Bitcoin

Arnis Parsovs

December 17, 2013

Abstract

Bitcoin is a distributed, peer-to-peer cryptocurrency that functions without any central authority and in recent years has gained large popularity. This paper describes how Bitcoin functions and what are the assumptions that must hold for Bitcoin to be healthy and attractive currency.

1 Introduction

Bitcoin concept [1] was introduced in 2008 by a pseudonymous person or group known as "Satoshi Nakamoto". On January 2009 Satoshi released the first Bitcoin payment system software and was the first to run the node on the Bitcoin network. Today Bitcoin network processes 60 thousand transactions per day with the total amount of money in Bitcoin network estimated to be worth more than 8 billion USD [2].

The popularity of Bitcoin currency can be explained by its property that no central authority is required for it to function. This has attracted people who support anti-government philosophy and those that are afraid that government could block their transactions or confiscate the money held in their accounts.

Bitcoin has been named as the next big thing after the invention of Internet, therefore, let's see how it works and whether the claims brought by Bitcoin actually hold.

2 Bitcoin system

Traditional banks function by maintaining a central ledger of all transactions that have been made. This way the bank can tell what is the balance of a particular account and new transactions can be added into the ledger after the account holder has been identified and his will to perform the transactions has been verified. The bank here is a central authority and it is the bank's responsibility to preserve integrity of the ledger and authenticate the account holders before registering transactions. Since the Bitcoin aims to eliminate central authority, it has to provide alternative means for account holders to

verify integrity of Bitcoin ledger in order to agree on "who owns what" and to authenticate account holders before transaction can be written in the ledger.

Bitcoin provides decentralization by maintaining distributed transaction log of all transactions that have been made. Accounts are identified by ECDSA public keys and transactions are authorized by account holders signing transactions using corresponding private key. The authenticity and integrity of transaction log is maintained using proof-of-work system.

2.1 Addresses

Bitcoin has a concept of sending bitcoins to an address [3]. The address is RIPEMD-160 hash of SHA-256 hashed ECDSA public key. After the transaction has been made to the address, whoever has a corresponding private key can respend that money. Anyone who has a ECDSA key pair is a potential account holder in Bitcoin system.

2.2 Transactions

Transactions are shown in Figure 1. Any transaction can have several inputs and outputs. Input specifies reference to previous transaction output which will be respent in current transaction. Every input must be unlocked, i.e., the transaction has to be signed using the key pairs specified in the outputs that current transaction is referencing in its inputs. Outputs specify amount of bitcoins and Bitcoin addresses where the bitcoins should be sent. Every referenced input must be completely spent, which means that usually the second output of transaction is used to specify address where the change should be sent. If the sum of output amount is less then unlocked inputs, then this difference is considered to be a transaction fee.

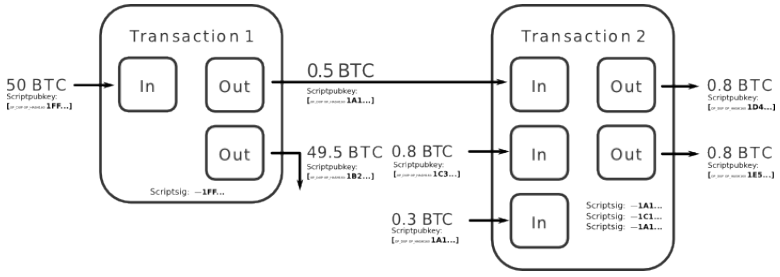

Figure 1: Transaction example[1]

[1]Source: `https://bitcointalk.org/index.php?topic=279249`

2.3 Proof-of-Work System

The authenticity of Bitcoin transaction log is provided by Hashcash [4] proof-of-work system. Proof-of-work system allows a verifier to verify that prover has performed some type of work. In Hashcash system the prover proves that he has spent specific amount of computing resources in order to solve the challenge received from the verifier. The challenge presented requires the prover to find a *nonce* such that the hash of this nonce is prefixed with specific amount of zero bits. While the prover has to use brute force to find a solution, the verifier can verify whether the solution is found by single hash operation. By changing the number of prefixed zero bits that needs to be found in the hash, the *difficulty* of proof-of-work system can be adjusted.

2.4 Blockchain

In Bitcoin system the authenticity of the public transaction log is provided by process called "mining". The transactions are included in blocks that are constructed using proof-of-work system and where every block is cryptographically bound to previous block thus creating a blockchain.

The contents of block is shown in Figure 2. In mining process, the miners are trying different nonce values until the block header hashes to value that satisfies proof-of-work difficulty required by the protocol. Once the block is mined, the miner broadcasts the mined block through the network. At this point all miners stop their mining process and start to work on a new block that has a reference to the recently found block. If there are two blocks found simultaneously, the miners work on the first block received, but keeping in memory alternative block. Once the another block is found the miners switch to the longest chain that has largest total difficulty.

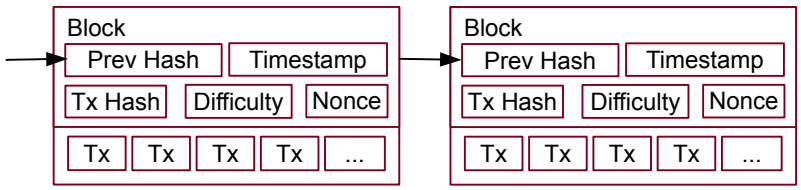

Figure 2: Contents of Bitcoin block

Blockchain produced in this mining process allows anyone to calculate the amount of computing resources that were required to construct the blockchain. The blockchain that was produced by using significant computing resources gives an assurance that the blockchain could not have been produced by an individual attacker. This provides a confidence that the transaction log was most likely produced by whole community and therefore should be consensus log.

The mining is motivated by allowing miners to receive all transaction fees of transactions that are included in the mined block and receiving 25 bitcoins

per mined block "out of thin air". The amount of bitcoins that can be received through mining process is hardcoded in the protocol. This amount is halved every 210000 blocks. The difficulty of proof-of-work system is also adjusted per every 2016 blocks such that the difficulty for mining the block would be 10 minutes on average. The difficulty is adjusted by all participants using timestamp that is included in every block. The timestamp of recently mined block must fall in certain boundaries [5]

2.5 Peer-to-Peer Network

Bitcoin peer joins the Bitcoin network by connecting to other peers using TCP port 8333. Peers should connect to several other peers in order to provide better network connectivity and distribution of information. The Bitcoin protocol [6] allows peers to broadcast IP addresses of other network peers, transactions received in unconfirmed transaction pool and recently mined blocks. Peer can also request any historical block or block header stored in the transaction log.

Every peer must relay only these transactions and blocks that have been verified to be valid. In order to prevent denial-of-service attacks, peers should disconnect and temporary block other peers who do not follow the protocol.

2.6 Anonymity

Since the transaction log is public and all transactions are stored forever, the transaction log can be analyzed by anyone using state of the art data mining techniques. Although the transactions are performed between public keys, the research [7] has shown that the owners of public keys can be identified with some effort.

In order to use Bitcoin anonymously, the user has to make sure that the party that sends bitcoins to the user and the party that receives bitcoins from the user does not know any additional information that can be used to link user's Bitcoin address to the user's physical identity. To make transaction tracing more difficult the mixing services [8] can be used. The mixing service works by collecting bitcoins from several clients, then aggregating them together and finally forwarding the coins to some new Bitcoin addresses that are owned by the same clients. This makes harder for the observer to track transaction flow. However, the mixing service must be trusted to destroy logs and to not disappear with the coins.

Zerocoin [9] proposal provides true anonymity by using zero-knowledge proofs and one-way accumulators. However, the scheme is currently not very efficient since the proof requires 40KB of space and takes 2 seconds to verify.

3 Security Assumptions

There are several assumptions that must hold for Bitcoin system to be healthy and bitcoins valuable.

3.1 Security of Cryptographic Primitives

ECDSA curve secp256k1 is used to authorize Bitcoin transactions. If it were to be compromised, the attackers could respend coins that do not belong to them. Similar attack is possible if the attackers could generate another ECDSA key pair whose public key RIPEMD-160(SHA-256()) hash would collide with the hash that is encoded in victim's Bitcoin address.

Proof-of-work function used by Bitcoin uses double SHA-256 hash on block header. If the attacker would know a shortcut that would allow him to find solution faster than the other participants could find, he would have unequal advantage that could result in producing most of the solutions thus controlling majority of network hashpower.

Although the primitives used by Bitcoin system are believed to be secure, there has been a case where incorrect use of random generator on Android platform has allowed attacker to steal bitcoins [10].

3.2 Majority of Network Hashpower

Security of Bitcoin system depends on honest participants having majority of network hashpower. Malicious majority could overwrite transaction history at will, which would allow to execute double spending attacks. Similarly, malicious majority could paralyze the network by not including transactions in mined blocks or extort other participants by requiring transactions to have large transaction fees. Satoshi in [1] states that profit-seeking majority will always gain more by following the rules. However, this ignores the attacker who would gain more by destroying the Bitcoin. For example, the attacker who is short selling bitcoins is interested in bitcoins losing its value. Similarly, the attacker who runs competitive digital currency network is interested in moving clients from the destroyed Bitcoin network to his network. The attacker who has a pure political objective in destroying the network should also not be neglected.

Some researchers believe [11] that even a coalition with 1/3 of the hashpower could gain control over the network by employing so called selfish-mining strategy, where selfish miners always try to work on their own branch without immediately announcing mined blocks.

Currently hashpower distribution between Bitcoin users is unequal, since currently mining is performed by relatively small group of people who use special purpose hardware that provides considerably more hashpower than general purpose CPUs can provide. There have been suggestions to switch to other proof-of-work function that would not create a significant advantage by using special purpose hardware for mining [12].

It is not clear how much money currently must be invested in special mining hardware in order to obtain majority of hashpower, but it is believed that the existence of such majority would create a immediate threat to confidence in the system.

3.3 Network Integrity

Another significant security assumption requires that the attacker is not able to isolate or partition honest participants from the Bitcoin network. If the network would be split into two parts, every part would mine on its own blocks which would create two forks of the blockchain. Since the forks cannot be merged, after the reunion the chain having largest total difficulty would win, leaving transactions in losing chain unconfirmed. This would create havoc and immediately undermine confidence in the system. However, it is unlikely for the Internet to be partitioned such that no link exists between the network parts.

More realistic is the attack where single participant is targeted by isolating him from the network and impersonating network peers he is trying to communicate with. However, since the attacker would have relatively small hashpower, the attacker could not be able to produce new blocks in meaningful time and therefore successful double spending attack will not succeed before the victim detects sudden abnormal hashpower decrease. However, if major miners can be isolated from the network, the attacker might obtain majority of hashpower.

3.4 Efficiency

Since the Bitcoin network does not have any trusted authority, the Bitcoin participants themselves have to enforce every rule, which requires them to obtain and validate every transaction in the transaction log. Currently size of the transaction log is 11 GB [13] and we can expect that it will grow even faster by Bitcoin gaining popularity. The obvious problem is that running Bitcoin node will require to have a significant CPU, memory and storage resources. While the requirements are not yet a problem for specialized servers, the mobile devices are not going to have such resources. We see that increasingly popular becomes concept of thin clients [14], where clients offload transaction verification to trusted nodes operating on full transaction log. Other trend is to store Bitcoin wallets and perform transactions using web services. Both of these approaches introduce trusted authorities that may become central point of failure to the decentralized Bitcoin system.

While Satoshi in [1] describes a method on pruning transaction log from spent transactions, the method has never been implemented in Bitcoin client and is unlikely to solve the problem of ever growing transaction log.

3.5 Rationality of Participants

As described before, the security of Bitcoin depends on participants acting rationally, since only then they can benefit from the network. While the participants

could deviate from the protocol, the rationale tells that this would damage the system and at the end they would be losers themselves, since the bitcoins they have earned by cheating would lose their value by the act of cheating. For example, there is no direct incentive for miners to pause mining process in order to include in the block the transactions that do not contain transaction fees. However, they have indirect incentive in keeping network healthy and attractive to users.

As shown previously, we believe that this assumption might not hold and that there might be scenarios where not following the protocol could give significant short-term benefits that can be more favorable than the possible long-term losses ("tragedy of the commons" phenomenon). Even more, the behavior of human beings cannot always be explained by rationality and their perception of rational behavior may be influenced by external events.

3.6 Regulation Resistance

As mentioned before, Bitcoin has gained popularity because it is assumed that no central authority can regulate the currency by, for example, inducing additional money supply thereby devaluating the currency or by blocking certain transactions as it can be seen in traditional banking. It is clearly known how much bitcoins will ever be in the system and this certainty is what makes the currency particularly valuable.

However, the hardcoded rules in the client software are not cut into the stone. Even more, in the course of time there might be a need to update the rules in order to improve Bitcoin's system or to fix security flaws that may emerge. It is important to note that the rule change must be supported by (close to) unanimous agreement between Bitcoin users. Otherwise the transaction created or block mined which is valid by one group of users, but invalid by another, will fork blockchain, that, depending on the size of groups, might have unpredictable consequences to the system.

The accidental blockchain fork introduced by software bug in March 11, 2013 [15] showed that agreements between miners can be concluded very fast (although the agreement was not about rule change, but on which forked chain the mining should continue). On the other hand, convincing all Bitcoin users on rule change would need to have very persuasive arguments. One important question here is to what extent such agreements could change the Bitcoin system and would it always serve in the interests of whole population of bitcoin holders.

Currently largest part of community uses official Bitcoin client to run Bitcoin node. This allows software developers of the client to introduce rule changes that most likely will be accepted automatically in the software update process. Any other party that would want to propose rule change is in a disadvantageous position, since they would have to actively convince the whole community about benefits of using their Bitcoin client fork. This rises the question, whether the Bitcoin Project that develops the software does not hold a significant control over the Bitcoin system.

There are some signs that some regulation is actually requested by Bitcoin

users. For example, after frequent cases of large amount bitcoin theft the CoinValidation [16] initiative was created to not process transactions that involve tainted bitcoins, where "tainted" is defined as having relation in the transaction graph with bitcoins that have been reported as stolen. One could argue that removing initiative to steal bitcoins is in the interest of bitcoin system, however, such blacklisting approach not only makes the coins with clean history be more valuable than others, but also allows the authority who maintains the blacklist to enforce regulation on transaction flow.

4 Conclusion

We see that beyond the cryptographic assumptions, the Bitcoin system makes several other assumptions that have not been studied in detail. Bitcoin security must be analyzed in interdisciplinary manner, by including all these aspects in the security model.

References

[1] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. `http://bitcoin.org/bitcoin.pdf`.

[2] blockchain.info. Market capitalization. November 2013. `https://blockchain.info/charts/market-cap`.

[3] Bitcoin community wiki. Address. `https://en.bitcoin.it/wiki/Address`.

[4] Adam Back. *Hashcash - A Denial of Service Counter-Measure*. August 2002. `http://www.hashcash.org/papers/hashcash.pdf`.

[5] Bitcoin community wiki. Block timestamp. `https://en.bitcoin.it/wiki/Block_timestamp`.

[6] Bitcoin community wiki. Protocol specification. `https://en.bitcoin.it/wiki/Protocol_specification`.

[7] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. 2011. `http://arxiv.org/abs/1107.4524`.

[8] Bitcoin community wiki. Mixing service. `https://en.bitcoin.it/wiki/Mixing_service`.

[9] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, SP '13, pages 397–411, Washington, DC, USA, 2013. IEEE Computer Society.

[10] Bitcoin Project. Android security vulnerability. August 2013. http://bitcoin.org/en/alert/2013-08-11-android.

[11] Ittay Eyal and Emin G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. November 2013. http://arxiv.org/abs/1311.0243.

[12] Morgen E. Peck. Bitcoins computing crisis. October 2013. http://spectrum.ieee.org/computing/networks/bitcoins-computing-crisis.

[13] blockchain.info. Blockchain size. November 2013. https://blockchain.info/charts/blocks-size.

[14] Bitcoin community wiki. Thin client security. https://en.bitcoin.it/wiki/Thin_Client_Security.

[15] Bitcoin Project. 11/12 march 2013 chain fork information. March 2013. http://bitcoin.org/en/alert/2013-03-11-chain-fork.

[16] Kashmir Hill. Sanitizing bitcoin: This company wants to track 'clean' bitcoin accounts. November 2013. http://www.forbes.com/sites/kashmirhill/2013/11/13/sanitizing-bitcoin-coin-validation/.