ISSN 2348 - 9928
IJAICT Volume 7, Issue 10, October 2020 Doi:10.46532/ijaict-2020031 Published on 05 (10) 2020

Digital cash system of Invisibility of user Identity and Concealment

[1]Meghan Bani Assad
[1]Vancouver Campus, The University of British Columbia, Vancouver, BC Canada.
[1]meghanabani@hotmail.com

ArticleInfo
International Journal of Advanced Information and Communication Technology
(https://www.ijaict.com/journals/ijaict/ijaict_home.html)
https://doi.org/10.46532/ijaict-2020031
Received 02 May 2020; Revised form 28 July 2020; Accepted 18 September 2020; Available online 05 October 2020.

Abstract — Bitcoin can be considered as one of the most prevailed applications of Blockchain technology developed so far. It is the most eminent, decentralized and distributed network-based platform. Without using real names, it provides a pseudo name interface through which management and verification of transactions are performed by the user being anonymous. Blockchain which itself works as a virtual ledger consists of data in the form of various blocks connected in a chain. Although it is providing the Invisibility of user Identity but extracting and combining the data and profile from the Blockchain, the identity can be revealed. Thus, in contrast to that, many researchers and data scientists have suggested the amendments and proposals to enhance the Invisibility of user Identity and Concealment of Bitcoin customer. We project out some theories, project analyses and methodologies that certainly supports the concern of the improvement of Bitcoin Customer anonymity.

Keywords – User Identity and Concealment; Bitcoin; Blockchain; Cryptocurrency; Peer-to-peer Networking.

1 Introduction

Safe and Secure transfer of money has always remained a topic of big concern for society. With the advancement in Internet and technologies, most people have shifted from offline to online money transactions. Being an active part of the internet, banks also have implemented the latest technologies enhancing the criteria's such as speed, accuracy, and efficiency. Also, the world is connecting each other through globalization, liberalization, and commercialization.

A system based on electronic payment which does not involve trust can be further explained using the methods of cryptography. A decentralized platform where no one is the main authority forming rules and regulations. All the nodes or peers are having the same level due to which it is called peer-to-peer networking. These use the concepts of virtual and digital assets which when merged with cryptography for serving the purpose of verification forms the 'Cryptocurrency [1]'.

Bitcoin [2] was the term coined in the year 2008 by an anonymous individual or a group of people named 'Satoshi Nakamoto [3]'. It was launched as an open-source application where the value i.e. Bitcoin generated through the process of Mining [4]. Mining [4] is nothing but the procedure of maintaining the records of transactions. An individual need to create a setup of the computer where the record of the various transactions is added and payments are verified. For this process, the bitcoins will be rewarded to all users depending on their particular statistics.

Individuals are not supposed to enter their true names to use Bitcoin [2]. In place of that, pseudonyms are taken into use. This is done to let the real identity remain hidden. As all the contracts and transactions are publicly visible, every single event can easily be traced and connected. The customer and user details can thus easily be retrieved. This confirms that Bitcoin users cannot simply remain anonymous. This is one of the breakthroughs in Blockchain technology.

2 Layout

Invisibility of user Identity and Concealment

The invisibility of user Identity simply means the condition of being anonymous or when the true identity of the owner is hidden. The protection of personal data is a must for usage to be proper. Concealment plays the most important role when comes to online systems and applications. On the contrary, it can be a vital key feature that the criminals seek. With the presence of anonymity, pointing someone responsible for any action is not feasible. Most Popular example can be of the voting in free-held elections where the secret ballot box is used. To guarantee the perfect Invisibility of user Identity is not easy. Most of the applications and software's that seemed to be claiming anonymous were proved wrong since they had many flaws which leaked the personal information of its users.

To enhance the scope of this property, systems require more and more resources including time complexity and computing power, since the extra work needs to be done.

Even the users of the Blockchain need to purchase this additional feature to avail their Concealment.

Bitcoin

Bitcoin is a distributed digital currency (P2P) in which there is no rules and regulations forming main authority. BTC also known as the abbreviated form of bitcoin is the smallest unit of bitcoin currency. (0.00000001 BTC = 100 millionth of 1 bitcoin). Its basic unit is called Satoshi. It is also possible to convert bitcoin to another address from one single address. A transaction is considered as the transfer of Satoshis. Thus, the transactions of bitcoin take place collectively through peer to peer networks.

Blockchain

A distributed, decentralized open ledger that is publicly accessible by all of its users, consists of the record of all the transactions and the data that has been shared between each and every single node. Basically, a blockchain consists of a chain of blocks connected to each other through peer to peer networking. One part of it consists of the transactions that are in the waiting process for the block to be added in that chain. Those particular transaction needs to be verified and confirmed by the others in order to make it a part of the chain. On its verification the network adds that block to the blockchain. Each block consists of 3 sections where first part consists of the hash key in the form of merkle root of that particular block, second part consists of the data and the third part has the hash key of the previous block. In this way each and every block gets connected in the blockchain. The fundamental Blockchain structure is shown in the Fig.1.

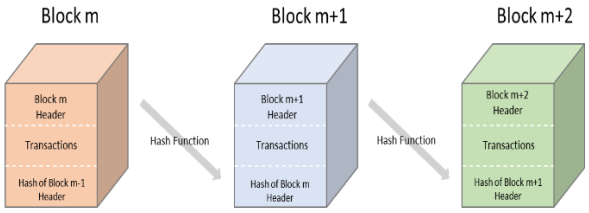

Fig 1. A simple model demonstrating the technology of Blockchain

Transactions

In the process of exchange of data between two blocks, here in case of Bitcoin. Basically, every transaction consists of an input and an output which includes its particular data about the transacted amount. This flow leads to a chain arrangement of transactions.

Output which is present as unspent by the input, remains as "not spent transaction output". For example, if a user has 10 bitcoins, it means that 10 Bitcoins or not spent transaction outputs are assigned to him. The difference between the total output and the addition of all those inputs in a transaction is the transaction charge. The user who created that new block (or the miner), shall bear transaction charges on all the transactions. This chain structure is illustrated by an example in Fig.2.

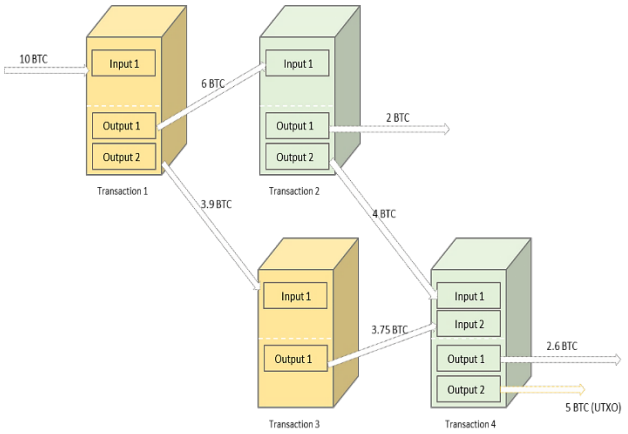

Fig 2. A Specimen of bitcoin transactions flow

The conditions on which the coin transfer depends, are carried out in output of that particular transaction to the input of another one. It is framed in a basic Non-Turing-complete scripting language, through a script. The input transaction n+1 receives the output transaction n. Further, for that amount, the one satisfying the terms and conditions of pub-key script becomes it's owner. The process is shown in Fig.3.

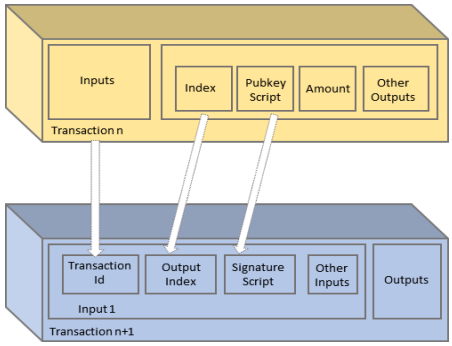

Fig 3. Transactions showing Output and Input segments

Incentives and Mining

The reward for generating block comes into the picture when a new, special transaction is put into the block by its creator who is the one that pays for all the transactions related to that block. Here Coinbase transaction is the term given to this first initial transaction. Thus, the new block is added to the latest copy of Blockchain and passed on to several nodes. This procedure is called as Mining [4] process since every block has a reward. Bitcoin mining is the process by which transaction records are added to the previous Bitcoin public leader or blockchain. transactions. New bitcoins will be released and assigned to the block designer in each block generation.

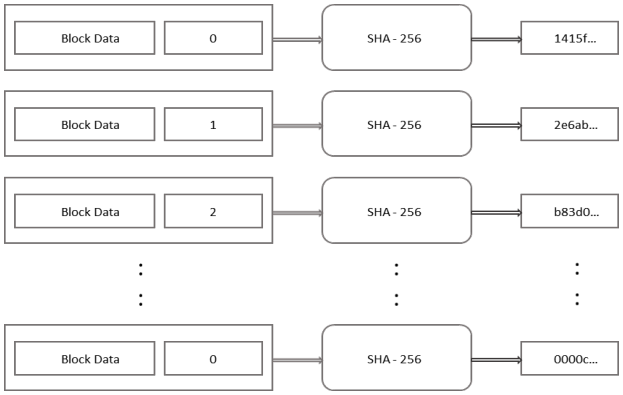

Fig 1. An example of an Hashcash

PoW [Proof of work]:

The prevention of Denial of Service [7] attacks and other such misuses of the system is considered as Proof of Work. A user has to show if he has performed any work or spent any effort. Although this proof can easily be verified. Hashcash algorithm is used for this Proof of work in Bitcoin. The value of hash needs to start with a certain number of zeroes., but is needed to reveal the time and efforts spent by the user. Since it cannot be received directly Hashcash algorithm is used over here. An example is given for the Hashcash implementation in the figure. In it, the addition of nonce value at the end serves the purpose. It is incremental starting from zero. It usually takes 1,405 tries to obtain a legit value for hash.

Difficulty target is the term used for the quantity of zero bits that determine the proof-of-work. The generation rate of blocks gets affected due to the improvement in rapid changes in the number of running nodes over the network and also due to the change in speed of the hardware.

Double-Spending:

The double-spending problem is the most prominent problem that arises in the cases of cryptocurrencies, where the malicious user can try to spend the same amount of money or same money to two different payees. It must be surely confirmed that any crypto-coin is not used more than once by its owner. Here in the case of bitcoin, the Blockchain formulates one unique verification source, further the next transaction is not added to blockchain by the network. Through the nodes following the rules of consensus, it can be accomplished. As the blocks get verified through these validation rules, any block that does not follows them is directly removed.

P2P Network:

Within the same level of the hierarchy, the nodes get connected from one another through the encrypted channel of TCP [Transmission Control Protocol]. For peer to enter in the network, DNS seed that is nothing but the DNS servers are queried.

Thus, to find the active peers, those DNA seeds are hardcoded in Bitcoin clients. The response is inclusive of the block, current time, the version number of the sender peer.

The transaction always propagates among two peers only if that transaction is a legit one. A Reputational protocol allows each and every peer to keep every connection's penalty score for each of their faulty messages. On reaching the threshold, Peer connection gets banned for 24 hours.

Summary of the Process:

The whole process can be summarized through following statements. New Transactions get broadcasted to all nodes. Each block collects new transactions through the help of minor nodes. Each Minor also carries out the task of searching proof-of-work. On finding POW i.e., Proof-of-work, Blockchain with the added block is broadcasted. In case of the invalid transactions, minor nodes get rejected.

Through the accepted block's hash, as that is the hash of the previous block, further blocks are created through minor nodes as a result of showing their acceptance. The extension of chain continues and chain keeps on getting longer. When two minor nodes broadcast distinct versions of Blockchain at the same time with a new addition of block, miners only work on the initial one they receive but there's also the possibility of it becoming longer.

3.Invisibility of User Identity And Concealment In Bitcoin

In the world of traditional banking, the details and information about the parties involved in the transaction need to be limitedly shared and secured by the trusted third parties. Here, in the today's world where banks follow traditional method, it becomes a collective responsibility of the third parties to ensure the safety, privacy and security of all the data regarding the transaction between different parties. Where the bitcoin is concerned, all the things are almost transparent, all the transactions are candidly announced. Each one of the users transfers bitcoins to each other but their true identity remains hidden. Instead, the pseudonyms are prevalently used. Thus, it can be said that Bitcoin provides anonymity. Moreover, being anonymous it is also made clear that Bitcoin is the only platform that keeps each and every record transparent. If someone wants to check balances, it can be obtained by tracking and managing the records of all those particular transactions related to their respective users.

It can also be stated that during the bitcoin usage, the nature of any user describes the level of Invisibility of the user's Identity. Bitcoin itself provides a few suggestions in order to enhance the Concealment of the user's identity. For every single transaction, a new key pair has to be developed. It is due to the reason that when the new key pair gets generated, previous transactions cannot be merged to it. This prevents the information about the bitcoin quantity from getting leaked. Next suggestion is to use wallets for specific purposes. Wallet relates to the

Corresponding author at: Meghan Bani Assad, The University of British Columbia, Vancouver, BC Canada.

files or programs used for creating and maintaining Bitcoin addresses, managing transactions, and public-private key pairs. Through this, the transactions at different wallets can remain isolated without getting disclosed.

For all the users that use wallets, their location during the transaction and address are always tracked by the Hosted wallet services. Additional details like mail identity, contact number and other such data give them the ease of access to merge that data with the user's identity. Sometimes the hosted wallet service providers try to obtain the Bitcoin address through their IP address and track it through them, linking them to their respective transactions. Further using the relays, IP address can be revealed. For prevention of this, Bitcoin provides a feature for its users i.e., TOR [The-Onion-Router]. Also, many services are there which basically mix up the transactions of sending and receiving relays which makes impossible to detect any of them. The idea of Bitcoin was based on the Blockchain technology which is meant to be public, although it doesn't provide Concealment. However, technology can be a lot more useful for serving various purposes in various sectors.

Here We'll go with some of the crucial Concealment studies related to Blockchain. Enigma [8] which is a P2P network where several factions merge their information's altogether. Current researches on smart contract based blockchain platform "Ethereum" shows that it also has its transactions as public and distributed just as in the case of bitcoin. It even configures private and permission Blockchains to improve its Invisibility of user Identity and Concealment. Concealment is also obtained in another smart contract platform, Hyperledger fabric through the use of hash functions and symmetric encryptions.

5.

6. 4. Classification of studies on Invisibility of user Identity and Concealment analysis in bitcoin

Here, we have classified the various methods of analyzing Concealment and Invisibility of user Identity in Bitcoin that are explained. Importantly, the analysis of Invisibility of user Identity and Concealment is done through deanonymization and extraction of information that can impair Concealment of Bitcoin users. The outcomes of the studies mentioned are given in the below part of the figure. Methods are also explained in brief in the initial sections. Further section examines these studies based on other characteristics and properties determined to test these studies.

Outcomes

These are basically the potential targets to be achieved post analysis. Here are five outcomes analyzing Invisibility of user Identity and Concealment in bitcoin shown in table 1.

Table 1. Outcome analysis for the invisibility of user identity and concealment

S. No	Analysis	Possibly discovered Outcome
1	Bitcoin Addresses	Of any person or any entity starting from identity information
2	Identities	Received through Bitcoin addresses.
3	IP to Bitcoin address mapping.	All over the chain where the transactions are formulated, the mapping takes place.
4	Bitcoin addresses connection	This output combines all the addresses that are possibly expected to belong to an identified user.
5	Geo-Locations getting mapped to Bitcoin addresses	As Bitcoin address is linked to IP address, through IP address the geolocation address can be traced.

Methods

All the methods are elaborated in the details and related researches are given below for each particular method.

Transacting:

For the transaction to take place between two nodes, the things that are required are the bitcoin and the IP addresses of the sender block and the receiver block. The purchasing client needs to know the IP and Bitcoin address of the selling client to make the payment. Here what happens is the buyer comes to know the Bitcoin address of the seller. This process includes coin marking or running a money laundry facility. All these can be considered as money laundering tools in the researches.

Using Out-of-Network Details:

Out-of-network sources of data that are publicly available and which are obtained externally can discover IDs from Bitcoin addresses or vice versa. Bitcoin data sources are available for the distributor. F. Reid and M. Harrigan [9] have used websites for public donations that publish, together with the IPs and key information, such as the Bitcoin faucet and the voluntary public keys. By using non-network information, they identified certain entities associated with an alleged theft of BTC 25,000. This led to the next method which utilized the network details.

Utilizing Network:

Pure Analysis of network traffic in bitcoin helps in obtaining information about the transactions. The analytical methods that use the Bitcoin Network are the

Corresponding author at: Meghan Bani Assad, The University of British Columbia, Vancouver, BC Canada.

abnormally relayed transactions, the use of entry nodes, the use of the first relator information and the user fingerprint address cookie. Using these the expected threats related to identity concealment were detected, which got corrected through the upcoming methods.

Utilizing anonymously relayed transactions:

The relay can be called by sending a message to others by a peer. By analyzing Bitcoin network traffic and monthly relay transactions, abnormal relay patterns, such as one person's relays or the relay of a transaction by at least one user can be defined. Mapping of Bitcoin addresses to IP addresses may involve transactions matching these patterns. These were basically motivated by Kaminsky's [10] idea to use the P2P information network in his research, he proposed the initial method to match Bitcoin addresses and IP addresses. He created a Bitcoin client named CoinSeer to collect details. Using it, an outward-bounded link got established for every listener with an IP address.

Using the first transmitted information:

At the time of linking nodes in bitcoin, the source node becomes the first to declare the transaction that is the holder of the transaction is supposed to be the source. First of all, Kaminsky [10], who proposed the use of first transmitted information, introduced a P2P network and relays as a further data source for deanonymization. His development included the development of a tool to de-anonymize a transaction end. Their focus was to examine the impact on the grouping of Bitcoin addresses of network information. Further, the findings showed that for a large number of users, network data does not allow the grouping of addresses.

3.2.3.3 Using the underlying network plot:

By using the underlying P2P network plot, users of bitcoin can be easily tracked. The method of using entry nodes has been introduced. Bitcoin applicant has the entry nodes connected to it. Data is gathered for a node which gets connected to the network so that the sources (especially owners) of transactions can be identified and mapped to match the IP addresses to Bitcoin addresses. The first method is to find client input nodes, then listen to servers and map transactions, then the users. This method can connect Bitcoin addresses that are not limited to anomaly relayed transactions. This prevents Bitcoin servers from accepting connections via TOR and other Invisibility of user Identity facilities. Although this threat is mostly observable, another such method was implemented.

Configuring cookie for the address:

Address cookie configuration over the system or device of the user can lead to the linking of different transactions where IP and bitcoin addresses can be combined. Through the configuration of address cookie, the system of the user can be fingerprinted. This method does not require examination or verification of Blockchain and is based on the P2P detection Bitcoin process.

Analysing Blockchain Data:

Since the whole transaction's past record is visible publicly in the public ledger, Bitcoin flows are traceable between Bitcoin addresses. Blockchain data can be collected using Bitcoin Client APIs. Blockchain's Invisibility of user Identity and Concealment for Bitcoin was first analyzed by F. Reid and M. Harrigan [9]. They established dual network structures and user networks that are extensively used in the following research. In the transaction system of bitcoin, the client network shows the bitcoin flow among transactions. Transactions are represented as nodes and Bitcoin flows as pointed edges, with quantity. A root node output is entered into a destination node.

Users are represented in the user network as block points, while pointed fringes, which also have information on amounts along with timestamps, represent Bitcoin flow between them. A root node is a drawee, while the destination point node is a payee. The Blockchain user network cannot be directly derived; additional work is required. At first, each address with the node as shown in the figure can be shown. In this figure, the addresses of each square are Bitcoin and Bitcoin are transferred between addresses.

The numbers given in the studies are given for all the metrics in Table 2.

Table 2. Metrics For Concealment In Bitcoin

Study	No. of blocks		No. of transactions	No. of unique bitcoin addresses	Grouping of bitcoin addresses with multi-input and input heuristics
[9]	-135,700		1,019,356	1,235,154	1,253,034 addresses to 881,474 users
[12]	140,100		-1,185,451	1,366,488	1,632,548 addresses to 1,059,599 users
[11]	180,100		-3,142,685	3,720,118	3,230,318 addresses to 2,360,614 users
[18]	215,299		-10,698,631	-12,611,255	Not Specified

Using transactions with many-inputs:

Through the many-input transactions, various addresses can be connected to one user. A many-inputs transaction

occurs when the user makes a payment by linking these addresses within the transaction using more than one address. This may occur, for instance, when the amount of payment in the addresses of the user is greater than each balance. This fact is also stated by Nakamoto [3], which shows that multi-input transactions are possessed by the same user itself, and when the holder of one of these inputs is revealed, then the other transactions are possessed by the same client with other entered addresses. The real Bitcoin system was first analyzed by Androulaki et al [12]. Then he used a prototype clone to simulate the usage of bitcoin as the main currency in a university in order to provide basic information on the truth. They introduced non-linkability and non-differential profiles as concepts of Concealment for Bitcoin and defined the metrics to be used for quantification. It is stated that a user of Bitcoin can remain pseudonymous only without outside information. In order to maximize Invisibility of user Identity and non-linkability of the transactions, it is recommended to (I) have only one address and (ii) be active for a short time with this address. The Invisibility of user Identity set increases with a single address. Address restricts the connectivity of transactions for less time.

In a sample transaction, Kaminsky [10] demonstrated his acceptance of this heuristic. He stated that all transaction entered addresses are possessed by the same client. The examples provided for Bitcoin Address Identification in the transaction graph also demonstrated the approval of this procedure. He stated that Bitcoin addresses cited as entries within the concordant transaction could be taken as proof that they are possessed definitely by the same user.

He also indicated that the transaction input addresses of the same user pertain to a non-mixing transaction, however, their purpose is to search for the mixed transactions. Mixing was normalized with graph notation in order to regulate four types of transactions in a mixing process according to their relation. About ten billion transactions in bitcoin have been classified correspondingly, and mixing transactions have been discovered as quite frequently occurring with mixed transactions accounting for approximately 3.75 percent of all the transactions taking place in bitcoin.

Using the altered addresses:

The altered address is nothing but the address of the bitcoin that allow users for making changes. If there exist two outcomes of any possible transactions and one of them has a previous address and the next one has a new address. then the new address can be supposed to be changed and possessed by the client having the input address. Blockchain transactions can be analyzed in order to find changes that will be provided by the users who entered the transactions and linked to them.

It was stated that for the transactions generated through a user's application along with its source code, its outcomes and the change can be discovered. Further, that change address can be linked through the client with whom the transaction was generated. In their experiments, however, they used only multi-input transactions.

Kaminsky [10] gave a sample transaction and indicated that one of the outputs was probably owned by the client who possessed the transaction's entered addresses. They showed the approval of this procedure with the help of examples. It also stated that any transaction generally has dual outcomes, one is the real output and the other one is the change. It indicates that one of these outputs is from the same client that possesses the transaction's entered addresses. It is also said that probably the most crucial change is the small output.

These procedures are used to reveal the details in combination.

Other Characteristic Properties

Bitcoin Constructed User:

This feature used a bitcoin constructed user. Basically, the feature proved to be legit for studies pertaining to the network where the customer can be altered according to the desired requirements. The result of this research is the mapping of IP address and bitcoin address.

Utilizing Observation Directed Data:

The data that is directly fetched from the observations during any experiment is considered as Observation directed data. Researches that provided analysis of the data regarding blockchain differentiated the blockchain transactional information with observation directed. For this research, the outcomes link the address of the bitcoin along with bitcoin address to geo-location mapping. Since Bitcoin addresses belonging to the same user and geo-locations related to Bitcoin addresses are the basic data of the studies. Studies analyzing the P2P network compared data on ground truth with information obtained from the network. The result of these studies is to map Bitcoin addresses to IP addresses.

Shamir tried to merge the addresses of a specific large user using all the transactions available and then compared their findings with ground truth data. They found that about a quarter of his real addresses could be identified.

Benchmark to Scale the level of Concealment:

The benchmarks that have been provided to measure the level of Concealment are provided in Bitcoin. Research analysis of blockchain data for connecting Bitcoin addresses using the Peer-to-Peer network gives metrics for mapping the two addresses. The outcomes of these researches link the two addresses to each other.

Androulaki et al [12] established Bitcoin Concealment conceptions: unlinkability of tasks and indistinguishability of account. It even gave the measurements to scale these concepts. For the dissociation of the activity, it aimed at the dissociation of addresses, that they cannot link two different Bitcoin addresses. Profile indistinguishability means that all users cannot reconstruct profiles.

Corresponding author at: Meghan Bani Assad, The University of British Columbia, Vancouver, BC Canada.

Other such features and properties for the researches that analyze invisibility of user identity and concealment in Bitcoin are given below in Table 3.

Table 3. Features Analysing Invisibility Of User Identity And Concealment

Property	[9]	[12]	[11]	[13]
Bitcoin client build	X	X	X	X
Use of ground truth data	X	✓	✓	X
Gives metrics to quantify concealment	X	✓	X	✓
Implantation of concealment enhancement	✓	✓	X	X
Real Deanonymization	✓	X	✓	X
Flow analysis performance	✓	X	✓	X
Theft case investigation	✓	X	X	X
Cost Information	X	X	X	X
Analysis of network metrics	✓	X	X	X
Investigates inactive addresses	X	X	✓	✓

Fulfilment of Real De-anonymization:

In this research, Out-of-network data-driven methods along with the transactions are used for serving the purpose of de-anonymization. Related results are the revelations of Bitcoin addresses and identities.

Biryukov et al. [13] said that for ethical reasons, they carried out a deanonymization attack on real customers. Many papers, on the other hand, provided examples of deanonymization. F. Reid and M. Harrigan [9] identified the main account of the Slush pool and the LulzSec computer hacker group using off-network data. It showed that Silk Road really belonged to an alleged address belonging to the Silk Road. Ron and Shamir [11] identified Mt 's addresses. Gox, Bitcoin Exchange's most popular site and Deepbit, Bitcoin's largest Mining [4] pool.

Accomplish flow examination:

In the flow examination, the analysis of user's Bitcoin influxes and outfluxes within a certain period of transactions carried out by blockchain data analysis. In this kind of analysis, transactions and user networks are used. This property is insignificant to taxonomical results. F. Reid and M. Harrigan [9] have implemented a tool to keep track of the bitcoin flow among clients. They noticed the flow post thievery. They stressed the effect on flow analysis of the use of changing addresses. Address flow supposedly possessed by them were documented. They traced flows through the mixing services they analyzed for the transactions they had made.

Inspection of a theft crisis:

The inquiry of a known thievery crisis involves the analysis of Blockchain data and the use of out-of-network data. This feature uses an analytical approach for flows and does not affect the results of the classification.

F. Reid and sM. Harrigan [9] examined a professed 26,000 BTC robbery reported by a user in vain in the Bitcoin Forums. This number of bitcoins had a market value of about half a million United States dollars at the time of the theft. At the time of the thievery, the amount of bitcoin value was equivalent to the bitcoin market value of approximately 0.5 million US dollars.

Delivers cost report:

The charge of attacking is in forms of currency, repository or time-period. The feature thus remains self-reliant of methods, i.e. for entire methods. That also becomes insignificant to the outcomes of classification in consideration of the motive of this feature is not a proper de-anonymization.

Biryukov et al. [13] assumed the charge of their assault on the whole bitcoin grid as less than EUR 1600 per month. Ron & Shamir [11] assumed the charge of their assault as less than USD 2600 monthly.

Evaluate Grid Using Network Benchmark:

Bitcoin network metrics are used to analyze the network. In this type of analysis, transactions, client grids developed by the evaluation of Blockchain data is handled using the Peer-to-Peer computing grid. Although, this feature is insignificant to the results because its motive is not to de-anonymize. Usually, the focus of the research with this feature is to detect and evaluate the characteristics of Bitcoin.

Examines Dormant Bitcoin Addresses:

Addresses that are mostly dormant and pertaining to uncirculated bitcoins are examined using out-of-network details and also through Blockchain data analysis. De-anonymization remains dissociated with dormant addresses/bitcoins, so this feature remains insignificant to the classification outcomes.

7. 5. Classification Of Studies With Invisibility Of User 8. Identity And Concealment Improvements

We classified methods to improve the Invisibility of user Identity and Concealment in Bitcoin-like digital cash systems. Studies that applied the method are given for each method. The outcomes and the procedures are elaborated in the undermentioned paragraphs. The quantitative network analysis propositions are less than as compared to the number of quantitative analysis propositions and a detailed classification cannot be provided for network analysis research.

Bitcoin addresses are discovered by effectuating out-of-network data. Measures cannot be taken against transactions, if in case the recipient wants to collect

bitcoins, then he must supply the sender with his address (Bitcoin).

The discovery of individuality is performed by using out-of-network data, which means that the enhancement procedures against Blockchain evaluation cannot address this outcome. Any information related to Bitcoin addresses need not be allotted in the out-of-network in order for their identity to avert from getting discovered.

We describe the results and methods in the first two paragraphs of this section. In the third paragraph, we confer (i) the relationship of Bitcoin propositions (ii) the procedure's performance.

Results and Outcomes

There are four main results of methods for improving the Invisibility of user Identity and Concealment. These results are (i) collapsing connections between transaction influx-outflux addresses, (ii) collapsing connections between transactions, (iii) concealing amounts and (iv) concealing IP addresses.

Collapsing Connections Between Transaction's Influx-Outflux Addresses:

Connections between the transaction influx(input) and outflux(outputs) are disconnected. It is quite impossible to obtain an output address for any particular input address in any transaction. Similarly, it is also impossible to obtain the input address for any output address in a transaction.

Collapsing Connections Between Transactions

If an input is linked to the other, two transactions are linked. Collapsing connections between the transactions mean eradicating connections by adding methods that obscure midway connections. Another transactions output on becoming a source of input cannot be tracked if the connection between 2 transactions is disconnected or removed.

Concealing Amount:

To improve Concealment, amounts are hidden in transactions. Although this outcome helps this result inhibits the uprightness of the system entirely from being checked, as an example, the entire quantity of coins in the system cannot be counted because the amounts are concealed. Consequently, if someone can fissure the setup, he can create coins without its discovery.

Concealing IP Addresses

The Bitcoin user's IP address needs to be hidden. This prevents the connection between the addresses of bitcoins and IP.

Procedures and Methods

Propositions that enhances Invisibility of user Identity and Concealment of bitcoin and other such cryptocurrency cash systems' can be classified into two primary types. The first type is the network analysis group of propositions that are not in favour of de-anonymization and the second type is the Blockchain analysis cluster of propositions that are also not in favour of de-anonymization.

The outcomes of the procedures and methods used to prevent network determination are that addresses pertaining to IP are hidden. It is advised to use analytical methods of blockchain in association with analytical methods of a network including The Onion Router nodes which is the prominent too developed to provide invisibility of user's identity as well as concealment. Basically, it conceals the actual Internet Protocol (IP)address at the time when the system is connected to the web. TOR is more generally a dispersed superimposed network which has nodes developed in such a way that it provides Invisibility of user Identity to applications based on Transmission control protocol (TCP). The Onion Router (TOR)'s data is initially encrypted several times based on the 3 nodes of TOR as picked up by the client.

Another tool that resembles the features of The Onion Router came into the picture when there was a need to discover a concealed grid on the Internet. That tool was termed as The Invisible Internet Project(I2P) [16] which developed the concealed networks that were termed as Darknet. Since "The Onion Router" adopted the technical term "onion encryption", here "The Invisible Internet Project" used the term "garlic encryption". The difference came as the formation of garlic encryption enables summing up numerous instructions and messages within the layered sheets of encryption. The drawback of the later developed technique was its smaller number of out proxies which were required for approaching the Web services through "The Invisible Internet Project" [15].

The new and improvised bitcoin concealment technique that has arrived after getting aspired by TOR is Transaction Remote Release [17]. Its model intention is to eradicate the assaults that arise during the time period when Bitcoin is adopted over TOR. Routing and multi-layer encryption in TRR are similar to "The Onion Router". Although, the approach of transmission in the transactions of bitcoin varies. TOR encodes the entire data on the Blockchain. But "Transaction Remote Release" just encodes and send new transactions, since it is specifically developed for the usage in Blockchain based Cryptocurrencies. Due to these, as a result, the overall node execution and maximum rate of production got enhanced. The vulnerability of Transaction Remote Release is the requirement to rectify the conventions and protocols of the cryptocurrencies. In mid-attacks, Transaction Remote Release is less open to attack to man but is susceptible to Denial of Service (DoS).

The analytical propositions in the field of blockchain where the de-anonymization is concerned divide it into 2 widely described classes. First, are the Backward compatible propositions where the rectification of cryptocurrency conventions is not needed. Further through the propositional way it can be deployed within no time. Deployment of this type of a proposition influences the accuracy of former transactions as well as

Corresponding author at: Meghan Bani Assad, The University of British Columbia, Vancouver, BC Canada.

the Blockchain till the time it gets deployed. The second class consists of a proposition that isn't exactly revertible. The above-described propositions need to be developed for such cryptocurrencies, but the Bitcoin convention requires modification to apprehend without being dependent on others. These two major classes for propositions for enhancement are broadly classified into subclasses according to their ways to connect, conventions, and Procedures. These are explained in the subsequent paragraphs.

Revertible:

Conjoining is a major technique practised by the revertible propositions. Conjoining can be acquired by complicate and befuddling transaction inputs and outputs. Maxwell presented the concept in front of the cryptocurrency committee with its proposition for CoinJoin. It is basically a method of transaction training for enhancing the Concealment, clients create combined payments through transactions that are also combined. However, many types of research analyzing Blockchain data estimated that many-input transaction inputs are possessed by the same client, Maxwell demonstrated and made clear that it was not needed and on its contrary was feasible. CoinJoin facilitates the cryptocurrency clients to go through a transaction individually and separately, while they are ready to accept the batch of input-output addresses. Their signatures are merged afterwards. As a result, the shuffling of addresses achieves obfuscation. A transaction thus created cannot be distinguished from a conventionally formed transaction.

CoinJoin can be centrally and decentrally implemented, as Maxwell described four alternatives. Clients can assemble on a medium and comply to take part in a transaction as the first option. Clients also understand this way through which input-output addresses of various other members involved in the transaction. The second alternative is the way for centralized conjoining in which a mixing server receives the requests and mixes them. In this approach, the server learns the user's input and output addresses. The third alternative is centralized again; however, the connection between influx and outflux addresses is concealed from the conjoining server using cryptographic formulations such as unfolded signatures, as mentioned by Maxwell [18]. The last option is the decentralized conjoining approach, where there is no blind signing server of third parties and participants in the mixing.

Integrated Conjoining:

An integrated conjoining server is for the users who want to blend the cryptocurrencies to share information about their influx and outflux addresses also the conjoining server disrupts their connection. A user sends his bitcoins to one of the conjoining server addresses. Inside the conjoining server pool, the cryptocurrencies are blended all together with other such cryptocurrencies.

In the explicit shuffling address, the relationship of influx-outflux addresses to their conjoining server is explicit. The conjoining server can link user input-output addresses. Clients, therefore, cannot remain invisible against the conjoining server, even though for other parties it is not possible to track the flow of coins after the conjoining.

Fair Exchange protocol:

A fair exchange protocol ensures that the exchanged item is received by the participants or that they do not receive anything. TumbleBit [20] is a course of action which permits invisible payments via a conjoining server and requires confidence in the server. TumbleBit [20] was made on aimlessly registered contracts which were not supporting Bitcoin backwards. It contained 2 interconnected protocols for the exchange of currency. Initially, the bearer exchanges bitcoins to an invisible check certificate from the server, and in the second instance, the bearer receives bitcoins from the server swapping the check certificate. For the outcome, the connection between the input-output address of the cryptocurrencies is disrupted by several transactions also the outcome converts into a fissure among the transactions.

Decentralized mixing:

In the decentralized mixing process, no external party, i.e. Any Integrated Conjoining server is needed. Collective conjoining is carried out by the clients involved. Disintegrated Conjoining is carried out either by extended shuffling or by the concealed rearranging of address.

Blind Signatures:

As already mentioned, the CoinJoin [19] of Maxwell can be applied in a disintegrated manner through the use of connection-disrupting blind signatures amidst the transaction's input addresses and output addresses.

Decoded Conjoined Networks:

D. Chaum introduced Decoded Conjoined Networks. A tuple of influxes passes from a tuple of conjoining nodes of these structures, where each mixing node shuffles the inputs and applies encryption and decryption.

Cryptocurrency Swapping Agreement:

The scripting functions of Bitcoin can be used for two-party decentralized conjoining via a cryptocurrency swapping agreement. The Fair Exchange Protocol was proposed by Coutu and can be used as a mixing protocol by two parties. In the approach explained briefly in the study, an incision and select agreement and cryptocurrency composing properties got used. The study did not cover pairing, i.e. the identification of peers to be mixed with.

Corresponding author at: Meghan Bani Assad, The University of British Columbia, Vancouver, BC Canada.

Network of Transactions:
Coutu introduced the transaction approach network, where a transaction network consists of two small part switch boxes combined in a network with a view to permuting address. Further, the switch box's output gets revealed to switch box participants only as the input and output mapping are determined. The study explained the use of various network structures, such as random pairings, the network butterfly and the omega network. However, encryption and decrying operations are not carried out. This approach is similar to decryption mixnet. The results of a transaction break down links between input-output addresses.

Protected Multiple-Party Calculation:
Protected Multiple-Party Calculation (PMC) or Secure multiple-party calculation (SMC) enables a set of clients to use private data to calculate the value of a public function while retaining private data. In 1982, Yao introduced SMC. The SMC was first proposed by an associate called hashcoin in the talk forum of bitcoin. This proposition uses a permutated alteration feature in SMC to shuffle addresses as well as the interrupt connections between the input addresses and output addresses within a created transaction.

Irreversible / Proposed Option
It has multiple enhancement plans, some of which are intended to be used with Bitcoin, while others, based on Bitcoin, have been designed as Bitcoin-like, but completely autonomous, as an alternative digital cash system from Bitcoin.

Hidden address shuffling:
Bitcoin address(s) are rearranged from each other in this method of hidden address shuffling. Even the input address that connects to any particular output address is concealed. The motive is to disrupt the possibility of flow tracking of cryptocurrencies. Procedures in this methodology use signatures and watermarks such as blind, ring and composite.

Blind Signatures:
Few data scientists introduced a new transaction forming procedure for cutting, choosing and using blind signatures. Changes to Bitcoin script features such as adding a new type of signature are also necessary. In order to implement a fair-trade protocol, blindly signed contracts used before the TumbleBit [20] study use blind signatures and smart contracts. They have employed Boldyreva, instantiated with elliptical curves that are computable efficiently for the Weil or Tate pairings and the Haillman computational puzzle is quite complicated. Even if cryptocurrency assists elliptical arcs, the used arc does not support the bilinear pairing required. An opcode supporting those arcs with effective duo linear coupling is therefore needed; changes are needed. Darkcoin is a Concealment-centric Bitcoin-based cryptographic currency that uses a decentralized CoinJoin implementation called DarkSend.

Ring Signatures:
It is a certain kind of signature of a set in which no group manager exists. In 2001, Rivest, Shamir, and Truman introduced this type of signature. Any group member can sign with the ring signature, and no ring signature can identify the signing member. As the base scheme which contains solutions to major bitcoin and CryptoNote weaknesses could be used as a groundwork for various cryptocurrency methods, Darkcoin was proposed It uses a single ring signature established on the cyclic-signature-mark of Sujisaki and Fuzuki. In Darkcoin, for the Concealment of sender sends addresses are grouped by ring signatures to other addresses, senders produce a signature that can be verified by the use of a set of public keys, not just a public key, or the single time usable cyclic signature.

Combined Signatures:
A composite signature combines a number of different signatures, in which no order exists. It allows additional signatures to be added at any time and it is difficult to compute the composite signatures for individual signatures. Composite signatures are used in Bitcoin-like cryptocurrencies to enhance anonymity.

Ownership shuffling:
Coins ownership is transformed into a shuffling approach to ownership. This is obtained by disrupting the link between coin and the owner, while also gathering and saving which client has what number of coins. The client may then demonstrate that he possesses and spends that particular number of coins. This shuffles ownership of the coins and prevents the use of coins. The use of zero-knowledge evidence can be used for shuffling ownership.

Zero-knowledge proofs (Transaction breaker & Hiding amounts):
EZC, Zerocoin extended version, has been suggested for hiding transaction amounts that Zerocoin cannot deliver because Zerocoin requires the conversion of zero coins to bitcoins in order to use. This will be achieved by enabling EZC to build multi-value zero coins with values which are the ones known to the communities within any transaction and spend zero-coins without turning them into cryptocurrencies.

Data encrypting:
The data encryption in this approach preserves confidentiality. The encryption uses homomorphic commitments.

Homomorphic Commitments:
Homorphic commitments allow a value to be committed by using homomorphic encryption technology, beyond disclosing it to other communities. It allows ciphertext

computations, in which the results are decrypted and are equivalent to the result of simple text operations. Back initially suggested this technique. For information about transactions in quantity, he proposed to use ZKP signatures by Schoenmakers and EC-Schnorr, namely to encrypt and only make the amounts visible to participants in a transaction. Maxwell suggested confidential transactions (CT).

Data disintegrating:
Data in this approach is partially broken down and stored in Blockchain. The non-Blockchain data remains unknown. For example, the Blockchain can store certain transactions and only the sender and recipient can remain in the remaining transactions. The Blockchain storage of the only hash of transactions is another example. So, we call the method used as off-chain storage in this approach. The data to be kept away are designed in accordance with the other methods employed.

5. Future Research Scope

Though Bitcoin continues to dominate the market, we see that day after day uses of alternative cryptocurrencies that improve Invisibility of User Identity and Concealment. Dash, Monero, ZCash, for example, can be used for implementing generally recognized proposals. Based on our inspiration, the use of digital cash systems in a world of digitalization and globalization, with developments in cryptography and computer technology, we anticipate and develop further instruments to increase Invisibility of User Identity and Concealment in these systems. In this connection, we identify four issues worth researching.

Performance:
We conjecture that while a great deal of research has been used-up on enhancing invisibility of user's identity and concealment performance, Further study will contain research into many other efficient procedures. Additional details are needed, in order to reduce the time required to process transactions, particularly for propositions which are load full in terms of cryptography.

Security:
There is an immensely changing case study going on digital cash systems, there has been a drastic rise in the number of optional propositions to improve invisibility of user identity and concealment in cryptocurrencies. However, the proposed protocols and cryptographic structures require a very recent and more detailed study.

Scalability:
Scalability while improved anonymity and confidentiality are other challenges. However, bitcoin cryptocurrency is the highly see-through grid network, scalability studies continue and the improvement of concealment may lead to further scalability limitations.

Anonymity and Trust:
Cryptocurrency addresses can be easily tracked as well as the amount of transaction is public. These characteristics allow monitoring system integrity. However, the steps are carried out to enhance Invisibility of User Identity and Concealment but then it becomes harder to control the integrity of the system. For example, the overall quantity of the coins in the arrangement cannot be calculated if transaction amounts are hidden, and when anyone disrupts the arrangement, coins get issued irrespective of the recognition. When the connections between transactions are broken, similar questions arise. If additional mechanisms for enhancing Invisibility of User Identity and Concealment are added to the arrangement, confidence in the system increases.

6 Conclusions

In this research survey analysis, we tried to introduce an all-inclusive study analyzing futuristic Invisibility of user Identity and data protection research in cryptocurrencies. It has been classified into 2 main classes: Research analyzing Invisibility of user Identity and Concealment, and studies proposing improvements in Invisibility of user Identity and Concealment. The first category deals with the disclosure of information through the use of de-anonymization. We inspected and determined a classification for 35 types of research in this class and obtained 11 methods and 7 results from those researches. The motive of the research is mainly to discover de-anonymization methodologies and get details which compromise Concealment, such as exploring cryptocurrency's addresses, identifying individuality, matching cryptocurrency addresses to IP addresses, connecting cryptocurrency's addresses to geographical-location coordinate. Our examination shows that the analytical survey of Blockchain comprises most research in this class and there are some analytical research.

References

[1]. Cryptocurrency Market Capitalizations. Accessed: Dec. 15, 2017. [Online]. Available: https://coinmarketcap.com
[2]. "What is Bitcoin?". CNN Money. Archived from the original on 31 October 2015. Retrieved 16 November 2015.
[3]. Satoshi. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[4]. mining? Hint: Don't mine Archived 5 May 2014 at the Wayback Machine, The Week, 15 April 2013
[5]. "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016.
[6]. Merkle, "A digital signature based on a conventional Encryption function," in Advances in Cryptology—CRYPTO '87 (Lecture Notes in Computer Science),

Corresponding author at: Meghan Bani Assad, The University of British Columbia, Vancouver, BC Canada.

vol. 293. Heidelberg, Germany: Springer, 1988, pp. 369–378.
[7]. Denial of Service, Hashcash—A Denial of Service Counter-Measure. Accessed: Jul. 6, 2016. [Online]. Available: HTTP:// www.hashcash.org/hashcash.pdf
[8]. "Enigma: Decentralized computation platform with guaranteed privacy," arXiv preprint arXiv:1506.03471, Jun. 2015. [Online]. Available: https://arxiv.org/abs/1506.03471
[9]. F. Reid and M. Harrigan, "An analysis of anonymity in the Bitcoin system," in Security and Privacy in Social Networks. New York, NY, USA: Springer, 2012, pp. 197–223.
[10]. D. Kaminsky (2011, Aug.). Black OPS of TCP/IP, Black Hat USA, 2011
[11]. A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[12]. E. Androulaki and G. O. Karame, "Hiding transaction amounts and balances in bitcoin," in Proc. 7th Int. Conf. Trust Trustworthy Comput. (TRUST'14), Jun. 2014, pp. 161–178.
[13]. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in Bitcoin P2P network," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, Scottsdale, AZ, USA, 2014, pp. 15–29.
[14]. P. Koshy, D. Koshy, and P. Mcdaniel, "An analysis of anonymity in Bitcoin using P2P network traffic," in Financial Cryptography and Data Security (LNCS 8437). Heidelberg, Germany: Springer, 2014, pp. 469–485.
[15]. I2P—The Invisible Internet Project. Accessed: Feb. 17, 2017. [Online]. Available: http://mediatechnology. leiden.edu/images/uploads/docs/
[16]. I2P Darknet, Bitcoin Forum. Accessed: Jan. 3, 2017. [Online]. Available: https://bitcointalk.org/ index.php?topic=1481693.0
[17]. "Transaction remote release (TRR): A new anonymization technology for bitcoin," arXiv preprint
[18]. arXiv: 1509.06160, Sep. 2015. [Online]. Available: https://arxiv.org/ abs/1509.06160
[19]. [18] Gmaxwell: CoinJoin: Bitcoin Privacy for the Real World, Bitcoin Forum. Accessed: Jan. 12, 2017. [Online].
[20]. CoinJoin Sudoku |Weaknesses in Shared Coin, and CoinJoin Research. Accessed: Jan. 19, 2017. [Online]. Available: http://www.coinjoinsudoku.com
[21]. "TumbleBit: An untrusted bitcoin-compatible anonymous payment hub," IACR Cryptol. ePrint Archive, Rep. 2016/575, Jun. 2016. [Online]. Available: https://eprint.iacr.org/2016/575