Masaryk University

Faculty of Economics and Administration

Major: International Relations – Economic Policy

ECONOMIC CONSEQUENCES OF CRYPTOCURRENCIES AND ASSOCIATED DECENTRALIZED SYSTEMS

Bachelor Thesis

Thesis Advisor:	Author:
Ing. Jan JONÁŠ, Ph.D.	Dávid STANCEL

Brno, 2015

Author:	Dávid Stancel
Bachelor Thesis Topic:	Economic Consequences of Cryptocurrencies and Associated Decentralized Systems
Department:	Economics
Thesis Supervisor:	Ing. Jan Jonáš, Ph.D.
Rok obhajoby:	2015

Anotácia:

Predmetom bakalárskej práce „Hospodársko-politické dôsledky využitia kryptomien a ďalších pridružených decentralizovaných systémov“ je analýza kryptotechnológií, hlavne kryptomien, a možné implikácie ich využitia v rôznych organizáciách nielen štátnej správe, za účelom ich zefektívnenia a zvýšenia transparentnosti. Hlavným teoretickým východiskom práce je analýza technologických aspektov decentralizovaných systémov, na ktorých sú kryptomeny postavené, a na základe ktorých autor ďalej vyvodzuje ich ekonomické dôsledky.

Annotation:

The goal of the submitted thesis: “Economic Consequences of Cryptocurrencies and Associated Decentralized Systems” is to analyze crypto technologies, mainly crypto currencies, and the possible implications of their utilization in various organizations not only in state administration. The key theoretical background of the work is the analysis of the technological aspects of decentralized systems which crypto currencies are based upon, and upon which the author concludes their economic consequences.

Kľúčové slová

Kryptomeny, Bitcoin, blockchain, decentralizované systémy, krypto-technológie

Keywords

Crypto currencies, Bitcoin, blockchain, decentralized systems, crypto technologies

Declaration

I hereby declare that thesis *Economic Consequences of Cryptocurrencies and Associated decentralized Systems* is the result of my own independent scholarly work under the supervision of Ing. Jan Jonáš, Ph.D. All references contained in the thesis have been properly cited and original authors acknowledged in accordance with legislation, internal regulations of Masaryk University and internal managing acts of Masaryk University and Faculty of Economics and Administration of Masaryk University.

Brno, April 21st 2015

Dávid Stancel

Acknowledgments

I would like to express my appreciation to my thesis supervisor Ing. Jan Jonáš Ph.D., for his assistance and valuable comments. My gratitude also goes to Pavol Lupták whose lecture inspired me to investigate this topic.

Contents

Introduction.........7

1. Crypto technology.........9

1.1 Cryptography used in Bitcoin.........10

2. Centralized vs. Decentralized Ledgers.........12

3. The Byzantine Generals Problem.........13

3.1 What is The Byzantine Generals Problem?.........13

4. Bitcoin.........17

5. The blockchain.........19

5.2 Synchronization of the blockchain.........20

5.3 Possible jeopardy.........23

6. Alternative uses of the blockchain.........25

6.1 Escrow service.........25

6.2 Meta coins.........26

6.3 Attestation and Sidechains.........27

6.4 Smart contracts and Smart property.........28

6.5 Financial contracts and instruments.........30

6.6 Political Speech and Ethereum.........31

7. “Disruptive” Substitution Technology.........33

7.1 Central cadaster, company register.........33

7.2 Government procurement.........34

7.3 Government money.........35

7.4 Revenue service and Customs office.........37

7.5 Smart money.........37

Conclusion.........39

Reference.........40

List of tables and figures.........43

List of abbreviations.........44

Introduction

In the past couple of months, the rise of Bitcoin had caused that cryptocurrencies have been getting increasingly more traction across the world. Despite of that, majority of them is mostly affiliated merely with decentralized payment systems. Interestingly enough, the potential hidden behind these sophisticated systems and networks has not been examined yet to the extent it deserves. Therefore, the purpose of this work is to discover what economic consequences this cutting edge technology may bring to our society in terms of the way our, not only, government organizations work, along with possible implications for economic policy.

Cryptocurrencies, and particularly Bitcoin, have been recently a subject of many studies and analyses mainly in terms of their economic properties. The analyses, such as of Pattison (2011), Hamacher and Katzenbeisser (2011), Britto and Castillo (2013) or Combs and Mitsoff (2014) are usually focused on very narrow range of functions of cryptocurrencies, and lack the broader context. The goal of my thesis is to show that emergence of crypto, often referred to as disruptive, technology creates a bridge between the field of information technology and economics because it allows to change the way some of our institutions work. I attempt to highlight a completely new point of view on the utilization of crypto currencies, and thus examine those that are the most relevant for this purpose. Since the abovementioned studies, focus on monetary properties of cryptocurrencies and particularly Bitcoin, unlike those I focus on their technological properties in order to conclude economic consequences with possible far-reaching impact. I examine the possible implementation of not only Bitcoin but also other cryptocurrencies and their underlying blockchain mechanism. The blockchain being a technological advancement so powerful that it possesses the potential to make various, not only government, organizations much more efficient and transparent. This is because it can change the concept of ownership and trust as we know it today, and thus fundamentally influences the way our economy and governance systems work. Given this, a fundamental question arises. Can we use crypto currencies and its technology to make, not only financial, organizations work in a more transparent and more efficient way?

The thesis analyzes the most recent information and sources dedicated to decentralized consensus technology, and it suggests how these can be implemented in state administration.

As mentioned above, the subject of the thesis is a largely unexplored field in which progress is being made every day. This is reflected in lack of resources that are dedicated to this topic. Therefore, I do research of primary resources such as so called white papers of particular cryptocurrencies, and I also examine collections of forum posts of the creator one of the most prominent crypto currency - Bitcoin. Furthermore, I analyze given implications using online courses lead by experts in the field of cryptography such as Boneh (2015), Narayanan et. al, (2015) and Antonopoulos (2014) and digital currencies, respectively.

The work does not examine technical aspects that are not relevant for its goal; rather it summarizes those upon which it makes conclusions in a comprehensive and easy-to-read way. The paper is structured into seven chapters with subheadings. The first chapter deals with introduction to cryptography in order to provide basic overview of the field for a reader. In the second chapter I lay out the main differences between centralized and decentralized ledgers that are essential for understanding of problems that are addressed later on in the work. The third chapter discusses a well-known computational problem of building purely decentralized and trusted networks. The next chapter then introduces one of the most popular crypto currency – Bitcoin – and deals with its technologic properties. In the fifth chapter I analyze the peer-to-peer mechanism upon which Bitcoin and some other crypto currencies are based upon – the blockchain. In this chapter the whole mechanism is explained into details in order to clarify the technology´s potential. The following chapter then provides a comprehensive outline of cryptocurrencies and applications that utilize the blockchain. At the end of my work, in the chapter number seven, upon the synthesis of the concepts and findings from the previous chapters I draw my conclusion on the possible way these technology´s utilization will most probably look like in various areas of economy in the future.

1. Crypto technology

For better understanding of crypto currencies is essential to be aware of certain facts related to the field of crypto technology. Crypto technologies are technologies that are based on cryptography. Cryptography has a long tradition in human history. However, modern mathematical cryptography has been developed only over the last few decades. Public key cryptography, that will be mentioned below, was introduced for the first time in 1976 and first attempts to create a cryptocurrency were made in the beginning of 1980´s (Omohundro, 2014:19). Crypto-technology is a class of software systems that use cryptography. Generally, these software systems can implement a system to transfer virtual goods and at the same time they can implement complex agreements between parties. There are various kinds of virtual goods such as songs, online documents, or pieces of software. However, there are other kinds of virtual goods that might not be that obvious such as *ownership* of almost anything, *an approval, notarization or verification* of almost anything or a unit of currency (Eckersley, 2004:87). There are three main problems, relevant for the purpose of this work that are addressed by crypto technologies. First of all, it is *counterfeiting* in other words, assurance of the parties that the original virtual good was transferred, not a copy. Secondly, it is *trust.* This means that the *trust* of the counter-party is not required to transfer the virtual goods. This is because the transfers are verified. Last but not least, another problem addressed by the technology is *central authority*, meaning that it enables absence of such an authority in order to process transactions or maintain the ledger – there is no middleman involved (Boneh, 2015, lecture 1).

All crypto-technology is underpinned by the two main ideas: *Public Key Cryptography* and *the blockchain.* The first one – public key cryptography – is a sophisticated math concept that allows an individual to encode a virtual good that can only be decoded by the intended recipient. Even the sender cannot decode it once the good has been encoded. In this concept there are two numbers deployed: a private key and a public key. The second idea is the blockchain which can be described as a special form of ledger that keeps track of evidences who holds what, and that is extremely hard to be deceitfully modified (Antonopoulos, 2014, lecture 3). Also, one of the important properties of the blockchain is its pseudo-anonymity. In the next chapters, these ideas will be described more into details.

1.1 Cryptography used in Bitcoin

For the purpose of this work is not necessary to understand all the technological details behind this whole sophisticated machinery that Bitcoin is based upon. However, it is crucial to reach a certain level of understanding some basic rules of cryptography used within the system. Therefore, in this chapter I will explain these in a simplified way, and filter out information that are not relevant for the purpose I have set in my work.

The whole concept of Bitcoin is based on two main cryptographic technologies:

a) Cryptographic hash function [1]
b) Public Key Cryptography [2]

In the network, all the users communicate between each other through messages, so called *transactions.* These usually carry information about transfers of bitcoins from one address to another one. Ownership is established via digital keys and digital signatures (Antonopoulos, 2014, lecture 3). *Digital keys* consist of a mathematically-related Private-Public key pairs, and are stored offline. The *private key* is randomly generated and kept (secretly) by the owner of bitcoins. It is used for authorization of transactions by digital signature that confirms ownership and verifys authenticity of the transactions. On the other hand, *public key* is generated from the private key (using one-way cryptographic hash function), and it is used for validation of the transaction´s digital signature by the new owner. The public key is also visible by everyone (Narayanan, and Bonneau, 2015, lecture 1).

Bitcoins can be transferred between *addresses.* Each address is a unique identifier of a user, and is encoded so it is represented by 58 alphanumeric characters. All the transactions are stored in blocks that are *chained* together. This is how the blockchain is created. Its chronological order as well as block integrity verification is done via *hash functions.* These are mathematical functions used for verification of data integrity by transforming *identical* data (input) to a unique code (digest) of fixed size. Any modification of the data, whether it is by accidence or by purpose, leads to changed hash code (Antonopoulos, 2014, lecture 3).

Since blocks contain a history of the bitcoin addresses that a coin has been transferred to also the issue of anonymity emerges. Nakamoto, the creator of Bitcoin, addresses this issue as follows:

[1] In this case – SHA-256 and RIPEMD-160

[2] ECDSA – Elliptic Curve Digital Signature Algorithm

> *"If the identities of the people using the bitcoin addresses are not known and each address is used only once, then this information only reveals that some unknown person transferred some amount to someone else. The possibility to be anonymous or pseudonymous relies on you not revealing any identifying information about yourself in connection with the bitcoin addresses you use. If you post your bitcoin address on the web, then you're associating that address and any transactions with it with the name you posted under. If you posted under a handle that you haven't associated with your real identity, then you're still pseudonymous. For greater privacy, it's best to use bitcoin addresses only once."* (Champagne, 2014:118).

It is also important to understand how these transactions work and go more under the surface. A detailed and at the same time easy to understand description of it is interpreted in the course of Andreas Antonopoulos where he states:

> *The sender encrypts the message (M) using the recipient´s public key: C = encrypt (M, Kpub[3]).*
>
> *The recipient decrypts the encrypted message (C) using his own private key: M = decrypt (C, Kpriv[4]).*
>
> *Where: the decrypted message (C) is the result of encryption (also known as "ciphertext"), and (M) is unencrypted/decrypted message (also known as "plaintext")*
>
> *There is an asymmetric mathematical relationship between the public and private keys:*
>
> - *The public key can be easily derived from the private key*
> - *The private key is nearly impossible (or computationally infeasible) to derive from the public key* (Antonopoulos, 2014, lecture 3).

The above stated facts provide us with crucial insight into the whole process. It should be clear now that every transaction connects certain amount of bitcoins with an address, records the path of those, and includes a valid signature. Moreover, it broadcasts to the entire network the change of ownership of the bitcoins. The complete history of all transactions is stored in each node´s "memory" so ownership of particular bitcoins can be verified easily. All this is essential in order fully understand new possibilities that are revealed to us by this technology.

[3] Public Key

[4] Private Key

2. Centralized vs. Decentralized Ledgers

Before I proceed to examination of the ways aforementioned technology can be implemented, it is important to address what kind of issues it is supposed to solve. Therefore, in this chapter I will deal with centralized and decentralized ledgers and possible implications of emergence of latest crypto technology.

When we think of *ledger* we usually imagine some "*collection of an entire group of similar accounts in double-entry bookkeeping* or *records classified and summarized financial information from journals as debits and credits and current balances"* (Business Dictionary, 2015). However, ledgers are not only used in accounting but also generally in any kind of record keeping. Many of, not only, government organizations such as cadasters, registers or banks use ledgers in order to store information of any kind, for instance records of ownership. Given this, we can see the concept of centralized ledger very often in our daily life, and thus we take it for granted. In our modern society pretty much all important ledgers have a *trusted* party in charge that administrates it and that vouches for the trustworthiness of the records stored in the ledgers.

However, there are some problems connected to centralized ledgers, more precisely to their record-keepers. In reality, these entities are often dishonest and they may take bribes to manipulate the records in a ledger. Secondly, they also may act as gatekeepers and exclude certain parties that they disapprove. Third, the problem does not have to be their deceitfulness rather than just carelessness or other reasons why they can lose important records. On the contrary, decentralized ledgers would avoid these possible flaws, and thus become preserved against censorship and exclusion as well as against misconducting of record-keepers, and finally against loss of records. Of course, if a ledger is to accomplish this it must fulfill one crucial condition – to build a purely distributed but mainly *trusted* system (Antonopoulos, 2014, lecture 2). The reason why this can be such a difficult task to execute is examined in the next chapter.

3. The Byzantine Generals Problem

As previously mentioned, when building a decentralized ledger one faces a couple of obstacles which the most important one of them is *trust.* In this chapter I will explain and demonstrate why is trust such an important, and hard to reach, issue. The problem is not new and has been present here for decades. This challenge, to enforce trust in distributed systems, where distributed components that need to communicate between each other information that might be communicated inaccurately, was portrayed for the first time by Marshall Pease, Robert Shostak and Leslie Lamport in 1982 and it was named The Byzantine Generals Problem (BGP) (Antonopoulos, 2014, lecture 3).

3.1 What is The Byzantine Generals Problem?

The reason why the problem of building a distributed but trusted system has gotten the name it has is described can be found directly in the paper of Pease, Shostak and Lamport from 1982:

"We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that:

A. All loyal generals decide upon the same plan of action.

The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition A regardless of what the traitors do.
The loyal generals should not only reach agreement, but should agree upon a reasonable plan. We therefore want to insure that

B. A small number of traitors cannot cause the loyal generals to adopt a bad plan."

Figure 1: Lieutenant 2 a traitor

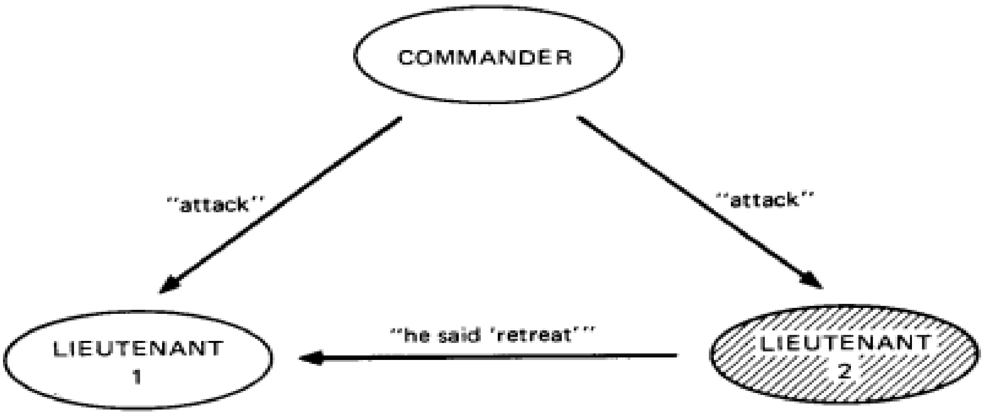

Fig. 1. Lieutenant 2 a traitor.

Source: PEase, Shostak, and Lamport, 1982:385

Figure 2: The commander a traitor

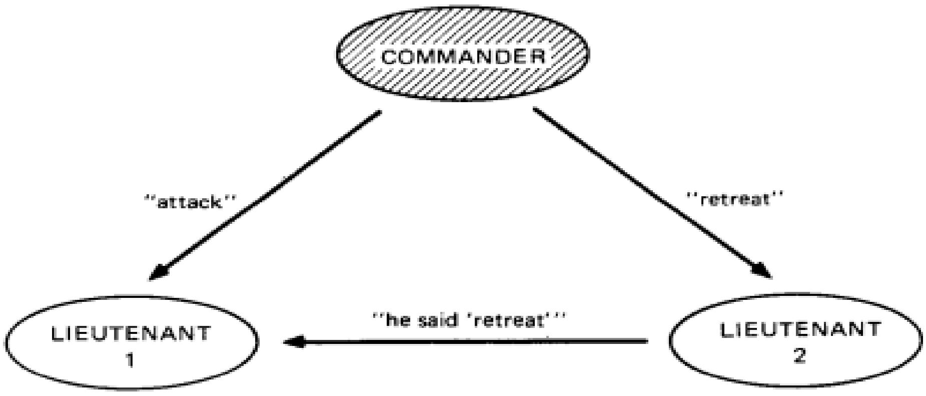

Fig. 2. The commander a traitor.

Source: Pease, Shostak, and Lamport, 1982:385

A reliable computer system must be able to cope with malfunctioning components that give incompatible information to different parts of the system. As stated above, such a situation can be expressed abstractly as a group of generals of the Byzantine army camping with their troops around an enemy city. They must agree upon a common battle plan, whereas communication amongst them can be maintained only by messenger. We assume that in this "network" of generals one or more of them may be traitors (figures 1 and 2) trying to confuse the others. This assumption puts the possibility of generals reaching agreement to question. The problem is to find an algorithm to ensure that they will do so. Using only oral messages, the problem is to be resolved only if more than two-thirds of the generals are loyal; meaning that a single traitor can throw into confusion two loyal generals. However, with nonchangeable written messages that restrict traitors´ ability to lie, the problem is solvable for any number of generals and possible traitors. As the number of the parties in the system increase, as seen on the figure 3, the number of channels for communication increase diametrically (and opportunities for mistrust increase exponentially). So does increase the complexity of a decentralized system with thousands of parties involved in order to build consensus (Pease, Shostak, and Lamport, 1982:385).

Figure 3: Algorithm OM (1), Lieutenant 3 a traitor; and the Commander a traitor

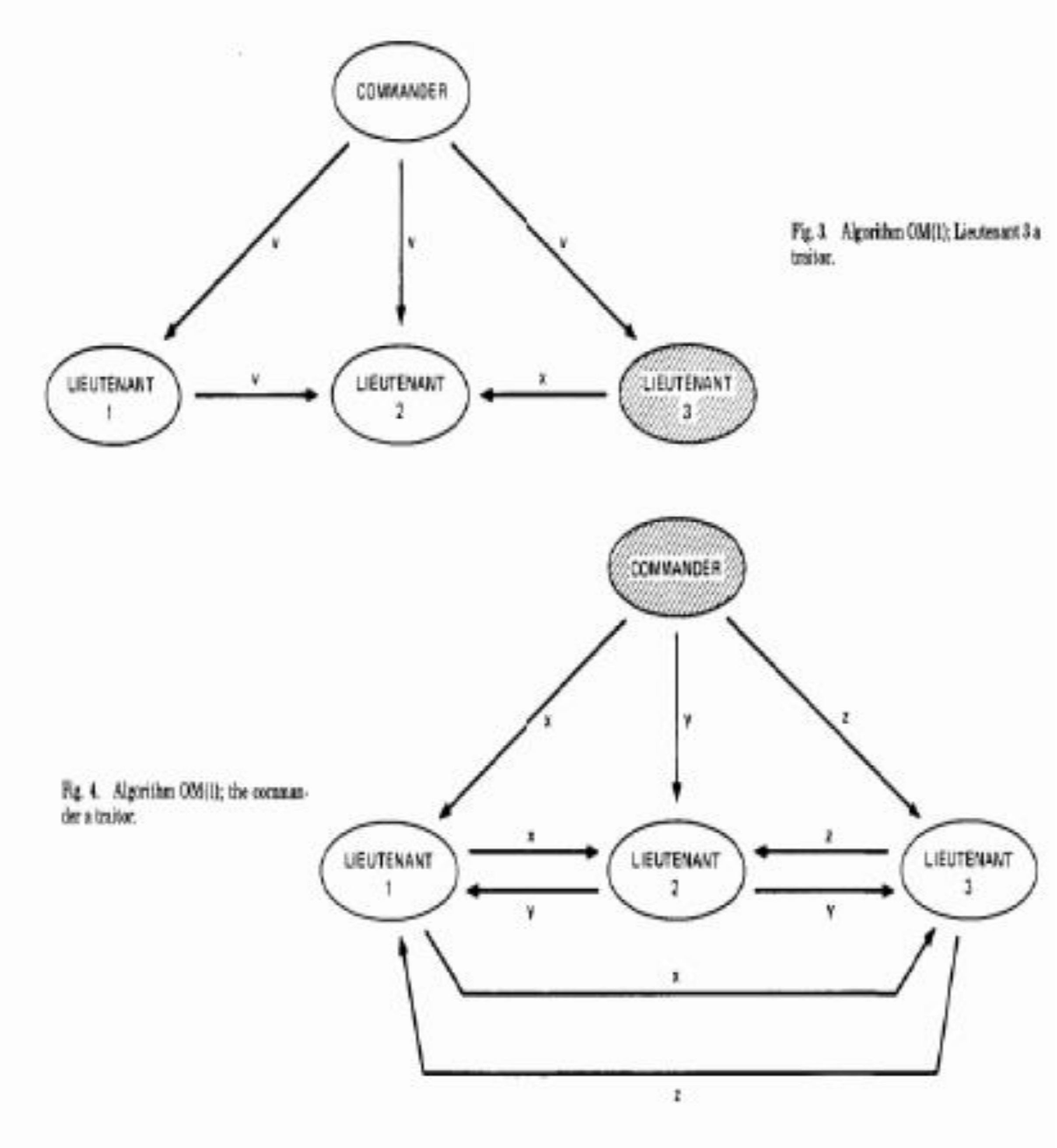

Fig. 3. Algorithm OM(1); Lieutenant 3 a traitor.

Fig. 4. Algorithm OM(1); the commander a traitor.

Source: Pease, Shostak, and Lamport, 1982:385

4. Bitcoin

As chapter 4 discusses the problems that are arising from the decentralized character of distributed and trusted systems, in this chapter I examine the way Bitcoin addresses the Byzantine Generals Problem. People often think of Bitcoin as merely a virtual currency or a transaction system. However, a thorough look at all its complexity reveals that the monetary aspect is just a tip of the iceberg. What can be seen under its surface can be described as a ground-breaking internet technology, for which money is only one of the possible applications. In order to gain enough comprehension of the issue one must be familiar with basic technical features of the Bitcoin. Its concept was first discussed in 1998 by group of people who were members of the Cypherphunk mailing list. After a decade, in 2008, someone named Satoshi Nakamoto published *The White Paper* where the whole concept is described into details. The identity of Nakamoto is unclear and there are some speculations that there is actually a group of people, behind this name, who worked together in this complex project (Combs and Mitsoff, 2014:18).

To avoid confusion, the terminology needs to be clarified. When I talk about *Bitcoin* I mean the concept, or the entire network itself. When referring to a unit of account, I use *bitcoin* without capitalization. Bitcoin is a peer-to-peer[5] online payment system where users can transact directly without an intermediary being involved. All transactions within the network are verified by network *nodes* on the basis of complicated state of the art mathematical principles, and are recorded in a public distributed ledger. Due to this principles it is ensured that all the nodes in the network automatically reach agreement about the actual state of the ledger. This ledger is called *the blockchain* and it uses its own unit of accounting – bitcoin. Each node – a user´s computer - in the network operates through certain Bitcoin “client” software. Once a node is added to the network, in other words when a user downloads a piece of software, the blockchain – the ledger of all transactions in the history of Bitcoin – is downloaded by this software. This means that every single node of the network stores the complete record of all transactions which are locked, including information of the time, date, participants and amount of every single transaction, in the blockchain. If there is a fraudulent attempt to crook a transaction being made the unanimous consensus won´t be reached, and hence the transaction will be refused to be incorporated in the blockchain. Since all transactions are public, and approved by thousands of nodes, it is almost like there is a notary

[5] Distributed amongst equally privileged peers.

present at every executed transaction. This creates single source of truth that is accessible to everyone in the network. In other words, Bitcoin software enables a network of computers to maintain a collective book-keeping via the internet. This book-keeping is neither closed, nor in control of one party, and thus central record-keeper is absent (Antonopoulos, 2014, lecture 3).

As indicated above, Bitcoin is not only digital money, but also, more importantly, a sum of technologies that create an ecosystem. There are four important technologic aspects included here:

a) a decentralized peer-to-peer network,
b) a public transaction ledger,
c) a mathematical currency issuance mechanism that is completely decentralized, and
d) a decentralized transaction verification system.

All of these will be discussed more into depth in the next chapter.

5. The blockchain

The blockchain itself, compared to Bitcoin, has not gotten that much of traction in the media neither in academia yet. It is important to note that blockchain as a technology is not only behind Bitcoin neither behind all cryptocurrencies since it is limited only to decentralized crypto currencies that use proof-of-work and proof-of-stake protocols which are explained later in this chapter. While many books that have been released in past three years focus on cryptocurrencies´ monetary properties and Bitcoin as a payment system, the main reason for the excitement about this technology – practical manifestation of possibility to decentralize all ledgers – have not been discovered by mainstream media and neither by most of the academicians. However, scientific articles that pursue to discover its full potential are on increase in the past couple of months. Presumably, one of the first scholars who put together some more comprehensive scientific materials dedicated to the other properties of the Blockchain were those from the University of Nicosia, where also the first master degree in digital currencies was launched. They created an MOOC (Massive Online Open Course) *Introduction to Digital Currencies* which provides quite deep explanation of this sophisticated technological machinery.

In the course we can find the blockchain defined as a "*publicly reviewable ledger containing a verified record of every transaction"* (Antonopoulos, 2014, lecture 3). In order to understand why this seemingly simple formula is so ground-breaking, one needs to grasp the whole process behind it.

From the user point of view all this starts when a piece of software – Bitcoin *client* – is downloaded by a user. The client initially downloads the blockchain, in other words the history of all transactions that ever happened. This complete ledger of all transactions is stored by each client. Since all the records are distributed among nodes, there is no central record-keeper involved (Antonopoulos, 2014, lecture 7).

At this point, the issue of synchronization emerges, because blockchains (ledgers) must be kept synchronized with each other, which means they must reach "distributed consensus" without any central authority or, in other words there must be a mechanism that prevents a client accepting conflicting messages about a transaction, and that enables to clients distinguish between truthful and deceitful; using the analogy of generals, to distinguish between loyal generals and traitors. And this is where the magic occurs (Antonopoulos, 2014. lecture 3).

5.2 Synchronization of the blockchain

By now, it should be clear that keeping the blockchain copies in synchronization is a manifestation of the Byzantine General Problem. In this chapter I will describe the way this problem is addressed by the blockchain.

When there is a transaction executed by a client, it broadcasts the transaction also to all other users in the system. Therefore, in a few seconds almost all the nodes in the network possess information about the transaction. By now, we still cannot tell whether the client sending the transaction is not moving the same bitcoins to two different addresses. In other words, it is not clear if the message (transaction) broadcasted by the general (client) is truthful or fraudulent, and thus the transaction is unconfirmed.

The crucial aspect of the system, and also the answer to the BGP is a process known as *mining.* The term “mining” is a quite misleading analogy for what is being done by miners. To understand the role of miners it helps to think of them as bookkeepers. The process consists of three main steps. In the first one, a miner creates a file that contains:

(a) *The hash* – a product of an algorithm turning data of a variable length into data of a fixed length – of the block in the existing blockchain,

(b) A block of the new proposed transactions broadcast in the Bitcoin network, and

(c) A random number that the miner guesses, a so called “nonce” (Antonopoulos, 2014, lecture 2).

The combination of these three makes the data used as the input for the second step. In this step a cryptographic function is applied to the data by miners. The most important feature of the function is the unique sting of characters, produced by the function, that cannot be reversed; so even knowing the result does not allow us to retrace to the initial data. This string of data is known as “data hash”.

In the last step, the hash is reviewed against a desired pattern. If the hash and the pattern match, the miner has a valid block and gets reward. If they do not match, the miner returns back to the first step guessing a new once while repeating the exercise (Antonopoulos, 2014, lecture 2).

Once the hash and pattern matched the miner has a wining block. This is broadcasted as a “block” of confirmed transactions. The match is verified by the nodes in the network and they accept the new block as they add it to the existing blockchain that they all store. After this they start to search for the next block. This happens already with the new and larger blockchain incorporated. The miner which has a winning block can collect an allocation of new bitcoins (currently circa 25 bitcoins per block) that are added to the total number of bitcoins. This reward for blocks is halving every 210, 000 transactions which is approximately, given the current base of users, in every 4 years (Britto, and Castillo, 2013:6).

As indicated above; it may be concluded that the more computing power client has the faster it can execute aforementioned operations and more likely it is to be rewarded. However, this is not the case since the prizes, new blocks, auto-adjust the difficulty of guessing a random number (nonce) every 2016 blocks according how much power is in the network. Meaning that the difficulty is adjusted approximately every two weeks and a block is mined approximately every 10 minutes (Champagne, 2014:21). It may take more or less time to create a block due to luck, however if it is produced to often or not often enough the difficulty adjusts accordingly and the pace is restored. In the end it does not matter if the whole network comprises of a few old computers, or millions of super machines, because either way the blocks are being created every 10 minutes. Only the money incentive changes since a miner´s expected reward is equal to his percentage share on the total network´s computing power. This is the point where the Byzantine Generals Problem is being addressed. And the answer is quite simple. When a Bitcoin client is deciding which blockchain version to accept, it must choose the one that is longer. It must choose the one that has “greatest combined difficulty” of the hashes used to create it; the one that took the most computation power to create. The unaccepted chain, the shorter one, is discarded and we call it an “orphan block”[6]. This means that malicious nodes cannot keep inserting bad signals into the blockchain (double spending) unless they can produce the longest block. Given the essentially random nature of creation of blocks, this is statistically highly unlikely to happen (Antonopoulos, 2014, lecture 7). This feature that is often subject of confusion by laymen since it is sometimes considered to be an indication of poor design of the system. However, this cannot be further from the truth. It is

[6] Since transactions in the orphan block were not in the longer chain they need to be reprocessed.

exactly this – *proof of work* [7] – in form of mining that is the most crucial aspect of providing ledger security since it prevents any party from taking over the ledger (Guttman, 2014:393). In the case of Bitcoin *Hashcash*[8] proof of work is used. It is useful to think of this random character of creation of blocks as a kind of lottery that determines who enters the next transaction in the system (Bitcoin Wiki, 2015). The groundbreaking implication of what I just explained stated Nakamoto in the Cryptography Mailing List, using a modified analogy of the BGP:

> *"A number of Byzantine Generals want to attack the King's Wi-Fi by forcing the password, which they've learned is a certain number of characters in length. Once they stimulate the network to generate a packet, they must crack the password within a limited time to break in and erase the logs, otherwise they will be discovered. They only have enough CPU power to crack it fast enough if a majority of them attack at the same time. They don't particularly care when the attack will be so they decide that anyone who feels like it will announce a time, and whatever time is heard first will be the official attack time. The problem is that the network is not instantaneous, and if two generals announce different attack times at close to the same time, some may hear one first and others hear the other first. They use a proof-of-work chain to solve the problem. Once each general receives whatever attack time he hears first, he sets his computer to solve an extremely difficult proof-of-work problem that includes the attack time in its hash. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work in the hash they're working on. If anyone was working on a different attack time, they switch to this one, because its proof-of-work chain is now longer.*
>
> *After two hours, one attack time should be hashed by a chain of 12 proofs-of-work. Every general, just by verifying the difficulty of the proof-of-work chain, can estimate how much parallel CPU power per hour was expended on it and see that it must have required the majority of the computers to produce that much proof-of-work in the*

[7] Proof of work refers to some data that was costly, or at least time-consuming, to produce in order to satisfy certain requirements. It can be a random process with low probability.

[8] Hashcash is a cryptographic algorithm that sets up a framework within all miners create proof-of-work which validate the blockchain transaction.

> *allotted time. They had to all have seen it because the proof-of-work is proof that they worked on it. If the CPU power exhibited by the proof-of-work chain is sufficient to crack the password, they can safely attack at the agreed time. The proof-of-work chain is how all the synchronization, distributed database and global view problems you've asked about are solved."* (Champagne, 2014:69).

In conclusion, the fundament of the solution consists of two parts. First, it is random work – guessing of a nonce. Second, selecting the chain that is the most difficult to create.

5.3 Possible jeopardy

In the previous chapter I discussed the process of the blockchain synchronization and its implications. As any other system, neither this one is flawless. Even such a sophisticated and complex machinery as the blockchain has its limits. There are few possible threats.

First one is something called the *51% attack*. This name refers to a situation when majority of the hashing power of the system is fraudulent. In other words the blockchain is capable of solving the BGP as long as the majority of miners, and thus computation power, are "honest", or at least not collaborating. If a node (or a group of nodes) possesses more than 50% [9]of the network, in terms of hashing power, it can produce a *longer* chain than all other nodes combined. Subsequently, it can reverse its own past transactions. The node would simply become a centralized ledger-keeper such as can be found in banks or credit card companies. Though, the node cannot even in this situation spend the bitcoins of other miners, even though it could prevent them from being spent (Antonopoulos, 2014, lecture 2). Nakamoto in this regard explains following in the Cryptography Mailing List:

"Even if a bad guy does overpower the network, it´s not like he´s instantly rich. All he can accomplish is to take back money he himself spent, like bouncing a check. To exploit it, he would have to buy something from a merchant, wait till it ships, then overpower the network and try to take his money back. I don´t think he could make as much money trying to pull a carding scheme like that as he could by generating bitcoins. With a zombie farm that big, he could generate more bitcoins than everyone else combined. The Bitcoin network might

[9] In recent history some mining pools of miners have gained over 40% of the all hashing power in the network. This fact is raising concerns, even though these pools have assured the public that they will decrease their share of the network voluntarily if needed in order to protect confidence and reputation of the system.

actually reduce spam by diverting zombie farms to generating bitcoins instead."(Champagne, 2014:41).

Another concern is connected to its hash – SHA256. Since this hash is used also in the banking industry by various financial institutions, it is likely to be a subject of efforts that pursue break it. If any weakness were discovered in it, the whole industry would be seriously affected. Nakamoto suggested that if this breakdown comes gradually, transition to a new hash would be possible and the software would be programmed accordingly. All users would need to upgrade by that time. Though, he suggests that this is not likely to be the case in our lifetime (Champagne, 2014:157).

Among other possibly problematic issues, even though marginal ones, is for instance that some software flaws will occur. It has already happened when due to the protocol fault, senders were allowed to send invalid transactions. By the time it was discovered, millions of invalid bitcoins had been created. They were also later erased once the flaw was discovered (Champagne, 2014:203). Also, it might conceivably happen that two users would be assigned the same Bitcoin address since they are not meant to be used more than once. However, it is important to distinguish that addresses are not wallets neither accounts. They are just channels through which funds are received. Therefore, if there was a collision, the user client who first encounters the payment sent to the address would spend those money, but not the whole wallet (Champagne, 2014:144). Given this, the losses in this case seem to be acceptable. Finally, there is a danger of a DOS[10] attack or its equivalent such as where an entity sends millions of transactions of small amounts, say 1 satoshi[11], in order to make the network unavailable of its intended users. As Bitcoin´s creator admitted, this kind of danger is for a peer-to-peer network always present. And its probability has been decreased by implementing transaction fees (Champagne, 2014:212).

[10] Denial of Service.

[11] 1 Satoshi = 000000001 BTC

6. Alternative uses of the blockchain

As for now, all important mechanisms and features have been described in the previous chapters. In this chapter I will analyze implications that arise from those. When thinking of Blockchain it is always important to keep in mind that the blockchain as a technology is not connected only to Bitcoin, neither all cryptocurrencies because not all of them are decentralized and using proof-of-work or proof-of-stake algorithms. Another important fact that needs to be considered is that research of the blockchain is just a recently discovered field of constant innovation lead mainly by crypto enthusiasts and young entrepreneurs and technological start-ups. Despite of this, I will lay out some of the conceivable uses of the blockchain.

6.1 Escrow service

Escrow service is commonly used already in various projects[12]. It is defined as a contractual arrangement in which money flows through a third party (in this case a smart contract) that supervises if conditions of the contract are fulfilled Transactions that are built in to the Bitcoin protocol require multiple signatures and can be used by escrow services. For example, there are three keys involved in a transaction. One key is owned by the payer, another one by the payee, and the third one by escrow agent. Usually only two of the keys, the payer and the payee, have to sign the transaction so that the payee can receive the funds. This happens when no disputes need to be solved. However, if there is a conflict between the parties the escrow agent is needed. The agent reviews the dispute, decides in favor either the payer or the payee, and signs the transaction accordingly. How such escrow services would work in Bitcoin Nakamoto describes as follows:

> *"The buyer commits a payment to escrow. The seller receives a transaction with the money in escrow, but he can't spend it until the buyer unlocks it. The buyer can release the payment at any time after that, which could be never. This does not allow the buyer to take the money back, but it does give him the option to burn the money out of spite by never releasing it. The seller has the option to release the money back to the buyer. While this system does not guarantee the parties against loss, it takes the profit out of cheating. If the seller doesn't send the goods, he doesn't get paid. The buyer would still be out the money, but at least the seller has no monetary motivation*

[12] E.g. www.elance.com

> *to stiff him. The buyer can't benefit by failing to pay. He can't get the escrow money back. He can't fail to pay due to lack of funds. The seller can see that the funds are committed to his key and can't be sent to anyone else." (*Champagne, 2014:219).

In this kind of escrow, profit incentives are taken away from a cheater so he cannot win while is still possible for both parties to loose which can be seen as a drawback.

6.2 Meta coins

Meta Coins further extend features of Bitcoin utilizing its existing blockchain while providing some additional functions on the top of it. One of such notable implementations are Zerocoin, that pursues enhancing the privacy of payments within Bitcoin, or Zerocash that is concerned with the fact that Bitcoin is currently less private than bank accounts due to its public ledger. In order to address this, Zerocash developed "zerocoin" which is a separate anonymous currency. It also extends Bitcoin with two new types of transaction. First, *mint transaction* that is used for conversion of existing bitcoins to zerocoins and based on "cryptographic commitment" which is a scheme that permits a party to commit to a certain value or a statement while keeping it unrevealed to any other parties. The party can reveal the committed value later, and this can be verified by third party. The second, *pour transaction* that enables anonymous payments where existing user´s coins create new coins. While doing so the transaction are based on zero-knowledge proofs. This term refers to a feature when a party can prove to another one that some statement is truthful without revealing any other information beyond this fact (Antonopoulos, 2014, lecture 9).

Colored Coins is a highly innovative feature. Colored coins make issuing shares and bonds possible while utilizing Bitcoin´s blockchain. It enables to a group to agree about a certain amount of coins representing another value and potentially use these tokens to transact the value (Antonopoulos, 2014, lecture 9). In other words, the feature enables to the situation where bitcoins represent basically anything, whether it is some other currency such as dollar, gold, or certificate of ownership or even vote in elections, to come true. One bitcoin is divisible into 100 000 000 units and every single unit can be individually programmed and identified, and thus assigned properties. When creating a new color a so called "genesis transaction" that contains specific rules must be created. Consequently, a "transfer transaction" must be created as well in order to be able to send these newly colored coins. This transfer transaction uses "tagging-based coloring" algorithm which brings the advantage of multi-color support. This means that one may send bitcoins of different colors or kinds of asset. (Asia et al, 2014).

Mastercoin enables the existing Bitcoin network to be used as a protocol layer upon which further applications can be built, for example smart contracts which I explain on the next page. Some of its features will be unlock only after they become more stable (Willet et al, 2014).

Counterparty is an open-source meta-coin that uses and extends existing Bitcoin blockchain in order to build a fully decentralized digital currency exchange service. It also pursues support of asset registration. Furthermore, it uses its own currency “XCP” and it enables to overlay Bitcoin transactions with certain characteristics such as encoding of source address, destination address, and asset´s quantity and miners´ fee (Antonopoulos, 2014, lecture 9).

6.3 Attestation and Sidechains

Attestation is a term that refers to the ability of authenticated nodes to monitor behavior of other nodes in the network. Thanks to these, misbehavior can be detected and the vicious nodes can be disconnected from the network, if global consensus is reached. However, this may have another interesting applications since it makes creation of a *decentralized certificate authority* possible. This means that we could replace certificate authorities that we know today. These are usually centralized entities that are authorized to issue and certify ownership of digital certificate which proves ownership of a public-private key pair. By this, a certificate authority – a third trusted party – certifies ownership of a subject to any other party. This practice is commonly used today for example for secure web browsing (Antonopoulos, 2015). However, this all can be soon obsolete since now we have the capacity to build completely decentralized certificate authorities by leveraging the concept of *Decentralized Anonymous Attestation”,* as well as zero-knowledge proof, and the blockchain. Such a system can provide decentralized and trusted notary service (Antonopoulos, 2014, lecture 9). It is not a surprise that there are already such attempts being made, namely *Namecoin* that allows registration of domain names in a completely decentralized manner (Namecoin, 2015). However, this is already much more being developed in this regard. A notable digital notary project is also *Proof of existence*. It serves to certify or prove that a certain document existed at a certain time (ProofOfExistence, 2015).

Sidechains is another very interesting concept with a huge potential that pursues to reshape the ecosystem of digital currencies. It allows for the creation of multi-block chain systems, with Bitcoin serving as the “parent chain”, where assets could be transferred not only to individuals, or addresses but also between one another. This, however, could take years to be implemented (Coindesk, 2014). The authors of the concept argue that if Bitcoin is to succeed the issues of scalability and capability need to be addressed. They find “altcoin” market to be an effective laboratory for new ideas to be developed. Furthermore, an important role in this concept is played by “*SPV (Simplified Payment Verification) proofs*”. It enables to verifiers to check amount of work that was committed to the existence of a special output, and also to determine history due to longer chain principle. The technical underpinning of sidechains is called the *two-way peg,* and it has two models, symmetric and asymmetric one (Back et al, 2014:8). The technological details behind those are not necessary to understand for the purpose of this work.

6.4 Smart contracts and Smart property

Another interesting application are *smart contracts*. Smart contracts are contractual agreements between parties that are implemented using software. It is a computer protocol that verifys, enforces, or facilitates the negotiation of performance of a contract. Unlike a usual contract a smart contract is self-enforced. This feature is feasible due to the software that is monitoring whether specific conditions were met. Taking into account this fact, smart contracts provide inherently a couple of benefits. They automatically enforce equality of all parties involved. Moreover, the possibility of any signatory defaulting on their obligations is eliminated (Antonopoulos, 2014, lecture 9). The term was coined by computer scientist Nick Szabo [13]in 1990´s. As Bitcoin has turned out to be a success, a several proposals have been made that incorporate more sophisticated forms of smart contracts. Among those, one that has procured so far the most is Ethereum which I discuss later but for now is important to note that Ethereum possesses a blockchain similar to Bitcoin´s but has a very sophisticated contracting language that is executed on the blockchain. This feature provides an opportunity for very complex contracts to be created and automatically enforced (Omohundro, 2014:19). Its facility allows insurance contracts, financial exchanges, financial derivatives, and plenty of other kinds of transactions to be defined and conducted.

[13] http://szabo.best.vwh.net/idea.html

Smart property is property whose ownership is controlled via the blockchain, and thus is cryptographically protected and digitally transferable. We could think of a vending machine as a sort of an ancestor for this kind of contract. By the words of its "creator" Nick Szabo:

> *"Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The Lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas."* (Szabo, 1997).

Andreas Antonopoulos in his course further explains:

> "*Much like a vending machine is a low risk automated contract with vendor and the customer, the ownership transference that the blockchain provides, is a dis-intermediated way to enable digital contracts that depend on specific parameters. These could be used to "access control" services and actual property including cars, home keys, etc."* (Antonopoulos, 2014, lecture 9).

Let me demonstrate this on a more understandable example. Assume a car rental company. Each car that the company possesses can be represented by a *colored* coin released by the company. The cars can be configured in a way that they are turned on only if they receive a message signed with the private key that has the colored coin. The company can create a platform, say a smartphone application that enables to anybody to broadcast a message containing the private key, and where the company can trade the colored coins. In such conditions anyone can purchase a coin, and use the car while using the application as a "car key". Once a user does not need the car anymore he can just sell the coin through the platform.

What implies from the above may have far reaching consequences because it dramatically reduces fraud and mediation fees which allows trades, that would otherwise never happened, to take place. Moreover, it allows for instance to loan money between parties that do not trust and know each other since the smart property can be used as collateral. This may have significant consequences in terms of global financial inclusivity as it allows people from non-developed countries access the financial market since they are usually excluded due to lack of organizational infrastructure. Utilization of blockchain-based technologies allow these people to build accessible digital history, earn reputation and subsequently get microfinance through peer-to-peer applications. This may conclude in far more competition on financial markets, and thus make credit cheaper (Hoskinson, 2014). Furthermore, if property is made smart there is much less of trust needed to trade it. Modern organizations and corporations are defined usually by a set of contracts with employees, customers, and investors. If all those could be automated, then "Distributed Autonomous Organizations" (DAO) may be possible. This means that these entities could buy and sell things and make decisions of all kinds such as to hire or fire contractors, without human management. However, there is still a possibility to create an organization run by humans in which decisions can be made by voting on the blockchain. This may be a ground breaking "invention" with a huge impact not only in the field of management, but also in governance as such since many of the current functions of government might be replaced by smart contracts, and thus become more reliable, efficient and cheaper (Omohundro, 2014:20).

6.5 Financial contracts and instruments

Financial Contracts and instruments is another field where cryptocurrencies may leave a tremendous footstep. Since the most of financial instruments are essentially a contracts defined by the set of rules and conditions. Nowadays, markets are regulated by authorities monitoring the compliance of the issuer and user of the contracts to the rules set. As indicated above these authorities could be replaced by mathematic algorithms so called *oracles.* Antonopoulos describes how these can be used on the following simple example:

> *"Alice and bob want to play rock, paper, scissors and the winner of three games wins a bet of 1mBTC. In this case oracle can:*
>
> - *Hold both their funds in escrow until a winner is determined*
> - *Make sure that both players do not know what choice the others player commits to before they commit their own*
> - *Have a rule set that determines that rock beats scissors, paper beats rock, and scissors beat paper*
> - *Keep account of the winner of each game until someone wins three times*
> - *Pay out the full sum to the final winner of three games.*

> *All these can be done objectively, transparently and without trust between Alice and Bob. The same can take place for more complicated financial instruments which rely on various external conditions."* (Antonopoulos, 2014, lecture 9).

Such external conditions, of course, need to be quantified and digitized. There are already a few ongoing projects that pursue to build sophisticated systems that would allow creation of complex contracts. One of those is Orisi which is a distributed oracles system for cryptocurrency contracts. The creators of the project suggest that an oracle might be subjected to similar drawbacks as a central authority does. It may be hacked, or bribed to deliver faulty results. Therefore, one oracle is replaced by a whole set of them. They need to reach consensus in order to finalize a transaction. Given this, it is costly to bribe more than half of them and also the risk of oracles being hacked is minimized due to the variety of oracle hosting providers. Moreover, the software will become secure over time with growing base of users (Lewis, 2014).

6.6 Political Speech and Ethereum

Political speech is another area where consequences of using a blockchain might be visible. Projects such as BitCongress have come with an idea of implementing a blockchain-based decentralized voting system. While doing so the projects is based on two technologies, Votecoin which is supposed to be a token that is equivalent to votes within system that is based on Ethereum (Rockwel, 2014:3).

Ethereum seems to be very promising project so far. This hybrid altcoin [14] attempts to build a revolutionary new platform for applications that would target large scale of areas from voting to financial exchanges, to smart property and decentralized autonomous organizations.[15] It pursues to provide a standardized platform, a coding language to facilitate the creation of distributed applications by anybody. It also build its own currency – the ether with certain sub denominations that are used for paying transaction fees. More importantly, Ethereum is based on the concept of self-executing smart contract. Some experts argue that the project is too ambitious since it wants to even upgrade the Bitcoin´s blockchain and reach the level of

[14] Using combined proof-of-work and proof-of-stake schemes.

[15] Decentralized organization is an organization managed, instead of a hierarchical structure, by a set of humans interacting in person and controlling property via the legal system. It involves a set of humans interacting with each other according to a protocol specified in code, and enforced on the blockchain.

Turing completeness[16]. The founder of Ethereum, Vitalik Buterin, in his White Paper explains why Ethereum is engaged in such an effort:

> *"... in general, there are two approaches toward building a consensus protocol: building an independent network, and building a protocol on top of Bitcoin. The former approach, while reasonably successful in the case of applications like Namecoin, is difficult to implement; each individual implementation needs to bootstrap an independent blockchain, as well as building and testing all of the necessary state transition and networking code. Additionally, we predict that the set of applications for decentralized consensus technology will follow a power law distribution where the vast majority of applications would be too small to warrant their own blockchain, and we note that there exist large classes of decentralized applications, particularly decentralized autonomous organizations, that need to interact with each other.*
>
> *The Bitcoin based approach, on the other hand, has the flaw that it does not inherit the simplified payment verification features of Bitcoin. SPV works for Bitcoin because it can use blockchain depth as a proxy for validity; at some point, once the ancestors of a transaction go far enough back, it is safe to say that they were legitimately part of the state. Blockchain-based meta-protocols, on the other hand cannot force the blockchain not to include transactions that are not valid within the context of their own protocols. Hence, a fully secure SPV meta-protocol would need to backward scan all the way to the beginning of the Bitcoin blockchain to determine whether or not certain transactions are valid. Currently, all "light" implementations of Bitcoin-based meta-protocols rely on a trusted server to provide the data, arguably a highly suboptimal result especially when one of the primary purpose of a cryptocurrency is to eliminate the need for trust."* (Buterin, 2014:11).

[16] Being computationally universal

7. “Disruptive” Substitution Technology

In the previous chapter I analyzed the latest cryptocurrencies and blockchain-based technologies. Moreover, I have proven that this technology might be utilized in countless areas. Despite of its young age, latest visions made by experts suggest that it may change the whole basis upon which majority of both public and private records are operated. This *grand* change may be in regard to voter records, court records and criminal records as well as land titles, certifications, and even wills and trusts. In the following chapter I will make a synthesis of the aforementioned facts upon which I will conclude findings and lay out possibilities how these technologies may prove to be “disruptive” in selected areas.

7.1 Central cadaster, company register

From what stated above, the most obvious consequences are implying for any kind of register administrated by a central authority. I am going to show how the blockchain can prove its usefulness on example of a central cadaster and company register. As both the central cadaster and company register essentially assign a piece of information to an entity, they could make use of the blockchain technology to achieve better transparency, redundancy and manageability.

By leveraging the public ledger aspect of blockchain the cadastral and registry data becomes more transparent, auditable, and open. This in turn allows software engineers to develop better tools for browsing and analyzing the data. Yet another advantage is that the data can be used for legal purposes directly, without the need for additional overhead of having it certified by a notary or a governmental body (ÚGKK SR, 2015). This is made possible by the tamper-proof nature of the blockchain.

Redundancy of cadastral and company registry data would be achieved by the fact that the whole blockchain network stores it in a tamper-proof form - as special transactions on the public ledger. The storage requirements for the network can be reduced dramatically by employing techniques such as proof of existence and distributing the data itself via other, but still accessible means such as a downloadable archive on a web page and so on[17].

Since the information in both the central cadaster and company register is changing quite often and the blockchain does not allow any changes to the transaction data stored within,

[17] Possibly provided by services such as already mentioned proofofexistnece.com.

some sort of scheme needs to be devised to manage the data. The requirements for such a scheme are:

a) an ability to invalidate old records, so that if anyone requests an invalidated record by its identification number (a transaction ID in the blockchain parlance) they must also receive a warning stating the data is out-of-date,
b) and some means of publishing the identifiers of up-to-date documents

The first requirement can be satisfied by using Colored Coins protocol, since it further extends the properties of Bitcoin. It is essentially an ownership token represented by a unit of currency on the blockchain ledger and can always be traced from its inception to the current owner address and also the other way around. As I discussed already earlier these tokens can be used to represent basically anything. One could realize an IPO (Initial Public Offer) by issuing shares as colored coins, or simply store his house on the blockchain by issuing a single coin that would represent the ownership of the house, and thus the proprietary could be transferred with a simple Bitcoin transaction (Buterin, 2014:11).

The procedure of changing a record generates a new record on the blockchain (e.g. in the form of an address containing a transaction representing the record data itself) and then moving the colored coin from the old record's blockchain address to the new one. This way anyone with an up-to-date version of the blockchain can see that the invalidated record does not contain the token and can also follow said token to its new destination, thus also fulfilling the second requirement. The new identifiers can additionally be published on the website of the appropriate governmental body, but the colored coin token identifier will suffice to reliably reconstruct the whole change log of given record. This way of asset registration would be much easier and more transparent than it is in the current system (Antonopoulos, 2014, lecture 9).

7.2 Government procurement

Another way Bitcoin-based technology can improve government services, regardless of its current level of quality, which of course differs from one country to another is *public procurement.* Government procurement usually includes all public works, services and supply contracts made by a public authority (McCurden, 2007:121). Public tenders organized by governmental bodies can be made more transparent, automated and self-enforcing by using

Smart or Distributed Contracts to manage the whole process. With these contracts, transparency is achieved by the fact that the contract is made public and every single offer is forever recorded in the blockchain. This way everyone can verify whether the best offer was selected. However, there is no need to publicly disclose the identities of all participants if not desired -- all the offers can be pseudonymous as the blockchain key pairs/addresses do not have to have a real-world identity associated to them. Still, any of the participants (e.g. the winner) can provide a verifiable proof linking the pseudonym with their real-world identity in the form of a digital signature.

The automation level of the procurement procedure can be increased by the use of scripting abilities of the blockchain transactions, possibly in conjunction with oracles which can measure arbitrary real-world conditions (Earlytemple, 2015). This means for example that a public tender smart contract can automatically select an offer with the lowest cost after a predetermined time window for making offers. This could be followed by another smart contract to enforce the proper completion of the task. This contract will wait for the task to be fulfilled by the contractor while holding the reward in escrow. After an oracle confirms that the task has been completed successfully, the reward is automatically released from *escrow* and transferred to the contractor. In case the contractor fails to fulfill the contract the reward will be returned back to the organizer.

7.3 Government money

For the purpose of this thesis I won´t discuss the origin of money, neither analyze the current monetary system and fiat money because this has been subject of many studies for decades. In this chapter I will point out some ways that cryptocurrencies may challenge fiat money. Using a crypto currency as a legal tender offers numerous advantages to both the government and citizens, as well as a few potential issues. One of the major advantages, should the government decide to implement it, is the ability to limit the money supply. This could potentially result in exceptional increase of the people’s trust in the currency and make it more competitive on the foreign exchange market. Bitcoin, for example, has a finite supply of 21 million coins that can ever be created, governed by an immutable decreasing supply algorithm out of which over 14 million have been created so far, in April 2015 (Blockchain, 2015).

Another improvement over a traditional fiat currency is that the money cannot be counterfeit or duplicated in any way. The main threat remaining, described in the chapter dedicated to the 51% attack, requires considerable resources to be expended by the attacker and is easily mitigated by waiting for transaction to be “confirmed” by multiple consecutive “blocks” in the blockchain (e.g. you can sell a cup of coffee instantly without waiting for a confirmation, but wait 6 confirmations when selling a house), so as such is not feasible. Still, there is a choice remaining whether to allow citizens to use the government crypto currency pseudonymously or require each address to be associated with a specific body. Both options are feasible, should the currency be distributed by a central authority initially controlling all the coins. Requiring an identity to be attached to each address is analogous to having a bank account, while a pseudonymous usage is similar to cash. However, having all transactions essentially public (and potentially directly tied to real-world identities) can be a major drawback. While it can be regarded as a full transparency in regards to government spending, it would also affect every other party using the currency.

Data mining, for example, could have devastating results when employed by an entity having access to the address-identity mapping (and this could be potentially everyone). To illustrate this say a woman goes to a pharmacy to buy a pregnancy test and pay using a crypto currency. This transaction is now part of a public ledger. Now everyone knowing the real-world identities behind both the sending and receiving address can draw the inference that you bought *something* in a particular pharmacy. Coupled with the knowledge about all the prices in the pharmacy, it is quite probable that they will also be able to conclude which exact item you bought. Other than one´s health status and shopping habits, it would also be possible to track and predict one´s physical movement, similarly to common ATM withdrawal tracking featured in countless movies. This has serious privacy implications and is best avoided by not tying a real-world identity to a crypto currency address. Even though there might not be an identity-address mapping directly available to anyone (including the government), it’s still extraordinarily hard to keep one’s wallet (a collection of addresses) pseudonymous. There are already tools[18] publicly available to compute a transitive closure over all the transactions contained in the block chain with the purpose of clustering addresses into a set of wallets, each controlled by single entity (person, company, etc.). This in turn makes it much easier to

[18] Can be found here https://github.com/znort987/blockparser

completely de-pseudonymize the whole wallet given only one “mistake” on the part of the user (Champagne, 2014:118).

Furthermore, laundering crypto coins is not that easy, either. This is because every single coin can be tracked back to its inception via the transactions stored publicly in the block chain, so “just” breaking out of the transitive closure still does not mean one is anonymous (Cryptocoinsnews, 2015). There are various methods[19] being used that leverage either transaction metadata (e.g. time stamps or an IP address of Bitcoin node a particular transaction went through first) or bad anonymity practices, respectively.

7.4 Revenue service and Customs office

Assuming the universal use of a government-issued crypto currency, it would be trivial for the government to make a much better estimate of how much revenue tax it should receive. Also, the government would be able to identify merchants and other entities not paying their taxes in full by analyzing all the transactions stored in the block chain. Consequently, it would also be possible to pinpoint entities conducting business in other forms of currency (e.g. gold or other crypto-currency) by estimating their real revenue, given operational expenses as a baseline. If, however, we assume that the government-issued crypto currency is not generally used for buying goods/services (normal cash being used here) and serves only as the current bank system, then the above is no longer valid and the old, quite ineffective methods for estimation and auditing related to revenue tax would have to be used. Using crypto currency for import and export duties does not seem to provide any additional benefits, aside from those inherent to the use of such currencies.

7.5 Smart money

Finally I will conclude with, assumingly, the most astonishing feature that is connected to wide-spread usage of cryptocurrencies – smart money. Protocols such as Colored Coins could enable us to make our currencies smarter and simply automatize cash and money flows in economy. It allows us to designate certain coins to be spent for certain services for example create allowance, even in dollars or euros, which can be only used to pay healthcare at certified parties. Moreover, doing so would not require having some bureaucratic body to supervise this process. All these rules can be simply programmed into the money. It is

[19] More on this here https://crypto.stanford.edu/seclab/sem-14-15/pustogarov.html

possible even to program units in such a way that they would automatically return to the provider, if a condition, such as if the receiver does not spend the money after certain amount of time, is unfulfilled.

Even more amazingly, in a similar way a company may keep its spending under control, and simply program its budget for any kind of expenditures e.g. salaries, materials and maintenance, etc. Such a specification restrains the money from being spent otherwise. Moreover, automatizing such processes may lead to tremendous decrease of bureaucracy that could save resources also in terms of human energy since it would decrease dramatically the burden that lays on the shoulder of accountants and controllers. It is reasonable to assume that it may save a large amount of time to the organizations as well.

As indicated above, the open-source and programmable character of most of the cryptocurrencies allows us to rebuild our financial sector, and administrative processes from scratch and keep coming with new innovative solutions at very high pace.

Conclusion

Historically we have been surrounded by various organizations, financial institutions, or government agencies that have been based on centralized systems. This was for a good reason. Any kind of information or resources possessed by these entities needed to be administrated by some certain authority that was trustworthy and credible. These entities usually, due to the centralized character of the system, represent single point of access. Given this, they are necessarily exposed to conceivable risk of corruption, manipulation, censorship, or technical failures. Centralized systems thus inherently retain their weaknesses.

On the other hand, for a long time creation of decentralized systems had been technologically infeasible. This is because such a system inherently lacks any kind of hierarchy, and thus also the authority that supervises the whole system, and provides its trustworthiness. However, nowadays we have technologies available that eliminate the need of trust in such systems by state of the art mathematical algorithms.

Cryptography, due to recent rise of the crypto currencies, allows us to build purely decentralized systems and networks where zero trust is needed, the possibility of fraud and malicious manipulation is reduced, and so are the mediation fees. This, in its consequences, may foster trade across the world since it allows trading people that don´t need to trust each other, and who would not have done it otherwise. Moreover, since majority of organizations are defined by set of various contracts, and all these can be made smart and automated, the utilization of the blockchain may bring far-reaching consequences in the field of economics and governance.

However, this is only the beginning. This technology is disruptive and breaks the status quo. It opens markets and breaks the positions of middlemen of the time. Bitcoin and other cryptocurrencies may cause the paradigm shift in miscellaneous areas since they create a platform for, constructive, critical and open discussion as well as for endless exploration and innovation of the blockchain.

References

ANTONOPOULOS, Andreas. *Introduction to Digital Currencies MOOC 2.0.* University of Nicosia, 2014. Accessible at: http://mooc.universityofnicosia-online.com/ (Retrieved: 20/04/2015).

ANTONOPOULOS, Andreas. *The potential of Blockchain Technology.* Youtube. Accessible at: https://www.youtube.com/watch?v=r8JopZWlvtw (Retrieved: 20/04/2015).

ASSIA, Yoni, VITALIK Buterin, Lior HAKIM, Meni ROSENFELD, 2014: Colored Coins Whitepaper. Bitcoin X. Online at: https://tinyurl.com/coloredcoinwhitepaper (Retrieved: 20/04/2015).

BACK, Adam. *Enabling Blockchain Innovation with Pegged Sidechains.* 2014. Accessible at: http://www.blockstream.com/sidechains.pdf (Retrieved: 20/04/2015).

BITCOIN WIKI, 2015. *Proof of Work.* Accessible at: https://en.bitcoin.it/wiki/Proof_of_work (Retrieved: 20/04/2015).

BLOCKCHAIN, 2015: B*lockchain.* Accessible at*:* https://blockchain.info/charts/total-bitcoins (Retrieved: 20/04/2015).

BONEH, Dan. *Cryptography I.* Stanford University, 2015. Accessible at: https://www.coursera.org/course/crypto (Retrieved: 20/04/2015).

BRITO, Jerry and Andrea CASTILLO. *Bitcoin a Primer for Policymakers*. Mercatus Center at George Mason University, 2013.

BUSINESS DICTIONARY, 2015: *Ledger.* Accessible at: http://www.businessdictionary.com/definition/ledger.html (Retrieved: 20/04/2015).

BUTERIN, Vitalik. *Ethereum White Paper*. 2014. Accessible at: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf (Retrieved: 20/04/2015).

COINDESK, 2015: *Sidechains White Paper.* Accessible at: http://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/ (Retrieved: 20/04/2015).

COMBS, Brett and Tom MITSOFF. *Bitcoin decoded*. San Bernandino, CA: Propellerhead Marketing Group, c2014, 86 s. ISBN 978-061-5955-247

EARYLTEMPLE, 2015: *Earlytemple.* Accessible at: https://earlytemple.com:8181/index.jsp#protocol (Retrieved: 20/04/2015).

ECKERSLEY, Peter. *Virtual Markets for Virtual Goods: The Mirror Image Of Digital Copyright?* Harward Journal of Law & Technology Vol. 18, Number 1, p. 86–118, 2004.

GUTTMAN, Benjamin. *The Bitcoin Bible.* Books on Demand, 2014. ISBN 978-3-7322-9696-5

HAMACHER, Kay and KATZENBEISSER Stefan. *Bitcoin – An analysis (28C3).* Youtube. Accessible at: https://www.youtube.com/watch?v=-FaQNPCqG58 Retrieved on 15. February 2015.

HOSKINSON, Charles. *The Future Will Be Decentralized.* 2014. TEDx. Accessible at: https://www.youtube.com/watch?v=97ufCT6lQcY (Retrieved: 20/04/2015).

CHAMPAGNE, Phil. *The Books of Satoshi: The collected Writings of Bitcoin Creator Satoshi Nakamoto.* E53 Publishing LLC, 372 p. 2014. ISBN 978-0-9960613-1-5

LAMPORT, Leslie and SHOSTAK, Robert and MARSHALL, Pease. *The Byzantine Generals Problem.* Journal ACM Transactions on Programming Languages and Systems (TOPLAS) Vol. 4 Issue 3 s. 382-401, 1982.

LEWIS, Antony. *Orisi White Paper.* 2014. Github. Accessible at: https://github.com/orisi/wiki/wiki/Orisi-White-Paper (Retrieved: 20/04/2015).

MCCRUDDEN, Christopher. *Buying social justice: equality, government procurement, and legal change*. New York: Oxford University Press, 2007, li, 680 p. ISBN 978-019-9232-437.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008 Accessible at: https://bitcoin.org/bitcoin.pdf. (Retrieved: 20/04/2015).

NAMECOIN, 2015: *Namecoin.* Accessible at: http://namecoin.info/ (Retrieved: 20/04/2015).

NARAYANAN, Arvind and BONNEAU, Joseph and FELTEN, Edward. *BTC-Tech: Bitcoin and Cryptocurrency Technologies.* Princeton University, 2015. Accessible at: https://piazza.com/princeton/spring2015/btctech/home (Retrieved: 20/04/2015).

OMOHUNDRO, Steve. *Cryptocurrencies, smart contracts, and artifical intelligence.* AI Matters Vol. 1, Issue 2 p.19-21, 2014. Accessible at: http://dl.acm.org/citation.cfm?id=2685334 (Retrieved: 20/04/2015).

ROCKWEL, Morgan. *BitCongress White Paper.* 2014. BitCongress. Accessible at: http://bitcongress.org/BitCongressWhitepaper.pdf (Retrieved: 20/04/2015).

SZABO,Nick. *The Idea of Smart Contract.* 1997. Accessible at: http://szabo.best.vwh.net/smart_contracts_idea.html. (Retrieved: 20/04/2015).

ÚGKK SR, 2015. Úrad geodézie, kartografie a katastra Slovenskej republiky. Question: *"Can I use ownership document printed from the Cadastral Portal for legal purposes?"* Accessible at: http://www.katasterportal.sk/kapor/faq.do (Retrieved: 20/04/2015).

WILLET, J.R., Maran HIDSKES, David JOHNSTON, Ron GROSS, Marv SCHNEIDER, 2014: The Master: Protocol/Mastercoin Complete Specification. Github. Acessible at: https://github.com/mastercoinMSC/spec (Retrieved: 20/04/2015).

List of tables and figures

Figure 1: Lieutenant 2 a traitor ……………………………………………………….….. 14

Figure 2: The commander a traitor …………………………………………………..... 14

Figure 3: Algorithm OM (1), Lieutenant 3 a traitor; and the Commander a traitor …. 16

List of abbreviations

BGP – Byzantine Generals Problem

DOS – Denial of Service

DAO – Decentralized Autonomous Organization

ECDSA – Elliptic Curve Digital Signature Algorithm

IPO- Initial Public Offering

MOOC – Massive Online Open Courses

SPV – Simplified Payment Verification