The Anti-Social System Properties: Bitcoin Network Data Analysis

As Published: 10.1109/TSMC.2018.2883678

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Persistent URL: https://hdl.handle.net/1721.1/134903

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

The Anti-Social System Properties: Bitcoin Network Data Analysis

Israa Alqassem, Iyad Rahwan and Davor Svetinovic, *Senior Member, IEEE*

***Abstract*—Bitcoin is a cryptocurrency and a decentralized semi-anonymous peer-to-peer payment system in which the transactions are verified by network nodes and recorded in a public massively-replicated ledger called the blockchain. Bitcoin is currently considered as one of the most disruptive technologies. Bitcoin represents a paradox of opposing forces. On one hand, it is fundamentally social, allowing people to transact in a peer-to-peer manner to create and exchange value. On the other hand, Bitcoin's core design philosophy and user base contain strong anti-social elements and constraints, emphasizing anonymity, privacy and subversion of traditional centralized financial systems. We believe that the success of Bitcoin, and the financial ecosystem built around it, will likely rely on achieving an optimal balance between these social and anti-social forces. To elucidate the role of these forces, we analyze the evolution of the entire Bitcoin transaction graph from its inception, and quantify the evolution of its key structural properties. We observe that despite its different nature, the Bitcoin transaction graph exhibits many universal dynamics typical of social networks. However, we also find that Bitcoin deviates in important ways due to anonymity-seeking behavioral patterns of its users. As a result, the network exhibits a two-orders-of-magnitude larger diameter, sparse tree-like communities, and an overwhelming majority of transitional or intermediate accounts with incoming and outgoing edges but zero cumulative balances. These results illuminate the evolutionary dynamics of the most popular cryptocurrency, and provide us with initial understanding of social networks rooted in and driven by anti-social constraints.**

***Index Terms*—Social networks, Bitcoin, Cryptocurrency**

I. Introduction

Bitcoin is a complex socio-cyber-physical system, e.g., [1], consisting of a decentralized peer-to-peer payment network, a currency unit, publicly preserved transaction history kept in a massively-replicated public ledger, i.e., the blockchain, an algorithm that controls money generation, and an ownership verification mechanism using public-key cryptography, where each Bitcoin address consists of a pair of public and private keys [2]. The process of creating new coins in the system is called mining. The mining process is computationally expensive. Any node connected to the Bitcoin network can participate in Bitcoin mining either as a part of a group of miners (called mining pool) or individually. In pooled mining, the generated coins are shared based on each member's contributed computational power.

Many commentators liken Bitcoin's present state to the early days of the Internet, and suggest that its technology will transcend financial transactions to encompass all kinds of new social transactions.

The structure and evolution dynamics of various social networks are well-studied [3], [4], [5], [6], [7], [8]. However, the Bitcoin transaction graph represents a novel kind of network that consists of global financial transactions carried out by users hidden behind pseudonyms represented by public keys (accounts, addresses, or public keys are used interchangeably to refer to users' unique identifiers used in Bitcoin system). These transactions are continually validated by Bitcoin computational nodes; running on users' computers and other specialized mining hardware, added to blocks, and newly generated blocks appended to the blockchain, which serves as a key innovation of the Bitcoin network [2].

One of the main driving forces behind the creation of Bitcoin was to counter the systematic move towards more transparency (i.e., reduction of privacy) and centralization. The original cash-based financial system got replaced with credit cards, audited transactions, automatic reporting to governmental entities, etc. As a reaction to such increased lack of privacy, centralization of control, and extensive monitoring, there appeared a need to develop a system that re-establishes and protects the financial privacy. The second driving force behind the creation of Bitcoin was to develop a currency with a predictable, algorithm-controlled inflation rate, as opposed to the unpredictable, human-controlled inflation rate of fiat currencies.

As such, Bitcoin presents a paradox of social and anti-social forces. On one hand, Bitcoin's main function is to facilitate economic transactions among individuals, which is a highly social function. Indeed, by eliminating expensive, trustworthy intermediaries, Bitcoin reduces the cost of transactions, thus facilitating more open economic transactions, transcending geographical and social boundaries.

On the other hand, at the core of the Bitcoin design philosophy are strong anti-social elements. Among Bitcoin's user community, there is a strong emphasis on privacy and anonymity, manifested in the fact that transactions only require cryptographic public keys in order to take place. Furthermore, the Bitcoin system embodies greater trust in algorithmic, rather than human, control of the money supply. In addition, Bitcoin's key distinguishing feature is its ability to process and verify transactions without transaction intermediaries that hold privileged positions in the network. As such, Bitcoin is distrustful, and arguably subversive, of centralized financial institutions or intermediaries that may abuse their power.

I. Alqassem is with the Department of Computer Science, Purdue University, West Lafayette, IN 47907, USA, Email: ialqasse@purdue.edu.

I. Rahwan is with the MIT Media Lab, Massachusetts Institute of Technology, Cambridge, MA 02139, USA, Email: irahwan@mit.edu.

D. Svetinovic is with the Center on Cyber-Physical Systems, Department of Computer Science, Khalifa University of Science and Technology, Abu Dhabi, UAE, Email: davor.svetinovic@ku.ac.ae (*Corresponding Author).

These seemingly contradictory social and anti-social elements of Bitcoin are, in fact, the key features behind its disruptive proliferation. However, we still lack a deep quantitative understanding of Bitcoin's adoption, use and growth dynamics. In order to acquire such understanding, we need to quantify the way in which Bitcoin's transaction network evolves over time, and to characterize the structural properties produced by the social and anti-social forces and their interactions. This will pave the way towards more complex analyses and may facilitate the development of scalable algorithms and online services that provide real-time insights into the blockchain and its vulnerabilities.

In this paper, we inspect the Bitcoin transaction network's evolution dynamics. Our findings indicate that despite the distinction in the nature of Bitcoin's transaction network when compared to other social networks, the Bitcoin transaction network follows the common normal evolution patterns, i.e., the densification power law and shrinking diameter (although the diameter shrinks only after the network reaches maturity).

On the other hand, we find that the absolute value of the transaction graph diameter is extremely large when compared to the other social networks which can be attributed to the presence of long chains of transactions. The transaction graph has less dense communities. Furthermore, the majority of public keys ($> 90\%$ of total public keys in the network) represent transitional or intermediate accounts with incoming and outgoing edges but zero cumulative balances. Most of the intermediate accounts are generated to complicate tracing users' wealth and identities. These observations can be attributed to the anti-social component of the behavior among Bitcoin users, i.e., they generate and discard accounts constantly to preserve and even further protect their anonymity.

II. Related Work

We cover three categories of related work. First, we discuss the related work that examined the blockchain data either as a single snapshot or at different time frames for various purposes, such as analyzing the level of privacy and anonymity in Bitcoin. Second, we discuss the related work which examined the universal characteristics that govern graph growth over time, from which we borrowed the graph growth metrics. Third, we discuss the related work that covers various applications of social network data analytics studies.

A. Blockchain Data Studies

Kondor et al. [9] investigated the evolution of basic characteristics of the blockchain over time. They identified two main phases of Bitcoin's life, the initial phase and the trading phase. The initial phase lasted until fall 2010, during which there was no real-world value associated with a bitcoin. Then MtGox, the previously popular Bitcoin exchange, went online and the Bitcoin trading phase has begun, through which bitcoins have gained market value. They examined the degree distribution, degree correlation and clustering coefficients, and wealth distribution. They showed that preferential attachment was shaping both the degree of Bitcoin addresses and the wealth distributions among these addresses which are fundamentally related in Bitcoin transaction network. In our analysis, we examine various network characteristics that were not covered here. We also repeat our analysis on the approximation of Bitcoin user graph based on a heuristic, that we discuss later, and was built based on the fact that all input addresses of a transaction must belong to a single entity that holds the private keys of these addresses.

Ron et al. [10] examined different statistical properties of Bitcoin transaction graph and analyzed the graph of the largest transaction that took place at the time of their analysis, May 13^{th} 2012, where an entity sent $90,000$ bitcoins to itself multiple times. Instead of looking at global network properties over time such as market price of bitcoins, number of daily transactions, etc. they examined the typical behavior of Bitcoin users e.g., the balances kept in their accounts, addresses associated with the largest balances, the size distribution of Bitcoin transactions, and the percentage of micropayments. One of their interesting findings was that the majority of bitcoins were not circulating in the network. Other findings were: (i) Bitcoin users tended to move their bitcoins large number of times in self-loops manner between different accounts, (ii) large sums of bitcoins were distributed in a binary tree-like structure, (iii) Approximately $156,722$ addresses were associated with Mt.Gox exchange at the time of their study. Their dataset contained transaction data up to block $180,000$ ($3,120,948$ addresses). This research did not look into the evolution of the transaction graph over time, instead they focused on statistical properties in a single snapshot.

Maesa et al. [11] presented a scalable clustering algorithm that constructed Bitcoin user graph with less false positives, thus they reduced the size of the original transaction graph. Then they analyzed the time evolution of the generated user graph with a late starting point (January 2013), after the Bitcoin system has matured and gained significant financial impact. They examined the nodes richness in terms of their degree and accumulated balances, and they confirmed the previous finding [9] that the Bitcoin network is a scale-free one where the richness is concentrated, and where high-degree nodes play a vital role for network connectivity and their constructed graph confirmed small-word phenomenon. They also showed that the distribution of clusters follow a power-law model. They inferred some address identities relying on publically available tag datasets. In our analysis, we look into different network characteristics in the full Bitcoin transaction graph before and after the system gained its popularity and we highlight how the users behavior changes over time to adapt to the system. We do not examine the in- and out-degree distributions and the distribution of the wealth in the network since that were already verified in previous research.

In the next three papers, [12], [13], [14], the authors analyzed the transaction graph in order to investigate the claimed anonymity that Bitcoin promised to offer. In doing so, they matched some Bitcoin addresses to real-world entities while constructing the Bitcoin transaction graph. Our work, however, inspects different network characteristics without touching the anonymity subject. We think Bitcoin supports pseudonymity not full anonymity and the users of the network are responsible to manage their addresses, i.e., public keys, in order to protect their privacy.

Fleder et al. [12] analyzed seven-month blockchain data between March 25^{th} 2013 and October 25^{th} 2013 for the purpose of examining the anonymity levels in Bitcoin. They developed a system to link public keys to their real-world entities by web scraping Bitcoin forum, public social network, donation sites, and other services where Bitcoin fans publicly announced their addresses. They also applied the PageRank algorithm to figure out the most important nodes, i.e., the ones that received large traffic like SatoshiDICE[1]). Furthermore, they de-anonymized a number of Bitcoin users, e.g., they identified some of Bitcoin forum users: (i) who gambled at SatoshiDICE, (ii) who were one hop away from Silk Road,[2] (iii) who had direct transactions with Wikileaks. In addition to an address belonged to FBI. This work focused on the level of anonymity that Bitcoin was supposed to offer and showed that it is possible to link real-world identities to Bitcoin addresses.

Meiklejohn et al. [13] explored the evolution of Bitcoin network through tracing the flows of both unspent and in-circulation bitcoins over time. Their methodology was divided into two stages. First, they identified public keys of well-known Bitcoin merchants and services (such as Mt. Gox and Silk Road) by making direct purchases from them. Additionally, they extracted self-labeled public keys from Bitcoin forum. Then, they clustered the users of known public keys into a graph where the nodes represent known services instead of merely representing anonymous addresses. They, by no means, aimed to de-anonymize all Bitcoin network, but rather they leveraged certain characteristics of Bitcoin protocol (e.g., multi-input transactions in which all input addresses belong to the same entity, and Bitcoin change) to reveal the identities of certain Bitcoin services, then categorized these services in order to calculate their overall balances, the percentage of transactions they involved in, etc. Their dataset contained blockchain data up to block $231,207$ ($16,086,073$ transactions and $12,056,684$ addresses).

Reid et al. [14] explored the limits of anonymity in Bitcoin transaction and user networks. They showed that one could easily figure out the total balance and incoming and outgoing transaction of Bitcoin public keys and users. As an example they visualized all WikiLeaks' payments and degree distribution over time and the number of transactions involving its public key. As a case study of potential risks to the anonymity in Bitcoin, they investigated the $25,000$ bitcoins theft reported in June $a3^{th}$, 2011, and they developed a tool to trace the stolen bitcoins which was transferred among several public keys. Their results showed that it is easy for Bitcoin centralized service providers (such as exchanges and wallet services) that have details on users' identities to identify and track considerable portions of their users. Furthermore, They suggested some enhancements to Bitcoin protocol to protect user's privacy. It is worth pointing out that this research is among the earliest attempts that analyzed Bitcoin network. Their dataset contained 1,253,054 public keys.

B. Social Network Analysis

Leskovec et al. [15] examined graph time evolution process in terms of the average node in- and out-degree and the effective diameter in nine graphs obtained from four diverse datasets. These datasets are: (i) ArXiv citation graph ($29,555$ papers, $352,807$ edges), (ii) U.S. patent citation graph ($3,923,922$ patents, $16,522,438$ citations), (iii) autonomous systems graph, this one exhibits addition and deletion of nodes and edges from November 1997 to January 2000, (iv) bipartite affiliation graphs ($57,381$ nodes, $133,170$ edges). These datasets were divided into regularly spaced snapshots in time. And the results they obtained showed that *densification power laws*[3] and *shrinking diameters*[4] are fundamental natural phenomena in all the graphs they examined. To produce graphs that capture shrinking diameter, heavy-tailed in- and out-degree distributions, and densification properties they proposed the Forest Fire Model. Indeed, shrinking diameter is rather surprising; as one would expect the graph's diameter to grow as the number of nodes increases. Shrinking diameter may be attributed to two reasons. One reason is the addition of edges, as in the stylized Erdös-Renyi random graph model where the diameter of the largest connected component (LCC) starts quite large and then it decreases as edges are being added continually. An alternative reason is what happens in real graphs where the nodes become well-connected to each other over time even after a graph reaches maturity, i.e., the diameter continues to decrease in a steady manner when the LCC contains almost all nodes. From this research we borrowed the characteristics which define how real graphs evolve over time. We also compare and contrast the growth patterns of Bitcoin to the growth patterns observed in this research while highlighting the novelty of Bitcoin network.

C. Applications

Kong et al. [16] have emphasized the need for social network and media analysis within the context of the systems development. They have explored the evolution patterns of popularity with respect to the burst forms and decays. They found that predicting the trends of popularity evolution is beneficial for decision making for various types of systems, e.g., emergency management, business intelligence, and public security. They evaluated their approach using tweets in SinaWeibo, a Chinese Twitter-like social media platform, with positive results and improvements.

Liu et al. [17] have demonstrated the importance of the social network analysis with respect to preserving system properties such as privacy and anonymity. They emphasized that the network analysis is even more effective when multiple network analysis are performed for the identification of the users. This is putting the context of our focus on the financial social network in the perspective with respect to the other types

[1] The biggest Bitcoin gambling website.

[2] An online marketplace uses bitcoins to trade in illegal drugs, firearms and other goods, operated as a Tor hidden service. It was shut down temporarily by FBI in October 2013 but it reopened again as Silk Road 2.0 in November 2013.

[3] Number of edges grows super-linearly in the number of nodes.

[4] Diameter decreases as network grows.

of social networks. While their method has shown positive results, it is unclear how it would perform within the context of blockchain-based social networks.

Zhang et al. [18] have studied evolutionary game dynamics of multiagent systems on multiple community networks. Given the fast evolution of blockchain systems and their potential integration with the artificial intelligence (AI) systems is opening even further application areas of the social network analysis in the context of blockchain systems. The further integration of the various blockchain systems is expending the analysis opportunities on multiple social network systems. The ability of agents to perform this analysis and interpret the data, will open up a whole another range of application opportunities for blockchain in complex AI-backed social networks.

Chang et al. [19] have used blockchain network data to analyze different patterns of transactions occurring in the Bitcoin network in order to cluster addresses that share the same ownership. This clustering approach has increased our ability to trace Bitcoin ownership thus potentially reducing the privacy of the users.

III. Method and Results

The temporal information of Bitcoin transactions embedded in the blockchain enables us to inspect the evolution dynamics and the key structural properties of this innovative payment network, where Bitcoin accounts represent the nodes and the transactions occurring between these accounts correspond to the edges. We identify 11 time-spaced sequential snapshots of the blockchain between January 2009 and September 2014. Six-month interval separates any two consecutive snapshots, except for the last one which contains the blockchain transactions up to the last block in our dataset. Table I shows our snapshots statistics.

TABLE I
Main characteristics of blockchain snapshots.

Snapshot index	*Block depth*	*#nodes*	*#edges*	*End date*
1	18,650	1,054	1,098	03-Jul-09
2	32,800	2,877	3,630	03-Jan-10
3	64,000	24,404	34,965	03-Jul-10
4	100,800	126,353	259,669	03-Jan-11
5	134,500	1,060,648	2,962,425	03-Jul-11
6	160,400	2,736,480	8,554,243	03-Jan-12
7	187,300	4,662,573	20,875,170	03-Jul-12
8	215,000	8,725,003	50,567,140	03-Jan-13
9	244,600	14,998,319	102,040,630	03-Jul-13
10	278,400	24,882,840	165,402,563	03-Jan-14
11	319,359	46,043,947	398,145,539	06-Sep-14

In Bitcoin there is a special type of transaction without input addresses, these transactions are called coinbase transactions. One coinbase transaction is generated per block to send block's mining reward and transaction fees (whenever available) to miners who participated in creating that block. The input address of all coinbase transactions are mapped to a dummy source address, then all coinbase transactions are excluded from the subsequent analysis. Including coinbase transactions would distort the results as they do not represent actual transactions occurring between Bitcoin users or services but merely transactions that generate coins in the system.

Two distinct stages of Bitcoin evolution are identified, i.e., the initial stage and the trading stage [9]. The initial stage continued until the first half of 2010. After that, Bitcoin started to attract growing number of users and online service providers such as Mt. Gox exchange which went online in July 2010 and Slush's pool; the first mining pool that started in December 2010. Then, Bitcoin was recognized as a cryptocurrency and a payment system, thus it gained a real purchase value and its trading stage has begun after the beginning of 2011. While the period in between represents a transitional stage. During which, Bitcoin was adapted by more than amateur beginners but it was still not yet recognized as a payment system neither as a cryptocurrency. Fig. 1 shows how this intermediate stage acts as a tipping point in the history of the first decentralized cryptocurrency. Here we quantify the evolution of Bitcoin and we show that some network properties differ noticeably throughout these stages.

A. Bitcoin Accounts

There is no upper bound on the number of accounts a Bitcoin user may have, nor a limit exists on the number of transactions' neighbours, unlike many of social networks which constrain the maximum allowable number of outgoing/incoming links. Moreover, in Bitcoin it is considered a good practice to generate different key pairs to receive the various incoming transactions in an attempt to maintain users' anonymity by complicating the tracking of addresses' owners and their wealth. This results in the emerging of different nodes types (i.e., Bitcoin account categories) which we categorize based on incoming transaction, outgoing transaction, and total balance each account accumulates. These categories are:

- Checking accounts: appeared as source and destination of one or more transaction and have cumulative balance greater than zero.
- Saving accounts: appeared only as destination of transaction(s) with cumulative balance greater than zero.
- Intermediate (transitional) accounts: accounts with zero cumulative balance. These accounts are mostly created by Bitcoin user or service, e.g., mixing or exchange service, to transfer money between other accounts. A fraction of these accounts may belong to users departing the network and selling all their coins.

As Fig. 1 depicts, during the initial stage, saving accounts were dominant since bitcoins did not have corresponding purchase value in fiat money and consequently no merchants were accepting them in exchange for goods or services. At that stage, the checking and intermediate accounts represented accounts owned by the early adopters who were trying or testing the Bitcoin system. Later on, during the latter stage, the intermediate accounts formed more than 90% of the total created accounts. This reveals an expected common behavior among Bitcoin users, i.e., they generate and discard public keys constantly to preserve their anonymity which results in a continually increasing transaction volume in the network. On the other hand, the percentage of saving accounts has relatively diminished in the trading stage compared with the initial stage. While the absolute number of newly created checking accounts went up by several orders of magnitude, from less than 30 in July 2009 to more than 250K in September 2014. This can be an indication of more people nowadays considering Bitcoin as a viable medium of exchange.

Two points can emphasize the aforementioned indication. First, the growing merchant adoption and the increasing number of service providers supporting Bitcoin payment directly or indirectly, (i.e., via conversion services such as Coinbase and BitPay) have enhanced Bitcoin's utility. Currently, big businesses and multinational corporations such as Microsoft, Dell, and Expedia support Bitcoin payments, moreover users can buy a wide range of physical goods with bitcoins, different gift card businesses accept bitcoins, and numerous physical stores, hotels, restaurants, and charities are welcoming Bitcoin payments [20]. Second, even though saving accounts have not faded away, Bitcoin currently can not be viewed as a stable store of value due to its high volatile price. Roughly speaking, the average market price around the beginning of July 2013 reached 85 USD, six months later this value jumped to 793 USD, while in March 2015 it was about 270 USD. This high price fluctuation leaves the user uncertain whether the bitcoins he has today will worth the same value tomorrow, hence incentivizes him to invest them in daily transactions (checking or speculation in Bitcoin) rather than saving them. Unlike the early adopters who used to keep their coins for the hope of making more profit for the exact opposite reasons: (i) due to limited options they had for spending their bitcoins on, and (ii) the chances were high at that time for bitcoin's purchase value to increase day after day.

B. Largest Connected Component (LCC) and its Diameter

The LCC of a graph connects the majority of the graph nodes. We examine the connectivity of Bitcoin transaction graph over time by quantifying the percentage of Bitcoin accounts taking part of its LCC, in addition to the diameter of this LCC as shown in Fig. 1. In graph theory, the diameter represents an important topological metric that helps in understanding the size and density of a network. To find the diameter of a graph (or its LCC), first we find the shortest paths between each pair of vertices. Then, the path with the maximum length represents the diameter of the graph, hence the diameter is the largest shortest path.

Bitcoin addresses are almost fully connected with more than 99.9% of Bitcoin accounts taking part of the LCC by the end date of the taken last snapshot. Network connectivity, in the context of the nodes taking part of the LCC, in Bitcoin scenario is similar to was reported for the LCCs of other social networks. For example, in May 2011, the LCC of Facebook had 99.91% of the total registered users [21]. In August 2009, the LCC of Twitter had 94.8% of twitter profiles [22]. Further, similar high percentage of nodes connecting to the LCC of their graphs was observed for arXiv and U.S. patent citation graphs [4].

There is a significant difference between the absolute value of the transaction graph's diameter in the last taken snapshot (> 2000) and the reported diameter values in a single snapshot of other social social networks. For example the diameter of Facebook is 41, the diameter of Twitter is 18, and the diameter of Google+ is 22 as reported in [23]. Four possible causes of this dramatic increase in the diameter of the transaction graph:

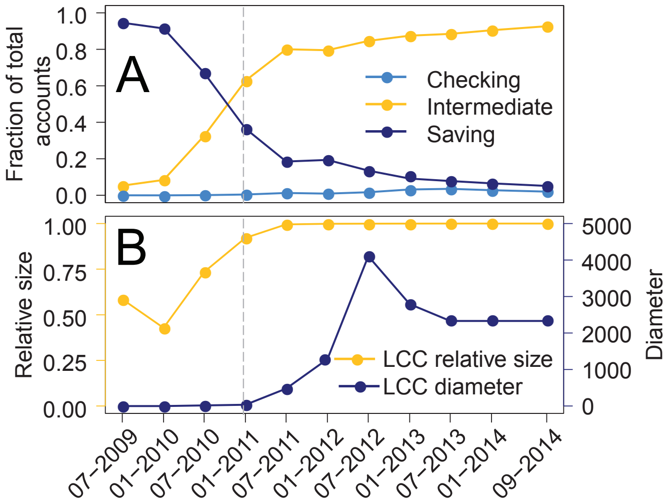


Fig. 1. (A) The evolution of Bitcoin account categories. A growth trend towards intermediate accounts after the beginning of trading stage (vertical dashed line). Intermediate accounts have incoming and outgoing transactions but zero cumulative balances. Bitcoin users generate and discard such accounts as a general practice to maintain their anonymity and avoid financial tracking. (B) The evolution of the relative size of the transaction graph's LCC and its diameter. More than 99.9% of Bitcoin accounts are taking part of the LCC as of September 2014. Similar high percentages are reported for nodes connecting to the LCC in other social networks such as Twitter, Facebook, and arXiv citation graph. After the beginning of the trading stage (vertical dashed line), Bitcoin starts attracting growing number of users, therefore the graph's diameter expands, its transaction graph becomes sparser and the distances between nodes increase continually until mid-2012. The expansion in diameter at the beginning is observed for the earliest Facebook and Google+ datasets. Later on, the diameter starts decreasing monotonically. The Shrinking diameter after the network reaches maturity is also one of the observed phenomenon in social networks, i.e., the diameter continues to decrease even after the LCC contains almost all nodes since the graph becomes denser. The absolute values of transaction graph's diameter are two-orders-of-magnitude larger than what is reported for social networks such as Facebook and Twitter which can be attributed to the presence of long chains of transactions.

- Anonymity which acts as an incentive for Bitcoin supporters to create several accounts to transfer their unspent coins.
- Thieves usually exhaust the network by generating enormous number of public keys to transfer and spread the stolen bitcoins. For instance, in [14] it was reported that more than 34,100 new addresses were created by the suspicious of Bitcoin theft which occurred in June 2011.
- The change addresses generated by Bitcoin client to transfer the remainder of the payment back to the payer, as bitcoins cannot be spent partially (Fig. 2).
- Bitcoin mixing services such as Bitcoin Fog and BitLaundry which offer mixing users' bitcoins with each other by generating many new accounts. Mixing services are generally used for Bitcoin laundry to complicate trailing illegal fund [24].

All of the aforementioned points lead to the presence of long transaction chains which in turn increases the shortest paths between graph nodes.

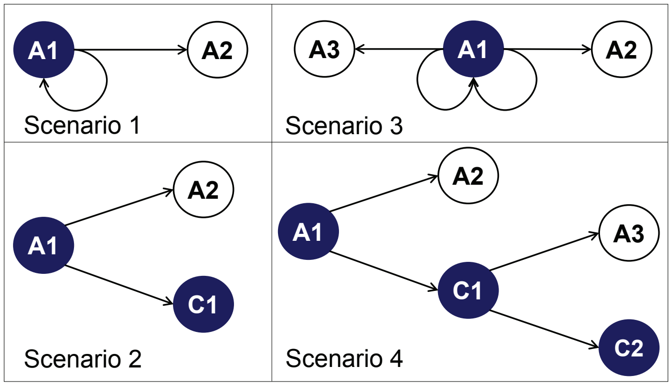


Fig. 2. In Bitcoin the change is not returned to the same address to protect user's privacy. Here, we assume that blue circles represent addresses owned by the same user. In scenarios 1&2, the user who owns address $A1$ sends a transaction to the user who owns address $A2$. The second scenario demonstrates how the change address concept protects user's privacy because it is difficult to distinguish the recipient(s) of the payment. In scenarios 3&4, the user who owns address $A1$ sends another transaction from the change of previous transaction (partial amount of that change). In scenario 3, there is no change address so the bitcoins are sent from the same address $A1$. In scenario 4, the bitcoins are transferred from the change address $C1$ to an address $A3$ owned by another user, a new change address $C2$ is created after this transaction. In this example we try to demonstrate how these change addresses increase the distance between nodes (here $A2$ and $A3$).

C. Densification Power Law

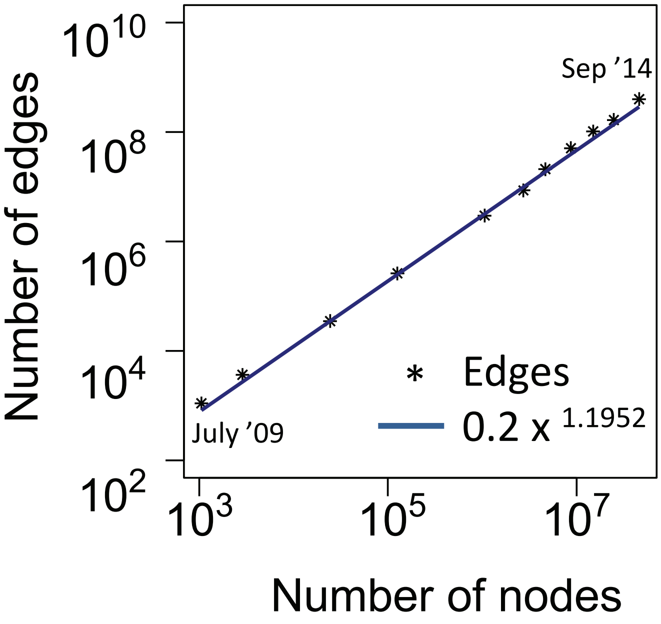


Fig. 3. The transaction graph follows densification power law, i.e., the average degree increases over time. The densification exponent is 1.1952.

The densification power law, or growth power law is an empirical observation examined by other researchers when studying the evolution of real graphs over time [4]. This law of graph evolution states that the growth of graph's edges is super linear in terms of the growth of its nodes. The Bitcoin transaction graph obeys this power law. In Bitcoin evolution context, it indicates despite that Bitcoin addresses (i.e., public and private key pairs) are being created continually, the edges grow super linearly as a function of the growth of newly added accounts. In other words, the growth of the network is attributed to the increase number of transactions, which means increase adaption and use of the Bitcoin financial system over time.

The densification power law is represented mathematically, as follows:

$$E(t) \propto N(t)^{\alpha} \qquad \text{where } 1 < \alpha \leq 2$$

$E(t)$ and $N(t)$ are the number of graph's edges and nodes respectively at each timestamp t. The Bitcoin transaction graph is becoming denser and its densification fits a power-law pattern with a slope $\alpha = 1.1952$, as shown in Fig. 3. The values of the densification exponents are 1.69 and 1.12 for arXive and Email networks, respectively. Although Bitcoin users change their accounts frequently, i.e., new nodes are being added continually to the transaction graph, still the growth of the transaction graph's edges is superlinear as a function of the growth of its nodes over time, similar to what was reported for other social networks such as IMDB actors to movies network and Email network [4].

D. Degree Assortativity

The degree assortativity acts an ingredient of community structure in a graph [25]. Degree assortativity coefficient measures whether or not graph's nodes have tendency to interact with similar nodes with regard to their in and out degree in directed graph (or degree in undirected one) [26], [27]. Its value lies between $[-1, 1]$, where values close to or equal to 1 is a sign of assortative mixing. 0 indicates neutral assortativity. Negative values reveal the opposite, i.e., "disassortativity". Social groups of real world typically have assortative mixing as 'birds of a feather flock together". Whereas there is no rule for online social networks [28]. For example, Flickr shows assortative mixing (0.202), while Youtube demonstrates the opposite (-0.033).

To measure degree assortativity in the transaction graph self-edges are excluded as they are irrespective to how nodes connect to each other. Table II shows negative assortativity over time. Since in Bitcoin payment system, transactions occur at two different levels: (i) internal, i.e., between different accounts that belong to the same user, and (ii) external, i.e., between different users in the network. In the internal transactions users usually transfer their coins from high-degree checking accounts to low-degree saving accounts. In the external transactions bitcoins are usually sent from low-degree addresses to high-degree addresses owned by known merchants and service providers.

E. Time-evolving Community Structure

Communities are graph modules with internally dense edges but relatively sparse external connections. We examine the evolution of statistical properties of transaction graph's communities, i.e., hub dominance, scaled link density, and

TABLE II
DEGREE ASSORTATIVITY COEFFICIENT, THESE VALUES ARE STATISTICALLY SIGNIFICANT (T-TEST P-VALUE ¡0.05).

Date	*Degree assortativity coefficient*
03-Jul-09	-0.239
03-Jan-10	-0.043
03-Jul-10	-0.021
03-Jan-11	-0.034
03-Jul-11	-0.022
03-Jan-12	-0.041
03-Jul-12	-0.04
03-Jan-13	-0.041
03-Jul-13	-0.041
03-Jan-14	-0.027
06-Sep-14	-0.011

community size distribution which are proposed in [29]. Self-edges cannot be indicative of how communities evolve thus we discard them to simplify our graph, similar approach is followed in [30].

Modularity is the first thing to look at when examining community structure. It is a quality index for measuring the presence of community structure in a graph by comparing the edge coverage of a community with the coverage an algorithm would achieve in a randomized null-model graph [31].

Modularity value depends on the community detection algorithm used, in addition to how modular a network is. Its value lies between $[-0.5, 1.0]$, where higher values indicate more modular networks, as such transaction graph tends to be a modular network (Fig. 4). Remarkably, the number of communities does not grow all the time, e.g., the number of the total evolving communities declined in six-month period between January 2011 and July 2011 which indicates that smaller communities getting merged into larger ones. This merge in communities coincided with the operation of the first Bitcoin pooled mining service "Slush's pool" which attracted an increasing number of miners as soon as it was released. The growth of evolving communities, on the other hand, can be attributed to split in existing communities or/and new nodes joining the network and establishing new well-connected clusters.

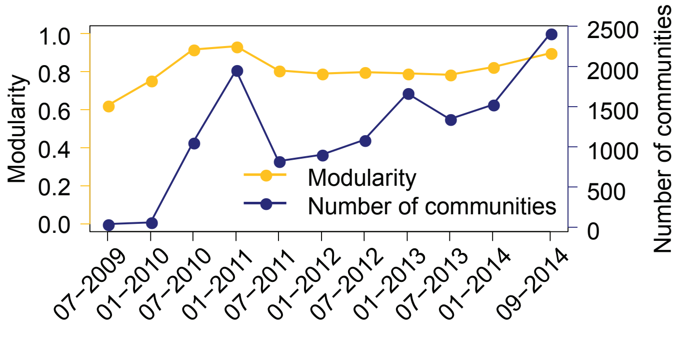


Fig. 4. Network's modularity and the number of evolving communities. We use a parallel implementation of *Louvain* method to detect Bitcoin communities. Based on these relatively high modularity values, the transaction graph tends to have modular structure.

1) Scaled link density: This property is defined as the average internal degree[5] of nodes within a community.

$$\rho = \frac{2t}{s(s-1)} \qquad Link\,density$$
$$\tilde{\rho} = \rho s = \frac{2t}{s-1} \qquad Scaled\,link\,density$$

Where, t is the number of edges within a community and s represents the size of that community, i.e., the number of nodes forming it. Scaled link density reveals community's nature. For example, tree-like community has number of edges equals to the lower limit ($t_{tree} = s - 1$), substituting this value in the second equation above gives us 2, therefore tree-like communities always have scaled link density value equals to 2. Whereas in a full clique, each node is connected to all other nodes, i.e., the number of edges in the undirected clique equals to the upper limit ($t_{clique} = \frac{s(s-1)}{2}$), substituting this value in the scaled link density equation gives us a value of s, therefore clique-like communities always have scaled link equals to s.

To examine the dependency of this property on the size of the community, the median of scaled link densities are plotted as a function of communities' sizes over time as illustrated in Fig. 5. The median values are chosen here given the skewness in the distribution of scaled link density values. Bitcoin communities' scaled link densities lie in the interval $[2, 5]$, closer to the lower limit, which indicate tree-like structure behind the majority of Bitcoin communities (Fig. 5). Whereas social networks have denser communities than trees but sparser than cliques based on the finding of a previous study [29].

2) Hub-dominance: How dominant are the biggest hubs within Bitcoin communities? This can be quantified according to the following formula:

$$Hub - dominance = \frac{max(k_{in})}{s-1}$$

Where, $max(k_{in})$ is the maximum degree of a node within a community. The maximum possible degree is $s - 1$ when a central node within a community is connected to all other nodes in its community, consequently the value of the above ratio will equal to 1 in such extreme case. For the majority of social networks this ratio decline with community size until dominant hubs almost vanished from large communities. However, in the Email and the web graphs the dominant hubs existed independent of community size [29]. We also study this property as a function of community size over time. In the transaction graph there is a hybrid existence of dominant and non-dominant hubs. Roughly speaking, smaller communities ($s \leq 100$) tend to have full- to half-dominant hubs opposite to larger ones ($s > 10^4$) which lack dominant nodes as depicted in Fig. 6.

3) Distribution of communities' sizes: The distribution of communities sizes is an important statistic describing community structure. After the beginning of the trading stage the community size distribution almost preserve the same shape. We run a comparative test that leverages the log likelihood ratios to compare the fit between various pairs of distributions and find that the exponentially truncated power law represents the best fit.

[5] Internal degree: node's degree in the subgraph of the community.

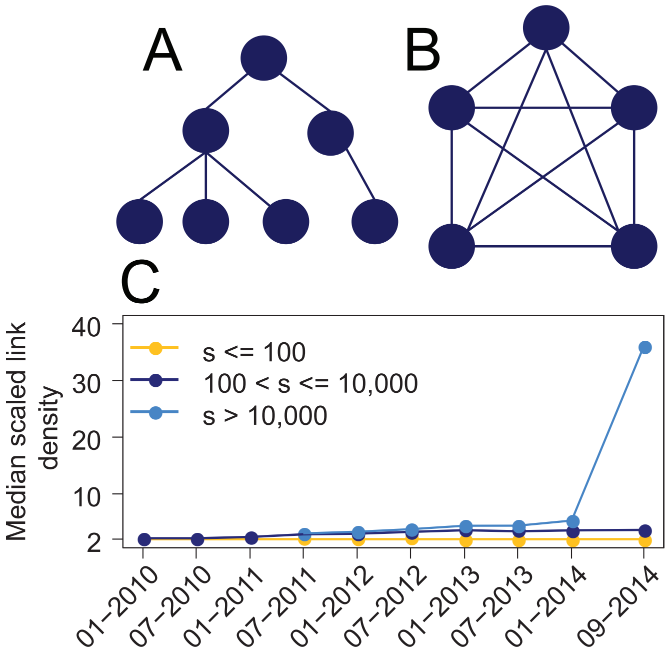


Fig. 5. Scaled link density. (A) Tree-like subgraph with scaled link density equals to 2. (B) Clique-like subgraph with scaled link density equals to the number of nodes 5. (C) The evolution of median values of scaled link density in transaction graph as a function of community size s. In spite of community size, the scaled link density median values are close to the lower limit which indicates a tree-like structure behind the majority of Bitcoin communities, which indicates "split or merge" of coins between accounts. The median value of scaled link density spikes at the end for large communities $> 10^4$. More investigation is needed to figure out the nature or causes of these relatively sparse communities.

F. Inequality as measured by Gini Index

Here we study the distribution of wealth among these accounts. From economics perspective, Lorenz curve measures the inequality of the wealth distribution. In Fig. 7 the diagonal (45°) represents the line of perfect equality. The increase in the area between this diagonal and Lorenz curve indicates the greater the gap in wealth distribution among Bitcoin accounts over time. Gini coefficient can be computed from this curve, Kondor et al. conducted a detailed analysis into the Bitcoin wealth distribution [9].

IV. Discussion

Bitcoin aims at establishing a global financial network facilitating transactions among people from all around the world without the need for expensive, trustworthy intermediaries. Despite the different purposes of the various social networks and Bitcoin transaction network, one can observe universal dynamics such as the densification power law, shrinking diameter, and modular structure as discussed previously in the results section, and the power-law degree distribution as reported in the previous work [9].

Social networks generally exhibit addition and deletion of nodes and edges over time. However, in Bitcoin, after a transaction gets confirmed, all of the addresses encapsulated within that transaction can never be deleted from the blockchain. This criterion together with the financial nature of Bitcoin network stimulate an anonymity-seeking behaviour among Bitcoin users which in turn leads to the key distinction between Bitcoin transaction network and other social networks.

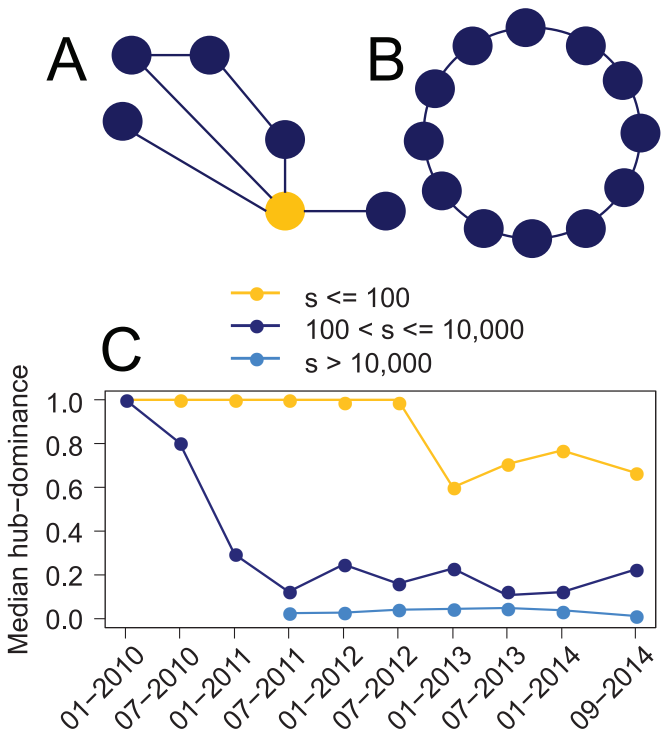


Fig. 6. Hub-dominance. (A) In this subgraph, the yellow node has the maximum degree, it is connected to 4 out of 5 nodes, therefore the hub-dominance value equals to 0.8. (B) The circular subgraph lacks of hub presence. (C) Shows the evolution of median values of hub-dominance as a function of community size s. The presence of hubs within Bitcoin communities depends directly on community size, i.e., the hub-dominance values decline with community size until dominant hubs vanish from large communities. Similar to what is reported for other social networks. Noticeably, communities of size $> 10^4$ appeared only after January 2011, after the Bitcoin gained real market value and consequently started to attract growing number of users and services. We examine different values of community size (s) and the same trend holds for all values.

Thus, the vulnerable anonymity together and the inability to erase addresses or transactions from the blockchain threaten users with potential financial tracking. This is especially the case if a user converts from a fiat currency to bitcoins from a traditional financial account. In this scenario, their real identity is linked to their Bitcoin account [14]. To prevent this identity linking, the users engage in even further anonymity seeking behavior. This is done using the features of the Bitcoin's core design which is equipped with the necessary capabilities emphasizing anonymity and privacy, i.e., the concept of change addresses in addition to user's ability to generate as many new addresses as desired.

Further, to improve anonymity, mixing services, which are called sometimes laundry services, have been developed by Bitcoin supporters. These services, when implemented properly, hide any connection between the user's source address (the account used to deposit an amount of bitcoins into the service) and the destination address (the account used to withdraw bitcoins) [24]. Consequently, Bitcoin users, sometimes with the aid of mixing services, create various categories of accounts as discussed previously and minimize the reusability

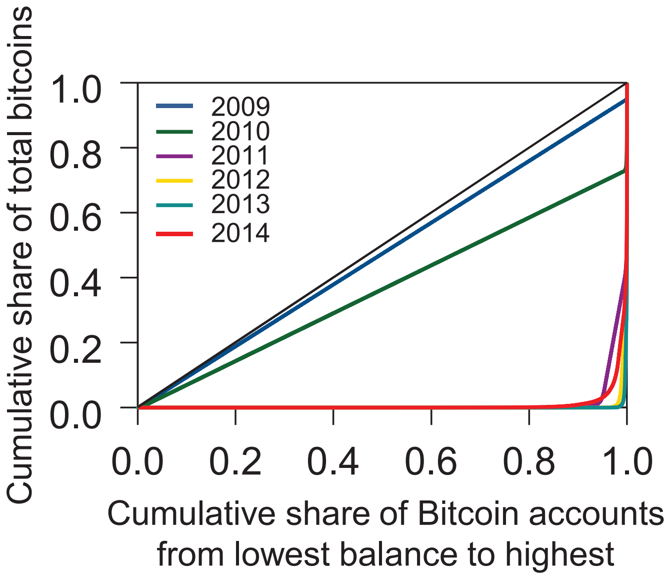


Fig. 7. The evolution of Lorenz curve. The x axis is the cumulative share of Bitcoin accounts from lowest balance to highest. The y axis is the cumulative share of total bitcoins. The increase in the area between this diagonal and Lorenz curve indicates the greater the gap in wealth distribution among Bitcoin accounts. The distribution of wealth in the Bitcoin financial system has become heterogeneous since 2011, i.e., users who own less than 10% of addresses almost control the whole wealth. Prior to 2011, the Bitcoin network was in its trial version where a few enthusiasts and developers (the number of users by the end of initial stage was less than $< 8,000$) tried the system and split their coins among many accounts.

of their addresses by splitting or merging their coins in long transaction chains which result in a huge diameter, different account categories, and sparse tree-like communities which distinguish the Bitcoin anti-social network from the other social networks.

We also examined the same graph properties for an approximation of Bitcoin user graph. In that approximation graph, a single node represents a group of addresses that belong to the same user [6]. To generate an approximation of Bitcoin user graph we used a heuristic that was developed and effectively used in the previous research [10], [13]. This heuristic relies upon the fact that all input addresses of a transaction must belong to a single entity that holds the private keys of these addresses. Quoting Satoshi Nakamoto from the original Bitcoin white paper [2]: “Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner.” Establishing a user graph from a transaction graph can be viewed as a variation of the Union-Find known graph algorithm [32] as illustrated in Fig. 9. However, the exact users of Bitcoin cannot be determined precisely because the Bitcoin protocol was intentionally designed to maximize user’s anonymity by minimizing the possibility of linking the different addresses owned by the same user.

The analysis of the approximation user graph confirmed our previous findings since we discovered similar properties in the approximation user graph: same large diameter, confirmation of the densification power law, the disassortative mixing, in addition to high modularity values (within the range $(0.70, 0.92)$) which, as stated earlier, reflect the presence of a community structure. We even found close similarities between the underlying trends of scaled link density and hub-dominance median values as shown in Fig. 8. These results strengthen our reasoning behind the unique nature of the Bitcoin.

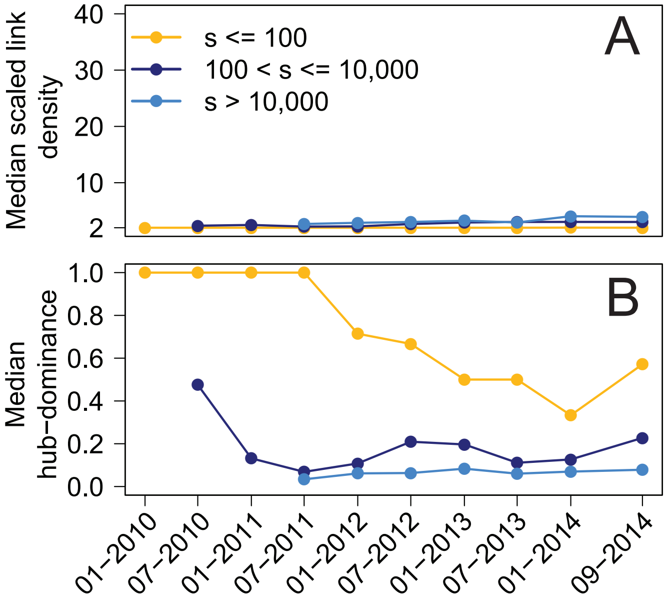
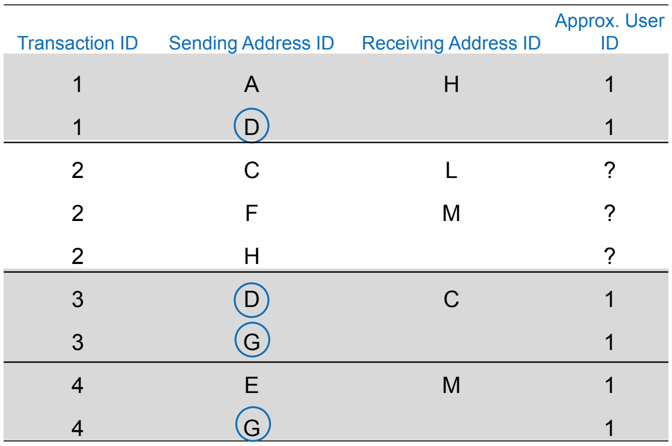


Fig. 8. (A) Similarly, the scaled link density median values for the approximation graph indicates a tree-like structure behind the majority of the approximation user graph communities. The spike shown previously in Fig. 5 vanishes indicating those relatively denser communities where mapped to a single entity in the approximation graph. (B) Here as well, our finding indicates that the presence of hubs in our approximation graph depends directly on community size.

From the systems perspective, it was observed that some of these anti-social incentives are effecting ritical system properties such as security and privacy, e.g., [33], [34], [35]. The anti-social incentives are leading to formation or disintegration of certain network communities. This in turn is leading to the improper use or the intentional misuse of the overall system. These community alteration present serious threats to a subset of the system properties that we identified: decentralization, longevity (of the system that’s supposed to evolve over next hundreds of years), trust, participation incentive, privacy, security, and usage ethics. As such, our contribution in understanding and measuring social network properties that lead to the identification of the anti-social incentives and properties represent a contribution with a potentially significant systems impact in the design of this new generation of cryptocurrency networks.

Given the recent expansion of the blockchain use as a system infrastructure to support other kinds of mission critical systems, such as smart grids, Internet of Things (IoT), autonomous driving vehicles, health records management, assets trading, etc., e.g., [34], [36], [37], [38], we are shifting from Bitcoin as a socio-cyber network [1] to full blockchain-based socio-cyber-physical systems. This integration is putting a

[6] A user can have multiple nodes representing them in that graph, hence this is just an approximation.



Transaction ID	Sending Address ID	Receiving Address ID	Approx. User ID
1	A	H	1
1	Ⓓ		1
2	C	L	?
2	F	M	?
2	H		?
3	Ⓓ	C	1
3	Ⓖ		1
4	E	M	1
4	Ⓖ		1

Fig. 9. The addresses $\{A, D\}$ are inputs to the same transaction, on this account they are owned by the same entity. Address $\{D\}$ appeared as sending address in transactions $\{1, 3\}$ then all sending addresses of both transactions belong to the same user. Moreover, address $\{G\}$ appears as a common input address to the transactions $\{3, 4\}$, which leads us to conclude that a single entity holds the private keys of $\{A, D, G, E\}$ and that entity initiated all the three transaction $\{1, 3, 4\}$. We cannot assign a new user id to the input addresses of the second transaction until we see the complete list of all transactions; we might encounter a common address that link them to the aforementioned user.

combination of additional system properties of safety and trust as critical with respect to potential anti-social incentives in these new mission critical systems. To deal with these issues, we have to develop additional social network measures and to work on design of community detection technologies. This will help us support the development of blockchain-enabled trust infrastructures that can ensure sufficient levels of privacy, security, safety, trust and overall dependability. This must be done in the context of planning for systems longevity, i.e., these systems are supposed to last hundreds of years, e.g, Bitcoin's longevity is critical to assume if it is to be considered as the financial system infrastructure for these mission critical socio-cyber-physical systems.

Finally, while this paper covers data from 2009–2014 that correspond to the initial phase and trading phase identified in [9], the paper does not cover the period from late 2014 until present that represents the currently ongoing heavy mass media and heavy financial speculation phase. While this can be considered as a limitation of this work, we believe that the data from the ongoing speculation phase is worth studying in its own light once the speculation phase is over. At the time of the writing, we were unable to take into account either the mass media coverage variable or heavy financial speculation variable neither qualitatively nor quantitatively.

V. Conclusion

In summary, Bitcoin represents a move from relatively local, transparent social networks created through the use of traditional fiat currencies to relatively global, semi-anonymous social networks created through the use of cryptocurrencies, with Bitcoin being the leading example. If we assume that the ultimate goal of social networks is to connect globally, one could argue that the traditional currency networks could be considered anti-social. The need to control a fiat currency and to have a certain level of transparency within a local currency network creates control conflicts among the sovereigns. This in turn prevents effective, inexpensive expansion of the local social financial networks evident through expensive financial conversion protocols and services.

To fight this anti-social component of the local traditional currency social networks, Bitcoin relies upon a set of its own anti-social forces as observed in this paper. As we have seen in our results, the evolutionary dynamics of the Bitcoin as the most popular cryptocurrency provides us with the initial understanding of social networks rooted in and driven by anti-social behaviours. We can conclude that it is indeed the optimal balance of the social and anti-social forces that is critical for the success and acceptance of a particular currency and the corresponding financial social network. And the enforcement of anti-social behaviours is critical for the users, even at the expense of adding the additional social network noise as the results have shown.

As a part of our future research, we will work on the development of other cryptocurrency network specific measures and community detection approaches, and combine them with our natural language analysis approach [39], [40] and generic infrastructure models [41] to provide enhanced privacy, security, and trust blockchain solution in the smart grid systems domain. This will be combined with the use of questionable arbitrary data recorded in the blockchains [34] in order to tackle the issues of higher-level system usage ethics and trust-ethical constraints.

References

[1] A. Ahmad, M. Babar, S. Din, S. Khalid, M. M. Ullah, A. Paul, A. G. Reddy, and N. Min-Allah, "Socio-cyber network: The potential of cyber-physical system to define human behaviors using big data analytics," *Future Generation Computer Systems*, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17307781

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, vol. 1, no. 2012, p. 28, 2008.

[3] M. E. Newman, "The structure and function of complex networks," *SIAM review*, vol. 45, no. 2, pp. 167–256, 2003.

[4] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graph evolution: Densification and shrinking diameters," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, p. 2, 2007.

[5] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," in *Link mining: models, algorithms, and applications*. Springer, 2010, pp. 337–357.

[6] D. Easley and J. Kleinberg, *Networks, crowds, and markets: Reasoning about a highly connected world.* Cambridge University Press, 2010.

[7] A. Z. Jacobs, S. F. Way, J. Ugander, and A. Clauset, "Assembling thefacebook: Using heterogeneity to understand online social network assembly," *arXiv preprint arXiv:1503.06772*, 2015.

[8] A.-L. Barabâsi, H. Jeong, Z. Néda, E. Ravasz, A. Schubert, and T. Vicsek, "Evolution of the social network of scientific collaborations," *Physica A: Statistical mechanics and its applications*, vol. 311, no. 3, pp. 590–614, 2002.

[9] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? An empirical analysis of the BitCoin transaction network," *PloS one*, vol. 9, no. 2, p. e86197, 2014.

[10] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 6–24.

[11] D. D. F. Maesa, A. Marino, and L. Ricci, "Uncovering the bitcoin blockchain: an analysis of the full users graph," in *Data Science and Advanced Analytics (DSAA), 2016 IEEE International Conference on*. IEEE, 2016, pp. 537–546.

[12] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," *arXiv preprint arXiv:1502.01657*, 2015.

[13] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 127–140.

[14] F. Reid and M. Harrigan, *An analysis of anonymity in the bitcoin system*. Springer, 2013.

[15] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graphs over time: densification laws, shrinking diameters and possible explanations," in *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*. ACM, 2005, pp. 177–187.

[16] Q. Kong, W. Mao, G. Chen, and D. Zeng, "Exploring trends and patterns of popularity stage evolution in social media," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–11, 2018.

[17] X. Liu, C. Shen, X. Guan, and Y. Zhou, "We know who you are: Discovering similar groups across multiple social networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–12, 2018.

[18] J. Zhang, Y. Zhu, and Z. Chen, "Evolutionary game dynamics of multiagent systems on multiple community networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–17, 2018.

[19] T. Chang and D. Svetinovic, "Improving bitcoin ownership identification using transaction patterns analysis," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–12, 2018.

[20] coindesk.com, "What can you buy with bitcoins?" October 2015 (accessed October 26, 2015). [Online]. Available: http://goo.gl/Kc6WW5

[21] J. Ugander, B. Karrer, L. Backstrom, and C. Marlow, "The anatomy of the facebook social graph," *arXiv preprint arXiv:1111.4503*, 2011.

[22] M. Cha, H. Haddadi, F. Benevenuto, and P. K. Gummadi, "Measuring user influence in twitter: The million follower fallacy." *ICWSM*, vol. 10, pp. 10–17, 2010.

[23] R. Gonzalez, R. Cuevas, R. Motamedi, R. Rejaie, and A. Cuevas, "Google+ or google-?: dissecting the evolution of the new osn in its first year," in *Proceedings of the 22nd international conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2013, pp. 483–494.

[24] M. Moser, R. Bohme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *eCrime Researchers Summit (eCRS), 2013*. IEEE, 2013, pp. 1–14.

[25] M. Catanzaro, G. Caldarelli, and L. Pietronero, "Assortative model for social networks," *Physical Review E*, vol. 70, no. 3, p. 037101, 2004.

[26] M. E. Newman, "Assortative mixing in networks," *Physical review letters*, vol. 89, no. 20, p. 208701, 2002.

[27] ——, "Mixing patterns in networks," *Physical Review E*, vol. 67, no. 2, p. 026126, 2003.

[28] H.-B. Hu and X.-F. Wang, "Disassortative mixing in online social networks," *EPL (Europhysics Letters)*, vol. 86, no. 1, p. 18003, 2009.

[29] A. Lancichinetti, M. Kivelä, J. Saramäki, and S. Fortunato, "Characterizing the community structure of complex networks," *PloS one*, vol. 5, no. 8, p. e11976, 2010.

[30] D. J. Fenn, M. A. Porter, M. McDonald, S. Williams, N. F. Johnson, and N. S. Jones, "Dynamic communities in multichannel data: An application to the foreign exchange market during the 2007–2008 credit crisis," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 3, p. 033119, 2009.

[31] C. L. Staudt, A. Sazonovs, and H. Meyerhenke, "Networkit: An interactive tool suite for high-performance network analysis," *arXiv preprint arXiv:1403.3005*, 2014.

[32] T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein *et al.*, *Introduction to algorithms - Chapter 21*. MIT press Cambridge, 2001, vol. 2.

[33] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018. [Online]. Available: http://doi.acm.org/10.1145/3212998

[34] M. Conti, S. K. E, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.

[35] Y. Yuan and F. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, Sept 2018.

[36] E. Al Kawasmi, E. Arnautovic, and D. Svetinovic, "Bitcoin-based decentralized carbon emissions trading infrastructure model," *Systems Engineering*, vol. 18, no. 2, pp. 115–130, 2015.

[37] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, Sept 2018.

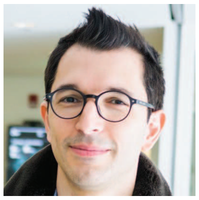
[38] B. Ojetunde, N. Shibata, and J. Gao, "Secure payment system utilizing manet for disaster areas," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–13, 2018.

[39] E. Casagrande, S. Woldeamlak, W. L. Woon, H. H. Zeineldin, and D. Svetinovic, "Nlp-kaos for systems goal elicitation: Smart metering system case study," *IEEE Transactions on Software Engineering*, vol. 40, no. 10, pp. 941–956, 2014.

[40] E. Casagrande, E. Arnautovic, W. L. Woon, H. H. Zeineldin, and D. Svetinovic, "Semiautomatic system domain data analysis: a smart grid feasibility case study," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 12, pp. 3117–3127, 2017.

[41] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic, "Integrated smart grid systems security threat model," *Information Systems*, vol. 53, pp. 147–160, 2015.

Israa Alqassem is a PhD student at Purdue university, USA. She is interested in machine learning, blockchain technology, and the IoT. Currently, she is a visiting research student at Ludwig Maximilian University of Munich, Germany. Her research focus is the development of statistical methods and computational tools for analyzing genomic data.



Iyad Rahwan is the AT&T Career Development Professor and an Associate Professor of Media Arts & Sciences at the MIT Media Lab, where he leads the Scalable Cooperation group. A native of Aleppo, Syria, Rahwan holds a PhD from the University of Melbourne, Australia. He is an affiliate faculty at the MIT Institute of Data, Systems and Society (IDSS), and member of the MIT Taskforce on the Work of the Future.

Rahwan's work lies at the intersection of computer science and human behavior, with a focus on collective intelligence, large-scale cooperation, and the societal impact of Artificial Intelligence and social media. His early work explored how social media can be used to achieve unprecedented feats, such as searching an entire continent within 9 hours, and re-assembling shredded documents. He led the winning team in the US State Department's Tag Challenge, using social media to locate individuals in remote cities within 12 hours using only their mug shots.

Recently, Rahwan led a team that crowdsourced 40 million decisions from people worldwide about the ethics of autonomous vehicles. Through a series of projects, he also exposed tens of millions of people world-wide to new implications of AI, such as bias in machine learning, human-AI creativity and the ability of AI to induce fear and empathy in humans at scale.

Another theme that interests Iyad is the future of work and human-machine cooperation. He demonstrated the world's first human-level strategic cooperation by an AI, and innovated new methods to anticipate the potential impact of AI on human labor.

Iyad Rahwan's work appeared in major academic journals, including Science and PNAS, and features regularly in major media outlets, including the New York Times, The Economist, and the Wall Street Journal.

Davor Svetinovic is an Associate Professor of Computer Science at Masdar Institute, Khalifa University of Science and Technology, UAE. He received his PhD (2006) degree in Computer Science from University of Waterloo, Canada. Previously, he worked as a visiting professor and research affiliate at the Massachusetts Institute of Technology (MIT); and as a postdoctoral researcher at Lero – the Irish Software Engineering Center, Ireland, and Vienna University of Technology, Austria. He leads the Strategic Requirements and Systems Security Group (SRSSG), and he has extensive experience working on complex multi-disciplinary research projects. He has published over 65 papers in leading journals and conferences. His current research interests include systems security and privacy, blockchain engineering, cryptocurrencies, and requirements engineering. He is a Senior Member of IEEE and ACM.