Bitcoin in 7 Layers

Information Systems Mass Attacks and Defence

Robert Pallas 106573 IVCM

Instructors:

Jaan Priisalu

Rain Ottis

Tallinn University of Technology

2011

Table of Contents

1. Introduction

Bitcoin is the world's first decentralized digital currency[1]. It was introduced by programmer Satoshi Nakomoto, who published his paper “Bitcoin: A Peer-to-Peer Electronic Cash System”[2] in cryptography mailing list in 2008 . First piece of client software was released in January 9th 2009[3]. Nakamoto is most likely not a real person[4], but his work might become revolutionary breakthrough in financial world after many commercial ventures to popularize digital currencies like David Chaums Digicash have failed[5]. Unlike other virtual monies it does not have a central clearing house run by a single company or organization. Nor is it pegged to any real-world currency, which it resembles in that it can be used to purchase real-world goods and services, not just virtual ones. However, rather than rely on a central monetary authority to monitor, verify and approve transactions, and manage the money supply, Bitcoin is underwritten by a peer-to-peer network akin to file-sharing services like BitTorrent[6].

To study Bitcoin, describe how it works, look for its shortcomings and possible points of failure a study by Ian Grigg is used as foundation. “Financial Cryptography in 7 Layers” presents a model that seeks to simplify the substantially complex field by placing disciplines that make up financial cryptography into a seven layer model of introductory nature, where the relationship between each adjacent layer is clear[7]. Layers of the model are cryptography, software engineering, rights, accounting, governance, value and finance.

2. Layers of Bitcoin

2.1. Cryptography

At the bottom of the 7 layer model is Cryptography. To some extent, the pure science domain of cryptography solves problems in a mathematical sense only, but it delivers useful properties like confidentiality, integrity and authentication[8]. Those are used by disciplines on higher layers of the model to create a secure system.

Bitcoins use of cryptography is unorthodox, but several security experts such as Dan Kaminsky have audited the system and the code of the original client software and found that it is really well designed[9]. Bitcoin is based on public-key cryptography using Elliptic Curve Digital Signature Algorithm[10]. Well known hashing algorithms SHA-256 and RIPEMD-160 are used to compute Bitcoin addresses and Merkle trees to link the transactions to each other and easily verify them[11]. All transactions are stored in a file called block. Every block contains a hash of previous block and all the files in Bitcoin network to each other creating a block chain.

Another interesting concept added to Bitcoin design is proof-of-work. Proof-of-work is a piece of data that is difficult to produce as generating it is a random process with low probability. Every new block starts with someone finding a nonce to add to previous block so that the hash of this previous block starts with a run of zeros. The found value becomes proof-of-work and the finder gets a reward. Currently the reward is 50 Bitcoins and the one who creates a new block also collects a small fee on every transaction that is recorded within this block. Process of looking for the proof-of-work is called mining.

2.2. Software engineering

It takes Software Engineering to usefully benefit from the properties of cryptography. Database theory and networking theory are used in order to add such properties as reliability and robustness. Software engineering layer provides us with a practical network[12]. Bitcoins network is purely peer-to-peer. All transaction messages are broadcast across the network and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone[13]. This means that in original implementation of Bitcoin all participants hold a copy of database that contains all the transactions that have ever taken place in Bitcoin network, making it very transparent and easy to audit.

Original Bitcoin client is written in C++ and is open-source[14], but several other pieces of software are available to connect to Bitcoin network and participate like Java client BitCoinJ where only headers of blocks are downloaded[15]. One may also choose to use eWallet services to avoid downloading the ever increasing block chain with all transactions, but this results in giving away some of the control over their Bitcoins as well as possibly accepting higher fees on transactions.

Bitcoins strengths versus credit cards, Paypal or any other currency with central clearing house are much lower fees, bigger independence and higher security. Bitcoin user can not be affected by problems with the company running the system, because it is peer-to-peer. Users do not have to worry about losing their data when central entity gets compromised and they are not vulnerable to phising attacks. They can and should however encrypt and backup their private keys because if someone was to gain access to Bitcoin users file system they could take the key and authorize transactions with coins that belong to person who lost their private key.

Bitcoin supports strong anonymity, but current implementation is usually not very anonymous[16]. Network analysis and Bitcoin transaction history can help determine the real people behind Bitcoin transactions in most cases, but using TOR and Bitcoin laundry services decrease the chance of linking dramatically. Overall the anonymity of Bitcoin is somewhere between real cash and credit cards.

2.3. Rights

Rights layer of the model describes users control over their assets. It will provide us with information on who owns what and how can they use it, help us ensure that funds can be sent only by their rightful owners.

Each Bitcoin is associated with its owner's public key. Public key can be calculated from private key, but not vice versa, and Bitcoin address that represent the possible destination of a Bitcoin payment is converted from the public key using series of hashing techniques[17]. Private key is a randomly generated number that is known only to the person who generated it and only someone who knows the private part of the key pair can send the Bitcoins that are associated with the public part of this pair[18]. Transaction of coins means attaching new owners public key to them and signing the message with the private key. This message is then broadcast over the network so all the nodes will know the new owner of the Bitcoins and they can easily verify the transaction.

2.4. Accounting

The previous layers provide methods reliable enough to be used for passing something of value, which we call rights, over an otherwise unsuitable network. Now, we need the techniques of Accounting in order to store and manage rights over time. Accounting concepts permit builders of Financial Cryptography systems to build complex systems that guarantee not to lose value as long as everyone follows the rules and to efficiently identify where the rules are not followed[19].

It is in accounting that Bitcoin may have its greatest impact. It may have shown the first successful wide-scale test of triple entry bookkeeping. Triple entry is a simple idea, albeit revolutionary to accounting, big improvement on double entry bookkeeping which has been used for more than 500 years. A triple entry transaction is a 3 party one, in which each transaction is digitally signed by multiple parties, including at least one independent[20]. According to original design all nodes in peer-to-peer network have information on all transactions which are linked to each other. Transactions get confirmed only after they become acknowledged in a collectively maintained timestamped-list of all known transactions.

2.5. Governance

After we have guaranteed that the digital amounts can be securely passed over the net, and stored on nodes safely, we need to cast our view wider to threats outside the technical domain. Model has a layer labeled Governance to seek solution to the agency problem – how to manage threats from parties who are trusted to manage the system[21] and how to deal with other threats that can not be dealt with in lower layers.

Bitcoin is not a system that relies on trust. All nodes in the network are effectively policing each other. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they will generate the longest chain and outpace attackers[22]. The input of CPU power that is put into mining is rewarded and this makes playing by the rules more profitable. Even creators and administrators of malicious programs and their networks are known to mine Bitcoins with their botnets rather than trying to attack or deceive the system[23].

Perhaps governance layer is where most of Bitcoins problems hide. First of all there is a threat from governments, who are afraid that Bitcoins are used for illegal activities like funding terrorists or other criminal organizations, buying drugs and laundering money. Shutting down the Bitcoin system is extremely difficult, but interested powers may target real-world businesses and stop them from dealing with Bitcoins, possibly removing the chance to exchange Bitcoins to US Dollars and other fiat currencies.

Another problem that Bitcoin might face in the future is not being scalable to very high amount of transactions. As current implementation sees all users hold the copy of entire block chain with all transactions and thus seeing all the traffic in peer-to-peer network running a Bitcoin wallet might become very resource consuming. It might become unfeasible for regular users to have all data on their computers and they must rely on supernodes to confirm transactions and send or receive money. This means that if Bitcoin grows it might become more centralized as fewer entities can and will act as supernodes. Satoshi Nakamoto suggested a solution to this problem in his original white-paper. It is called Simplified Payment Verification, where users need to keep only a copy of the block headers of the longest proof-of-work chain[24]. It is already implemented in BitCoinJ mentioned earlier and core development team is most likely ready to release their version of Bitcoin wallet software with Simplified Payment Verification when needed.

2.6. Value

When a system has stability and security thanks to correctly dealing with challenges in previous layers we need to assign value to the structure. It is important to define the unit of account, the meaning of that unit and the range of numbers that are applicable[25].

The unit of Bitcoin system is 1 BTC. The money supply as well as reward from Bitcoin mining is halved every 4 years. Currently the reward of discovering a block and adding it to the chain is 50 BTC. It will be 25 some time in 2013 and drop until year 2033 after which no more coins will enter circulation. There will be a total of approximately 21 million of them. This is hard-coded into original Bitcoin software and creates high certainty on the supply. Nobody can randomly create extra money out of nothing, proof-of-work is needed. Bitcoins are divisible down to eight decimal places so the range of numbers is huge, making dealing with possible deflation in case of mass adoption in the future feasible[26].

As of December 13 2011 BTC is worth about 3,2 USD (2,4 EUR)[27]. The volatility of Bitcoin has been huge during its short existence. After getting a lot of media attention in the spring off 2011 the price of Bitcoin exploded. From early April to the end of May, the going rate for 1 BTC rose from 86 cents to $8,89. After Gawker published a story about currency’s popularity among online drug dealers, it more than tripled in a week, reaching a maximum of almost $30[28]. Bitcoin bubble exploded as fast as it was created and the fact that Mt. Gox, the site responsible for most of the Bitcoin to USD currency exchange got hacked did not influence the value of Bitcoins positively[29]. During the last few months Bitcoins exchange rate to real-world currency's has been more stable however, but there is no certainty that the value is given to it by normal users not speculators. Bitcoin economy is still pretty small and the amount of total users seems to be dropping[30]. This is probably due to investors losing faith and miners giving up as cost of electricity that is needed to mine Bitcoins is higher than the reward in current competitive environment of looking for proof-of-work to create a new block.

2.7. Finance

On top of the value layer we can build our application. The last layer in the model is called Finance. Here we give the system financial meaning. How can the owners of the currency use it, what services and goods are available, what sort of trading and investment opportunities are there and how the currency acts as intermediary in the labor market[31] are answered in this part of the 7 layer model.

Although the amount of total users is decreasing the amount of total businesses willing to trade in Bitcoins is still pretty good. One may buy music, clothing, electronics, web hosting, pay for professional services, accommodation or their bar tabs via Bitcoin. There are tons of possibilities and accepting Bitcoins has been made very easy for merchants. Several parties accept donations in BTC. Unfortunately many of them are not found on the list of good guys. Anonymous, Wikileaks and LulzSec are not in favor of governments and can not use traditional methods to ask for donations so they use Bitcoins instead. This brings wrong kind of attention on the currency. But shadowy organizations are not the ones bringing the most heat on Bitcoin. Through the anonymizing network TOR anyone can shop for illegal drugs like heroin or cocaine online and pay for them in Bitcoin on Silk Road marketplace[32].

3. Summary

Bitcoin is a peer-to-peer digital currency. “Financial Cryptography in 7 Layers” by Ian Grigg was used to study Bitcoin. Bitcoin is a great idea that is well designed. It uses cryptography to serve layers built on top of it better than any other financial cryptography system in the past. There are possible points of failure in the Bitcoin system, but successful workarounds can easily be implemented in the future. Bitcoin is still very new and needs to gain popularity, but it certainly has no real technical shortcomings and could become a major player in the financial world very soon.

[1] What is Bitcoin?, We Use Coins, March 22 2011, http://www.weusecoins.com/

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October 31 2008, http://bitcoin.org/bitcoin.pdf

[3] Satoshi Nakamoto, Bitcoin v0.1 released, Cryptography mailinglist, January 9 2009, http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

[4] Joshua Davis, The Crypto-currency, The New Yorker, October 10 2011, http://cryptome.org/0005/bitcoin-who.pdf

[5] Steve Bowbrick, Past currency, The Guardian, February 25 2003, http://www.guardian.co.uk/technology/2003/feb/25/comment.comment

[6] Bits and bob, The Economist blog, June 13 2011, http://www.economist.com/blogs/babbage/2011/06/virtual-currency

[7] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[8] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[9] Dan Kaminsky, Some Thoughts on Bitcoin, August 2011, http://www.slideshare.net/dakami/bitcoin-8776098

[10] ECDSA, Bitcoin Wiki, retrieved December 13 2011, https://en.bitcoin.it/wiki/ECDSA

[11] Protocol specification, Bitcoin wiki, retrieved December 13 2011, https://en.bitcoin.it/wiki/Protocol_specification

[12] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[13] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October 31 2008, http://bitcoin.org/bitcoin.pdf

[14] Bitcoin project, Sourceforge, retrieved December 13 2011, http://sourceforge.net/projects/bitcoin/

[15] Software, Bitcoin wiki, retrieved December 13 2011, https://en.bitcoin.it/wiki/Software

[16] Anonymity, Bitcoin talk, July 7 2011, https://bitcointalk.org/index.php?topic=241.0

[17] Bitcoin addresses, Bitcoin wiki, retrieved December 13 2011, https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses

[18] ECDSA, Bitcoin wiki, retrieved December 13 2011, https://en.bitcoin.it/wiki/ECDSA

[19] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[20] Ian Grigg, Is Bitcoin a Triple Entry System?, Financial Cryptography, June 13 2011, https://financialcryptography.com/mt/archives/001325.html

[21] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[22] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October 31 2008, http://bitcoin.org/bitcoin.pdf

[23] Researcher Discovers Distrobuted Bitcoin Cracking Trojan Malware, Infosecurity Magazine, August 19 2011, http://www.infosecurity-magazine.com/view/20211/researcher-discovers-distributed-bitcoin-cracking-trojan-malware/

[24] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October 31 2008, http://bitcoin.org/bitcoin.pdf

[25] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[26] Nathan Willis, Bitcoin: Virtual money created by CPU cycles, Linux info from the source, November 10 2011, http://lwn.net/Articles/414452/

[27] Mt Gox, Currency exchange, December 13 2011, https://mtgox.com/index.html?Currency=USD

[28] Benjamin Wallace, The Rise and Fall of Bitcoin, Wired Magazine, November 23 2011, http://www.wired.com/magazine/2011/11/mf_bitcoin/all/1

[29] Jason Mick, Inside the MegaHack of Bitcoin, DailyTech, June 19 2011, http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm

[30] RowIT – Bitcoin Peer to Peer Network Status, December 13 2011, http://bitcoinstatus.rowit.co.uk/

[31] Ian Grigg, Financial Cryptography in 7 Layers, 2000, http://iang.org/papers/fc7.html

[32] Adrian Chen, The Underground Website Where You Can Buy Any Drug Imaginable, Gawker, June 1 2011, http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable