Seminar paper

Bitcoin

BY:
Katarina Juhasova

SUPERVISOR:
Associate Prof. Dipl.-Ing.
Dr.techn. Stefan Gerhold

Vienna, December 14, 2017
## Contents

1 Introduction
   1.1 What is Bitcoin? .................................................. 3
   1.2 History of Bitcoin ............................................... 3
   1.3 Features of Bitcoin ............................................. 4
   1.4 Interesting facts ............................................... 6

2 Regulations
   2.1 Bitcoin friendly countries ..................................... 8
   2.2 Bitcoin unfriendly countries .................................. 9
   2.3 Situation in Austria ........................................... 10

3 How to get bitcoins
   3.1 Mining ............................................................. 10
   3.2 Currency exchange markets ................................... 13
   3.3 Alternative ways of getting free bitcoins .................. 14

4 Volatility of Bitcoin .............................................. 15

5 Blockchain .................................................................. 17

6 Sending and spending bitcoins
   6.1 Public key cryptography and cryptocurrency ............... 20
   6.2 Private and public keys ......................................... 20
   6.3 Private key .......................................................... 21
   6.4 Public key ............................................................ 21
   6.5 Bitcoin addresses ............................................... 21

7 Conclusion .................................................................. 22

8 Bibliography ................................................................ 23
Dictionary for this seminar paper:

*Address (aka public key)*
A bitcoin address looks like 1DSrfJdB2AnWaFNgSbv3MZC2m74996JaIv - it consists of a string of letters and numbers starting with a “1”. Just like you ask others to send an email to your email address, you would ask others to send you bitcoin to your bitcoin address. There is no limit to the number of addresses a user can create.

*Bitcoin*
The name of the currency unit (the coin), the network and the software.

*Block*
A grouping of transactions, marked with a timestamp, and a fingerprint of the previous block. The block header is hashed to find a proof-of-work, thereby validating the transactions. Valid blocks are added to the main blockchain by network consensus.

*Blockchain*
A list of validated blocks, each linking to its predecessor all the way to the genesis block.

*Fiat money*
It is a currency without intrinsic value established as money by government regulation. It has an assigned value only because the government uses its power to enforce the value of a fiat currency.

*Hash*
A digital fingerprint of some binary input.

*Secret key (aka private key)*
The secret number that unlocks bitcoins sent to the corresponding address. A secret key looks like 5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh.

*Transaction*
In simple terms, a transfer of bitcoins from one address to another. More precisely, a transaction is a signed data structure expressing a transfer of value. Transactions are transmitted over the bitcoin network, collected by miners and included into blocks, made permanent on the blockchain.

*Wallet*
Software that holds all your bitcoin addresses and secret keys. Use it to send, receive and store your bitcoin.
1 Introduction

The number of cryptocurrencies available over the internet as of 27 November 2017 is over 1324 and growing, but as a topic for my seminar paper, I have chosen bitcoin. Why? It is not only the most known one, but also the first one. There’s a lot of excitement about Bitcoin and other cryptocurrencies as well. Optimists claim that Bitcoin will fundamentally alter payments, economics and even politics around the world. Pessimists claim Bitcoin is inherently broken and will suffer an inevitable and spectacular collapse. Whether we like it or not, its adoption and attention prove that a lot of people believe in the possibilities of Bitcoin becoming a worldwide currency, or at least, a widely used medium of exchange.

1.1 What is Bitcoin?

Bitcoin is an internet based cryptocurrency, a digital asset that only exists as data. We all have money in the bank that is digital, but those digits are equal to physical currency. It does not work like this with Bitcoin. The value of Bitcoin is dictated entirely by the market. Users can transfer bitcoin over the network and do just about anything with it that can be also done with conventional currencies, such as buy and sell goods, send money to people or organizations, or extend credit. Bitcoin technology includes features that are based on encryption and digital signatures to ensure the security of the bitcoin network. Bitcoin in a sense is the perfect form of money for the Internet because it is fast, secure, and borderless.

Unlike traditional currencies, bitcoins are entirely virtual. There are no physical coins or even digital coins per se. The coins are implied in transactions which transfer value from sender to recipient. Users of bitcoin own keys which allow them to prove ownership of transactions in the bitcoin network, unlocking the value to spend it and transfer it to a new recipient. Those keys are often stored in a digital wallet on each user’s computer. Possession of the key that unlocks a transaction is the only prerequisite to spending bitcoins, putting the control entirely in the hands of each user.

1.2 History of Bitcoin

It was founded by an anonymous programmer using a pseudonym Satoshi Nakamoto and his identity is till now still unknown. But we know that Satoshi started coding Bitcoin around May 2007. He registered the domain bitcoin.org in August 2008. At that time, he started sending private emails to a few people who he thought might be interested in the proposal. Then a little later in October 2008, he publicly released a white paper that described the protocol, and soon after, he released the initial code for Bitcoin as well. Then he stuck around for about two years, during which he posted lots of messages on forums, emailed with lots of people, and responded to people’s concerns. On the programming side, he submitted patches to the code. He maintained the source code in conjunction with other developers, fixing issues as they arose. By December 2010, others had slowly taken over the maintenance of the project, and he stopped communicating with them. But why exactly in 2010? It is not that hard to explain. On 18.5.2010 posted
Laszlo Hanyecz on bitcoin talk a proposal to trade 10 000 Bitcoins for couple of pizzas and then on 22.5 he wrote that he had successfully traded 10 000 Bitcoins for 2 pizzas. The value of 1 Bitcoin on this day was exactly 0,003 $. Now is 22.5 also marked as Bitcoin Pizza Day. This was the first transaction ever using Bitcoin as cash in history and exactly one year later, in May 2011, went Bitcoin viral.

1.3 Features of Bitcoin

- Decentralization

Bitcoin has no central control: no central repository of information, no central management, and, crucially, no central point of failure. And yet, most of the actual services and businesses built within the Bitcoin ecosystem are centralized. They are run by specific people, in specific locations, with specific computer systems, and they are susceptible to specific legal entanglements. This situation creates tension and certainly a little irony— we have a decentralized technology, yet most things existing upon it are centralized. So isn’t Bitcoin’s claim of decentralization a lie? No. And here is the reason why: to understand Bitcoin one must understand the difference between coercive centralization and market-based centralization. Bitcoin possesses the latter, but avoids the former, and that is a crucial distinction. Coercive centralization is what we all experience in the legacy financial industry. The world’s monetary system, based upon national fiat currencies created and managed by government-sponsored central banks, is coercive. It is coercive because the entities with the power over money’s creation, regulation, and transfer have the will and the power to hurt you if you disobey. Not only that, but you are coerced into it in the first place, being forced to pay taxes and settle debts using only your government’s anointed currency. The entire financial system as it exists today rests upon this anti-market model of coercion— money moves only with the permission of those in control, and they’re not in control by mutual contract, but by the privilege of violence. But this is not the case with bitcoin. Nobody can force you to give away your bitcoins or take them without your permission. Market-based centralization is fundamentally different. Its key feature is the ability to opt out. A user of conventional currencies is always forced to utilize a centralized service. A user of Bitcoin is never forced to utilize a centralized service. This is the key distinction between centralization found in Bitcoin (which is market-based) and centralization found in the traditional banking industry (which is coercive). The key to judging the legitimacy of centralization is always the ability of users
to opt out. Bitcoin provides this, while fiat and central banks do not.

- Payments are irreversible

- Bitcoin is divisible

Small amounts of bitcoin used as alternative units are millibitcoin and satoshi. Named in homage to Bitcoin’s creator, a satoshi is the smallest amount within Bitcoin representing 0.00000001 bitcoin, one hundred millionth of a bitcoin. A millibitcoin equals to 0.001 bitcoin, one thousandth of a bitcoin or 100,000 satoshis.

- Quick and free

Whereas opening a bank account is a long procedure and most of them are not free of charge. But creating of bitcoin address doesn’t take more than few minutes and it is totally free.

- Pseudonymous

Bitcoin is often described as an anonymous currency because it is possible to send and receive bitcoins without giving away any personally identifying information. However, everyone sees your transaction and everyone can also see how many bitcoins you own but they only sees your bitcoin address. So if your address is ever linked to your identity, every transaction will be linked to you. One way to increase anonymity is to use multiple wallets. This is like maintaining multiple separate identities.

- Total number of bitcoins is limited

Bitcoin is like gold in many ways. Like gold, Bitcoin can not simply be created arbitrarily. Gold must be mined out of the ground, and Bitcoin must be mined via digital means. And also like gold, it has a limited and finite supply. In fact, there are only 21 Million bitcoins that can be mined in total and 80% of all have already been mined. It is calculable that the last one will be mined in 2140. There are also stockpiles of inactive coins that are held around the world, the largest supply of which belongs to the person or group of people who founded Bitcoin, Satoshi Nakamoto. Perhaps this supply, consisting of roughly 1 Million bitcoins, is intentionally being saved for a time when the global supply is facing increased levels of demand.
- If you lose your private keys to your bitcoin wallet, you lose everything

- Probably 60% of all bitcoins are unused

1.4 Interesting facts

There have been more than 275 Million transactions made since its formation and the first one was on 12.1.2009 when Satoshi Nakamoto sent 10 bitcoins to someone. The largest transaction processed so far by the network was 150 Million $.

The number of places where it is possible to pay with Bitcoin is increasing from one day to another but on 5.12.2017 it was possible to pay with Bitcoin in 10 903 places in the whole world. It is even possible to pay tuition fees at some universities with Bitcoin (e.g. NY King College, University of Cumbrie (UK)... and University of Nicosia (Cyprus) is the first university that offers Master of Science degree in Digital Currency. The map below shows the distribution of all places in the world where it is possible to pay with bitcoins. The red colour represents the highest, the green one the lowest distribution of places and yellow represents something in between.
First ever Bitcoin Documentary was released in September 2017 (Bitcoin: Shape the Future).

70% of transactions are made by speculators

Surprising places where it is possible to pay with Bitcoin:
- Microsoft users can use Bitcoin to purchase games, movies and apps in the Windows and Xbox stores, as well as the Microsoft online stores.
- Subway franchises in Buenos Aires recently accept Bitcoin for payments at the restaurants for their “Eat Fresh” products.
- eGifter is a popular gift card mobile app, which allows users to buy gift cards for different places, such as Amazon, Sephora, Home Depot and Kohls. Bitcoins are accepted for purchasing gift cards for places that do not directly accept Bitcoins.
- Since 2013, Virgin Galactic, a commercial space flight venture owned by Entrepreneur Sir Richard Branson, that includes companies such as Virgin Mobile and Virgin Airline, accepts purchases using Bitcoin. You can even pay for space travel with Bitcoin.

The total number of accounts on the platform is now around 13.1 million. Here we can clearly see the distribution of Bitcoin.

![Figure 4: Bitcoin rich list](image)

### 2 Regulations

Bitcoin has been around for almost 10 years, yet only few countries have their own regulations on Bitcoin and cryptocurrency in general. Some countries welcomed Bitcoin to the finance world and looked at it as a cost effective way of making financial services modern. The others, however, do not consider it as an official way of payment and are not interested in implementing blockchain technology into their ecosystem. But why? I would say that the main reason is that transactions are not traceable, so if criminals use it to launder money, then it would be very hard for monitoring department of police to locate who is trading these bitcoins and where these bitcoins are going.
2.1 Bitcoin friendly countries

- Japan

This Asian country is known worldwide as one of the friendliest countries in the world towards Bitcoin and cryptocurrencies in general. Japan is one of the biggest trading hubs on earth concentrating lot of the cryptocurrency trading volume. Earlier this year in April, Japan passed a long discussed law that recognizes Bitcoin and other cryptocurrencies as means of payment that is legal. Japan’s Financial Services Agency has approved 11 companies as operators of cryptocurrency exchanges. It does not mean that there are no regulations regarding the cryptocurrency market. Enterprises, financial institutions and exchange platforms must follow a strict anti-money laundering requirements. In addition to this, they also must have a strict knowledge of the customers they are working with. The country distinguishes itself from its neighbours, China and South Korea, where Bitcoin exchanges were banned by the government. This situation allows Japan to bring into its country investments in cryptocurrencies that the other countries would not able to attract.

- England

In the United Kingdom, enterprises and financial institutions are regulated by the Financial Conduct Authority (FCA). But this regulatory arm does not regulate Bitcoin and cryptocurrency exchanges and businesses. As the FCA explained, Bitcoin businesses in the UK are not obliged to register with the FCA to operate freely and under the rule of law. But what is interesting is that British enterprises related to Bitcoin and cryptocurrencies regulate themselves in order to follow the FCA regulations, even when it is not required.

- Denmark

The National Bank of Denmark released a statement in which they explain that Cryptocurrencies are not regulated neither at the European level nor in Denmark. Even when the use of cryptocurrencies is not spread everywhere, they can be used freely, without paying taxes, because for the Danish Central Bank, Bitcoin is not a currency. Besides, the Financial Supervisory Authority claims that it will not prevent anybody who would like to start or open a cryptocurrency business in the country.

- Netherlands

Holland is known for having a Bitcoin Embassy in Amsterdam. They call themselves a Bitcoin Community that wants to spread knowledge related to Bitcoin and the entire cryptocurrency ecosystem. At this place people can sit at the Bitcoin coffee or reserve a table to eat at the Bitcoin Restaurant. At the end of the day, everyone can pay with Bitcoin without any problem. In the same place, you can also ask for good quality information about Bitcoin and cryptocurrencies in case you would like to know more. If the Bitcoin Embassy is not enough, then the Bitcoin City, Arnhem, would be worth mentioning. Located near the German borders, it is a city that opened itself to Bitcoin.
Lots of shops, businesses and people use Bitcoin on a daily basis. In the other countries mentioned before, Bitcoin is free and legal, but not so widely spread as it is in Arnhem. The city created a Bitcoin economy, alternative to the current financial system, in which some merchants use bitcoins to buy supplies for their own businesses. The goal of this city is to spread Bitcoin until it will be part of the daily life of its citizens and visitors. In the country, Bitcoin and cryptocurrency trade is not regulated by financial authorities.

- Australia

Across the whole country is trading, mining and buying Bitcoin allowed. Australian authorities perceive Bitcoin as non-harmful mean of transaction.

### 2.2 Bitcoin unfriendly countries

- Nigeria

The Central Bank of Nigeria (CBN) on 17.1.2017 passed a circular to inform all Nigerian banks that all transaction in Bitcoin and other virtual currencies had been banned in Nigeria.

- Taiwan

The Chairman of the Financial Supervisory Commission (FSC) has declared Bitcoin to be illegal in Taiwan. The announcement came after high-profile incident in 2015, in which prominent Hong Kong business tycoon was kidnapped by a criminal gang who demanded over 10 Million $ to be paid in Bitcoin. (The victim was rescued soon after a payment of 1.6 Million $.)

- Bolivia

Back in June 2014, the Bolivian central bank officially banned any currency or coins that are not regulated by the government. Included in its list of examples was Bitcoin. Bolivia’s central bank also prohibited its citizens from denominating prices in any currency other than its national institutions have not previously approved.

- Marocco

The newest ban, coming as of November 2017, was in Morocco, which ironically came just days after domestic digital services provider MTDS announced that it would accept Bitcoin as payment for the first time. Like the other countries before, Morocco’s central bank cited "a hidden payment system that is not backed by any financial institution" as its reasoning for banning bitcoin and other digital currencies.
2.3 Situation in Austria

In the view of the Austrian Federal Ministry of Finance (BMF), cryptocurrencies are an intangible, non-depreciating economic asset that, however, is not classified as a payment method under income tax law. I would call Austria a bitcoin friendly country. It is possible to order food at www.lieferservice.at and pay with bitcoins. At www.myproduct.at it is also possible to pay with cryptocurrencies and since October you even can buy clothes in Shopping City Süd and pay with bitcoins.

More than half of Austrians are familiar with cryptocurrencies such as Bitcoin or Ethereum. 12 % think that they know it quite well. But only 6 % have already used Bitcoin. This is the result of a recent survey by MarketAgent on behalf of the trade association. The market researcher surveyed in July and August 2017 500 people who are regularly active online. In Vienna there is even a retail store for Bitcoin. The House of Nakamoto was opened at the beginning of 2017 on Mariahilferstraße. Not only it is possible to buy and sell bitcoins there, but employees will help you and explain you everything you need to know about Bitcoin.

3 How to get bitcoins

To make my writing and your reading a little bit easier I will use the letter B for representation of currency unit „bitcoin“ (100 Million satoshis).

3.1 Mining

Only by mining new bitcoins are generated. Bitcoins are mined in units called "blocks". When Bitcoin was first mined in 2009, mining one block would earn you 50 B. In 2012, this was halved to 25 B and in 2016, this was halved to the current level of 12.5 B. In 2020 (in June), the reward size will be halved again to 6.25 B. At the time of writing, 497 574 blocks have already been mined. Miners are getting paid for their work as auditors. They are verifying previous Bitcoin transactions. This convention is meant to keep Bitcoin users honest, and was conceived by Satoshi Nakamoto. By verifying transactions, miners are helping to prevent the "double-spending problem". Double spending means, as the name suggests, that a Bitcoin user is illicitly spending the same money twice. Let’s say you had one legit 20 $ bill and one really good photocopy of that same 20 $ bill. If someone were to try to spend both, the real bill and the fake one, someone who took the trouble of looking at both of the bills’ serial numbers would see that they were the same number, and thus one of them had to be fake. What Bitcoin miners do is analogous to that- they check transactions to make sure that users have not illegitimately tried to spend the same Bitcoin twice. As soon as miners verify 1 MB (megabyte) worth of Bitcoin transactions, they are eligible to win the 12.5 B. The 1 MB limit was set by Satoshi Nakamoto. 1 MB of transactions can theoretically be as small as 1 transaction (though this is not at all common) or several thousand. It depends on how much data the transactions take up. But this is only the first part (the easy one) that only makes you eligible to earn bitcoins- not everyone who verifies transactions will get paid out. The second part is that you have to be the first miner to arrive at the right answer to a
numeric problem. This process is also known as a proof of work.

**The good news:** No advanced math or computation is involved. You may have heard that miners are solving difficult mathematical problems—that’s not true at all. What they are actually doing is trying to be the first miner to come up with a 64-digit hexadecimal number (a "hash") that is less than or equal to the target hash. It’s basically a guess work.

**The bad news:** Because it is guesswork, you need a lot of computing power in order to get there first. To mine successfully, you need to have a high "hash rate," which is measured in terms of megahashes per second (MH/s), gigahashes per second (GH/s), and terahashes per second (TH/s). For that you not only need a computer but also some special equipment (Either a graphics processing unit (GPU) miner or an application-specific integrated circuit (ASIC) miner. These can cost from 500 $ to the tens of thousands.)

In Bitcoin terms, simultaneous answers occur frequently, but at the end of the day there can only be one winning answer. When multiple simultaneous answers are presented that are equal to or less than the target number, the Bitcoin network will decide by a simple majority (51 %) which miner to honour. Typically, it is the miner who has done more work (the one that who has verified more transactions.

What exactly is this 64-digit hexadecimal number? For example here is one:

```
0000000000000000057fcc708cf0130d95e27c5819203e9f967ac56e4df598ee
```

The number above has 64 digits. That is easy enough to understand. It consists not just of numbers, but also letters of the alphabet. In order to understand what these letters are doing in the middle of numbers, we must understand the word "hexadecimal". Hexadecimal means base 16, as "hex" is derived from the Greek word for 6 and "deca" is derived from the Greek word for 10. In a hexadecimal system, each digit has 16 possibilities. But our numeric system only offers 10 ways of representing numbers (0-9). That’s why we have to put letters in, specifically letters a, b, c, d, e, and f. But this is just for background. If you are mining Bitcoin, you do not need to calculate the total value of that 64-digit number (the hash). What miners are doing with those huge computers is guessing at the target hash. Miners make these guesses by randomly generating as many "nonces" as possible, as fast as possible. A nonce is short for "number only used once," and the nonce is the key to generating these 64-bit hexadecimal numbers. In Bitcoin mining, a nonce is 32 bits in size- much smaller than the hash, which is 256 bits. The first miner whose nonce generates a hash that is less than or equal to the target hash is awarded credit for completing that block, those 12.5 B that I mentioned before and then publishes that block into the blockchain (next chapter).

All target hashes begin with zeros- at least eight zeros, and up to 63 zeros. There is no minimum target, but there is a maximum target set by the Bitcoin Protocol. No target can be greater than this number:
Here are some examples of randomized hashes and the criteria for whether they will lead to success for the miner:

![Figure 5: Example of hashes](image)

What do need to do to maximize chances to guess the target hash before anyone else does? You would have to get a fast mining rig (extremely expensive and long waiting time till you actually can buy it) or, more realistically, join a mining pool- a group of miners who combine their computing power and split the mined bitcoin.

Any participant in the bitcoin network (i.e., any device running the full bitcoin protocol stack) may operate as a miner, using their computer’s processing power to attempt to find solutions to this problem. China is the number 1 miner and holds about 30 % of global hash rate- why? Average electricity price in $ cents/ kWh is only 8 (Germany- 35, Denmark- 41, UK- 20) and that could be the main reason.

Is Bitcoin mining profitable in 2017? Each person asking himself this will get a slightly different answer since Bitcoin mining profitability depends on many different factors. In order to figure out the correct profitability for everyone something like “mining profitability calculators” were invented. These calculators take into account different parameters and give you an estimate of your projected profit. Before answering this question it is important to know what kind of parameters you are going to need.

**Bitcoin Difficulty**- Since the Bitcoin network is designed to produce a constant amount of Bitcoins every 10 minutes, the difficulty of solving the mathematical problems has to increase in order to adjust to the network’s Hash Rate increase. Basically this means that the more miners that join, the harder it gets to actually mine Bitcoins.

**Electricity Rate**- Operating a Bitcoin miner consumes a lot of electricity. You will need to find out your electricity rate in order to calculate profitability.
Power consumption- Each miner consumes a different amount of energy. Make sure to find out the exact power consumption of your miner before calculating profitability.

Pool fees- In order to mine you’ll need to join a mining pool. As I mentioned before, mining pool is a group of miners that join together in order to mine more effectively (because today it is really impossible to mine on your own). The platform that brings them together is called a mining pool and it deducts some sort of a fee in order to maintain its operations. Once the pool manages to mine Bitcoins, the profits are divided between the pool members depending on how much work each miner has done.

Profitability decline per year- This is probably the most important and elusive variable of them all. The idea is that since no one can actually predict the rate of miners joining the network no one can also predict how difficult it will be to mine in 6 weeks, 6 months or 6 years from now. This is one of the two reasons no one will ever be able to answer the question for once and for all weather Bitcoin mining is profitable or not.

Conversion rate- Since no one knows what the BTC/USD exchange rate will be in the future it’s hard to predict if Bitcoin mining will be profitable. If you’re into mining in order to accumulate Bitcoins only then this doesn’t need to bother you. But if you are planning to convert these Bitcoins in the future to any other currency this factor will have a major impact of course.

Transaction fees (tx fees)- Transaction fees are voluntary on the part of the person making the bitcoin transaction, as the person attempting to make a transaction can include any fee or none at all in the transaction. This means, that sometimes you can get a few extra bitcoins only from tx fees and sometimes you can get nothing at all.

![Figure 6: Mining profitability](image)

3.2 Currency exchange markets

You certainly don’t have to be a miner to own bitcoins, but you also can buy them. By currency exchange I mean trading bitcoins against fiat currency like dollars or euros. The first thing to understand is that it operates in many ways like the market between two fiat currencies. The price will fluctuate back and forth depending on how badly people want to buy euros versus how badly people want to buy dollars on a particular day. In
the Bitcoin world there are sites like www.bitcoincharts.com that show the exchange rate with various fiat currencies on a number of different exchanges. As you will see if you explore the site, there is a lot of trading going on, and the prices move in real time as trades are made. It is a liquid market and there are plenty of places that you can go to to buy or sell bitcoins.

Another option is to meet people to trade bitcoins in real life. There are sites that help you do this. On www.localbitcoins.com, for example, you can specify your location and that you wish to buy bitcoins with cash. You will get a bunch of results of people who at the time of your search are willing to sell bitcoins at your location, and in each case it tells you what price and how many bitcoins they are offering. You can then contact any of them and arrange to meet, give them your fiat currency and receive bitcoins in exchange.

Finally, in some places there are regular meet-ups where people go to trade bitcoins. There are 28 places in Vienna where you can go almost anytime to trade bitcoins (fiat -> crypto but also crypto -> fiat).

3.3 Alternative ways of getting free bitcoins

Getting free bitcoins is not a way to get rich, and certainly not the most profitable use of one’s time, but rather if you have some free time and would like to pick up a small amount of extra Bitcoin now and then.

- The Blockchain Game
  The game pays out once per week. It is important to note that like most free games, the Blockchain Game has a lot of advertisements. This is how they are able to afford to pay others. Playing the Blockchain game is fun, challenging, and mildly addictive. The frequent interruptions by advertising are, of course, less than ideal, but a necessary evil. Gameplay involves getting to the top level, which has the highest reward. Getting to only the first level is easy, but each level after that, requires that you place the block directly above the previous level. This can be difficult because the block moves on its own and it moves faster with each level. Every ten levels, you get the option to cash out or go further. Here’s what gameplay looks like:
If you fail to place a block, you get the option to continue for watching a short ad. And of course, this is just one example of game. There exist „few“ more.

- Reading books
   It is one of the more interesting and engaging methods of receiving free money, as it gives the user the opportunity to engage in more ways than simply using free time by pressing a couple of buttons.

4 Volatility of Bitcoin

In the last ten days of August this year, the dollar price of Bitcoin shot up nearly 25 %. Anyone who bought a Bitcoin on August 21st would have paid 4055 $. If they had sold it on September 1st, they would have pocketed a nice 896 $ in profit. Within two weeks, the price had fallen to 3226 $. The poor buyer who picked up that Bitcoin at the start of the month and sold it in mid-September would have lost some 1725 $.

With that kind of movement, putting your money into Bitcoin can feel really scary.

Bitcoin’s volatility has all sorts of causes. As I mentioned before, the release of new bitcoins is strictly limited. No matter how quickly demand grows, production remains the same so as long as more people want to buy Bitcoin, the price will continue to rise. It is also highly vulnerable to news. A hacked exchange, a new government regulation or even a devaluation in China can have the price of Bitcoin increasing and decreasing very fast. Also when we look to the past- in 2016 Bitcoin started to recover. Why? There were a lot of changes in situation in many countries. It may sound like that has nothing to do with Bitcoin, but what we can not deny is once people are losing their confidence on their governments and their legal currency, then can Bitcoin be seen as a better way of avoiding risks.
There is an easy way to protect yourself against Bitcoin volatility, though. You can just hold onto it. Bitcoin is volatile in the short-term. Swings, whether upward or downward, are difficult to predict, but the overall direction is generally upward at least when we look at year 2017. The dollar price of Bitcoin might have dived in the first two weeks of September but the price in the third week of October was nudging $6000. Someone who bought a Bitcoin at the end of August and held onto it through the drop would have found themselves sitting on a profit of around $1000, a nice 20% increase, in under two months. And someone who waited till beginning of December, would have made profit of about $7000. Here is also comparison of Bitcoin’s volatility from previous years.

Figure 8: Volatility 2017

Figure 9: Volatility 2015-2016
5 Blockchain

Historically, when it comes to transacting money or anything of value, people and businesses have relied heavily on intermediaries like banks and governments to ensure trust and certainty. Middlemen perform a range of important tasks that help build trust into the transactional process like authentication and record keeping. The need for intermediaries is especially acute when making a digital transaction. Because digital assets like money, stocks and intellectual property, are essentially files that are incredibly easy to reproduce. This creates what’s known as the double spending problem that I mentioned before.

Blockchain is a type of distributed ledger or decentralized database that keeps continuously updated digital records of who owns what. Rather than having a central administrator like a traditional database (think banks, governments and accountants), a distributed ledger has a network of replicated databases, synchronized via the internet and visible to anyone within the network. Blockchain networks can be private with restricted membership similar to an intranet, or public, like the Internet, accessible to any person in the world. When a digital transaction is carried out, it is grouped together in a cryptographically protected block with other transactions that have occurred in the last 10 minutes and sent out to the entire network—> Mining. The validated block of transactions is then timestamped and added to a chain in a linear, chronological order. New blocks of validated transactions are linked to older blocks, making a chain of blocks that show every transaction made in the history of that blockchain. The entire chain is continually updated so that every ledger in the network is the same, giving each member the ability to prove who owns what at any given time.
Blockchain’s decentralized, open and cryptographic nature allows people to trust each other and transact peer to peer, making the need for intermediaries obsolete. This also brings unprecedented security benefits. If someone wanted to hack into a particular block in a blockchain, a hacker would not only need to hack into that specific block, but all of the previous blocks going back the entire history of that blockchain. And they would need to do it on every ledger in the network, which could be millions, and they would need to do it simultaneously (and that is kind of impossible).

Although blockchain is commonly associated with Bitcoin, it also has many other applications. Bitcoin is merely the first and most well-known use. In fact, Bitcoin is only one of about seven hundred applications that use the blockchain operating system today. Blockchain has applications that go way beyond obvious things like digital currencies and money transfers. From electronic voting, smart contracts and digitally recorded property assets to patient health records management and proof of ownership for digital content.

And what is its possible future? Blockchain could profoundly disrupt hundreds of industries that rely on intermediaries, including banking, finance, academia, real estate, insurance, legal, health care and the public sector- amongst many others. This would result in job losses and the complete transformation of entire industries. But overall, the elimination of intermediaries would bring mostly positive benefits. Banks and governments for example, often impede the free flow of business because of the time it takes to process transactions and regulatory requirements. The blockchain would enable an increased amount of people and businesses to trade much more frequently and efficiently, significantly boosting local and international trade. Blockchain technology would also eliminate expensive intermediary fees that have become a burden on individuals and businesses, especially in the remittances space.

Perhaps most profoundly, blockchain promises to democratize and expand the global financial system. Giving people who have limited exposure to the global economy, better access to financial and payment systems and stronger protection against corruption and exploitation.
6 Sending and spending bitcoins

Ownership of Bitcoin is established through digital keys, bitcoin addresses and digital signatures. The digital keys are not actually stored in the network, but are instead created and stored by end-users in a file, or simple database, called a wallet. The digital keys in a user’s wallet are completely independent of the Bitcoin protocol and can be generated and managed by the user’s wallet software without reference to the blockchain or access to the Internet. Keys enable many of the interesting properties of Bitcoin, including decentralized trust and control, ownership attestation and the cryptographic-proof security model.

Every bitcoin transaction requires a valid signature to be included in the blockchain, which can only be generated with valid digital keys, therefore anyone with a copy of those keys has control of the Bitcoin in that account. Keys come in pairs consisting of a private and public key. Think of the public key as similar to a bank account number and the private key as similar to the secret PIN number, or signature on a cheque that provides control over the account. These digital keys are very rarely seen by the users of bitcoin. For the most part, they are stored inside the wallet file and managed by the bitcoin wallet software.

In the payment portion of a bitcoin transaction, the recipient’s public key is represented by its digital fingerprint, called a bitcoin address, which is used in the same way as the beneficiary name on a cheque (i.e. “Pay to the order of ”). In most cases, a bitcoin address is generated from and corresponds to a public key. Bitcoin addresses abstract the recipient of funds, making transaction destinations flexible, similar to paper cheques: a single payment instrument that can be used to pay into people’s accounts, company accounts, pay for bills or pay to cash. The bitcoin address is the only representation of the keys that users will routinely see, as this is the part they need to share with the world.

![What about sending and receiving bitcoin?](image)

Figure 12: Public and private keys
6.1 Public key cryptography and cryptocurrency

Public key cryptography was invented in the 1970s and is a mathematical foundation for computer and information security.

Since the invention of public key cryptography, several suitable mathematical functions, such as prime number exponentiation and elliptic curve multiplication, have been discovered. These mathematical functions are practically irreversible, meaning that they are easy to calculate in one direction and infeasible to calculate in the opposite direction. Based on these mathematical functions, cryptography enables the creation of digital secrets and unforgeable digital signatures. Bitcoin uses elliptic curve multiplication as the basis for its public key cryptography.

In bitcoin, we use public key cryptography to create a key pair that controls access to bitcoins. The key pair consists of a private key and — derived from it — a unique public key. The public key is used to receive bitcoins, and the private key is used to sign transactions to spend those bitcoins.

There is a mathematical relationship between the public and the private key that allows the private key to be used to generate signatures on messages. This signature can be validated against the public key without revealing the private key.

When spending bitcoins, the current bitcoin owner presents their public key and a signature (different each time, but created from the same private key) in a transaction to spend those bitcoins. Through the presentation of the public key and signature everyone in the bitcoin network can verify and accept the transaction as valid, confirming that the person transferring the bitcoins owned them at the time of the transfer.

6.2 Private and public keys

The private key (k) is a number, usually picked at random. From the private key, we use elliptic curve multiplication, a one-way cryptographic function, to generate a public key (K). From the public key (K), we use a one-way cryptographic hash function to generate a bitcoin address (A).

![Relationship between keys](image)

Figure 13: Relationship between keys
6.3 Private key

A private key is simply a number, picked at random. Ownership and control over the private key is the root of user control over all funds associated with the corresponding bitcoin address. The private key is used to create signatures that are required to spend bitcoins by proving ownership of funds used in a transaction. The private key must remain secret at all times, as revealing it to a third party is equivalent to giving them control over the bitcoins secured by that key. The private key must also be backed up and protected from accidental loss, since if lost it cannot be recovered and the funds secured by it are forever lost too.

Generating a private key from a random number:

The first and most important step in generating keys is to find a secure source of entropy (randomness). Creating a bitcoin key is essentially the same as “Pick a number between 1 and 2256”. The exact method you use to pick that number does not matter as long as it is not predictable or repeatable. Bitcoin software uses the underlying operating system’s random number generators to produce 256 bits of entropy. Usually, the OS random number generator is initialized by a human source of randomness, which is why you may be asked to wiggle your mouse around for a few seconds. But if you are paranoid, you also can generate it by yourself using pencil and paper.

6.4 Public key

The public key is calculated from the private key using elliptic curve multiplication, which is irreversible: \( K = k \times G \) where \( k \) is the private key, \( G \) is a constant point called the Generator Point and \( K \) is the resulting public key. The reverse operation, known as “finding the discrete logarithm” — calculating \( k \) if you know \( K \) — is as difficult as trying all possible values of \( k \). The relationship between \( k \) and \( K \) is fixed. Its irreversibility is the reason why bitcoin address (derived from \( K \)) can be shared with anyone and does not reveal the user’s private key (\( k \)).

6.5 Bitcoin addresses

A bitcoin address is a string of digits and characters that can be shared with anyone who wants to send you money. Addresses produced from public keys consist of a string of numbers and letters, beginning with the digit “1”. Here’s an example of a bitcoin address:

1thMirt546mngXqvPEz532S8fLwbozud8

The bitcoin address is what appears most commonly in a transaction as the “recipient” of the funds. If we were to compare a bitcoin transaction to a paper cheque, the bitcoin address is the beneficiary, which is what we write on the line after “Pay to the order of”. On a paper cheque, that beneficiary can sometimes be the name of a bank account holder, but can also include corporations, institutions or even cash. Because paper cheques do not need to specify an account, but rather use an abstract name as the recipient of funds,
that makes paper cheques very flexible as payment instruments. Bitcoin transactions use a similar abstraction, the bitcoin address, to make them very flexible. A bitcoin address can represent the owner of a private/public key pair.

The bitcoin address is derived from the public key through the use of one-way cryptographic hashing; a “hashing algorithm” or simply “hash algorithm” is a one-way function that produces a fingerprint or “hash” of an arbitrary sized input. Cryptographic hash functions are used extensively in bitcoin: in bitcoin addresses, in script addresses and in the mining “Proof-of-Work” algorithm. The algorithms used to make a bitcoin address from a public key are the Secure Hash Algorithm (SHA) and the RACE Integrity Primitives Evaluation Message Digest (RIPEMD), specifically SHA256 and RIPEMD160.

7 Conclusion

I am neither strictly for nor against digital currencies, just like I am not for or against any individual stocks. There are times that they are appealing and times that they are not appealing. Normally I do not regret things that I have done or haven’t done in the past, but not investing in Bitcoin could be the one thing that I do regret not doing. But as we all know, we can not change the past. I am glad that I chose this topic for my seminar paper, because I know that I learnt a lot and I will also continue searching for more information after finishing this paper.

I mentioned Bitcoin Documentary (Bitcoin: Shape the future) before and when you are interested in this topic then I would definitely recommend watching it.
8 Bibliography


https://www.buybitcoinworldwide.com/anonymity/ (27.11.2017 18:27)
