MATH5248 – Cryptology and Number Theory
Fall 2017 – Group Project about Cryptocurrency/Bitcoin

Lars Henry B. Olsen, Peter Irvine and Patrick Dee

December 6, 2017

Abstract

The transaction system we use today has a centralized structure where currency gets transferred through a financial institution. When you pay an invoice online or transfer money to a friend, you actually pay the bank and rely on the bank's servers to redirect the money to the intended receiver. This means that the financial institutions have a lot of responsibility, which they might exploit. In 2008 Satoshi Nakamoto wrote *Bitcoin: A Peer-to-Peer Electronic Cash System* [14] where he introduced a pure peer-to-peer transaction protocol. This system allows payments to be directly transferred from the transmitter to the receiver without going through a centralized financial institution.

Introduction

Bitcoin is a digital currency that was invented in 2009 by an anonymous person, or group, that goes by the name of Satoshi Nakamoto. The interesting part of Bitcoin is that transactions can be recorded without the use of financial institutions, such as banks and credit unions. For the most part, Bitcoin can be used just like any other form of currency. You can use it to buy anything ranging from pizza to illegal weapons and drugs on the blackmarket. Bitcoin is one of the preferred currencies for completing illegal transactions, because merchandise and services can be purchased without displaying, or revealing your true identity, if desired. So other than complete anonymity, what makes Bitcoin so attractive compared to other forms of currency? Well, for one, international payments are made a lot cheaper and easier, since Bitcoin isn't tied to any one country and therefore not subject to regulation. There are also no credit card fees when using Bitcoin.

One of the primary reasons for the creation of Bitcoin was to have a currency that was completely decentralized, quick to transact with very low fees. This was the vision that Satoshi Nakamoto had when he proposed the idea of the now famous cryptocurrency. Satoshi Nakamoto is the anonymous name used by the software developer(s) that led the creation and implementation of Bitcoin. There isn't all that much that is truly known about Nakamoto, because he chose to leave his true indenity a secret. What is known, is that on top of creating Bitcoin itself, he also created its original reference implementation. He also devised the first blockchain database, by doing this he became the first person to solve the double spending problem in digital currency. The double spending problem is a potential flaw in the digital cash scheme where a single digital token can be spent more than once, since the digital file associated with the digital token can be falsified. Ultimately, this would lead to inflation and the the digital currency losing its value relative to other currencies. Nakamoto remained active in the maintenance of Bitcoin until 2010.

Throughout the rest of this paper we will explore many different subjects and categories relating to Bitcoin. We will start by exploring Bitcoin protocol and ledgers. From there we will move into multiple other topics, in the following order: digital signatures, transactions, anonymity, blockchains, supply, hardfork, 51 percent majority weakness, security and other cryptocurrencies. [1] [6]

The Bitcoin Protocol

In this section we are going to describe how the underlying system of the Bitcoin protocol works. To make it easier to understand the fundamental principles of the system, we are going to explain them through an analogy/example which is more down to earth. We start by introducing the idea about a ledger.

Ledger

Let's introduce 4 friends to make our example easier to follow; Alice, Bob, Charlie and David. This group does a lot of activities together and they discovered that it is inconvenient to exchange money each time a person covers an expense for another person in the group. So they come up with the idea about having a public ledger, where they write what they owe the others. Say that David buy ice cream for the others and he paid $16 in total. Then they would add the following statements, more precisely called transactions, to the ledger; "Alice owes $4 to David", "Bob owes $4 to David" and "Charlie owes $4 to David".

At the end of each week they would meet up and conduct the exchange. If you owed more than you received then you put that money in a public pot, and if you received more than you owed you would take that money from the pot. This systems works fine for a small group consisting of individuals with mutual trust. However, say that Charlie has an evil side and he wants to steal money from Alice. There is nothing that stops him from putting ”Alice owes $100 to Charlie” on the ledger, based on the current protocol. Alice could state that it is a false transaction, but there is no way for Bob and David to verify who actually tells the truth. Luckily, we can solve this problem with some techniques from cryptology. We add an extra feature to each transaction, so that we later can verify the authenticity of the transaction. This feature is called a digital signature.

Digital Signatures

A digital signature is a mathematical scheme for demonstrating the authenticity of a transaction. Before we dive into the technical details, we will just explain the main idea. Alice should be able to write a digital signature, a string of bits, next to the transaction, to verify that she approves it. This signature should be unfraudable, i.e. Charlie should not be able to generate her unique bit representation in any way or copy it from another place. To be able to do this we employ asymmetric cryptography. The characteristics for asymmetric cryptography is that there exist one key for encrypting a message, the plaintext, and another key to decrypt the encrypted message, the ciphertext. We call these keys the private key and public key, respectively, and for the Bitcoin protocol they are generated from the Elliptic Curve Digital Signature Algorithm (ECDSA). The technicalities of the ECDSA are far too advanced to cover in this short paper on Bitcoin, but they are based on the modular arithmetic/number theory and cryptographic hash function. The latter will be described in *Blockchain*. What you need to know is that that the ECDSA system is secure as long as you follow the algorithm. [1]

The ECDSA has a signature generation algorithm and signature verification algorithm. These work an encryption and decryption function. When Alice wants to add a transaction to the ledger, she will have to generate a signature. She does this by following the signature generation algorithm, which uses the message and her private key as parameters. This will generate an unfraduable signature,[2] which is a pair of integers (r, s). Then the other people in the network can verify the authenticity of her signature by

[1] Bitcoin users with an Android wallet was in 2013 victims of theft after thieves discovered that the Java class SecureRandom didn’t generate random numbers. The thieves were able to find the private keys of users and transferred the victim’s Bitcoins from their wallets. [13]

[2] When we say unfraduable, we mean that there doesn’t exist a clever way to get your hand on someone’s private and generate fake signatures. The only to do this should be by brute force where you try all possible keys until you find the private key.

applying the signature verification algorithm to the signature (r, s) and her public key. The verification algorithm will either confirm the signature or derive a mathematical contradiction, in which case the signature is invalid. If it is valid, we would feel extremely confident that it was in fact signed by Alice, since we know it's nearly impossible to forge the signature.

In the current protocol, there is still room for fraud. We need each transaction to be unique. This is because we use a static private key and the transaction to generate the signature. If the transactions are not unique, Charlie could copy the signature from a legitimate transaction; "Alice pays Charlie \$10" and make as many copies of this transaction as he wants. This is a minor problem. You can think of the solution as we order the transactions in a chronological matter and include the transaction number in the transaction. I.e. for transaction number \$16, we would have "16. Alice pays Charlie \$10". Then each transaction would generate a unique signature and it would not been possible to copy it to the fake transaction "17. Alice pays Charlie \$10". This is a simple analogy, the real technicalities will be derived in *Transactions.*

Transactions

Transactions between two parties with Bitcoin are a bit more complicated than traditional transactional methods. When two parties wish to exchange Bitcoin, the exchanges have to follow a series of steps. To the user, it seems pretty straight forward: you enter the destination wallet and amount and away it goes. However, underneath the surface it is much more complicated. When a party wants to send Bitcoin to another party, the exchange first divides the order into three parts: {SOURCE, AMOUNT, DESTINATION}. The SOURCE part of the request is where the Bitcoin currently exists, such as Alice's Bitcoin wallet. The AMOUNT is how much she wishes to send to Charlie and the DESTINATION is the address of Charlie's wallet. Every Bitcoin wallet has a set of public and private keys that are assigned to it. The public key is used to identify the wallet and the private key is used to access the wallet. This means that anyone can look up how much any wallet contains, but can't access those coins. When Alice wants to send money to Charlie she sends him a message that is signed with her private key and the amount she wants to send. From there the order goes out to the network where the amount is verified by the miners. Every transaction on the Bitcoin network has to be verified by a network of miners to make sure that the part of the block chain that is valid. Once that happens the amount that Alice sent to Charlie appears in his wallet and he can now spend the money. [3]

All transactions that are made on the Bitcoin network have to be verified. This is to ensure that the people who are exchanging funds are allowed to and are using allowed funds. In order for the transaction to be verified it has to pass certain criteria:

- All outputs claimed by inputs of this transaction are in the UTXO pool. Unspent outputs can only ever be claimed once.
- The signatures on each input are valid. More precisely the combined scripts return true after executing them one after the other.
- No UTXO is spent more than once by this transaction.
- All of the transaction's output values are non-negative.
- The sum of this transaction's input values is greater than the sum of its output values; however if the numbers are different, the difference is considered to be a transaction fee that can be claimed by the miner[11]

If a transaction successfully passes all of these criteria then it will be posted and both parties will notice the difference in Bitcoins in their accounts. If a transaction does not pass one of the criteria then it will be voided and no Bitcoin exchange will happen.

Anonymity

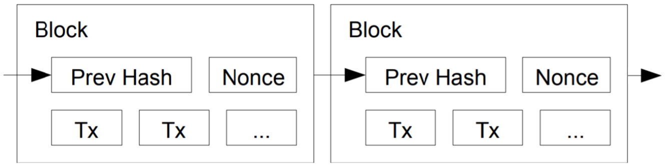
The Bitcoin protocol itself is not anonymous. Every transaction that is made on the network can be traced to a wallet and the wallet before that. However, how you set up these wallets and how you use the wallets is what helps make Bitcoin anonymous. The purpose of an anonymous Bitcoin wallet is if the user finds themselves in a situation where their identities could be compromised - such as the "darknet" or ransomware attacks. In order to set up a truly anonymous Bitcoin wallet you have to complete a lot of steps that involve using VPN services, the TOR network, and acquiring Bitcoins without using anything that can be traced back to you such as bank accounts, credit cards, or actually going into a bank to buy prepaid cards. For most users of Bitcoin, there is very little anonymity with the protocol, however, there is just enough for most transactions.

Blockchain

We have earlier stated that Bitcoin is a decentralized monetary unit. In a centralized structure you have a financial institution which keeps track of your spending, you cannot double spend the same money, and we trust that what they transfer is actually money. In a decentralized system we remove this institution, which results in some problems, like double spending. Before we cover how we solve that, we have to go through some preliminaries about how the Bitcoin network works.

The Bitcoin protocol allows everybody to download the whole transaction history, and see who has payed whom. Or more correctly, see the transaction history between anonymous digital wallets. Each person in the network keeps a local version of the transaction history. When someone wants to do a transaction, they broadcast it, with a signature, to the rest of the network. This means that everybody has to listen for transactions. In every network we can have delays, so some people will hear the transactions in different orders. This is big problem. Say that Charlie only has \$10 in his wallet and he owes both Alice and Bob \$10. He broadcasts to the other people in the network that he pays \$10 to Alice and \$10 to Bob. The first transaction is valid, but the second is invalid since he didn't have the necessary funds for it. However, people hear about the transactions in different order. Alice hears about her transaction first, and Bob does the same. Then they both think they have received the money, and that Charlie still owes the other person \$10. This is major problem, since it would lead to hyperinflation. This is the problem that the original Bitcoin paper [14] addresses. The solution is that we should trust whichever ledger has the most computational work put into it.

Before we describe what we mean with "computational work", we have to define what a cryptographic hash function is and what a blockchain is. We are taking it one step at the time, and starting with the latter. A hash function is a function that takes an input of any size and returns an output, called a "hash", of a fixed length. This means that a string of length 1 would generate a hash with the same length as the hash of a novel. The meaning of cryptographic is that it should be infeasible to find the input of a hash, i.e. finding a hash's inverse. The Bitcoin Protocol uses the hash function SHA256, which belongs to the the family of Secure Hash Algorithm 2 developed by the National Security Agency. The suffix, 256, is because the length of the SHA256 hash is 256 bits. The hash should look random, meaning that if you slightly change the input the hash should be completely different. The SHA256 is also collision resistant which means that it is hard to find two inputs that has the same hash. There are a lot of inputs with identical hashes. This is because the domain of SHA256 is infinite, but the image/range consists of 2^{256} different values. However, to find two inputs whose images are identical, you have to do an infeasible brute-force attack. There is no way to reverse engineer a hash from the SHA256 so you end up with the input.



A blockchain is data structure in which we record all the transactions. As the word indicates, it's a chain of blocks, and in each block there are about 2400 transactions, denoted Tx in the figure. We note that there are two things in each block in the figure we have not talked about; "Prev Hash" and "Nonce". We start with the latter. The idea in the Bitcoin protocol is that for a block to be added to the Bitcoin chain, we have to do a *proof by work*. A proof by work is finding a unique number, called a nonce, such that if we use SHA256 on the block we would get a hash which starts with n zeros. The only way to find a nonce is by hashing the block, check if the hash has n preceding zeros. If not, increase the nonce and repeat. In the Bitcoin system it should take 10 min to find a nonce, so n will vary depending on the total hashing power in the network combined. If there are a lot of people looking for this nonce then n will be higher than if it's only a couple of people. To verify that people don't later regret a transaction we include the hash of the previous block in each block. This creates a chain, so that if someone tries to alter a transaction in a block, then that block's hash would be invalid and all later blocks' too. We said earlier that Bitcoin users should trust the ledger which has the most computational work put into it. We now have the knowledge to understand what that means.

Members of the Bitcoin network should trust the transactions that are a part of the longest blockchain. This protocol makes it possible for a user to go offline and not keep track of the blockchain, and when he comes online again he can simply query other users about the longest blockchain. If he receives two different blockchains of equal length, he can simply wait for someone to add an extra block to one of the chains which will break the tie. To be 100% sure that a transaction is valid, a user can wait until the block containing that transaction has many subsequent blocks. We said that "someone" added a valid block to the blockchain. Everybody in the Bitcoin Network can do this, but there are people who specialize in doing this. These people are called miners, and what they do are the following: they listen for transactions published by normal Bitcoin users, they check that the transactions are valid, then they add them to a new block. When the block is full they start to find the nonce such that the hash of the block starts with n zeros. When they find this number, they broadcast the new block to everybody. The other miners will check for validity of the block. If it's valid, the other miners will start to work on this block's descendant and discard the previous block they were working on. These miners buy expensive equipment and use a lot of electricity because of the Bitcoin reward they get when they add a block to the chain, as described in the *Supply* section.

Supply

Bitcoin doesn't function like a standard currency and neither does its supply. Bitcoin supply works in a similar way to how the US dollar worked when based on the gold standard. There can only be a certain amount of currency in circulation once all the Bitcoin has been mined. The maximum amount of Bitcoin that can be in circulation is 21 million Bitcoin. The supply of Bitcoin is tied directly to mining Bitcoin, which was touched on in the *Blockchain* section.

As mentioned earlier, mining is essentially a record keeping service done through the use of computer processing power. When a miner is successful at finding a new block for the blockchain he is rewarded with newly created Bitcoins and transaction fees. When Bitcoin was first invented the reward was set at 50 Bitcoin per block mined. The code specified that every $210,000$ blocks mined that the reward would be cut in half, leading to a decrease geometrically. Eventually the reward will be set to zero, after 64 halvings, and there will be a total of $21,000,000$ Bitcoin in circulation. Markets account for this halving of mining value by increasing the exchange rate leading up to the halving. The rate of block creation also varies over time. After every 2016 blocks to aim for a constant two week adjustment period. The reasoning for having a the total capacity set at 21 million is not specifically defined. One speculation is that 21 million matches a four year reward halving schedule. Another idea is that 21 million is equivalent to the total number of Satoshis that will be mined is close to the maximum capacity of a 64-bit floating point number. The real reason for some of these constants has never been explained by Satoshi himself. The decreasing supply algorithm was chosen because it approximates the rate at which gold is mined. The exact algorithm is as follows:

$$\Sigma_{i=0}^{32}(210000)\frac{\lfloor\frac{50*10^8}{2^i}\rfloor}{10^8} \tag{1}$$

While it is impossible for Bitcoin to ever grow larger than 21 million in circulation, each Bitcoin is divisible into smaller units. The smallest divisible unit of Bitcoin is one Satoshi and is equivalent to one one hundred millionth of a Bitcoin.

While some currencies were based on valuable goods like gold or silver, the supply of Bitcoin is based on mathematics. Lastly, Bitcoin, on the individual level, is stored in something called a digital wallet. A digital wallet is basically a virtual bank account that allows users to send and receive Bitcoins.

While all of this sounds like it is set up perfectly and that it functions without flaws, in reality it doesn't. Because mining was very profitable for some, it started to become monopolized by large mining companies. Many felt that this was agaisnt the very nature of Bitcoin itself and therefore came up with a solution. This solution came to be known as a hardfork and will bring us into our next section. [18] [17] [7]

Hard fork

The Bitcoin hard fork is a form of splitting that has occurred on the blockchain. Each blockchain would then have a set of its own coins. ”The so-called hard fork, which has the potential to create two blockchains, each with its own set of coins, brings to a head a three-year-long battle between two factions who've been warring over a seemingly technical question over how to increase the amount of transactions the blockchain can process per second” [15]. The reasoning for the hard fork was primarily because Bitcoin technology is extremely slow, especially when compared to regular banks processing credit card transactions. ”Visa processes 150 million transactions per day, averaging out to roughly $1,700$ transactions per second. And their capability far surpasses that, at $24,000$ transactions per second” [10]. Not only this, as of mid to late 2017, Bitcoin mining companies were responsible for $80-90\%$ of the computing power necessary for Bitcoin to operate. These mining companies proposed something known as segregated witness, or SegWit2x. SegWit2x, at a very high-level, makes the amount of data that needs to be verified in each block smaller, by removing signature data.

After the first hard fork, Bitcoin Cash came to fruition. Bitcoin Cash is a much different story than your regular, run-of-the-mill Bitcoin. Bitcoin Cash was founded by miners that felt SegWit2x was going against everything that Bitcoin stood for when it was created. It also came about to help speed up the verification process. ”On August 1st, some miners and developers initiated what is known as a hard fork, effectively creating a new currency: Bitcoin Cash. Bitcoin Cash has implemented an increased block size of 8mb, to accelerate the verification process, with an adjustable level of difficulty to ensure the chain's survival and transaction verification speed, regardless of the number of miners supporting it. This has raised concerns about the security of Bitcoin Cash” [10]. As it can be seen, Bitcoin Cash brought many positives, even with all the controversy. Stemming from this positive feedback came another hard fork of sorts.

Introducing Bitcoin Gold. Bitcoin Gold was formed from a sort of rebellion. This seperation from the two current blockchains, would be mainly to rival Bitcoin Cash. Bitcoin gold launched in November of 2017. This Bitcoin spinoff brands itself as another version of the original Bitcoin, and all those that owend Bitcoin before the fork, would own the same amount of Bitcoin Gold afterwards. The main reason for Bitcoin Gold is to solve Bitcoin's problem with the increasing centralization of the mining industry. The way Bitcoin Gold looks to do this is by introducing new algorithms that are less susceptible to ASIC optimization. ASIC optimization is what the leading mining companies have done to take over the mining market. "The original vision for Bitcoin was that anyone would be able to participate in Bitcoin mining with their personal PCs, earning a bit of extra cash as they helped to support the network. But as Bitcoin became more valuable, people discovered that Bitcoin mining could be done much more efficiently with custom-built application-specific integrated circuits (ASICs)" [12]. This could be a very good way to keep Bitcoin from becoming centralized, which is exactly what Satoshi Nakamoto would want. Only time will tell, though, as this is still an extremely new addition to the now famous cryptocurrency.

The 51% majority weakness

The protocol described in *Bitcoin Protocol* makes it nearly impossible to trick the blockchain unless you have the majority of the hashing power in the network. If you have that much power you could potentially make your own chain that always would be the longest. There are still a limited amount of things they can do. 1) they could decide which transactions get approved or not. 2) They could go some blocks back and removes transactions and start a new fork from there. In this case they would have to catch up with the legitimate chain again. 3) They could double spend their money. Say they want to buy some merchandises. They broadcast the transaction. The merchant waits until he has gotten several confirmations, i.e. the block containing this transaction has several subsequent blocks, before he sends the merchandises. Meanwhile the thieves have been working on an alternative chain with all other transactions except theirs. When they have received the merchandises they publish their private chain where they still have their money. We see that just having 51% of the hashrate just gives you a fifty-fifty chance of having your chain be the longest chain. See section 11 in [14] for calculations.

The current hashing rate of the Bitcoin system is about 10^{19} hashes per second. This correspond to 80 704 petafLops per second. The top500 supercomputer per June 2017 had a combined performance of 749 pflop/s [16]. This illustrates the magnitude of the networks power. One should note that this is a biased comparison. The supercomputers have enormous CPU power, while the miners us application-specific integrated circuits (ASICs) which are designed to just calculate SHA256 hashes. The web page [9] they have calculated the cost of getting 51% hashing power based on the cheapest ASIC. The results are that the hardware would cost 3.5 billion dollars and that it would consume 123 636 699 kWh per day (6.2 million dollars per day). This is a sum which is affordable for major companies and governments.

Security

All Bitcoins are stored in digital accounts called wallets. These wallets can either exist on hosted services such as Coinbase or BitGo, or locally on someone's personal hardware. Both of these options have pros and cons and different security risks. As with everything that is stored on the "cloud" there are inherent risks of a breach happening. In order to combat this the online wallets are implementing two factor authentication with tokens to enable secure logins to their services. This is different than the two factor with texting because it uses an authentication app such as Google Authenticator to produce a unique token for each login.

However, some people don't trust online sources to keep their Bitcoins safe. An example of this was in 2014 when Mt. Gox filed for bankruptcy. Mt. Gox was an online solution for holding and trading Bitcoins. At its peak, Mt. Gox was responsible for 70% of all Bitcoin transactions in the world. When Mt. Gox filed for bankruptcy almost all of the 850,000 Bitcoins that they were holding went missing and were assumed to be stolen. Since then, about 200,000 of those Bitcoins have been found and returned to their owners [5].

The alternative to keeping your coins on an online wallet is to keep them locally on your own machine and hardware. While this does make it easier to ensure the security of coins when it comes to hacking, it does not do anything to ensure the safety of your coins when it comes to crashes. Hardware always fails. It just does and if your coins are on the hardware that crashes and you don't have any backups you permanently lose those coins and can't recover them. So by slightly removing the hacking threat you add the crashing threat. It is all a game of risk and chance and it is something that a person has to consider when choosing where to put their wallets.

Other Cryptocurrencies

Bitcoin is not the only type of cryptocurrency that is on the market today. There are over 1,000 different kinds all having different market caps and market values. However, there are two others that are relatively common: Ethereum, and Litecoin. Both of these currencies are based off of a block chain and have minor differences from Bitcoin. For exmple, Litecoin is different in that while it takes miners about 10 minutes to process a block with Bitcion it only takes about 2.5 minutes with Litecoin. It also ”uses scrypt in its proof-of-work algorithm, a sequential memory-hard function requiring asymptotically more memory than an algorithm which is not memory-hard” [4]. What this means is that it uses considerably more memory than Bitcoin does when mining. Ethereum is a currency that was created because the founder disagreed with how Bitcoin was being developed and decided that he needed to add a scripting language to the development of applications [2]. So the underlying blockchain is not that different from Bitcoin, it is just that the applications used to mine it are different.

Conclusion

When it is all said and done, Bitcoin has brought to us both innovation and headaches. Some see Bitcoin as a menace to society. These people believe that Bitcoin has enabled cybercrime to an unprecedented extent. ”Using the currency is also increasingly easy to do, and that also applies to cybercriminals seeking to launch ransomware attacks... The developers of these tools make money themselves by including a means for taking a cut of any criminal proceeds gained by the user. That's automated, too, and the sophistication and accessibility of the software means attacks can be launched at scale. Ransom demands are made affordable, with instructions for how to create a virtual wallet and buy the sufficient Bitcoins to pay the money in return for a code that will unlock the data on a computer or network” [19]. Not only can Bitcoin be used for ransomware, but it is also untraceable, making it perfect for illegal purchases on the darkweb. However, there are many upsides to the technology. Bitcoin is seen by many others as one of the top inventions since the internet itself. Components, such as the blockchain, have helped to revolutionize crytpocurrency as a whole. ”First, Bitcoin at its most fundamental level is a breakthrough in computer science – one that builds on 20 years of research into cryptographic currency, and 40 years of research in cryptography, by thousands of researchers around the world” [8]. It is apparent that Bitcoin has its benefits and its drawbacks. Either way, it will be interesting to see where this technology takes us in the future and to see how Bitcoin itself blossoms, or potentially crumbles.

References

[1] Bitcoin: ”https://en.wikipedia.org/wiki/bitcoin” accessed: 2017-11-22.

[2] Ethereum: ”https://en.wikipedia.org/wiki/ethereum” accessed: 2017-11-26.

[3] How do bitcoin transactions work?: ”https://www.coindesk.com/information/how-do-bitcoin-transactions-work/” accessed: 2017-11-26.

[4] Litecoin: ”https://en.wikipedia.org/wiki/litecoin” accessed: 2017-11-26.

[5] Mt. gox: ”https://en.wikipedia.org/wiki/mt.$_{g}ox$”$accessed : 2017 - 11 - 26$.

[6] Satoshi nakamoto: ”https://en.wikipedia.org/wiki/satoshi$_{n}akamoto$”$accessed : 2017 - 11 - 22$.

[7] What is bitcoin?: ”https://www.coindesk.com/information/what-is-bitcoin/” accessed: 2017-11-22.

[8] M. Andreessen. Why bitcoin matters: ”https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/” accessed: 2017-11-23.

[9] J. L. for GoBitcoin.io. Cost of a 51% attack: ”https://gobitcoin.io/tools/cost-51-attack/?” accessed: 2017-11-19.

[10] J. Frakenfield. Bitcoin vs. bitcoin cash: What’s the difference: ”https://www.investopedia.com/tech/bitcoin-vs-bitcoin-cash-whats-difference/” accessed: 2017-11-23.

[11] R. Kotcher. Blockgeeks: ”https://blockgeeks.com/bitcoin-transactions/” accessed: 2017-11-29.

[12] T. B. Lee. Bitcoin gold, the latest bitcoin fork, explained: ”https://arstechnica.com/tech-policy/2017/11/bitcoin-gold-the-latest-bitcoin-fork-explained/”, accessed: 2017-11-23.

[13] C. Meyer, J. Somorovsky, E. Weiss, J. Schwenk, S. Schinzel, and E. Tews. Revisiting ssl/tls implementations: New bleichenbacher side channels and attacks. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 733–748, San Diego, CA, 2014. USENIX Association.

[14] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system,” http://bitcoin.org/bitcoin.pdf, 2008.

[15] L. Shin. What will happen at the time of the bitcoin hard fork?: ”https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/7882741b337d” accessed: 2017-11-23.

[16] E. Strohmaier and H. Simon. Highlights - june 2017: "https://www.top500.org/lists/2017/06/highlights/" accessed: 2017-11-19.

[17] J. P. Tal Yellin, Dominic Aratari. What is bitcoin?: "http://money.cnn.com/infographic/technology/what-is-bitcoin/" accessed: 2017-11-22.

[18] F. Tepper. The reward for mining bitcoin was just cut in half: "https://techcrunch.com/2016/07/09/the-reward-for-mining-bitcoin-was-just-cut-in-half/" accessed: 2017-11-22.

[19] S. Usborne. Digital gold: why hackers love bitcoin: "https://www.theguardian.com/technology/2017/may/15/digital-gold-why-hackers-love-bitcoin-ransomware" accessed: 2017-11-23.