FinTech PROJECT

Report

GROUP MEMBERS:
SHREEDHAR TIWARI (201000049)(CSE)
ZORAWAR SINGH (201010260)(CSE)
SHUBHAM RAJ (201000051)(CSE)

SUPERVISOR OF THE PROJECT: DR.SANTOSH KUMAR

PROJECT NAME- Development of Secure Framework for Prevention of Crypto-Currency Crimes and Prevention of Money Laundering Using Blockchain.

PROBLEM:

1. To develop an efficient digital payment method for cryptocurrency using a payment gateway in local native languages for rural regions in tribal communities.
2. To develop a secure model to identify money laundering accounts using blockchain and machine learning techniques. 3. 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

RELEVANCE:

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.

IMPLEMENTATION:

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 on data pattern, (4) prevention mechanism based on learning from given data, (5) classification of cryptocurrency crimes or non-crime.
DERIVABLE:

1. The primary motivation of the project is to leverage a platform for sustainable growth of the tribal 2. The novelty of this project is to integrate ground trials related to suspicious activities related to money transfers and critical analysis of cryptocurrency crimes based on collected datasets in India with developed novel concepts, techniques, instrumentation, or interventions

Methodology

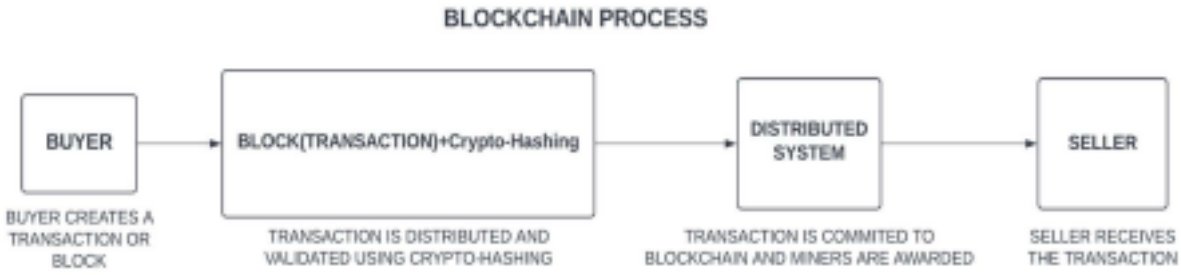


Figure: Show block diagram of blockchain process for cryptocurrency crimes

The proposed methodology for early prevention of cryptocurrency crime consists of 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.

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 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 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.

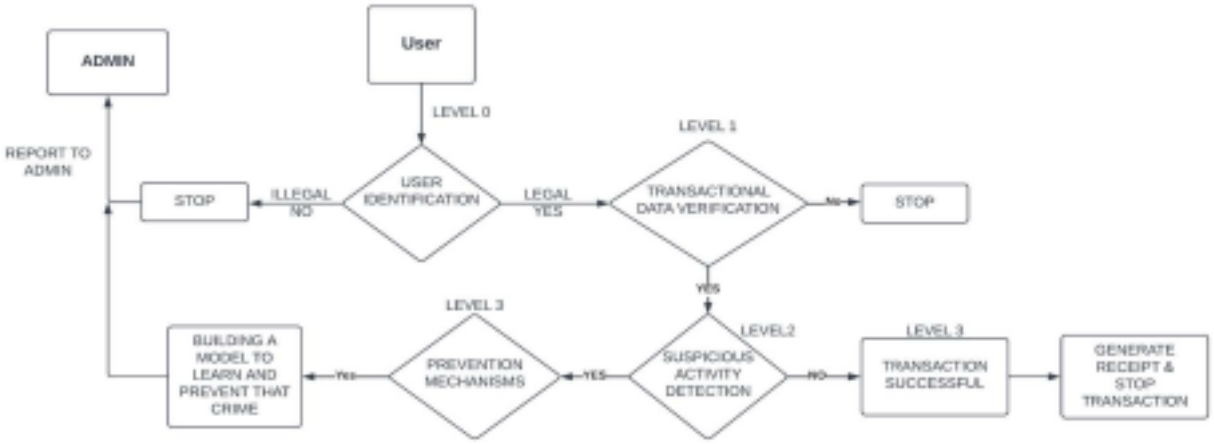


Figure: Block diagram for the explaining working of the models.

Cryptocurrency crimes prevention method:

Illegal activities are also taking place in the region as the use of cryptocurrencies is reportedly on the rise. According to blockchain platform Chainalysis, cryptocurrency transaction volume increased by 567% from 2020 to 2021, while illegal transaction volume increased by 79%. According to the report, the increase in legitimate currency use has outpaced the increase in cryptocurrency crime. Illegal transactions reportedly accounted for 0.15% of all cryptocurrency transactions in 2021, and according to the latest crypto crime report, 0.34% of cryptocurrency transactions in 2020 were related to illegal transactions. Nonetheless, the year-over

year trend is that cryptocurrency crime is reportedly declining in all but 2019, and law enforcement is expected to play a role.Some of the Preventive measures which could be taken to stop Cryptocurrency crimes can be:

1)The most reliable data regarding the use of cryptocurrencies in illicit activities seems to come from a number of specialized blockchain analytics firms. One of these is Chainalysis and Elliptic, which provides research and tools to uncover criminal networks operating with cryptocurrencies.

2)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 cryptocurrencies activities.

3)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.

4)Similarities between Chainalysis and Elliptic- Both method will offer cryptocurrencies data tracking services

Summary of Chainalysis and Elliptic-Chainalysis specializes in developing compliance software to detect and investigate cryptocurrency breaches and money laundering, while Elliptic specializes in financial services, anti-money laundering software,

and cryptocurrency exchanges. increase. Both offer cryptocurrency data tracking services and are close competitors

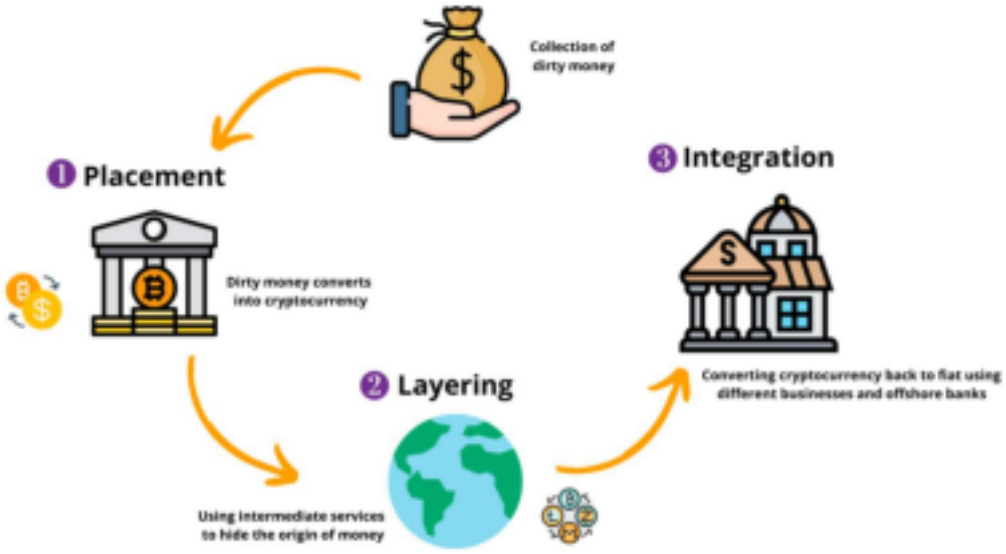
5)Video and blockchain-based Know Your Customer (KYC): This method is being used in many countries to trick people into revealing their identity before making cryptocurrency transactions. Further steps will also be taken to align digital currencies with existing anti-money laundering (AML) and counter-terrorism financing (CTF) laws.

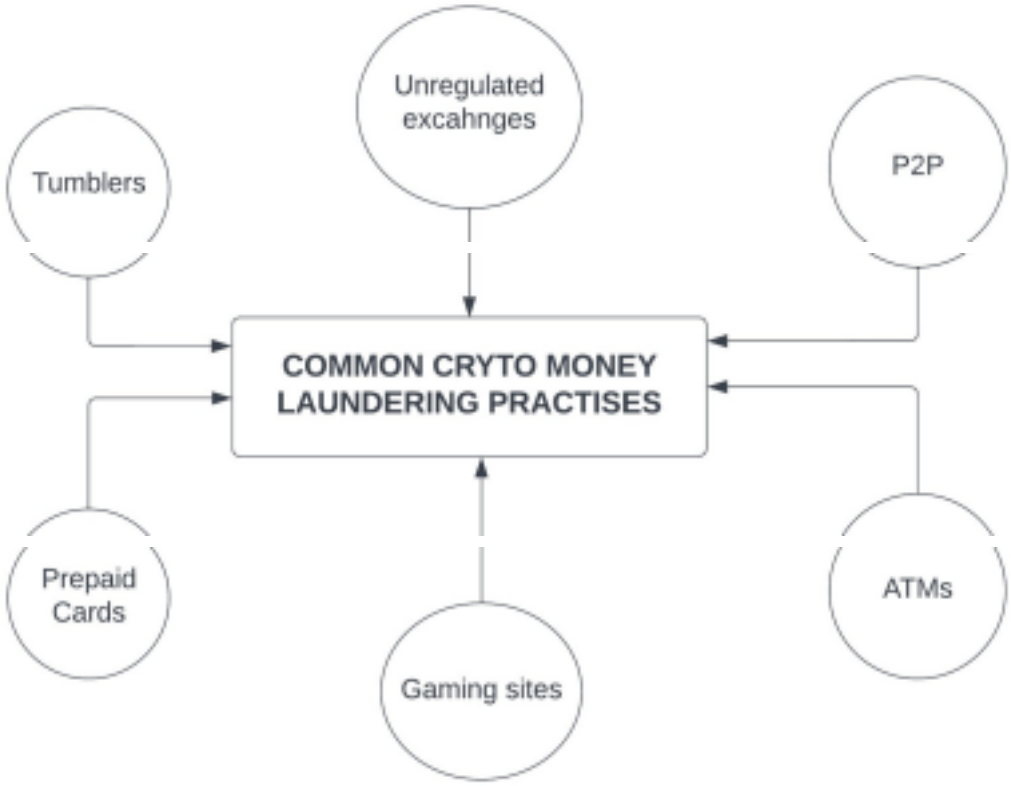
6)Several private intelligence companies, such as CipherBlade, have devoted significant resources to developing blockchain intelligence tools and technologies.Techniques like detecting hacked wallets, putting risk scores on wallet addresses, and employing analytics and artificial intelligence to highlight questionable trends are all examples of this. They work with law enforcement agencies, providing tools and expertise to tackle cryptocrime.

7)Enforcing the highest standards of the Know Your Customer and also the Anti-Money Laundering protocols 8)All activity on the blockchain must be monitored and suspicious activity should be reported.

9)Establish all appropriate transaction limits and acceptable use cases password reset due to wrong transactions. 10)Exclude jurisdictions where cryptocurrencies are disallowed.

Prevention of money Laundering





The decentralized nature of the blockchain technology, requiring each participant or node to verify changes, makes it an incredibly secure supercomputer that doesn't exist yet, making other nodes immune to unauthorized changes. It counters automatically. Because each node has a record of the entire ledger, each change can be compared to the record to detect unauthorized changes. This aspect of blockchain technology means that the blockchain ledger is fully trusted. Regulatory authorities can therefore audit the records, knowing the reliability and accuracy of the information they contain..Some of the Prevention methods of money laundering using Blockchain can be:

1)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.

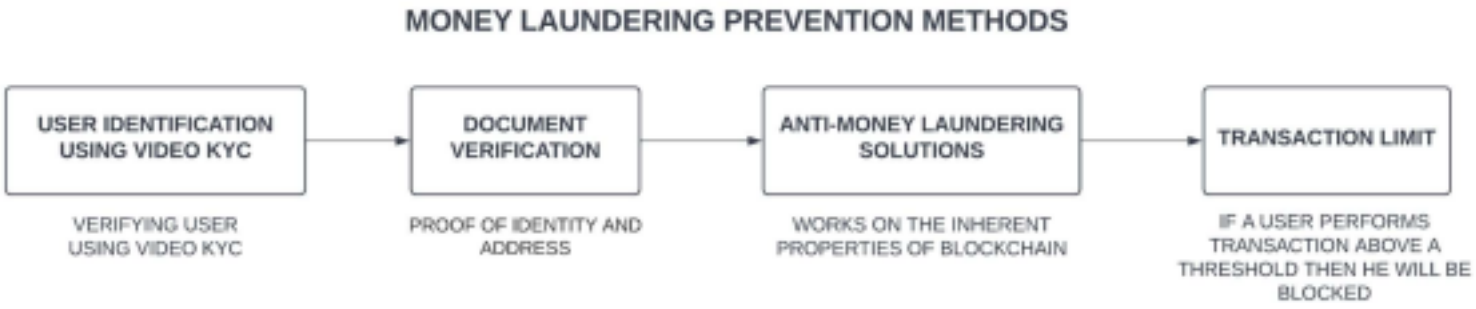
2)User identification using Video KYC Without initial identification, you cannot ascertain that your prospective client will not engage in a dubious activity. During the customer due diligence(CDD) process, the firm must perform the following two things: Verify the information supplied by the potential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

These two steps broadly help to ascertain whether the prospective client will be likely to engage in money

laundering or not.

3)The information collected depends on the type of customer, but for individuals it is typically proof of identity and address. Documents containing this data must be verified for authenticity. Since we are talking about cryptography, this is probably done with the help of documents and biometric providers

4)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.



In this project proposal, the objective framework facilitates early identification of money laundering accounts based on transactions recorded on bank pages. In other words, the goal is not to replace anti-money laundering experts, but to narrow the search space to save the manual effort required. Preventing fraud (recall) and identifying genuine money laundering accounts (i.e. accuracy) are important. At the same time, we need insight into money laundering practices. The proposed framework, motivated by current requirements, consists of a two-stage discriminative model based on blockchain and machine learning and data analysis techniques. 1)The first stage of the proposed framework recommends all potentially suspicious activity, such as tracking money laundering accounts and cryptocurrency activity for systematic long-term monitoring of transactions.

2)The second stage, on the other hand, manually detects highly suspicious accounts and evaluates multiple transaction flows for small accounts at various time intervals.

The details of the two phases are introduced in the following.