Do Bitcoin Users Really Care About Anonymity? An Analysis of the Bitcoin Transaction Graph

Anil Gaihre Yan Luo Hang Liu
University of Massachusetts Lowell

***Abstract*—The pseudonymous nature of Bitcoin has sparked the twin rivaling researches in Bitcoin community, that is, either protecting or attacking anonymity. In spite of this intense battle, the answer to a primary question is absent – *Do Bitcoin users themselves care about anonymity?* This paper demystifies this doubt via analyzing the Bitcoin transaction graphs with the following three contributions: 1). We outline three representative metrics that can signify whether users concern about anonymity. 2). We examine the collective trend of anonymity concerns from a macroscope. 3). We pay particular attention on critical addresses in a microscope to unveil their anonymity concerns.**

This paper arrives at both expected conclusions and unexpected surprises. In particular, the expected ones are: rich addresses concern more about anonymity than poor ones. Miner addresses start caring about anonymity when exchange rate soars. Stock addresses never hide their intent of jump-and-dump. The surprises are: the majority of the users show weak concerns on anonymity. One can easily find both hot and cold wallet addresses owned by big organizations.

I. Introduction

When Satoshi Nakamoto first introduced Bitcoin blockchain technology [1] to the world in January 2009, the twin radical components of Bitcoin have affirmed its taken off, that is, decentralization and anonymity. It is important to mention that *the only target of digital currency is to avoid double-spending without a centralized trusted verification institution, such as banks*. Toward that end, Bitcoin relies on a collection of decentralized miners to check whether the ongoing transactions comply with all previously approved ones, such as whether current payer has sufficient budget for this transaction. All the validated transactions are further grouped together in a block and chained together into a public ledger. The process of creating transaction blocks will result in Bitcoin generation which attracts a collection of miners [1] to verify the transactions.

While decentralized miner requires all the transaction data to be publicly announced for verification purposes, exposing the real world identities of the Bitcoin practitioners is unacceptable. Bitcoin thus adopts pseudonyms to conceal the information of Bitcoin participants. The bad news is anonymity can also evolve into the major vehicle for criminals, such as money laundering [2] and human trafficking [3]. Consequently, *anonymity becomes a key battleground in Bitcoin research and commercialization*.

On one hand, there exist four directions of de-anonymization endeavors as follows: 1). Interacting with Bitcoin users to track the Bitcoin. For instance, [4] studies the Coinjoin (i.e., for the purpose of mixing Bitcoin) for anti-money laundering analysis. 2). Crawling third party information. For instance, [5], [6] introduce BitIodine, an open blockchain analytical framework which uses a set of web scrapers that automatically collect and update the lists of Bitcoin addresses belonging to known identities. 3). Tweaking Bitcoin client software to uncover the network address of the users. Biryukov et al. [7], Koshy et al. [8], [9] work on de-anonymizing the users Internet Protocal (IP) address in the Bitcoin Peer-to-Peer (P2P) network. 4). Analyzing the Bitcoin transaction graph. Meiklejohn et al. [10] group Bitcoin wallets based on shared authority in order to cluster criminal or fraudulent Bitcoin addresses. Reid et al. [11] exploit context discovery and flow analysis of the Bitcoin graph to trace the alleged theft of Bitcoins. A recent work [12] uses graph learning to identify yet unknown entities based upon given training structures on the transaction graph.

On the other hand, researchers also attempt to enhance the anonymity of Bitcoin. [13] redesigns the P2P network of the Bitcoin with the first priority on strengthening the anonymity of the Bitcoin. There are several Bitcoin mixing protocols which claim to provide trustless, low cost and low time overhead like [14], [15]. In particular, [15] proposes a protocol to improve the anonymous payment in Bitcoin with concepts of cryptographic accountability and randomized mixing fees. Bitcoin core developer Gregor Maxwell introduces the concept of Coinjoin [16] operation which can avoid the changes toward Bitcoin protocol. JoinMarket [17], Coinsuffle [14] are the existing Coinjoin implementations. We also observe an array of emerging Alternative coins (i.e., *Altcoin*) like Dashcoin [18] and Monero [19] that are developed for improving the anonymity.

Despite such an intense battle atop Bitcoin anonymity, no one attempts to answer a key quest – **Do Bitcoin users themselves concern about anonymity?** To unveil that intent, this work conducts a systematic analysis on the Bitcoin transaction graph that spans for more than nine years with nearly 400 million addresses and 321 millions transactions. Our findings contain both surprises and expected conclusions. Below we discuss our designs, without which, the conclusion cannot arrive at.

First, we introduce three metrics to formally signify whether a Bitcoin address concerns about anonymity. The first metric links the extent of anonymity concern with reuse frequencies, that is, lower reusage flags higher anonymity concerns. The second metric – zero balance – finds that address turns to

978-1-5386-5035-6/18/$31.00 ©2018 IEEE

zero balance tends to concern about anonymity. Last but not the least, we find the intention of an address is also relevant to anonymity. That is, if an address rarely hides its intention or the type of organization it belongs to, it is less concerned about anonymity. We also explore the dynamics of anonymity by collectively analyzing the former two metrics.

Second, we exploit the macroscope analysis on Bitcoin transaction graphs to reveal the collective anonymity concern trend of all Bitcoin addresses. In this analysis, we approximate the diameter of the Bitcoin transaction graph at different time points with iBFS [20] and unveil that *whether new transactions bringing in new addresses is the key for diameter dynamics*. In particular, the increment of diameter is caused by the addition of new addresses, signifying more concerns about anonymity. For instance, our statistics exhibit higher new addresses additions than old addresses re-usage from 2011/January to 2012/March, which results in the swelling of Bitcoin graph diameters. Further, we categorize the addresses into rich and poor addresses on the basis of Bitcoin balance and observe rich addresses concern more about anonymity.

Third, we summarize the representative features of critical Bitcoin addresses, which allows any of us to hunt for the key addresses quickly and precisely. In particular, we find strong correlations between stock addresses and Bitcoin exchange rate which perfectly matches stock buyers' jump-and-dump nature [21]. We develop algorithms that can reap the key addresses (hot and cold wallet addresses) from big organizations like miners, gambling sites and exchange centers. Notably, that algorithm obtains both tagged key addresses and untagged ones. We believe those untagged ones are the key addresses that are intentionally hidden by certain organizations. Further, as the major force that drives the success of Bitcoin, miner's intention is also studied. We find they start concerning about anonymity only when the Bitcoin price begins to climb.

Evidence. It is important to note that those aforementioned expected and unexpected insights are evident by real-world facts. In particular, for macroscope analysis, Benjamin et al. [22], a parallel work to this paper, interview 125 active Bitcoin users and reveal that majority of them understand the risk of de-anonymizing in Bitcoin, indicating that they disregard anonymity not because of unaware of the penalty. Toward microscope analysis, our intention-based de-anonymization analysis on critical addresses matches the real examples which are crawled from popular blockchain forums [23], [24]. Further detailed discussions about these examples can be found in Table III and IV, and Figure 10 of Section VI.

The rest of this paper is organized as follows: Section II presents the landscape of the background and related works for Bitcoin. Section III discusses the proposed anonymity metrics. Section IV describes the datasets and processing tools we used for the analysis. Section V understands the overall anonymity concerns of Bitcoin addresses. Section VI zooms into the anonymity analysis of the critical addresses. Section VII concludes the paper.

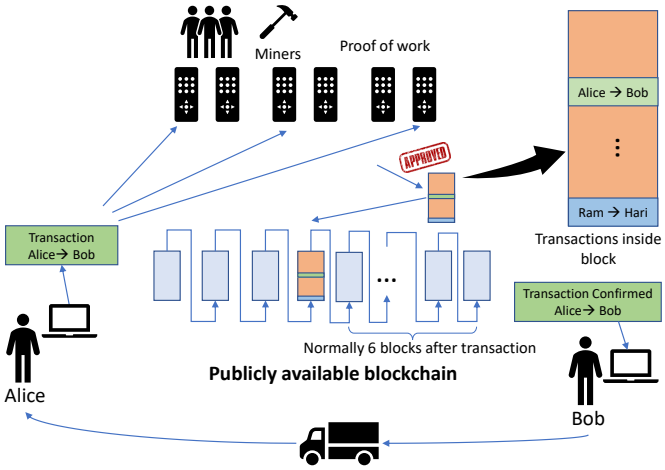

Fig. 1: The workflow of Bitcoin transactions, assuming Alice is sending Bitcoin to Bob.

II. Background

This section presents the background of cryptocurrency and blockchain technologies, as well as privacy and anonymity features. Further, we discuss the related work surrounding anonymity of blockchain currency.

A. Bitcoin and Blockchain Currency

Assuming Alice is purchasing some products (i.e., transferred by the truck) from Bob, Alice will send a certain amount Bitcoin to Bob for this transaction. In particular, this Bitcoin transfer process is comprised of two steps: *preparation* and *verification*. In the first step, Alice needs to provide three types of addresses, that is, which set of output addresses from which set of transactions will she uses to pay the Bitcoin[1], the addresses used to receive the *changes*[2], and the addresses Bob used to receive that transfer.

Figure 1 plots the workflow of the second step – verification. In particular, Alice will initialize this transfer with the three types of addresses and her "private key" to the source addresses through her wallet like Bitcoin Core software [25]. Since Bitcoin follows Peer-to-Peer (P2P) network communication, this software will broadcast the transaction on the entire network. Subsequently, miners will race to validate this transaction. If the transaction is valid, the miner will insert this transaction in a block. The miners need to perform proof-of-work (PoW) [1] in order to mine a block. Once the block is mined it is linked to the most recently approved block in the block chain (in the middle of Figure 1). After that block is dipped (i.e. followed by other blocks) sufficiently (normally 6 and 7 blocks depth) inside the blockchain [26], the transaction, which is very unlikely to reverse, is confirmed. Then Bob can confirm the transaction and ship the goods to Alice.

[1]Note, the amount of Bitcoin of each address is not immediately clear. This is the value-blindness feature of Bitcoin.

[2]The change address can be provided by a user or wallet software does that for the user.

Note, Bitcoin is also referred to as a type of Blockchain currency stemming from the fact that all the transactions are packed into "blocks" and "chained" together. In particular, each block contains approximately 2,020 transactions that consumes $\leq$1 MB space.

Incentives are provided to compensate the miners that volunteer to verify the transactions. To avoid Sybil attack that may subvert the previously approved transactions, Bitcoin adopts one-CPU-one-vote instead of one-IP-address-one-vote paradigm. That is, one needs significant CPU power to conduct the PoW fast enough in order to combat the other miners and subvert the prior transactions. In this setting, as long as more than 50% of the miners are legitimate, Bitcoin can guarantee the legality [27]. Eventually, the longer chain will stand out while the other forks will be dumped away.

Bitcoin is pseudo-anonymous. Since Bitcoin encourages decentralized miner, all transactions are publicly accessible. To protect the privacy of Bitcoin users, anonymity is engaged. That is, Bitcoin uses SHA-256 [1] to generate key pairs in order to represent virtual users. In each key pair, the public key serves as the address in Bitcoin currency while the private one is kept by the owner. One user can own arbitrary amounts of such pairs of addresses, all of which can further be managed by a *wallet software*. In order to conduct transactions with an address, such as transferring money from an address to another, a private key is required to digitally sign, i.e., authorize, this transaction. We refer the readers to [28] for more details regarding how the transactions are generated, validated by the miners and confirmed by the receiver.

B. Related Work

Bitcoin community has officially acknowledged that "current implementation of Bitcoin is not very anonymous" [29], which is evidenced by an array of attempts that successfully revealed the real world identities of the Bitcoin addresses. While certain users with more concern on anonymity can shift to *altcoins* according to [30], we argue Bitcoin still deserves this analysis stemming from the fact that Bitcoin occupies the largest market in cryptocurrency. This section summarizes the de-anonymization efforts on Bitcoin platform.

Interacting with Bitcoin users. One can act as a buyer in Bitcoin transaction and learn the address of the merchant. If an adversary wishes to know the public address of an organization or merchant, he/she can buy some goods from them. By doing that the merchant should give him/her an address that belongs to them. Meiklejohn et al. [10] conduct this kind of interaction with merchants like Silk Road [31] and Mt. Gox [32]. Likewise Moser et al. [4] study the anonymized transaction by participating in the Coinjoin service.

Crawling third party information. Every type of cryptocurrency, including Bitcoin, often comes with a collection of communication forums. For instance, [33], [34], [35], [36] are the Internet-based discussion forums. Fleder et al. [37] develop a system for extracting Bitcoin addresses from public forums. An adversary can get the public address of users which are leaked or made public by crawling from these sites. Besides, certain merchants and organizations are also publishing their Bitcoin addresses to accept donations, such as WikiLeaks [38] which relies on an array of address to receive donations. Ron and Shamir [39] are able to find out that there are at least 83 addresses owned by the Wikileaks for such a purpose. Obviously, digesting the information of these sites will help reveal the real world identities of the addresses.

Network addresses. In Bitcoin P2P communication network, the payer/buyer will be the one who initializes the communication. By analyzing the communication time stamp and pattern, one can reveal the IP addresses of the source of the Bitcoin transaction. Further associating network addresses to the real world identities can be achieved via linking IP address with geographical locations. Koshy et al. [8] are the first one that attempts to map the Bitcoin address to an IP address by continuously listening to the transactions made by the nodes in the Bitcoin P2P network. They develop their own Bitcoin client called CoinSeer to record the IP addresses.

Analyzing transaction graph, which perform graph computations on the Bitcoin transactions for anonymity analysis, is closely related to this work. Reid and Harrigan [11] pioneer this effort. In particular, they exploit multi-input, change address and behavior based clustering heuristics to create one-to-one mapping between address and user. [10] uses this mechanism to identify unknown addresses through linking which to known ones. Later, Ron and Shamir [40] exploit this method to analyze the transactions related to Ross William Ulbricht (a.k.a. Dead Pirate Roberts in Bitcoin), owner of online black market known for illegal drug trade and money laundering.

Moser et al. [4] brings up the concept of change address, which is most likely the output address with smaller amount of Bitcoins. As a comparison, Ortega [41] suggests a change address of a transaction should have more decimals. It is also worthy of noting Ober et al. [42], which analyzes all the transactions occurred before January 2013, and discover that the Bitcoin anonymity is reduced in the last 12 to 18 months due to the entity sizes and the overall pattern of usage becoming more stationary.

Instead of how to compromise or strengthen the anonymity of Bitcoin users, we focus on whether users care about anonymity. We believe this is the very first question that we need to discuss before blindly fighting for decreasing or increasing the anonymity of Bitcoin, since changes on anonymity will draw non-trivial efforts. Towards that end, we deduce three topological dynamics surrounding the Bitcoin transaction graph that can indicate the anonymity concerns of the users (Section III). To the best of our knowledge, this is the first work to find out the collective anonymity concerns reflected by all the Bitcoin addresses (Section V), as well as the critical addresses (Section VI) over a period of nearly ten years.

III. Anonymity Metrics

This section takes the inspiration from Section II-B and goes further by introducing metrics that can indicate the extent of

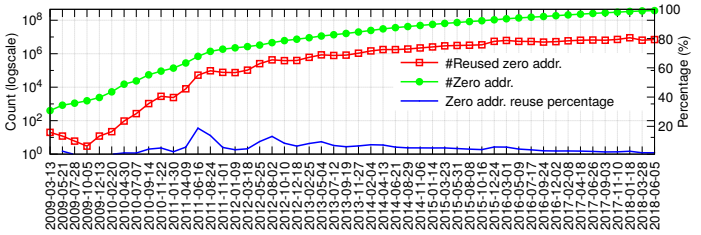

Fig. 2: Zero address reuse percentage over time.

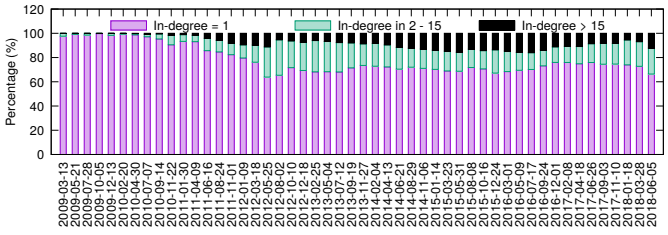

Fig. 3: Bitcoin address turning to zero address with in-degree 1,2 to 15, greater than 15

anonymity and privacy concerns expressed by each address. In particular, we extract two types of directions, that is, whether the address attempts to cover its *real world identity* and *intention*.

Claim 1 (Reusing Frequency)**.** *The reuse frequencies of an address, especially those re-usage for receiving money, can signal whether an address concerns about anonymity.*

Explanation. For a user to be considered as anonymity concerned, he/she is unlikely to reuse old addresses[1] to receive Bitcoins. If one address is repeatedly used to receive Bitcoins, the chance of associating this address to its real world identity will soar [43], [44], [1], [45], [42], [39]. In particular, assuming the probability of seizing the real world identity of an address from one transaction is p, N transactions will increase the probability to $N \cdot p$. The following twin methods are proven solutions to identity the users:

1) Transacting with the address of interest [4], can improve the probability of tracing the coins through Coinjoin operations.
2) IP address association [8]: Intercepting the Bitcoin network can help reveal the IP address of the source Bitcoin address.

The *in-degree* of an address signifies how frequent the address is used to receive Bitcoin. If a user uses an address to receive Bitcoin only once, then reduce the balance of the address to zero, meaning the reusage frequency is low. In this case, we assume the user is serious about anonymity. Note this is different from typical Coinjoin operations which attempt to mix various Bitcoins for, potentially, the purpose of money laundering [4]. □

Claim 2 (Zero Balance)**.** *Addresses with zero balance concern about anonymity.*

Explanation. We consider an address to be zero balance if the Bitcoin accumulated/associated to the address is zero. There are two anonymity concern cases that produce zero balanced addresses:

1) Change address: In each transactions, all the Bitcoin is spent from the input addresses and the changes are deposited to new addresses, called change address. Note, users can also choose an existing address to receive the changes. Using new addresses for changes means the user is serious about anonymity [46].
2) Intentional Bitcoin transfer: This includes the combining and splitting [1] of the Bitcoin. The splitting activity is mostly motivated by the anonymity concern as it splits large amount of Bitcoin for safety. The combining, which happens very rarely, is driven by dust Bitcoin [47], that is, users combine a collection of addresses with small amount of Bitcoin for the convenience of Bitcoin management.

While a non-zero balance address turning to zero-balance can indicate this address starts concerning anonymity, an address may also become zero balance due to all Bitcoin is spent. In that case, a user who is not concerned about anonymity may reuse that address in the near future. Figure 2 thus studies this doubt. In particular, we find that the reuse percentage of zero balance addresses through all Bitcoin history stay very low – 5.2% – with minimum and maximum as 0% and 18%. This implies that a zero balance address is unlikely to be reused, indicating majority of the addresses becomes zero balance due to anonymity concern. □

Nevertheless, one interesting observation is *high in-degree addresses may also turn to zero balance*. This represents the sudden change of anonymity concerns. That is, high in-degree means unconcerned about anonymity while turning to zero balance means serious about anonymity. Figure 3 studies this contradictory. In particular, we separate the zero balance addresses into three categories based upon in-degrees – (0, 1], (1, 15] and (15, $+\infty$). Table I presents the statistics summary of Figure 3. **The trend shows that the change of anonymity concerns is possible. But the possibility of changing from lower in-degree is larger than that from higher in-degrees.**

TABLE I: Percentage of different in-degrees on concerned addresses.

In-degree when balance turn to 0	Min % (date)	Max % (date)	Average %
(0, 1]	66.39 (2012-05-25)	99.77 (2009-10-05)	78.23
(1,15]	0.23 (2009-10-05)	29.25 (2012-08-02)	13.89
(15, $+\infty$)	0 (Until 2010-02-20)	16.01 (2016-07-17)	7.87

While revealing the real world identity of an address is useful, exposing the intentions of certain addresses are of equivalent importance. For instance, searching the identity of an address takes non-trivial efforts, knowing their intentions

[1]**Old Address**: If an address already appeared as output address in at least one of the transactions before in the blockchain. **New Address**: If the address appears for the first time as an output address in the entire blockchain history

would help cybercriminal fighters narrow down the searching space toward the addresses of interest.

Claim 3 (Address Intention)**.** *If one address attempts to hide its intention, we assume it cares about anonymity.*

TABLE II: Address definitions.

Address type	Description
Hot wallet address	Private key is online for convenient transactions
Cold wallet address	Private key is offline for security purpose
Miner address	Reward address
Stock buyer address	Purchasing Bitcoin as an stock investment
Normal address	Exploited for normal business

Explanation. This claims "zooms in" the anonymity analysis toward the particular addresses in the transaction graph. Using the critical addresses from Table II as an example, these are *hot wallet address*, *cold wallet address*, *miner address*, *stock buyer address*. It should be noted that any organizations and individual can maintain hot/cold wallet addresses, this manuscript will only target those from big organizations, such as, exchange centers, gambling sites and miners.

Use cases: Unveiling the intention of these addresses are of particular importance. For instance, to maximize the profits, criminals may target cold wallet addresses of big organizations [48] when steal Bitcoins. Law enforcement, on the other hand, may want to locate those hot/cold wallet addresses from illicit organizations, such as Backpage.com, for investigations [3]. In both cases, unveiling the intention of Bitcoin addresses is indispensable. □

IV. Datasets and Toolsets

This section details the specifics of the Bitcoin transaction graph, as well as, the graph algorithms that are used to analyze this graph in order to extract insights.

A. Datasets and Machines

We download the publicly available Blockchain raw data using Bitcoin Core v0.16.0 [25]. This file consists of the transactions for 9.5 years, ranging from January 3, 2009 to June 7 2018. The size of this dataset is 230 GB. We exploit the popular rusty-block-parser [49] script to decrypt and parse the encrypted blocks and transactions. The output of this process contain several comma-separated value (CSV) files that consists of the information of each block, including the timestamps, hash of blocks, transaction IDs, output addresses in a transaction and inputs as reference to the previous transaction output. The collective size of these files hikes to 441 GB.

With the available transaction and address information from the tool, we create mappings from transactions and addresses to numerical vertex IDs. Since each edge in the graph always connects to one address and one transaction, this graph is thus a bipartite graph [50]. Further, to conduct time evolving analysis of the transaction graph, we select vertices based upon their timestamps. In total, the amounts of transactions and addresses are 321,043,952 (321 million) and 399,344,697 (399 million), respectively, as well as edges are 1,692,308,191 (1.6 billion).

We build the analytical toolset (from Section IV-B) and edge list generator with approximatey 2,000 lines of C++ code and use the compressed sparse row (CSR) tool from [51] to store the graph. Further, we leverage the Bridges supercomputer from Extreme Science and Engineering Discovery Environment (XSEDE) [52] to preprocess, store and execute the analysis. In particular, each Bridges server features quad-socket Intel(R) Xeon(R) CPU E7-8880 v4 @ 2.20GHz CPUs, 3TB memory and 14 TB LUSTRE filesystem [53].

B. Graph Algorithms

We leverage a variety of graph algorithms and heuristics to analyze the Bitcoin transaction graph and deduce whether the Bitcoin addresses are serious about anonymity. In particular, the following four graph algorithms are used to examine the Bitcoin transaction graphs. Below, we explain the design of these algorithms with our intent of using them.

Connected component [54] of an undirected graph is a subgraph where each vertex can reach the others. On analysis of the connected component of the graph, we aim to find out the amounts and sizes of connected components in Bitcoin transaction graph. Since each miner reward address, mostly new ones, will introduce a new connected component, the reason behind being a separate and small connected component could indicate the miner addresses lack anonymity concerns.

Diameter detection [55]. The diameter is the longest path of all the shortest paths in the graph. Ideally, one has to calculate the shortest path from every vertex in order to find the perfect diameter of a graph. Given the graph consists of 720 million vertices and 3.38 billion undirected edges, it will take days to compute the diameter for one timestamps [20]. In this context, we approximate the diameter of the Bitcoin graph with iBFS [20]. Note BFS is equivalent to single source shortest path (SSSP) in this transaction graph because the Bitcoin flow on the edge is not weight. As shown in Section VI), we exploit the change of diameter over time to deduce the anonymity concerns of the users. It should be noted that we consider the diameter of the main connected component as that of the entire graph because this component consists of more than 99.9% of the vertices.

In-degree analysis [56]. The number of incoming edges to a vertex is the in-degree. In Bitcoin transaction-address graph, this parameter stands for the number of times an address is used to receive Bitcoin. In contrast to in-degree, out-degree represents the amounts of times an address is spending the Bitcoin. The transaction inputs have to refer the unspent Bitcoin from the outputs of prior transactions in the Blockchain which suggests the in-degree analysis already covers that of out-degree. Besides the low out-degree of an address doesn't necessarily mean that the address is reused infrequently. Consequently, we only cite in-degree as the evaluation metric.

Flow analysis [57] is necessary because Bitcoin is a value-blind cryptocurrency [58]. However, one can analyze the flow

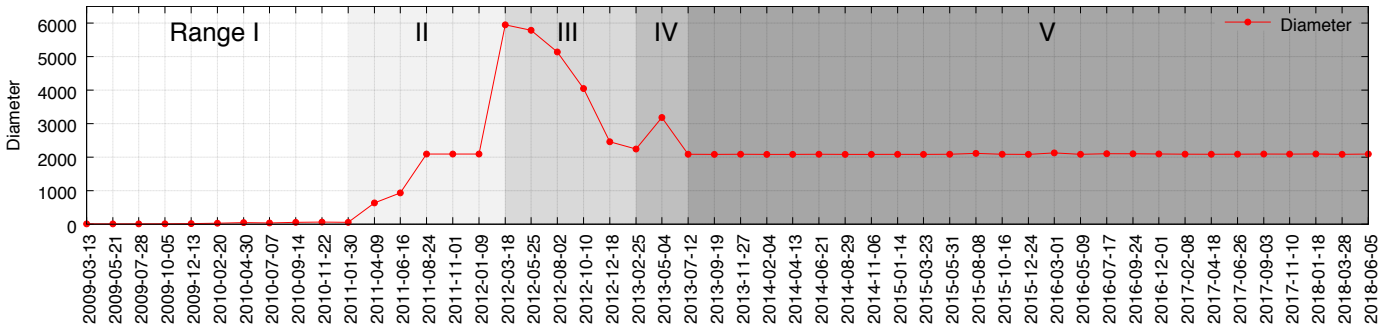

Fig. 4: The dynamics of graph diameter for the Bitcoin transaction graph over time.

of Bitcoins on the transaction edges to arrive at the amount of Bitcoin accumulated at each address, as well as the amount of Bitcoin involved in each transaction. We find this tool to be particularly useful for analysis on rich and poor, and hot and cold wallet addresses.

V. MacroScope Analysis

This section explores the collective anonymity concern from all Bitcoin users. In addition, we study the anonymity concern differences between rich and poor addresses.

A. Observation

Figure 4 studies the diameters of Bitcoin transaction graph that spans for ∼9.5 years – from March/13/2009 to June/5/2018. Given computing diameter is time consuming, we sample 50 time points to calculate the diameter. The time difference between two consecutive sample points is ∼69 days. For ease of understanding, we mark the xtics in Figure 4 with the specific dates, that is, 2009-03-13 stands for March 13 of 2009, similarly for the rest of the xtics, as well as rest of the figures in this paper.

The diameter dynamics in Figure 4 can be summarized into five ranges, as shown in Figure 4. The diameter remains stable during ranges I and V. It climbs in range II. Afterwards, we observe the diameter collapse in range III. A slight diameter fluctuation happens in range IV.

B. The Cause of Diameter Dynamics

Taking the inspiration from [59], we arrive at the conclusion that the diameter will either swell or remain unchanged when new transactions also bring in new addresses. In contrast, when new transactions only happen between old addresses the diameter tends to remain or shrink.

Figure 5 exemplifies both cases. Let us suppose, transactions T1, T2 and addresses A1, A2 and A3 already exist in Figure 5(a) - (d) with the diameters to be four. Figure 5(a) and 5(b) assume the new transaction happens between the new and old addresses while 5(c) and 5(d) suppose transactions happen only between old addresses.

As shown in Figure 5(a), an old address A2 sends Bitcoin to A4 in transaction T3. Although the address A4 is new, the diameter of the graph remains the same. But this may not happen all the time. Using Figure 5(b) as an instance, when

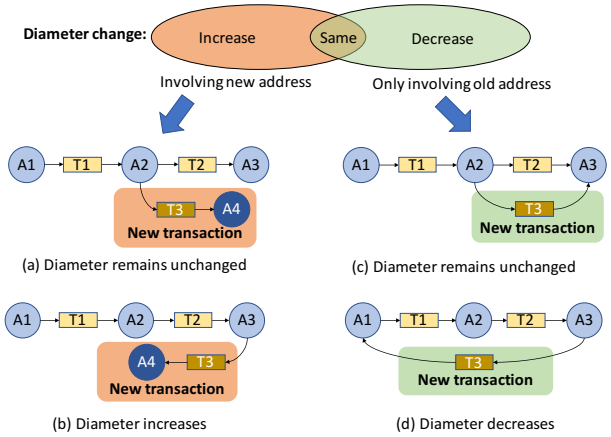

Fig. 5: The dynamics of diameter with respect to new transactions, where the circles with label starting with "A" are the addresses and the rectangles starting with label "T" are the transactions. In particular, (a) diameter remains unchanged and (b) diameter increases when new transaction brings in new addresses. In contrast, new transaction with old addresses may result in (c) diameter remains unchanged and (d) diameter decreases.

address A3 sends Bitcoin to a new address A4 in transaction T3, the diameter of the graph increases to 6.

Figure 5(c) and 5(d) outline the cases when new transactions happen between existing addresses. In Figure 5(c), the new transaction between the addresses A2 and A3 will not change the diameter but the transaction between the addresses A1 and A3, as shown in Figure 5(d), shrinks the diameter of the graph to three. We refer the readers to [59] for the reasons what cases of transactions with new addresses may increase the diameter.

This analysis suggests that more Bitcoin users are concerning about anonymity in range II while fewer of them are concerning in the period of range III. The initial period of range I and range II were mostly dominated by the bitcoin enthusiast and the cryptographers who used new addresses to receive the Bitcoin [60] . The rest of time ranges, when diameter remains unchanged, demand more analysis on the graph to unveil whether users are concerning about anonymity or not. Note, according to Section VI, because miners are trying to mine the blocks without normal business transactions that can link the transaction, the diameter of Bitcoin graph in range I remains small.

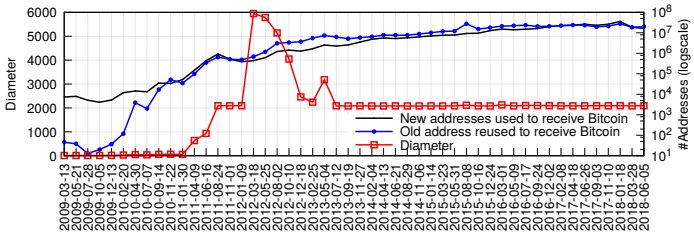

Fig. 6: New vs old addresses used in Bitcoin transaction over period of time. The address count is number of old addresses and new addresses used for receiving Bitcoin from prior date.

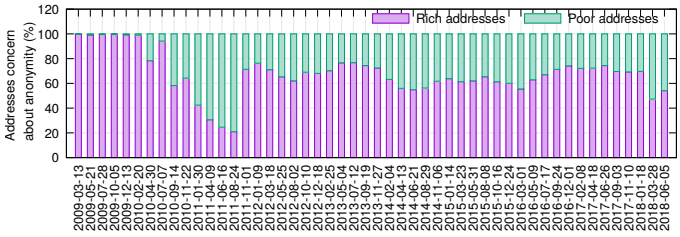

Fig. 7: Rich vs poor among the addresses that are concerned about anonymity.

The spike of range IV is potentially caused by new addresses keep attaching to the tail/head of the existing transaction graph, analogous to a repeated case of Figure 5(b). Afterwards, some of those newly generated addresses start transacting with existing old addresses like Figure 5(d). A real case of the spike can be found in Case II of Figure 10.

C. New vs Old Addresses to Receive Bitcoin

The reuse of old addresses to receive the Bitcoin from a transaction is significantly high and most of the time exceeds the use of new addresses. Below we will explain why this leads to unchanged diameter in the transaction graph.

Figure 6 shows the number of old and new addresses used to receive the Bitcoin in a transaction. Despite new addresses maybe caused by newly joined users or old users added for anonymity concern purpose, the number of old addresses used to receive Bitcoin is generally higher than that of new addresses for most of the time. This signifies most of the transactions happening in Bitcoin do not take anonymity as a serious concern. Of the total amount of addresses that is used to receive Bitcoin in transactions, on average, the use of old address is 55.25% and the new addresses is 44.75%.

It is important to note that the diameter may also increase as long as new addresses are added, albeit the number of new addresses is smaller than the reuse of old addresses. Our further observation negates this doubt. That is, those new addresses consist of considerable stock buyer address thus are directly connected to exchange centers which are at the center of the graph, resulting in zero impact to the diameter.

We will only use two real world events to explain the hikes of the addition of new addresses, leaving the rigorous analysis to Section VI. For instance, in around 2011, the establishment of exchange centers [61] during those periods causing more users to join the Bitcoin, this also explains the sudden spike of new addresses used to receive Bitcoin. Second, the period between Jan 2017 and December 2017 is the time when the Bitcoin price was continuously climbing to reach a peak value. During this time, the use of new addresses is more than the old addresses to receive Bitcoin. The number of old address use again surpasses the new address use in 2018-3-28 which is the time when Bitcoin price plunged into the amount of around 10,000 USD from 19,000 December/2017-January/2018 [62]. That should have discouraged new users buying Bitcoins (joining the network).

There exist significant number of users who own Bitcoin as an investment [63]. Since Section VI-A specifies there are significant number of Bitcoin users joining Bitcoin for investment, we can offset these new addresses from Figure 6. This will further reduce the actual number of new addresses that are introduced for the concern of anonymity.

D. Rich vs Poor Addresses

The difference between rich and poor always draws attentions [64]. This Section studies their anonymity and privacy concerns differences. In particular, we regard the addresses with top 25% Bitcoin addresses across all nonzero balance addresses as rich and the rest as poor. Along with the dynamics of the Bitcoin distribution among addresses we also update our threshold (i.e., third quartile Bitcoin among the addresses with non zero balance) in order to retain the updated rich and poor addresses. With in-degree (Claim 1) and zero balance (Claim 2) heuristics along with flow analysis, we find out which kind of addresses is more concerned about anonymity.

Figure 7 shows that more rich addresses concern about anonymity. Here, we use Claim 2 to indicate whether an address concerns about anonymity. Overall 65% of the addresses that are seriously concerned about anonymity are rich addresses and the remaining are poor addresses. Below, we explain the trends. 1). Initially, most of the addresses belong to miner and have high amount of Bitcoin. Virtually all transactions are created for mining purpose – transferring Bitcoin from one address to another. This explains why only rich addresses concern about anonymity at early stage. 2). From mid 2010 to mid 2011, the Bitcoin exchange rate starts to climb, more and more miners begin to merge Bitcoin (Case I in Figure 10) in order to sell it for profits. That said, the swelling ratio of poor addresses from mid 2010 to mid 2011 in Figure 7 does not mean poor addresses concern more about anonymity. 3). The spike of Bitcoin exchange rate has also attracted hackers [65]. This encourages the rich addresses to start concerning about anonymity and security. Toward that goal, the rich users are likely to use new addresses as change addresses even in normal business transactions or simply split/combine Bitcoin to remain anonymous.

In summary, Figure 7 concludes that the rich addresses are more concerned about anonymity than the poor counterparts.

TABLE III: Hot wallets belonging to big organizations.

Tag	Address ID	Total inflow from other addresses	Bitcoin balance	Degree
Deepbit	1VayNert3x1KzbpzMGt2qdqrAThiRovi8	25467352.64	0.2	1565611
SatoshiDICE Hot Wallet	18uvwkMJsg9cxFEd1QDFgQpoeXWmmSnqSs	399678.8714	0.00053	414842
SatoshiDICE Hot Wallet	1MSzmVTBaaSpKDARK3VGvP8v7aCtwZ9zbw	386456.4036	0.00033	414270
SatoshiDICE Hot Wallet	1PeohaRGaTF8cSzDqP1yYfzDah66xiriEQ	384443.0361	0.00079806	413407
SatoshiDICE Hot Wallet	1Bd5wrFxHYRkk4UCFttcPNMYzqJnQKfXUE	383879.8434	0.05339999	415362
SatoshiDICE Hot Wallet	15fXdTyFL1p53qQ8NkrjBqPUbPWvWmZ3G9	383444.5918	0.00028	415042
FoxBit Hot Wallet	1FoxBitjXcBeZUS4eDzPZ7b124q3N7QJK7	156329.1069	0.04314468	560202
Unknown	13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	17600542.04	0.00306531	1011905
Unknown	19iVyH1qUxgywY8LJSbpV4VavjZmyuEyxV	9326468.877	0.00000651	430643

TABLE IV: Big organizations cold wallet addresses and other potential cold wallet addresses on June 7 2018.

Tags	Address Id	Bitcoin balance	Degree
wallet: Bitfinex-coldwallet	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	172236.0323	9065
wallet: Bittrex-coldwallet	16rCmCmbuWDhPjWTrpQGaU3EPdZF7MTdUk	117203.0673	213
wallet:Bitstamp-coldwallet	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v	97848.28321	238
wallet: Coincheck-coldwallet	336xGpGweq1wtY4kRTuA4w6d7yDkBU9czU	34276.54041	11007
Unknown	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	79957.17569	196
Unknown	16FSBGvQfy4K8dYvPPWWpmzgKM6CvrCoVy	35970.01951	865
Unknown	1AhTjUMztCihiTyA4K6E3QEpobjWLwKhkR	66378.8101	204

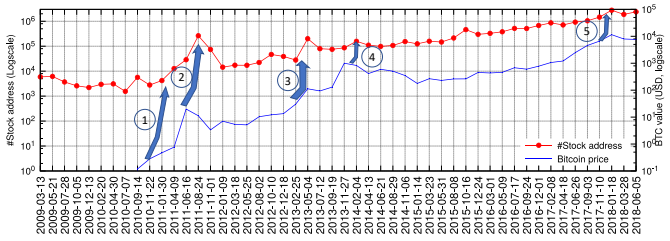

Fig. 8: Number of stock buyer with respect to the price of Bitcoin from the start of Bitcoin. There are a total of 17.8 million unspent addresses by June 7 2018.

VI. MicroScope Analysis

This section further studies the privacy concerns of those four types of addresses from Table II and concludes majority of them do not hide their intentions.

A. Stock Address

Since the day of its start, Bitcoin has experienced ups and downs in the exchange rate. Following typical jump-and-dump stock market phenomenon [21], this price fluctuation has attracted a number of Bitcoin stock buyers. In particular, stock buyers likely purchase Bitcoin, i.e., creating new Bitcoin addresses, at the climbing Bitcoin price as an investment, hoping this trend can bring in profits. In contrast, falling price will draw fewer investment, thus fewer Bitcoin addresses will be created by stock buyers.

Stock address features. Inspired by the aforementioned observation, we find the innate traits of the stock addresses are two folds: 1). They are those addresses that accumulate Bitcoins and don't spend (a.k.a. 0 out-degrees) 2). The amounts of emerging stock addresses are immediately influenced by the exchange rate of Bitcoin.

Figure 8 plots the dynamics of stock addresses and Bitcoin exchange rate. Based upon the first feature, we first obtain 21.7 million (21,747,636) addresses by June 7 2018 are non-zero balance addresses, ∼17.8 million of which are never used as inputs in any transactions. From Figure 8, one can easily notice the trend, peak and valley correlations between the amount of stock addresses and Bitcoin exchange rates. In particular, the exchange rate hikes of Bitcoin immediately added many new stock addresses. Such a close correlation is perfectly reflected by Figure 8, such as the highlighted ① – ⑤. On price reduction during the start of 2018, the number of the new stock addresses are also reduced. The number of addition of stock buyer almost remain constant during start to the mid of 2010 when the Bitcoin has almost no value.

Note, this analysis of stock address also contains some of the reported lost Bitcoin addresses which is caused by forgetting the wallets passwords, or simply discarding the wallets (storage containing private keys) when exchange rate is low. Whereas these cases only happen at the early stage when Bitcoin has very little value.

B. Key Addresses From Big Organization

Big Bitcoin organizations, e.g., exchange centers and gaming sites, often maintain a twin-address for business, that is, **hot wallet and cold wallet addresses** stemming from the security reasons. In particular, hot wallet addresses are used to receive/send Bitcoins. To avoid security breach [66], hot wallet addresses will transfer their amassed Bitcoin to cold wallet addresses. Suggested by its name, cold wallet addresses maintain their private key offline for security purposes. When hot wallets run out of Bitcoin, cold wallet will transfer some Bitcoin back to maintain the business.

Hot wallet addresses often come with three features. 1). The hot wallet addresses of big organizations normally have extremely high in- and out- degrees. 2). The amount of Bitcoin flowing through these hot wallet addresses is extremely high. However, 3). The balance of hot wallet addresses is low.

These three-pronged features can be instantiated as $degree \geq 50,000$, $flow \geq 150,000 BTC$ and $balance \leq 10 BTC$ at June 7 2018. As shown in the bottom of Table III, we retain, in total, 60 addresses, 31 of which are tagged as hot

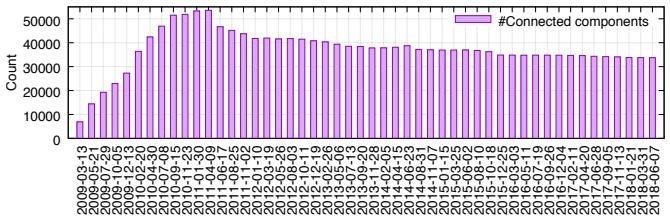

Fig. 9: Number of connected components over period of time.

wallets from [23]. Most of these hot wallet addresses belong to the organizations like mining pools, gambling sites and the exchange centers. Some of the addresses are untagged but present similar characteristics as the tagged ones. This implies that these untagged ones should also be hot wallets from some big organizations, except that these organizations attempt to hide the ownership. Now, our analysis can help uncover them.

Cold wallet addresses also come with three potential features. 1). Cold wallet addresses will be close, in terms of edge distance, to hot wallet addresses. 2). Cold wallet addresses should govern comparably smaller degrees than the hot wallet addresses they link to. 3). The balance of cold wallet addresses will be high.

Table IV, which follows the above extracted features, identities seven cold wallet addresses. In particular, we conduct the BFS traversal with depth of two from some of the hot wallet addresses and filter out the vertices whose accumulated Bitcoin is greater than 10,000 BTC. The degree of the cold wallets are relatively lower than that of the hot wallet addresses. As expected, four out of those seven cold wallets are tagged as cold wallets by [24]. Again, we also capture some suspicious cold wallets that are untagged. Again, regardless whether this is intentionally or unintentionally untagged, our tool can help unveil similar cold wallet addresses.

C. Miner Address

Of all the critical addresses, miner address presents the most distinguishable feature. That is, a transaction without input addresses will be the rewarding transaction. And the output addresses from those transactions are the miner addresses. This nature yields an interesting graph relevant phenomenon – the transaction and output address vertices may yield a new connected components as long as the output address is disconnected from prior connected components.

Figure 9 thus studies the #connected components in Bitcoin transaction graph. In particular, the count increases from the beginning, reaches peak at around April of 2011 and gradually comes to a stable number of around 34,000. The connected component count soars before 2011 because the almost negligible Bitcoin exchange rate leads to the mined Bitcoins left unused. But after the establishment of exchange centers around 2010 (Mt. Gox) and 2011 (BTCChina, BTC-e) [61], these inactive connected components spring back to transacting with the main connected components (most likely selling Bitcoins to exchange centers), causing the number of connected components in the graph to shrink till today.

A closer look at miner address, as shown in Figure 10 which presents the **real intentions** of several miner addresses, further

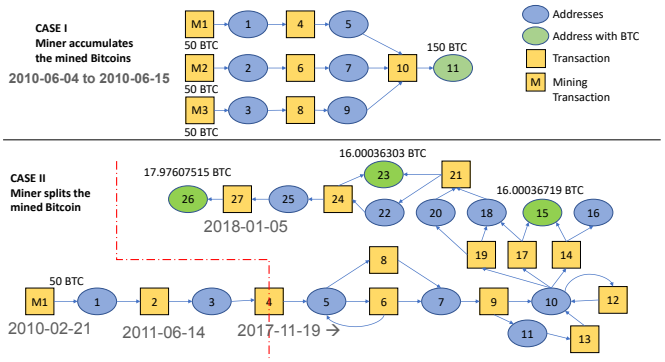

Fig. 10: Miner behavior dynamics from 2010 to 2018. In particular, Case I: Miner accumulates the mined Bitcoin. Case II: Miner splits the mined Bitcoin.

extracts two interesting facts. In Case I[2] , where the Bitcoin is untouched since 2010, the miner accumulates its three mined Bitcoin addresses into one address. Back in 2010 the rate of Bitcoins is low, this behavior is perceived as merging Bitcoin for ease of management. In Case II[3], we notice the miner is dividing the rewards into smaller amounts of more new addresses. Even though for the Bitcoin that is mined back in 2010, we observe division of them in December 2017 which is the time of peak Bitcoin exchange rate. This shows that the anonymity and security concern is strongly correlated to exchange rate.

VII. Conclusion

This paper examines the Bitcoin transaction graphs to answer two critical yet unanswered questions concerning anonymity and privacy: *Do typical Bitcoin users care about anonymity? Do critical users care about anonymity?* The first analysis is a macroscope investigation and finds majority of the addresses enjoy the remarkable simplicity of Bitcoin and disregard the anonymity concerns. The second exploration arrives at the conclusion that the hot wallets, Bitcoin stock buyer and miner addresses are, also, not caring about anonymity on the basis of their intention. In conclusion, the value of the Bitcoin (i.e., amount and rate) governs whether Bitcoin users concern about anonymity.

Acknowledgment

We thank the anonymous reviewers, Hans-Edward Hoene and Zhenlin Wu for their helpful suggestions. We gracefully acknowledge the support from XSEDE supercomputers and Amazon AWS, as well as NVIDIA Corporation for the donation of the Titan Xp and Quadro P6000 GPUs. Yan Luo is supported in part by the US National Science Foundation (No. 1547428, No. 1541434, No. 1738965, and No. 1450996).

[2]Mining transactions:
fa796ffd60affebb030d7ff8e81474ceb7e3fba91e92235f809469e434025f1b,
e9e2747a9a10db68912d3215a4fda1a5ff0d4c018928851ac5f8e0e80d0c091c,
c43ed2ff2dbc51f7c677ce88c416050e13e892707bd12738a1f68bdd81226c3e

[3]Mining transactions:
089bf008a36a182f816498f3f15aa56885dda745b678d8f9fd7f51b05aab502f

REFERENCES

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Danton Bryans. Bitcoin and money laundering: mining for an effective solution. *Ind. LJ*, 89:441, 2014.

[3] Rebecca S Portnoff, et al. Backpage and bitcoin: Uncovering human traffickers. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1595–1604. ACM, 2017.

[4] Malte Moser, et al. An inquiry into money laundering tools in the bitcoin ecosystem. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–14. IEEE, 2013.

[5] Bitiodine github. Available at https://github.com/mikispag/bitiodine.

[6] Michele Spagnuolo, et al. Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security*, pages 457–468. Springer, 2014.

[7] Alex Biryukov, et al. Deanonymisation of clients in bitcoin p2p network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 15–29. ACM, 2014.

[8] Philip Koshy, et al. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*, pages 469–485. Springer, 2014.

[9] Philip Koshy. Coinseer: A telescope into bitcoin. 2013.

[10] Sarah Meiklejohn, et al. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.

[11] Fergal Reid et al. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[12] Mikkel Alexander Harlev, et al. Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[13] Shaileshh Bojja Venkatakrishnan, et al. Dandelion: Redesigning the bitcoin network for anonymity. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 1(1):22, 2017.

[14] Tim Ruffing, et al. Coinshuffle: Practical decentralized coin mixing for bitcoin. In *European Symposium on Research in Computer Security*, pages 345–364. Springer, 2014.

[15] Joseph Bonneau, et al. Mixcoin: Anonymity for bitcoin with accountable mixes. In *International Conference on Financial Cryptography and Data Security*, pages 486–504. Springer, 2014.

[16] Gregory Maxwell. Coinjoin: Bitcoin privacy for the real world, 2013. Available at https://bitcointalk.org/?topic=279249.

[17] joinmarket github repository. Available at https://github.com/gcarq/rusty-blockparser.

[18] DashCoin, Anonymous peer-to-peer Internet currency. Available at http://dashcoin.info/.

[19] MONERO, Private Digital Currency. Available at https://getmonero.org/.

[20] Hang Liu, et al. ibfs: Concurrent breadth-first search on gpus. In *Proceedings of the 2016 International Conference on Management of Data*, pages 403–416. ACM, 2016.

[21] Traders are talking up cryptocurrencies, then dumping them, costing other millions. Available at https://www.wsj.com/graphics/cryptocurrency-schemes-generate-big-coin/?mod=article_inline?mod=hp_lead_pos5.

[22] Benjamin Fabian, et al. Adoption of security and privacy measures in bitcoin–stated and actual behavior. *transactions (Barber et al. 2012, Brito and Castillo 2013)*, 8:20, 2018.

[23] Blockchain.com. Available at https://www.blockchain.com/.

[24] Bitinfo charts. Available at https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html.

[25] Bitcoin Core Software. Available at https://bitcoin.org/en/bitcoin-core/.

[26] Transaction confirmation condition. Available at https://en.bitcoin.it/wiki/Confirmation.

[27] Majority attack. Available at https://en.bitcoin.it/wiki/Majority_attack.

[28] Deepak Puthal, et al. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 7(4):6–14, 2018.

[29] Bitcoin wiki, *Anonymity*. Available at https://en.bitcoin.it/wiki/Anonymity. Accessed: 2018, August 9.

[30] Y Fanusie et al. Bitcoin laundering: an analysis of illicit flows into digital currency services. *Center on Sanctions & Illicit Finance memorandum, January*, 2018.

[31] Silk road , *(marketplace)*. Available at https://en.wikipedia.org/wiki/Silk_Road_(marketplace). Accessed: 2018, August 14.

[32] Mt. gox. Available at https://en.wikipedia.org/wiki/Mt._Gox. Accessed: 2018, August 14.

[34] Bitcoin stack exchange forum. Available at https://bitcoin.stackexchange.com/.

[33] Bitcoin forum. Available at https://bitcointalk.org/index.php?board=1.0.

[35] Bitcoin discussion forum. Available at https://forum.bitcoin.com/bitcoin-discussion//.

[36] Bitcoin investing forum. Available at https://www.investing.com/crypto/bitcoin/chat/.

[37] Michael Fleder, et al. Bitcoin transaction graph analysis. *arXiv preprint arXiv:1502.01657*, 2015.

[38] Wikileaks. Available at https://wikileaks.org/. Accessed: 2018, August 14.

[39] Dorit Ron et al. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*, pages 6–24. Springer, 2013.

[40] Dorit Ron et al. How did dread pirate roberts acquire and protect his bitcoin wealth? In *International Conference on Financial Cryptography and Data Security*, pages 3–15. Springer, 2014.

[41] Marc Santamaria Ortega. *The bitcoin transaction graph—anonymity*. PhD thesis, Master's thesis, Universitat Oberta de Catalunya, 2013.

[42] Micha Ober, et al. Structure and anonymity of the bitcoin transaction graph. *Future internet*, 5(2):237–250, 2013.

[43] AddressReuse. Available at https://en.bitcoin.it/wiki/Address_reuse.

[44] Jaume Barcelo. User privacy in the public bitcoin blockchain. *URL: http://www. dtic. upf. edu/˜ jbarcelo/papers/20140704_User_Privacy_in_the_Public_Bitcoin_Blockchain/paper. pdf (Accessed 09/05/2016)*, 2014.

[45] Benjamin Fabian, et al. Anonymity in bitcoin?–the users' perspective. 2016.

[46] Shayan Eskandari, et al. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*, 2018.

[47] Bitcoin dust – what is it and why it should be eliminated?. Available at https://cryptodaily.co.uk/2018/04/bitcoin-dust-eliminated/. Accessed: 2018, August 15.

[48] Why bitcoin exchanges keep getting hacked — and how to protect yourself. Available at https://www.washingtonpost.com/news/the-switch/wp/2018/06/20/why-bitcoin-exchanges-keep-getting-hacked-and-how-to-protect-yourself/?noredirect=on&utm_term=.9585a3079c23.

[49] Rusty blockparser github repository. Available at https://github.com/JoinMarket-Org/joinmarket.

[50] Bipartite graph. Available at https://en.wikipedia.org/wiki/Bipartite_graph/.

[51] Graph project start. Available at https://github.com/asherliu/graph_project_start. Accessed: 2018, August 14.

[52] The extreme science and engineering discovery environment(xsede). Available at https://www.xsede.org/.

[53] Lustre. Available at http://lustre.org/. Accessed: 2018, August 14.

[54] Connected Component (graph theory). Available at https://en.wikipedia.org/wiki/Connected_component_(graph_theory).

[55] Distance-Diameter (graph theory). Available at https://en.wikipedia.org/wiki/Distance_(graph_theory).

[56] Directed Graph-Indegree (graph theory). Available at https://en.wikipedia.org/wiki/Directed_graph.

[57] Flow Network (graph theory). Available at https://en.wikipedia.org/wiki/Flow_network.

[58] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[59] Jure Leskovec, et al. Graph evolution: Densification and shrinking diameters. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 1(1):2, 2007.

[60] David Dinkins. Bitcoin owes success to three different waves of innovators. Available at https://cointelegraph.com/news/bitcoin-owes-success-to-three-different-waves-of-innovators. Accessed: 2018, August 15.

[61] Bitcoin Exchange Centers. Available at https://www.investopedia.com/articles/investing/111914/look-most-popular-bitcoin-exchanges.asp.

[62] Bitcoin Exchange Rates. Available at https://www.blockchain.com/en/charts/market-price?timespan=all.

[63] Steve Fiorillo. How to make your bitcoin an investment. Available at https://www.thestreet.com/investing/bitcoin/how-to-invest-in-bitcoin-14551377/. Accessed: 2018, August 15.

[64] Dániel Kondor, et al. Do the rich get richer? an empirical analysis of the bitcoin transaction network. *PloS one*, 9(2):e86197, 2014.

[65] Timothy B. Lee. A brief history of Bitcoin hacks and frauds. Available at https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/.

[66] Bitcoin price plunges after cryptocurrency exchange is hacked. Available at https://www.theguardian.com/technology/2018/jun/11/bitcoin-price-cryptocurrency-hacked-south-korea-coincheck.