Is Bitcoin a Decentralized Currency?

Arthur Gervais | ETH Zurich
Ghassan O. Karame | NEC Laboratories Europe
Vedran Čapkun | HEC Paris
Srdjan Čapkun | ETH Zurich

Bitcoin has achieved popularity by promising users a fully decentralized, low-cost virtual currency system. However, a limited set of entities controls Bitcoin's services, decision-making, mining, and incident resolution processes. These entities can decide Bitcoin's fate, bypassing the will of the multitude of users that populate the network.

Bitcoin has witnessed wider adoption and more attention than any other digital currency proposed to date. One reason for this has been the promise of a low-cost and decentralized currency that's inherently independent of governments and any centralized authority. In this article, we analyze Bitcoin and show that, contrary to widespread belief, it isn't truly decentralized as it's deployed and implemented today. We also explore possible solutions to enhance Bitcoin's decentralization. We hope our findings solicit further research in this area. (For related work on Bitcoin, see the sidebar.)

Background

Users transfer *Bitcoin coins* (BTCs) to one other by issuing transactions. Each transaction references users by their virtual pseudonyms, called *Bitcoin addresses*. Each address corresponds to a unique public–private key pair, which is used to transfer BTC ownership among addresses. A transaction is formed when a user digitally signs a hash of the previous transaction where this BTC was last spent, along with the future owner's public key, and incorporates this signature in the transaction.[1] Any peer can verify BTC authenticity by checking the signature chain.

Transactions are included in Bitcoin *blocks* that are broadcast to the entire network. To prevent *double-spending attacks*—that is, signing over of the same coin to two different users—Bitcoin uses a hash-based proof-of-work (PoW) scheme to generate blocks. More specifically, a Bitcoin user must find a nonce value that results in a value below a given target when hashed with additional fields (that is, the Merkle hash of a block's valid and received transactions, the hash of the previous block, and a timestamp). If such a nonce is found, users 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*.

After users successfully generate a block, they're granted a fixed amount of BTCs, plus the transaction fees included in the block. This is an incentive for them to continuously support Bitcoin. All users in the network can check the resulting block's correctness by verifying the hash computation. If the block is deemed valid, users append it to their previously accepted blocks, "voting" with their computing power to confirm the BTC's validity. Because each block links to the previously generated block, the chain grows each time a block is generated. To double-spend a BTC, malicious users would have to redo all the work required to compute the block where that BTC was spent and recompute all subsequent blocks in the chain.

Bitcoin's Centralized Processes

Bitcoin aims to fully decentralize its transaction generation and confirmation processes. In fact, the majority of users must support Bitcoin decisions by voting with

 Copublished by the IEEE Computer and Reliability Societies

Related Work on Bitcoin

Bitcoin has received considerable attention in the literature. In "Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy," Matthew Elias investigated the legal aspects of Bitcoin privacy.[1] In "On Bitcoin and Red Balloons," Moshe Babaioff and his colleagues addressed the lack of incentives for Bitcoin users to include recently announced transactions in a block.[2] Furthermore, in "Bitcoin Gateway, A Peer-to-Peer Bitcoin Vault and Payment Network," Omar Syed and Aamir Syed proposed a user-friendly technique to manage Bitcoin wallets.[3] In "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," Karame and his colleagues investigated double-spending attacks in Bitcoin and showed that users can double-spend fast payments in spite of Bitcoin developers' recommended measures.[4] This analysis was later extended by Christian Decker and Roger Wattenhofer in "Information Propagation in the Bitcoin Network."[5]

In "An Analysis of Anonymity in the Bitcoin System," Fergal Reid and Martin Harrigan analyzed the flow of Bitcoin transactions in a small part of a Bitcoin log.[6] In "Evaluating User Privacy in Bitcoin," Elli Androulaki and her colleagues evaluated Bitcoin users' privacy and showed that Bitcoin leaks considerable information about users' profiles.[7] In "Quantitative Analysis of the Full Bitcoin Transaction Graph," Dorit Ron and Adi Shamir analyzed Bitcoin users' behavior.[8] In "Structure and Anonymity of the Bitcoin Transaction Graph," Micha Ober and his colleagues studied Bitcoin's time evolution properties by analyzing its transaction graph.[9] Finally, in "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," Tyler Moore and Nicolas Christin studied the economic risks that investors face owing to Bitcoin exchanges.[10]

References

1. M. Elias, "Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy," Social Science Research Network, 3 Oct. 2011; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769.
2. M. Babaioff et al., "On Bitcoin and Red Balloons," *Proc. ACM Conf. Electronic Commerce* (EC 12), 2012, pp. 56–73.
3. O. Syed and A. Syed, "Bitcoin Gateway, A Peer-to-Peer Bitcoin Vault and Payment Network," Arimaa, 26 July 2011; http://arimaa.com/bitcoin.
4. G.O. Karame, E. Androulaki, and S. Čapkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," ACM CCS, 2012; http://eprint.iacr.org/2012/248.pdf.
5. C. Decker and R. Wattenhofer, "Information Propagation in the Bitcoin Network," *Proc. 13th IEEE Int'l Conf. Peer-to-Peer Computing*, 2013, pp. 1–10.
6. F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," *Security and Privacy in Social Networks*, Y. Altshuler et al., eds., Springer, 2013, pp. 197–223.
7. E. Androulaki et al., "Evaluating User Privacy in Bitcoin," *Proc. Financial Cryptography and Data Security Conference* (FC 13), 2013; http://eprint.iacr.org/2012/596.pdf.
8. D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *Financial Cryptography and Data Security*, LNCS 7859, Springer, 2013, pp. 6–24.
9. M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and Anonymity of the Bitcoin Transaction Graph," *Future Internet*, vol. 5, no. 2, 2013, pp. 237–250.
10. T. Moore and N. Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," *Financial Cryptography and Data Security*, LNCS 7859, Springer, 2013, pp. 25–33.

their computing power. Given the huge computing power the Bitcoin system harnesses—approximately 70,000 tera hashes per second—users believe that it's unlikely for any one entity to acquire too much power. However, critical processes in the Bitcoin ecosystem are controlled by a small set of entities whose influence doesn't depend on their computing power but on their function in the system.

Bitcoin Services

Bitcoin has led to the emergence of several centralized services that take up a considerable share of the Bitcoin market.

Mining pools. Again, Bitcoin resists double-spending attacks by using a distributed PoW-based service.[1] The idea is that as long as the majority of users expending computing power are honest, Bitcoin can guarantee transactions' security. This implicitly assumes that computing power is shared among all network users that participate in the mining process.

Because block mining in Bitcoin is rewarded with BTCs, it's become a competitive process. An "arms race" has emerged using various hashing technologies specifically designed for mining, including high-end graphical processing units; field-programmable gate arrays; and recently, application-specific integrated circuits

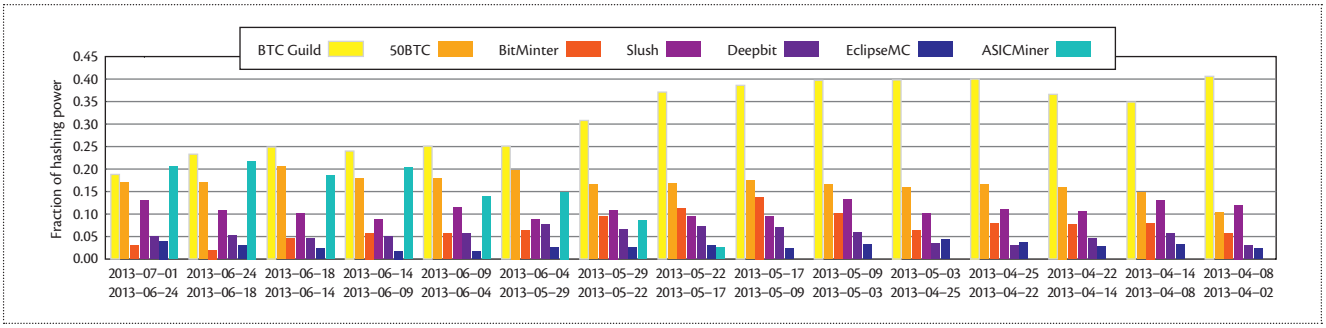

Figure 1. Bitcoin's computing power distribution between 2 April 2013 and 1 July 2013. BTC Guild and 50BTC controlled more than 55 percent of network computing power, until ASICMiner achieved more than 20 percent of the hashing power.

(ASICs). Currently, the probability of finding a block in a single trial is approximately $3 \cdot 10^{-20}$.

To guarantee miners' regular payouts, a central *mining pool* combines their computing power and coordinates participants' mining activities. Here, a mining pool administrator outsources the search inputs for a PoW problem—for instance, the version, difficulty, and last block hash—and asks miners to find a solution for the specific problem. In these systems, all participating miners receive a fraction of BTCs each time a PoW is found; this payment is proportional to the computing power they invested in finding the PoW.

This business model has led to the emergence of several such mining pools. Figure 1 depicts Bitcoin's computing power distribution from April to July 2013. Six major centralized mining pools controlled more than 75 percent of Bitcoin's computing power. If these pools colluded to acquire more than 50 percent of computing power share, they could effectively control all transactions, for example, preventing certain transactions' execution, approving a specific set of transactions, or approving double-spending transactions.

Bitcoin Web wallets. A Bitcoin client installation currently takes more than 16 Gbytes of disk space and requires several hours to download and index the block chain. Therefore, users started relying on *Web wallets*, centralized services that host the main Bitcoin functionalities on a remote server. Accessible through a website, Web wallets are instantly functional, don't occupy hard disk space, are accessible anywhere, and are more convenient than a local Bitcoin client.

Different types of Web wallets have emerged. Some store the private keys on the server side, whereas others store them locally in users' browsers. Depending on where the private key is stored, Web wallet operators can gain unilateral power over their users' BTCs. For example, in April 2013, a theft of 923 BTCs occurred in the OzCoin mining pool. A subset of the stolen BTCs was transferred to a Web wallet hosted by StrongCoin. Although StrongCoin claims that it supports user privacy and doesn't have access to users' funds, it intercepted the allegedly stolen BTCs and transferred them back to OzCoin. StrongCoin's decision was made by a few entities without acquiring consensus from the majority of network users.

Simplified payment verification. SPV consists of a modified Bitcoin client, or node, that partially verifies transactions or blocks in the Bitcoin network. SPV relies on several Bitcoin nodes that forward transactions and blocks to all connecting nodes; the SPV nodes then simply verify the validity of the blocks and transactions that they receive. SPV clients were introduced because the default Bitcoin client consumes a significant amount of power and storage, which most smartphones can't afford. This service comes at cost of decentralization because many clients now place their trust in a smaller group of nodes.

Protocol Maintenance

Bitcoin's core developers have the authority to modify Bitcoin protocol. According to the Bitcoin Github repository, all radical decisions require consensus among all the developers. For example, in Bitcoin client version 0.8.2, the developers unilaterally decided to lower the default fee for low-priority transactions from 0.0005 BTC to 0.0001 BTC. This empowers the developers to regulate the entire Bitcoin economy.

Bitcoin developers try to increase the client development process's transparency by logging ideas and thoughts on public forums and Internet Relay Chat channels. However, it's unclear how potential disputes would be resolved because this would require appropriate regulatory frameworks—a move that goes against Bitcoin's very nature.

In addition, Bitcoin users don't have direct influence over the administrators' appointment, which is somewhat ironic because some users opt for Bitcoin to avoid centralized control typically exercised over national currencies.

Block chain forks. During normal Bitcoin operation, miners work to extend the network's longest block chain. If miners don't share the same view—for instance, owing to network partitioning—they might work on different chains, resulting in forks.

Block chain forks are detrimental for Bitcoin operation. Because one block chain will eventually prevail and become the longest, all transactions included in all other chains will be invalidated by miners in the system. Note that Bitcoin doesn't embed a mechanism to alleviate this problem; instead, if a fork persists for a considerable time period, Bitcoin developers must favor one chain at the expense of the other.

On 11 March 2013, a fork required developer intervention. Bitcoin client version 0.7 stored the block chain in Berkeley DB, whereas client version 0.8 switched to the more efficient LevelDB database. Version 0.7 sets its threshold for the maximum number of concurrency locks per database update to 10,000; version 0.8's limit was 40,000. This discrepancy caused a serious fork starting from block 225,430. The block contained approximately 1,700 transactions, affected more than 5,000 block index entries, and exceeded the required number of locks for version 0.7 (each block index entry requires around two locks in Berkeley DB).

All version 0.7 miners rejected block 225,430 and continued working on a block chain that didn't include it, whereas version 0.8 miners accepted the block and added it to their chain (see Figure 2). The chain that version 0.8 clients adopted was supported by the majority of the network's computing power, exceeding the 0.7 clients' chain by 13 blocks at block 225,451. Nevertheless, 90 minutes after the fork occurred, the Bitcoin developers decided the shorter chain should be the genuine one and convinced the owner of BTC Guild, the biggest mining pool, to support this decision.

This decision was odds with Bitcoin's claim that it's a decentralized system and that the majority of the computing power regulates its decisions. Fewer than 10 entities outvoted the majority of the network's computing power (http://bitcoinstats.com/irc/bitcoin-dev/logs/2013/03/11). Such influential entities can also make more radical decisions, including accepting or rejecting transactions.

Alert mechanism. The Bitcoin client introduced alert messages after version 0.3.10. These messages serve to alert the users of critical incidents; for example, if there's a severe vulnerability in the Bitcoin client, the developers can issue an alert message. However, as we demonstrate later, these messages can be abused, for instance, to deflate the value of coins in the system.

Because alert messages are cryptographically signed, they can be sent only by people who possess the appropriate cryptographic key (Satoshi Nakamoto, the anonymous founder of Bitcoin, still has access to the key). Currently, this key is shared among Bitcoin developers, giving them power to reach out to users and urge them to adopt a given Bitcoin release. The alert payload format supports a `RESERVED` string that currently isn't being used.

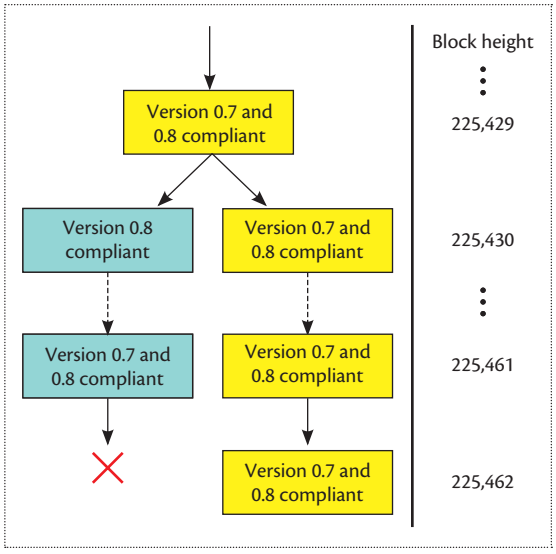

Figure 2. Sketch of the block chain fork that occurred in Bitcoin on 11 March 2013. Despite receiving less support from users, version 0.7 was chosen by developers to be the official chain.

Bitcoin Improvement Proposals. To gather suggestions on Bitcoin development processes, the developers ask users to file a Bitcoin Improvement Proposal (BIP). The developers assess the BIPs and unilaterally decide whether each proposal will be reflected in future Bitcoin releases. This limits users' impact—irrespective of their computing power—to affect the development of the official Bitcoin client. Bitcoin developers have acknowledged the BIP submission process's limitations and proposed adopting methodologies similar to the Internet Engineering Task Force drafts wherein participants describe methods, new protocols, or techniques applicable to the Internet.[2]

Coin Tainting

Because Bitcoin transactions basically consist of a chain of digital signatures, expenditure of individual coins can be tracked publicly. These public logs can have negative effects that extend beyond known privacy and anonymity concerns.[3] For example, because any BTC (or its fraction) can be traced to its origin, Bitcoin users can decide not to accept coins that appear to have originated from a particular address. This user decision will deflate these

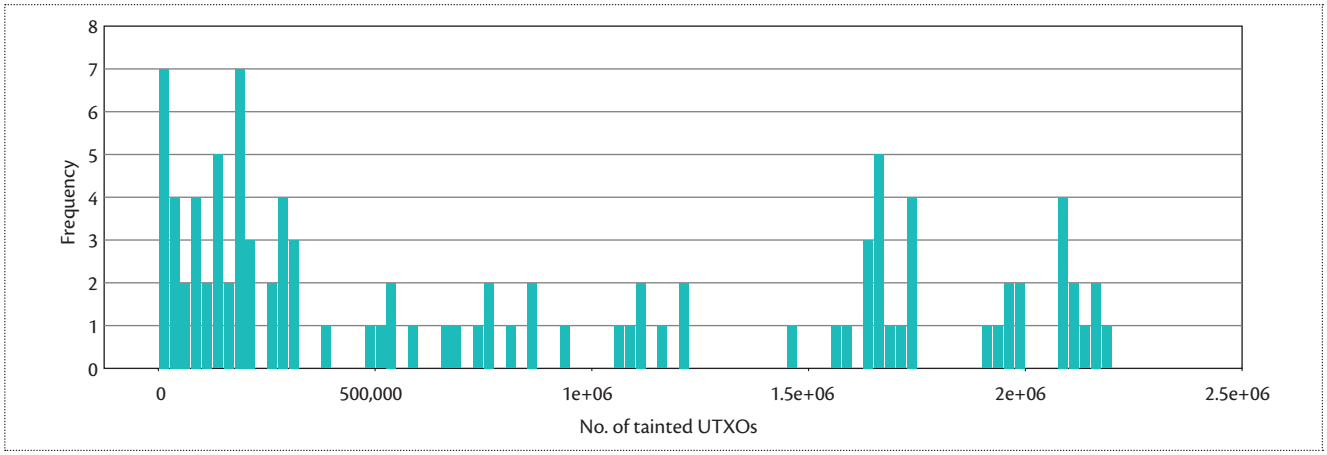

Figure 3. We tainted 100 random coinbases between blocks 227,054 and 247,054 and counted the number of affected unspent transaction outputs (UTXOs). Tainting a single coinbase affected, on average, 857,239 UTXOs, with a standard deviation of 767,528, accounting for 12.9 percent of all UTXOs.

coins' value because other users become reluctant to accept them as payment. We call this effect *coin tainting*.

Any entity can taint coins belonging to a specific address or set of addresses and monitor their expenditure across the network. The literature features several proposals that cluster Bitcoin addresses[3–5] and gather behavioral information about them.[5,6]

Coin tainting is used to achieve a degree of accountability in the Bitcoin network; if an address misbehaves, Bitcoin users can decide to stop interacting with it—that is, not accept its coins—thus deflating the value of all BTCs connected to that address. For instance, after a theft of 43,000 BTCs from trading platform Bitcoinica, Bitcoin service MtGox traced the stolen BTCs and locked accounts that received the tainted coins.

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 who have privileged rights in the system, they can warn all Bitcoin users not to accept BTCs from a given address, for instance, by using alert messages. Even worse, developers can hardcode a list of banned Bitcoin addresses in the official Bitcoin client releases, blocking all interactions with a given address without users' consent.

Furthermore, coin tainting can be abused to control the financial flows in the network. A few powerful entities that aren't necessarily part of the Bitcoin network, such as governments and activists, could regulate the Bitcoin economy, for example, by legally penalizing trade with specific addresses. Even if all Bitcoin decisions and operations were completely decentralized, coin tainting presents an obstacle to a truly decentralized Bitcoin.

Coin tainting is especially detrimental if BTCs aren't widely exchanged among Bitcoin addresses. This enables entities to damage only a specific set of addresses without alienating others. Other users would also likely boycott the tainted coins.

We conducted two experiments to analyze coin tainting's impact on the Bitcoin network. In the first experiment, we measured the number of unspent transaction outputs (UTXOs) affected when tainting a *coinbase*. A coinbase is the first transaction in a block and attributes the block mining reward to an address. We randomly sampled 100 coinbases from the last 20,000 blocks of a chain that, at the time of the experiment, had a maximum block height of 247,054.

Our results show that tainting a single coinbase affects many transaction outputs—on average, 857,239 UTXOs, with a standard deviation of 767,528, accounting for 12.9 percent of all UTXOs. Figure 3 depicts our sampled coinbases' resulting distribution of affected UTXOs.

In a second experiment, we analyzed the effect of tainting addresses belonging to a single Bitcoin entity. Given the absence of data to identify these addresses, we relied on two heuristics, adapted from Elli Androulaki and her colleagues, to cluster addresses across entities.[3]

Heuristic I—multi-input transactions. A multi-input transaction occurs when a user wants to perform a payment, and the payment amount exceeds the value of each of the available input BTCs in the user's wallet. Bitcoin clients choose a set of BTCs from the user's wallet, such that the aggregate value matches the payment, and perform the payment using multi-input transactions. If these BTCs are owned by different addresses, we can conclude that the input addresses belong to the same user.

Heuristic II—shadow addresses. When a user performs a transaction, the main Bitcoin client generates a shadow

address to collect change. This mechanism lets us distinguish shadow addresses. If a Bitcoin transaction has n output addresses with only one new address—that is, the address has never appeared in the transactions log—and all other addresses correspond to an old address, we can assume with reasonable confidence that the new one is a shadow address for the input address. Note that the official Bitcoin client began supporting multiple-recipient transactions on 16 December 2010.

Tainting a single entity. These heuristics combined can provide only a best-effort estimate on the number of addresses per entity. Eight-five percent of the entities that we discovered using these heuristics had only one address, whereas 9,845—0.122 percent—had more than 40. Our results show that tainting a single entity's addresses in Bitcoin would result in devaluating an average of 1.42 BTCs, with a standard deviation of 127.58 BTCs. Figure 4 shows the distribution of Bitcoin addresses per Bitcoin entity.

As an exemplary application of our analysis, we identified two Bitcoin addresses belonging to Torservers.net using information available from https://blockchain.info. Given the knowledge of these two addresses, we identified 47 addresses belonging to the Torservers operator, with a total balance of 498.20 BTCs. If an external entity, such as a government institution, wanted to stop Torservers from receiving Bitcoin donations, it could taint all UTXOs of the affected Bitcoin addresses.

This situation occurred with Silk Road—one of the most well-known underground online black markets, which the Federal Bureau of Investigation shut down in October 2013. Note that Silk Road was accessible only through the Tor network; however, the FBI seized more than 27,000 BTCs stored in one or more Bitcoin addresses.

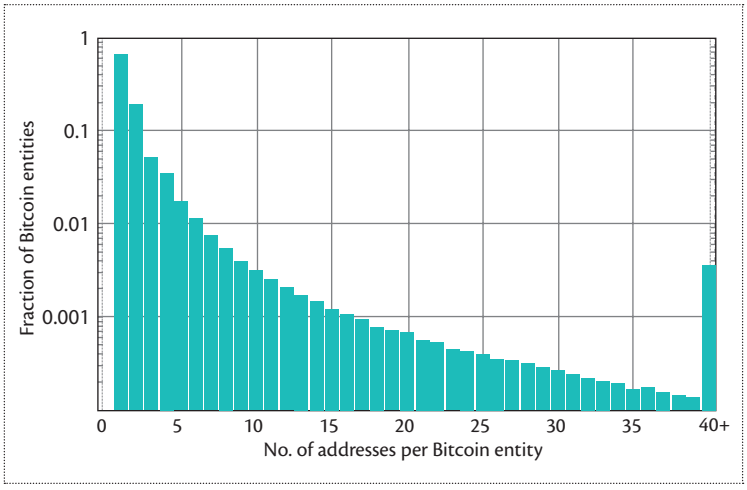

Figure 4. Number of addresses per Bitcoin entity. Eighty-five percent of the entities had only one address, whereas 9,845—0.122 percent—had more than 40.

Enhancing Decentralization

Here, we explore possible ways to enhance Bitcoin's decentralization.

Mining Pools

Whereas most mining pool protocols have a logically centralized operator that orchestrates the block generation process, several fully decentralized mining pools, such as P2Pool, are emerging. Such pools share the benefit of centralized pools because all participating users get regular payouts that reflect their contribution to block generation. However, these pools don't require a centralized coordinator and operate in a completely decentralized fashion. P2Pool holds only a marginal share of the network's computing power; we hope that such decentralized pools become profitable businesses and attract a majority of miners.

One Vote per Client

Bitcoin relies on the notion of *controlled supply*; the number of BTCs generated for each block is halved every four years. This limits the total number of generated BTCs, so mining pools' dominance is expected to decrease with time because their profits will likely depend less on self-awarded BTCs and more on transaction fees. This, in turn, will increase individual users' contribution to the Bitcoin economy because users decide which Bitcoin client they operate and how much they're willing to pay in fees per transaction. Consequently, mining pool operators would have less incentive to accept client versions adopted by a minority of clients. Users would then contribute more to Bitcoin's decision-making process by adopting a client version that suits their preferences. Recall that because Bitcoin's source code is open source, several different Bitcoin implementations already exist.

Transparent Decision-Making

In some settings, it's inevitable that various client versions and implementations require constant maintenance and development by a group of leading developers. Here, problems arise in situations in which the developers must resolve possible conflicts. This process must be completely transparent and should be tightly regulated to avoid abusing users' trust and minimize unilateral interventions. To prevent the abuse of alert messages, the developers could append justifications to their alerts. Users can decide whether to accept the warnings on the basis of these justifications. For instance, double-spending alerts can include transactions showing that a given address is double-spending.[7]

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

Marketplaces, SPV Clients, and Web Wallets

Centralized services, such as marketplaces and Web wallets, have emerged to facilitate the use of Bitcoin's decentralized protocol. Indeed, this shows the lack of foresight when deploying Bitcoin because several of its decentralized aspects aren't user friendly. For instance, users find maintaining local wallets cumbersome and don't want to download the entire block chain during client installation.

Note that, despite its many limitations, decentralization of services provides users higher availability assurances. In February 2014, MtGox first stopped BTC withdrawals and then closed its website—a move that affected thousands of Bitcoin users. Currently, only a handful of services enable user-friendly BTC trade and storage. As of March 2014, three Bitcoin exchanges—Bitstamp, Bitfinex, and btc-e—handle more than 80 percent of USD-to-Bitcoin trading. We hope similar services will form to reduce the current oligopoly's market share.

Although Bitcoin originally aimed to be fully decentralized, recent events revealed the limits of decentralization in this system. Many centralized services host Bitcoin and control a considerable share of the Bitcoin market. Even worse, Bitcoin developers retain privileged rights in conflict resolution and maintenance of the official client version. Together, these entities can decide the Bitcoin system's fate, bypassing the will, rights, and computing power of the multitude of users on the network.

Governments and banks control almost every financial system; Bitcoin substitutes these powerful entities with other entities, such as IT developers and mining pool owners. Whereas 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 now finds itself in unfamiliar territory: on one hand, the Bitcoin ecosystem is far from being decentralized; on the other, the system's increasing centralization doesn't abide by any transparent regulations or legislations. This could lead to severe consequences to Bitcoin's fate and reputation. ■

Acknowledgments

Vedran Čapkun received financial support from the HEC Foundation, Investissements d'Avenir (ANR-11-IDEX-0003/Labex Ecodec/ANR-11-LABX-0047).

References

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009; https://bitcoin.org/bitcoin.pdf.
2. J. Garzik, "[Bitcoin-Development] Revisiting the BIPS Process," Mail Archive, 21 Oct. 2013; https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg02982.html.
3. E. Androulaki et al., "Evaluating User Privacy in Bitcoin," *Financial Cryptography and Data Security*, LNCS 7859, Springer, 2013; http://eprint.iacr.org/2012/596.pdf.
4. F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," *Security and Privacy in Social Networks*, Y. Altshuler et al., eds., Springer, 2013, pp. 197–223.
5. D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *Financial Cryptography and Data Security*, LNCS 7859, Springer, 2013, pp. 6–24.
6. M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and Anonymity of the Bitcoin Transaction Graph," *Future Internet*, vol. 5, no. 2, 2013, pp. 237–250.
7. G.O. Karame and E. Androulaki, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," *Proc. ACM Conf. Computer and Communications Security* (CCS 12), 2012; http://eprint.iacr.org/2012/248.pdf.

Arthur Gervais is a PhD student in the Institute of Information Security at ETH Zurich. His research interests include Bitcoin security and Web privacy. Gervais received MS degrees in security and mobile computing from KTH Stockholm and Aalto University, Finland, as well as a diplôme d'ingénieur in computer science from INSA de Lyon. Contact him at arthur.gervais@inf.ethz.ch.

Ghassan O. Karame is a senior researcher in the Security Group of NEC Research Laboratories, Germany. His research interests include security, privacy, and applied cryptography, with a focus on cloud, SDN/network, and Bitcoin security. Ghassan received a PhD in computer science from ETH Zurich. Contact him at ghassan@karame.org.

Vedran Čapkun is an associate professor in the Department of Accounting and Management Control, HEC Paris, and a member of GREGHEC. His research interests include operational efficiency, bankruptcy, and international accounting. Čapkun received a PhD in management from the University of Lausanne. Contact him at capkun@hec.fr.

Srdjan Čapkun is an associate professor in ETH Zurich's Department of Computer Science and director of the Zurich Information Security and Privacy Center. His research interests include system and network security, particularly wireless security. Čapkun received a PhD in communication systems from EPFL. Contact him at capkuns@inf.ethz.ch.