An Analysis of Anonymity in the Bitcoin System

Fergal Reid and Martin Harrigan

Abstract Anonymity in Bitcoin, a peer-to-peer electronic currency system, is a complicated issue. Within the system, users are identified only by public-keys. An attacker wishing to de-anonymize users will attempt to construct the one-to-many mapping between users and public-keys, and associate information external to the system with the users. Bitcoin tries to prevent this attack by storing the mapping of a user to his or her public-keys on that user's node only and by allowing each user to generate as many public-keys as required. In this chapter we consider the topological structure of two networks derived from Bitcoin's public transaction history. We show that the two networks have a non-trivial topological structure, provide complementary views of the Bitcoin system, and have implications for anonymity. We combine these structures with external information and techniques such as context discovery and flow analysis to investigate an alleged theft of Bitcoins, which, at the time of the theft, had a market value of approximately US$500,000.

Keywords Network analysis • Anonymity • Bitcoin

1 Introduction

Bitcoin is a peer-to-peer electronic currency system first described in a paper by Satoshi Nakamoto (a pseudonym) in 2008 [19]. It relies on digital signatures to prove ownership and a public history of transactions to prevent double-spending. The history of transactions is shared using a peer-to-peer network and is agreed upon using a proof-of-work system [3, 11].

F. Reid (✉) • M. Harrigan
Clique Research Cluster, Complex and Adaptive Systems Laboratory,
University College Dublin, Dublin, Ireland
e-mail: fergal.reid@gmail.com; martin.harrigan@ucd.ie

Y. Altshuler et al. (eds.), *Security and Privacy in Social Networks*,
DOI 10.1007/978-1-4614-4139-7_10,

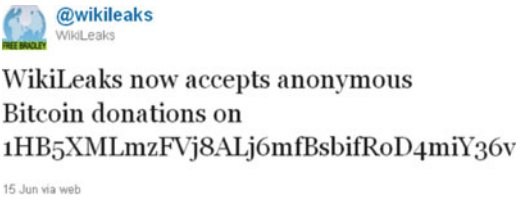

Fig. 1 Screen capture of a tweet from WikiLeaks announcing their acceptance of 'anonymous Bitcoin donations'

The first Bitcoins were transacted in January 2009, and by June 2011 there were 6.5 million Bitcoins in circulation among an estimated 10,000 users [27]. In recent months, the currency has seen rapid growth in both media attention and market price relative to existing currencies. At its peak, a single Bitcoin traded for more than US$30 on popular Bitcoin exchanges. At the same time, U.S. Senators and lobby groups in Germany, such as Der Bundesverband Digitale Wirtschaft (the Federal Association of Digital Economy), raised concerns regarding the untraceability of Bitcoins and their potential to harm society through tax evasion, money laundering and illegal transactions. The implications of the decentralized nature of Bitcoin with respect to the authorities' ability to regulate and monitor the flow of currency is as yet unclear.

Many users adopt Bitcoin for political and philosophical reasons, as much as pragmatic ones. There is an understanding amongst Bitcoin's more technical users that anonymity is not a primary design goal of the system; however, opinions vary widely as to how anonymous the system is in practice. Jeff Garzik, a member of Bitcoin's development team, is quoted as saying that it would be unwise "to attempt major illicit transactions with Bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement".[1] However, prior to the present work, no analysis of anonymity in Bitcoin was publicly available to substantiate or refute these claims. Furthermore, many other users of the system do not share this belief. For example, WikiLeaks, an international organization for anonymous whistleblowers, recently advised its Twitter followers that it now accepts *anonymous* donations via Bitcoin (see Fig. 1) and states the following[2]:

> Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are [sic] safer and faster alternative to other donation methods.

They proceed to describe a more secure method of donating Bitcoins that involves the generation of a one-time public-key but the implications for those who donate using the tweeted public-key are unclear. Is it possible to associate a donation with other Bitcoin transactions performed by the same user or perhaps identify them using external information? The extent to which this anonymity holds in the face of determined analysis remains to be tested.

[1] http://www.theatlantic.com/technology/archive/2011/06/libertarian-dream-a-site-where-you-buy-drugs-with-digital-dollars/239776 –Retrieved 2011-11-12.

[2] http://wikileaks.org/support.html – Retrieved: 2011-07-22.

This chapter is organized as follows. In Sect. 2 we consider some existing work relating to electronic currencies and anonymity. The economic aspects of the system, interesting in their own right, are beyond the scope of this work. In Sect. 3 we present an overview of the Bitcoin system; we focus on three features that are particularly relevant to our analysis. In Sect. 4 we construct two network structures, the transaction network and the user network using the publicly available transaction history. We study the static and dynamic properties of these networks. In Sect. 5 we consider the implications of these network structures for anonymity. We also combine information external to the Bitcoin system with techniques such as flow and temporal analysis to illustrate how various types of information leakage can contribute to the de-anonymization of the system's users. Finally, we conclude in Sect. 6.

1.1 A Note Regarding Motivation and Disclosure

Our motivation for this analysis is not to de-anonymize individual users of the Bitcoin system. Rather, it is to demonstrate, using a passive analysis of a publicly available dataset, the inherent limits of anonymity when using Bitcoin. This will ensure that users do not have expectations that are not being fulfilled by the system.

In security-related research, there is considerable disagreement over how best to disclose vulnerabilities [7]. Many researchers favor full disclosure wherein all information regarding a vulnerability is promptly released. This enables informed users to promptly take defensive measures. Other researchers favor limited disclosure; while this provides attackers with a window in which to exploit uninformed users, a mitigation strategy can be prepared and implemented before public announcement, thus limiting damage (e.g. through a software update). Our analysis illustrates some potential risks and pitfalls with regard to anonymity in the Bitcoin system. However, there is no central authority that can fundamentally change the system's behavior. Furthermore, it is not possible to prevent analysis of the existing transaction history.

There are also two noteworthy features of the dataset when compared to contentious social network datasets (e.g. the Facebook profiles of Harvard University students) [18]. First, the delineation between what is considered public and private is clear: the entire history of Bitcoin transactions is publicly available. Secondly, the Bitcoin system does not have a usage policy. After joining Bitcoin's peer-to-peer network, a client can freely request the entire history of Bitcoin transactions; no crawling or scraping is required.

Thus, we believe the best strategy to minimize the threat to user anonymity is to be descriptive about the risks of the Bitcoin system. We do not identify individual users apart from those in the case study, but we note that it is not difficult for other groups to replicate our work. Indeed, given the passive nature of our analysis, other parties may already be conducting similar analyses.

2 Related Work

2.1 Electronic Currencies

Electronic currencies can be technically classified according to their mechanisms for establishing ownership, protecting against double-spending, ensuring anonymity and/or privacy, and generating and issuing new currency. Bitcoin is particularly noteworthy for the last of these mechanisms. The proof-of-work system [3, 11] that establishes consensus regarding the history of transactions also doubles as a minting mechanism. The scheme was first outlined in the B-Money Proposal [10]. We briefly consider some alternative mechanisms in this section. Ripple [12] is an electronic currency wherein every user can issue currency. However, the currency is only accepted by peers who trust the issuer. Transactions between arbitrary pairs of users require chains of trusted intermediaries between the users. Saito [24] formalized and implemented a similar system, i-WAT, in which the chain of intermediaries can be established without their immediate presence using digital signatures. KARMA [28] is an electronic currency wherein the central authority is distributed over a set of users that are involved in all transactions. PPay [30] is a micropayment scheme for peer-to-peer systems in which the issuer of the currency is responsible for keeping track of it. However, both KARMA and PPay can incur large overhead when the rate of transactions is high. Mondex is a smart-card electronic currency [26]. It preserves a central bank's role in the generation and issuance of electronic currency. Mondex was an electronic replacement for cash in the physical world whereas Bitcoin is an electronic analog of cash in the online world.

The authors are not aware of any studies of the network structure of electronic currencies. However, there are such studies of physical currencies. The community currency Tomamae-cho was introduced into the Hokkaido Prefecture in Japan for a 3-month period during 2004–2005 in a bid to revitalize the local economy. The Tomamae-cho system involved gift-certificates that were re-usable and legally redeemable into yen. There was an entry space on the reverse side of each certificate for recipients to record transaction dates, their names and addresses, and the purposes of use, up to a maximum of five recipients. Kichiji and Nishibe [16] used the collected certificates to derive a network structure that represented the flow of currency during the period. They showed that the cumulative degree distribution of the network obeyed a power-law distribution, the network had small-world properties (the average clustering coefficient was high whereas the average path length was low), the directionality and the value of transactions were significant features, and the double-triangle system [22] was effective. Studies have also been performed on the physical movement of currency: "Where's George?" [29] is a crowd-sourced method for tracking U.S. dollar bills in which users record the serial numbers of bills in their possession, along with their current location. If a bill is recorded sufficiently often, its geographical movement can be tracked over time. Brockmann et al. [6] used

this dataset as a proxy for studying multi-scale human mobility and as a tool for computing geographic borders inherent to human mobility.

Grinberg [13] considered some of the legal issues that may be relevant to Bitcoin in the United States. For example, does Bitcoin violate the Stamp Payments Act of 1862? The currency can be used as a token for "a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States". However, the authors of the act could not have conceived of digital currencies at the time of its writing and therefore Bitcoin may not fall under its scope. Grinberg believes that Bitcoin is unlikely to be a security, or more specifically an "investment contract", and therefore does not fall under the Securities Act of 1933. He also believes that the Bank Secrecy Act of 1970 and the Money Laundering Control Act of 1986 pose the greatest risk for Bitcoin developers, exchanges, wallet providers, mining pool operators, and businesses that accept Bitcoins. These acts require certain kinds of financial businesses, even if they are located abroad, to register with a bureau of the United States Department of the Treasury known as the Financial Crimes Enforcement Network (FinCEN). The legality of Bitcoin is outside the scope of our work, but is interesting nonetheless.

2.2 *Anonymity*

Previous work has shown the difficulty in maintaining anonymity in the context of networked data and online services that expose partial user information. Narayanan and Shmatikov [21] and Backstrom et al. [4] considered privacy attacks that identify users using the structure of networks, and showed the difficulty in guaranteeing anonymity in the presence of network data. Crandall et al. [9] infer social ties between users where none are explicitly stated by looking at patterns of "coincidences" or common off-network co-occurrences. Gross and Acquisiti [14] discuss the privacy of early users in the Facebook social network, and how information from multiple sources could be combined to identify pseudonymous network users. Narayanan and Shmatikov [20] de-anonymized the Netflix Prize dataset using information from IMDB[3] that had similar user content, showing that statistical matching between different but related datasets can be used to attack anonymity. Puzis et al. [23] simulated the monitoring of a communications network using strategically-located monitoring nodes. They showed that, using real-world network topologies, a relatively small number of nodes could collaborate to pose a significant threat to anonymity. Korolova et al. [17] studied strategies for efficiently compromising network nodes to maximize link information

[3] http://www.imdb.com

observed. Altshuler et al. [1] discussed the increasing dangers of attacks targeting similar types of information, and provided measures of the difficulty of such attacks, on particular networks. All of this work points to the difficulty in maintaining anonymity where network data on user behavior is available, and illustrates how seemingly minor information leaks can be aggregated to pose significant risks. Security researcher Dan Kaminsky independently performed an investigation of some aspects of anonymity in the Bitcoin system, and presented his findings at a security conference [15] shortly after an initial draft of our work was made public. He investigated the 'linking problem' that we analyze and describe in Sect. 4.2. In addition to the analysis we conducted, his work investigated the Bitcoin system from an angle we did not consider – the TCP/IP operation of the underlying peer-to-peer network. Kaminsky's TCP/IP layer findings strengthen the core claims of our work that Bitcoin does not anonymise user activity. We provide a summary of Kaminsky's findings in Sect. 5.2.

3 The Bitcoin System

The following is a simplified description of the Bitcoin system (see Nakamoto [19] for a more thorough treatment). Bitcoin is an electronic currency with no central authority or issuer. There is no central bank or fractional reserve system controlling the supply of Bitcoins. Instead, they are generated at a predictable rate such that the eventual total number will be 21 million. There is no requirement for a trusted third-party when making transactions. Suppose Alice wishes to 'send' a number of Bitcoins to Bob. Alice uses a Bitcoin client to join the Bitcoin peer-to-peer network. She then makes a public transaction or declaration stating that one or more identities that she controls (which can be verified using public-key cryptography), and which previously had a number of Bitcoins assigned to them, wishes to re-assign those Bitcoins to one or more other identities, at least one of which is controlled by Bob. The participants of the peer-to-peer network form a collective consensus regarding the validity of this transaction by appending it to the public history of previously agreed-upon transactions (the *block-chain*). This process involves the repeated computation of a cryptographic hash function so that the digest of the transaction, along with other pending transactions, and an arbitrary nonce, has a specific form. This process is designed to require considerable computational effort, from which the security of the Bitcoin mechanism is derived. To encourage users to pay this computational cost, the process is incentivized using newly generated Bitcoins and/or transaction fees, and so this whole process is known as *mining*.

In this chapter, three features of the Bitcoin system are of particular interest. First, the entire history of Bitcoin transactions is publicly available. This is necessary in order to validate transactions and to prevent double-spending in the absence of a central authority. The only way to confirm the absence of a previous transaction

is to be aware of all previous transactions. The second feature of interest is that a transaction can have multiple inputs and multiple outputs. An input to a transaction is either the output of a previous transaction or a sum of newly generated Bitcoins and transaction fees. A transaction frequently has either a single input from a previous larger transaction or multiple inputs from previous smaller transactions. Also, a transaction frequently has two outputs: one sending payment and one returning change. Third, the payer and payee(s) of a transaction are identified through public-keys from public-private key-pairs. However, a user can have multiple public-keys. In fact, it is considered good practice for a payee to generate a new public-private key-pair for every transaction. Furthermore, a user can take the following steps to better protect their identity: they can avoid revealing any identifying information in connection with their public-keys; they can repeatedly send varying fractions of their Bitcoins to themselves using multiple (newly generated) public-keys; and/or they can use a trusted third-party mixer or laundry. However, these practices are not universally applied.

The three aforementioned features, namely the public availability of Bitcoin transactions, the input-output relationship between transactions and the re-use and co-use of public-keys, provide a basis for two distinct network structures: the *transaction network* and the *user network*. The transaction network represents the flow of Bitcoins between *transactions* over time. Each vertex represents a transaction, and each directed edge between a source and a target represents an output of the transaction corresponding to a source that is an input to the transaction corresponding to the target. Each directed edge also includes a value in Bitcoins and a timestamp. The user network represents the flow of Bitcoins between *users* over time. Each vertex represents a user, and each directed edge between a source and a target represents an input-output pair of a single transaction wherein the input's public-key belongs to the user corresponding to the source and the output's public-key belongs to the user corresponding to the target. Each directed edge also includes a value in Bitcoins and a timestamp.

We gathered the entire history of Bitcoin transactions from the first transaction on January 3, 2009 up to and including the last transaction that occurred on July 12, 2011. We gathered the dataset using the Bitcoin client[4] and a modified version of Gavin Andresen's `bitcointools` project.[5] The dataset comprises 1,019,486 transactions between 1,253,054 unique public-keys. We describe the construction of the corresponding transaction and user networks, and their analyses, in the following sections. We will show that the two networks are complex, have non-trivial topological structure, provide complementary views of the Bitcoin system, and have implications for the anonymity of users.

[4] http://www.bitcoin.org

[5] http://github.com/gavinandresen/bitcointools

4 The Transaction and User Networks

4.1 The Transaction Network

The transaction network $\mathcal{T}$ represents the flow of Bitcoins between *transactions* over time. Each vertex represents a transaction and each directed edge between a source and a target represents an output of the transaction corresponding to the source that is an input to the transaction corresponding to the target. Each directed edge also includes a value in Bitcoins and a timestamp. It is straight-forward to construct $\mathcal{T}$ from our dataset.

Figure 2 shows an example sub-network of $\mathcal{T}$. t_1 is a transaction with one input and two outputs.[6] It was added to the block-chain on May 1, 2011. One of its outputs assigned 1.2 Bitcoins (BTC) to a user identified by the public-key pk_1.[7] The public-keys are not shown in Fig. 2. Similarly, t_2 is a transaction with two inputs and two outputs.[8] It was accepted on May 5, 2011. One of its outputs sent 0.12 BTC to a user identified by a different public-key, pk_2.[9] t_3 is a transaction with two inputs and one output.[10] It was accepted on May 5, 2011. Both of its inputs are connected to the two aforementioned outputs of t_1 and t_2. The only output of t_3 was redeemed by t_4.[11]

$\mathcal{T}$ has 974,520 vertices and 1,558,854 directed edges. The number of vertices is less than the total number of transactions in the dataset because we omit transactions that are not connected to at least one other transaction. The omitted transactions correspond to newly generated Bitcoins and transaction fees that are not yet redeemed. The network has neither multi-edges (multiple edges between the same pair of vertices in the same direction) nor loops. It is a directed acyclic graph (DAG) since the output of a transaction can never be an input (either directly or indirectly) to the same transaction.

Figure 3a shows a log–log plot of the cumulative degree distributions: the solid red curve is the cumulative degree distribution (in-degree and out-degree); the dashed green curve is the cumulative in-degree distribution; and the dotted blue curve is the cumulative out-degree distribution. We fitted power-law distributions of the form $p(x) \sim x^{-\alpha}$ for $x > x_{min}$ to the three distributions by estimating the parameters α and x_{min} using a goodness-of-fit (GoF) method [8]. Table 1 shows the estimates along

[6] The transactions and public-keys used in our examples exist in our dataset. The unique identifier for the transaction t_1 is 09441d3c52fa0018365fcd2949925182f6307322138773d52c201f5cc2bb5976. You can query the details of a transaction or public-key by examining Bitcoin's block-chain using, for example, the Bitcoin Block Explorer (http://www.blockexplorer.com).

[7] 13eBhR3oHFD5wkE4oGtrLdbdi2PvK3ijMC

[8] 0c4d41d0f5d2aff14d449daa550c7d9b0eaaf35d81ee5e6e77f8948b14d62378

[9] 19smBSUoRGmbH13vif1Nu17S63Tnmg7h9n

[10] 0c034fb964257ecbf4eb953e2362e165dea9c1d008032bc9ece5cebbc7cd4697

[11] f16ece066f6e4cf92d9a72eb1359d8401602a23990990cb84498cdbb93026402

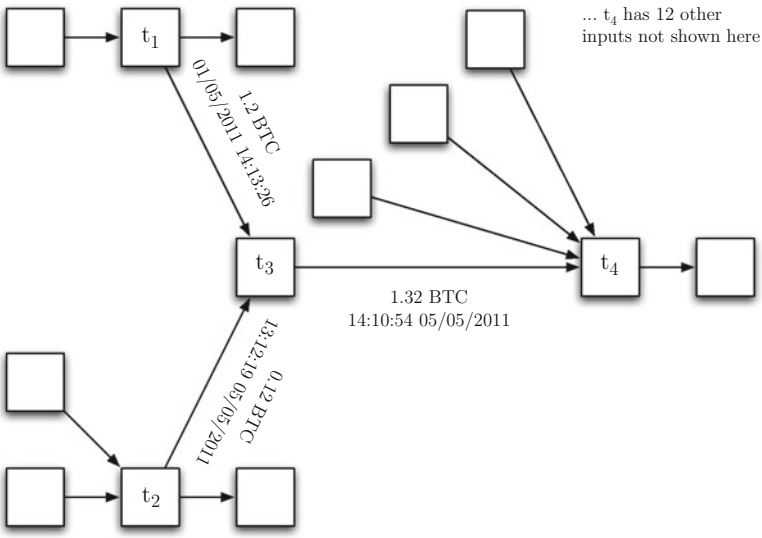

Fig. 2 An example sub-network from the transaction network. Each rectangular vertex represents a transaction and each directed edge represents a flow of Bitcoins from an output of one transaction to an input of another

with the corresponding Kolmogorov–Smirnov GoF statistics and p-values. We note that no distributions for which the empirically-best scaling region is non-trivial has a power-law as a plausible hypothesis ($p > 0.1$). This is probably due to the fact that there is no preferential attachment [5, 25]: new vertices are joined to existing vertices whose corresponding transactions are not yet fully redeemed.

There are 1,949 (maximal weakly) connected components in the network. Figure 3b shows a log–log plot of the cumulative component size distribution. There are 948,287 vertices (97.31%) in the giant component. This component also contains a giant biconnected component with 716,354 vertices (75.54% of the vertices in the giant component).

We also performed a rudimentary dynamic analysis of the network. Figure 3c–e show the edge number, density and average path length of the transaction network on a monthly basis, respectively. These measurements are not cumulative. The network's growth and sparsification are evident. We also note some anomalies in the average path length during July and November of 2010.

4.2 The User Network

The user network $\mathcal{U}$ represents the flow of Bitcoins between *users* over time. Each vertex represents a user. Each directed edge between a source and a target represents an input-output pair of a single transaction wherein the input's public-key

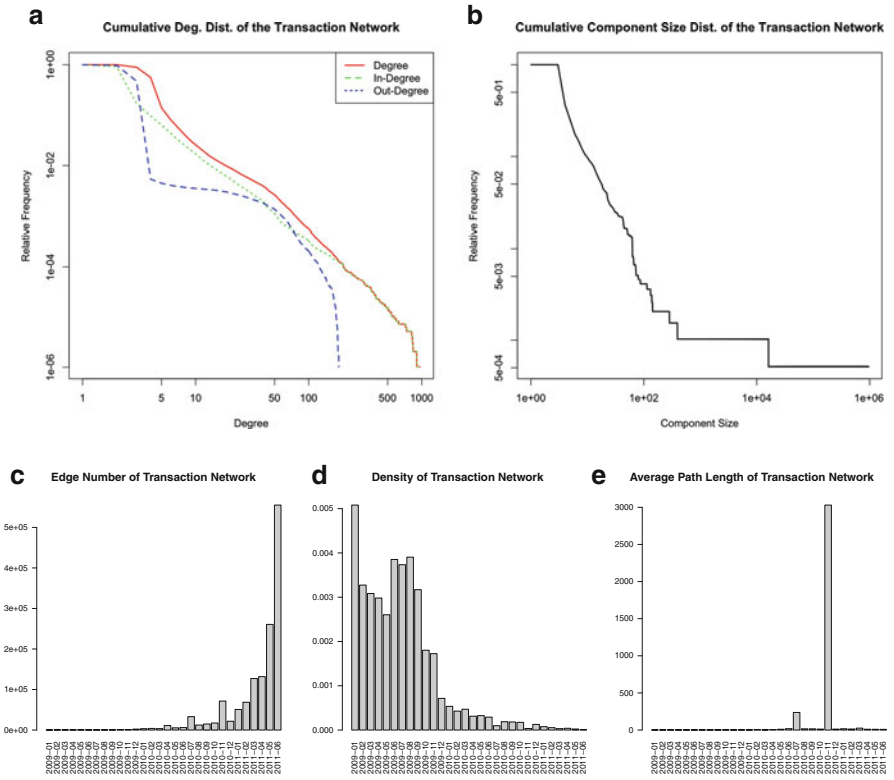

Fig. 3 Transaction network. (**a**) Log–log plot of the cumulative degree distributions. (**b**) Log–log plot of the cumulative component size distribution. (**c**) Temporal histogram showing the number of edges per month. (**d**) Temporal histogram showing the density per month. (**e**) Temporal histogram showing the average path length per month

Table 1 The degree, in-degree and out-degree distributions of $\mathcal{T}$

Variable	$\widetilde{x}$	$\bar{x}$	s	α	x_{min}	GoF	p-val.
Degree	3	3.20	6.20	3.24	50	0.02	0.05
In-degree	1	1.60	5.31	2.50	4	0.01	0.00
Out-degree	1	1.60	3.17	3.50	51	0.05	0.00

belongs to the user corresponding to the source and the output's public-key belongs to the user corresponding to the target. Each directed edge also includes a value in Bitcoins and a timestamp.

We must perform a preprocessing step before $\mathcal{U}$ can be constructed from our dataset. Suppose $\mathcal{U}$ is, at first, incomplete in the sense that each vertex represents a single public-key rather than a user and that each directed edge between a source and a target represents an input-output pair of a single transaction. In this case the input's public-key corresponds to the source and the output's public-key corresponds to the target. In order to perfect this network, we need to contract

each subset of vertices whose corresponding public-keys belong to a single user. The difficulty is that public-keys are Bitcoin's mechanism for ensuring anonymity: "the public can see that someone (identified by a public-key) is sending an amount to someone else (identified by another public-key), but without information linking the transaction to anyone." [19]. In fact, it is considered good practice for a payee to generate a new public-private key-pair for every transaction to keep transactions from being linked to a common owner. Therefore, it is impossible to completely perfect the network using our dataset alone. However, as noted by Nakamoto [19],

> Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

We will use this property of transactions with multiple inputs to contract subsets of vertices in the incomplete network. We constructed an ancillary network in which each vertex represents a public-key. We connected pairs of vertices with undirected edges where each edge joins a pair of public-keys that are both inputs to the same transaction and are thus controlled by the same user. From our dataset, this ancillary network has 1,253,054 vertices (unique public-keys) and 4,929,950 edges. More importantly, it has 86,641 non-trivial maximal connected components. Each maximal connected component in this graph corresponds to a user, and each component's constituent vertices correspond to that user's public-keys.

Figure 4 shows an example sub-network of the incomplete network overlaid onto the example sub-network of $\mathcal{T}$ from Fig. 2. The outputs of t_1 and t_2 that were eventually redeemed by t_3 were sent to a user whose public-key was pk_1 and a user whose public-key was pk_2 respectively. Figure 5 shows an example sub-network of the user network overlaid onto the example sub-network of the incomplete network from Fig. 4. pk_1 and pk_2 are contracted into a single vertex u_1 since they correspond to a pair inputs of a single transaction. In other words, they are in the same maximal connected component of the ancillary network (see the vertices representing pk_1 and pk_2 in the dashed grey box in Fig. 5). A single user owns both public-keys. We note that the maximal connected component in this case is not simply a clique; it has a diameter of length four indicating that there are at least two public-keys belonging to that same user that are connected indirectly via three transactions. The 16 inputs to transaction t_4 result in the contraction of 16 additional public-keys into a single vertex u_2. The value and timestamp of the flow of Bitcoins from u_1 to u_2 is derived from the transaction network.

After the preprocessing step, $\mathcal{U}$ has 881,678 vertices (86,641 non-trivial maximal connected components and 795,037 isolated vertices in the ancillary network) and 1,961,636 directed edges. The network is still incomplete. We have not contracted all possible vertices but this approximation will suffice for our present analysis. Unlike $\mathcal{T}$, $\mathcal{U}$ has multi-edges, loops and directed cycles.

Figure 6a shows a log–log plot of the network's cumulative degree distributions. We fitted power-law distributions to the three distributions and calculated their GoF

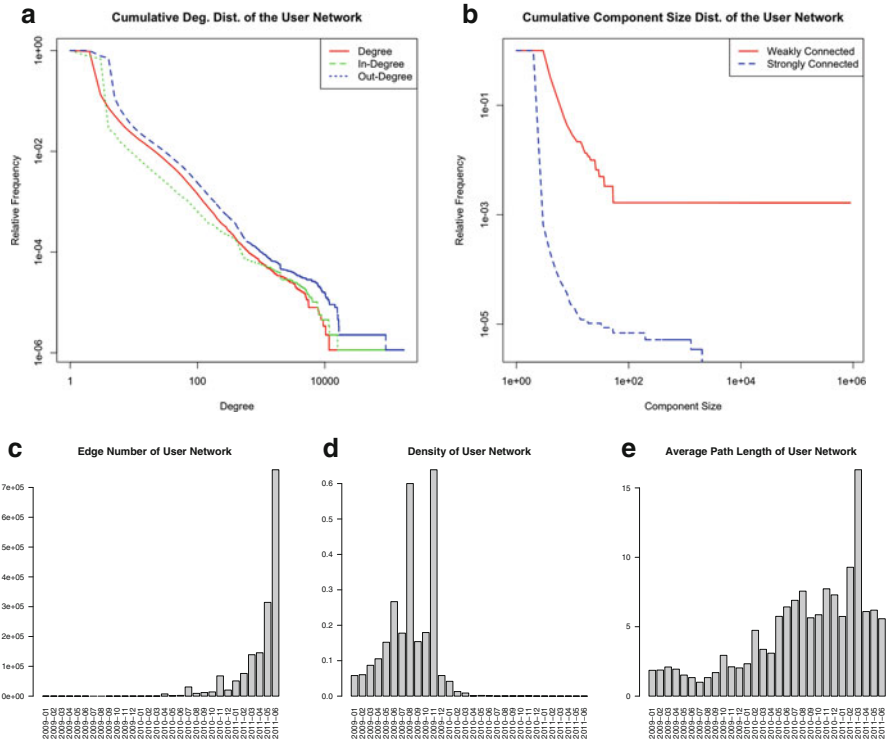

Fig. 4 User network. (**a**) Log–log plot of the cumulative degree distributions. (**b**) Log–log plot of the cumulative component size distribution. (**c**) Temporal histogram showing the number of edges per month. (**d**) Temporal histogram showing the density per month. (**e**) Temporal histogram showing the average path length per month

and statistical significance as in the previous section. Table 2 shows the results. We note that none of the distributions have a power-law as a plausible hypothesis.

There are 604 (maximal) weakly connected components and 579,355 (maximal) strongly connected components in the network; Fig. 6b shows a log–log plot of the cumulative component size distribution for both variations. There are 879,859 vertices (99.79%) in the giant weakly connected component. This component also contains a giant weakly biconnected component with 652,892 vertices (74.20% of the vertices in the giant component).

Our dynamic analysis of the user network mirrors that of the transaction network in the previous subsection. Figure 6c–e show the edge number, density and average path length of the user network on a monthly basis, respectively. These measurements are not cumulative. The network's growth and sparsification are evident. We note that even though our dynamic analysis of the user network was on a monthly basis, the preprocessing step was performed using the ancillary network of the entire incomplete network. This enables us to resolve public-keys to a single user irrespective of the month in which the linking transactions occur.

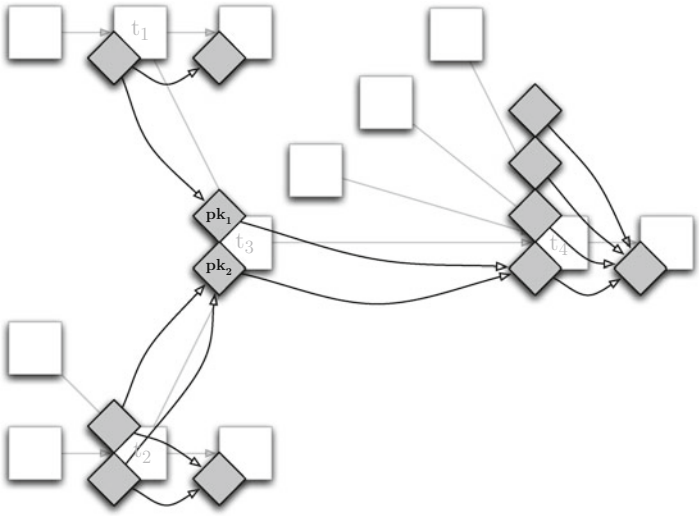

Fig. 5 An example sub-network from the incomplete network. Each diamond vertex represents a public-key and each directed edge between diamond vertices represents a flow of Bitcoins from one public-key to another

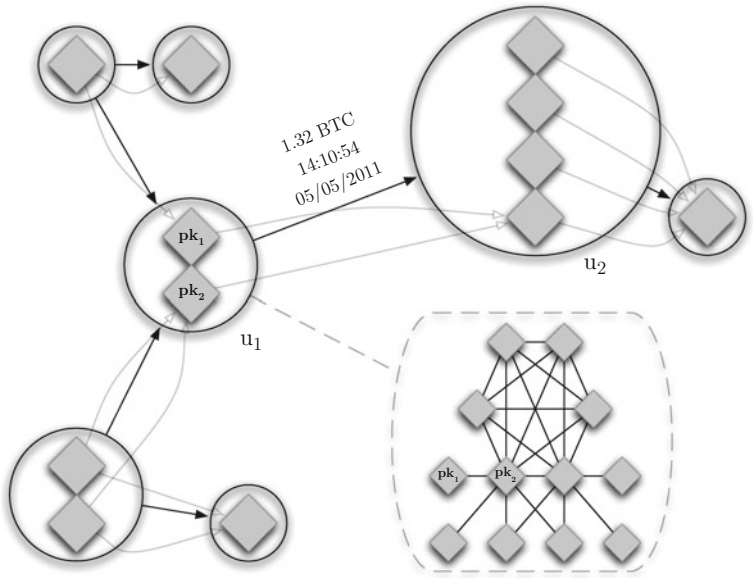

Fig. 6 An example sub-network from the user network. Each circular vertex represents a user and each directed edge between circular vertices represents a flow of Bitcoins from one user to another. The maximal connected component from the ancillary network that corresponds to the vertex u_1 is shown within the *dashed grey box*

Table 2 The degree, in-degree and out-degree distributions of $\mathcal{U}$

Variable	$\widetilde{x}$	$\bar{x}$	**s**	α	x_{min}	GoF	p-val.
Degree	3	4.45	218.10	2.38	66	0.02	0.00
In-degree	1	2.22	86.40	2.45	57	0.05	0.00
Out-degree	2	2.22	183.91	2.03	10	0.22	0.00

The contraction of public-keys into users, while incomplete, generates a network that is in many ways a proxy for the social network of Bitcoin users. The edges represent financial transactions between pairs of users. For example, it may be possible to identify communities, central users and hoarders within this social network.

5 Anonymity Analysis

Prior to performing the aforementioned analysis, we expected the user network to be largely composed of trees representing Bitcoin flows between one-time public-keys that were not linked to other public-keys. However, our analysis reveals that the user network has considerable cyclic structure. We now consider the implications of this structure, coupled with other aspects of the Bitcoin system, on anonymity.

There are several ways in which the user network can be used to deduce information about Bitcoin users. We can use global network properties, such as degree distribution, to identify outliers. We can use local network properties to examine the context in which a user operates by observing the users with whom he or she interacts, either directly or indirectly. The dynamic nature of the user network also enables us to perform flow and temporal analyses. In addition, we can examine the significant Bitcoin flows between groups of users over time. We will now discuss each of these possibilities in more detail and provide a case study to demonstrate their use in practice.

5.1 Integrating Off-Network Information

There is no user directory for the Bitcoin system. However, we can attempt to build a partial user directory associating Bitcoin users (and their known public-keys) with off-network information. If we can make sufficient associations and combine them with the previously described network structures, a potentially serious threat to anonymity emerges.

Many organizations and services (such as on-line stores) that accept Bitcoins, exchanges, laundry services and mixers have access to identifying information regarding their users; e.g. e-mail addresses, shipping addresses, credit card and bank account details, IP addresses, etc. If any of this information is publicly

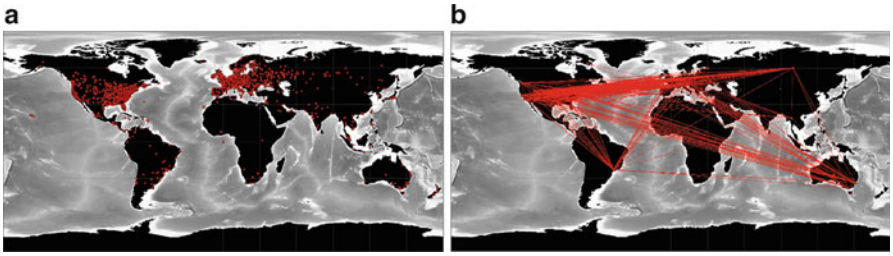

Fig. 7 The Bitcoin Faucet can be used to map users to geolocated IP addresses. (**a**) A map of geolocated IP addresses associated with users receiving Bitcoins from the Bitcoin Faucet during a 1-week period. (**b**) A map of a sample of the geolocated IP addresses in (**a**) connected by edges where the corresponding users are connected by a path of length at most three in the user network that does not include the vertex representing the Bitcoin Faucet

available, or accessible by, for example, law enforcement agencies, then the identities of users involved in related transactions may also be at risk. To illustrate this point, we consider a number of publicly available data sources and integrate their information with the user network.

5.1.1 The Bitcoin Faucet

The Bitcoin Faucet[12] is a website where users can donate Bitcoins to be redistributed in small amounts to other users. In order to prevent abuse of this service, a history of recent give-aways are published along with the IP addresses of the recipients. When the Bitcoin Faucet does not batch the re-distribution, it is possible to associate the IP addresses with the recipients' public-keys. This page can be scraped over time to produce a time-stamped mapping of IP addresses to Bitcoin users.

We found that the public-keys associated with many of the IP addresses that received Bitcoins were contracted with other public-keys in the ancillary network, thus revealing IP addresses that are related to previous transactions. Figure 7a shows a map of geolocated IP addresses belonging to users who received Bitcoins over a period of 1 week. Figure 7b overlays the user network onto a sample of those users. An edge between two geolocated IP addresses indicates that the corresponding users are linked by an undirected path with a length of at most three in the user network (after we exclude paths containing the Bitcoin Faucet itself).

These figures serve as a proof-of-concept from a small publicly available data source. We note that large centralized Bitcoin service providers are capable of producing much more detailed maps.

[12] http://freebitcoins.appspot.com

5.1.2 Voluntary Disclosures

Another source of identifying information is the voluntary disclosure of public-keys by users, for example when posting to the Bitcoin forums.[13] Bitcoin public-keys are typically represented as strings approximately 33 characters in length and starting with the digit one. They are well indexed by popular search engines. We identified many high-degree vertices with external information, using a search engine alone. We scraped the Bitcoin Forums in which users frequently attach a public-key to their signatures. We also gathered public-keys from Twitter streams and user-generated public directories. It is important to note that in many cases we are able to resolve the 'public' public-keys with other public-keys belonging to the same user, using the ancillary network. We also note that large centralized Bitcoin service providers can do the same with their user information.

5.2 TCP/IP Layer Information

Security researcher Dan Kaminsky performed an analysis of the Bitcoin system, and investigated identity leakage at the TCP/IP layer. He found that by opening a connection to all public peers in the network simultaneously, he could map IP addresses to Bitcoin public-keys, working from the assumption that "the first node to inform you of a transaction is the source of it. . .[this is] more or less true, and absolutely over time" [15]. Using this approach it is possible to map public-keys to IP addresses unless users are using an anonymising proxy technology such as TOR.

5.3 Egocentric Analysis and Visualization

For any particular user, we can directly derive several pieces of information from the user network. We can compute the balance held by a single public-key. We can also aggregate the balances belonging to public-keys that are controlled by a particular user. For example, Fig. 8a, b show the receipts and payments to and from WikiLeaks' public-key in terms of Bitcoins, and the number of transactions, respectively. The donations are relatively small and are forwarded to other public-keys periodically. There was also a noticeable spike in donations when the facility was first announced. Figure 8c shows the receipts and payments to and from the creator of a popular Bitcoin trading website aggregated over a number of public-keys that are linked through the ancillary network.

An important advantage of deriving network structures from the Bitcoin transaction history is the ability to use network visualization and analysis tools to investigate the flow of Bitcoins. For example, Fig. 9 shows the network structure

[13] http://forum.bitcoin.org

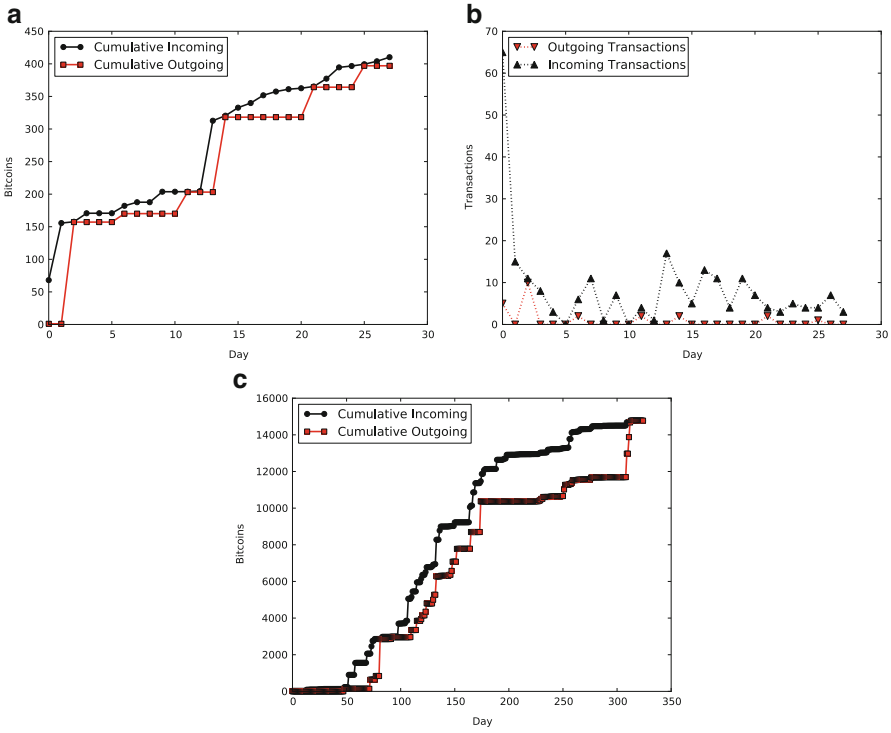

Fig. 8 Plot of cumulative receipts and payments to and from Bitcoin public-keys and users. (**a**) The receipts and payments to and from WikiLeaks' public-key over time. (**b**) The number of transactions involving WikiLeaks' public-key over time. (**c**) The receipts and payments to and from the creator of a popular Bitcoin trading website aggregated over a number of public-keys

surrounding the WikiLeaks public-key in the incomplete user network. Our tools resolve several of the vertices with identifying information described in Sect. 5.1. These users can be linked either directly or indirectly to their donations.

5.4 Context Discovery

Given a number of public-keys or users of interest, we can use network structure and context to better understand the flow of Bitcoins between them. For example, we can examine all shortest paths between a set of vertices, or consider the maximum number of Bitcoins that can flow from a source to a destination given the transactions and their 'capacities' in time-window of interest. For example, Fig. 10 shows all shortest paths between vertices representing the users we identified using off-network information in

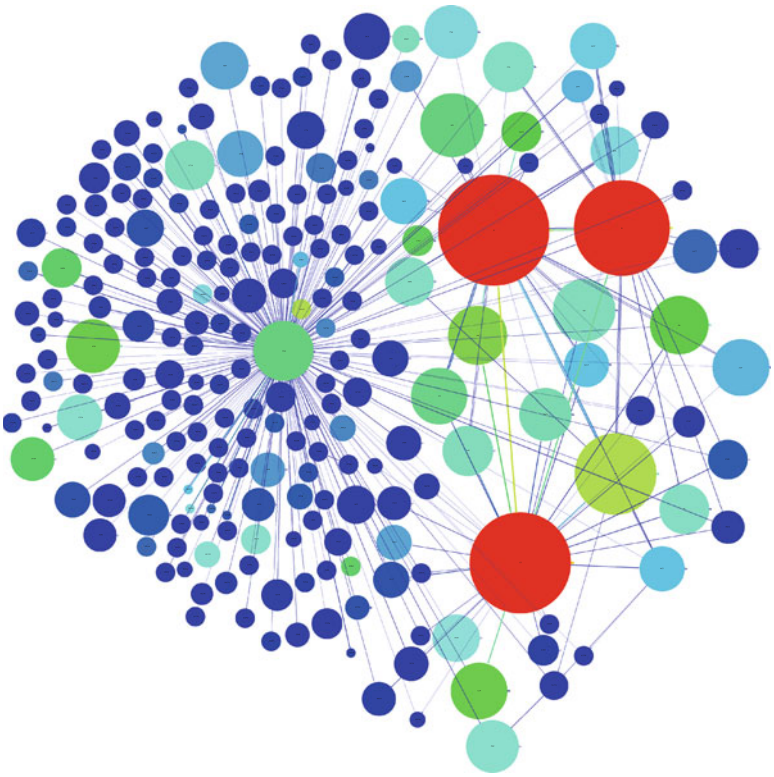

Fig. 9 An egocentric visualization of the vertex representing the WikiLeaks public-key in the incomplete user network. The size of a vertex corresponds to its degree in the entire incomplete user network. The *color* denotes the volume of Bitcoins – lighter colors have larger volumes flowing through them

Sect. 5.1, and the vertex that represents the MyBitcoin service[14] in the user network. We can identify more than 60% of the users in this visualization and deduce many direct and indirect relationships between them.

Case study-Part I : We analyzed an alleged theft of 25,000 BTC reported in the Bitcoin Forums[15] by a user known as `allinvain`. The victim reported that a large portion of his Bitcoins were sent to pk_{red}[16] on June 13, 2011 at 16:52:23 UTC. The theft occurred shortly after somebody broke into the victim's Slush pool account[17] and changed the payout address to pk_{blue}.[18] The Bitcoins rightfully belonged to

[14] http://www.mybitcoin.com

[15] http://forum.bitcoin.org/index.php?topic=16457.0

[16] 1KPTdMb6p7H3YCwsyFqrEmKGmsHqe1Q3jg

[17] http://mining.bitcoin.cz

[18] 15iUDqk6nLmav3B1xUHPQivDpfMruVsu9f

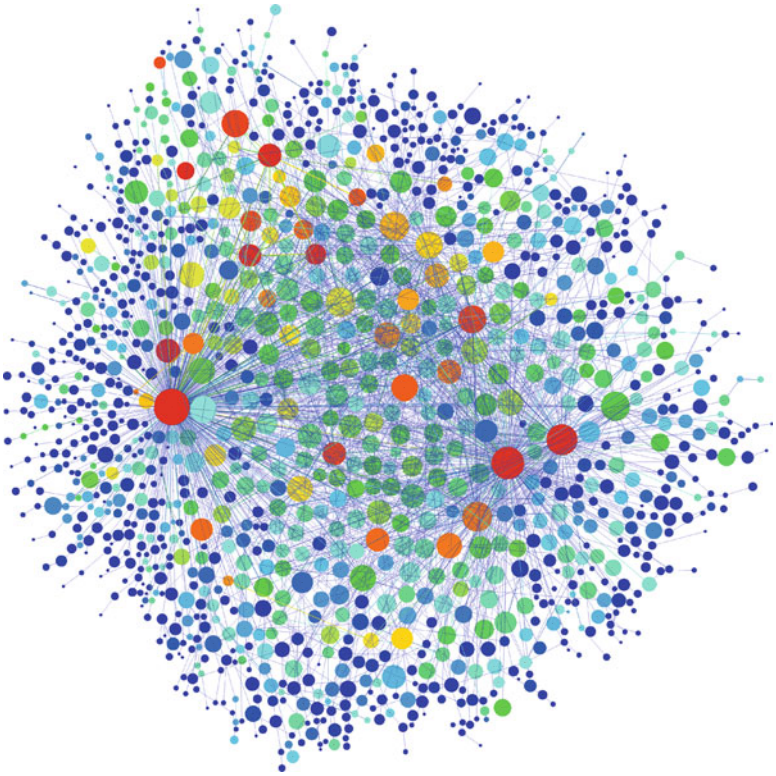

Fig. 10 A visualisation of all users identified in Sect. 5.1 and all shortest paths between the *vertices* representing those users and the *vertex* representing the MyBitcoin service in the user network

pk_{green}.[19] At the time of the theft, the stolen Bitcoins had a market value of approximately US$500,000. This case study illustrates potential risks to the anonymity of a user (the thief) who has good reason to remain anonymous.

We considered the incomplete user network before any contractions. We restricted our analysis to the egocentric network surrounding the thief: we include every vertex reachable by a path of length at most two, ignoring directionality and all edges induced by these vertices. To avoid clutter, we also removed all loops, multiple edges, and edges that were not contained in some biconnected component. In Fig. 11, the red vertex represents the thief who owns the public-key pk_{red} and the green vertex represents the victim who owns the public-key pk_{green}. The theft is represented by a green edge joining the victim to the thief.

Interestingly, the victim and thief are joined by paths (ignoring directionality) other than the green edge representing the theft. For example, consider the

[19] 1J18yk7D353z3gRVcdbS7PV5Q8h5w6oWWG

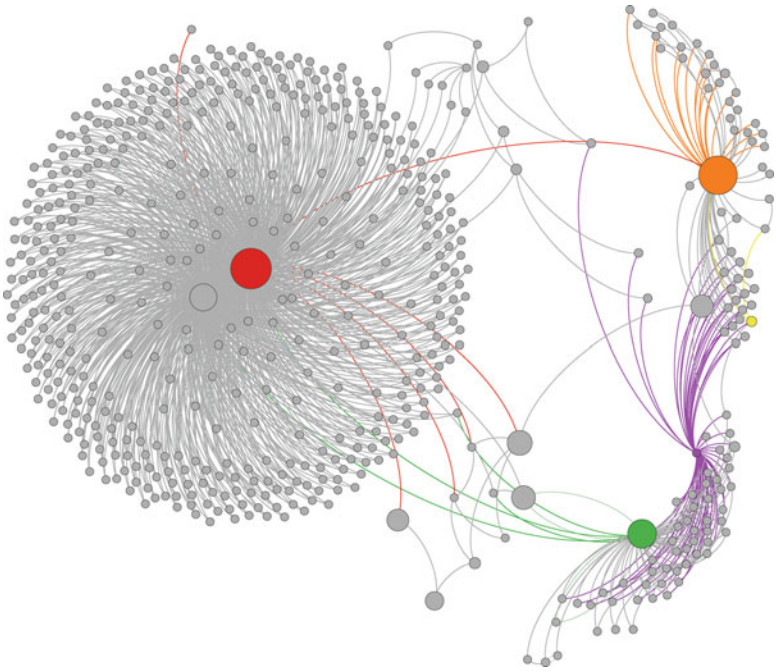

Fig. 11 An egocentric visualization of the thief in the incomplete user network. For this visualization, vertices are colored according to the text, edges are colored according to the color of their sources and the size of each vertex is proportional to its edge-betweenness within the egocentric network

sub-network shown in Fig. 12 induced by the red, green, purple, yellow and orange vertices. This sub-network is a cycle. We contract all vertices whose corresponding public-keys belong to the same user. This allows us to attach values in Bitcoins and timestamps to the directed edges. We can make a number of observations. First, we note that the theft of 25,000 BTC was preceded by a smaller theft of 1 BTC. This was later reported by the victim using the Bitcoin forums. Second, using off-network data, we identified some of the other colored vertices: the purple vertex represents the main Slush pool account, and the orange vertex represents the computer hacker group known as LulzSec.[20] We note that there has been at least one attempt to associate the thief with LulzSec.[21] This was a fake; it was created after the theft. However, the identification of the orange vertex with LulzSec is genuine and was established before the theft. We observe that the thief sent 0.31337 BTC to LulzSec shortly after the theft but we cannot otherwise associate him with the group. The main Slush pool account sent a total of 441.83 BTC to the victim

[20] http://twitter.com/LulzSec/status/76388576832651265

[21] http://pastebin.com/88nGp508

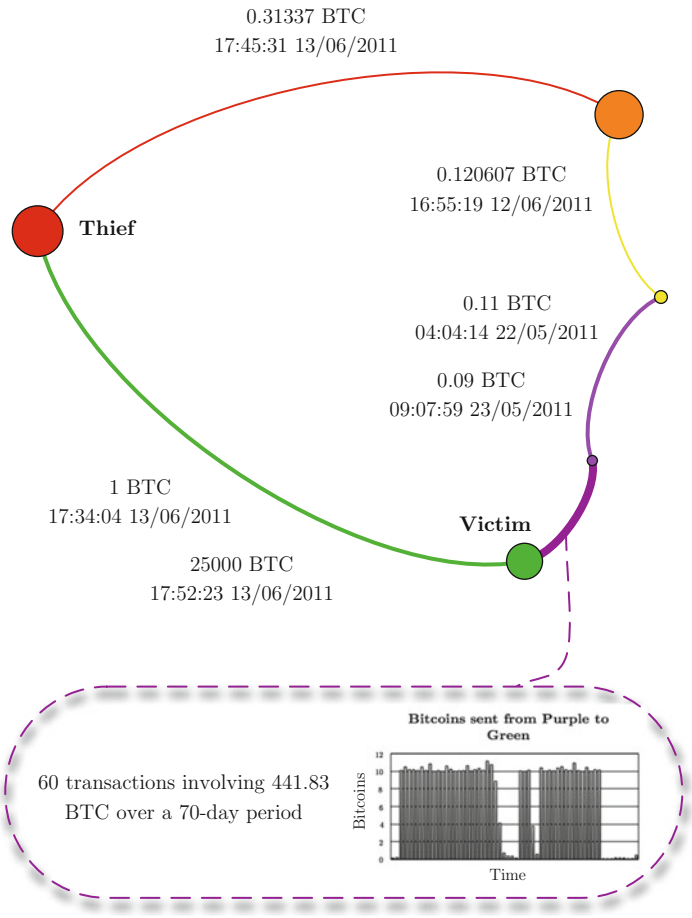

Fig. 12 An interesting sub-network induced by the thief, the victim, and three other vertices. The notation is the same as in Fig. 11

over a 70-day period. It also sent a total of 0.2 BTC to the yellow vertex over a 2 day period. One day before the theft, the yellow vertex also sent 0.120607 BTC to LulzSec.

The yellow vertex represents a user who is the owner of at least five public-keys.[22] Like the victim, he is a member of the Slush pool, and like the thief, he is a one-time donator to LulzSec. This donation, the day before the theft, is his last known activity using these public-keys.

[22] 1MUpbAY7rjWxvLtUwLkARViqSdzypMgVW413tst9ukW294Q7f6zRJr3VmLq6zp1C68EK1DcQvXMD87MaYcFZqHzDZyH3sAv8R5hMZe1AEW9ToWWwKoLFYSsLkPqDyHeS2feDVsVZ1EWASKF9DLU CgEFqfgrNaHzp3q4oEgjTsF

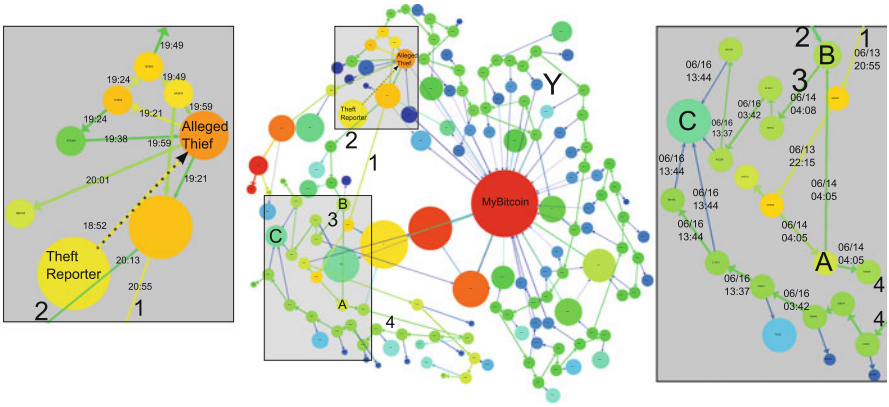

Fig. 13 Visualization of Bitcoin flow from the alleged theft. The *left* inset shows the initial shuffling of Bitcoins among accounts close to that of the alleged thief. The *right* inset shows the flow of Bitcoins during several subsequent days. The flows split, but later merge, validating that the flows found by the tool are probably still controlled by a single user

5.5 *Flow and Temporal Analyses*

In addition to visualizing egocentric networks with a fixed radius, we can follow significant flows of value through the network over time. If a vertex representing a user receives a large volume of Bitcoins relative to their estimated balance and, shortly after, transfers a significant proportion of those Bitcoins to another user, we deemed this interesting. We built a special purpose tool that, starting with a chosen vertex or set of vertices, traces significant flows of Bitcoins over time. In practice we found this tool to be quite revealing when analyzing the user network.

Case Study – Part II: To demonstrate this tool, we re-considered the Bitcoin theft described previously. We note that the victim developed their own tool to generate an exhaustive list of public-keys that received some portion of the stolen Bitcoins after the theft.[23] However, this list grows very quickly and, at the time of writing, contained more than 34,100 public-keys. Figure 13 shows an annotated visualization produced using our tool. We note several interesting flows in the aftermath of the theft. The initial theft of a small volume of 1 BTC was immediately followed by the theft of 25,000 BTC. This is represented as a dotted black line between the relevant vertices, magnified in the left inset of the figure.

In the left inset, we note that the Bitcoins were shuffled between a small number of accounts and then transferred back to the initial account. After this shuffling step,

[23] http://folk.uio.no/vegardno/allinvain-addresses.txt

we identified four significant outflows of Bitcoins that began at 19:49, 20:01, 20:13 and 20:55. Of particular interest are the outflows that began at 20:55 (labeled as "1" in both insets) and 20:13 (labeled as "2" in both insets). These outflows pass through several subsequent accounts over a period of several hours. Flow 1 splits at the vertex labeled *A* in the right inset at 04:05 on the day after the theft. Some of its Bitcoins rejoin Flow 2 at the vertex labeled *B*. This new combined flow is labeled as "3" in the right inset. The remaining Bitcoins from Flow 1 pass through several additional vertices in the next 2 days. This flow is labeled as "4" in the right inset.

A surprising event occurs on June 16, 2011 at approximately 13:37. A small number of Bitcoins were transferred from Flow 3 to a heretofore unseen public-key pk_1.[24] Approximately 7 min later, a small number of Bitcoins were transferred from Flow 3 to another heretofore unseen public-key pk_2.[25] Finally, there were two simultaneous transfers from Flow 4 to two more heretofore unseen public-keys: pk_3[26] and pk_4.[27] We have determined that these four public-keys, pk_1, pk_2, pk_3 and pk_4 – which received Bitcoins from two separate flows that split from each other 2 days previously – were all contracted to the same user in our ancillary network. This user is represented as *C* in Fig. 13.

There are several other examples of interesting flow. The flow labeled *Y* involves the movement of Bitcoins through 30 unique public-keys in a very short period of time. At each step, a small number of Bitcoins (typically 30 BTC which had a market value of approximately US$500 at the time of the transactions) were siphoned off. The public-keys that received the small number of Bitcoins are typically represented by small blue vertices due to their low volume and degree. On June 20, 2011 at 12:35, each of these public-keys made a transfer to a public-key operated by the MyBitcoin service.[28] Curiously, this public-key was previously involved in a separate Bitcoin theft.[29]

We also observe that the Bitcoins in many of the aforementioned flows were transferred between public-keys very quickly. Figure 14 shows two flows in particular wherein the intermediate parties waited for very few confirmations before re-sending the Bitcoins to other public-keys.

Much of this analysis is circumstantial. We cannot say for certain whether or not these flows imply a shared agency in both incidents. However, our analysis does illustrate the power of our tool when tracing the flow of Bitcoins and generating hypotheses. It also suggests that a centralized service may have additional details on the user(s) in control of the implicated public-keys.

[24] 1FKFiCYJSFqxT3zkZntHjfU47SvAzauZXN

[25] 1FhYawPhWDvkZCJVBrDfQoo2qC3EuKtb94

[26] 1MJZZmmSrQZ9NzeQt3hYP76oFC5dWAf2nD

[27] 12dJo17jcR78Uk1Ak5wfgyXtciU62MzcEc

[28] 1MAazCWMydsQB5ynYXqSGQDjNQMN3HFmEu

[29] http://forum.bitcoin.org/index.php?topic=20427.0

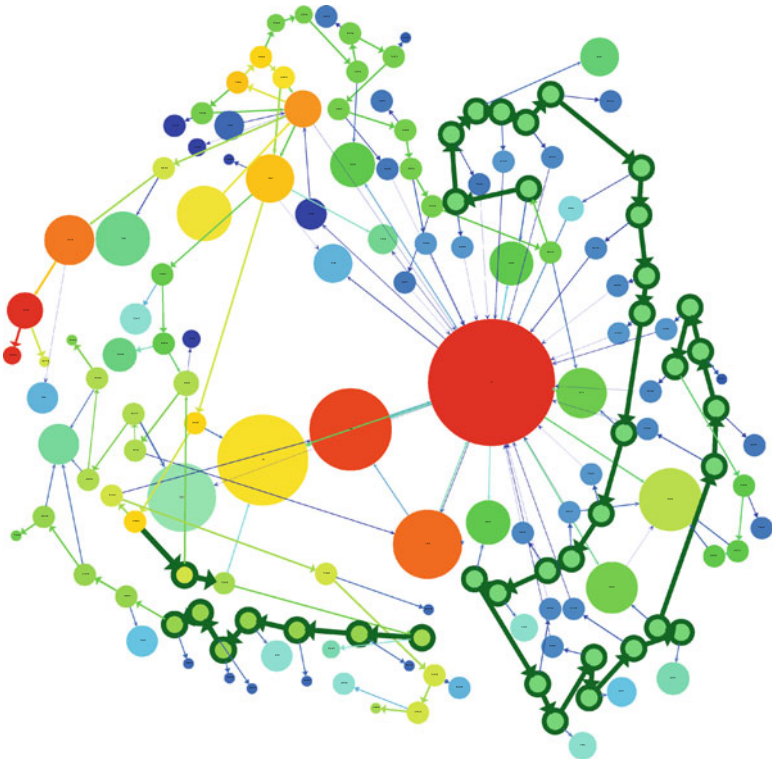

Fig. 14 Bitcoins are transferred very quickly, between the public-keys on the highlighted paths

5.6 Other Forms of Analysis

Many other forms of analysis could be applied to de-anonymize the workings of the Bitcoin system:

- Many transactions have two outputs, where one is the payment from a payer to a payee and the other is the return of change to the payer. If we assume that a transaction was created using a particular client implementation and we have access to the client's source code, then we might be able to distinguish, in some cases, between the payment and the change. We can then map the public-key that the change was assigned to, back to the user who created the transaction.
- Order books for Bitcoin exchanges are typically available to support trading tools. As orders are often placed in Bitcoin values converted from other currencies, they have a precise decimal value with eight significant digits. It might be possible to find transactions with corresponding amounts and thus map public-keys and transactions to the exchanges.
- Over an extended time period, several public-keys, if used at similar times, might belong to the same user. It might be possible to construct and cluster a co-occurrence network to help deduce mappings between public-keys and users.

- Finally, there are far more sophisticated forms of attack wherein the attacker actively participates in the network; for example, using marked Bitcoins or operating a laundry service.

5.7 Mitigation Strategies

In addition to educating users about the limits of anonymity in the Bitcoin system, some risks to privacy could potentially be mitigated by making changes to the system. A patch to the official Bitcoin client has been developed[30] that allows users to prevent the linking of public-keys by making the user aware of potential links within the Bitcoin client user-interface. It is also possible for the client to automatically proxy Bitcoins through dummy public-keys. This would come at the cost of increased transaction fees but would increase deniability and obfuscate the chain of transaction histories. Finally, if a future version of the protocol supported protocol-level mixing of Bitcoins, then the difficulty for a passive third-party to track individual user histories would increase.

6 Conclusions

For the past half-century futurists have heralded the advent of a cash-less society [2]. Many of their predictions have been realized, e.g. the 'on-line real-time' payment system and bank-maintained 'central information files' described by Anderson et al. [2]. However, cash is still a competitive and relatively anonymous means of payment. Bitcoin is an electronic analog of cash in the online world. It is decentralized: there is no central authority responsible for the issuance of Bitcoins and there is no need to involve a trusted third-party when making online transfers. However, this flexibility comes at a price: the entire history of Bitcoin transactions is publicly available. In this chapter we described the results of our investigation of the structure of two networks derived from this dataset, and their implications for user anonymity.

Using an appropriate network representation, it is possible to associate many public-keys with each other, and with external identifying information. With appropriate tools, the activity of known users can be observed in detail. This can be performed using a passive analysis only. Active analyses, by which an interested party can potentially deploy 'marked' Bitcoins and collaborate with other users can be used to discover even more information. We also believe that large centralized services (such as the exchanges and wallet services) are capable of identifying and tracking considerable subsets of user activity.

[30] http://coderrr.wordpress.com/2011/06/30/patching-the-bitcoin-client-to-make-it-more-anonymous – Retrieved 2011-11-04.

Technical members of the Bitcoin community have cautioned that strong anonymity is not a primary design goal of the Bitcoin system. However, casual users need to be aware of this, especially when sending Bitcoins to users and organizations with whom they would prefer not to be publicly associated.

Acknowledgements This research was supported by Science Foundation Ireland (SFI) Grant number 08/SRC/I1407: Clique: Graph and Network Analysis Cluster. The authors gratefully acknowledge this support. Both authors contributed equally to this work, which was performed independently of any industrial partnership or collaboration of the Clique Cluster.

References

1. Altshuler Y, Aharony N, Elovici Y, Pentland A, Cebrian M (2011) Stealing reality: when criminals become data scientists (or vice versa). IEEE Int Syst 26(6):22–30
2. Anderson A, Cannell D, Gibbons T, Grote G, Henn J, Kennedy J, Muir M, Potter N, Whitby R (1966) An electronic cash and credit system. American Management Association, New York
3. Back A (2002) Hashcash – a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf, Retrieved 12 Nov 2011
4. Backstrom L, Dwork C, Kleinberg J (2007) Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of the 16th International Conference on World Wide Web, Banff. ACM, New York, pp 181–190
5. Barabási A, Albert R (1999) Emergence of scaling in random networks. Science 286(5439):509–512
6. Brockmann D, Hufnagel L, Geisel T (2006) The scaling laws of human travel. Nature 439(26):462–465
7. Cavusoglu H, Cavusoglu H, Raghunathan S (2005) Emerging issues in responsible vulnerability disclosure. In: Proceedings of the 4th Annual Workshop on Economics of Information Security (WEIS'05), Cambridge
8. Clauset A, Shalizi C, Newman M (2009) Power-law distributions in empirical data. SIAM Rev 51(4):661–703
9. Crandall D, Backstrom L, Cosley D, Suri S, Huttenlocher D, Kleinberg J (2010) Inferring social ties from geographic coincidences. Proc Natl Acad Sci U S A 107(52):22436
10. Dai W (1998) B-money proposal, http://www.weidai.com/bmoney.txt, Retrieved 12 Nov 2011
11. Dwork C, Naor M (1992) Pricing via processing or combatting junk mail. In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'92), Santa Barbara. Springer, pp 139–147
12. Fugger R (2004) Money as IOUs in social trust networks a proposal for a decentralized currency network protocol, http://ripple-project.org/decentralizedcurrency.pdf, Retrieved 12 Nov 2011
13. Grinberg R (2011) Bitcoin: an innovative alternative digital currency. Hastings Sci Tech Law J 4:159–208
14. Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria. ACM, New York, pp 71–80
15. Kaminsky D (2011) Black ops of TCP/IP presentation. Black Hat, Chaos Communication Camp
16. Kichiji N, Nishibe M (2008) Network analyses of the circulation flow of community currency. Evol Inst Econ Rev 4(2):267–300

17. Korolova A, Motwani R, Nabar S, Xu Y (2008) Link privacy in social networks. In: Proceedings of the 17th ACM Conference on Information and Knowledge Management, Napa Valley. ACM, New York, pp 289–298
18. Lewis K, Kaufman J, Gonzalez M, Wimmer A, Christakis N (2008) Tastes, ties, and time: a new social network dataset using {F}acebook.com. Soc Netw 30:330–342
19. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, Retrieved 12 Nov 2011
20. Narayanan A, Shmatikov V (2008) Robust de-anonymization of large sparse datasets. In: Proceedings of the 29th Symposium on Security and Privacy, Oakland. IEEE, pp 111–125
21. Narayanan A, Shmatikov V (2009) De-anonymizing social networks. In: Proceedings of the 30th Symposium on Security and Privacy, Oakland. IEEE, pp 173–187
22. Nishibe M (2004) Chiiki Tuka No Susume (in Japanese). Hokkaido Shokoukai Rengou
23. Puzis R, Yagil D, Elovici Y, Braha D (2009) Collaborative attack on internet users' anonymity. Internet Res 19(1):60–77
24. Saito K (2006) i-WAT: the internet WAT system – an architecture for maintaining trust and facilitating peer-to-peer barter relationships. Ph.D. thesis, Keio University
25. Simon H (1955) On a class of skew distribution functions. Biometrika 42:425–440
26. Stalder F (2002) Failures and successes: notes on the development of electronic cash. Inf Soc 18(3):209–219
27. The Economist (2011) Digital currencies – bits and bob, http://www.economist.com/node/18836780, Retrieved 12 Nov 2011
28. Vishnumurthy V, Chandrakumar S, Sirer E (2003) KARMA: a secure economic framework for peer-to-peer resource sharing. In: Proceedings of the 1st Workshop on Economics of Peer-to-Peer Systems, Berkeley, California
29. Where's George? http://www.wheresgeorge.com, Retrieved 12 Nov 2011
30. Yang B, Garcia-Molin H (2003) PPay: micropayments for peer-to-peer systems. In: Atluri V, Liu P (eds) Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS'03), Fairfax. ACM Press, New York, pp 300–310