“Development of Secure Framework for Prevention of Crypto-Currency Crimes and Prevention of Money Laundering Using Blockchain”

Department of ECE and CSE

By,

Zorawar Singh (201010260)
Shreedhar Tiwari(201000049)
Shubham Raj (201000051)

Department of ECE and CSE

Dr. Shyama Prasad Mukherjee
International Institute of Information Technology, Naya Raipur
(A Joint Initiative of Govt. of Chhattisgarh and NTPC)
Email: iiitnr@iiitnr.ac.in, Tel: (0771) 2474040, Web: www.iiitnr.ac.in

CERTIFICATE

This is to certify that the project titled " Development of Secure Framework for Prevention of Crypto-Currency Crimes and Prevention of Money Laundering Using Blockchain." by "Zorawar Singh, Shreedhar Tiwari and Shubham Raj" has been carried out under my/our supervision and that this work has not been submitted elsewhere for a degree/diploma.

(Signature of Guide)

_____

Guide Name
Designation of Guide
Department of _____
Dr. SPM IIIT-NR
Month, Year

DECLARATION

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature of Author)

_____

Author Name
(Roll Number)

Date : _____

ABSTRACT

The problem nowadays is online transaction fraud and money laundering and also to reduce the cost of payment gateway and OTPS systems. It is possible to lose your virtual wallet or delete your currency. There have also been thefts that let you store your cryptocurrency remotely. As the value of cryptocurrency is not stable, the major con is that there can be price volatility with cryptocurrencies - meaning the profits could go up one day only to come down the next because prices change quickly. So our payment gateway (www) will try to keep the prices of crypto as much stability as possible. Also, a cryptocurrency payment gateway comes at a higher cost as compared to directly transferring payments on the blockchain. This is because crypto payment gateways are intermediaries that charge their own fees on top of the transaction fees incurred on a blockchain network. Recently, futuristic applications have increased the early detection and prevention of money laundering activities and cryptocurrency crimes. Therefore, anti-money laundering mechanisms play a vital role in preventing cryptocurrency crime, much needed around the world. Most crimes are committed to enriching the individual or group that commits the crime. Money laundering is the process of concealing illegal sources of criminal proceeds. It allows criminals to collect profits without jeopardizing the source of funds. Organized criminal activities such as illegal arms sales, smuggling, drug trafficking, and prostitution rings can bring in huge sums of money. Schemes involving computer fraud, insider trading, bribery, and embezzlement can also generate huge profits and create incentives to "justify" illicit earnings through money laundering.
When a criminal activity generates large profits, the individuals or groups involved must find ways to manage the funds without drawing attention to the underlying activities or individuals involved. Criminals do this by hiding the source of their funds, reshaping them, or moving them to lesser-noticed locations.

ACKNOWLEDGEMENT

On this great occasion of accomplishment of our Minor Project on " Development of Secure Framework for Prevention of Crypto-Currency Crimes and Prevention of Money Laundering Using Blockchain.", we would like to sincerely express our gratitude to Mr.Santosh Kumar, our supervisor who has been supportive through the completion of our project. His willingness to give his time so generously has been very much appreciated.

We would also be thankful to our respected Director Dr. Pradeep Kumar Sinha of IIIT NR for providing all the required facilities for the completion of this project.

Finally, as one of the team members, I would like to appreciate all my group members for their support and coordination. I hope we will achieve more in our future endeavors.

LIST OF TABLES

LIST OF FIGURES

Table of Contents

CHAPTER 1- INTRODUCTION

1.1 BASIC TERMINOLOGY:

- ## Cryptocurrency:

Cryptocurrency, sometimes called crypto-currency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units.

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions.

- ## Blockchain

A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in a digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions.

Blockchain is an especially promising and revolutionary technology because it helps reduce security risks, stamp out fraud and bring transparency in a scalable way.Popularized by its association with cryptocurrency and NFTs, blockchain technology has since evolved to become a management solution for all types of global industries. Today, we can find blockchain technology providing transparency for the food supply chain, securing healthcare data, innovating gaming, and overall changing how we handle data and ownership on a large scale.

For proof-of-work blockchains, this technology consists of three important concepts: blocks, nodes, and miners. Every chain consists of multiple blocks, and each block has three basic elements:

1. The **data** in the block.
2. The **nonce** — "number used only once." A nonce in the blockchain is a whole number that's randomly generated when a block is created, which then generates a block header hash.
3. The **hash** — a hash in the blockchain is a number permanently attached to the nonce. For Bitcoin hashes, these values must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined. Miners create new blocks on the chain through a process called mining. Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash.

One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the **nodes** connected to the chain. Blockchain nodes can be any kind of electronic device that maintains copies of the chain and keeps the network functioning. Every node has its own copy of the blockchain, and the network must algorithmically approve any newly mined block for the chain to be updated, trusted, and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed, creating inherent blockchain security. Each participant is given a unique alphanumeric identification number that shows their transactions.

- ## Bitcoin:

Bitcoin is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, thus removing the need for third-party involvement in financial transactions. It is rewarded to blockchain miners for the work done to verify transactions and can be purchased on several exchanges.

Launched in 2009, Bitcoin is the world's largest cryptocurrency by market capitalization. The underlying technology of bitcoin is blockchain. Blockchain technology combines multiple computer technologies such as encryption, distributed storage, consensus, and peer-to-peer (P2P) networking. These key technologies make blockchain open, secure, and trustworthy. Moreover, these techniques allow transactions to be continuously linked to the blockchain, which records all transactions and historical data by establishing a jointly maintained and untampered database.

- ## Cryptocurrency crimes

Crimes that take place in transactions having Cryptocurrency as the currency or the spending unit. There has been an increase in the percentage of these crimes in recent years. According to blockchain platform Chainalysis, cryptocurrency transaction volume went up by 567% in 2021 from 2020, while illicit transaction volume went up by 79%. Categories of illicit activity which have been growing are stolen funds and scams.

- ## Money Laundering:

In essence, money laundering is the process that involves converting illegally obtained money into what appears to be legally obtained. Money laundering is one of the most prominent crimes in the crypto market, growing by almost 30% between 2020 and 2021, according to a preview of the 2022 Crypto Crime Report report by blockchain data firm Chainalysis. Cybercriminals laundered $8.6 billion worth of cryptocurrency in 2021, and these illegal activities increased by nearly 30% between 2020 and 2021.

Money laundering is definitely a way in which cryptocurrency crime is done, especially when criminals open online accounts on digital currency exchanges that accept fiat currency from traditional bank accounts. Then the "refining process" (mixing and layering) begins where they use mixers, tumblers, and chain hopping (also known as cross-currency) to move money into cryptocurrency systems. Money is moved from one cryptocurrency to another via a digital currency exchange. It is more anonymous than other payment methods because the public keys involved in the transaction cannot be directly associated with an individual.

- **Electronic Money Laundering**:

Money can also be laundered through online auctions and sales, gambling websites, and virtual gaming sites, where ill-gotten money is converted into gaming currency, then back into real, usable, and untraceable “clean” money. The newest frontier of money laundering involves cryptocurrency, such as Bitcoin. While not totally anonymous, they are increasingly being used in blackmail schemes, the drug trade, and other criminal activities due to their relative anonymity compared with more conventional forms of currency.

Its best examples are Online Net Banking, E-commerce websites, digital currencies, Online Gambling Online video games, etc.

1.2 BACKGROUND

- Bitcoin was the first decentralized virtual money to emerge in 2009. While prior virtual currencies used centralized companies as intermediaries, this new currency gained popularity due to the lack of a third party involved in the transactions.

- The revolutionary nature of this type of currency did not allow an immediate legislative and enforcement response. AML (Anti-Money Laundering) and KYC(Know-Your-Customer) processes were not originally designed to cater for cryptocurrencies.

- Criminals, in particular cybercriminals, took advantage of the favorable environment and started using cryptocurrencies for trading on the dark web and as part of fraud and extortion schemes. Bitcoins have always been traceable and are not completely anonymous.

- Another well-known issue that opens the possibility for exploits on Bitcoin is the transaction malleability probem.

1.3 SCOPE OF THE PROJECT

- **The Future of Cryptocurrency**: Reduction of Cryptocurrency crimes can be a game changer in terms of what holds the future of digital currencies as Analysts estimate that the global cryptocurrency market will more than triple by 2030, hitting a valuation of nearly $5 billion.

- **Financial Institutions(Cryptocurrency Exchange Platform):** Cryptocurrency banking is sometimes considered an inaccurate term, as digital coins are not regulated by a central authority. Exchange companies and firms that offer services of managing digital currency are not technically banks. Cryptocurrency banking mostly just allows people to hold their funds in a digital wallet or spend it like they would spend traditional money. People can manage their cryptocurrency balances on exchange platforms. The main benefit of cryptocurrency banking is that the exchange platform allows consumers to use the digital coin balance just like any other currency to make day-to-day withdrawals and purchases, just like cash, instead of keeping it as an investment. Crypto debit cards - commonly known as bitcoin debit cards, which are issued by cryptocurrency exchange platforms, operate like prepaid debit cards.

- **Boosting the World Economy and Development**: fewer crimes means more authenticity and more economic development in terms of investment and personal savings leading to a better world economy

- **Useful and safe for people using digital payments.**

CHAPTER - 2 LITERATURE REVIEW:

2.1 OBJECTIVES

- To develop an efficient digital payment method for cryptocurrency using a payment gateway in local native languages for rural regions in tribal communities.
- To develop a secure model to identify money laundering accounts by blockchain and machine learning techniques.
- To develop a machine learning-based cooperating layering simulation method that will provide the two-phase identification of money laundering accounts and prevention of cryptocurrency crimes using blockchain techniques capable of simultaneously recommending suspicious accounts to be long-term monitored systematically and retrieving real money laundering accounts.

2.2 LITERATURE SURVEY:

1. **Global Anti-Money Laundering Governance** *(by Malcolm Campbell-Verduyn)* - This article assesses the effectiveness of the global anti-money laundering regime in balancing the challenges and opportunities presented by these new "altcoins". Two main arguments are presented. First, the implications that crypto-coins currently pose for global anti-money laundering efforts stem less from the threats of their illicit use as digital currencies and more from the opportunities offered by their underlying blockchain technologies. Second, despite several shortcomings, the risk-based approach advocated by the Financial Action Task Force (FATF) strikes an effective balance between the existing threats and opportunities that crypto-coins currently represent. Rather than a conclusive assessment, this article highlights the need for continued monitoring and exploration of the broader ethical implications CCs have raised for global anti-money laundering efforts in an era of rapid technological change. This article has argued that, despite several important limits, the risk-based approach pursued by the FATF provides an effective balance in mitigating the potential risks and real opportunities that CCs present to global anti-money laundering efforts. Its decentralized, risk-based approach was considered suitable for addressing money laundering in decentralized networks where CC transactions occur. FATF's broader approach is consistent with networked and experimental forms of governance that may be more effective than centralized forms of coercion in digital spheres, where operations can move relatively easily and quickly to less restrictive jurisdictions. However, this argument has been advanced cautiously, recognizing several risks in the risk-based approach, such as reliance on technology and market solutions.

2. **<u>Community Level anomaly detection for Anti-Money Laundering</u>** *(by Andra Baltoiu, Andrei Patrascu, Paul Irofti)* - One such example where there are more of them or less complex schemes are used to avoid transactional security protocols is financial fraud schemes. Investigation of the problem of learning graph structure representations using adaptations of dictionary learning focused on encoding connection patterns. In particular, we adapt vocabulary learning strategies to the specificity of network topologies and propose new methods that impose Laplacian structure dictionaries themselves. In one modification, we focus on the classification of topologies by direct work Laplacian graphs and cast the learning problem to fit its 2D structure. We solve the same problem by learning dictionaries that consist of vectorized atomic Laplacians and provide a block coordinate descent scheme to solve a new dictionary learning formulation. Embedding the Laplacian structure in the dictionaries is also proposed in the one-block orthogonal modification learning method. Results on sets of synthetic graphs containing different graph topologies confirm the potential of dictionaries to directly represent graph structure information. Solutions are focused on identifying anomalies structures focusing, among other things, on anti-money laundering applications. When working directly with graph structure, our method of imposing a Laplacian structure on the atoms in the dictionary produced better results compared to the standard dictionary classification algorithm and OCSVM. Our adaptation of the separable dictionary learning problem that considers nearby patterns in 2D data also represents a better alternative to the classical solution, which is indifferent to the background structure, just like OCSVM. As for the more general problem of signals lying on charts, ouran adaptation of the block orthogonal algorithm that imposes a Laplacian-like structure on the dictionary yielded similar performance compared to the classic dictionary classification method. However, with known computational advantage

CHAPTER-3 PROPOSED SOLUTION

3.1 PROBLEM STATEMENT

To develop a secure framework for the prevention of cryptocurrency crimes and money laundering using blockchain.

3.2 PROPOSED METHODOLOGY

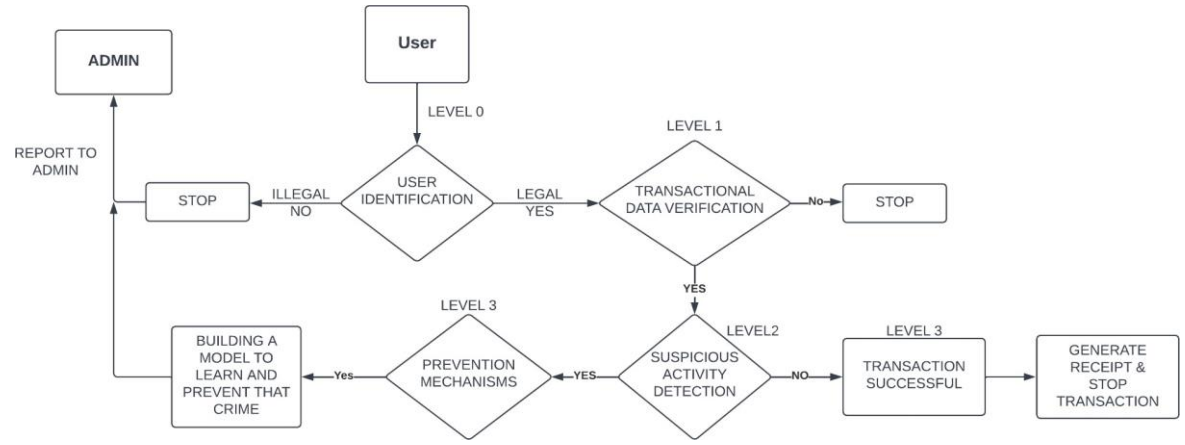


Fig 3.1 - Proposed Methodology

The proposed methodology for early prevention of cryptocurrency crime consists of the following steps:

(1) user identification,
(2) Transactional data verification,
(3) Suspicious activities detection based data pattern,
(4) prevention mechanism-based learning from given data,
(5) classification of cryptocurrency crimes or non-crime.

The suspicious activities detection-based pattern step consists of applying machine learning algorithms to detect fraud transactions by using some specific features from the dataset.

1) **User Identification:** Many crypto companies are increasingly utilizing identity verification tools to confirm users' identities as they try to achieve a balance between security, compliance, and ease. ID verification services often evaluate and verify account holders' identities by processing data from a variety of sources. This may also contain third-party data, such as voter registration data, or contextual data, like phone numbers and IP addresses, in addition to identification documents. Crypto exchanges and other businesses may drastically lower the danger of identity fraud by consulting numerous data sets. Digital identity verification i.e. Know Your Customer (KYC) method using video calls and biometrics can be an important part of user identification in cryptocurrency payments providing the information needed to quickly spot and stop fraudsters at scale while delivering a seamless and secure experience that users now expect when completing transactions.

2) **Transactional data verification:** The status and verification of any transaction can be done through the concept of Blockchain. Blockchain may be characterized as a distributed database technology in which data is kept across numerous nodes of the system rather than in a single location, preventing data corruption. Each transaction may therefore be verified by any

community member, ensuring the accuracy of the data and providing proof that it cannot be changed. To ensure that a bitcoin transaction is authentic, the transaction must be validated on a blockchain. A transaction becomes a part of the blockchain when it is confirmed, indicating that it has been included to a block. That proves the transaction has been accurately verified and recorded, enabling the processing of the payment at this time and making the transaction irreversible.

3) **Suspicious activities detection-based data pattern:** Though not every transaction following a certain pattern would result in something deemed as an unacceptable transaction, based on previous instances resulting in crypto crime, some patterns can be classified as potential crimes. One such indication is a sudden increase in the transaction volume. Transactions having an increase in the volume of the order 180-200 % within a span of say, 24Hrs is highly susceptible. Also, unusually large transactions for a particular account per say, also raise suspicion. Further, the lack of social and geological footprints calls for it to be flagged.

4) **Prevention mechanism-based learning from given data:** Some of the effective ways to prevent such activities is by trying to stop them at the basic stage by performing identity verification checks (thorough KYC procedure). The IP addresses, email IDs, phone numbers and the type of device used can be studied to be sure about any malicious activity. This method is surprisingly effective since it is not very common on such platforms. Also, suspicious activity records and reports must be prepared.

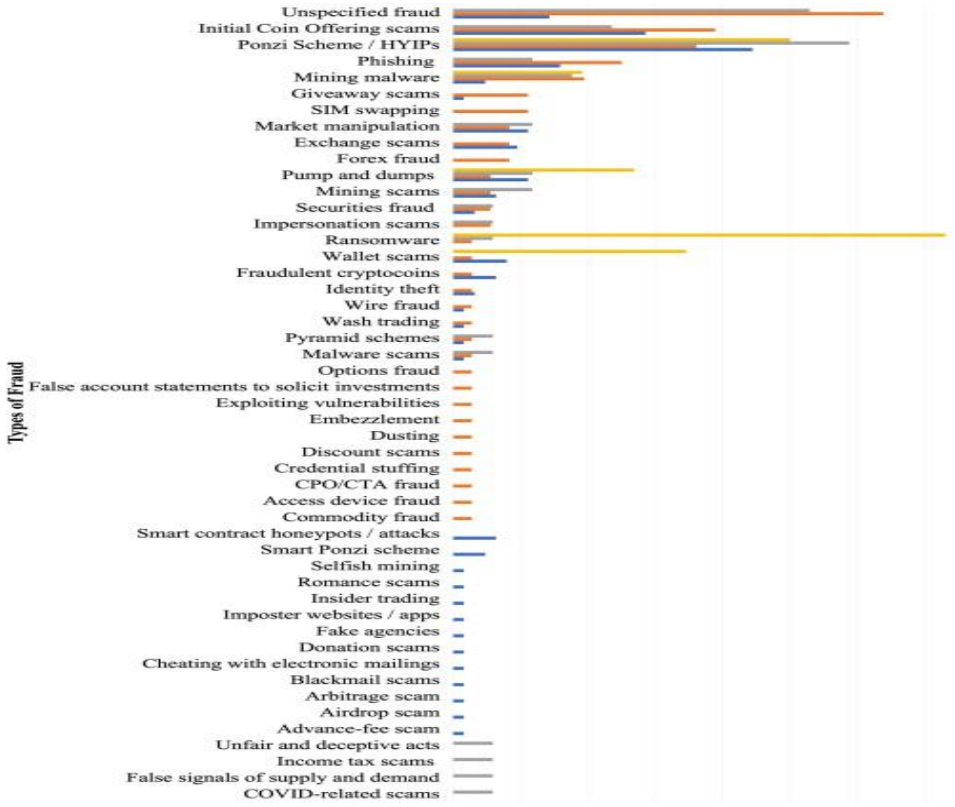


Fig 3.2 : Types of cryptocurrency crimes

3.3 FRAUD TRANSACTION DETECTION

1. Model To Detect Fraud Transaction

Introduction:

- To protect criminals, fraud detection techniques are regularly improved. They make it possible for us to spot fraud quickly and simply. In this scenario, we will concentrate on fraud detection in bitcoin transactions.
- A single algorithm may not best serve every problem. Therefore, choosing an algorithm that works well in certain circumstances is really important.
- In this paper, the decision tree method, the random forest algorithm, and the logistic regression algorithm are compared.
- For bitcoin fraud detection, we employ Apache Spark's machine learning library (MLlib).
- The data utilized in our simulation is created at random using a normal distribution, and it has two features—generated coins and TxCount—that help us discriminate between legitimate transactions and anomalous ones.
- The parameters of Total Running Time and Accuracy are used to analyze the

performance.

- The outcomes demonstrated that the Decision Tree Classifier produced the worst results and the Random Forest method produced the best result

Different Types of Algorithms Applied

Decision Tree classifier:

- Decision Tree is a Supervised learning approach that may be used for both classification and regression issues, however, it is most commonly employed for classification. It is a tree-structured classifier in which internal nodes contain dataset attributes, branches represent decision rules, and each leaf node represents the result.

- A Decision tree has two nodes: the Decision Node and the Leaf Node. Decision nodes are used to make decisions and have numerous branches, whereas Leaf nodes represent the results of those decisions and do not have any more branches.

- It is a graphical depiction of all possible solutions to a problem/decision depending on specific criteria.

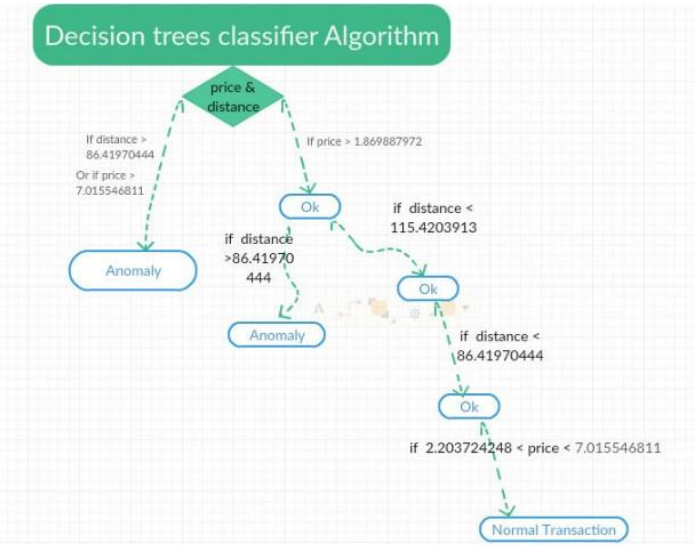


Fig. 4: A simple decision tree

Fig 3.3 : Decision Tree Classifier

Random Forest Classifier:

- Random Forest is a well-known machine learning algorithm from the supervised learning approach. It may be applied to both classification and regression issues in machine learning. It is built on the notion of ensemble learning, which is a method that involves integrating several classifiers to solve a complicated issue and enhance

the model's performance.

- Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset.

- Random Forest is a classifier that uses a number of decision trees on different subsets of a given dataset and averages them to enhance the predicted accuracy of that dataset.

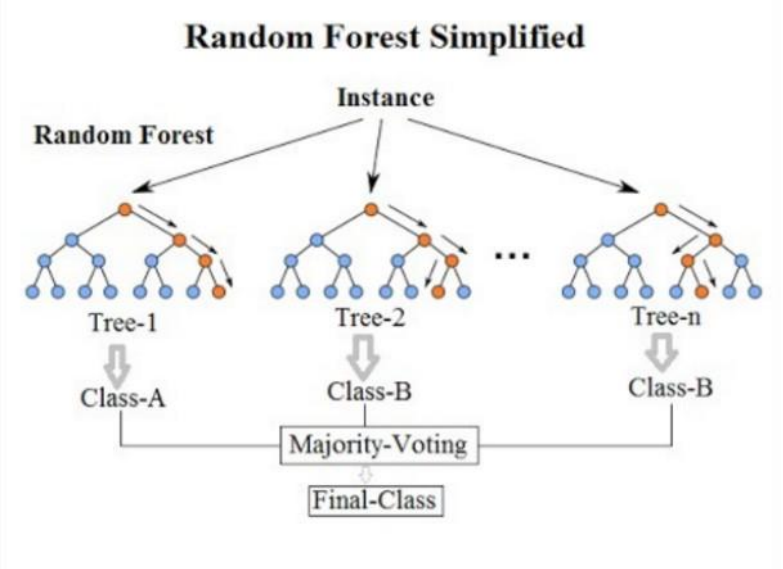


Fig: Random Forest Classifier

Logistic regression:

- The method of modeling the likelihood of a discrete result given an input variable is known as logistic regression. The most frequent logistic regression models include a binary result, which can accept two values like true/false, yes/no, and so on. Logistic regression is a helpful analytical tool.

- Logistic regression is a popular method for solving prediction and classification issues. Among these use cases are: Fraud detection: Logistic regression methods can assist teams in identifying data abnormalities

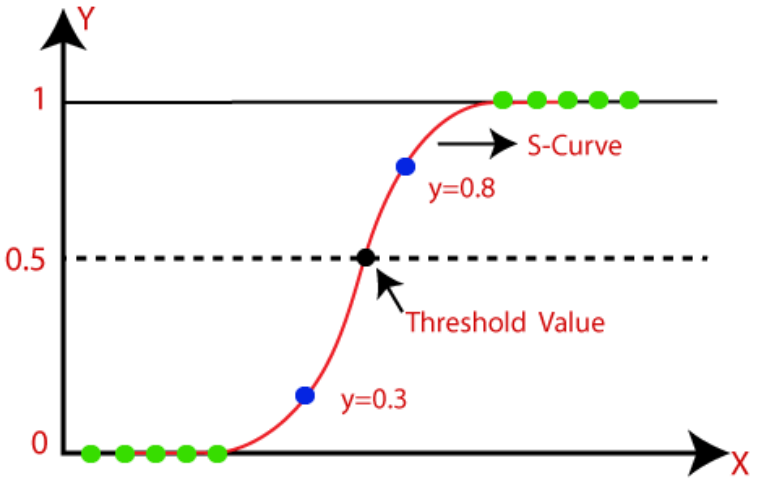


Fig 3.5 : Logistic regression

Apache Spark:

- Apache Spark is a data processing framework that can conduct processing jobs on very large data sets fast, as well as spread data processing activities over several computers, either on its own or in collaboration with other distributed computing technologies. These two characteristics are critical in the areas of big data and machine learning, which demand huge computational power to chew through large data repositories. Spark also relieves developers of some of the programming responsibilities associated with these activities by providing an easy-to-use API that abstracts away most of the grunt work of distributed computing and large data processing.

- Apache Spark is a distributed processing engine that is open source and used for large data applications. For quick analytic queries against any quantity of data, it uses in-memory caching and efficient query execution. It offers Java, Scala, Python, and R development APIs and facilitates code reuse across many workloads—batch processing, interactive queries, real-time analytics, machine learning, and graph analysis.

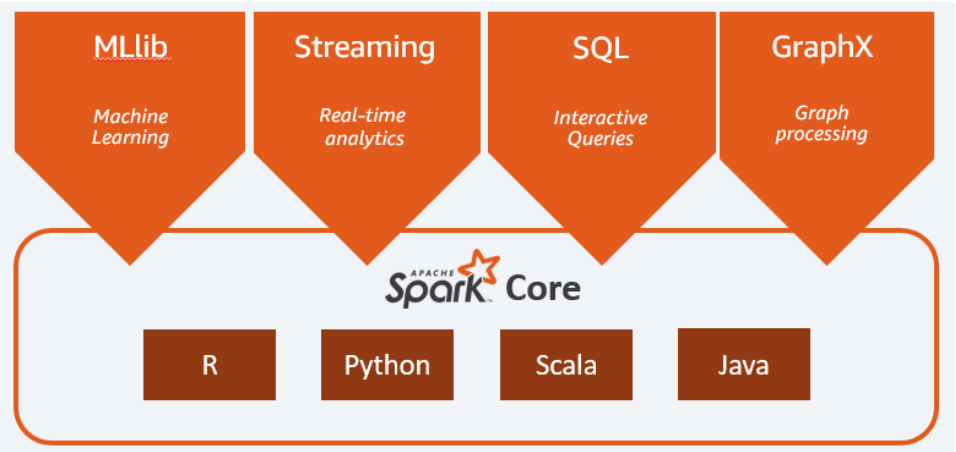


Fig 3.6 : Apache Spark Framework

Working of the Model:

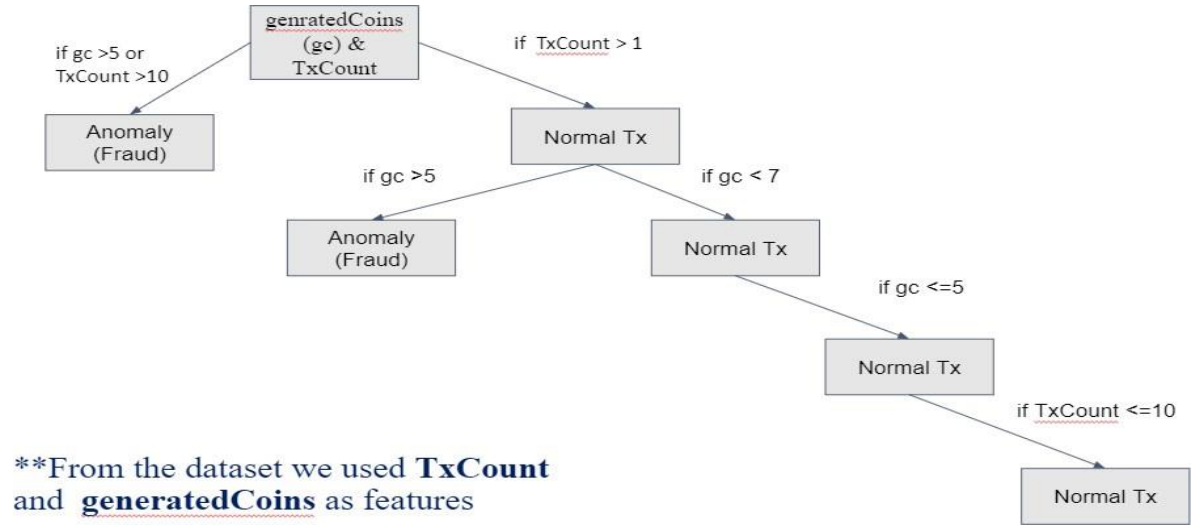
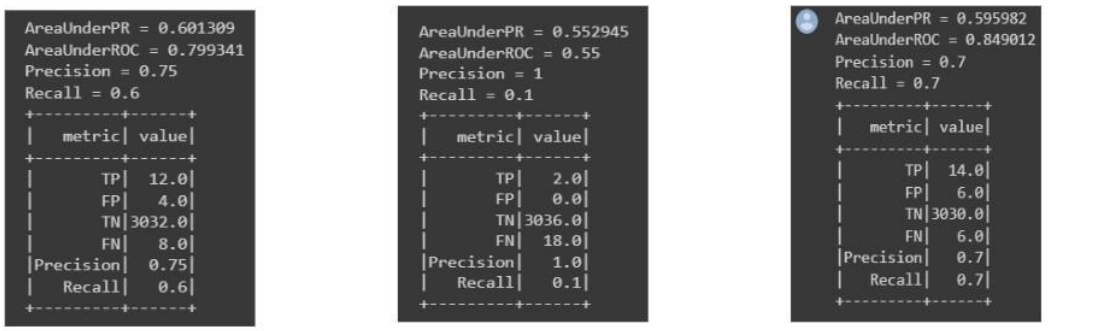


Fig 3.7 : Model Procedure

Comparing the Algorithm:



Random Forest Classifier **Logistic Regression** **Decision Tree Classifier**

Fig 3.8 : Results of Different Algorithms

The above figure shows the results we got after implementing the different algorithms on our transactional dataset in which we basically used Classification by the MLib, a machine learning library of Apache Spark.

Choosing the Best Algorithm:

Algorithm	Total Running Time(in sec)	Accuracy(%)
LOGISTIC REGRESSION	9	84.86
DECISION TREE CLASSIFIER	5	89.32
RANDOM FOREST CLASSIFIER	6	98.18

Table 1.1 : Algorithm Comparison Table

We have provided a comparison of different algorithms based on two criteria: the total execution time and the accuracy of each algorithm(based on F1 Score). On one hand, the random forest algorithm gives the best total execution time and is even more accurate. On the other hand, the decision tree classifier algorithm takes more execution time and gives the worst accuracy.

2. Model To Detect Fraud Transaction:

Introduction:

- Due to the positive image of this technology, electronic transactions using cryptocurrency systems based on blockchain have been quite popular in recent years. Despite their stellar reputation, cryptocurrencies still carry significant dangers and abnormalities. In this paper, we suggest a novel approach for detecting anomalies in bitcoin electronic transactions. In our proposal, we employed two machine learning techniques: the One-Class Support Vector Machines (OCSVM) algorithm for outlier detection and the KMeans algorithm for clustering outliers with similar anomalies. By producing detection results, we evaluated our work and got highly accurate performance results.

- Our objective in this paper is to propose a new model for anomaly detection at the Bitcoin electronic transaction using machine learning algorithms on two stages.

- In the first stage, we used the One-Class SVM method to detect the outliers and in the second phase, we used the K-means algorithm to regroup the outliers according to a similarity index in order to specify the type of attack.

Model Framework:

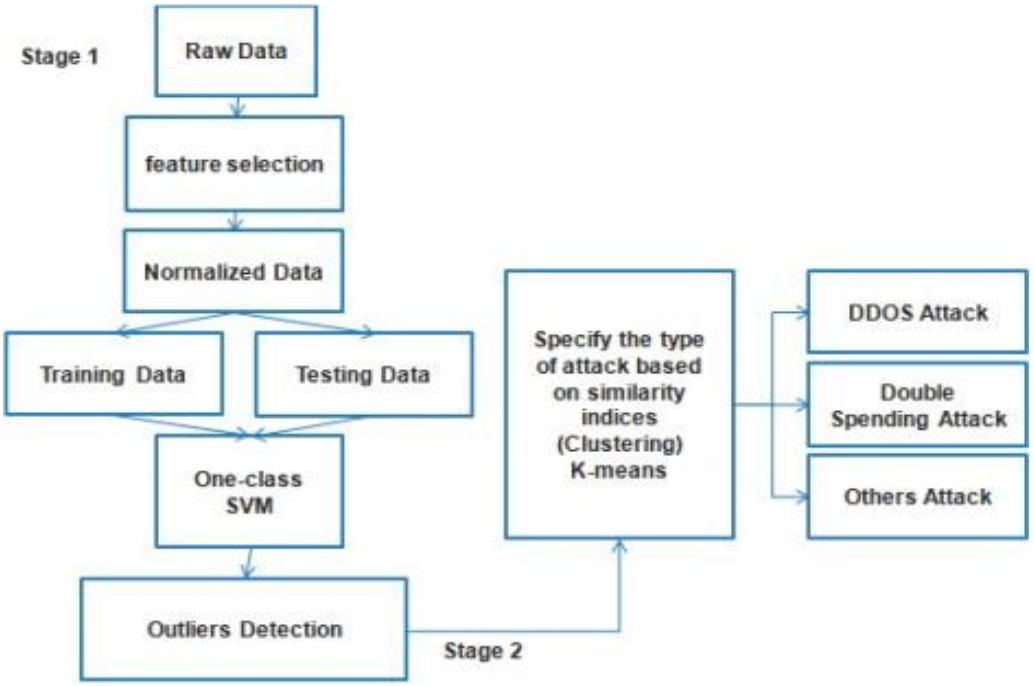


Fig 3.9 : Model Framework

- To detect the anomalies(outliers) - One-Class Support Vector Machine(SVM)
- To group the similar outliers having the same type of anomalies - K-Clustering

One-Class SVM:

- One-Class SVM is an unsupervised learning approach that teaches the capacity to distinguish test samples from other classes. 1-SVM is one of the most practical approaches to OCC problem statements, including AD. 1-SVM is based on the basic idea of minimizing the hypersphere of a single class of examples in training data and treating all samples outside the hypersphere as outliers or outside the training data distribution. The image below depicts the hypersphere formed by 1-SVM to learn the ability to classify out-of-training distribution data using the hypersphere.

- Using sklearn, you can easily implement 1-SVM. The 1-SVM from libsvm is implemented by SK-learn. SK-learn includes a class called 'OneClassSVM' that internally executes the mathematical modeling of reducing the hypersphere through data sample training. Positive numbers are class +1 in the One-Class SVM model, whereas negative integers are class -1
.

K-Clustering:

- It is an unsupervised learning method used in machine learning or data science to handle clustering issues. In this topic, we will learn about the K-means clustering method, how it works, and the Python implementation of the algorithm.
.
- It enables us to cluster the data into distinct groups and provides a straightforward method for discovering the categories of groups in the unlabeled dataset without the requirement for training. The algorithm starts with an unlabeled dataset, separates it into k clusters, and then continues the procedure until it does not identify the optimal clusters. In this algorithm, the value of k should be preset. The k-means clustering technique is primarily responsible for two tasks:

- Determines the best value for K center points or centroids by an iterative process.

- Assigns each data point to its closest k-center. Those data points which are near the particular k-center, create a cluster.

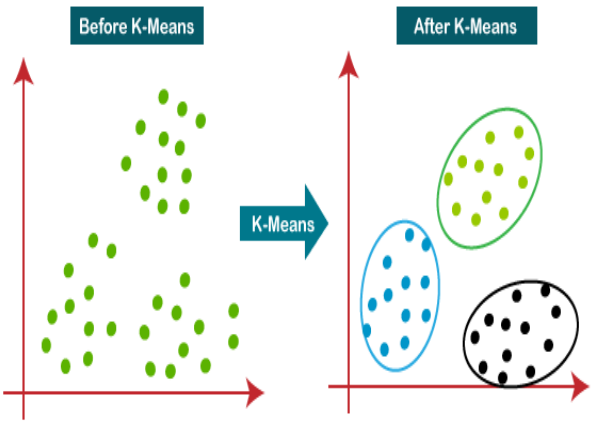


Fig 3.10: K-Clustering

Feature Selection:

In the dataset mentioned above, we can select any two of the following features:

- Blockchain size
- TxCount**:** the number of transactions completed per day
- TxVolume: the total output volume with the addition of an algorithm that attempts to remove change from the total value.
- generatedcoins: Total number of unique Bitcoin transactions per day.
- Avg block size

*In our model, we chose Txcount and generated coins as the features.

Procedure:

1. applying a behavioral analysis by using the One-Class SVM algorithm to detect outliers.

2. applying the K-means clustering algorithm to gather similar attacks in order to specify their types.

Results:

A score will be given to the One-Class SVM anomaly detection model for each type of outputting a decision, (1) if normal data or (−1) if abnormal data.

3.4 NOVELTY OF THE PROJECT

- **Anti-money laundering solutions** built on the blockchain can use the inherent properties of the blockchain to identify and prevent illegal transactions. If the software used to monitor transactions is AI with machine learning capabilities, it can effectively traverse the chain of data to determine if money laundering activity is taking place. This works because AI will be able to recognize patterns in large amounts of data, while at the same time using machine learning capabilities to adapt to changes in criminal activity over time.

- **Chain Analysis** - Chain analysis is an emerging field involving the study of the fundamentals, utilities, and transactional activity of cryptocurrencies and their blockchain data. This project will use the chain analysis method to record the transactional records of individual cryptocurrency activities.

- **Elliptic curve**- Elliptic-curve based public-key cryptography method is used. It uses the algebraic structure of elliptic curves over finite fields. This is an attachment that specializes in financial services, anti-money laundering software, and cryptocurrency exchanges. This project will provide law enforcement services by tracking the funding of Bitcoin terrorists through forensic software. It benefits Bitcoin-related businesses and transactions by reducing associated risk factors. It also helps financial institutions comply with regulations.

- **User identification using Video KYC** Without initial identification, you cannot ascertain that your prospective client will not engage in a dubious activity. During the customer due diligence(CDD) process, the firm must perform the following two things: Verify the information supplied by the potential client throughout the identification process to identify the entity posing as a prospective client (i.e., learn about the identity and supporting papers).

- **Transaction limits** may be imposed. This means that whenever a person exchanges cryptocurrency for fiat or spends it above a certain threshold, it will be blocked without triggering an alert. Customer, and prompt them to review such Customer activity. This could lead to further questioning and investigation of all activities, possible termination of relationships/freezing of assets, and possible reporting to the National Financial Intelligence Agency.

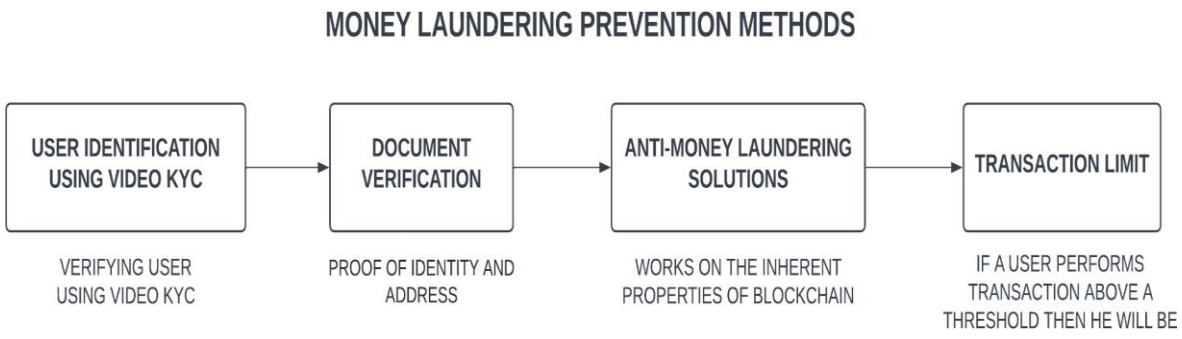


Fig 3.11 : Money Laundering Prevention Methods

3.5 PAYMENT GATEWAY

A cryptocurrency payment gateway is a payment processor for digital currencies, similar to payment processors, gateways, and acquiring bank credit cards use. Cryptocurrency gateways enable you to accept digital payments and receive fiat currency immediately in exchange.

These companies remove any uncertainties or reservations you might have about cryptocurrency and allow you to offer more payment options.

It's important to note that digital currency payment gateways are not required. It's perfectly acceptable to use your personal wallet to accept cryptocurrency payments; however, gateways take the extra work of exchanging cryptocurrency and managing a wallet out of your hands.

We are making a payment gateway for cryptocurrency transactions using Web3.0, Solidity, and Metamask.

Web 3.0:

Web 3.0 (Web3) is the third generation of the evolution of web technologies. The web, also known as the World Wide Web, is the foundational layer for how the internet is used, providing website and application services.

In the blockchain and Web 3.0 communities, the idea of a decentralized autonomous organization(DAO)is an emerging form of governance. With a DAO, Web 3.0 technologies and communities offer a type of self-governance in an effort to move away from centralized control over platform operations. More so than with fiat money, Web 3.0 also functions fundamentally with cryptocurrencies. The use of cryptocurrencies, which are all constructed and enabled on top of blockchain technology, enables finance and the use of a decentralized form of payment throughout Web 3.0.

Solidity:

For the purpose of constructing smart contracts across several blockchain systems, most notably Ethereum, Solidity is an object-oriented programming language.

Solidity is highly influenced by C++, Python, and JavaScript and has been designed to target the Ethereum Virtual Machine (EVM).

Smart Contracts:

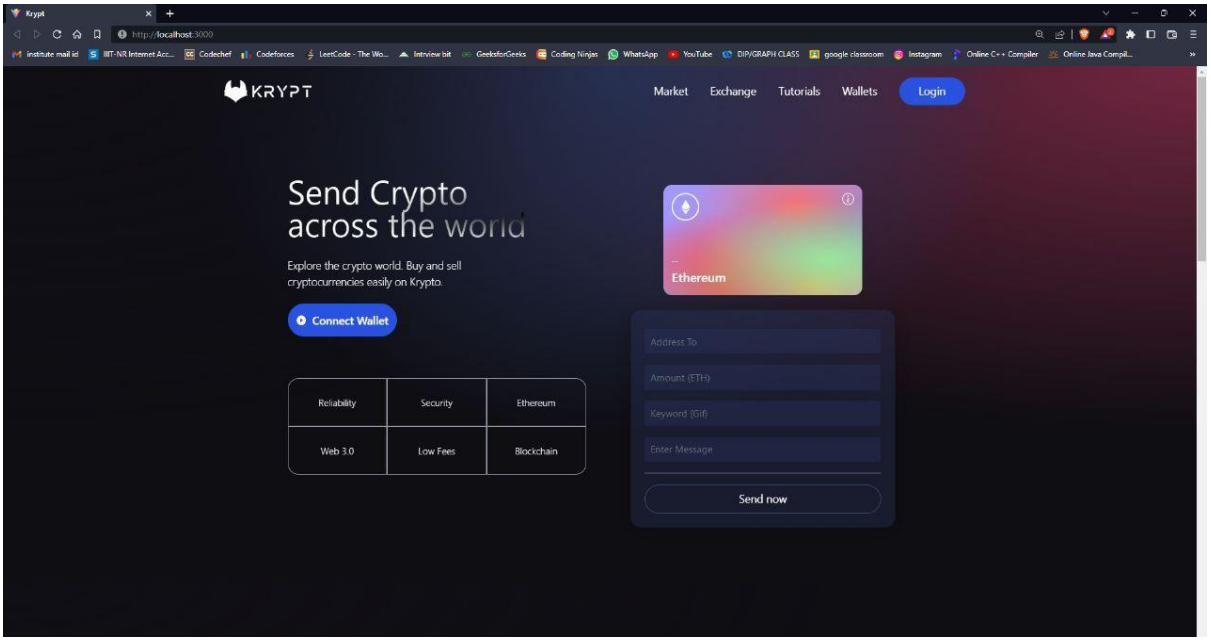
Simply put, smart contracts are blockchain-based algorithms that execute when certain criteria are met. They are typically used to automate the execution of an agreement so that all parties can be certain of the outcome right away, without the need for an intermediary or additional time. They can also automate a workflow so that when conditions are met, the next action is taken.

Metamask

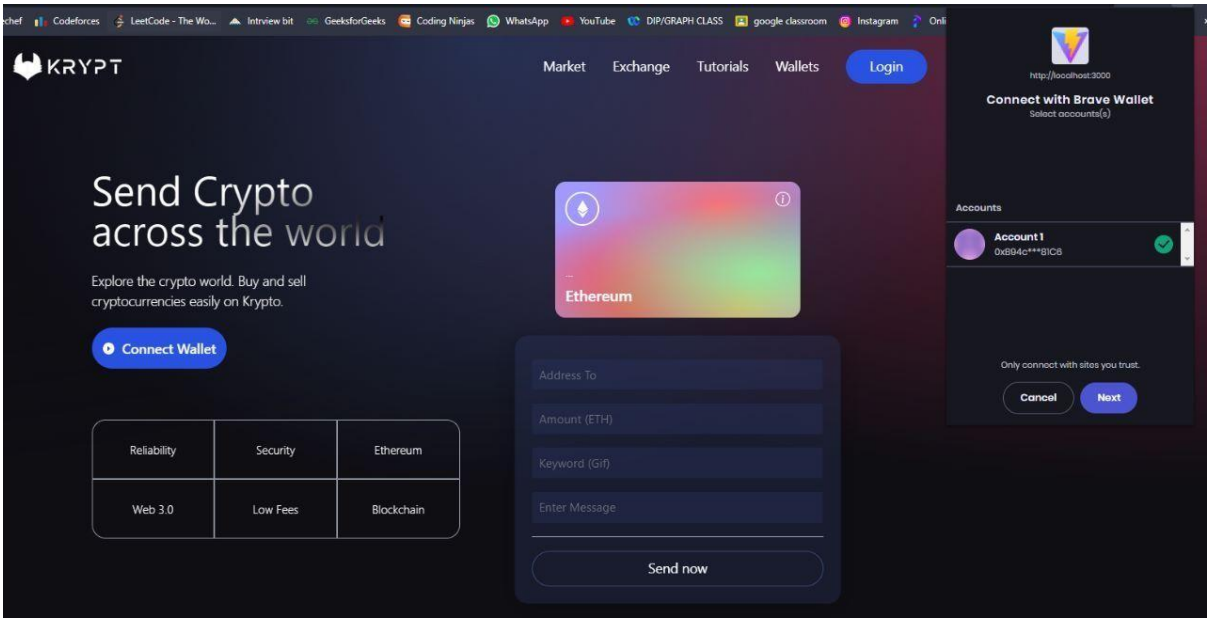
A software cryptocurrency wallet called MetaMask is used to communicate with the Ethereum network. It enables users to use a browser extension or mobile app to access their Ethereum wallet, which can subsequently be used to connect with decentralised applications.

With MetaMask, users can send and receive Ethereum-based cryptocurrencies and tokens, broadcast transactions, store and manage account keys, and securely connect to decentralised applications using a compatible web browser or the built-in browser of the mobile app.

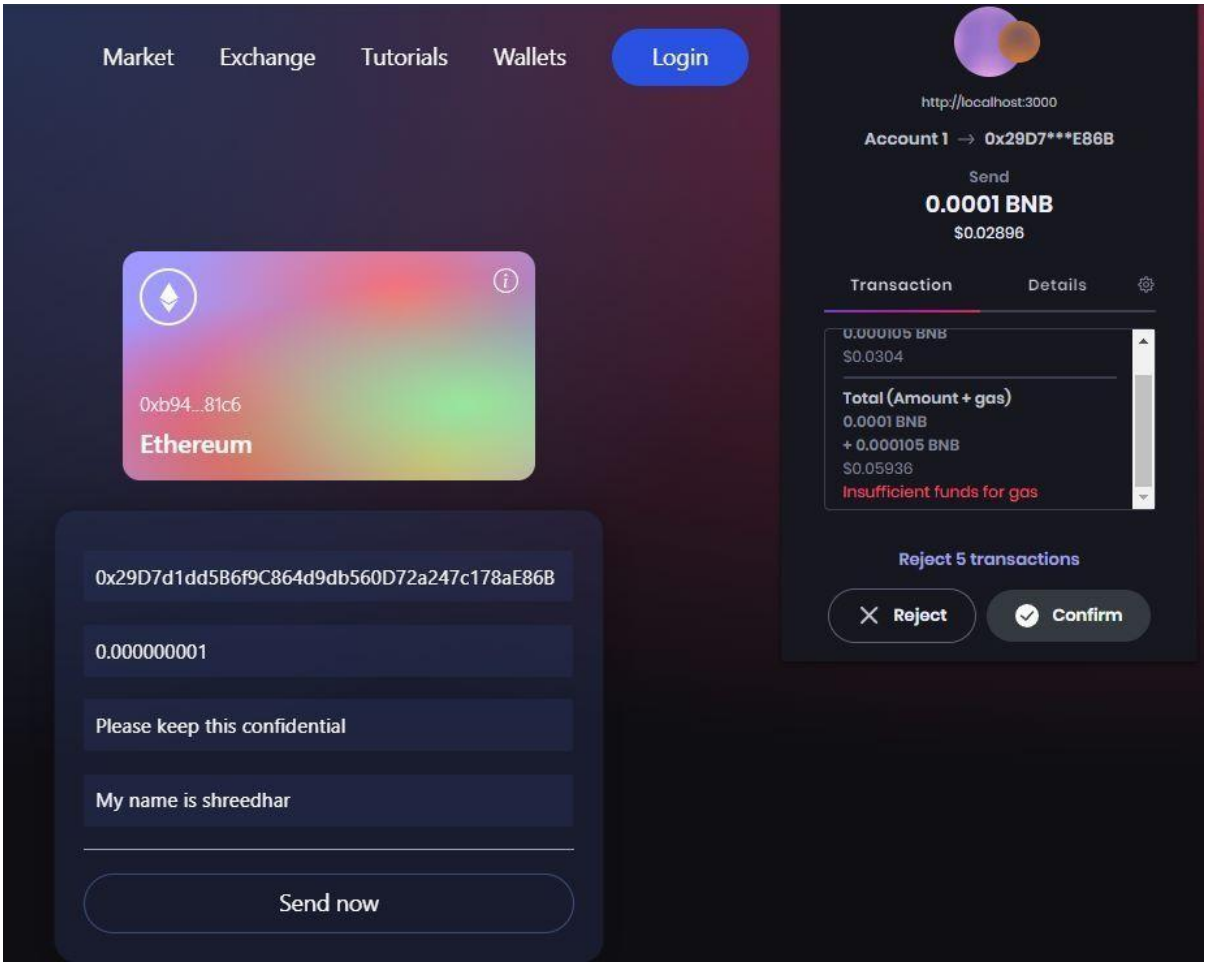
Screenshots of our webapp 3.0



Home page of our web application



Metamask connection to our web app



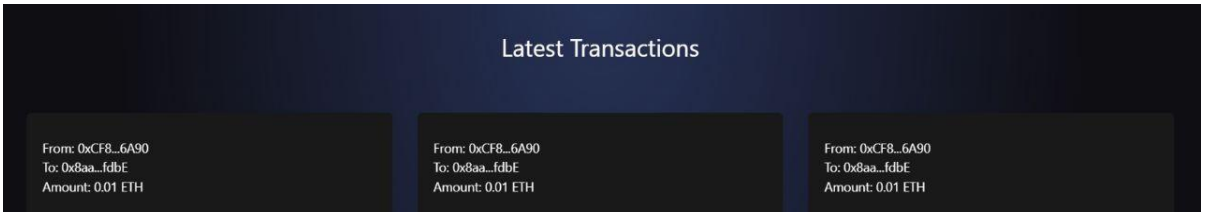
Transaction procedure from one metamask to another

index.html | Transactions.sol 2, M | Release Notes: 1.74.0

smart_contract > contracts > Transactions.sol

```sol
pragma solidity ^0.8.0;

import "hardhat/console.sol";

contract Transactions {
    uint256 transactionCount;

    event Transfer(address from, address receiver, uint amount, string message, uint256 timestamp, string keyword);

    struct TransferStruct {
        address sender;
        address receiver;
        uint amount;
        string message;
        uint256 timestamp;
        string keyword;
    }

    TransferStruct[] transactions;

    function addToBlockchain(address payable receiver, uint amount, string memory message, string memory keyword) public {
        transactionCount += 1;
        transactions.push(TransferStruct(msg.sender, receiver, amount, message, block.timestamp, keyword));

        emit Transfer(msg.sender, receiver, amount, message, block.timestamp, keyword);
    }

    function getAllTransactions() public view returns (TransferStruct[] memory) {
        return transactions;
    }

    function getTransactionCount() public view returns (uint256) {
        return transactionCount;
    }
}
```

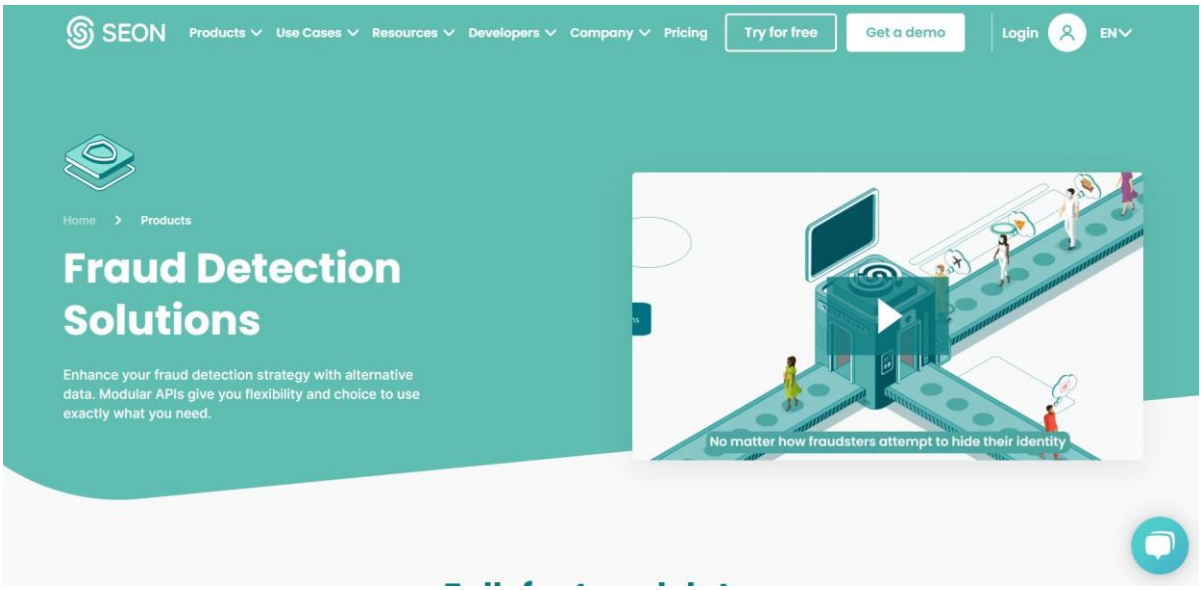
Solidity code Blockchain implementation

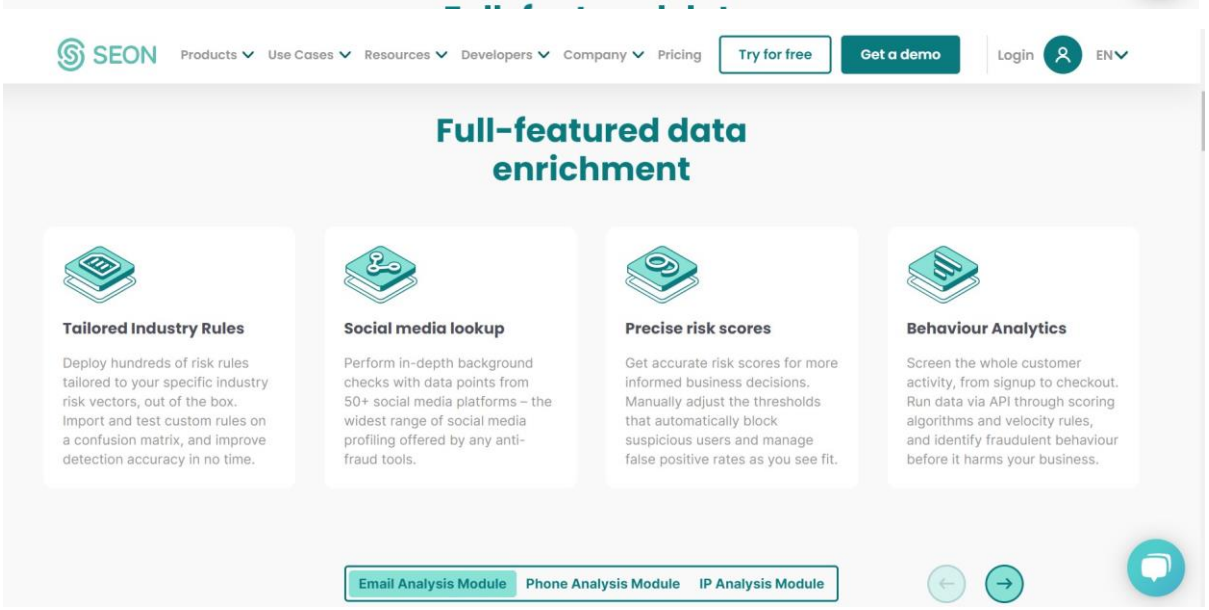


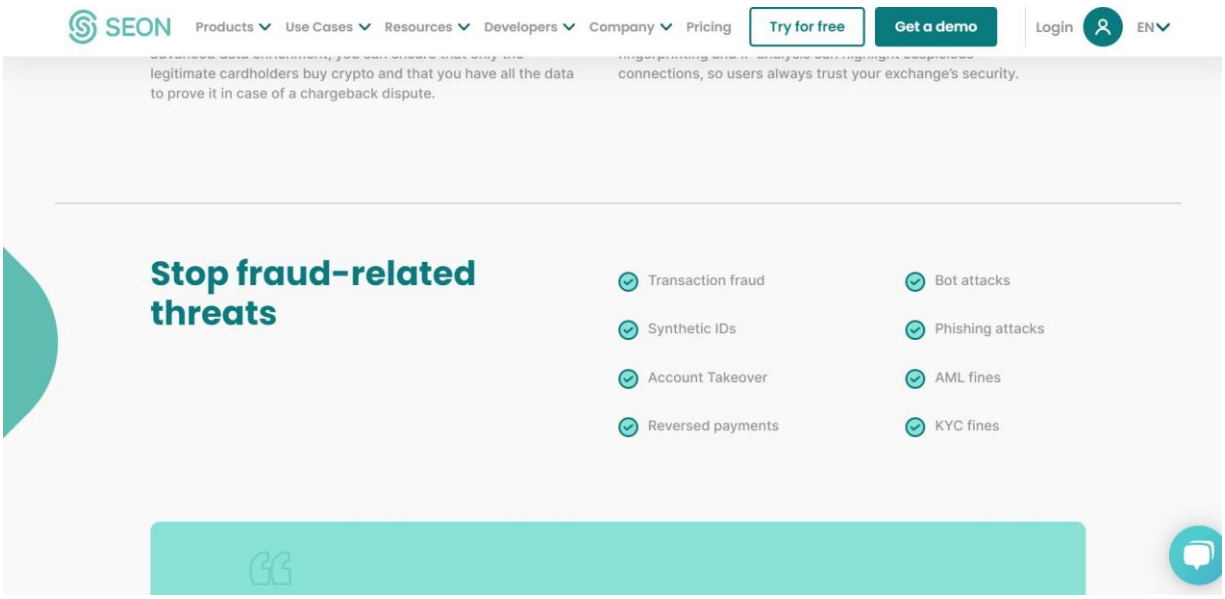
Transaction details history

COLLABORATION:

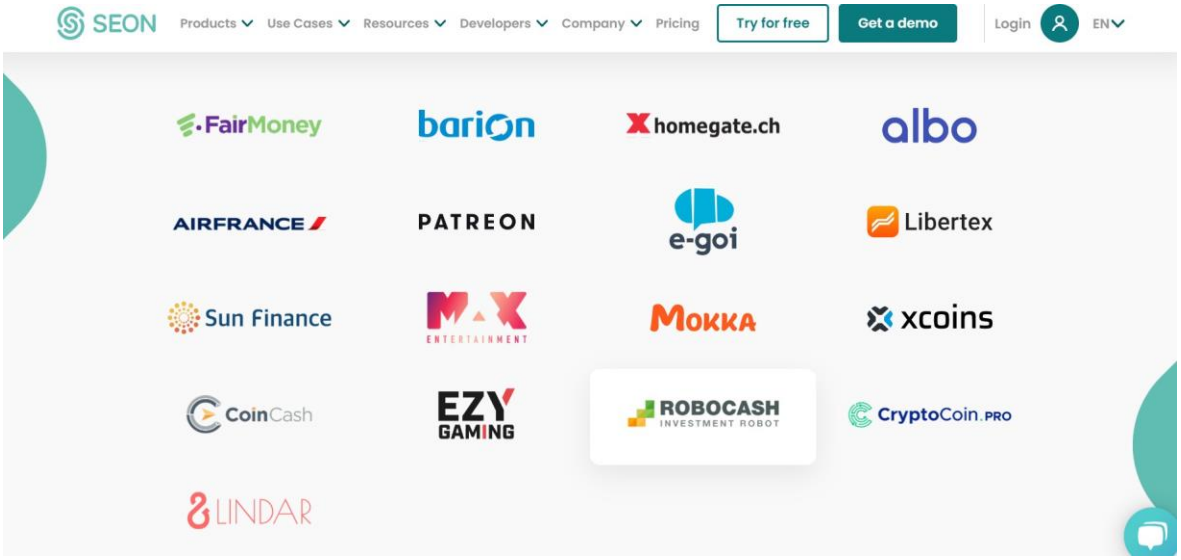
There is a collaboration with SEON. It provides access to the anti-fraud framework which helps to monitor suspicious activities ranging from detection at the initial to transactional state.







SEON is a trusted brand for the requirements of the project as it has been featured in the following,



CHAPTER- 4 CONCLUSIONS

4.1 INFERENCE OF PROJECT

In particular, cryptocurrency Bitcoin provides a new, practical, and attractive payment method model that can increase business and operator income. In addition, it offers alternatives to real money that make it simple for users to do financial transactions including buying, selling, transferring, and exchanging.We have used machine learning to detect cryptocurrency crime and money laundering and further used blockchain to built a payment gateway. Numerous bitcoin systems are affected by a variety of worries, difficulties, and problems. Users of cryptocurrencies should exercise additional caution while utilising it until it is properly regulated and managed. Therefore, the primary concern in cryptocurrency systems is the lack of regulations. In India, a market for dealers, exchanges, and businesses that accept bitcoin payments has developed. Since bitcoins are already widely accepted worldwide, India would not be able to outlaw them. Instead, this sector would require regulation.

REFERENCES

Research papers

- a study on opportunities and challenges of cryptocurrency in india with special reference to bitcoin by dr. anil kumar & swathy
- Luther, W. (2016). Bitcoin and the Future of Digital Payments. The Independent Review,20(3), 397-404. Retrieved from http://www.jstor.org/stable/24562161
- Blockchain and Smart Contract for Digital Certificate by Jiin-Chiou Cheng, Narn-Yih Lee , Chien Chi , and Yi-Hua Chen
- A Case Study on Digital Currency with a Special Reference to India byy Dr. Pradipta Mukhopadhyay
- Journey of Cryptocurrency in India In View of Financial Budget 2022-23 by Varun Shukla, Manoj Kumar Misra, Atul Chaturvedi
- https://en.wikipedia.org/wiki/List_of_cryptocurrencies
- https://www.thehindu.com/opinion/op-ed/all-about-bitcoins/article17961273.ece
- https://www.ccn.com/time-indian-digital-rupee-says-former-head-lehman-brothers-india/