International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

Software Solution To Identify The End Receiver Of Cryptocurrency Transaction

Prof.Rita Kadam[1], Aishwarya Kakade[2], Aarati Pawar[3],Badadhe Tanaya[4],Jadhav Vaishnavi[5]

[1]Guide Department Of AIDS
[2345]Students ,Department Of Computer Engineering
Dy Patil School Of Engineering And Technology Ambi, Pune, Maharashtra ,India

---

Abstract - *Blockchain, a distributed record technology, may be used for a variety of purposes. Perhaps the most advanced blockchain applications with unavoidable appropriation among these are decentralized payment systems, like Bitcoin. This thesis offers methods for examining transactions in untested services and cryptocurrencies. Online payments are made safely using cryptocurrencies. Bitcoin, the original cryptocurrency, uses pseudonymous addresses for payments with little assurance of privacy or anonymity.*

Key Words: **1.blockchain, 2.cryptocurrency, 3.smart contract, 4.anonymity, 5.privacy regulation, 4.decentralized 5.conditional anonymous payment.**

1.INTRODUCTION

Money laundering or mixing services are among the most deceptive tools that bury the link between sender and recipient of money in cryptocurrencies: combining different sources of money with dirty money makes tracking dirty money complicated and obscure and distorts the relationship between the sender and receiver of money. As a result, money laundering services are widely used to eliminate the track of income from ransomware, thefts, sales of weapons and drugs, and other illegal activities by combining these incomes with other sources of money and disrupting the tracking of these incomes. Blockchain is a relatively recent trend, especially fueled by the popularity of Bitcoin and its capacity to create a trustworthy ecosystem for conducting business in a setting where information is asymmetrical and identities are unpredictable (for example, because of its decentralized, immutable, verifiable, and programmable features). This serves as an additional degree of privacy for some people, shielding their financial activities from prying eyes. For others, this serves as a veil that hides their illegal activities, such as currency theft or the sale of counterfeit items.

1.1 REVIEW OF LITERATURE

A. An advanced Decentralized Conditional Anonymous Payment System for Cryptocurrency using Blockchain

In contrast to standard e-money schemes, decentralized payment systems rely on a distributed record rather than trusted parties. The Decentralized Anonymous Payment (DAP) structures in the current system are completely unmanageable. Ultimately, these frameworks can be misused for criminal purposes, such as unlawful tax evasion and cybercrime instances (such as paying a ransomwarepayout or engaging in online coercion). can be used for illegal purposes. Anyone can deanonymize without much difficulty. An efficient Decentralized Contingent Anonymous Payment (DCAP) system is used in the proposed work to achieve some degree of balance between security guarantees and guidelines. Certain compounds are allowed to be included in our proposed framework. We also provide a strongconstruction of the DCAP framework (based on the proposed CAPCondition Anonymous Payment scheme) and assess the proposal's ability to meet security standards. In this research, we developed a decentralized restricted anonymous payment (DCAP) system that achieves both obscurity and guideline properties. Our suggested framework is incredibly strong and safe.

B. Mixing detection on Bitcoin transactions using statistical patterns

Financial crimes have expanded dramatically in these services, along with the growing popularity of cryptocurrencies and their use in many situations. Money laundering or money-mixing services are among the most dishonest instruments that conceal the connection between the source and the recipient of cryptocurrency. The relationship between the originator and the recipient of money is distorted when many sources of funding are combined with dirty money, making tracking it difficult and elusive. This characteristic has led to the widespread usage of money laundering services, which combine income from ransomware, theft, the selling of guns and drugs, and other illicit activities with other sources of funding and interfere with the tracking of these incomes.

C. Identity Chain

As a public ledger, blockchain is a decentralized system that is run by a network and is independent of any reliable third party. Blockchain, a cutting-edge technology, has made it possible for a wide range of applications, particularly in the banking industry (usually known as DeFi), including borderless transactions and smart contracts. Blockchain has made it possible for a whole new sector of finance, but its full potential has not yet been realized. Utilizing blockchain's full potential is hindered by a number of obstacles, chief among them being regulatory. Using blockchain and holding users accountable are regulatory concerns in several nations.

D. Sending Money Like Sending E-mails: Cryptoaddresses, The Universal Decentralised Identities

Decentralization is a fundamental prerequisite for a system that maps user-friendly identities to the initial user-unfriendly strings. While decentralized trustless systems frequently lack user-friendly identities, centralized systems typically do. In order to avoid becoming centralized (and possibly a single point of failure) in a decentralized environment, the new system must be able to keep up with the systems for which it offers IDs. This paper presents our cryptoaddress system, which uses the current DNS infrastructure to offer e-mail-like IDs. By assigning a user-selected server to each of their domain names, DNS usage offers simple decentralization at the "domain namespace" level. The resolution of cryptoaddresses to the original cryptographic identities is provided by servers.

Both the DNS and server communication aspects of the system are safeguarded. The system is global and has a wide range of potential uses; therefore, its applicability is not restricted to cryptocurrencies.

E.Investigating transactions in cryptocurrencies

The issues of censorship and centralization in a financial system are lessened by Bitcoin. Just by supplying their public key, anyone can freely build a bitcoin wallet and receive coins. To create such a wallet, no user identification, passport, or verification is required. This gets beyond the conventional financial Know Your Customer (KYC) principles, which form the basis of a set of guidelines that financial institutions employ to identify customers before doing business and, as a result, predict and prevent criminal activity. This independence allows coins to be sent to any address without hindrance or discrimination. Unless the new owner specifically requests it, these coins cannot be exchanged or returned. According to the Bitcoin white paper, the system by default provides pseudonymity for transactions.

1.2 PROBLEM DEFINITION

A new paradigm in digital banking has emerged as a result of the quick rise of cryptocurrencies, offering consumers safe, decentralized, and frequently anonymous means of conducting business. Blockchain technology's pseudonymity has privacy benefits, but it also presents serious problems for regulatory monitoring, fraud prevention, and compliance. The challenge of identifying the final recipient in bitcoin transactions is one of the main issues facing regulators, financial institutions, and law enforcement. The following areas are where this problem is most problematic:

1. Money Laundering and Financial Crime:

Because pseudonymous addresses, mixers, and privacy coins may frequently conceal the eventual recipient, cryptocurrencies are being used more and more in money laundering, tax evasion, and other financial crimes. Finding transaction endpoints is crucial for tracking down illegal cash and prosecuting people engaged in illegal activity.

1. Regulatory Compliance: To adhere to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) norms, numerous nations are enacting laws mandating that bitcoin transactions be traceable. Conducting client due diligence is mandatory for financial institutions and exchanges, but it can be difficult without tools to determine the transaction destination.

2. Fraud and Scam Prevention: Because end-receiver identification is opaque, criminals might take advantage of blockchain systems to create intricate, hard-to-trace hoaxes. In order to evade detection, scams like Ponzi schemes and phishing attacks frequently use anonymous or pseudonymous addresses, which makes it challenging to recover assets or identify the scammers.

2. Privacy-Preserving Technology Challenges:

Additional challenges arise from privacy-focused cryptocurrencies and devices, like tumblers or mixers, which purposefully obscure transaction histories. To solve this problem and understand complicated transactions without jeopardizing the rights of lawful users who respect their privacy, sophisticated solutions are needed

3. Methodology

This section will outline our approach, which includes gathering the necessary information and identifying recurring themes in the mixing transactions in order to develop an algorithm for filtering them.

1. DATA COLLECTION We require access to the complete blockchain transaction data and labels for transactions that took part in mixing services procedures in order to look into mixing transactions.

1.1) Extracting Blockchain Information Using a full-node Bitcoin client, we gathered the necessary data from the blockchain using its JSON-RPC APIs in order to access transaction data. Information about blocks and transactions, including block hashes, transaction input and output addresses, transferred values, timestamps, and other necessary information included in the blockchain, can be obtained after executing the Bitcoin client in accordance with its established RPC capabilities. 1..2) Gathering Labels for Transaction Mixing People use mixing services for a variety of reasons, such as hiding their financial activities to avoid taxes, commit crimes, or protect their privacy. It is evident that people are hesitant to reveal their mixing transactions, regardless of their motivations, and as anticipated, there is no dataset of exchanges pertaining to service mixing. Even though there are certain labels available for money laundering service addresses, heuristics and clustering techniques that label other addresses based on the previously labeled addresses may cause inaccuracies. Ordinary addresses could be linked to money laundering services throughout this procedure, making it misleading to examine their transactions. We had to gather precise data on our own since there was no predefined dataset.

Three of the most popular mixing services that were mostly discussed on Reddit2 and BitcoinTalk1 were chosen in order to compile a dataset of mixing transactions. By using their service, putting funds to the designated address, and then transferring funds from them to our target address via the money laundering procedure, every time we used these services, we conducted two mixed transactions: one for the deposit and one for the withdrawal. These three chosen mixing services are listed in Table along with the quantity of mixing transactions we produced for each.

2. STATISTICAL PATTERN EXTRACTION We had to use straightforward statistical techniques that work well with small data in order to extract the mixing pattern because gathering a rich dataset of mixing transactions was both expensive and time-consuming. First, we briefly go over the mechanisms that various mixing providers employ. Two primary categories of mixing services are described. • Conventional mixing services: In classic mixing services, the service decides how much money from desired transactions can be combined with a predetermined quantity of money. These services facilitate the transfer of funds between senders and recipients at random. The service generates a fresh random deposit address for the sender in the first stage. The address is updated every time the user reloads the page containing the mixing request. A sender must then wait until at least N − 1 other mixing requests with the same amount have been recorded before depositing their funds into the address they have created. In order to remove the trace of the money transfer between the sender and the recipient, the mixing service in this stage, also known as the intermediate stage, generates transactions in which these N inputs are switched at random and sent to N anonymous output addresses. The anonymity set is set to a probability of 1/N by this action. This displays the likelihood of discovering the right connection between a sender and their matching recipient. The operation of these services is depicted in Figure 1. • Contemporary mixing services: These services have three stages, just as conventional services. The requested funds are first transferred to a randomly generated deposit address by the mixing service.

3. TRANSACTION-LEVEL PATTERNS IN THE FIRST PHASE OF DETECTION We discovered recurrent tendencies when we looked into the mixing transactions we made. Withdrawal transactions showed these trends. Since the format of the deposit transactions was standard across the whole blockchain and the senders made them by using their wallet application to deposit money to the mixing service, we were unable to identify any patterns in the deposit transactions at the transaction level.

Table -1: Key Solutions

Software/Tool	Key Feature	Use Case	Example
Chainalysis KYT	Real-time transctionmonitoringriskscoring	Detect Suspicious and esure AML compilance	Identify illict wallet addresses and tracing
TRM Labs	Blockchain intelligence AI powerd analytics	Investigate fraud, trace funds, and build compliance cases	Investigate fraud, trace funds, and build compliance cases
Scorechain	Multi-blockchain support, sanctions screening, real-time monitoring	Risk scoring and regulatory reporting	Risk scoring and regulatory reporting
Elliptic (Explore)	Tracing funds across over 100 crypto assets with configurable risk rules Source/destination tracing for financial	Source/destination tracing for financial institutions	Monitoring wallet behavior to prevent fraud.

The search results reveal a number of software applications designed to monitor cryptocurrency transactions and determine the ultimate receivers. These tools use wallet address tracking, blockchain analysis, and forensic techniques to track the flow of money, particularly in cases like drug trafficking. GitHub repositories, industry reports, and research articles are some of the resources that discuss the methods and technology used in this subject. The following is a summary of the findings:

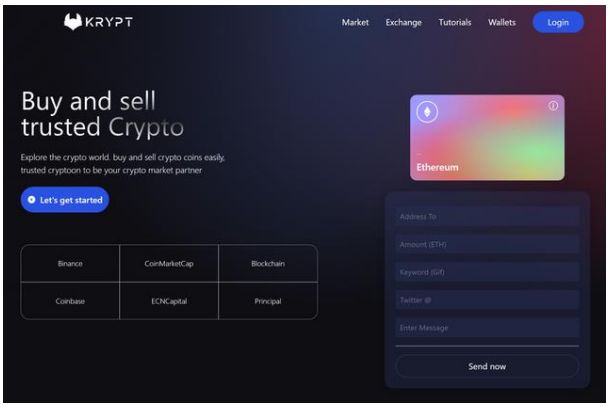

Fig -1: **Login Page**

One of the most dishonest methods that conceals the connection between the source and the recipient of funds is money laundering or money mixing services. The picture displays a program named "Krypt" that is intended to identify the final cryptocurrency recipient. It positions itself as a crypto market partner by making it simple for customers to buy and sell reliable cryptocurrency. Numerous sources, including Binance, CoinMarketCap, Blockchain, Corbne, ECNCapital, and Principal, are supported by the platform. With a "Send now" option, it allows users to send bitcoin by entering the recipient's address, quantity (ETH), keyword, Twitter account, and message.

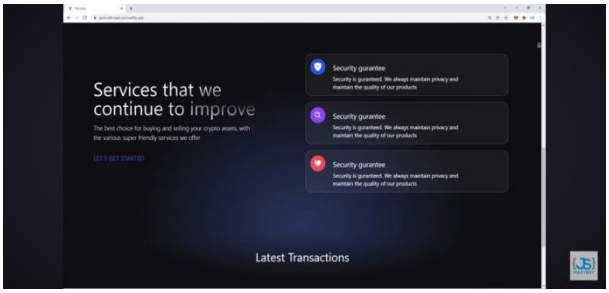

Fig -2:Services

The picture displays a program named "Krypt" that is intended to identify the final cryptocurrency recipient. It positions itself as a crypto market partner by making it simple for customers to buy and sell reliable cryptocurrency. Numerous sources, including Binance, CoinMarketCap, Blockchain, Corbne, ECNCapital, and Principal, are supported by the platform. With a "Send now" option, it allows users to send bitcoin by entering the recipient's address, quantity (ETH), keyword, Twitter account, and message.

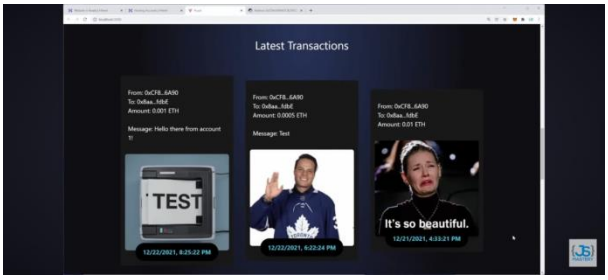

Fig -3 :Latest Transactions

The screen capture shows a log of "Latest Transactions," which appears to be related to cryptocurrencies or blockchains because ETH (Ether) and hexadecimal wallet addresses are mentioned. The address of the sender (From), the address of the recipient (To), the amount of ETH transferred, a message, and the transaction date and timestamp are all included in every transaction. 0.001 ETH was transferred on December 22, 2021, at 6:25:22 PM, with the message "Hello there from account T!" This is the first transaction. On the same day, at 6:22:24 PM, the second logs a 0.0005 ETH transfer with the message Test. The third transaction shows that on December 21, 2021, at 4:33:21 PM, 0.01 ETH was transferred with comment

4. CONCLUSIONS

The proposed work has effectively achieved anonymity and regulation properties in our decentralized conditional anonymous payment (DCAP) system. Before constructing our DCAP, we developed a conditional anonymous payment (CAP) method using the formal semantic and security models. It will also show its security inside the designated security model and provide a concrete CAP design based on our proposed knowledge scheme signature. Building on the proposed CAP, we created our DCAP and demonstrated how it might satisfy the related security requirements. Our prototype's performance will next be evaluated by comparing it to Zero Cash's under the same testing conditions. The results indicated that our plan could be implemented in the real world.We proposed a technique for detecting mixing transactions based on the statistical patterns we saw in the mixing process. Due to the lack of reliable labeled data, we constructed mixing transactions using three widely used mixing services: MixTum, Blender, and CryptoMixer. By looking at these transactions, we were able to identify recurring trends at both the transaction and chain levels. By examining each transaction in the blockchain, comparing it with the patterns we discovered, and identifying mixing transactions, we were able to differentiate between addresses connected to mixing services and addresses connected to the users of mixing services. Our approach is 100% accurate.

REFERENCES

[1] ArdeshirShojaeenasab,Amir Pasha Motamed., BehnamBahrak, “Mixing detection on Bitcoin transactions using statistical patterns,” © 2022

[2] Chavi Kapoor., VeeravalliShivadeepak ,Konthamvinaykumarreddy “An advanced Decentralized Conditional Anonymous Payment System for Cryptocurrency using Blockchain” © 2021

[3] Mahdi Darabi,AmirrezaFathi,"IdentityChain" © 2022

[4] HaaroonMYousaf,"Investigating transactions in cryptocurrencies" © 2022

[5] R. Muthumeenakshi, Balasubramaniam S., Charanjeet Singh, Pallavi V. Sapkale, "An Efficient and Secure Authentication Approach in VANET Using Location and Signature-Based Services", Ad Hoc & Sensor Wireless Networks 53 (Issue 1-2), 59-83, 2022

[6] Uttam D. Kolekar, "Development of Optimized and Secure Routing Algorithm using AODV, ACO and LSB Steganography for Mobile Ad-Hoc Network", Journal of Advanced Research in Dynamical and Control Systems (JARDCS),Vol. 11, issue 9, pp. 560-568, Sept 2019.

[7] Sandeep B Hake, "Design and development of universal test bench for engine aftertreatment controls system", International journal of advanced research in electronics and communication engineering, Volume 6, Issue 4, Pages 309-312, 2017.

[8] Samarjeet Powalkar, "Fast face recognition based on wavelet transform on pca" International Journal of Scientific Research in Science, Engineering & Technology, Vol 1, Issue 4, PP 21-24, 2015.

[9] U Waghmode, DP Deshmukh, S Ekshinge, A Kurund, "An Innovative Approach Using Cyber Security for Steganography for Wireless Adhoc Mobile Network Application"International Conference on Science Technology Engineering and Management (ICSTEM), Pages 1-5, 2024.

[10] C Kaur, DS Rao, S Bandhekar, "Enhanced Land Use and Land Cover Classification Through Human Group-based ParticleSwarm Optimization-Ant Colony Optimization Integration with Convolutional Neural Networ", International Journal of AdvancedComputer Science & Applications, Vol 14, Issue 11, 2023.

[11] Divya Rohatgi, Veera Ankalu Vuyyuru, KVSS Ramakrishna, Yousef A Baker El-Ebiary, V Antony Asir Daniel, "Feline Wolf Net: A Hybrid Lion-Grey Wolf Optimization Deep LearningModel for Ovarian Cancer Detection", International Journal of Advanced Computer Science and Applications, Vol 14, Issue 9, 2023.

[12] Uttam D. Kolekar, "Trust-Based Secure Routing in Mobile Ad Hoc Network Using Hybrid Optimization Algorithm", The Computer Journal, Oxford University Press, Vol. 62, issue 10, pp. 1528-1545, Oct 2019.

[13] Uttam D. Kolekar, "E-TDGO: An Encrypted Trust based dolphin glowworm optimization for secure routing in mobile ad-hoc network", International Journal of Communication Systems, Wiley publication, Vol. 33, issue 7, May 2020.

[14] Dilip P Deshmukh, Abhijeet Kadam, "Efficient Development of Gesture Language Translation System using CNN"15th International Conference on Computing Communication and Networking Technologies (ICCCNT) Pages 1-6, 2024.

[15] Prajwal Kote, Mounesha Zonde, Om Jadhav, Vaibhav Bhasme, Nitin A Dawande "Advanced and Secure Data Sharing Scheme with Blockchain and IPFS: A Brief Review"15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Pages 1-5, 2024.

[16] Prasant, P., Saravanan, D., Sangeethapriya, J., "NR layer 2 and layer 3" Machine Learning for Mobile Communications, Taylor & Francis, CRC Press, pp. 32–45, 2024.

[17] Borana, G.K., Vishwakarma, N.H., Tamboli, S.,M., Dawande, N.A., "Defending the Digital World: A Comprehensive Guide Against SQL Injection Threats" 2nd International Conference on Inventive Computing and Informatics, ICICI, pp. 707–714, 2024.

[18] Deshmukh, D.P. et.al, "An Innovative Approach Using Cyber Security for Steganography for Wireless AdhocMobile Network Application" International Conference on Science, Technology, Engineering and Management, 2024