A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Major Project submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

By

Bittu Harishankar	**(21R11A6208)**
Chinna Bheemanna Malathi	**(21R11A6213)**
Kethidi Rajinikar Reddy	**(21R11A6231)**

Under the esteemed guidance of

Dr. Shraban Kumar Apat
Assoc. Professor

Department of CSE(Cyber Security)

Geethanjali College of Engineering and Technology
(UGC Autonomous)
(Affiliated to J.N.T.U.H, Approved by AICTE, New Delhi, NAAC A+)
Cheeryal (V), Keesara (M), Medchal.Dist.-501 301.

April-2025

Geethanjali College of Engineering & Technology

(UGC Autonomous)

(Affiliated to JNTUH, Approved by AICTE, New Delhi, Accredited by NBA)
Cheeryal (V), Keesara(M), Medchal Dist.-501 301.

DEPARTMENT OF CSE (CYBER SECURITY)

CERTIFICATE

This is to certify that the B.Tech Major Project report entitled "**A Bitcoin Transaction Network Analytic Method For Future Blockchain Forensic Investigation** " is a bonafide work done by Bittu Hari shankar **(21R11A6208)**, Chinna bheemanna Malathi **(21R11A6213)**, Kethidi Rajinikar Reddy**(21R11A6231),** in partial fulfillment of the requirement of the award for the degree of Bachelor of Technology in **"CSE(Cyber Security)"** from Jawaharlal Nehru Technological University, Hyderabad during the year 2024-2025 .

Internal Guide	**HOD - CS**
Dr. Shraban Kumar Apat	**B. Dhanalaxmi**
Assoc. Professor	Associate Professor

External Examiner

Geethanjali College of Engineering & Technology

(UGC Autonomous)

(Affiliated to JNTUH Approved by AICTE, New Delhi, Accredited by NBA)
Cheeryal (V), Keesara(M), Medchal Dist.-501 301.

DEPARTMENT OF CSE(CYBER SECURITY)

DECLARATION BY THE CANDIDATE

We, **Bittu Harishankar, Chinna Bheemanna Malathi, Kethidi Rajinikar Reddy,** bearing Roll Nos. **21R11A6208, 21R11A6213, 21R11A6231**,hereby declare that Project Seminar report entitled **"A Bitcoin Transaction Network Analytic Method For Future Blockchain Forensic Investigation"** is done under the guidance of **Dr.Shraban Kumar Apat**, **Associate Professor**,Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, is submitted in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in CSE(Cyber Security**).

This is a record of bonafide work carried out by us in Geethanjali College of Engineering and Technology and the results embodied in this project have not been reproduced or copied from any source. The results embodied in this project report have not been submitted to any other University or Institute for the award of any other degree or diploma.

Bittu Harishankar (21R11A6208),

Chinna Bheemanna Malathi (21R11A6213),

Kethidi RajinikarReddy(21R11A6231),

Department of CSE(CS),

Geethanjali College of Engineering and Technology, Cheeryal.

ACKNOWLEDGEMENT

We are greatly indebted to the authorities of Geethanjali College of Engineering and Technology, Cheeryal, Medchal Dist., for proving us the necessary facilities to successfully carry out this Project Seminar work titled "**A Bitcoin Transaction Network Analytic Method For Future Blockchain Forensic Investigation**".

Firstly, we thank and express our solicit gratitude to **Dr.B.Dhanalaxmi** HOD, Cyber Security department, Geethanjali College of Engineering and Technology, for her invaluable help and support which helped us a lot in successfully completing our Major Project.

Secondly, we express our gratitude to **Dr.Shraban Kumar Apat**, **Assoc. Professor**, internal guide, Geethanjali College of Engineering and Technology, for his suggestion and encouragement which helped us in the successful completion of our major project. We would like to express our sincere gratitude to our Principal **Dr. K. Sagar** for providing the necessary infrastructure to complete our project. Finally, we would like to express our heartfelt thanks to our parents who were very supportive both financially and mentally and for their encouragement to achieve our set goals.

ABSTRACT

Blockchain-based currencies (especially Bitcoin) are increasingly being used to commit illegal activities. In recent years, methods for monitoring and analyzing suspected transactions and addresses associated with the Bitcoin network (e. g. address clustering and inflow patterns) have become more popular. However, such methods tend to strictly focus on Bitcoin address and transaction inflows and ignore other important data like the structure of sales and behavior of users engaging in the transaction. In order to address this gap and achieve maximum performance of all transaction features, this paper put forwards a novel Bitcoin transaction network model to facilitate blockchain forensic investigations on the basis of an advanced secure Petri Net framework. The model being suggested builds on the features and behaviors of Petri nets to outline both the static and dynamic aspects of Bitcoin transactions. We propose a new dataset of nineteen key attributes with efficient features to efficiently characterize Bitcoin transactions so as to facilitate detection of suspicious addresses. The Petri net transitions include genetic data on Bitcoin to enable direct prediction and analysis of Bitcoin inflows. We apply boundary distribution analysis of Bitcoin transaction features in order to better detect suspicious addresses with a lower false positive rate and introduce data visualization techniques. The Bitcoin transaction network model proposed not only is an effective forensic investigation tool but also acts as a prototype platform of financial security and it is shown by analysing real-world case studies.

LIST OF FIGURES

TABLE OF CONTENETS

Contents **Page No**

1. INTRODUCTION

1.1 About the project

Bitcoin has increasingly become a popular and important currency over several generations, and this growth has been inevitable since it was first introduced to the public by Satoshi Nakamoto[1]. The number of Bitcoin's requests has been observed to exceed more than $200 billion as of the end of 2017[2] Bitcoins are not typically associated with their stoner identifiers, as can be seen with stoner names, home addresses, and other additional identification information. Because of this, Bitcoin is incorrectly viewed as an anonymous currency on the Internet and is also incorrectly regarded as being used for untraceable transactions in illegal transactions [2].

Since the use of the suspected name Bitcoin has been used in illegal cultivation to illicit drug and deadly implements trafficking etc. Silk Road [3] is an online dark request and the first state-of-the-art dark net request designed and operated since 2011. The illegal use of Bitcoin has risen since it used Bitcoin as the main source of transaction; $15 million bones transactions have been recorded during the period between 3 February 2012 and 24 July 2012. Alpha Bay and Hansa are two of the largest dark web sites where illegal transactions happen for weapons, drugs, falsified documents, stolen credit card information, and other variety of products. The illegal use of Bitcoin has also increased. It is very difficult for authorities to track and closure of such types of online activity, and therefore the use of Bitcoin is quite easy to individuals.

It is also good to note that about 95 per cent of washed coins are associated with the nine Dark web trading. A teller of BTC-e[5], the retail trade in which Bitcoin has become fungible since 2011, vacuums encouraged more than $4 billion worth of illegal accounts of people involved in crime, from computer hacking to drug trafficking. Fear-based oppressors have also found themselves more closely tied with Bitcoin as early as 2012, using Bitcoin to exchange for illicit support transfers and gifts. also, Bitcoin is not recognized as legitimate electronic money at the exhibition room, so there is little evidence that even established rules for obtaining Bitcoin are being put into place until now.

1.2 Objective

The objective of the project, "A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation," is to develop a robust analytical framework that enables comprehensive forensic investigation of Bitcoin transactions. The specific objectives include:

1. Enhance Forensic Capabilities for Bitcoin Transactions: Develop a reliable method to trace, analyze, and identify suspicious Bitcoin transactions and addresses associated with illicit activities.

2. Integrate Structural and Behavioral Analysis: Utilize Petri net-based modeling to incorporate both static and dynamic features of Bitcoin transactions, moving beyond simple address clustering and flow analysis to include transaction structures and behavioral patterns.

3. Detect Anomalous Transaction Patterns**:** Apply pattern matching and simulation algorithms to identify irregularities in transaction flows, enabling accurate detection of potentially illegal or suspicious transactions.

4. Provide a Prototype Platform for Financial Security: Establish a prototype platform that law enforcement and financial institutions can use for investigating Bitcoin-related financial crimes, ultimately supporting broader anti-money laundering and regulatory compliance efforts.

5. Improve Analysis Accuracy and Efficiency: Use advanced data processing, pattern matching, and data visualization techniques to reduce false positives, thus increasing the accuracy of detecting suspicious addresses and improving the overall efficiency of the forensic investigation process.

1. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

The existing methods for analyzing Bitcoin transactions primarily consist of address clustering and Bitcoin flow analysis. Address clustering attempts to recognize instances of different addresses with common usage patterns (typically common input heuristics) in order to cluster them into wallets presumably belonging to the same entity. Bitcoin flow analysis aims to follow the trail of Bitcoins from one transaction to another in order to track flow of funds.

These approaches do not always work as they mostly remove the structural and behavioral aspects of the transaction data out of the picture. Certain things such as address correspondence evolution over time, the complexity of the transaction graphs and temporal behavior in particular are largely neglected. Due to the above problems malicious actors can take advantage of these missing features to obscure their activities and existing forensic tools can be ineffective for some cases.

Challenges Faced by the Existing System:

- **Overreliance on address clustering:** heuristic based address clustering can be inaccurate and may combine unrelated addresses together, or fail to detect connections between related addresses.
- **inability to capture behavioral patterns:** existing approaches do not adequately model user behavior or complexity of transaction interactions which are critical to detecting suspicious patterns.
- **No dynamic modeling:** No representation of the flow of Bitcoin as a dynamic system and this is necessary for detecting hidden connections between transactions.
- **Pseudonymity limitations**: Bitcoin is falsely believed to be anonymous, and therefore it is difficult for governments and law enforcement agencies to control or track illegal financial flows.

2.2 Proposed System

In this system an analytical framework built using safe Petri Net modeling is proposed as a more integrative approach to Bitcoin forensic investigation: instead of dealing with static transaction data and addresses, a model considers Bitcoin addresses as places and transactions as transitions, enabling the dynamic and structural simulation of Bitcoin transaction networks (BTNs).

This approach captures static features of the Bitcoin ecosystem (e. g. enter/output, time stamps, transaction flows, transaction timing patterns) and dynamic behaviors (e. g. flow of funds, Transaction timing patterns) by simulated state change within the transaction network. The model learns anomalous behavior across the transaction network that is outside known patterns of transactions, thus helping to identify suspected illegal behavior more easily.

Also there is another concept that I believe is called the Bitcoin Gene, which is basically what you run through Petri net transitions as a kind of "dye", and allows you to figure out exactly where certain transactions go in the network.

Enhanced Capabilities of the Proposed System:

- **Pattern-based anomaly detection:** Advanced pattern-matching algorithms are applied to detect anomalies in transaction behavior.
- **Behavioral modeling:** Uses transaction structure as well as behavior, resulting in more accurate identification of suspicious transactions.
- Marginal distribution analysis / visualization Data visualization techniques are used to reduce false positives in the analysis of data.
- **Simulation environment:** The simulation environment allows the testing of hypotheses, and forensic conclusions, against real data.
- **Legal and regulatory alignment:** To support AML/KYC compliance requirements, and to empower law enforcement agencies to implement comprehensive tools.

2.3 Feasibility Study

This study is conducted to assess technical feasibility—meaning— technical requirements of the system - Any system developed should not have a high requirement on the available technical resources. Such a system will result in high demands on the available technical resources. This will result in high demands on the client. The system developed should have small requirement because no substantial or nil changes are needed for implementing the system.

2.3.1 Details

Technical Feasibility:

This study should be performed in order to ensure the technical feasibility, that is to say the technical requirements of the system. Any system developed should not have a high demand of the available technical resources. That will result in high demands of the available technical resources. That will result in high demands being made on the client. The developed system should have modest requirement as only minimal or null changes are required to implement the system.

Economic Feasibility:

We carried out this study to assess the economic impact that the system will have on the organization, as the amount of money available to the company in terms of research and development of the system is limited, and expenditures must be justified. Therefore developed system was done within budget, and this resulted because most of the technologies used were free of charge, only the customized products needed to be purchased.

Social Feasibility:

The other aspect of this study is to assess the acceptance level of the system by the users i. e. training them in how to use the system effectively. The user should not feel threatened by the system but must accept it as a necessity. The acceptance of the users purely depends on the methods used to educate the user about the system and make him familiar with the system. He should also be given some degree of confidence so that he can also make some constructive criticism which may be welcomed because he is the final user of the system.

2.3.2 Impact on Environment

Energy Consumption of Blockchain Analysis:

- The project involves analyzing a significant amount of Bitcoin Blockchain data, which requires substantial computational resources. The heavy processing tasks for parsing Blockchain data, building Petri nets, and performing simulations can lead to increased energy consumption, contributing to the carbon footprint of the project.
- As Bitcoin transactions and Blockchain nodes inherently consume a lot of electricity due to the proof-of-work consensus mechanism, adding analytical tools can further increase resource demand, indirectly impacting the environment if powered by non-renewable energy sources.

Promoting Sustainable Blockchain Analysis:

- To mitigate environmental impact, the project could integrate energy-efficient algorithms and utilize cloud services that leverage renewable energy sources. Future iterations may also focus on optimizing computational processes to reduce energy consumption.

2.3.3 Safety

To preserve the integrity and confidentiality of critical Blockchain data, the project places a strong emphasis on data security through encryption, safe storage, and strict access controls. Adherence to legal frameworks, such as know-your-customer (KYC) and anti-money laundering (AML) requirements, guarantees regulatory adherence, reducing legal risks and boosting the tool's legitimacy. IProtections against misuse are crucial to prevent privacy violations or baseless accusations. In order to lower financial crime and promote a safer, more secure financial environment, the main goal is to help law enforcement detect and examine questionable Bitcoin transactions.

2.3.4 Ethics

The project also presents an ethical dilemma in weighing privacy against traceability, given that it intends to trace Bitcoin transactions that are likely to undermine the pseudonymous nature of Bitcoin, which was created to secure users' identities. While openness is crucial for the prevention of illegal activities such as money laundering and terrorism funding, it must be balanced with users' privacy rights. Ethical utilization involves strict compliance with legal frameworks, such that investigations are both justified and authorized. Misuse by unauthorized individuals also poses a risk, potentially invading user privacy or wrongly targeting individuals, necessitating strong safeguards, access controls, and compliance regimes. In spite of the aforementioned issues, the tool has enormous ethical advantages through its support of law enforcement in combating financial crime within the dark web and thereby advancing justice and public safety.

2.3.5 Cost

Cost of the project mostly happens in terms of software development, computing infrastructure, as well as data acquisition. Several open source tools like Python, TensorFlow and Pandas can help cut down development costs. Most probably one will have to invest in high performance computing infrastructure to process large amount of Blockchain data.. Operational expenses on a regular basis include server management, cloud facilities, and updates for improved algorithms. Expenses may also be incurred in the application of secure storage of data solutions and compliance with AML and KYC regulatory requirements. Albeit these costs, the benefits of savings realized through the avoidance of financial fraud and support of law enforcement investigation can provide huge value, justifying the project as a cost-saving solution to Bitcoin forensic analysis.

2.3.6 Type

The project is a state-of-the-art software product that analyses Bitcoin transactions as forensic analysis. At its core, it is a financial security and regulatory technology (RegTech) product, particularly dedicated to anti-money laundering (AML) activities and suppression of

financial crimes. It combines data analysis and patterns spotting, in order to leverage advanced algorithms and blockchain analytics, to identify and effectively track ill-gotten gains.

2.4 Scope of the Project

The project scope is to develop a sophisticated Bitcoin transaction analysis platform based on Petri net-based modeling for the purpose of facilitating forensic investigations. The platform should trace, analyze, and identify suspicious behavior by representing Bitcoin transactions and addresses as transitions and places in a Petri net.By integrating static (transactional structuring) and dynamic (behavioral pattern) attributes, the software is better than previous mechanisms of address group and flow analysis and provides a more comprehensive picture of transactional networks. The site also attempts to improve detection accuracy by using advanced pattern-matching software and simulation techniques that allow it to identify anomalous patterns of transactions indicative of illicit activity. The primary objective is to create an authentic and extendable system, which can provide support to financial regulators as well as law enforcement agencies in discovering Bitcoin-related monetary crimes.

In addition, the project also considers an easy-to-use and energy-saving system that makes use of automated pattern recognition and intermediary saving to optimize performanceIt also hopes to further develop its future capabilities by implementing forensic analysis for other cryptocurrencies and offering more comprehensive integrated solutions for Blockchain investigations. By creating a prototype platform, the project not only deals with existing forensic issues but also establishes a scalable platform for anti-money laundering activities and regulatory compliance. The scope involves creating a secure and sustainable platform with encryption, strong access controls, and adherence to legal and ethical standards to maintain credibility and efficient use in real-world settings.

2.5 Module Description

Upload Blockchain Transaction:

It lets you upload data file to have Bitcoin transactions data. That way it will extract data from raw Blockchain data (i. e. not mutable attributes like transaction ID, etc.

Parse & Construct Bitcoin Transaction Network (BTN) Using Petri Net:

During the module uploaded Blockchain dataset is analyzed and a Petri net model is constructed to simulate the Bitcoin Transaction Network (BTN). Places represent Bitcoin addresses and transitions represent Bitcoin transactions.Using this Petri net framework, the dynamic simulation of Bitcoin flow can be realized, as well as detecting transaction patterns.

Run Pattern Matching Rules Algorithm

This module uses pre-defined pattern-matching rules on the BTN model to identify anomalies or suspicious transactions. It scans the flow of Bitcoin by checking dynamic attributes such as deposit and withdrawal amounts. The algorithm marks any transaction that deviates from typical patterns, identifying possible fraudulent behavior.

Analyze Suspected Addresses

This module is dedicated to tracing and analyzing addresses that were labeled as suspicious in the previous step. It applies the Bitcoin "gene" functionality to trace the movement of funds via dyeing addresses, measuring the strength of the relationship between addresses.

2.6 System Configuration

1. Hardware Requirements

- Processor: At least 2 GHz, Quad-core (Intel/AMD)
- RAM: Minimum 8 GB (16 GB recommended)
- Storage: 256 GB SSD for fast performance
- Network: High-speed internet for blockchain sync
- Graphics Card: Optional, but helpful for testing environments

2. Software Requirements

Programming Languages:

- Python 3.7+ (for data analysis, pattern matching, and machine learning algorithms).
- JavaScript (for front-end user interface and data visualization).
- Solidity (optional, for analyzing smart contract-based transactions if extended to Ethereum).

Development Tools:

- Python IDE (PyCharm, Jupyter Notebook, or Visual Studio Code): For coding and debugging.
- Node.js (Version 12.3.1): For server-side operations and integration with Blockchain APIs.
- Visual Studio Community Version: For developing and integrating components.

Libraries and Frameworks:

- Pandas, NumPy: For data processing and analysis.
- Matplotlib, Plotly: For visualizations and plotting graphs.
- TensorFlow: For implementing any machine learning algorithms (optional).
- Scikit-learn: For pattern matching and anomaly detection.
- PyPetri: For Petri net simulation and analysis.

Database:

- SQLite or MySQL: For storing parsed Blockchain transaction data and analysis results.

Web Browser:

- Google Chrome, Mozilla Firefox, or any modern browser (for accessing web-based user interfaces).

APIs and Tools:

- Blockchain API: For fetching real-time Bitcoin transaction data if needed.
- BitcoinDatabase-Generator: An open-source tool for parsing and generating Bitcoin Blockchain dataset.

LITERATURE OVERVIEW

3.1 Research Paper 1

Bitcoin: A Peer-to-Peer Electronic Cash System

Link: https://bitcoin.org/bitcoin.pdf

ABSTRACT: : An entirely peer-to-peer form of electronic cash would permit online payments to be made directly between parties, bypassing the need for an intermediary financial institution. Digital signatures offer part of the solution, but the benefits are lost if a trusted third party is nevertheless needed to avert double-spending. We suggest a peer-to-peer solution to the problem of double-spending. The network timestamps blocks by including a hash of the previous block's header. This system allows for a record that is not only permanent, but also has a clear understanding of causality within it. The longest chain not only represents proof of the sequence of events that was witnessed, but proof that it originated from the largest pool of CPU power. Provided that the majority of CPU power is held by nodes which are not working together to assault the network, they'll produce the longest chain and outrun attackers. The network itself doesn't need much structure. Messages are delivered based on effort, and nodes in the network can join or leave whenever they want. When they return, they rely on the longest proof-of-work chain to understand what happened during their absence

3.2 Research Paper 2

Platform criminalism: The'lastmile'geography of the darknet market supply chain

Link: https://arxiv.org/abs/1712.10068

ABSTRACT: Does recent growth of darknet markets signify a slow reorganisation of the illicit drug trade? Where are darknet markets situated in the global drug supply chain? In principle, these platforms allow producers to sell directly to end users, bypassing traditional trafficking routes. And yet, there is evidence that many offerings originate from a small number of highly active consumer countries, rather than from countries that are primarily known for drug production. In a large-scale empirical study, we determine the darknet trading geography of

three plant-based drugs across four of the largest darknet markets, and compare it to the global footprint of production and consumption for these drugs. We present strong evidence that cannabis and cocaine vendors are primarily located in a small number of consumer countries, rather than producer countries, suggesting that darknet trading happens at the 'last mile', possibly leaving old trafficking routes intact. A model to explain trading volumes of opiates is inconclusive. We cannot find evidence for significant production-side offerings across any of the drug types or marketplaces. Our evidence further suggests that the geography of darknet market trades is primarily driven by existing consumer demand, rather than new demand fostered by individual markets.

3.3 Research Paper 3

Tracking digital footprints: anonymity within the bitcoin system

Link:https://www.researchgate.net/publication/316893801_Tracking_digital_footprints_anonymity_within_the_bitcoin_system

ABSTRACT: This paper critically explores the anonymity of Bitcoin transactions and evaluates the feasibility of law enforcement tracing illicit activities to a user's real-world identity. Building upon the methodology of Reid and Harrigan (2013), the study examines whether transaction data on the blockchain can be combined with external sources to identify individual users. In addition to a comprehensive literature review on Bitcoin's anonymity and traceability, the paper investigates the practices of four Bitcoin exchange services, focusing on the reliability of the user information submitted during sign-up. The research tests whether law enforcement can reasonably rely on this information for prosecution and whether these services accept fraudulent or illegitimate data during the verification process. Findings reveal that, while transaction histories may lead to exchanges, inadequate implementation of anti-money laundering (AML) laws and Know Your Customer (KYC) standards in some exchanges enables tech-savvy or resourceful criminals to circumvent identity controls, preserving their anonymity. The study underscores the urgent need for stricter compliance with KYC and customer due diligence regulations to enhance the reliability of data that law enforcement can access. Furthermore, the paper highlights the necessity for research into how criminals bypass existing

controls to finance illicit activities, emphasizing the importance of strengthening identification protocols to ensure accountability.

3.4 Research Paper 4

An analysis of anonymity in the bitcoin system

Link:https://ieeexplore.ieee.org/document/6113303

ABSTRACT: Anonymity in Bitcoin, a peer-to-peer electronic currency system, is a complicated issue. Within the system, users are identified by public-keys only. An attacker wishing to de-anonymize its users will attempt to construct the one to-many mapping between users and public-keys and associate information external to the system with the users. Bitcoinfrustrates this attack by storing the mapping of a user to his or her public-keys on that user's node only and by allowing each user to generate as many public-keys as required. In this paper we consider the topological structure of two networks derived from Bitcoin's public transaction history. We show that the two networks have a non-trivial topological structure, provide complementary views of the Bitcoin system and have implications for anonymity. We combine these structures with external information and techniques such as context discovery and flow analysis to investigate an alleged theft of Bitcoins, which, at the time of the theft, had a market value of approximately half a million U.S. dollars.

3.5 Quantitative analysis of the full bitcoin transaction graph

Link:https://eprint.iacr.org/2012/584.pdf

ABSTRACT: The Bitcoin scheme is a rare example of a large scale global payment system in which all the transactions are publicly accessible (but in an anonymous way). We downloaded the full history of this scheme, and analyzed many statistical properties of its associated transaction graph. In this paper we answer for the first time a variety of interesting questions about the typical behavior of users, how they acquire and how they spend their bitcoins, the balance of bitcoins they keep in their accounts, and how they move bitcoins between their various accounts in order to better protect their privacy. In addition, we isolated all the large transactions in the system, and discovered that almost all of them are closely related to a single large transaction that took place in November 2010, even though the associated users apparently

tried to hide this fact with many strange looking long chains and fork-merge structures in the transaction graph.

4. SYSTEM DESIGN

4.1 System Architecture

The proposed he proposed system architecture begins with uploading a blockchain transaction dataset, which is then processed to extract transaction addresses and timing details. This data is used to build a Petri Net simulation of the Bitcoin Transaction Network (BTN). The system runs a pattern-matching algorithm to detect and remove illegal payment addresses based on predefined rules. It also checks these transactions against a cached set of known illegal activities to avoid repeating the same analysis and to improve detection accuracy.

Once illegal addresses are filtered out, the system creates two transaction graphs: one for withdrawals and another for deposits. These graphs help visualize the flow of funds and trace suspicious movements. A comparison is then made between the proposed transaction patterns and the extended ones to identify unusual behavior. Finally, the system generates an execution time graph, which compares how long it takes for both sets of transactions to complete, helping investigators understand and analyze transaction speed and behavior more effectively.

4.1.1 Module Description

a) Upload Blockchain Transaction

It lets you upload data file to have Bitcoin transactions data. That way it will extract data from raw Blockchain data (i. e. not mutable attributes like transaction ID, etc.

b) Parse & Construct Bitcoin Transaction Network (BTN) Using Petri Net:

During the module uploaded Blockchain dataset is analyzed and a Petri net model is constructed to simulate the Bitcoin Transaction Network (BTN). Places represent Bitcoin addresses and transitions represent Bitcoin transactions.Using this Petri net framework, the dynamic simulation of Bitcoin flow can be realized, as well as detecting transaction patterns.

c)Run Pattern Matching Rules Algorithm

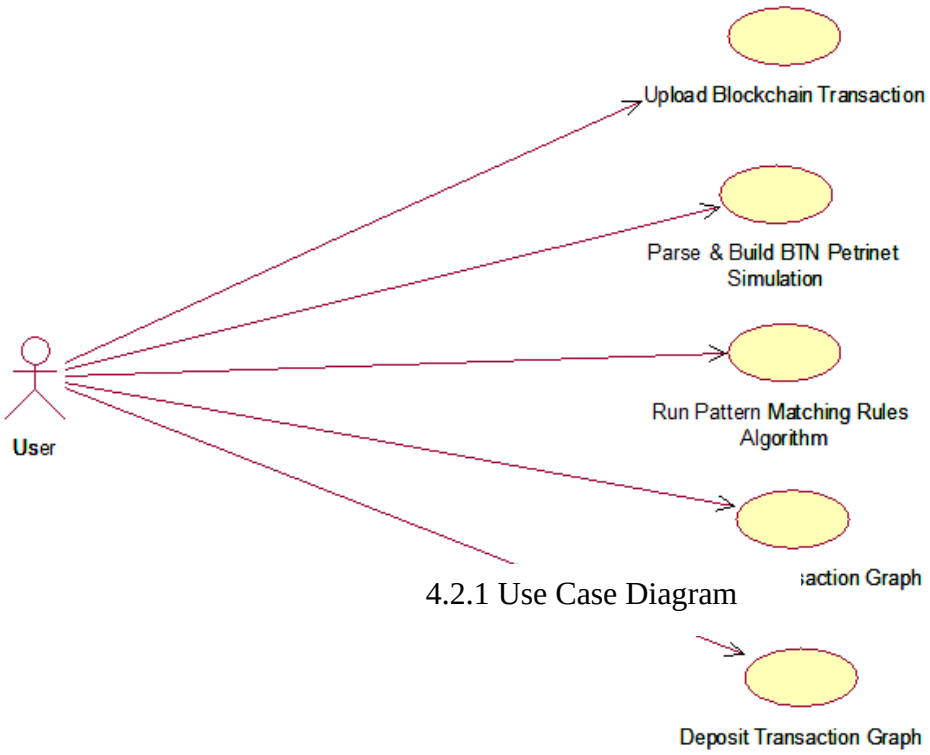
This module uses pre-defined pattern-matching rules on the BTN model to identify anomalies or suspicious transactions. It scans the flow of Bitcoin by checking dynamic attributes such as deposit and withdrawal amounts. The algorithm marks any transaction that deviates from typical patterns, identifying possible fraudulent behavior.

d)Analyze Suspected Addresses

This module is dedicated to tracing and analyzing addresses that were labeled as suspicious in the previous step. It applies the Bitcoin "gene" functionality to trace the movement of funds via dyeing addresses, measuring the strength of the relationship between addresses

4.2 UML DIAGRAMS

4.2.1 Use-Case Diagram

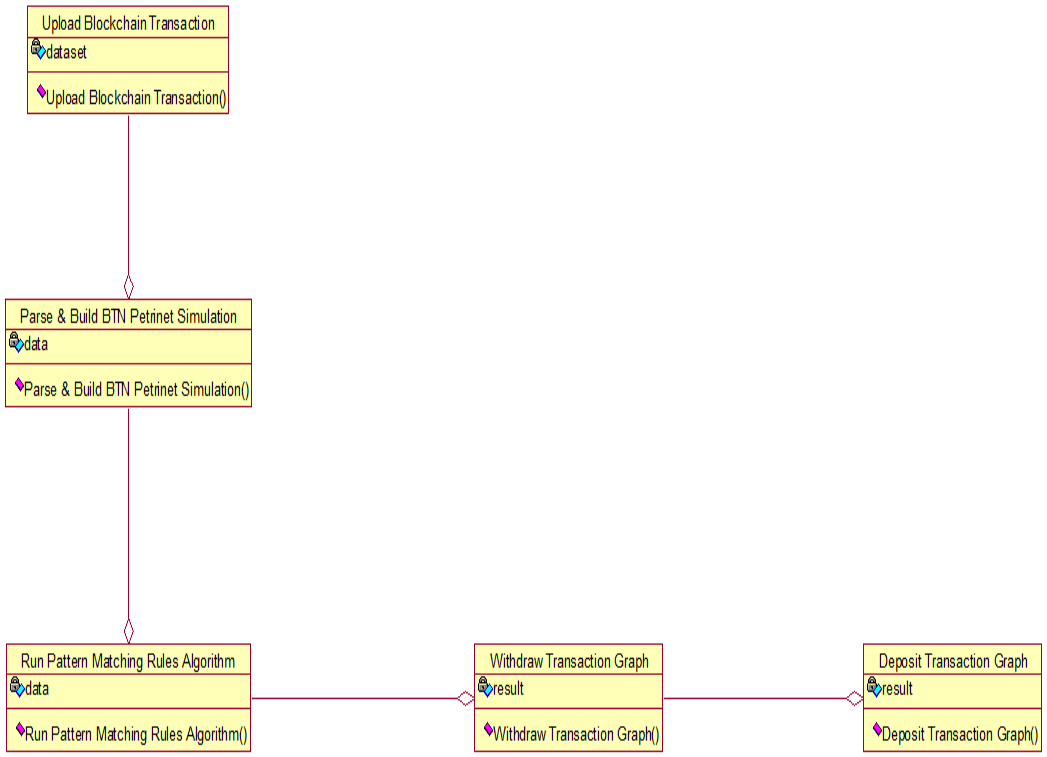


4.2.1 Use Case Diagram

The use case diagram illustrates the interaction between a user and a blockchain transaction analysis system designed to enhance forensic investigations. The system allows the user to upload blockchain transaction data, which serves as the initial step in the analysis process. After uploading, the system parses the data and builds a Behavior Token Net (BTN) Petri net simulation, transforming raw transaction data into a visual model for pattern analysis. The user can then initiate a pattern matching rules algorithm, which detects suspicious transaction behavior such as fraud or money laundering. Additionally, the system provides

functionalities to generate both withdrawal and deposit transaction graphs, helping users visually interpret outgoing and incoming transactions, respectively, for in-depth forensic and audit analysis.System in the provision of a secure, transparent, and tamper-proof management of the digital evidence.

4.2.2 Class Diagram

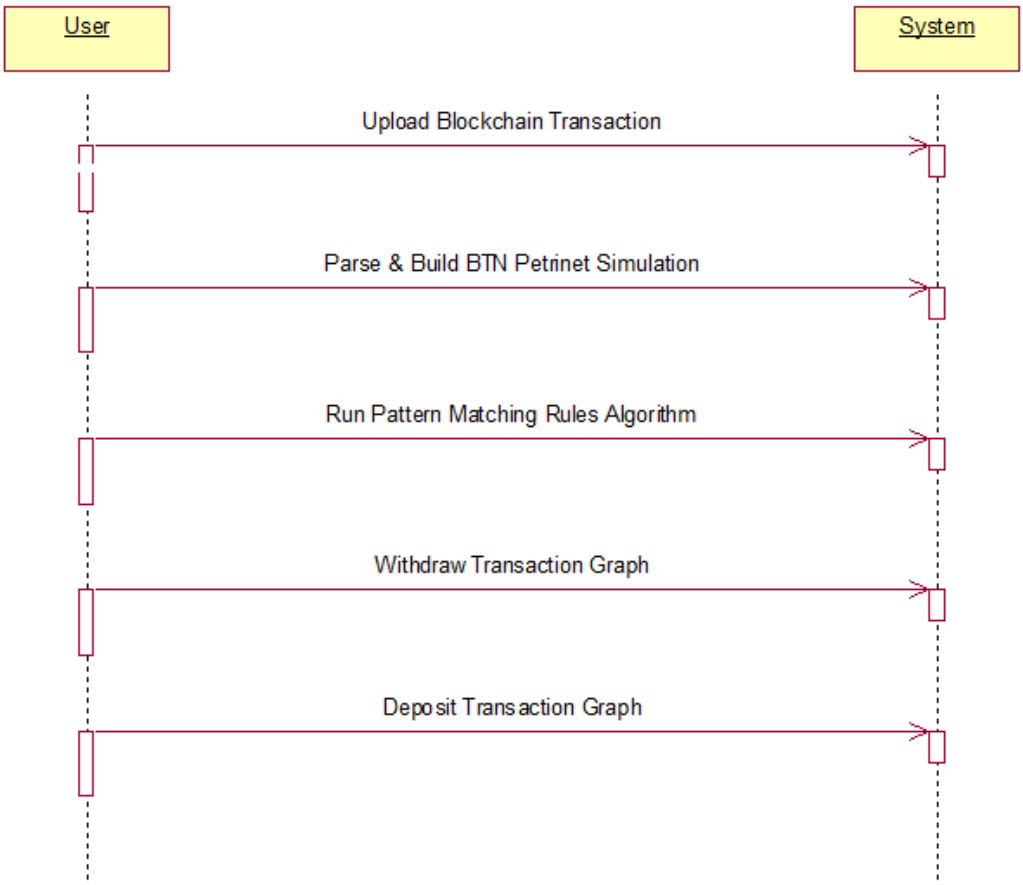


4.2.2 Class Diagram

The Class diagram of the blockchain transaction analysis system that utilizes Petri net simulations and pattern matching for forensic analysis. The process begins with the user uploading a blockchain transaction dataset, which serves as the foundational input. This dataset is then parsed and transformed into a Behavior Token Net (BTN) Petri net simulation to structure the data into an analyzable format. Following this, the system applies a pattern matching rules algorithm on the simulated data to detect any suspicious activity or irregular transaction behaviors. The results generated from this analysis can then be used to create two

types of graphical outputs: a Withdraw Transaction Graph and a Deposit Transaction Graph. These visual representations assist in understanding and monitoring the flow of outgoing and incoming transactions, thereby supporting investigative and auditing processes.

4.2.3 Sequence Diagram

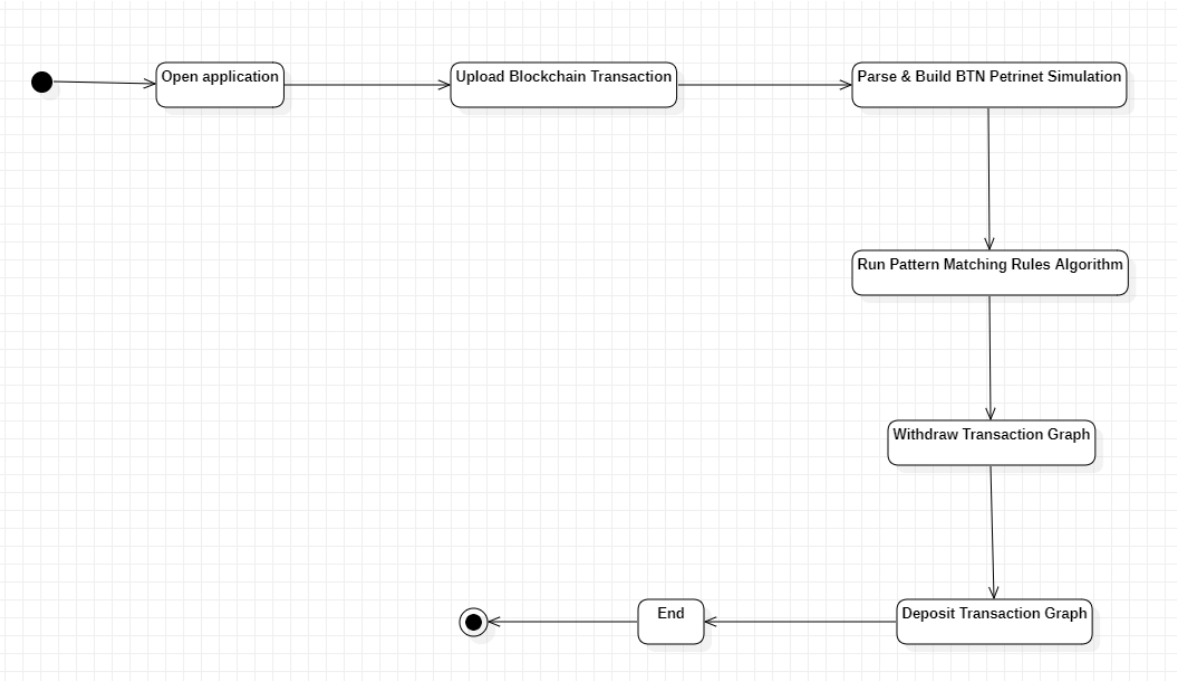


4.2.3 Sequence Diagram

The sequence diagram illustrates the step-by-step communication between the User and the System during the process of blockchain transaction analysis. Initially, the User sends a request to upload a blockchain transaction dataset, which the System receives and processes. Following this, the User initiates the parsing and construction of a Behavior Token Net

(BTN) Petri net simulation based on the uploaded data. Once the simulation is built, the User triggers the pattern matching rules algorithm, prompting the System to analyze the transaction patterns for suspicious activity. After the analysis, the User sequentially requests the generation of a Withdraw Transaction Graph and a Deposit Transaction Graph. The System responds by providing visual representations of outgoing and incoming transactions, respectively, allowing for comprehensive forensic and audit evaluation.

4.2.4 Activity Diagram



4.2.4 Activity Diagram

The activity diagram illustrates the sequential workflow of a blockchain transaction analysis system. The process begins with the user opening the application, followed by uploading a blockchain transaction dataset. Once the data is uploaded, the system proceeds to parse the information and constructs a Behavior Token Net (BTN) Petri net simulation. This

simulation provides a structured model of the transaction flow. The next step involves running a pattern matching rules algorithm to analyze the transaction data for any irregularities or suspicious behaviors. Based on the analysis, the system generates a Withdrawal Transaction Graph, which visualizes all outgoing transactions. Subsequently, it produces a Deposit Transaction Graph to represent incoming transactions. The process concludes after the generation of these visual analytics, providing the user with comprehensive insights into the transaction patterns.

5. IMPLEMENTATION

5.1 Implementation

The Bitcoin has become more of a important medium of money over the past few years, and has been virtually impossible to develop since the introduction of Bitcoin by Satoshi Nakamoto[1]At the end of 2017, the total market capitalization of Bitcoin was approximately $200 billion. Bitcoins are not typically associated with their stoner identities in the manner stoner names, home addresses, or other specific identification data were associated with stoners. As a result of this alias-like nature, Bitcoin is sometimes mistaken for being anonymous currency on the Internet and mistaken for representing untraceable transactions in illegal transactions. In this paper, the author employs a transition-based Safe Petri net simulation algorithm to describe state changes in a system through transitions. Bitcoin addresses act like locations in a Petri net, while Bitcoin transactions function as transitions. When a transaction on the Blockchain includes an address, the Petri net considers this a change of state and logs the transaction information in a system called the BTN (Bitcoin Transaction Network). Every transaction on the Blockchain will be analyzed and prepared for the BTN network. This BTN network will perform a deeper analysis using Bitcoin Gene, tracking addresses linked to illegal payments by looking closely at the accounts that have sent and received funds .This Gene will track Bitcoin movements through a specific address, known as the dyeing address, and evaluate the connections between this address and others. In the world of Bitcoin, users are identified solely by their addresses, and there are two main characteristics regarding coins: the balance and the amount received. Pattern matching rules

will be applied to the values of received and balance, where all withdrawals will be regarded as balance and deposits will be counted as received. To guarantee correctness, rules for pattern matching will check that every transaction includes a valid address, which should have one input and several outputs. If a transaction does not follow this format, it will be marked as a potentially suspicious address.

5.2 Sample Code

Filename: app.py

```
from flask import Flask, render_template, request
from datetime import datetime
import json
from web3 import Web3, HTTPProvider
import os
import datetime
app = Flask(__name__)
global details, user
def readDetails(contract_type):
    global details
    details = ""
    blockchain_address = 'http://127.0.0.1:8545'
    web3 = Web3(HTTPProvider(blockchain_address))
    web3.eth.defaultAccount = web3.eth.accounts[0]
    compiled_contract_path = 'Evidence.json'
    deployed_contract_address = '0xC8550864Fe1D8DBB3B87FF38b75009C69eAE37f6'
#hash address to access counter feit contract
    with open(compiled_contract_path) as file:
        contract_json = json.load(file)  # load contract info as JSON
        contract_abi = contract_json['abi']  # fetch contract's abi - necessary to call its
functions
    file.close()
```

```
    contract = web3.eth.contract(address=deployed_contract_address, abi=contract_abi)
#now calling contract to access data
    if contract_type == 'adduser':
        details = contract.functions.getuser().call()
    if contract_type == 'evidence':
        details = contract.functions.getevidence().call()
    if len(details) > 0:
        if 'empty' in details:
            details = details[5:len(details)]
def saveDataBlockChain(currentData, contract_type):
    global details
    global contract
    details = ""
    blockchain_address = 'http://127.0.0.1:8545'
    web3 = Web3(HTTPProvider(blockchain_address))
    web3.eth.defaultAccount = web3.eth.accounts[0]
    compiled_contract_path = 'Evidence.json'
    deployed_contract_address = '0xC8550864Fe1D8DBB3B87FF38b75009C69eAE37f6'
#contract address
    with open(compiled_contract_path) as file:
        contract_json = json.load(file)  # load contract info as JSON
        contract_abi = contract_json['abi']  # fetch contract's abi - necessary to call its
functions
    file.close()
    contract = web3.eth.contract(address=deployed_contract_address, abi=contract_abi)
    readDetails(contract_type)
    if contract_type == 'adduser':
        details+=currentData
        msg = contract.functions.setuser(details).transact()
        tx_receipt = web3.eth.waitForTransactionReceipt(msg)
```

```
    if contract_type == 'evidence':
        details+=currentData
        msg = contract.functions.setevidence(details).transact()
        tx_receipt = web3.eth.waitForTransactionReceipt(msg)
```

Filename: Evidence.Json

```
{
  "contractName": "Evidence",
  "abi": [
    {
      "inputs": [],
      "stateMutability": "nonpayable",
      "type": "constructor"
    },
    {
      "inputs": [],
      "name": "evidence",
      "outputs": [
        {
          "internalType": "string",
          "name": "",
          "type": "string"
        }
      ],
      "stateMutability": "view",
      "type": "function",
      "constant": true
    },
    {
```

```
  "inputs": [],
  "name": "users",
  "outputs": [
    {
      "internalType": "string",
      "name": "",
      "type": "string"
    }
  ],
  "stateMutability": "view",
  "type": "function",
  "constant": true
},
{
  "inputs": [
    {
      "internalType": "string",
      "name": "ca",
      "type": "string"
    }
  ],
  "name": "setevidence",
  "outputs": [],
  "stateMutability": "nonpayable",
  "type": "function"
},
{
  "inputs": [],
  "name": "getevidence",
  "outputs": [
```

```
        {
          "internalType": "string",
          "name": "",
          "type": "string"
        }
      ],
```

Filename: Evidence.sol

```
// SPDX-License-Identifier: MIT
pragma solidity >= 0.4.0 <= 0.9;
contract Evidence {
    string public evidence;
    string public users;
    function setevidence(string memory ca) public {
        evidence = ca;
    }
    function getevidence() public view returns (string memory) {
        return evidence;
    }
    function setuser(string memory pa) public {
        users = pa;
    }
    function getuser() public view returns (string memory) {
        return users;
    }
    constructor() public {
    evidence = "";
    users = "";
    }
}
```

6. TESTING

6.1 Testing

Unit Testing

This is a method of software testing where the individual components or modules of a program are tested in isolation to ensure their correct working. It is typically done by developers and is concerned with verifying the functional correctness of standalone modules before they are integrated. The main aim is to ensure early detection and correction of defects.

Unit Testing Techniques:

Black-Box Testing: In this method, the functionality of the module is tested with given inputs and expected outputs without knowledge of the internal code structure.

White-Box Testing: Internal logic of the functioning of the tested modules is evaluated to ensure that each possible case and condition under which the module exists have been handled.

Data Flow Testing

Data flow testing is a white-box testing method that focuses on the flow of data in a program. Tracking the points at which variables are defined, used, or modified will facilitate checking that the data is correctly handled. These concerns include uninitialized or wrongly modified data.

Integration Testing

Integration testing is performed after all individual units have been tested. The principal task remains to check whether there could be some interaction between these integrated components and check whether the functionality of the integrated units meets the system requirements as a whole. Other things that the test checks may include performance, reliability issues, and checking how well these modules communicate.

Big Bang Integration Testing

With this strategy, every module is integrated simultaneously and tested. This saves some time at the beginning, but once defects are encountered, it is very difficult to know which module is at fault, since there is no incremental validation of the interfaces between the different units.

User Interface Testing

User Interface (UI) testing is a process of evaluating an application by its graphical user interface to ensure that it meets design specifications and responds accurately from the user's perspective. The user interface focuses on visual aspects like buttons, forms, menus, and navigation with the aim of revealing usability issues and defects in the GUI.

6.2 Test Cases

S.NO	INPUT	If available	If not available
1	Add information	User can add information	There is no process
2	Check information	User can check information	There is no process

7.OUTPUT SCREENS

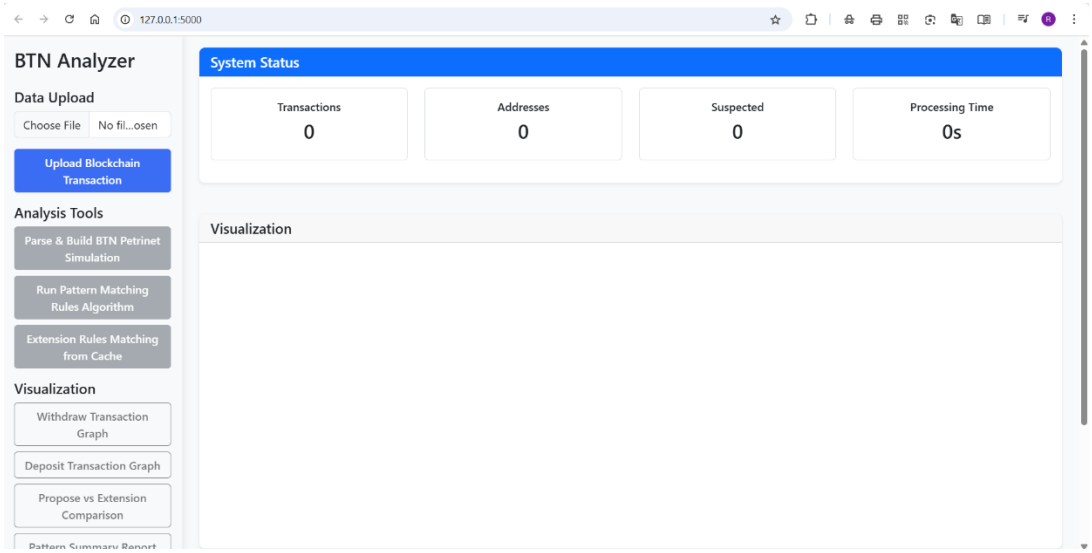


Fig 7.1 Home Page

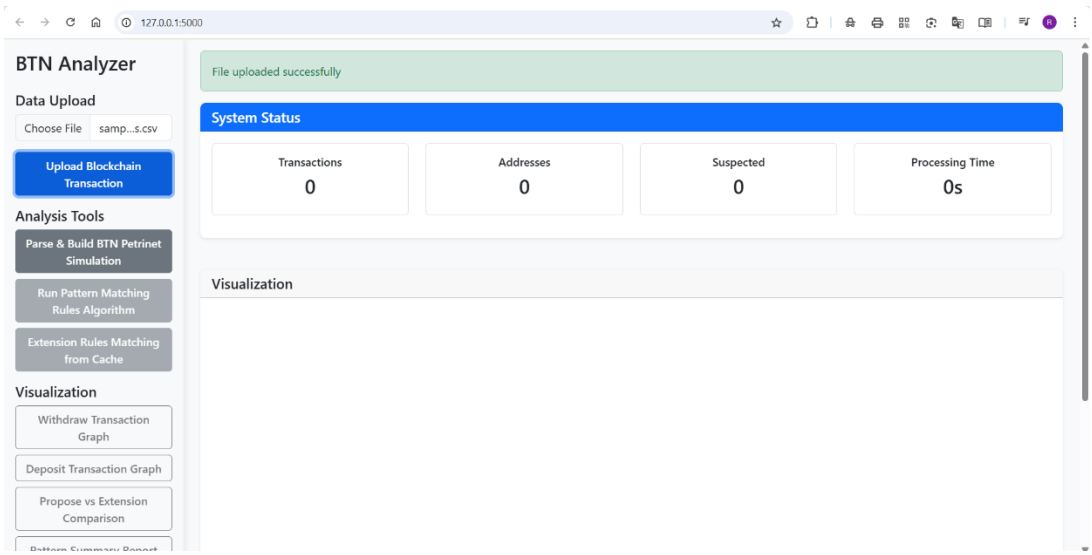


Fig 7.2 Dataset Uploaded

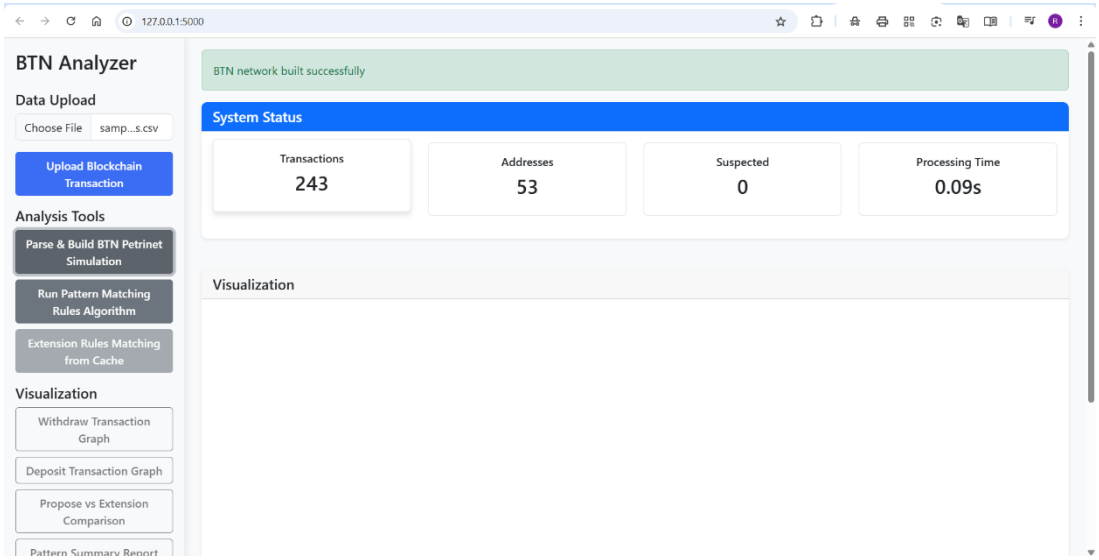


Fig 7.3 Parsing Data Into BTN Page

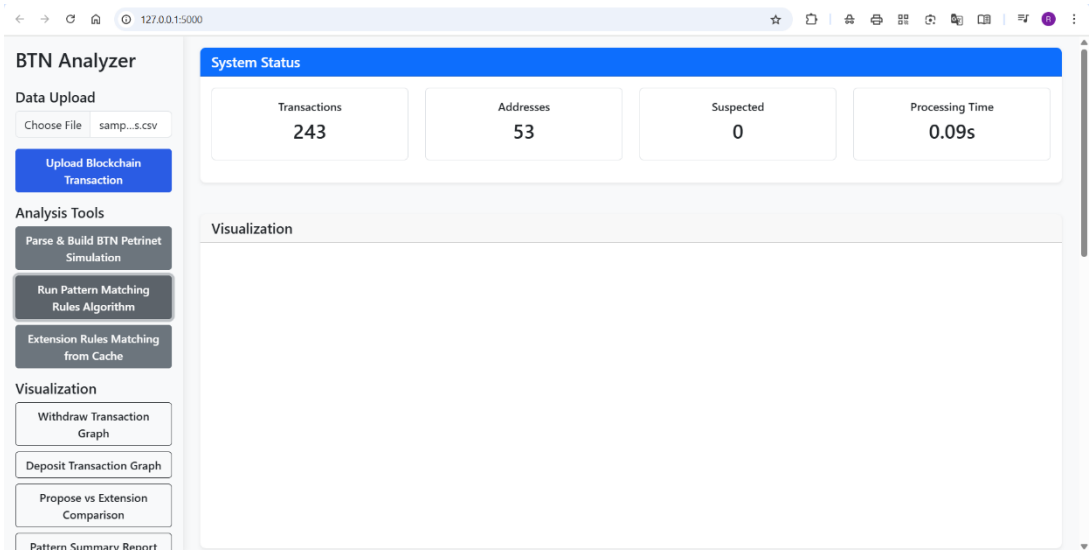


Fig 7.4 Pattern Matching

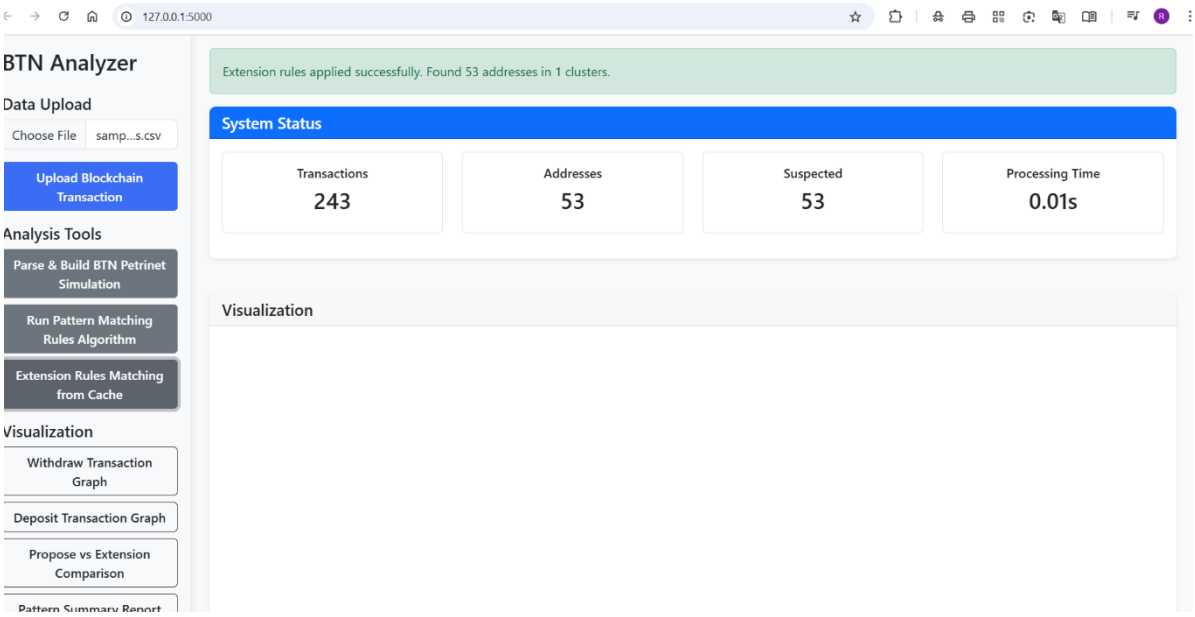


Fig 7.5 Extension Rules Matching Frm Cache

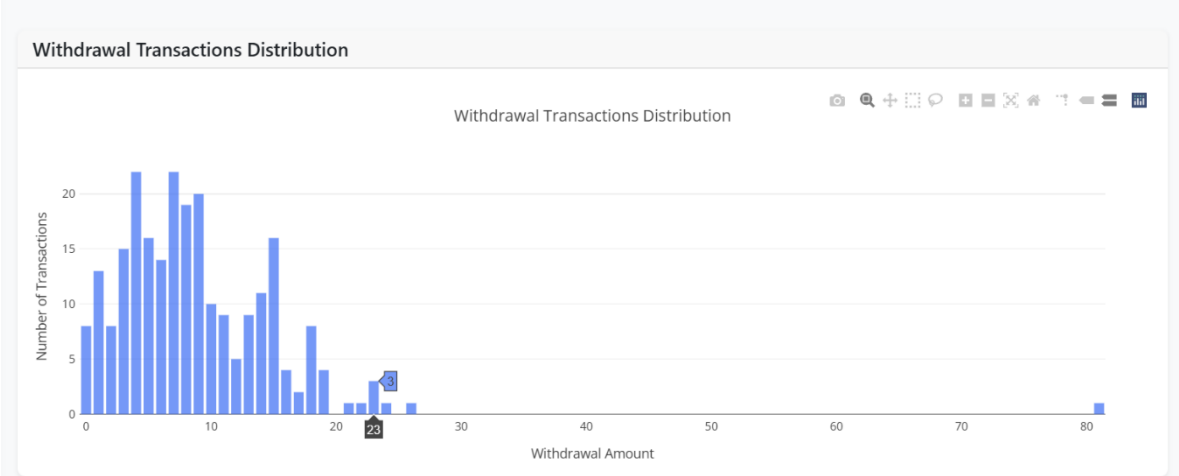
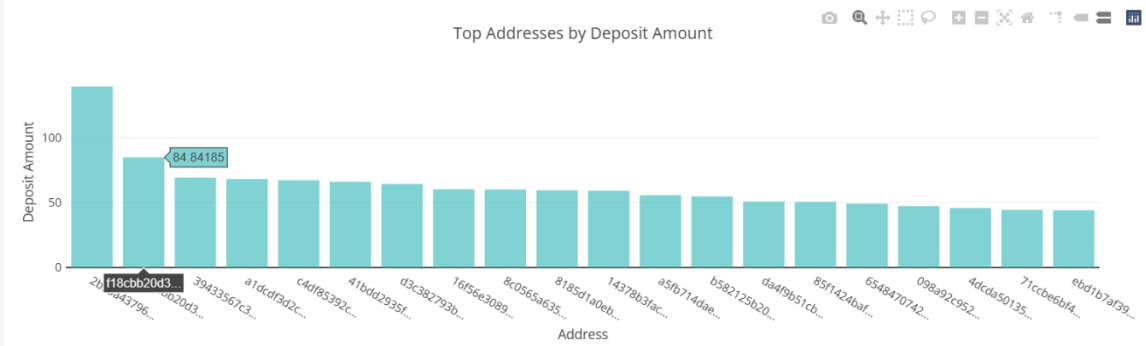
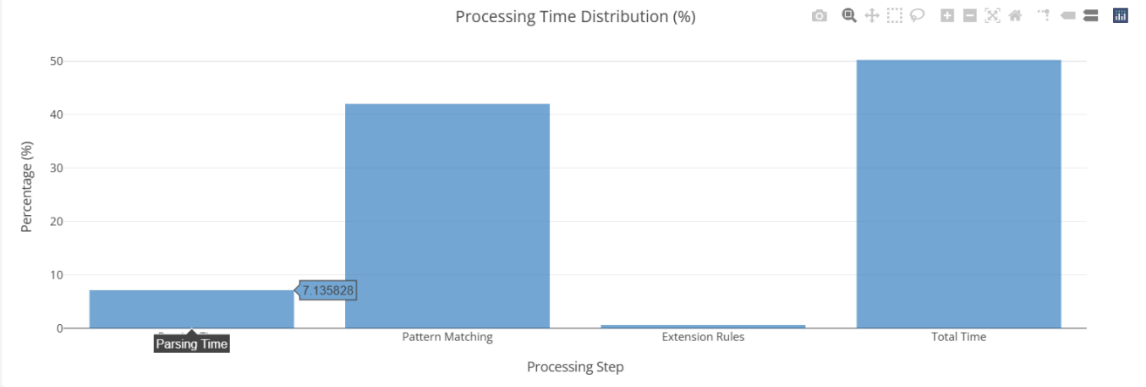


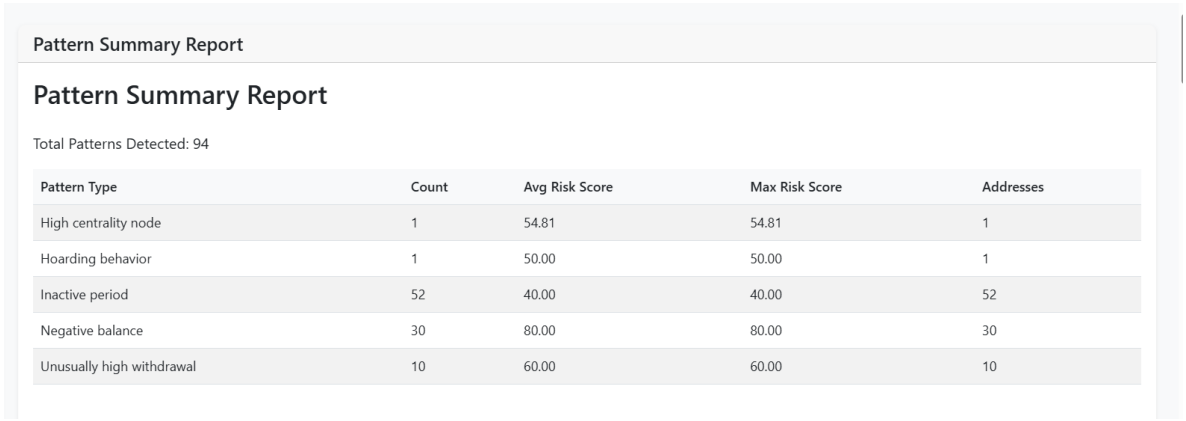
Fig 7.6 Withdrawal Transaction Graph Module

Top Addresses by Deposit Amount



Processing Time Distribution



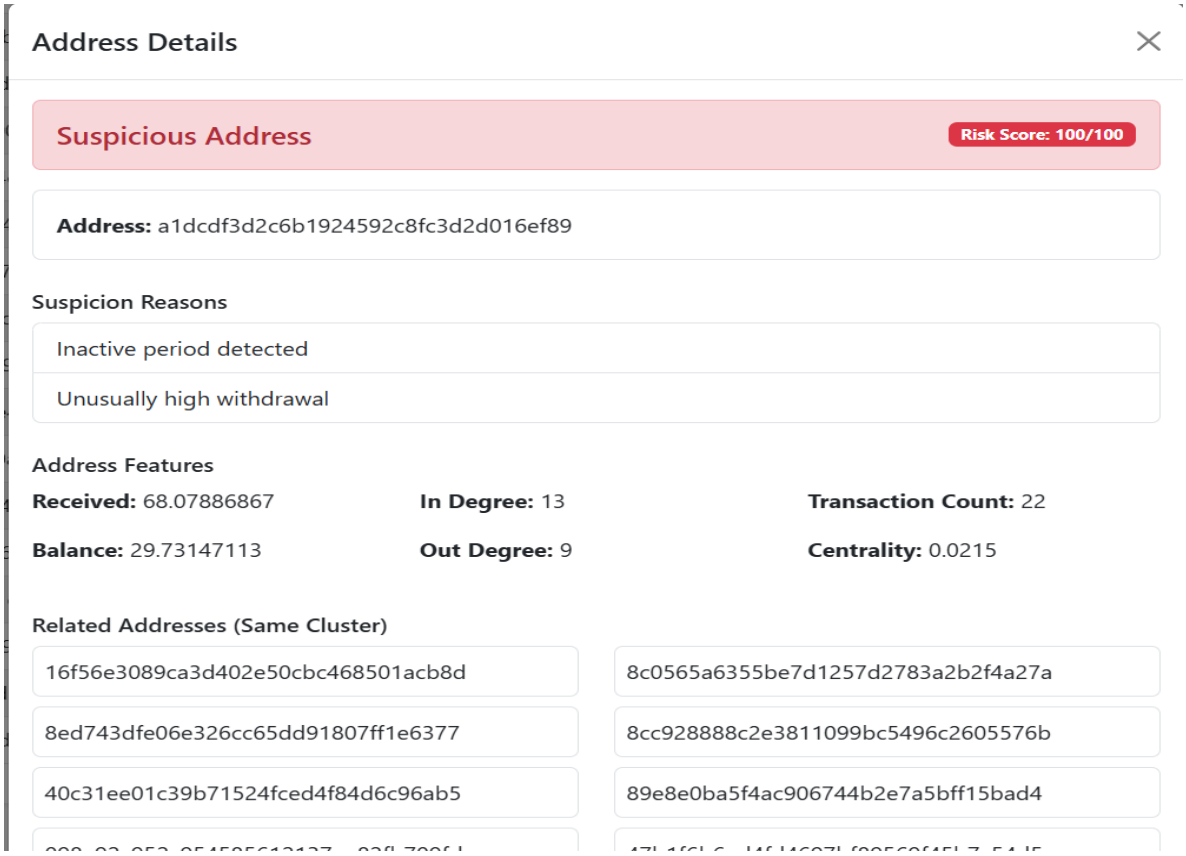


Pattern Summary Report

Pattern Summary Report

Total Patterns Detected: 94

Pattern Type	Count	Avg Risk Score	Max Risk Score	Addresses
High centrality node	1	54.81	54.81	1
Hoarding behavior	1	50.00	50.00	1
Inactive period	52	40.00	40.00	52
Negative balance	30	80.00	80.00	30
Unusually high withdrawal	10	60.00	60.00	10



Address Details

Suspicious Address

Risk Score: 100/100

Address: a1dcdf3d2c6b1924592c8fc3d2d016ef89

Suspicion Reasons

- Inactive period detected
- Unusually high withdrawal

Address Features

Received: 68.07886867 **In Degree:** 13 **Transaction Count:** 22

Balance: 29.73147113 **Out Degree:** 9 **Centrality:** 0.0215

Related Addresses (Same Cluster)

16f56e3089ca3d402e50cbc468501acb8d

8c0565a6355be7d1257d2783a2b2f4a27a

8ed743dfe06e326cc65dd91807ff1e6377

8cc928888c2e3811099bc5496c2605576b

40c31ee01c39b71524fced4f84d6c96ab5

89e8e0ba5f4ac906744b2e7a5bff15bad4

8. CONCLUSION

8.1 Conclusion

This work introduces a new approach to studying the network of Bitcoin transaction graphs. Here a particular class of Petri nets (BTN) is employed to model Bitcoin transactions. That is, it behaves like a good safe-deposit box. It facilitates understanding of both the stable and the dynamic nature of Bitcoin transaction. To understand where Bitcoins originated from is highly crucial when dealing with the flow of Bitcoin. Through finding particular characteristics we are able to find the correlations between single transactions and find addresses. This is found to be beneficial for forensic case studies of Bitcoin analysis, which evidently indicates that initially we manually define patterns and then we construct a compiler to convert the patterns into executable code. There is a very large data set in the Bitcoin Blockchain, so by maintaining snapshots of intermediate transaction states we can easily minimize the time to analyze even the most recent cases. We'll explore how to protect these intermediate states of BTN.The equipment employed for our experiments is a free (open source) software named Bitcoin Database-creator. Therefore, our experiments cannot be conducted unless the open source software is able to quantify the order of blocks and transactions. We will examine the limitations of the open source software in greater detail in the future.

8.2 Future Enhancements

The suggested analytical framework is the basis for an intelligent and agile blockchain crime investigation platform. However, as cryptocurrencies as well as cybercrime methods are continually evolving, many improvements can be envisioned to enhance the coverage and efficiency of this system. One of the key future directions is to combine real-time blockchain scraping with live transaction surveillance. This would help law enforcement and financial institutions detect suspicious activity in real-time, instead of waiting for it to be detected later. By connecting to large blockchain explorers and cryptocurrency exchanges through APIs, the system would be able to keep monitoring activity and produce alerts. Another thrilling development is the inclusion of support for multiple currencies, in which we can explore

various blockchain networks such as Ethereum, Monero, and Binance Smart Chain. Such networks have distinct challenges to investigate, particularly privacy coins such as Monero. Including support for smart contracts as well as cross-chain bridges on the platform will increase the value of investigations.

9.BIBLOGRAPHY

9.1 References

[1]In 2008, Nakamoto. S published a paper named “Blockchain Based Cryptocurrency Bitcoin Using POW”

[2] Bryans penned a composition," Bitcoin and plutocrat laundering mining for an effective result," in Indiana Law Journal, volume 89, runners 440 to 472, in 2014.

[3] A composition entitled" Silk Road eBay for medicines The journal publishes both invited and unasked letters" by M. J. Barratt appeared in Addiction, volume 107, runner 683, in 2012.

[4] Together with J. Wright and Graham, Dittus penned" Illegal conduct on Platforms The position of the Final Step in the Darknet Market Supply Chain" published in the Proceedings of the World Wide Web Conference, 2018, pp. 277 to 286.

[5] G. White wrote," A UK Company Linked to Billions of Bitcoin Laundering" for the BBC in 2018.

[6] N. J. Ajello published" trying to Force a Forecourt Shape Into a Indirect Opening Bitcoin, plutocrat in Brooklyn Law Review, vol. 80, pp. 434 to 461, in 2015.

[7] The paper" Digital vestiges covering maintaining obscurity in the bitcoin network" was written by P. Reynolds and A. S. M. Irwin and published in the Journal of plutocrat Laundering Control, volume 20, runners 172- 189, in 2017.

[8] F. Reid and M. Harrigan delivered" Examining obscurity within the bitcoin network" at the Proc. IEEE 3rd transnational Conference on sequestration, Security, Risk Trust and the IEEE 3rd International Conference on Social Computing, in 2011, pp. 1318 to 1326.

[9] A Polynomial restatement of Mobile Atmospheres into Safe Petri was authored by S. Göbel. Nets Understanding a math of Hierarchical Protection disciplines. It was published in New York and Berlin, Germany by Springer in 2016.

[10] D. Ron, A. Shamir presented the paper" Quantitative analysis of the full bitcoin sale graph" at the conference International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg2013, runners 6- 24.

[11] M. Fleder, M. S. Kester, and S. Pillai's composition," assaying Bitcoin sale graphs," was published on runners 1 to 8 in 2015, as arXiv1502. 01657

[16] J. Liu and P. Stachowski," A first look into de-anonymizing the Lightning Network," in IEEE European Symposium on Security. 10

[17] C. Miller," Survey of being Bitcoin analytics tools," Journal of Digital examinations, vol. 29, pp. 45 – 55, 2019.

[18] C. Lal, and R. Buya," A check on security and sequestration issues of blockchain technology," IEEE Dispatches checks & Tutorials, vol. 21, no. 4, pp. 3417 – 3452, 2019.

[19] D. Khovratovich, and I. Pustogarov," Deanonymisation of guests in Bitcoin P2P network," in Proceedings of the ACM SIGSAC Conference, 2014, pp. 15 – 29.

[20] M. Alhaidari, and A. A. Ghorbani," Detecting lawless cryptocurrency deals using machine literacy,"

[21] Lüders, and Kauer," A methodical frame for assessing obscurity in cryptocurrency systems," in Financial Cryptography and Data Security, Springer, 2019.

[22] A. J. Kroll and Felten," The economics of Bitcoin sale freights," in Proc. Factory on Economics of Information Security, 2013.

[23] Zyskind and A. Pentland," Decentralizing sequestration Using blockchain to cover particular data," in Proc. IEEE Security and Sequestration Workshops, 2015, pp. 180 – 184.

[24] Lischke, S. and Fabian, B., "Assaying the Bitcoin network: The first four times," Future Internet, vol. 8, no. 1, p. 7, 2016.

[25] Mazut and Wehrle," A quantitative analysis of the impact of arbitrary content on the Bitcoin blockchain," in Proc. IEEE Euros & P Workshops, 2018.

[26] Narayanan and Bonneau, "Bitcoin and Cryptocurrency Technologies," Princeton University Press.

[27] Z. Lin" An address gesture analysis- grounded abnormal sale discovery system," Journal of Network and Computer Applications, Vol. 180, 2021.

[28] Montjoye and Team," openPDS guarding the sequestration of metadata through safe answers," Plops One, vol. 9, no. 7, e98790, 2014.

[29] Böhme, R. and his platoon," Bitcoin Economics, technology, and governance," Journal of Economic Perspectives, vol. 29, no. 2, pp. 213 – 238, 2015.

[30] Böhme and Möser," Anonymous alone? Measuring Bitcoin's alternate-generation obscurity," in Proc. IEEE S&P Workshops, 2017.

10. APPENDICES

Appendices provide what you need to know beyond what is contained directly in the project document. This section contains additional data about software tools utilized, development methodologies employed, and testing techniques adopted in implementing the project. These elements are essential to understanding the technical underpinning and assuring system reliability and functionality.

10.1 Software Used

1. Development in the Backend

Python: Python, the programming language endowed with versatility and widely used, was preferred because of its simplicity and the rich library it offers for web development and integration tasks.

Flask: The backend part of the application was developed using Flask, a lightweight web framework available with Python, effectively handling routing, APIs, and server-side logic.

2. Blockchain Platform

Ethereum: Ethereum is a decentralized blockchain platform that allows operations using smart contracts. This characteristic makes it perfect for adoption owing to its security features and community support, as well as the running of logic by means of smart contracts.

Solidity: Solidity is the language for programming smart contracts on Ethereum. It allows to specify contract logic whereby proofs could be managed in a secure manner over the blockchain.

3. Integration of MetaMask

MetaMask: MetaMask is an online with a browser-based cryptocurrency wallet allowing users to connect with the Ethereum blockchain. This ensures a safe and secure arena for managing digital identities and transacting.

MetaMask Access to the Blockchain: Users can authenticate themselves with MetaMask as a secure method of signing transactions to access the blockchain seamlessly from within the browser.

4. Local Blockchain Development

Ganache: Ganache is a local in-memory blockchain, which is being developed with the idea of testing smart contracts. It provides a personal Ethereum blockchain environment in which you can iterate and debug faster.

Transaction Simulation: Ganache allows the developer to simulate transactions, examine gas fees, and evaluate contract behavior before deployment on the mainnet or testnet.

10.2 Methodologies Used

Agile Development Methodology: The project followed an iterative Agile development approach, allowing for frequent updates, continuous feedback, and improvement throughout the development cycle.

Modular Design: Each component, such as user authentication, evidence upload, and blockchain storage, was developed and tested independently to maintain clean separation of concerns.

Security-First Design: The system was developed with a focus on data integrity, encryption, and access control mechanisms to ensure evidence protection.

10.3 Testing Methods Used

Unit Testing: Individual modules were tested in isolation to ensure correctness. Both black box and white box testing techniques were applied.

Data Flow Testing: Verified the flow and usage of variables to identify improper data handling or logic issues.

Integration Testing: Ensured that all integrated modules worked together correctly, verifying the interaction between the blockchain, frontend, and storage layers.

Big Bang Integration Testing: Used at the final stage to validate the system as a whole after all modules were combined.

User Interface Testing: Evaluated the functionality and usability of the Graphical User Interface (GUI) to ensure a seamless user experience.