Previous work on detecting frauds with ML in blockchain area [9], studied a solution for detecting frauds on blockchain network. They have explored the integration of ML techniques with blockchain to enhance fraud detection capabilities. The study proposed a hybrid model combining XGBoost and Random Forest algorithms with blockchain technology to detect fraudulent transactions in the Bitcoin network. Their approach leverages synthetic data generation techniques like SMOTE to address data imbalance issues and employs smart contracts to classify transactions as legitimate or malicious. In contrast to the work, their work utilizes binary classification to detect fraudulent activities.

Traditional consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) ensure transaction validity but fail to detect malicious users or fraudulent transaction patterns. To address this, ML techniques have been widely adopted. Bhowmik et al. [10] conducted a comparative study of various supervised ML algorithms, including Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines (SVM), for fraud detection in blockchain networks. The study also proposed a six dense layered neural network with those seven ML algorithms. Their findings revealed that ensemble methods like AdaBoost and Random Forest achieved the highest accuracy (97%) in classifying fraudulent transactions.

Other studies, such as those by Pham and Lee, explored unsupervised learning methods like k-means clustering for anomaly detection in Bitcoin networks, [11] highlighting the challenges of handling unlabeled data. The study includes three different unsupervised learning techniques like SVM, k-Means and proposes Mahalanobis Distance Based Technique. They had to limit their dataset with 100k data points cause of the SVM method takes a long time to run. Additionally, Farrugia et al. focused on detecting illicit accounts in Ethereum by analyzing transaction history [12], identifying key features like transaction time differences and Ether balances. These studies collectively underscore the effectiveness of ML in enhancing fraud detection capabilities in blockchain systems, though challenges such as data imbalance and scalability remain. Future research directions include integrating unsupervised learning techniques and extending these methods to private blockchain networks.

The study focusing on the integrating ML and Blockchain for real-time fraud detection shows that, using AI methods for that task is powerful [13]. Bello et al. have proposed a conceptual framework that leverages the predictive capability of ML with the transparency, security, and immutability of blockchain. This integration allows the analysis of large data sets to identify patterns and anomalies that point to fraud, while blockchain technology provides data integrity and traceability. Supervised learning algorithms, including logistic regression, decision trees, and neural networks, are used to label transactions and make predictions of fraudulent activity with great accuracy. Unsupervised learning methods, such as clustering and anomaly detection, complement the system's capability to recognize new patterns of fraud without labeled data. The blockchain platform addresses weaknesses in traditional fraud detection systems, such as single points of failure and data tampering, by leveraging blockchain's distributed nature and ML's adaptability to changing fraud methods. The complementarity between blockchain and ML not only increases the speed and accuracy of fraud detection but also reduces false positives and builds confidence in financial transactions. JPMorgan Chase and HSBC demonstrate case studies of the practical implications of this complementarity with drastic improvements in the accuracy of fraud detection and operating efficiency. Despite its strengths, the integration of ML and blockchain is also confronted with scalability, data privacy, and regulatory compliance challenges. However, ongoing research and development in ML algorithms, blockchain scalability, and privacy-preserving techniques are expected to further enhance the effectiveness of this integrated system in combating financial fraud.

A secondary review paper [14] thoroughly explores existing blockchain-based loyalty solutions by evaluating publicly listed coins associated with loyalty programs. The authors categorize and analyze active loyalty programs that employ blockchain technology, offering insights into the present state and practical uses of blockchain in improving CRM via loyalty initiatives.

Though previous research work makes significant contributions to transaction analysis in blockchain systems as well as in fraud detection, there remain several crucial gaps that have yet to be filled by research work in this area. The previous work is mostly focused upon common blockchain anomalies as well as financial fraud but does not tackle the distinct dynamics of loyalty systems' interactions in terms of campaigns, reward schemes, as well as tenant-user interactions. In addition, little work is being done in this area to present an end-to-end solution encompassing PoA-based blockchain, automatic smart contract execution, rule-based pre-screening, as well as ML-based schemes, but all targeted at loyalty systems in a comprehensive manner, which is what this research work is going to attempt to fill by presenting an end-to-end solution in this area.

## II. METHODOLOGY

This study employs active and passive agents for fraud prevention and detection systems. The optimized and functional private

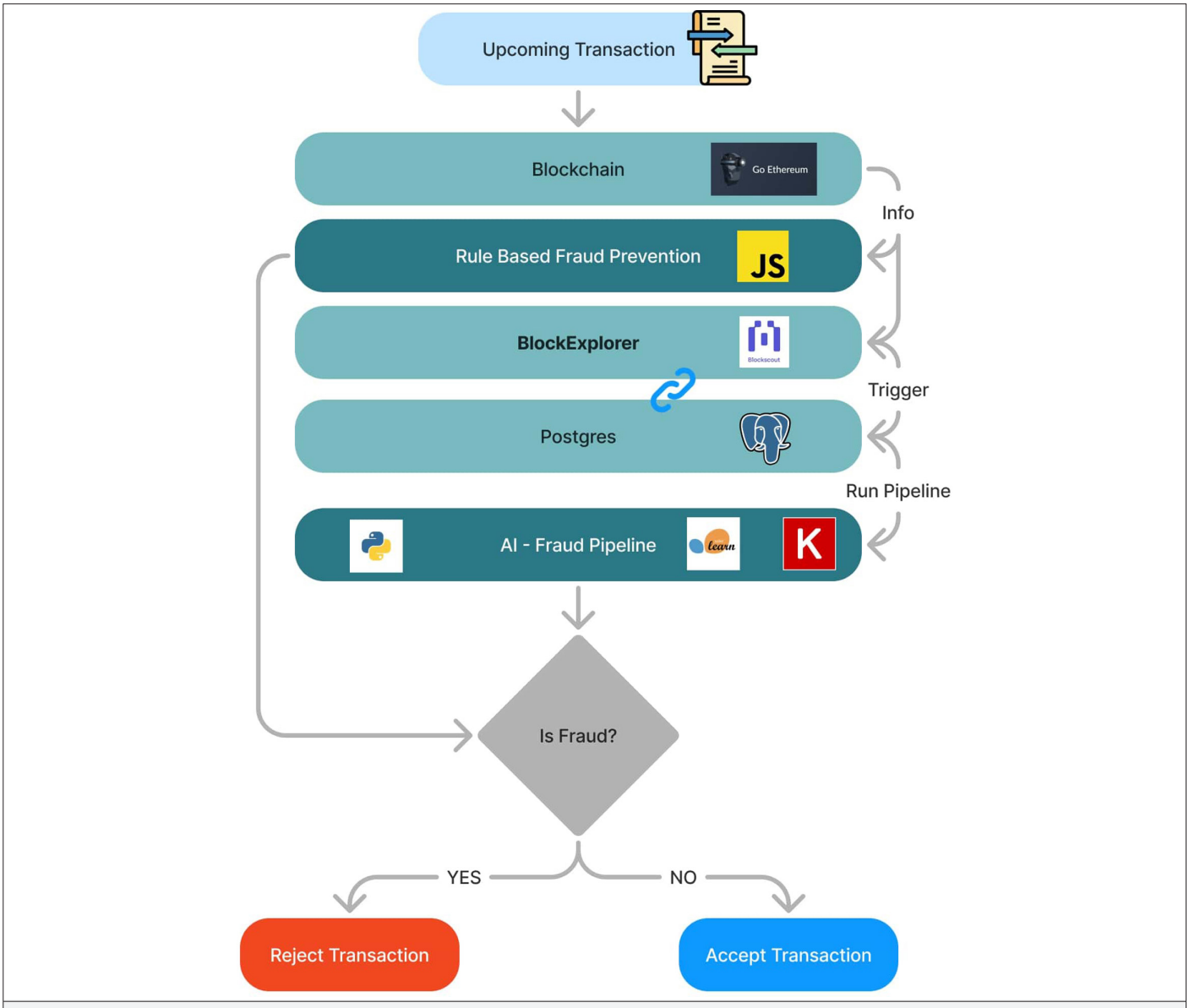



**Fig. 1.** High-level architecture of the blockchain-based loyalty platform.

blockchain system is utilized concurrently for testing purposes of the customer loyalty platform. The blockchain platform is customized as a variant of the GETH (go-ethereum) framework, recognized as the industry's leading option [15].

To better introduce the overall system before presenting the technical details, Fig. 1 provides a high-level architectural overview of the proposed blockchain-based loyalty platform. At the conceptual level, customer interactions originate from the CRM environment and are forwarded to the Customer Loyalty Management System, which orchestrates all loyalty-related operations. This system interfaces with the underlying blockchain layer, where smart contracts govern campaign rules and transaction logic. A block-explorer layer continuously monitors on-chain activity and stores relevant events in the Postgres database, which not only supports downstream analysis but also continuously feeds the Blockscout frontend to ensure real-time visibility of blockchain activity. The records maintained in the database serve as inputs to the fraud-detection pipeline, which combines rule-based controls with an AI-driven classification model to assess the legitimacy of each transaction. Based on this assessment, the system either accepts or rejects the operation, and this decision is forwarded back to the blockchain layer so that approved transactions are finalized on-chain while rejected ones are prevented from being committed to the ledger.

The workflow initiates with a forthcoming transaction. The transaction engages with the blockchain via a graphical user interface or an automated process within a smart contract. The rule-based fraud prevention layer of the blockchain signer evaluates the transaction prior to its entry into the blockchain. The JavaScript regulations are established to manage transactions in a passive manner. The "Accept Transaction" function within the Rule Based layer transmits the transaction. Once a transaction is broadcasted and included in a block, Blockscout continuously indexes the new block, extracts

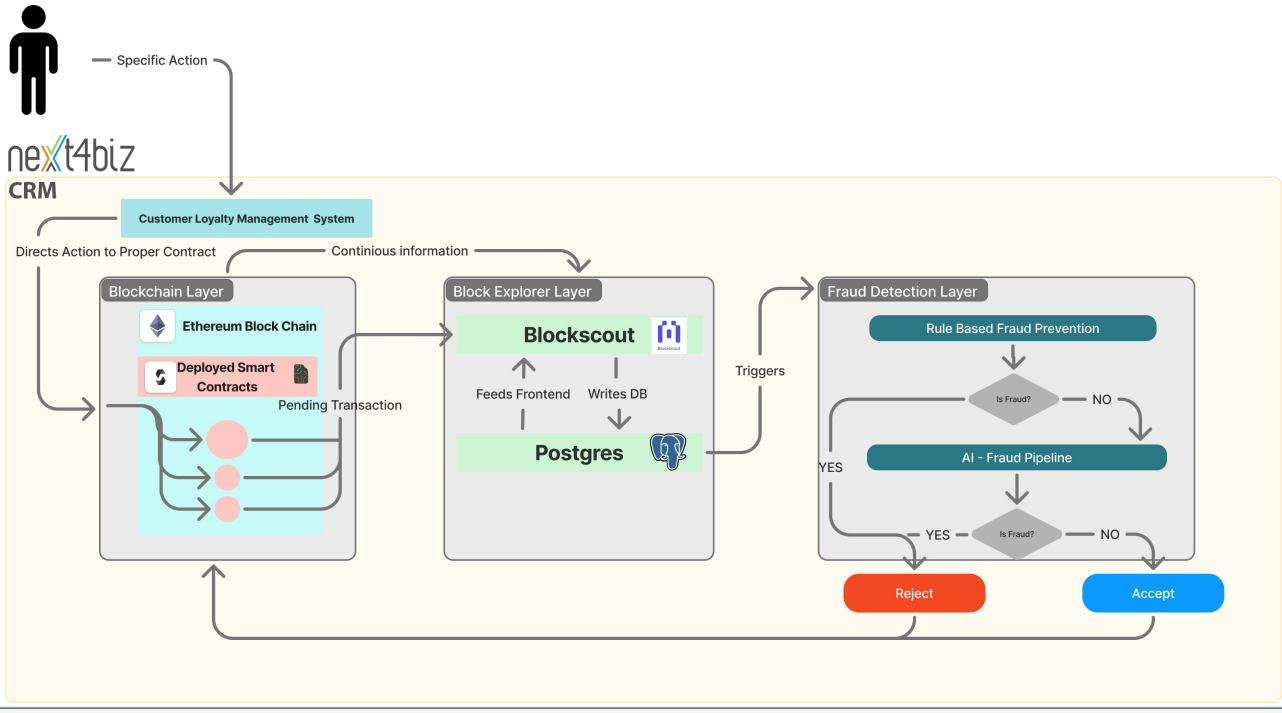



**Fig. 2.** Transaction-level fraud detection pipeline in a blockchain-based loyalty system.

transaction logs, and enriches them with metadata such as event signatures, sender/receiver mappings, and token transfer information. These indexed records are written into the Blockscout Postgres schema, where custom triggers forward relevant entries to the analytics tables used by the fraud detection pipeline. The pipeline operates within a Python-based service which listens for changes occurring in the analytics table through Postgres' asynchronous communication mechanism. Whenever the service is notified on an insertion to the analytics table, it examines the inserted row to determine if it is a user transaction. Then, the service initiates the fraud detection pipeline. The pipeline starts by querying corresponding tables from Postgres to feature engineer the transaction data. This includes the utilization of saved ABI codes of the contracts to parse parameters used in contract calls. After obtaining the parameters, several statistics are calculated about the user wallet such as number of campaigns the user has ever contributed, how many points user has spent, etc. Subsequently, the pipeline encodes and normalizes input data with prestored encoder and normalizer objects. Finally, preprocessed transaction data is given as an input to the model for prediction. Based on the model's classification, the transaction is either accepted or rejected before being written to the ledger. This mechanism provides a reliable and low-latency data bridge between the blockchain and AI layers, ensuring that inference can occur shortly after block finalization. Fig. 2 depicts the workflow of the system designed for the management of fraudulent transactions. The following sections of the methodology chapter will offer a comprehensive explanation of the pipeline outlined here.

In the deployed scenario, decisions for fraudulent transaction detection are calculated before the finalization of the block, and this allows the transaction to be analyzed shortly after it enters the pending state. Based on the 5-second block interval of the private PoA network, it can be identified that the delay in the operation in the fraud pipeline state will be in the range of 10–25 ms, irrespective of whether it is blocked or not. Though the proposed ANN model remains computationally light, taking into account the server usage and the current containerization process setup, it can be observed that the average reaction time remains in the range of 4–10 ms. Thus, the total reaction time for fraudulent action detection remains in the range of 20–40 ms.

### A. Blockchain Platform

The customer loyalty platform has been developed on a private blockchain utilizing Ethereum technology. Multiple blockchain frameworks were evaluated, including Besu, Hardhat, Hyperledger Fabric, and Geth. Geth (Go-Ethereum) was ultimately chosen for its flexibility and strong community support. Smart contracts enhance platform functionality by securing transactions, granting permissions, creating campaigns, and facilitating rewards distribution. Smart contracts are developed utilizing the Solidity programming language.

The Clique network of the GETH framework establishes the architecture for the blockchain platform. The Clique network inherently utilizes PoA consensus. In the case studies, the employed consensus mechanisms (PoS, PoW, etc.) were compared with the state-of-the-art PoA consensus, and PoA was determined to be advantageous due to its energy efficiency, scalability, and security [16].Proof of authority consensus is a mechanism whereby only designated signers possess the authority to generate blocks within a blockchain. The design includes a voting mechanism enabling each signer to authorize or de-authorize a new signer. The initial authorized signers can only be allocated by the genesis block, and modifications can only occur through forks.

From a scalability standpoint, having a PoA as a consensus algorithm assures reliable and efficient block generation, which makes

it adequate for loyalty schemes that involve frequent processing of low-value transactions. A total block time of 5 seconds, complemented by the two-node system by archive nodes and full sync nodes, ensures efficient synchronization of transactions as the number of users escalates. While this current study is focused on functional integration, in future studies, stress testing, scaling analysis of nodes, as well as system throughput, would also be taken into account to assess scalability in real-world applications of this system more comprehensively.

The genesis block represents the initial block within the blockchain structure. The creation of the Genesis Block is a pivotal event in blockchain development, as it establishes the initial parameters, defines the block structure, initiates the transaction ledger, and implements the PoA consensus mechanism. The Genesis Block establishes the initial signer addresses. Two distinct signers have been established to function on separate nodes for testing purposes. One node functions as an archive node, while the other operates as a full sync node. The distinction lies in the fact that if the chain halts or experiences a failure, the archive node retains all transactions and synchronizes them for the block explorer. Both nodes function as signers. Scalability within the blockchain framework presents a significant challenge for numerous cryptocurrencies [17]. In the project discussed, scalability is essential for a configuration intended for thousands of users. The block time has been established at 5 seconds, indicating the interval for the generation of consecutive blocks.

**B. Contract Environment**

Smart contracts are immutable code segments recorded on a blockchain network, programmed to execute automatically upon the fulfillment of specified conditions. A blockchain lacking smart contracts operates within a restricted scope. Smart contracts encompass the complete functionality of the blockchain platform [18].The design of the platform architecture is guided by high security and automated principles. Solidity is employed for the development of smart contracts, while Python is utilized for their integration on the blockchain. This research examines several significant contracts, specifically Access Control, Loyalty Token, Campaign Factory, and Campaign contracts. The main aim of the Access Control contract is to allocate access roles to the addresses of tenants that are designed to engage with other contracts. All contracts inherit from Access Control contract for authorization. Loyalty Token contract, which inherits from ERC-20, manages and generates loyalty tokens. The tenant is able to utilize the Campaign Factory contract for the creation and dissemination of campaigns on the blockchain. When tenants execute a campaign on the campaign factory contract, it generates a new contract with a distinct address, incorporating selections from the tenant, including the campaign name, reward amount, and campaign date. Fig. 3 illustrates the fundamental architecture of the contracts.

**C. Evaluation and Selection of Block Explorer**

This research involved testing some of the block explorers, including Chainlens, Dora, and Blockscout, to find the most suitable tool for the project. Blockscout Explorer was the final option due to its performance, compatibility, and easy integration advantages. Blockscout block explorer, as an open-source project, follows and records the transactions on the loyalty program. Like in the Chainlens project, the network's health and maintenance are followed through Grafana and Prometheus. Blockscout utilizes Nginx to manage load balancing in situations of high traffic and PostgreSQL and Redis for data storage, providing a quicker option than MongoDB. The findings indicate that while Chainlens is deployed using Docker and employs

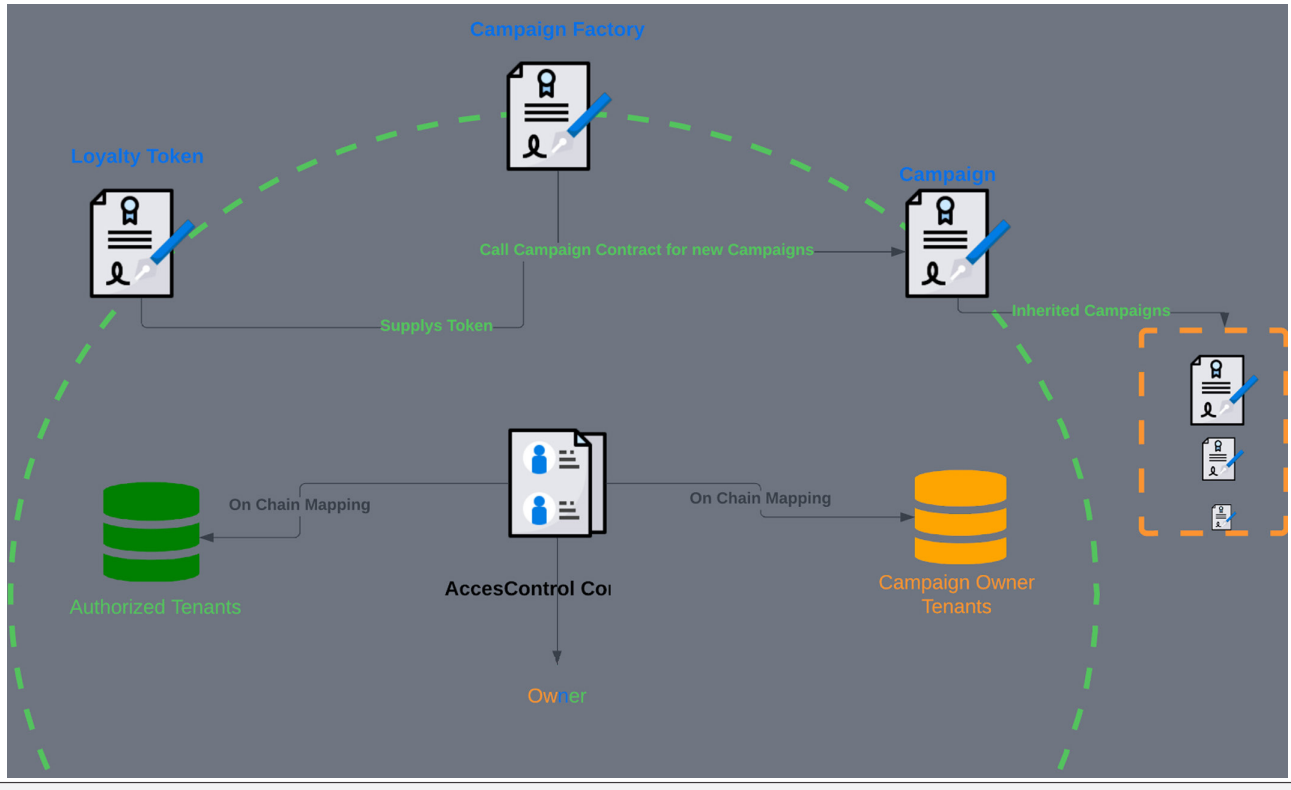



**Fig. 3.** Architecture of smart contracts.

MongoDB for data storage, it experiences delayed backup and data retrieval times, particularly in use cases where real-time data processing is required. Additionally, its inconsistencies in balance calculations were not suitable for the project.

Dora Chain Explorer, developed by ETHPANDAOPS, uses Kurtosis to operate containerized service environments through Docker and Kubernetes. However, as the project involves a private Ethereum chain, Dora's inclusion of Kurtosis introduced additional complexity and compatibility issues with PoA consensus algorithms. Blockscout, however, is suitable to meet the present needs due to its simple installation via Docker and PostgreSQL and good community support. Due to its enhanced data-processing ability, high performance speed, and compatibility, Blockscout was chosen to implement in the project.

**D. Security Mechanisms and Vulnerability Mitigation**

The local replica of the Ethereum blockchain platform functions on a designated private network and employs PoA consensus as part of the project's architecture. The PoA mechanism improves network security by allowing transaction verification solely via confirmed addresses. Utilizing blockchain technology instead of conventional loyalty programs will enhance data accessibility, ensure data security, and provide verification through transparently shared information. Blockchain technology utilizes advanced cryptographic methods, ensuring a high level of data encryption that protects the confidentiality of critical customer information and reduces vulnerability to unauthorized access [19].

Smart contracts lack effective mechanisms to prevent re-entry attacks. In such attacks, an attacker repeatedly invokes a function before the previous execution is finalized, thereby exploiting inconsistent contract states and obtaining an unfair advantage. Smart contracts are developed utilizing the check-effect-interact (CEI) pattern with the Solidity programming language to mitigate these vulnerabilities. OpenZeppelin's reentrancy guard mechanism has been implemented across all contracts. The CEI pattern and OpenZeppelin's mechanism will mitigate potential reentrancy attacks, thus protecting the network from such vulnerabilities.

During the development of the prototype contracts using the Solidity programming language, mathematical calculation errors were identified in earlier versions of Solidity. These errors result in significant consequences, including rounding the integer to its maximum or minimum value. The inclusion of the *safemath* library in the contract enhancements will mitigate the mathematical errors that have significant consequences in previous versions. The roles established in the smart contract limit the actions permissible for the respective control units, facilitating the distribution of contracts across the network. This access control will safeguard essential actions, including the creation, cessation, and modification of the campaign. Furthermore, this study employs the previously described pipeline, which incorporates rule-based fraud prevention techniques developed in Javascript and artificial intelligence models trained in Python to effectively protect against fraudulent transactions both actively and passively.

In particular, while the security analysis is focused on Solidity level issues such as reentrancy attacks or arithmetic anomalies, network attacks like Sybil attacks or denial of service attacks on the network, as well as adversarial data level attacks, are out of the threat model of this work. Indeed, this is intended as part of the scoping of this work and in view of the fact that the system at hand runs on a private permissioned PoA blockchain network in which the validity of the actors and their membership in the network are controlled. Accordingly, the security analysis prioritizes contract-level robustness, which is the primary attack surface relevant to the fraud-detection workflow examined in this study.

Apart from those measures already deployed at the contract level, to further augment security, this design proposes a hybrid on-chain/off-chain risk assessment model. The combination of a rule-based anti-fraud layer and an AI-assisted detection component makes it possible to undertake preventive screening of transactions prior to recording them to the blockchain, protecting against potential vulnerabilities commonly missed in state-of-the-art on-chain methods of ensuring data integrity for critical applications. Finally, in addition to PoA's requirement for signers to only allow those who have been verified to create blocks, this proposal makes them even more resistant to potential vulnerabilities of Sybil attacks, unauthorized block creation, as well as attacks to consensus, as compared to previous PoW-based systems like Bitcoin's current infrastructure.

**E. Dataset**

This study employs various ML models and artificial neural networks (ANNs) to improve security measures for detecting potential fraud in a blockchain-based customer loyalty platform. To train models for fraud identification, a dataset compatible with the blockchain network's contracts and the platform's data structure is necessary. The lack of suitable open-access datasets necessitated the construction of the own for the purposes of this research.

A total of 100,000 artificial user wallets, campaigns, and marketable items were generated to establish a synthetic training dataset. The platform assigned artificial user wallets at random to engage

**TABLE I.** SYNTHETIC DATASET COMPOSITION

| Column | Non-Null Count | Data Type |
|---|---|---|
| function_name | 197458 non-null | object |
| product_quantity | 197458 non-null | float64 |
| product_price | 197458 non-null | float64 |
| points_sent_amount | 197458 non-null | float64 |
| reward | 197458 non-null | float64 |
| balance | 197458 non-null | int64 |
| points_rewarded | 197458 non-null | float64 |
| points_retrieved | 197458 non-null | float64 |
| points_sent | 197458 non-null | float64 |
| points_spended | 197458 non-null | float64 |
| reward_count | 197458 non-null | float64 |
| send_count | 197458 non-null | float64 |
| retrieve_count | 197458 non-null | float64 |
| spend_count | 197458 non-null | float64 |
| target | 197458 non-null | float64 |

with the generated artificial campaigns. Subsequently, these users engage in random token transfers among themselves to obtain artificial discount coupons and products available in the market. These steps facilitated the inclusion of authentic transactions within the blockchain network, reflecting actual transfers and redemptions. Afterwards, fraud scenarios from loyalty programs were examined and incorporated into the network. The scenarios include: exploitation of the new user advantage; fraudulent transactions by personnel of tenant companies; fraud via referral campaigns; misuse of campaigns and interrelated market products; and scenarios involving account theft. Randomness was incorporated into the fraud scenarios during coding to replicate the complexity of actual data. The outlined steps have generated synthetic training data that aligns with the platform's architecture, enabling the training of artificial intelligence models on the blockchain network. Table I indicates that the dataset contains 197 458 instances (rows) and 15 features (columns), encompassing a range of data types, including integers, floats, and categorical variables.

**F. Models and Metrics**

A 3-layer ANN model was trained with the generated synthetic data, utilizing various shallow ML models such as Random Forest [20],XGBoost [21],Passive-Aggressive, and the Keras framework [22] for constructing the ANN model. The study employed two distinct model types: shallow ML models and a neural network model. This research utilized numerous ML algorithms such as Extra Tree [23],Random Forest, XGBoost Classifier, Logistic Regression, and Support Vector Classifier (SVC) (binary SVM), to investigate the effectiveness of enhancing blockchain security. Random Forest classifiers exemplify an ensemble learning technique that builds multiple decision trees during the training phase, subsequently producing a class that reflects the mode of the individual trees. Extra Trees differ in that they create multiple decision trees through random selection of features and split points, resulting in reduced variance and enhanced generalization relative to conventional decision tree approaches.

The XGBoost classifier, or Extreme Gradient Boosting, is a gradient-boosting algorithm recognized for its superior performance and efficiency. XGBoost constructs trees in a sequential manner, where each subsequent tree addresses the errors of its predecessors. Logistic regression is a linear classification technique that estimates the likelihood of an instance being assigned to a specific class. The final traditional ML model, SVM [24],serves as a classification model that identifies the optimal hyperplane for separating classes within high-dimensional space.

An ANN was utilized as the second type of model. A three-layer ANN architecture was utilized to address the classification task of fraud detection. The network architecture was constructed utilizing the Keras deep learning library, featuring ReLU activation functions in the hidden layers and a Sigmoid activation function in the output layer for binary classification. The Adam optimizer [25]and the binary cross-entropy loss function were used to facilitate probability-based predictions. Fig. 4 illustrates the architecture of the ANN.

The model performances are evaluated using five primary measures related to classification efficacy: F1-Score, Precision, Recall, ROC AUC, and PR AUC. The precision metric calculates the ratio of true positives to total number of positive guesses made by the model. In other words, it reflects how precise the model's guesses are. Recall computes the proportion of true positives out of all actual positive classes in the test data. This metric reveals how well the model detects positive classes. There is a well-known trade-off between precision and recall. For instance, if a low threshold is set for detecting positive classes, the model might catch all the positive examples. However, a small threshold might also lead to incorrectly classifying negative examples as positive, resulting in lower recall metric. The F1-score is a single metric to evaluate model performances by computing the harmonic mean of precision and recall. It is especially used with imbalance datasets to obtain a better measure than accuracy. Receiver operating characteristic is a curve that illustrates the correlation of

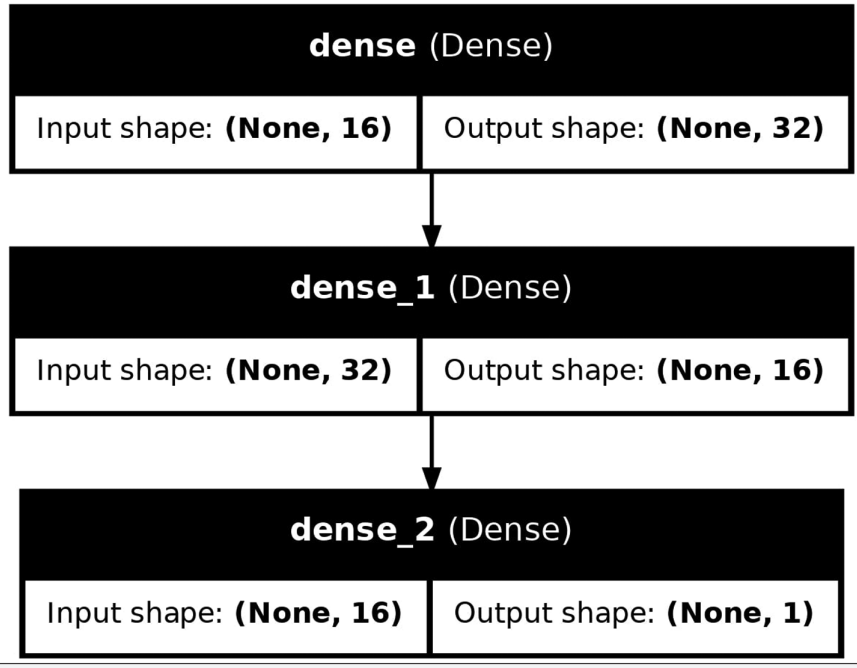



**Fig. 4.** Three-layer artificial neural network architecture.

true positive rate with false positive rate for different thresholds. Precision–Recall curve (PR curve) depicts the tradeoff between precision and recall for various thresholds. Area-under-curve metric, as it can be understood from the name, is a metric which allows these curve metrics to be expressed in a single value metric.

## III. EXPERIMENTAL RESULTS AND DISCUSSION

### A. General Findings

This study evaluates the effectiveness of well-known ML methods and a robust 3-layer ANN in identifying fraud within a blockchain-based loyalty platform, utilizing synthetically generated data on consumer usage and fraudulent behavior. All experiments were done on a dedicated research workstation, which operates under Ubuntu 22.04.5 LTS, featuring an Intel i9-14900KS CPU, a NVIDIA A6000 GPU, 128GB of RAM. This work utilizes both train/test split and cross validation procedures to obtain accurate performance results. For the purpose of constructing the train and test sets, the produced dataset has been grouped by user wallets which ensures that trained models do not learn from any previous transactions of fraudulent wallets that appear in the test set, preventing any kind of information leakage. Afterwards, the grouped dataset has been shuffled and divided into train and test sets, according to 80–20 stratified percentage split. To further verify the results, five-fold cross validation was done to ensure models obtain similar scores among different folds, presenting low variance. Folds are stratified and grouped in the same way as the train/test sets. The ANN model has been trained for ten epochs using 0.001 learning rate on Adam optimizer. The optimal number of epochs has been chosen by observing the train and test losses.

The experiments have been done on this section makes use of a synthetic test set described above, which is meticulously prepared to represent the real-world fraud transactions and customer behaviors, however, still this cannot be substitute for the real transactions. Therefore, the results here would not assure the performances of these selected models with real-world data. But we expect model performances and the model rankings to be close to the findings, considering the feature structure being the same, distributions of the target classes being similar and the injected fraudulent transactions were derived from the past occurrences.

Machine learning models each have their own weaknesses which must be acknowledged before evaluating their performances. The ANN typically require longer training times and provide lower interpretability compared to tree-based ensemble models, which inherently offer feature importance insights. Tree-based models may struggle with imbalance sets since gini and entropy do not account for rare classes. Logistic Regression tends to underfit due to its reliance on linear decision boundary. Support Vector Machines do not scale well with large datasets and exhibits a slow prediction time. Beyond these individual weaknesses, all of these models are unable to capture the sequential nature of fraudulent transactions, omitting valuable patterns. The experimental results demonstrate the better efficacy of neural network and tree-based ML methods. Table II presents the fraud classification performances of seven distinct models on the test set.

**TABLE II.** PERFORMANCE COMPARISON OF MACHINE LEARNING MODELS ON THE TEST SET

| Model Name | F1 Score | Precision | Recall | ROC AUC | PR AUC |
|---|---|---|---|---|---|
| Extra Tree | 0.60 | 0.93 | 0.44 | 0.72 | 0.69 |
| Random Forest | 0.62 | 1.00 | 0.44 | 0.72 | 0.72 |
| 3-Layer ANN | 0.66 | 0.89 | 0.52 | 0.9975 | 0.72 |
| XGBoost | 0.62 | 1.00 | 0.44 | 0.76 | 0.72 |
| Logistic Regression | 0.53 | 1.00 | 0.37 | 0.68 | 0.68 |
| SVC | 0.48 | 0.97 | 0.32 | 0.66 | 0.66 |
| Ridge Classifier | 0.17 | 1.00 | 0.10 | 0.55 | 0.54 |

F1-score is often preferred as a single number summary metric about how well the model performs. However, in extremely imbalance datasets where negative class dominates, such as in fraud detection, it can give subtly pessimistic scores. This problem occurs because both precision and recall metrics, which are used to calculate F1-score, do not take the number of false positives into account. Even with this slight drawback, the trained models obtained satisfactory F1-scores. The ANN model achieved an excellent F1-score of 0.66, surpassing the second highest score of 0.62 obtained by the XGBoost and Random Forest models. The SVM model yielded inadequate F1-score of 0.48, whereas Ridge Classifier exhibited a remarkably poor score of 0.17.

The ANN model demonstrated superior performance in the ROC AUC metric, achieving a score of 0.9975. Regarding the PR AUC metric, all ANN, XGBoost, and Random Forest models achieved an identical maximum score of 0.72. The 3-layer ANN demonstrated remarkable performance across most of the metrics compared to the evaluated models, indicating its effectiveness in identifying fraudulent activities within the customer loyalty sector. Investigating the cross-validation metric results of these models yields insights into the significance of their performance and their generalizability across different subsets. Table III reports 5-fold cross-validation results of selected models including the mean and standard deviation across the five folds.

**TABLE III.** 5-FOLD CROSS-VALIDATION PERFORMANCES OF MACHINE LEARNING MODELS (M ± Σ)

| Model Name | F1 Score | Precision | Recall | ROC AUC | PR AUC |
|---|---|---|---|---|---|
| Extra Tree | 0.62 ± 0.013 | 0.91 ± 0.009 | 0.47 ± 0.022 | 0.75 ± 0.023 | 0.69 ± 0.018 |
| Random Forest | 0.61 ± 0.012 | 0.96± 0.014 | 0.45 ± 0.021 | 0.74 ± 0.018 | 0.71 ± 0.021 |
| 3-Layer ANN | 0.66 ± 0.012 | 0.91± 0.011 | 0.52 ± 0.016 | 0.9942 ± 0.006 | 0.72 ± 0.017 |
| XGBoost | 0.62 ± 0.01 | 0.95± 0.013 | 0.46 ± 0.018 | 0.75 ± 0.016 | 0.72 ± 0.019 |
| Logistic Regression | 0.52 ± 0.013 | 0.96± 0.01 | 0.36 ± 0.016 | 0.70 ± 0.024 | 0.68 ± 0.018 |
| SVC | 0.5 ± 0.012 | 0.96± 0.01 | 0.34 ± 0.009 | 0.67 ± 0.014 | 0.67 ± 0.015 |
| Ridge Classifier | 0.16 ± 0.006 | 1.00± 0 | 0.09 ± 0.007 | 0.55 ± 0.008 | 0.55 ± 0.011 |

The cross-validation results demonstrate the mean of performances closely align with the findings from the test set. Moreover, the standard deviations of those metrics show that there is relatively low variance among the folds, suggesting minimal learning of the training

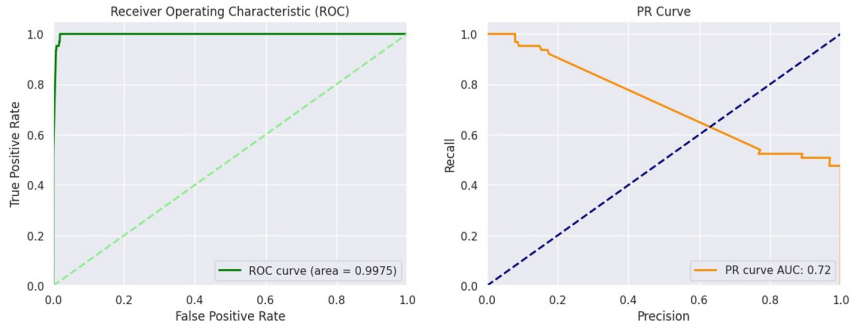



**Fig. 5.** a) ROC curve b) PR curve.

data noise. This is crucial as it provides a measure of generalization capability on unseen data. Consistent with the test set evaluation, the ANN model obtained the best results across F1-score, Recall, ROC AUC and PR AUC metrics. Observing recall and precision in isolation can be misleading since there is a well-known trade-off between them. The area under the precision-recall curve provides a more comprehensive measure. The PR AUC performances of XGBoost, ANN and Random Forest are overlapping each other when we take the standard deviations into account.

The ROC AUC performance of the ANN is markedly higher than other models, leaving no uncertainty regarding significance of this difference. However, the ANN's F1-score is closely followed by XGBoost, Random Forest, ExtraTree Classifier. Therefore, paired t-tests were employed to analyze whether performance improvements of ANN over the other models are statistically meaningful. The null hypothesis for the paired t-tests is that the mean difference of F1-scores between two models is zero. The F1-scores of XGBoost, Random Forest and ExtraTree are tested against ANN's F1-score to determine if the ANN's improvement on this metric is significant. The p-values obtained from paired t-tests are 0.009, 0.0048, 0.0231, respectively. By choosing a significance level of 0.05, paired *t*-tests reveal the ANN's improvement on F1-score over the other models is significant.

Analyzing ROC and PR curves itself provides useful insights into model performances across different thresholds (as indicated by the ROC curve) and the balance between precision and recall. Fig. 5a illustrates the ROC curve, while Fig. 5b presents the PR curve for the 3-layer ANN.

The ROC curve of the ANN model is positioned near the upper-left corner of the graph, indicating its effectiveness in distinguishing between legitimate and fraudulent transactions. It effectively distinguishes more fundamental legitimate transactions by assigning them a low prediction score. The near-perfect performance of the model related to the ROC curve does not mean that the model is

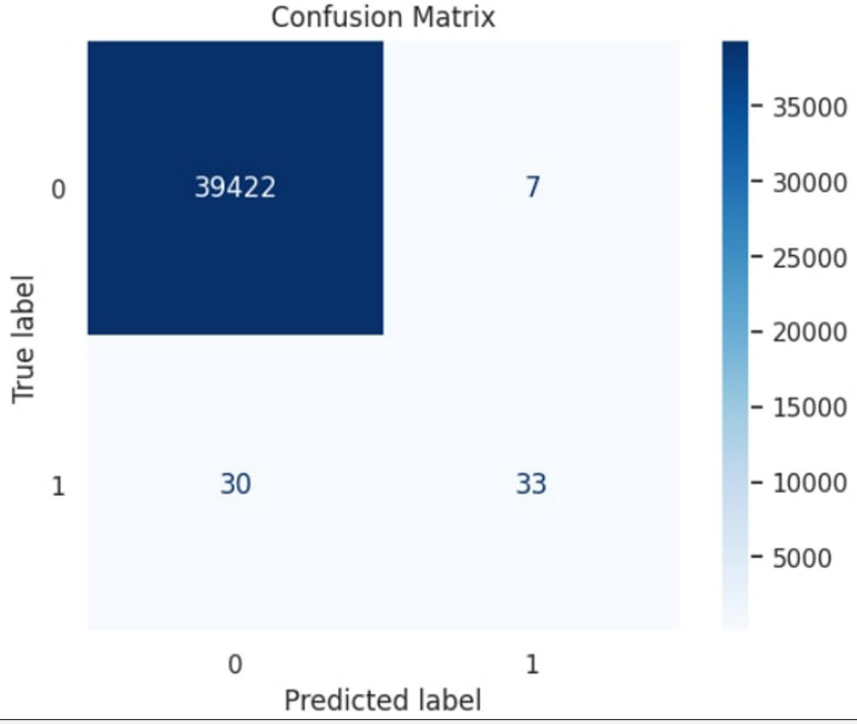



**Fig. 6.** 3-Layer ANN model confusion matrix for fraud detection.

overfit or a result of a synthetic dataset, but a consequence of the imbalance distribution of the target class which is highly common in fraud detection. Nevertheless, inspecting the ROC curve gives us some important insights such as how much the model is truly confident in its detections. The graph indicates that the true positive rate remains constant in the left section. This suggests that the model does not allocate low probabilities to fraudulent transactions, despite its inability to classify them as such.

Furthermore, an analysis of the PR curve for ANN models indicates that the model achieves a commendable balance between precision and recall. In fraud detection tasks, maintaining a high recall score is essential for identifying a significant number of fraudulent transactions; however, this often results in a reduction in precision. The PR curve of the ANN model indicates that when configured to detect 90% of all fraud instances, the precision is approximately 20%. This implies when the threshold is set to detect 90% of the fraudulent transactions, out of every ten fraud predictions made by the model, two are accurate. Alternatively, maintaining a high precision for guesses, approximately 80%, would result in the model identifying around 50% of all fraudulent transactions. The threshold can be altered according to what is wanted to be achieved. The threshold was set to achieve 0.6 precision and 0.6 recall for the launch of the loyalty program in order to maintain a great balance between number of detected frauds and false positives.

Confusion matrices facilitate the evaluation of model performance by displaying prediction outcomes at a specified threshold, indicating whether predictions are correct, mispredicted, missed, or incorrect. Fig. 6 illustrates the confusion matrix for the leading model, a 3-layer ANN. The selected threshold for this confusion matrix is 0.5, which is the default value.

The 3-layer ANN model demonstrates exceptional performance in accurately classifying fraud cases while maintaining a minimal rate of false positives at the 0.5 threshold. The model can be implemented on a platform to automatically halt transactions, as it misclassifies legitimate transactions as fraudulent only once in every 5632 instances, which corresponds to an excellent false-positive rate of 0.00017, while successfully interrupting 52% of all fraudulent transactions before they are complete.

### B. Comparison with Recent Blockchain Security Studies

Recent studies on blockchain security have mostly been about making cryptographic resilience and decentralized access control mechanisms stronger. For instance, a proposed hybrid quantum-blockchain architecture combines post-quantum encryption (Kyber) [26],IPFS-based storage, and a quantum-enhanced PoW protocol to make healthcare systems' long-term cryptographic security better. That work mostly deals with security at the infrastructure level and how strong consensus is against future quantum threats.

In the same way, a different study describes a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme that uses blockchain technology and is aware of its surroundings to share data safely in Internet of Medical Things (IoMT) environments [27].It focuses on fine-grained access control and attribute-based encryption to keep private information safe in distributed medical systems. The Cx-CP-ABE framework [28]builds on this work by combining context-aware ciphertext-policy attribute-based encryption with blockchain technology to make health data privacy more scalable and dynamic. The scheme improves fine-grained authorization in distributed healthcare systems by adding contextual parameters to access policies. Its main contribution, however, is still in cryptographic access governance, not in transaction-level behavioral analysis or fraud detection in blockchain applications.

Recent studies have also looked into using AI to analyze blockchain transactions. For example, a study on blockchain analytics combines several ML classifiers to improve the detection of fraud and anomalies in ledger transactions [29].That work focuses on comparing the performance of different classifiers and optimizing hybrid machine learning, but the framework puts supervised risk scoring right into the transaction lifecycle of a permissioned PoA network. This lets suspicious loyalty operations be rejected before they happen instead of after they happen. PrivChain-AI [30]is another related direction that combines blockchain governance with federated learning to protect financial reporting while keeping data private. This architecture improves privacy-preserving collaborative model training, but its main goal is still secure data exchange and reporting integrity. On the other hand, the work focuses on modeling behavioral fraud that is specific to applications within loyalty ecosystems. This means that AI-based anomaly detection is combined with smart-contract execution logic to reduce operational risk. In general, these studies strengthen blockchain security at the cryptographic, access-control, and analytical levels. The framework, on the other hand, adds to these areas by adding deployment-ready, transaction-level fraud intelligence to a loyalty infrastructure that is specific to the domain.

## IV. CONCLUSIONS

This study introduces an innovative strategy for enhancing the security of blockchain-based loyalty programs by incorporating ML-driven fraud detection techniques. This study utilizes blockchain's decentralized and immutable framework to address significant issues in loyalty programs, including fraud prevention and operational transparency. The trained models attained promising results in a carefully designed synthetic setup, with the ANN exhibiting exceptional performance, reaching an F1-score of 0.66 and a ROC AUC score of 0.9942, surpassing competing ML models like XGBoost and Random Forest. Furthermore, the ANN achieved a PR AUC value of 0.72, indicating an effective balance between accuracy and recall in fraud detection. The results underscore the efficacy of AI-driven methodologies in preserving loyalty programs, as the model effectively detected and interrupted 52% of fraudulent transactions before its conclusion, while maintaining a low false-positive rate. The trained ANN model will be employed to detect fraudulent transactions upon the launch of the loyalty program, allowing a more secure platform from day one. As user data accumulates in the blockchain, the model will be retrained using the same pipeline as in the synthetic setup.

This study enhances the existing literature on blockchain and AI integration by providing a scalable and efficient fraud detection framework for loyalty programs. The study uses synthetic data to replicate authentic fraud tendencies, offering a versatile methodology suitable for many loyalty program frameworks. The preliminary results indicate that the integration of blockchain technology with advanced ML models can enhance the security of loyalty programs by mitigating fraud, augmenting transparency, and bolstering trust among stakeholders. Subsequent study may enhance the model's adaptability to novel fraud strategies and investigate its applicability in more decentralized platforms, thereby bolstering the reliability

of blockchain-based loyalty programs in an increasingly digital marketplace.

Future research directions may focus on enriching the dataset with real transaction data from active loyalty platforms, thereby reducing distribution shift during evaluation and improving the robustness and precision of the final models in fraud detection. Furthermore, investigating the synthesis of this blockchain-based fraud detection framework with multi-chain ecosystems may provide insights into cross-platform fraud mitigation.

**Data Availability Statement:** The data that support the findings of this study are available on request from the corresponding author.

**Artificial Intelligence Usage Statement:** The authors declared that no artificial intelligence tool was used in the preparation of the manuscript.

**Peer-review:** Externally peer-reviewed.

**Acknowledgements:** The authors would like to thank TÜBİTAK for its financial support provided within the scope of the TEYDEB program.

**Author Contributions:** Concept – A.A., M.A.A.; Design – A.A., C.I., M.F.O.; Supervision – A.A., M.A.A.; Resources – A.A., A.E.C.; Materials – A.E.C.; Data Collection and/or Processing – C.I., M.F.O., A.E.C.; Analysis and/or Interpretation – C.I., M.F.O., A.A.; Literature Search –C.I., M.F.O.; Writing – C.I., M.F.O., A.A.; Critical Review – A.A., M.A.A.

**Declaration of Interests:** The authors have no conflicts of interest to declare.

**Funding:** This study was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under TEYDEB Grant No. 3240695.

## REFERENCES

1. Peppers D, Rogers M. *Managing Customer Experience and Relationships: A Strategic Framework*. John Wiley & Sons; Chichester, UK; 2016.
2. Faria J. Global spend on loyalty as part of the marketing budget 2024, by country; 2025,. Statista. https://www.statista.com/statistics/1603064/marketing-budget-dedicated-to-loyalty-worldwide-by-country/.
3. Ernst and Young. Unmasking loyalty scheme fraud; 2024, https://www.ey.com/content/dam/ey-unified-site/ey-com/en-ca/insights/financial-services/documents/ey-designed-loyalty-fraud-whitepaper-mvf.pdf.
4. Clohessy T, Acton T, Rogers N. Blockchain adoption: technological, organisational and environmental considerations. In: Treiblmaier H., Beck R., eds. *Business Transformation through Blockchain*; vol I. Springer International Publishing; Cham; 2019:47-76. [CrossRef].
5. Anudeep C, Santosh K, Kumar MS, et al. Constructing a blockchain-based loyalty program model for secure and transparent customer rewards in retail marketing. In: 13th International Conference on Communication Systems and Network Technologies (CSNT). IEEE; New York; 2024, 241-247. [CrossRef].
6. Kılıc B, Sen A, Özturan C. Fraud detection in blockchains using machine learning. In: 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA). IEEE; New York; 2022, 214-218.
7. Bogdanović Z, Labus A, Radenković M, et al. A blockchain-based loyalty program for a smart city. In: World Conference on Information Systems and Technologies. Cham: Springer International Publishing; 2021, 360-370.
8. Pranto TH, Hasib KTAM, Rahman T, et al. Blockchain and machine learning for fraud detection: a privacy-preserving and adaptive incentive based approach. *IEEE Access*. 2022;10:87115-87134. [CrossRef]
9. Ashfaq T, Khalid R, Yahaya AS, et al. A machine learning and blockchain based efficient fraud detection mechanism. *Sensors*. 2022;22(19):7162. [CrossRef]
10. Bello NHO, Idemudia NC, Iyelolu NTV. Integrating machine learning and blockchain: conceptual frameworks for real-time fraud detection and prevention. *World J Adv Res Rev*. 2024;23(1):56-68. [CrossRef]
11. Bhowmik M, Sai Siri Chandana TSS, Rudra B. Comparative study of machine learning algorithms for fraud detection in blockchain 6th International Conference on Computing Methodologies and Communication (ICCMC); 2021:539-541. [CrossRef]
12. Farrugia S, Ellul J, Azzopardi G. Detection of illicit accounts over the Ethereum blockchain. *Expert Syst Appl*. 2020;150:113318. [CrossRef]
13. Pham T, Lee S. Anomaly detection in Bitcoin network using unsupervised learning methods. *arXiv*; 2016. Cornell University. [CrossRef]
14. Abooleet S, Kinnett S. A systematic review of blockchain-based loyalty programs. *Proceedings of the Annual Hawaii International Conference on System Sciences*. 2023 (HICSS-56):4. [CrossRef]
15. Zheng Z, Xie S, Dai H, et al. An overview of blockchain technology: architecture, consensus, and future trends IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017; 2017:557-564. [CrossRef]
16. Samuel CN, Glock S, Verdier F, et al. Choice of Ethereum clients for private blockchain: assessment from proof of authority perspective IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2021:1-5. [CrossRef]
17. Sanka AI, Cheung RCC. A systematic review of blockchain scalability: issues, solutions, analysis and future research. *J Netw Comput Appl*. 2021;195:103232. [CrossRef]
18. Zheng Z, Xie S, Dai H-N, et al. An overview on smart contracts: challenges, advances and platforms. *Future Gener Comput Syst*. 2020;105:475-491. [CrossRef]
19. Utz M, Johanning S, Roth T, et al. From ambivalence to trust: using blockchain in customer loyalty programs. *Int J Inf Manag*. 2023;68:102496. [CrossRef]
20. Breiman L. Random forests. *Mach Learn*. 2001;45(1):5-32. [CrossRef]
21. Chen T, Guestrin C. XGBoost: a scalable tree boosting system. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM; New York, NY, USA; 2016:785-794. [CrossRef]
22. Chollet F. *Keras*; 2015. https://keras.io. Accessed on October 6, 2026.
23. Geurts P, Ernst D, Wehenkel L. Extremely randomized trees. *Mach Learn*. 2006;63(1):3-42. [CrossRef].
24. Cortes C, Vapnik V. Support-vector networks. *Chem Biol Drug Des*. 2009;297:273-297, 01. [CrossRef]
25. Kingma DP, Ba J. Adam: a method for stochastic optimization. *arXiv* [cs.LG]; 2017. http://arxiv.org/abs/1412.6980. Accessed on October 6, 2026.
26. Annane B, Djerboua A, Alti A. A hybrid quantum-blockchain model for enhancing security in electronic health records. In: International Conference on Networking and Advanced Systems (ICNAS). IEEE; New York; 2025, 1-6. [CrossRef].
27. Annane B, Alti A, Lakehal A. Blockchain based context-aware CP-ABE schema for Internet of Medical Things security. *Array*. 2022;14:100150. [CrossRef]
28. Annane B, Alti A, Laouamer L, et al. Cx-CP-ABE: context-aware attribute-based access control schema and blockchain technology to ensure scalable and efficient health data privacy. *Secur Privacy*. 2022;5(5):e249. [CrossRef]
29. Alutaibi AI. Blockchain analytics based on artificial intelligence: using machine learning for improved transaction analysis. *IET Inf Secur*. 2025;2025(1):5560771. [CrossRef]
30. Alaklabi S. PrivChain-AI leveraging blockchain and federated learning for private financial reporting and access control. *Sci Rep*. 2025;16(1):2786. [CrossRef]



Can İşcan received a B.S. degree in Computer Engineering from İstanbul Kültür University (IKU), Türkiye, in 2023. Currently, he is pursuing a M.S. degree in artificial intelligence and data science at Heinrich-Heine-Universitaet Düsseldorf, Germany. His areas of interest cover large language models, computer vision, and blockchain. Previously, he worked as a data scientist at FormicaAI, where he developed advanced machine learning models for fraud detection purposes. Afterwards, he joined Next4biz, where he engineered Q/A chatbot systems with RAG and engineered a campaign success prediction system. He has conducted research works concerning large language models, Q&A chatbot systems, fraud detection, and blockchain-based loyalty programs.



Muhammet Furkan Özara received his B.S. degree in engineering from İstanbul Kültür University in 2018–2023. Currently, he is working as a data scientist at the Next4biz R&D center since 2022. His current research interests are NLP, generative AI, deep learning, big data, and machine learning



Ahmet Erkan Çelik received his B.S. degree in Computer Systems Teaching in 1996-22000. He worked as a teacher and product developer in various institutions affiliated with the Ministry of National Education. He has been serving as a CRM Product Development Director at Next4biz R&D Center since 2015. His current research interests are NLP, deep learning, big data, machine learning, and databases



M. Ali Aydın received the B.S. degree in computer engineering from İstanbul University, İstanbul, Türkiye, in 2001, the M.Sc. degree from İstanbul Technical University, İstanbul, Türkiye, in 2005, and the Ph.D. degree in computer engineering from İstanbul University, İstanbul, Türkiye, in 2009. He conducted postdoctoral research with the Department of Computer Science at Télécom SudParis, where he worked on advanced topics in computer networks and security. He is currently a Professor and the Head of the Department of Computer Engineering at İstanbul University-Cerrahpaşa. His research interests include cybersecurity, cryptography, network security, and communication network protocols



Akhan AKBULUT received the B.S. and M.S. degrees in computer engineering from İstanbul Kültür University (IKU), Türkiye, in 2001 and 2008, respectively, and the Ph.D. degree in computer engineering from İstanbul University, Türkiye, in 2013. From 2004 to 2013, he served as a research assistant with the Department of Computer Engineering at IKU, where he was appointed as an Assistant Professor from 2013 to 2017. Between 2017 and 2019, he was a postdoctoral researcher with the Department of Computer Science at North Carolina State University, NC, USA. In 2019, he rejoined the Department of Computer Engineering at IKU and was promoted to Associate Professor, and in 2024, he became a Full Professor. He is currently the Chairperson of the Department of Computer Engineering at IKU. Since 2023, he has also been serving as the R&D Director of Next4biz. His current research interests include the design and performance optimization of software-intensive systems, machine learning–based applications, Internet architectures, and cloud computing systems.