MVE220 Financial Risk

Bitcoin

Daniel Forsström – 940214-3474
Ludvig Pauli – 950407-6630
Oscar Thorén – 940929-5079

Abstract

This statistical report will deal with the overall concept of Bitcoin and it therefore includes a description of how Bitcoin was created, how the technology works and how Bitcoin are used today. The report also includes discussed of what has been the main criticism of Bitcoin as well as the risks linked to the overall concept.

The conclusions to be drawn from this report is essentially that Bitcoin is about to change the financial system in the foundation and that the structure of the system is much safer than most people think. Furthermore, has Bitcoin demonstrated how adjustable and effective it can be to use the concept of blockchains and because of this it will probably in the future be several areas that we will see this concept be used.

Table of Contents

Introduction

Satoshi Nakamoto is said to be the founder of Bitcoin but it is still unknown if it is a he, she or an organisation. The software for the network was first launched by Nakamoto in January 2009. Bitcoin is the first decentralized digital network (in other words, there is no person or institution that controls it) and is in this way different from all other currencies today. There are approximately 13 million Bitcoin in the market today and it is estimated that the last Bitcoin will be created 2140. Bitcoin is created as a reward when users on the network verifies transactions that have taken place and this process is called mining. Mining is a process where the user lets the network use some of his computer power to solve a mathematical puzzle and when this is solved Bitcoin will be rewarded. One of the most revolutionary innovations bitcoin have contributed with is the concept of the blockchain. The Blockchain can be illustrated as the backbone of the Bitcoin network. It is in the blockchain that all transactions that take place are logged. Although Bitcoin seems like a safe and secure way to buy and sell goods, there are risks involved that must be considered. Bitcoin does not offer any security since there are no third party involved in the transactions. This leaves the users vulnerable against attacks to the system or your personal virtual wallet.

Aim

The purpose of this report is to give the reader a basic understanding of what Bitcoin is and how the underlying technology works and what risks are linked to Bitcoin.

Background and history

Bitcoin isn't the first attempt to develop a decentralized peer-to-peer network. Digicash was one of the first and it was released in the early 90's. The founder, David Chaum, developed the idea of an open ledger where all the transactions would be visible for all users. Digicash and Bitcoin had one important difference, digicash could only guarantee anonymity for the seller and not for the buyer which Bitcoin can. But Digicash was never implemented successfully due to several aspects but one major was because internet was in its earlier stages which held back its potential (Lovén, 2016).

In the end of the 90's it became more obvious that internet was here to stay and a new digital system for payments was launched, "Bitgold", by Nick Szabo. Nick Szabo has been suspected to be Satoshi Nakamoto since Bitgold and Bitcoin are very similar, but there is still no proof that the suspicions are correct. There was one problem with Bitgold, it couldn't assure that the money was used only one time, this where to be named the “The-double-spending-problem”. Even though this major problem it is still considered to be a precursor to Bitcoin (Lovén, 2016).

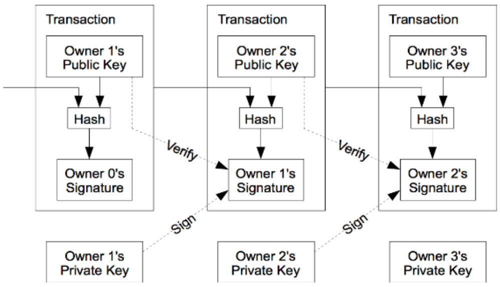
Around the same time as Bitgold was developed a new network was launched, “Hashcash”. What made hashcash revolutionary compared to Bitgold was because it had eliminated the double-spending-problem. The solution was quite simple and was about to be very important later for Bitcoin. The solution was built on hash functions, which is a function that in a very simple way solves an equation that is very complicated to figure out backwards. Hash functions is used e.g. every time someone logs into Facebook, the password changes into a combination of numbers through this function and then lets the user through to its page. It’s almost impossible to find the password from this combination of numbers. To explain it further here’s how it works: It’s very easy to find the product from 8576x9485 but to find the factors from the product 81 343 360 is very complicated (Lovén, 2016).

All these former attempts led to a sustainable system, Bitcoin. In 2008 Satoshi Nakamoto released a short white paper of only 9 pages. The paper described the basics of the idea and gave the reader a clear view of his invention. What he describes is a whole new way of sending value from one part to another completely anonymously through encryption. The reason for this is to remove the third party such as visa, mastercard, amex, banks etc. (Lovén, 2016).

Concept of bitcoin

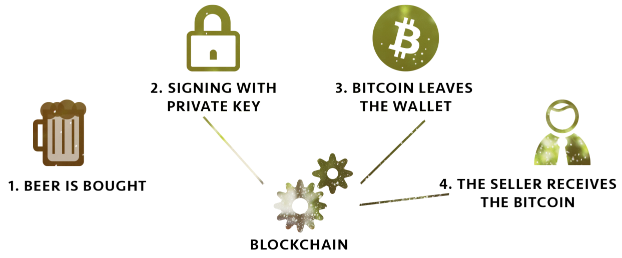
Transactions

What Satoshi Nakamoto wanted to achieve by creating Bitcoin was a new way of payments and transactions straight between the two actors, which means that he wanted to eliminate the third party. since that system is old and relies on the trust based model. As a customer, you basically must trust the third party to withdraw the exact amount as requested from your account but there is no certainty that they will. Bitcoin eliminates that problem by using digital signatures. According to Nakamoto this is what happens when a transaction takes place, “Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin”-here is how it works:

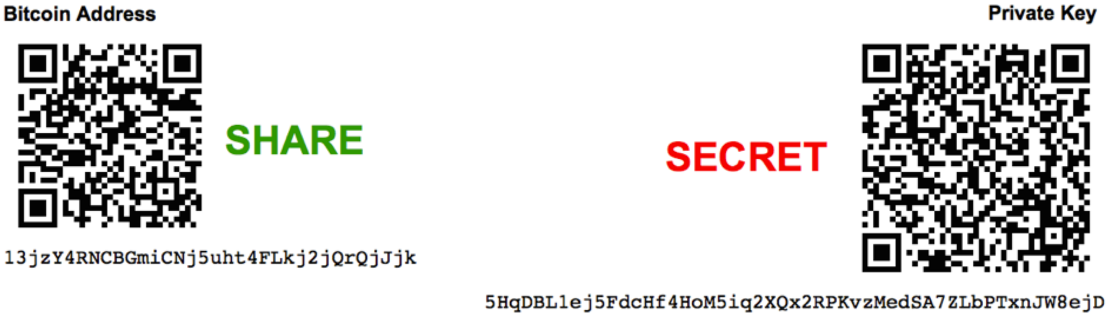


(Picture: Satoshi Nakamoto, Bitcoin: A peer-to-peer system)

In this stage bitcoin encountered a major problem that had been a significant problem for some of the previous attempts, the double spending problem. In this stage, the payee couldn’t be certain that the Bitcoin wasn’t double spent, the only way of ensuring this is by making all transactions publicly announced. By using a timestamp server, the payee gets prof of at every transaction has existed at the time end it contains all the earlier timestamps and so the earlier transactions (Nakamoto, 2008).


2. SIGNING WITH PRIVATE KEY
3. BITCOIN LEAVES THE WALLET
1. BEER IS BOUGHT
4. THE SELLER RECEIVES THE BITCOIN
BLOCKCHAIN

‘So the buyer logs on to his Bitcoin wallet with the private key and then gets the possibility to transfer the possessions. The seller provides the buyer with a QR-code which is specific for just this payment, the buyer scans the code and accept the purchase and there we have a transaction. This transaction gets put together with other transactions in a block and is then added to the blockchain. When this takes place the value transfers from part A to part B. Since it is the blockchain that verifies that the transaction is good it can be seen as the third party. The information given about the transaction is manly the value of the transaction and the time it was carried out. Something that is not given about the transaction is the information about who the seller or the buyer are, in other words the transaction is totally anonymous in the aspect of the persons involved in the transaction. This is one of the key attributes of the concept of Bitcoin and one of the mane things that differentiates Bitcoin from classical transactional systems. Another important thing that differentiates Bitcoin is that “money” can be earmarked to a specific purpose, for example when a person receives money from their health insurance these “money” (Bitcoin) could only be used to pay hospital bills, medicine and other related things for the person's illness which could make it more difficult to commit insurance fraud (Lovén, 2016).


Bitcoin Address
SHARE
13jzY4RNCBGmiCNj5uht4FLkj2jQrQjJjk
Private Key
SECRET
5HqDBL1ej5FdcHf4HoM5iq2XQx2RPKvzMedSA7ZLbPTxnJW8ejD

(Picture: Linus Lovén, Bitcoin - En finansiell Revolution, p.62)

Every combination of numbers and letters has never been written in any occasion earlier, so if you were to search on google there will be no results what so ever (Fritzson, 2015, 30 November).

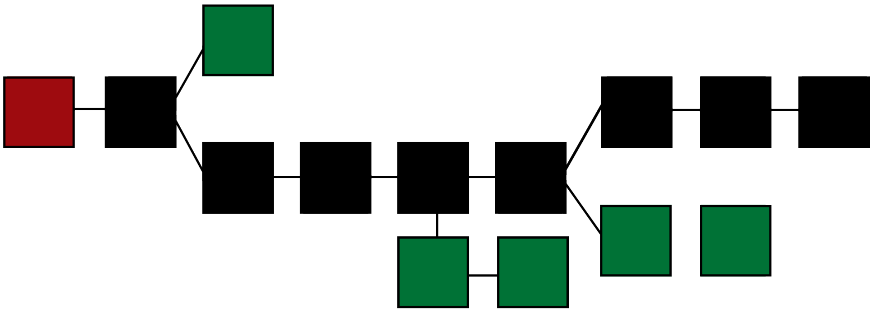
Mining

A metaphor frequently used for Bitcoin is “digital gold”, since its resources are limited just like gold. The blockchain is the engine of this structure and it is within the structure all miners verify all transactions which leads to the networks high credibility. The miners are contributing with computer power to solve the mathematical puzzle and at the same time confirming the transactions authenticity. The reward for this is new created Bitcoin. The mining process is sort of a competition about trying to find the correct hash value, the possibility of finding the right value increases when numbers of calculations increases therefore a strong computer has a greater chance of being first and gaining the block. Today there is “impossible” to mine on your own with a simple computer because of the numbers of users. There more users there are the harder it becomes to solve the puzzle. Therefore, you connect with others to try to solve it, then the odds go up but the reward goes down (Lovén, 2016).

Today there are two ways to receive Bitcoin, either you can mine or since they have become more common today you can also purchase them for other currencies. This works just like an ordinary stock purchase. If a person wants to purchase Bitcoin he/she transfers money to a depot and then places an order and then receives the Bitcoin (Lovén, 2016).

The blockchain

A blockchain is a database that contains a constantly growing list of ordered records, which are called blocks. Each block contains a link to the previous block and a timestamp. A Timestamp is a kind of watermark that provides information about what time a particular event has been registered. In the figure below, we see an illustration of how a blockchain could look like. The blockchain is secured from modification of its data by the way the blockchain is designed. The concept of the blockchain was first described by Stuart Haber and Scott Stornetta in 1991 and the concept was used for the first time with the launch of Bitcoin. (Bitcoin, 2016)



The blockchain in Bitcoin

The blockchain is the fundamental element of the Bitcoin. It is the blockchain that makes it possible for a distributed peer–to-peer digital currencies to exist. The blockchain in Bitcoin can be simply described as a secure decentralized database that contains all the Bitcoin transactions ever made (even the first transaction made by Satoshi Nakamoto himself). All computers connected to the Bitcoin network is called nodes, and all of these shares the information contained in the block chain. This allows anyone that are connected to the network to see all past transactions. The next paragraph will thoroughly explain the structure of Bitcoin blockchain. (Bitcoin, 2016)

Each block in the blockchain has a link to a previous block by a "hash". A hash is created through a hash algorithm and what the hash algorithm does is that it takes in data of an arbitrary length and converts it into fixed length, called a hash (Franco 2015). Bitcoin uses a hash algorithm called SHA-256 (Bitcoin 2016). By the fact that all blocks have a hash of the previous block it produces a chain of blocks, starting from the first block to the current block. The blocks chronological order is ensured by the block's hash, because if a hash is missing from a previous block then the next one can't be created. Furthermore, the hash of the blocks in the blockchain is almost impossible to computationally modify as it has been in the chain for a while, this is because it will have to re-create all of the next block again with the new hash. It is because of this characteristic of Bitcoin that makes double-spending so difficult to implement. (Franco, 2015)

A block contains in addition to the hash also a group of valid transactions and a nonce. The nonce is a number that makes the hash of the block to begin with a specific number of zero bits. Increasing the number of zero bits to the block makes it possible to adjust the blocks difficulty. The nonce is used to solve the partial hash inversion problem, in other words it solves Bitcoin's proof-of-work function which is explained in the next section. In the section after that, the process of how blocks are added to the blockchain will be explained. (Franco, 2015)

Proof-to-work

It is quite difficult to describe what a proof of work is, so to make it as simple as possible so you can use the following example. Suppose a person wants to join a network, for the person to get permission to do so the network requires the person to proves that some work has been done, the network may for example require that a mathematical problem is solved before the person has access to network. The proof-of-work function that Bitcoin uses is a partial hash inversion and this idea comes from hashcash. what the Partial hash inversion does, is that it requires that a block hash must match a specified pattern. The pattern to match contains the nonce, more frankly the pattern starts with a number of zeros. The greater the nonce is, the longer it takes to match the pattern of the hash. This process is called hash inversion because the proof to work is to invert a specific pattern inside the hash. The pattern-matching process is performed using computing power and the more computing power there is available, the faster it is possible to perform the matching (Franco, 2015).

The proof of work system is used by Bitcoin to generate and verify the new blocks. For the network to accept a new block, it must carry out a proof of work on all the data contained within the block. It's the node in the network that do and completes this proof-of-work. As mentioned earlier, it is through the nonce that the difficulty of the work is adjusted. The computing power in the network is constantly increasing because of the networks constant expansion. because of this, so does the difficulty automatically increases so that the network only can generate a new block every 10 minutes (Franco, 2016).

Criticism and risks

Although Bitcoin have revolutionised the way we look at money there are a lot of aspect that is necessary to take into account when dealing with Bitcoin. The consequences and downsides are rarely discussed and in some circles the Bitcoin movement works almost like a religion. When selling and buying Bitcoin it is first important to know how it all works and also which risks that is associated with these types of transactions.

Since Bitcoin do not have any underlying value like other currencies have, Bitcoin is very volatile. The price can vary a lot over a short period of time and this makes it very risky to poses. The unstable price depends on high volume buying and selling, laws and regulations stated by the government or news regarding the possibility to purchase goods with Bitcoin. In 2013 and 2014 the price of Bitcoin fell with 61 respectively 80 percent in one day which indicates how volatile the Bitcoin actually is (Investopedia, 2014).

The fact that Bitcoin is the first widely used “e-currency”, does not mean that this will be the most successful one or the one that is going to be used in ten years. The expression *First time failure* is something that is important to take into account when it comes to new technologies. It means that the first product on a new market do not automatically become the most successful one a few years later. Since the development of new technologies moves enormously fast, sceptics to Bitcoin says that new and more developed technologies will pass Bitcoin and take over the existing market. If we take a look in the past this prediction is not that crazy after all. The development of search engines is a very good example of how fast trend are moving. At first Altavista was the search engine that everyone used until 2003/2004. There were other alternatives like Yahoo but Altavista was the established one until google came and refined the whole concept. Altavista had opened the door but google came and made it the way it was supposed to work. Since Bitcoin has a few technical limitations, such as the number of transactions per second, this makes room for other similar services to release a better and more powerful block chain based “e-currency”. If that alternative is better than Bitcoin the change can happen very quickly that potentially will get the Bitcoin value to fall drastically (Lovén, 2016).

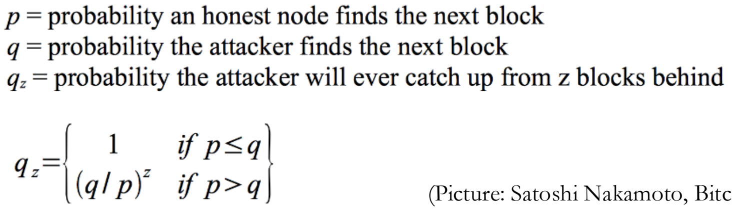
These types of competitors have already made it to the market but is still far from Bitcoin size in user base. Litecoin is one example of this which is very similar to Bitcoin blockchain concept but is a more developed version. Litecoin can both manage larger transaction volumes and a greater number of transactions at the same time (Litecoin 2016). The competitor is also estimated to produce 84 million litecoins verses Bitcoin 21 million. Some people think that the new Bitcoin competitors will create a competition on the market and others think that there are plenty of space for a variety of operators. Either way there is a risk that the now established Bitcoin will lose it's value if a competitor takes over the market. Even if the people using Bitcoin think that it works exactly how it is supposed to work banks or government may feel a threat that will cause new laws to be formed against Bitcoin. (Lovén, 2016).

Many governments are concerned over the fact that Bitcoin are used to pay for drugs and weapons anonymously, which can cause them to form regulations against it. The central bank in Russia for example stated in 2015 after a court decision that Bitcoin was illegal and all websites associated with it would be shut down. (Investopedia, 2014) The power of the governments should not be underestimated and if they find some sort of threat in using bitcoin this would probably be very hard to stand against (Lovén, 2016).

Regarding the individual security, Bitcoin does not offer any protection or insurance since there is no third party involved in the transactions. Therefore, Bitcoin which has been sent can only be sent back of the person who received them. If something goes wrong, chances of getting the money back is very small. The transaction is similar to a cash transaction which only involves two parties. Buying things through trusted organisations is therefore a simple and safe way to not get tricked. If Bitcoin get stolen the chance of getting them back is very limited. Your Bitcoin can get stolen if the wallet you store Bitcoin's in gets hacked and the hacker get access to the private key. If the private key is lost there are no chance of reaching the Bitcoin that you own. Storing your Bitcoin wallet on a computer that is not connected to the internet or making a paper wallet is two ways to keep your wallet safe. If the paper or hard drive somehow gets destroyed the money is gone.

In 2014 a major hacker attack was made against the world's largest Bitcoin exchange Mt. Gox which offered exchange service from Bitcoin to US dollars, Euros and Canadian dollars. Hackers took 460 million dollars and company later went into bankruptcy. (McMillan, 2015, 3 mars). This was not the first time that the exchange had been hacked. In 2011, 8,75 million dollars disappeared in another hack. People working at the company later said that Mt. Gox was inexperienced and hade major weaknesses in the system causing the possibility to get hacked.

Looking at the double spending problem mentioned earlier under blockchain, the possibility that a hacker can make it work is very small. Although the risk is minimal, the consequences if this would happen would be fatal for the system. The concept of this type of hack is that the attacker would create an own chain and extend it by one block at a time and race against the honest one and eventually catch up. The probability that the attackers chain would catch up is equivalent to something called a Gambler's Ruin problem. Assume that a gambler with an unlimited amount of money starts at a deficit and tries to catch up and reach breakeven, or similar, the attacker catches up with the honest chain (Nakamoto 2008).



p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{Bmatrix} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{Bmatrix}$$

(Picture: Satoshi Nakamoto, Bitcoin: A peer-to-peer system)

The attackers chance to catch up drops exponentially since the number of blocks increases. We can estimate the time it will take before the recipient can be sure that the sender can't reverse a transaction that has been sent. At the same time the transaction is sent, the attacker starts working on a chain that containing an other version of the transaction. The recipient doesn't know how much progress the attacker has made but we can assume the progress with a Poisson distribution (Nakamoto, 2008).

$$\lambda = z\frac{q}{p}$$

(Picture: Satoshi Nakamoto, Bitcoin: A peer-to-peer system)

We then multiply the Poisson density with the probability he could catch up from the starting point and receives the probability that the attacker could catch up now (Nakamoto, 2008).

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

(Picture: Satoshi Nakamoto, Bitcoin: A peer-to-peer system)

Conclusions and discussion

This new way of purchasing things and transfer value between individuals, companies or organisations have great opportunities but equally important challenges. To be able to keep your transactions anonymous and to be sure that the right amount will be transported opens up a new concept of transactions. Even though the concept of Bitcoin is fairly young it has already had an impact on the financial systems foundation.

The concept of the Bitcoin network with the blockchain as a backbone is based on that there are users who are willing to participate in the network, and as more and more people join the network it grows stronger. The way Bitcoin use the blockchain to store and verify information has proven to be very effective and very resistant to attacks. Due to this, it probably will be many more areas who will use this concept in their own networks system.

Although Bitcoin has been fairly secure in the past it doesn’t mean that hackers won’t be able to hack or attack users in the future. Hackers has manage to steal millions of dollars worth of Bitcoin and the possibility that this could happen in the future is not unlikely. Bitcoin is the first “virtual currency” with a lot of users but this doesn’t mean that it will last forever and be used as it does today. Competitors has built similar networks with more competent code, but if they will grow larger than Bitcoin is today hard to tell.

References

Lovén, L. (2016) BITCOIN: En finansiell revolution (1 uppl.). Malmö, Tryckfolket.

Franco, P. (2015) Understanding Bitcoin: cryptography, engineering and economics (1 uppl.). New york. John Wiley & Sons, Inc.

Fritzson, F (producent). (2015, 30 november). Allt du velat veta: 012 Om Bitcoin med Linus Lovén [Podcast]. Hämtad från http://podtail.com/podcast/allt-du-velat-veta/012-om-bitcoin-med-linus-loven/

Bitcoin. (2016). Blockchain. Hämtad 2017-03-27, från https://en.bitcoin.it/wiki/Block_chain

Investopedia. (2014). The Risks Of Buying Bitcoin. Hämtad 2017-03-28, från http://www.investopedia.com/articles/investing/111014/risks-buying-bitcoin.asp

Litecoin. (2016). Vad är Litcoin. Hämtad 2017-03-28, från https://litecoin.org/sv/

Nakamoto, S. (2008). Pdf – Bitcoin: A Peer-to-Peer Electronic Cash system. Hämtad 2017-03-24, från https://bitcoin.org/bitcoin.pdf

McMillan, R. (2014, 3 mars). The inside story of Mt.Gox, Bitcoin $460 million disaster. Wired. Hämtad 2017-04-03, från https://www.wired.com/2014/03/bitcoin-exchange/

Appendix

Bitcoin wallet – Is exactly what it sounds like, a wallet for your Bitcoin. There are two types of wallet, either you let it be on a server or you print it out on an ordinary paper also known as a paper wallet. If you chose to use a paper wallet then you need to store it somewhere very safe since if it's lost then the Bitcoin will be lost. The wallet contains two keys, one public and one private.

Blockchain – This is the core of the network. The blockchain is the sort of open ledger that register all transactions. These transactions are divided into blocks. The blockchain is available for everyone to review.

Hash - a hash is a fixed length of data, which has been produced by a hash function.

Hash rate – is the amount of power within the network. The ones who are mining tries to solve mathematical calculations, also known as hash functions. A hash rate of 3Th/s means that the network can do 5 trillion calculations per second.

Mining – This is what it means to let the network use some of your computer power. With all the users power combined a mathematical puzzle is solved to confirm the transactions made within the blockchain. By doing this every user gets a reward in the form of Bitcoin.

Private key – This key should always remain secret. Because it's the private key that makes transactions and movements of the Bitcoin available. If this key gets lost all the Bitcoin will be lost.

Public key – This key on the other hand can be shared with others. It's this key that makes deposits possible and it also allows you to see, only see, how much Bitcoin you have.

Volatility - is how much a trading price varies over a certain time period. High volatility indicates an unstable price with a lot of variations and vice versa.