Is Bitcoin a Decentralized Currency?

Arthur Gervais* Ghassan O. Karame** Srdjan Capkun*
Vedran Capkun***
*ETH Zurich, 8092 Zuerich, Switzerland.
**NEC Laboratories Europe, 69115 Heidelberg, Germany.
***HEC Paris, France.

Abstract

Bitcoin has achieved large-scale acceptance and popularity by promising its users a low-cost, anonymous, and completely decentralized exchange of transactions. However, recent incidents and observations are revealing the true limits of decentralization in the Bitcoin system. In this article, we show that the vital operations and decisions that Bitcoin is currently undertaking are not decentralized. More specifically, we show that a limited set of entities currently control the services, decision making, mining, and the incident resolution processes in Bitcoin. We also show that third-party entities can unilaterally decide to "devalue" any specific set of Bitcoin addresses pertaining to any entity participating in the system. Finally, we explore possible avenues to enhance the decentralization in the Bitcoin system.

Keywords: Bitcoin, Decentralized decision process

1 Introduction

Bitcoin has already witnessed a wider adoption and attention than any other digital currency proposed to date. One of the main reasons for such a broad adoption of Bitcoin has been a promise of a low-cost, anonymous, and decentralized currency that is inherently independent of governments and of any centralized authority [1].

In this work, we analyze the (de-)centralized nature of Bitcoin and show that—contrary to widespread belief—Bitcoin is not a truly decentralized system as it is deployed and implemented today.

Namely, in Bitcoin, the users "vote" with their computing power to prevent double-spending (i.e., by *power-voting*) which effectively limits the power of individual users and makes Sybil attacks difficult. Given the huge computing power that is harnessed in the Bitcoin system (currently around 6000 Tera hashes per second, more than 300 times faster than the top 500 super computers combined), users believe that it is unlikely for any entity to acquire such power alone, and control the network. However, even a quick look at the distribution of computing power in Bitcoin reveals that the power of dedicated "miners" far exceeds the power that individual users dedicate to mining, allowing few parties to effectively control the currency; currently the top-three (centrally managed) mining pools control more than 50% of the computing power in Bitcoin. Indeed, while mining and block generation in Bitcoin was originally designed to be decentralized, these processes are currently largely centralized.

On the other hand, other Bitcoin operations, like protocol updates and incident resolution are not designed to be decentralized, and are controlled by a small number of administrators whose influence does not depend on the computing power that they control but is rather derived from their function within the system. Bitcoin users do not have any direct influence over the appointment of the administrators—which is somewhat ironic since some of the Bitcoin users opt for Bitcoin in the hope of avoiding centralized control that is typically exercised over national currencies.

Furthermore, we note that Bitcoin introduces a level of transparency in terms of coin mining and spending since the transaction logs in Bitcoin are public and available for inspection by any interested party. However, it is not clear how any potential disputes would be resolved in Bitcoin since this would then require appropriate regulatory frameworks—a move which clearly goes against the very nature of Bitcoin.

We further observe that the existence of public logs in Bitcoin can have some negative effects on this currency which extend beyond known privacy concerns [2]. Bitcoin users can e.g., decide not to accept coins that appear to have originated from a particular address (i.e., that were mined by the owner of that address); since the use of any coin (or its fraction) can be traced back to its origin, this decision by the users will practically deflate the value of these coins, since other users become reluctant on accepting these coins as payments. We call this effect *coin tainting* and postulate that it can have a negative effect on the use of Bitcoin as a currency.

Finally, we explore possible solutions and recommendations to enhance the decentralization in Bitcoin. We hope that our findings solicit further research in this area.

The remainder of this article is organized as follows. In Section 2, we briefly describe the main operations in Bitcoin. In Section 3, we discuss the limits of decentralization in Bitcoin. In Section 4, we explore possible ways to enhance the decentralization of Bitcoin. In Section 5, we overview related work in the area, and we conclude in Section 6.

2 Background on Bitcoin

In Bitcoin, electronic payments are performed by generating *transactions* that transfer Bitcoin coins (BTCs) among Bitcoin users. Users are referenced in each transaction by means of virtual pseudonyms—referred to as *Bitcoin addresses*. Each address is mapped through a transformation function to a unique public/private key pair. These keys are used to transfer the ownership of BTCs among addresses.

Users transfer coins to each other by issuing a transaction. A transaction is formed by digitally signing a hash of the previous transaction where this coin was last spent along with the public key of the future owner and incorporating this signature in the coin [15]. Any peer can verify the authenticity of a BTC by checking the chain of signatures.

Transactions are included in Bitcoin *blocks* that are broadcasted in the entire network. To prevent double-spending of the same BTC, Bitcoin relies on a hash-based proof-of-work (PoW) scheme to generate blocks. More specifically, Bitcoin users must find a nonce value that, when hashed with additional fields (i.e., the Merkle hash of all valid and received transactions, the hash of the previous block, and a timestamp), the result is below a given target value. If such a nonce is found, users then include it (as well as the additional fields) in a new block thus allowing any entity to publicly verify the PoW. This process is referred to as *block mining*. Upon successfully generating a block, a peer is currently granted a fixed amount of BTCs. This provides an incentive for users to continuously support Bitcoin. The resulting block is forwarded to all users in the network, who can then check its correctness by verifying the hash computation. If the block is deemed to be

"valid", then the users append it to their previously accepted blocks. Since each block links to the previously generated block, the Bitcoin block *chain* grows upon the generation of a new block in the network.

Bitcoin relies on this mechanism to resist double-spending attacks. For malicious users to double-spend a BTC without being detected, they would not only have to redo all the work required to compute the block where that BTC was spent, but also they need to recompute all the subsequent blocks in the chain.

3 Centralized Processes in Bitcoin

The original design of Bitcoin (cf. Section 2) aims at fully decentralizing the transaction generation and confirmation processes. In fact, decisions in Bitcoin have to be approved by the majority of the computing power in the network (which is assumed to be honest) in order to be effective in practice.

In what follows, we demonstrate that critical processes in the Bitcoin ecosystem are controlled by a small set of Bitcoin entities, whose influence does not depend on the computing power that they control but is rather derived from their function within the system.

3.1 Bitcoin Services

Bitcoin has lead to the emergence of several centralized services that monopolize a considerable share of the Bitcoin market.

Mining Pools: Bitcoin resists double-spending attacks (i.e., signing-over the same coin to two different users) through the reliance on a distributed PoW-based service [15]. The underlying intuition is that as long as the majority of the computing power in the network is "honest", then the security of Bitcoin transactions can be guaranteed. This implicitly assumes that the computing power is shared among all users in the network, and as such the security of Bitcoin can be ensured as long as the majority of Bitcoin users are honest.

Since mining in Bitcoin is rewarded with BTC generation, this process has become very competitive; an "arms race" has emerged using the various hashing technologies that have been specifically designed to mine BTCs [1]: high-end Graphical Processing Units (GPUs), Field Programmable Gate Arrays (FPGAs) and recently Application-Specific Integrated Circuits (ASICs). Currently, the probability of finding a block in a single trial is about $3 \cdot 10^{-19}$.

To guarantee regular payouts of miners, their computing power is often "pooled" into a central "mining pool" that coordinates the mining activities of the participants. Here, the mining pool administrator outsources the search inputs for the PoW problem (e.g., the version, difficulty, last block hash) and asks them to find a solution for the specific outsourced problem. In these systems, all participating miners receive a number of BTCs every time a PoW is found; this payment is proportional to the computing power invested in finding that PoW.

This business model has lead to the emergence of a number of such mining pools. Figure 1 depicts the distribution of computing power in the Bitcoin network from April to July 2013. Our findings show that more than 75% computing power in Bitcoin is currently controlled by 6 major centralized mining pools. *If these pools were to collude in order to acquire more than 50% of computing power share in the network, they can effectively control the confirmation of all transactions occurring in*

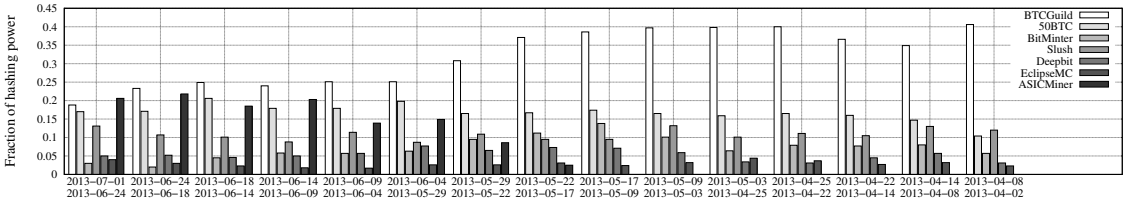

Figure 1: Distribution of computing power in Bitcoin between April, 2nd 2013 and the 1st of July 2013. More than 55% of the computing power in the network was controlled by BTCGuild and 50BTC, until ASICMiner recently achieved over 20% of hashing power.

the system. This includes preventing transactions from being executed, approving a specific set of transactions and double-spending transactions [1].

Bitcoin Web Wallets: A Bitcoin client installation currently takes more than 8 GB of disk space and requires several hours in order to download and index the current block chain. Therefore, users started relying on centralised services that host the main Bitcoin functionalities, called web wallets. A web wallet is an online wallet, hosted on a remote server and accessible through a website. It is instantly functional, does not occupy hard disk space, is accessible anywhere and is consequently more convenient than a local Bitcoin client.

Web wallets empower their operators with full unilateral powers of the BTCs of users. For instance, a malicious web wallet operator could potentially *(i)* steal or forward stolen Bitcoins, *(ii)* trade with non-used funds, and *(iii)* profile users. For example, in April 2013, a theft of 923 BTCs occurred in the mining pool OzCoin. A subset of the stolen BTCs were transferred to a web wallet hosted by StrongCoin. Although StrongCoin claims that it supports user privacy, and does not have access to the user funds, StrongCoin intercepted the allegedly stolen BTCs and transferred them back to OzCoin. *This decision was taken by few entities in the network without acquiring consensus from the majority of users in the network.*

SPV Mode: Simplified payment verification (SPV) consists of a modified Bitcoin node which does not verify transactions or blocks in the Bitcoin network. SPV relies on a trusted node which forwards transactions and blocks to all connecting nodes. SPV clients have been introduced because the default Bitcoin client consumes a significant amount of power, which most smartphones for example cannot afford. *This clearly comes at costs of decentralization, since a critical security component of the network is outsourced to a single node.*

3.2 Protocol Maintenance and Modifications

The Bitcoin core developers have the authority to make all the necessary modifications to the Bitcoin protocol; according to the Bitcoin Github repository, all "radical" decisions require consensus amongst all the developers. For example, in the Bitcoin client version 0.8.2 the developers unilaterally introduced a fee policy change and decided to lower the default fee for low-priority transactions from 0.0005 BTC to 0.0001 BTC. Clearly, this empowers the Bitcoin developers to regulate and control the entire Bitcoin economy. In what follows, we illustrate this by means of further recent examples in Bitcoin.

Block Chain Forks: During the normal Bitcoin operation, miners work on extending the longest block chain in the network. If miners do not share the same view in the network (e.g., due to network partitioning), they might work on different block chains, thus resulting in "forks" in the block chain.

Block chain forks are detrimental for the operation of the Bitcoin system. Since one block chain will eventually prevail (the longest), all transactions that were included in all other chains will be invalidated by the miners in the system. Note that Bitcoin does not embed any mechanism to alleviate this problem; instead, if the forks persist for a considerable period of time, Bitcoin developers have to take a decision in favoring one chain on the expense of another (e.g., by sending alert messages and hard-coding the preferred chain in the client code).

As an example, we proceed to describe a recent chain fork in March 2013, that solicited intervention from the Bitcoin developers. Recall that the Bitcoin client version 0.7 stored the block chain in the BerkleyDB database, while client version 0.8 switched to the more efficient LevelDB database. Version 0.7 sets the threshold for the maximum number of "locks" per BerkleyDB update to 10,000; this limit, on the other hand, is set to 40,000 in version 0.8. This discrepancy caused a serious fork in the block chain starting from block 225,430 on 11th of March 2013. This block contained around 1,700 transactions, affected more than 5,000 block index entries, and therefore exceeded the required number of locks for version 0.7 (each block index entry requires around 2 locks in BerkleyDB). As a consequence, this resulted in a severe block fork in the chain; all version 0.7 miners rejected block 225,430 and continued working on a block chain that does not include it, while miners with version 0.8 accepted that block and added it to their block chain. This process is depicted in Figure 2. The chain adopted by version 0.8 clients was supported by the majority of the computing power in the network (it exceeded the chain adopted by 0.7 clients by 13 blocks at block 225,451). Nevertheless, the Bitcoin developers decided, 90 minutes after the fork occurred, to force the smallest chain to be the "genuine" one, and convinced the owner of the biggest mining pool, Eleuthria from BTC Guild, to support this decision.

This decision comes at odds with the claim that Bitcoin is a decentralized system and that the majority of the computing power regulates Bitcoin. Less than 10 entities [3] took a decision to outvote the majority of the computing power in the network; this decision has affected the transactions of thousands of users. We also point out that such influential entities also have the power to make more "radical" decisions (e.g., accepting/rejecting transactions in the system, etc.).

Alert Mechanism: Alert messages have been introduced in the Bitcoin client after version 0.3.10. These messages serve to alert the Bitcoin users in case of critical incidents. For example, if a severe vulnerability is found in the Bitcoin client, Bitcoin developers can issue an alert message that will be displayed to the user. In Section 3.3, we show how such alert messages can be used to deflate the value of coins in the system.

Since alert messages are cryptographically signed, they can only be sent by people that possess the appropriate cryptographic key. Currently, this key is shared among the Bitcoin developers. *This gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release.* We point out that the current alert payload format supports a RESERVED string which is not currently being used. It is straightforward to see that this field can be abused in the future to send additional control commands (i.e., Botnet-like commands) to be executed by Bitcoin users [4].

Bitcoin Improvement Proposals: In order to affect the Bitcoin development process, Bitcoin

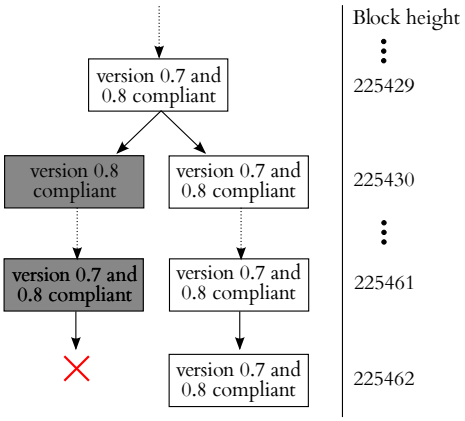

Figure 2: Sketch of the block chain fork that occurred in Bitcoin on 11.03.2013.

users are requested to file a Bitcoin Improvement Proposal (BIP) [1] that is assessed by the Bitcoin developers. The developers then unilaterally make a decision whether such a proposal will be supported by the future Bitcoin releases.

This limits the impact that users have, irrespective of their computing power, to affect the development of the official Bitcoin client. Recent events reveal that contributing within the Bitcoin community is not a trivial process [5].

3.3 Coin Tainting

Given that Bitcoin transactions basically consist of a chain of digital signatures, the expenditure of individual coins can be publicly tracked. This enables any entity to "taint" coins that belong to a specific (set of) addresses and monitor their expenditure across the network. The literature features a number of proposals that cluster Bitcoin addresses [2], and gather behavioural information about these addresses [12, 14].

Coin tainting is currently used to achieve a degree of accountability in the Bitcoin network; if an address misbehaves, then Bitcoin users can decide to stop interacting with the address (i.e., not accepting its coins), thus deflating the value of all the coins pertaining to that address. For instance, following a theft of 43,000 BTCs from the Bitcoin trading platform Bitcoinica, the Bitcoin service MtGox traced the stolen BTC and locked accounts that were receiving the tainted coins [4].

These incidents show that powerful entities in Bitcoin can—rightfully or not—deflate the value of BTCs owned by specific addresses. If these entities were to cooperate with the handful of developers that have privileged rights in the system, then all Bitcoin users can be warned not to accept BTCs that pertain from a given address (e.g., using alert messages). Even worse, developers can hard-code a list of banned Bitcoin addresses within the official Bitcoin client releases, thus blocking all interactions with a given Bitcoin address without the consent of users.

Furthermore, while coin tainting can be used to "punish" provably misbehaving addresses, it could also be abused to control the financial flows in the network subject to government pressure, but also due to social activism. *This empowers few powerful entities that are not necessarily part of the Bitcoin network, such as governments and activists, to regulate the Bitcoin economy. Even if all*

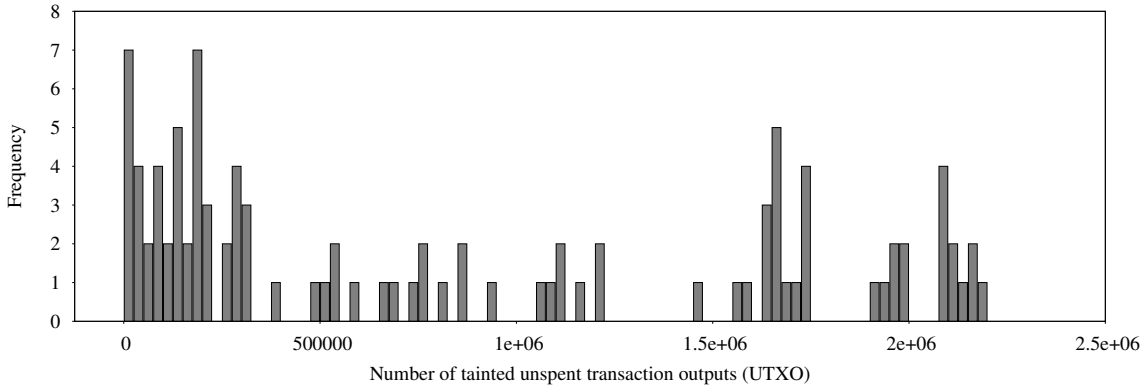

Figure 3: Tainting 100 random coinbases between block-height 227,054 and 247,054 and counting the number of affected UTXO.

Bitcoin decisions and operations were completely decentralized—which they are not—coin tainting presents an obstacle to a truly decentralized Bitcoin.

Coin tainting can be especially detrimental if coins are not widely exchanged among Bitcoin addresses. This enables entities to damage only a specific set of addresses, without alienating other addresses in the system. Other users are then also likely to "boycott" the tainted coins.

We conducted two experiments to analyze the impact of coin tainting on the Bitcoin network. In the first experiment, we measured the number of unspent transaction outputs (UTXO) that are affected when tainting a coinbase. Recall that a coinbase is the first transaction in a block, and attributes the block mining reward to a particular address. We randomly sampled 100 coinbases from the last 20,000 blocks of the block chain which by the time of the experiment had the highest block-height at 247,054. Our results show that a single coinbase tainting affects a large number of transaction outputs; on average, tainting a single coinbase affects 857,239 UTXO (with a standard deviation of 767,528), accounting for 12.9% of all possible UTXO. The resulting distribution of the number of affected UTXO within our sampled coinbases is depicted in Figure 3.

In a second experiment, we analyzed the effect of tainting addresses belonging to a single entity in Bitcoin. Given the absence of data to identify these addresses, we relied on two heuristics adapted from [2] in order to cluster addresses across Bitcoin entities.

Heuristic I—Multi-input Transactions: Multi-input transactions occur when a user wishes to perform a payment, and the payment amount exceeds the value of each of the available BTCs in the user's wallet. In fact, existing Bitcoin clients choose a set of BTCs from the user's wallet (such that their aggregate value matches the payment) and perform the payment through multi-input transactions. It is therefore straightforward to conclude that if these BTCs are owned by different addresses, then the input addresses belong to the same user.

Heuristic II—"Shadow" Addresses: Bitcoin generates a new address, the "shadow" address [1], onto which each sender can collect back the "change". This mechanism suggests a distinguisher for shadow addresses. In the case when a Bitcoin transaction has n output addresses, such that

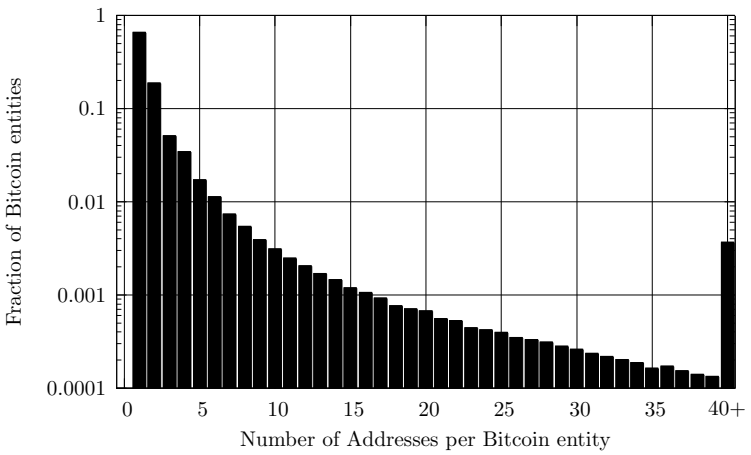

Figure 4: Number of addresses per Bitcoin entity derived from Heuristics I and II [2]

only one address is a new address (i.e., an address that has never appeared in the transactions log before), and all other addresses correspond to an old address (an address that has appeared previously in the transactions log), we can safely assume that the newly appearing address constitutes a shadow address for the input address. Note that the official Bitcoin client started to support transactions with multiple recipients since December 16, 2010.

We point out that these heuristics combined can only give a lower estimate on the number of addresses per entity. Given the aforementioned heuristics, most entities that we discovered (85%) were equipped with only one address, while there are 0.122% (i.e., almost 9845) of these entities with more than 40 addresses. On average, our results show that tainting the addresses of a single entity in Bitcoin would result in devaluating an average of 1.42 BTCs (with a standard deviation of 127.58 BTC). The actual distribution of Bitcoin addresses per Bitcoin entity can be seen in Figure 4.

As an exemplary application of our analysis, we identified two Bitcoin addresses belonging to Torservers.net (using information available from `blockchain.info`). Given the knowledge of these two addresses, we were able to identify a total of 47 addresses, belonging to the operator of Torservers, with a total balance of 498.20 BTC. If an external entity, e.g. a governmental institution, would like to stop the Torservers from receiving Bitcoin donations, it could taint all UTXO of the affected Bitcoin addresses. An exemplary application of the impact coin tainting was demonstrated by the shutdown of Silk Road—one of the most well known underground online black market—by the FBI in October 2013. Note that Silk Road was only accessible through the Tor network; the FBI seized over 27,000 BTCs stored within one or more Bitcoin addresses.

4 Enhancing the Decentralization in Bitcoin

In what follows, we explore possible avenues that could enhance the decentralization in Bitcoin.

Mining Pools: While most existing mining pool protocols assume the existence of a logically

centralized operator that orchestrates the block generation process, a number of fully decentralized mining pools, such as P2Pool, are emerging. Such pools share the benefits of centralized pools since all the participating users get regular payouts that reflect their contribution towards generating a block. However, these pools do not require the existence of any centralized coordinator and operate in a completely decentralized fashion. Currently, P2Pool only holds a marginal share of the computing power in the network; Bitcoin users can only hope that such decentralized pools can be transformed into profitable businesses in the near future in order to attract most miners.

One "Vote" per Client: Although few mining pools clearly control the computing power in the network (cf. Figure 1), we argue that there is still hope for reducing the impact of mining pools on the Bitcoin system. Given that Bitcoin relies on the notion of "controlled supply" which effectively limits the total number of generated BTCs (i.e., the amount of BTC that are generated for each block is halved every four years), the ultimate dominance of mining pools is expected to decrease with time, since their profits would depend less and less on self-awarded BTCs, and more on transaction fees. This, in turn, also increases the contribution of individual users to the Bitcoin economy. Indeed, mining pools operators would then have less incentives to accept client versions that are adopted by the minority of the clients (cf. Section 3.2). Users would then contribute more to the decision making process in Bitcoin by deciding to adopt a client version that suits their preferences. Recall that since the Bitcoin source code is open-source, there are already a considerable number of different Bitcoin implementations [1].

Transparent Decision Making: In some settings, it is inevitable that various client versions/implementations require constant maintenance and development by a group of leading developers. Here, problems arise in those situations where the developers have to take action in order to resolve possible conflicts that may have raised. Indeed, this process needs to be completely transparent and should be tightly regulated in order not to abuse the trust of users, and to minimize such unilateral interventions in the system. For example, in order to prevent the (ab-)use of alerts in Bitcoin, these alerts should be accompanied with provable and undeniable justifications. Based on these proofs, users can then decide whether to accept or not such warnings. For instance, double-spending alerts can include the double-spending transactions [6]; this provides irrefutable proof that a given address is double-spending.

Finally, careful planning and testing of version releases is required so as to ensure backward compatibility with previous versions.

Marketplaces, SPV Clients and Web-Wallets: Few centralized services, such as marketplaces and web-wallets, have emerged in order to facilitate the use of the decentralized Bitcoin protocol. Indeed, this shows the lack of foresight when deploying Bitcoin since several of the decentralized aspects of Bitcoin are not user-friendly; users find it cumbersome to maintain local wallets and do not wish to download the entire blockchain upon client installation. On the one hand, a truly decentralized Bitcoin is unlikely to be adopted by a vast majority of users since decentralization often comes at odds with user-friendly performance and service. On the other hand, decentralization has been one of the main attractions for users that decided to adopt Bitcoin.

Currently, there is only a handful of services that populate Bitcoin and enable a user-friendly trade and storage of BTCs. For instance, three Bitcoin marketplaces, MtGox, Bitstamp and BTC China handle more than 80% of the USD to Bitcoin trading. We can only hope that more similar services will form to reduce the market share of the current oligopoly.

5 Related Work

Bitcoin has received considerable attention in the literature. In [8], Elias investigates the legal aspects of privacy in Bitcoin. In [9], Babaioff *et al.* address the lack of incentives for Bitcoin users to include recently announced transactions in a block. Furthermore, in [7], Syed *et al.* propose a user-friendly technique for managing Bitcoin wallets. In [6], Karame *et al.* investigate double-spending attacks in Bitcoin and show that double-spending fast payments in Bitcoin can be performed in spite of the measures recommended by Bitcoin developers. This analysis was later extended in [10].

Reid and Harrigan [13] analyse the flow of Bitcoin transactions in a small part of Bitcoin log. In [2], Androulaki *et al.* evaluate user privacy in Bitcoin and show that Bitcoin leaks considerable information about the profiles of user. In [14], Ron and Shamir analyse the behaviour of Bitcoin users. In [12], Ober *et al.* studied the time-evolution properties of Bitcoin by analyzing its transaction graph. Finally, in [11], Moore and Christin study the economic risks that investors face due to Bitcoin exchanges.

6 Concluding Remarks

While the original design of Bitcoin aims at a fully decentralised Bitcoin, recent events in Bitcoin are revealing the true limits of decentralisation in this system. A large number of centralized services currently host Bitcoin and control a considerable share in the Bitcoin market. Even worse, Bitcoin developers retain privileged rights in conflict resolution and maintenance of the official client version. These entities altogether can decide the fate of the entire Bitcoin system, thus bypassing the will, rights, and computing power of the multitude of users that populate the network.

Currently, almost every financial system is controlled by governments and banks; Bitcoin substitutes these powerful entities with other entities such as IT developers and owners of mining pools. While current systems are governed by means of transparent and thoroughly investigated legislations, vital decisions in Bitcoin are taken through the exchange of opinions among developers and mining pool owners on mailing lists. In this sense, Bitcoin finds itself now in unfamiliar territory: on the one hand, the Bitcoin ecosystem is far from being decentralized; on the other hand, the increasing centralization of the system does not abide by any transparent regulations/legislations. This could, in turn, lead to severe consequences on the fate and reputation of the system, e.g., similar to the Libor scandal.

References

[1] Bitcoin Wiki, Available from https://en.bitcoin.it/wiki/.

[2] Evaluating User Privacy in Bitcoin, In Proceedings of Financial Cryptography and Data Security Conference (FC), 2013. Available from http://eprint.iacr.org/2012/596.pdf.

[3] IRC Bitcoin incident resolution, Available from http://bitcoinstats.com/irc/bitcoin-dev/logs/2013/03/11.

[4] Bitcointalk Forum - Available from https://bitcointalk.org/.

[5] Switch to namecoin; a reflection on community, Available from http://courses.ischool.berkeley.edu/i290m-ocpp/site/article/nmerrill-assign3.html.

[6] Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2012. Available from http://eprint.iacr.org/2012/248.pdf.

[7] Bitcoin Gateway, A Peer-to-peer Bitcoin Vault and Payment Network, 2011. Available from http://arimaa.com/bitcoin/.

[8] Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy, 2011. Available from http://ssrn.com/abstract=1937769ordoi:10.2139/ssrn.1937769.

[9] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On Bitcoin and Red Balloons. In Proceedings of the ACM Conference on Electronic Commerce (EC'12), 2012.

[10] C. Decker and R. Wattenhofer. Information Propagation in the Bitcoin Network. 13-th IEEE International Conference on Peer-to-Peer Computing, 2013.

[11] Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. Proceedings of Financial Cryptography, 2013.

[12] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. Structure and anonymity of the bitcoin transaction graph. *Future Internet*, 5(2):237–250, 2013.

[13] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In Yaniv Altshuler, Yuval Elovici, Armin B. Cremers, Nadav Aharony, and Alex Pentland, editors, *Security and Privacy in Social Networks*, pages 197–223. Springer New York, 2013.

[14] Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph. In Proceedings of Financial Cryptography, 2013.

[15] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.