

University of Pardubice
Faculty of Economics and Administration

Blockchain as modern information technology

Serhii Teslenko

Bachelor's Thesis

2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Serhii Teslenko**
Osobní číslo: **E150044**
Studijní program: **B6209 Systémové inženýrství a informatika**
Studijní obor: **Regionální a informační management**
Název tématu: **Blockchain as modern information technology**
Zadávající katedra: **Ústav systémového inženýrství a informatiky**

Z á s a d y p r o v y p r a c o v á n í :

The aim of work is explain and highlight existing features of Blockchain technology. Estimate the prospects and threats. As a practical part of work will be analyzing possibility of transition to Blockchain in public institutions and markets. Social survey for different age people towards blockchain economy and their forecasts will be analyzed.

Outline:

- The Concept of Blockchain technology
- Initial Coin Offering as an innovative crowdfunding model
- Smart contract
- The most significant crypto currency projects
- Regulation of cryptocurrency in the world
- Blockchain as a potential technology for modern markets of economy

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca. 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Jazyk zpracování bakalářské práce: **Angličtina**

Seznam odborné literatury:

Svetski, A. (2018). Homo Sapiens, Evolution, Money & Bitcoin. Hackernoon [online]. 1-24. Available from: <https://hackernoon.com/homo-sapiens-evolution-money-bitcoin-33f69701de>


Malekan, O. (2018) The Story of the Blockchain: A Beginner's Guide to the Technology That Nobody Understands. New York, U.S.: Triple Smoke Stack.

Narayanan, A., Bonneau, J., Felton, E., Miller, A., Goldfeder, S. (2016) Bitcoin and Cryptocurrency Technologies. Princeton, U.S.: Princeton University Press

Lipsey, R., Carlaw, K., Bekhar C. (2005). Economic Transformations. Oxford University. Press: Oxford

Williamson, O. (1979) 'Transaction cost economics: the governance of contractual relations' Journal of Law and Economics 22(2): 23361.

Vedoucí bakalářské práce:


Ing. Martin Ibl, Ph.D.


Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**


doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.


doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl/a jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2019

Serhii Teslenko

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor Mr. Ing. Martin Ibl Ph.D. for his unwavering support, patience and valuable instructions he gave me while I was writing the thesis. Additionally, I am very thankful for continuous support and advices of my family.

ANNOTATION

This thesis focuses on Blockchain technology and its applications. The main part reveals the potential of Blockchain to improve processes in modern markets by providing increased efficiency, transparency and security. The objective of this thesis is to define the concept of Blockchain, describe its applications, analyze use cases and prevalence of the technology, and define reasons for the general public interest.

KEYWORDS

Blockchain, Cryptocurrency, Bitcoin, Smart contract, Initial Coin Offering

NÁZEV

Blockchain jako moderní informační technologie

ANOTACE

Tato práce se zaměřuje na technologii Blockchain a jeho aplikaci. Hlavní část odhaluje potenciál Blockchainu pro účely zlepšování procesy na moderních trzích zvyšováním efektivity, transparentnosti a bezpečnosti. Cílem této práce je definovat pojem Blockchain, popsat aplikaci, analyzovat případy užití a obecné rozšíření technologie a definovat důvody zájmu veřejnosti.

KLÍČOVÁ SLOVA

Blockchain, kryptoměna, Bitcoin, chytrý kontrakt, Initial Coin Offering

CONTENTS

| | |
|---|-----------|
| INTRODUCTION..... | 10 |
| 1 THE CONCEPT OF BLOCKCHAIN TECHNOLOGY..... | 12 |
| 1.1 CONSENSUS MECHANISMS..... | 13 |
| 1.1.1 Proof of work (PoW)..... | 14 |
| 1.1.2 Proof of stake (PoS)..... | 14 |
| 1.1.3 Delegated Proof of Stake (DPoS)..... | 15 |
| 1.1.4 Proof of Elapsed Time (PoET)..... | 16 |
| 1.2 TYPES OF BLOCKCHAIN | 17 |
| 1.2.1 Public blockchains..... | 17 |
| 1.2.2 Private blockchains..... | 18 |
| 1.3 THE POTENTIAL DANGER FOR BLOCKCHAIN | 18 |
| 1.3.1 The 51% Attack..... | 18 |
| 1.3.2 Identity theft..... | 19 |
| 1.3.3 Illegal activities..... | 19 |
| 1.3.4 System hacking..... | 19 |
| 2 THE MOST SIGNIFICANT CRYPTOCURRENCY PROJECTS..... | 21 |
| 2.1 BITCOIN..... | 22 |
| 2.1.1 Bitcoin Blockchain Architecture..... | 23 |
| 2.1.2 Transaction legitimacy..... | 24 |
| 2.1.3 Monetary policy of Bitcoin..... | 25 |
| 2.2 ETHEREUM..... | 26 |
| 2.2.1 Ethereum Blockchain Architecture..... | 26 |
| 2.3 RIPPLE..... | 27 |
| 3 REGULATION OF CRYPTOCURRENCY IN THE WORLD | 29 |
| 3.1 UNITED STATES OF AMERICA..... | 29 |
| 3.2 CHINA..... | 30 |
| 3.3 EU..... | 30 |
| 3.4 SWITZERLAND..... | 30 |
| 4 OTHER SIGNIFICANT BLOCKCHAIN APPLICATIONS | 32 |
| 4.1 SMART CONTRACT..... | 32 |
| 4.1.1 Smart Contracts Use Cases..... | 34 |
| 4.1.2 The danger for smart contracts – The Oracle Protocol..... | 35 |
| 4.2 INITIAL COIN OFFERING AS AN INNOVATIVE CROWDFUNDING MODEL | 36 |
| 4.2.1 The Blockchain takes the concept of investment further..... | 36 |
| 4.2.2 Types of Token..... | 38 |
| 5 BLOCKCHAIN AS A POTENTIAL TECHNOLOGY FOR MODERN MARKETS OF ECONOMY | 40 |
| 5.1 POTENTIAL USES OF BLOCKCHAIN TECHNOLOGY APPLYING TO PUBLIC SECTOR ORGANIZATIONS AND MARKETS..... | 40 |
| 5.1.1 Banking..... | 40 |
| 5.1.2 Land title registration..... | 41 |
| 5.1.3 Voting..... | 41 |
| 5.1.4 Healthcare..... | 42 |
| 5.2 CONDITIONS FOR BLOCKCHAIN SUCCESS | 42 |
| 6 PUBLIC PERCEPTION OF BLOCKCHAIN TECHNOLOGIES | 44 |
| 6.1 ANALYSIS OF SOCIAL SURVEY TOWARDS BLOCKCHAIN | 44 |
| 6.2 ANALYSIS OF CRYPTOCURRENCY TREND..... | 47 |
| CONCLUSION..... | 49 |
| BIBLIOGRAPHY | 50 |

LIST OF FIGURES

| | |
|---|----|
| Figure 1: Centralized and decentralized networks architecture..... | 12 |
| Figure 2: Insight of Blockchain..... | 13 |
| Figure 3: Bitcoin Blockchain transaction flow..... | 22 |
| Figure 4: Blocks chaining..... | 24 |
| Figure 5: Patricia tree..... | 27 |
| Figure 6: The most significant cryptocurrencies projects events timeline..... | 28 |
| Figure 7: Structure of smart contract..... | 33 |
| Figure 8: Smart contracts benefits..... | 33 |
| Figure 9: Total funding raised by Blockchain Initial Coin Offerings (ICO) worldwide..... | 37 |
| Figure 10: Gender of survey participants..... | 44 |
| Figure 11: Age of respondents..... | 45 |
| Figure 12: Blockchain technology prevalence..... | 45 |
| Figure 13: Well-known applications for future users of Blockchain based technologies..... | 46 |
| Figure 14: Cryptocurrency trend..... | 47 |
| Figure 15: Bitcoin Price Index..... | 47 |
| Figure 16: Correlation between Cryptocurrency trend and Bitcoin Price Index..... | 48 |

LIST OF TABLES

| | |
|--|----|
| Table 1: Comparison of consensus mechanisms..... | 17 |
|--|----|

LIST OF ABBREVIATIONS

| | |
|-------|---|
| B2B | Business to business |
| B2C | Business to customer |
| CEO | Chief executive officer |
| DAO | Decentralized Autonomous Organization |
| Dapps | Decentralized applications |
| DPoS | Delegated proof of stake |
| ECB | European Central Bank |
| EU | European Union |
| EVM | Ethereum Virtual Machine |
| FBI | Federal Bureau of Investigation |
| ICO | Initial Coin Offering |
| IPO | Initial Public Offering |
| PoET | Proof of elapsed time |
| PoS | Proof of stake |
| PoW | Proof of work |
| P2P | Peer-to-peer |
| STO | Security Token Offering |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| VAT | Value added tax |

INTRODUCTION

Blockchain is an incorruptible digital ledger of economic transactions that can record everything of value. The technology was firstly proposed under nickname Satoshi Nakamoto as the underlying technology of the Bitcoin cryptocurrency. However, the areas of technology implementation are not limited only to financial services.

Blockchain is a new technology, which has a huge potential to improve processes in both public and private sectors of the economy by providing greater transparency, enhanced security and increased efficiency and speed of transactions. Comparing to the client-server model, data in the Blockchain are stored across a peer-to-peer network in a distributed form on many different devices. Distributed ledger Blockchain relies on specific consensus protocols that allow users to transfer value between themselves without the need to trust each other or any central authority. Using public-private key cryptography, users can sign transactions that transfer ownership to other users.

The objective of this thesis is to define the concept of Blockchain, describe its applications, analyze use cases and prevalence of the technology, and define reasons for the general public interest. The aim of work is also to determine the directions where Blockchain technology can bring benefits and design favorable conditions for Blockchain adoption.

This work serves for students and other readers to understand what the Blockchain is, where it can be implemented and how it can help to improve the functionality of modern markets and public institutions.

The structure organized as follows. Chapter 1 reveals the features of Blockchain technology, discover various consensus mechanisms and explains the difference between public and private blockchains. The Chapter ends with an analysis of potential danger for Blockchain. Chapter 2 deals with the most significant cryptocurrency projects such as Bitcoin, Ethereum and Ripple. In this part, the specific blockchains are described on the example of certain cryptocurrencies. In the end, the timeline of cryptocurrency projects appearance is provided. Chapter 3 is a brief overview of the opportunities and limitations of cryptocurrencies in selected regions (the priority is given to areas that have succeeded the most in innovation research). Chapter 4 is devoted to two other meaningful Blockchain applications and split into 2 parts. The first part of this Chapter reveals the properties of smart contract and its advantages. Furthermore, for better understanding Blockchain based smart contracts, the use cases and possible dangers are designed. The second part deals with modern types of investment and raising capital that

Blockchain technology makes possible. Besides, different types of tokens (digital assets built on an existing Blockchain) are explained. In Chapter 5, I design the potential directions where Blockchain based applications can be used to improve the functionality of the Public Institutions and Markets, and suggest conditions necessary for Blockchain success. In the end, in Chapter 6, I analyze the attitude of people towards Blockchain and its applications. Moreover, the second part of Chapter 6 deals with the analysis of cryptocurrency trend and shows the reason for the general public interest.

1 THE CONCEPT OF BLOCKCHAIN TECHNOLOGY

Blockchain was anonymously invented and publicly released (under the nickname Satoshi Nakamoto) as the technology underlying Bitcoin (see more in Chapter 2) – the first digital currency that solves the double-spending problem without the need of central authority.

Blockchain is the very first implementation of triple entry accounting, where we have an asset being recorded on the ledger in the context of a transaction. The third entry and triple entry accounting is cryptography, where we have a cryptographic account of the transaction that stored permanently and immutably on the ledger. A ledger is a collection of transactions. Assets are part of a transaction, but the ledger records the transaction. (The Linux Foundation, 2018) The ledger is distributed - no single copy of the ledger exists. In other words, it's decentralized - there is no single owner or controller of the data. Thus, Blockchain is digital decentralized ledger that store information about transactions.



Figure 1: Centralized and decentralized networks architecture

Source: (Osetskyi, 2018)

In the Blockchain, the differentiator is that no one owns the ledger, or all the participants own the ledger at the same time. Simply put, every user that decides to join and participate in the process of maintaining a Blockchain network keeps an electronic copy of the Blockchain data, which is frequently updated with all the latest transactions, in synchrony to the other user's copies. This is important because it makes difficult for anyone to take down the network or corrupt it.

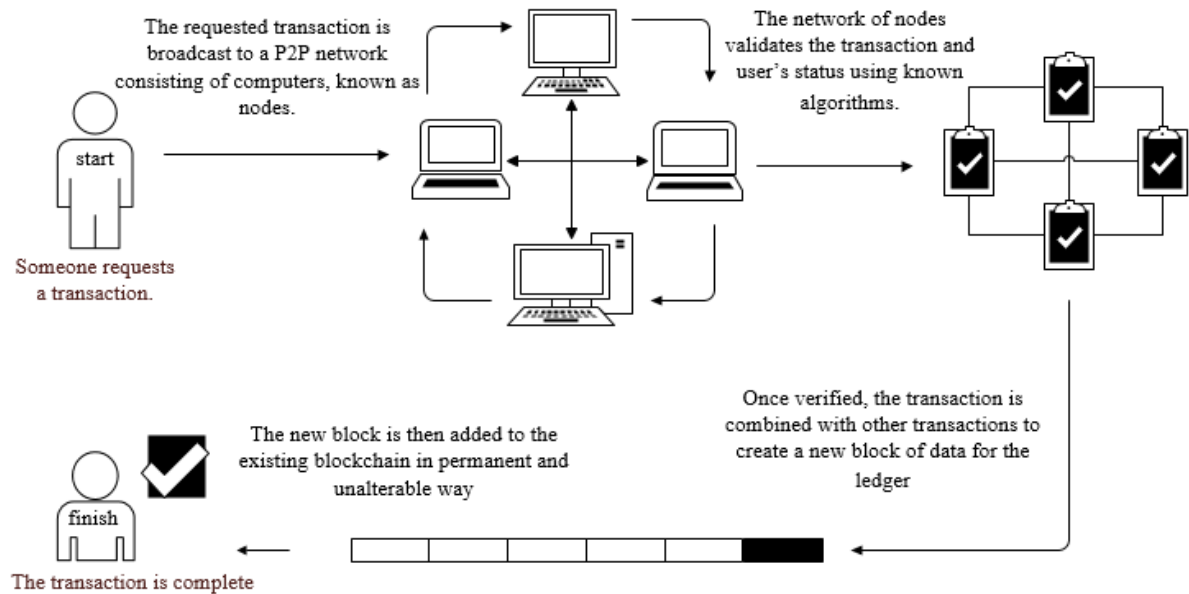


Figure 2: Insight of Blockchain

Source: own processing

“The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.” (Tapscott, 2016)

In simple words, the Blockchain is a time-stamped series of an immutable record of data that is managed by a cluster of computers not owned by any single entity (see figure 2). Each of these blocks of data is secured and bound to each other using cryptographic principles. (What is Blockchain Technology? A Step-by-Step Guide For Beginners, 2019) The technological novelty of Blockchain consists in the possibility to create consensus about the true state of a ledger that might record for instance exchanges, contracts, ownership, identity, data.

1.1 Consensus mechanisms

Most blockchains have a lot of things in common and function in similar ways, but one of the ways in which blockchains can be unique is the way consensus is reached. In short, consensus mechanisms are protocols that make sure all nodes (devices that maintain the Blockchain) are synchronized with each other and agree on which transactions are legitimate and must be added to the Blockchain. These consensus mechanisms are crucial for a Blockchain in order to function correctly. They make sure if everyone uses the same Blockchain. Everyone can submit things to be added to the Blockchain, so it's necessary that all transactions are constantly checked and the Blockchain is constantly audited by all nodes. Without a good consensus mechanism, blockchains are at risk of various attacks. (Blockgenic, 2018)

There are many different consensus mechanisms have appeared to this day, so we'll jump right into the most popular ones.

1.1.1 Proof of work (PoW)

Proof of Work (PoW) is the first Blockchain consensus mechanism and was first used by Bitcoin (see more in Chapter 2). Many cryptocurrencies have followed Bitcoin's example and have also adopted this consensus mechanism. The Proof of Work process is known as mining and the nodes are known as miners. Miners solve complex mathematical puzzles which require a lot of computational power. The first one to solve the puzzle gets the right to create a block and receives a reward for creating a block.

These mathematical puzzles have some interesting properties. First of all, they are asymmetric, meaning it takes a lot of time to find the answer, yet it's easy to verify if an answer is correct. Secondly, the only way to solve these puzzles is to 'guess' the answer. It is not possible to solve the puzzles quicker using any other method than trial and error. This also means that if someone wanted to find the solution to the puzzle faster, he would need more computational power, which can get very costly. Lastly, the difficulty of these puzzles' changes depending on how fast blocks are mined. To maintain a consistent supply of new coins, blocks must be created within a certain time frame. If blocks are created too fast, the puzzles get harder. This process ensures that to be able to create a block, you will need a lot of computational to solve the puzzle first. (Blockgenic, 2018)

There is a major drawback to this consensus mechanism though. Proof of Work uses a lot of resources (such electricity) and it's considered unsustainable in the future, therefore some blockchains are moving to other consensus mechanisms.

1.1.2 Proof of stake (PoS)

Proof of Stake is the more environmentally friendly brother of the Proof of Work protocol. Proof of Stake makes use of the premise that those who own most coins in a network have interested in keeping the network maintained and the value of its coins high.

In a system that uses Proof of Stake, a randomized process is used to determine who gets the right to produce the next block. Users can stake their tokens (digital assets that exist on specific Blockchain) to become a validator (someone who produce blocks; like a miner in PoW), which means they lock their tokens (see more in Chapter 4, about different types of tokens) up for a certain time. After doing so, they are eligible to forging (blocks producing).

The process that decides who gets the right to produce the next block takes a couple of factors into account. What these factors are, depends on the design of the Blockchain, but in general, the person who has the biggest stake has the highest chance to produce a block. An example of another factor that can be considered is how long the coins have been staked.

Validators are also rewarded for their work. The reward which the validator receives for creating the next block depends on the design of the Blockchain yet again. Usually, they either receive all newly-minted coins or part of, or they receive a fixed amount of coins and all commission fees of all the transactions in the block that was created.

Proof of Stake is not only much more energy efficient than the Proof of Work protocol, but it also has another major distinction. In a PoW mechanism, a miner may own none of the coins they are mining, meaning they only seek to maximize their profits without actually improving the network. In a Proof of Stake protocol validators have a much bigger incentive to maintain the network as they hold the coins of the Blockchain on which they are validating. (Blockgenic, 2018)

1.1.3 Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) is a very fast consensus mechanism and is often referred to digital democracy, thanks to its stake-weighted voting system. In a Delegated Proof of Stake system users can stake their coins to vote for a certain number of delegates. The weight of their vote depends on their stake, for example, if A stakes 10 coins for a delegate and B stakes 1 coin for a delegate, A's vote weighs 10 times heavier than B's vote. A delegate is a person or organization that wants to produce blocks on the network. The delegates that receive the highest number of votes get the right to produce blocks and are rewarded for creating these blocks. Just like with Proof of Stake, they are either paid from the transaction fees or they are paid a fixed amount of coins, which are created through inflation. How many delegates get the right to produce blocks depends on the design of the Blockchain.

Rather than simply taking a pay cut to be a delegate, delegates may get voted in, because they use the delegate pay on other tasks like marketing, legal work, or lobbying. They can thus perform some of the duties that employees of other types of companies would do. Thus, there are strong incentives for all delegates to not just secure the network, but also to provide value to shareholders in other ways. (Blockgenic, 2018)

Since delegates want to receive as many votes as possible, they are constantly incentivized to create things valuable to the community, as they are likely to receive extra votes for doing so.

1.1.4 Proof of Elapsed Time (PoET)

Proof of Elapsed Time (PoET) is a Blockchain network consensus mechanism algorithm that prevents high resource utilization and high energy consumption and keeps the process more efficient by following a fair lottery system.

PoET is a consensus mechanism algorithm that is often used on the permissioned Blockchain (see section 1.2.2) networks to decide the mining rights or the block winners on the network. Based on the principle of a fair lottery system where every single node is equally likely to be a winner, the PoET mechanism is based on spreading the chances of winning fairly across the largest possible number of network participants.

The working of the PoET algorithm is as follows. Each participating node in the network is required to wait for a randomly chosen time period, and the first one to complete the designated waiting time wins the new block. Each node in the Blockchain network generates a random wait time and goes to sleep for that specified duration. The one to wake up first – that is, the one with the shortest wait time – wakes up and commits a new block to the blockchain, broadcasting the necessary information to the whole peer network. The same process then repeats for the discovery of the next block.

The algorithm allows applications to execute trusted code in a protected environment, and this ensures that both requirements – for randomly selecting the waiting time for all participating nodes and genuine completion of waiting time by the winning participant - are fulfilled. Essentially, the workflow is similar to the consensus mechanism followed by Bitcoin's Proof of Work algorithm, but without its high-power consumption. Instead of being resource intensive, it allows a miner's processor to sleep and switch to other tasks for the specified time thereby increasing its efficiency. (Frankenfield, 2018)

PoET controls the cost of the consensus process and keeps it nimble, so the cost remains proportional to the value derived from the process, a key requirement for the cryptocurrency economy to continue flourishing. The PoET concept was invented during early 2016 by Intel, the famous chip manufacturing giant.

| | PoW | PoS | DPoS | PoET |
|-------------------------|----------------------|-------------------|-------------|-------------------------|
| Energy consumption | high | low | low | very low |
| Transaction rate | low | high | high | medium |
| Type of Blockchain used | public | both | both | both, mostly in private |
| Project Example | Bitcoin, Litecoin | Dash, Ethereum | BitShares | Hyperledger |

Table 1: Comparison of consensus mechanisms

Source: own processing

Table 1 illustrates the difference between the various consensus mechanisms and provides projects examples that running these mechanisms. In all cases, the objective of the consensus approach is to ensure the functioning of the system. Choice of the required consensus mechanism process should be made reliant on the project prerequisites.

1.2 Types of Blockchain

Depending on how is a Blockchain network operated and who can join this network, two main categories can be recognized:

- Public blockchains
- Private blockchains

1.2.1 Public blockchains

A public Blockchain is a permissionless Blockchain. A public Blockchain has absolutely no access restrictions. In other words, the code to operate a public Blockchain is open and free. It means anyone who installs on a computer specialized software of particular Blockchain can send and receive transactions or participate in the validation process in that network. We rely on economics and game theory incentives to ensure that everybody in the system behaves honestly and accordingly to the rules. On this basis, honest participants are economically rewarded, where dishonest ones only incur work or cost, with no possibility of ever recouping that cost. (Massessi, 2018) Transactions can be viewed on the Blockchain explorer (such a Blockchain.info) wherein keeping anonymity. So, permissionless blockchains are good for scenarios where protecting the anonymity of users is important or where all users should be treated equally (The Linux Foundation, 2018).

Cryptocurrencies (see more in Chapter 2) are the most popular and widely used applications of public blockchains.

1.2.2 Private blockchains

A private Blockchain is a permissioned Blockchain. Permissioned networks place restrictions on who can participate in the network and in what transactions. Besides, transactions are not publicly viewable in the Blockchain, and only select nodes can access the ledger. So, in a private permissioned Blockchain, we draw upon the fact that we know who a user is. We also assume that the users are going to behave fairly as we know who they are, and they know the consequences of any fraud. (Massessi, 2018) Widely used in corporate scenarios, for example, Blockchain for the business or Blockchain for supply value chains.

To conclude, that's obvious that Public and Private blockchains serve vastly different purposes. For instance, the public blockchains tend to focus more on B2C (business to consumer) scenarios, whereas private blockchains lend themselves well to B2B (business to business) scenarios or creating shared infrastructure between enterprises. (The Linux Foundation, 2018)

This is considerable debate in the Blockchain community in the value of a private Blockchain over a shared database. On the one hand, private blockchains provide higher levels of error checking, transaction validity and of course security than a shared database. On the other hand, experts say that is cheaper to run and maintain shared database than transfer to permissioned Blockchain.

1.3 The potential danger for Blockchain

Nevertheless, Blockchain technology prevents the majority of malicious attacks and reduces many associated risks, it doesn't eliminate all attacks. In this section, we consider the main risks of Blockchain technology and its ecosystem and give some recommendations for prevention that.

1.3.1 The 51% Attack

A 51% attack may happen when a single miner node that presumably has exceptionally more computational resources than the rest of the network nodes, dominates the verification and approval of transactions and controls the content of a Blockchain.

As it owns more than half (51%) of the network's processing power, the dominant node can outrun all other nodes, manipulate the Blockchain, insert fraudulent transactions, double-spend funds, or even steal asset from others.

Although no 51% attacks have occurred in the Bitcoin network since January 2009, when the first genesis block was created and added to the Blockchain. However, the risk still does exist, especially in blockchains with small networks. (Xu, 2016)

The wide adoption of the Blockchain can make the attack 51% unrealistic by splitting the mining resource between individuals. Detection techniques serve as a tool for controlling and prevention.

1.3.2 Identity theft

Although blockchains keep anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If one's private key is stolen, no third party can recover it. Hence, all the assets this person owns in the Blockchain will disappear, and it will be nearly impossible to identify the thief. (Xu, 2016)

Besides, current cryptography standards are not completely uncrackable. With the advent of quantum computing, nowadays in order to crack the cryptographic key - too much time is required. However, quantum computing is in its development and in the future - a period of the time can be reduced.

1.3.3 Illegal activities

Blockchain technology can become a venue for illegality (Bigmore, 2018). The Silk Road "dark web" is an online marketplace where anonymous users can do the business of selling illegal drugs using bitcoins (see more about Bitcoin in section 2.1).

A cryptocurrency (see more in Chapter 2) that uses Blockchain technology may also facilitate money laundering (Xu, 2016). As far as Bitcoin is not yet universally treated as a fiat currency, it makes it possible to create an "underground" channel for illegal movement of funds within its network.

The detection techniques and intervention of law and regulations (see more in Chapter 3) can prevent the flowering of these activities.

1.3.4 System hacking

It is difficult to hack a Blockchain itself and change the records, but not the programming codes and systems that implement its technology. MtGox, once the largest Tokyo-based cryptocurrency exchange, was hacked in March 2014, and bitcoins worth \$700 million were stolen because of poorly-maintained and outdated codes. As a result, Mt.Gox went offline and declare bankruptcy, thus investors been broken and bitcoin dropped in value. (Bigmore, 2018)

A more recent incident affected a DAO (Decentralized Autonomous Organization) that holds large quantities of Ethereum (see more about the second biggest cryptocurrency in section 2.2). The hacker exploited a software vulnerability and stole \$50 million worth of Ethereum. (Xu, 2016) As a result, Ethereum had to be split into two derivative cryptocurrencies Ethereum and Ethereum Classic to get around the scandal and keep their investors.

To avoid hacking, robust systems and advanced intrusion detection method must be used.

2 THE MOST SIGNIFICANT CRYPTOCURRENCY PROJECTS

In a historical retrospective, markets in general and financial markets have experienced a huge development. In this regard, the instruments used as exchange instruments have also experienced change and have evolved in accordance with the markets needs aiming to make trade transactions as easy as possible. Those instruments used to intermediate the exchange of goods are known as money.

Most of the economists define money as something that serves as a medium of exchange, a unit of accounting, and a store of value. Money is a medium of exchange in the sense that we all agree to accept it in making transactions. Merchants agree to accept money in exchange for their goods the same as employees agree to accept money in exchange for their labor. As a unit of accounting, money provides a simple device for identifying and communicating value. Money serves as a store of value in that it allows us to store the rewards of our labor or business in a convenient tool. In other words, money lets us store the value of a long, hard week of work in a tidy little stack of cash. (Bunjaku, 2017) The key problem of traditional fiat currencies (government issued money) is that they can function only with trust in hand.

From the era of barter to commodity money, metal, and coins, to gold and silver, continuing by modern monetary systems and checks and ending with the latest global currency developments, such as the introduction of cryptocurrencies known as Bitcoin and Ethereum, have passed centuries. Each type of money has played its indispensable role in transaction activities for the respective time. However, as the human society in general and markets evolved, there was a need for more sophisticated goods exchange instruments. (Bunjaku, 2017) In this regard, the introduction of cryptocurrencies has revolutionized the international payment system on a scale that just a few years ago was unimaginable.

A cryptocurrency is the first application of the Blockchain technology, that was invented and proposed on the Bitcoin protocol base. A cryptocurrency is a digital currency that uses cryptography for security that makes difficult to counterfeit it because of this security feature. A defining feature of a cryptocurrency and arguably its most endearing allure is its organic nature. It is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. (Vigna, 2015) The main benefits of cryptocurrencies are that they make it easier to transfer funds between two parties in a transaction. These transactions are facilitated by using public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks for international transactions. (Tapscott, 2016) Nowadays, there are up to 2 100 cryptocurrencies.

2.1 Bitcoin

Bitcoin is a currency, a digital unit of value, used by people to exchange goods, services or exchange for other currencies, the rate of which tends to be very fluctuating with respect to traditional, government-issued money. Its first use appears in a white paper released in 2008 in which Satoshi Nakamoto proposed Bitcoin, a system for electronic, peer-to-peer payments based on distributed ledger technology (Nakamoto, 2008).

The Bitcoin protocol built on Blockchain and available as open source software. The protocol contains instructions for computers, as well as information necessary for monitoring and verifying transactions between people in the system. The platform relies on a public Blockchain to record the complete history of currency transactions. (What is Blockchain Technology? A Step-by-Step Guide For Beginners, 2019) The nodes of the Bitcoin network use a Proof of Work consensus algorithm based on moderately hard puzzles to establish how to append a new block of transactions to the Blockchain (see figure 3).

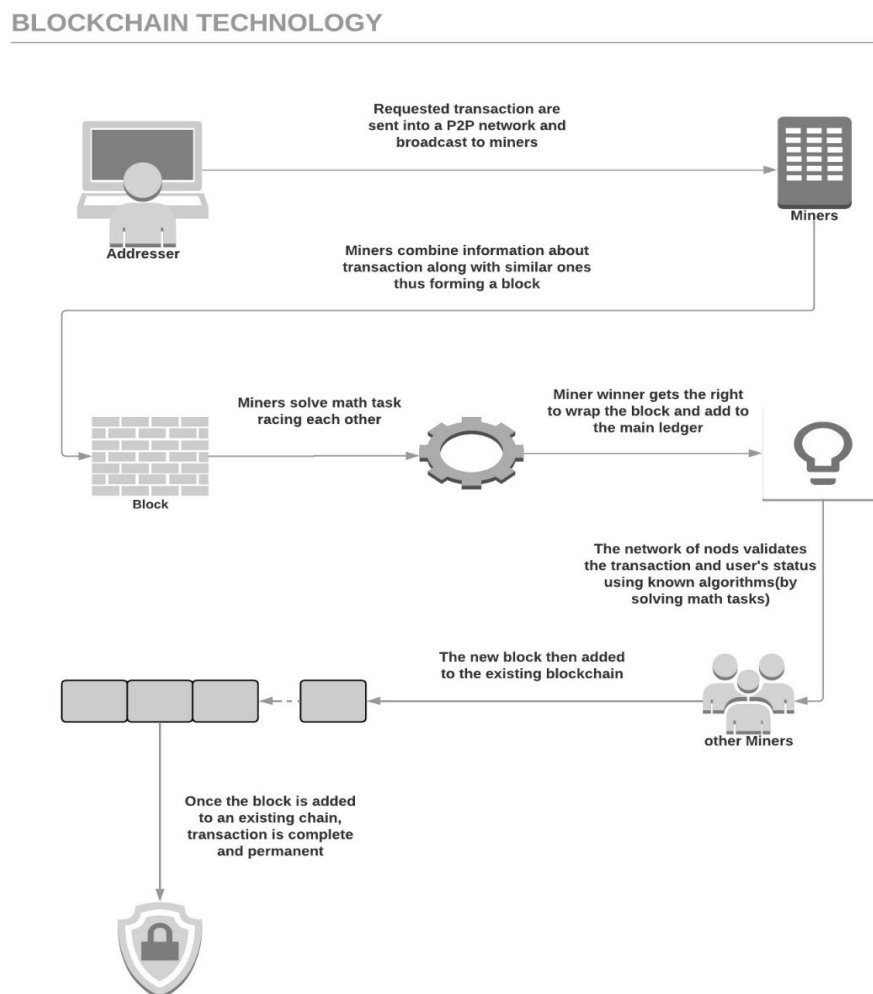


Figure 3: Bitcoin Blockchain transaction flow

Source: own processing

2.1.1 Bitcoin Blockchain Architecture

The ledger is stored, updated, and maintained by a peer-to-peer network. It is the job of the network to come to a consensus on the contents of each update to the ledger. Each node (non-traditional name - miner) in this network maintains its own copy of the ledger. This ensures that each individual copy of the ledger is identical without requiring a centralized official copy of the ledger.

The Bitcoin Blockchain consists of a sequence of blocks where each block builds on its predecessors and contains information about new Bitcoin transactions. When blocks fill up with data, transactions are hashed into what is known as a Merkle tree. Merkle trees provide for an easy way to find any specific transaction in a Blockchain. A hash function is a one-way function that takes any type of data and converts it into a unique character code. Merkle trees use hashing to convert large amounts of information into a much smaller amount of data (similar to data archiving process). Depending on the hashing algorithm, each transaction transformed into a fixed length code known as the Merkle root (or Root Hash) In the Bitcoin Blockchain hashing algorithm known as SHA-256 uses 64-digit character code. (The Linux Foundation, 2018)

For example, we will look at the hash value for the text - “The guy who passed.” The fingerprint of this text, which was calculated using the hash function dSHA256, is

71642707ba7c9be334f444ef5238f4k0b355481796fdddffaac4c5f2320eea68.

Now notice the small change in the original text to “the guy who passed.” It will cause an unpredictable change of the fingerprint, which can be seen from the corresponding new hash value:

423f5cd7246te6faf8b839c41bf46d303014cffa65784ab108431514e36c4cta.

As suggested by this example, a data file’s hash value cannot be prognosticated.

In this way, The Merkle Root summarizes all the data in the related transactions and stores in the block header. It maintains the integrity of the data. If a single detail in any of the transactions or the order of the transaction’s changes, so does the Merkle Root. Using a Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

A block header includes certain things determined by the blockchain, but most frequently consists header hash of the previous block, the Merkle root of the current block, and the nonce (contains timestamp to ensure exact timeliness). By including the previous block’s header (see figure 4), blocks are “chained” together. (Nakamoto, 2008)

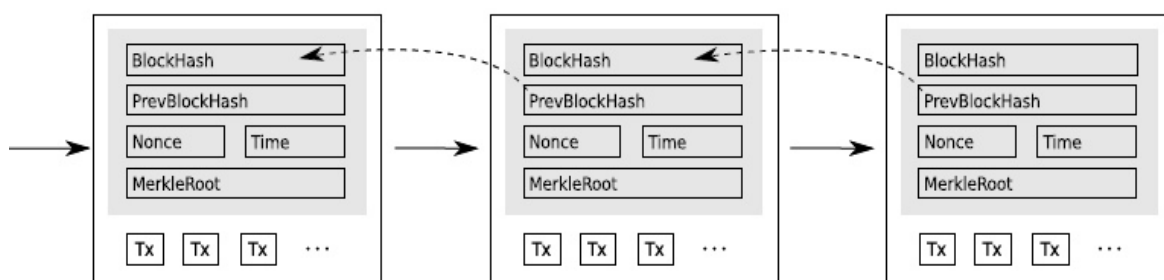


Figure 4: Blocks chaining

Source: (Tschorsch, 2016)

Chaining is important because blockchains are kept on millions of nodes across the network. Chaining allows blockchains to easily check and see if any data was altered just by comparing the hash of the current header. Simply put, Blockchains are immutable because the data on a block can never be changed or deleted. (The Linux Foundation, 2018) In other words, Blockchain is a linear chain of multiple blocks that are connected and secured by cryptographic proofs. If you wanted to steal a bitcoin, you'd to rewrite the coin's entire history on the Blockchain in broad daylight. That's practically impossible. So, the Blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. (Tapscott, 2016)

The chain keeps growing as long as the system will function. The system monitors the status of the account of each participant at any time and also identifies information (about when it was created, spent or received) attached to each Bitcoin transaction by creating a sequence with a fixed time of each operation. In the process of validation, each transaction added to the constantly updated Blockchain is compared with all previous entries. Based on the consensus mechanism that engaged in checking which transactions are legalized, the main ledger provides unquestionable evidence of Bitcoin availability in each user balance and the timeline of their receiving and spending (similar to receipt). Thus, it ensures the unambiguity of Bitcoin and prevents double-spending – the key advantage, provided by Blockchain (Nakamoto, 2008).

2.1.2 Transaction legitimacy

One of the critical properties of the Blockchain is its general availability. This requires users to be anonymous to avoid identities being tied to a specific transaction. Anonymity is achieved through public/private key cryptography. Your private key is for your eyes only. Your public key can be shared with the public. A public key, on the other hand, is derived from that number and can be shared freely. It serves as a pseudonym in the Bitcoin network. Your public key is the address you receive and send transactions from. To prove that your public key is associated with your private key, a digital signature is used. A digital signature uses math to show a relation

to your public key from your private key, without revealing your private key. In the language of cryptographers, by signing the public key with using a private key – transmits information that includes instructions on transferring a certain number of Bitcoins from one address to another. An important feature of this system is that with the current level of computer technology, it's impossible to find a private key by using a public key drawn upon on a back-calculation. (Vigna, 2015)

2.1.3 Monetary policy of Bitcoin

Every payment system needs rules that regulate how new monetary units are produced. The Bitcoin network is calibrated in such a way that, on average, a block candidate with a valid hash value is found every 10 minutes.

The winner of the mining contest receives a predefined number of newly created Bitcoin units. It had started at 50 bitcoins, dropped to 25 in late 2012 and to 12,5 Bitcoins in 2016. Hence, the coin reward will decrease to 6,25 in May 2020. The current number of rewards is 12.5. This halving process is programmed to continue for 64 times before new coin creation ceases.

In the Bitcoin system, money creation is scheduled so that the number of Bitcoin units will converge to 21 million units. A Bitcoin unit is divisible and can be divided into 100 million "Satoshis" (the smallest fraction of a Bitcoin). This limit exists because the reward for the miners is halved every 210,000 blocks (approximately every four years). New Bitcoins aren't the only way to compensate for the efforts of miners. The basic software also has a function of charging transaction fees from senders. When the releasing of new Bitcoins ends in 2140, commissions will be only one form of reward for maintaining the network. (Vigna, 2015)

In order to ensure the balance of the system, the creator (known to us under the nickname Satoshi Nakamoto) designed a hash rate of the entire network into the Bitcoin algorithm. In fact, this is the total computer power of the network per second. Moreover, he programmed autocorrecting of the complexity of the math puzzles in a manner that every 2016 blocks degree of complexity rises. This implies that the mining time of each 2016 blocks is directly proportional to the network's hash rate in so far as represent miner's involvement in the network processing Bitcoin transactions.

Thus, the miners forced to run more and more productive computers to win in solving Bitcoin math tasks. At the same time, it brings one of the biggest threats of the Bitcoin community – off-scale usage of electricity.

2.2 Ethereum

Released in 2015, Ethereum is the brainchild of Vitalik Buterin, who saw the potential uses of Blockchain technology as the next steps in furthering the expansion of the Blockchain community. Ethereum is an open source platform that enables developers to build and run decentralized applications (Dapps) namely smart contracts (see more in Chapter 4). Dapps are the applications that establish a direct connection between a user and a service.

The interesting thing about the blockchains that came before Ethereum is that their operating systems were only designed to exchange specific coded items over transactions, primarily being the network's supported cryptocurrency. Vitalik Buterin saw this as a feature that had plenty of room for expansion, and in response, he proposed a solution that would allow developers to customize the form of the data they could send and store over a Blockchain network. (What is Ethereum (ETH)?, b.r.)

The Ethereum Blockchain can be alternately described as a Blockchain with a built-in programming language, or as a consensus-based globally executed virtual machine. The core of Ethereum is the Ethereum Virtual Machine (EVM), which executes the code of random algorithmic complexity. Solidity is a statically-typed programming language with a like JavaScript syntax. Solidity is designed for developing smart contracts that run on the EVM. Solidity contracts are first compiled to bytecode which is ultimately executed on the EVM.

Ether is the name of the cryptocurrency used to pay for transactions on the Ethereum network. Just like users of the cryptocurrency often pay small transaction fees for monetary transactions, users of smart contracts pay small fees for computations executed by the EVM. In the case of Ethereum, this computation fee is called "gas". Again, it incentivizes users to put meaningful contracts onto the platform. Ether is the metric unit which also used to buy "gas".

When Buterin had presented the project, Ethereum received 14,5 million United State dollars. The result has achieved in six weeks that makes it the most successful crowdfunding experience ever happened on Kickstarter (Vigna, 2015). Ethereum is now currently the cryptocurrency with the second highest coin market capitalization that expects to surpass Bitcoin as both a valued investment and as the world's most popular cryptocurrency.

2.2.1 Ethereum Blockchain Architecture

Ethereum, unlike Bitcoin, has the property that every block contains something called the "state root" - the root hash of a specialized kind of Merkle tree (called Patricia tree) which stores

the entire state of the system: all account balances, contract storage, contract code and account nonce are inside.

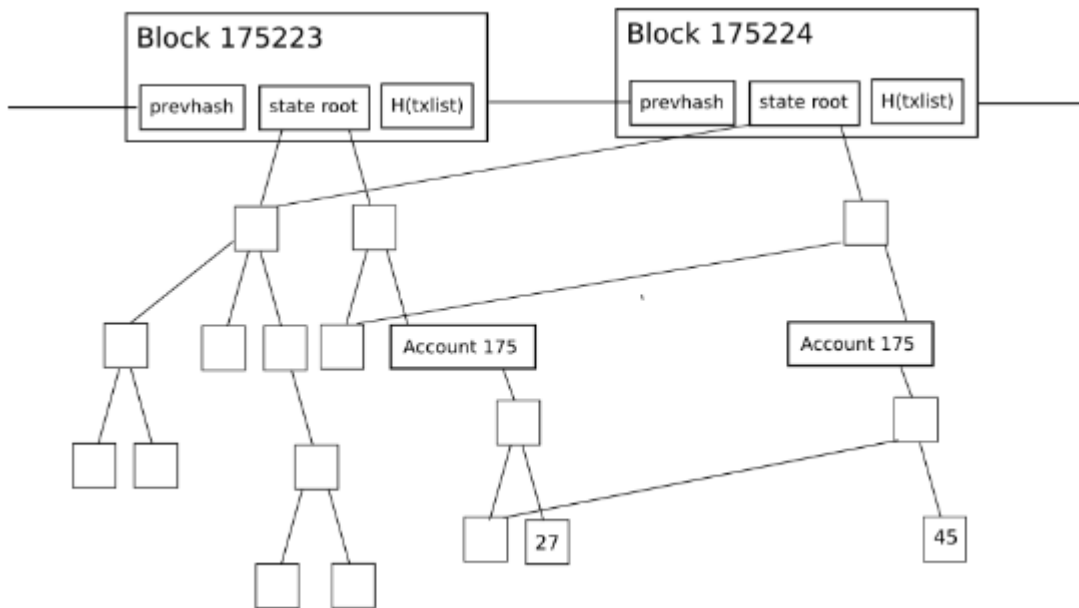


Figure 5: Patricia tree

Source: (Buterin, 2015)

Because of the way the Patricia tree works, if a few changes are made then most parts of the tree will be exactly the same as in the last block. Hence, there is no need to store data twice as nodes in the new tree will simply be able to point back to the same memory address (see figure 5) that stores the nodes of the old tree in places where the new tree and the old tree are exactly the same. (Ethereum Development Tutorial, 2017) If a thousand pieces of data are changed between block N and block $N + 1$, even if the total size of the tree is many gigabytes, the amount of new data that needs to be stored for block $N + 1$ is at most a few hundred kilobytes and often substantially less (especially if multiple changes happen inside the same contract).

2.3 Ripple

Ripple, one of the three largest crypto assets by market capitalization, is an enterprise-friendly alternative to bitcoin, geared toward displacing SWIFT and other global payment networks. (Tapscott, 2016) Ripple has the native token of the network (see more in Chapter 4 about different types of tokens), called XRP.

Ripple's architecture relying on a handful of trusted nodes rather than on miners to secure the Blockchain. It gives the ability to process more transactions but also makes it more centralized, which, in the eyes of some critics, entirely contradicts the original idea of decentralization the

main feature of Blockchain. The interesting thing is that these trusted nodes prevalently are the organizations itself which using Ripple's distributed ledger. Hence, Ripple has been very successful in courting large banks such as AstroPay in the United Kingdom or German Fidor Bank and other potential enterprise users to employ their products and services. The project can supersede Visa and MasterCard on the level of providing electronic funds transfer between banks and replace online payment system PayPal by offering lower commission fees.

In figure 6, I illustrate the timeline of appearance the most significant cryptocurrency projects.

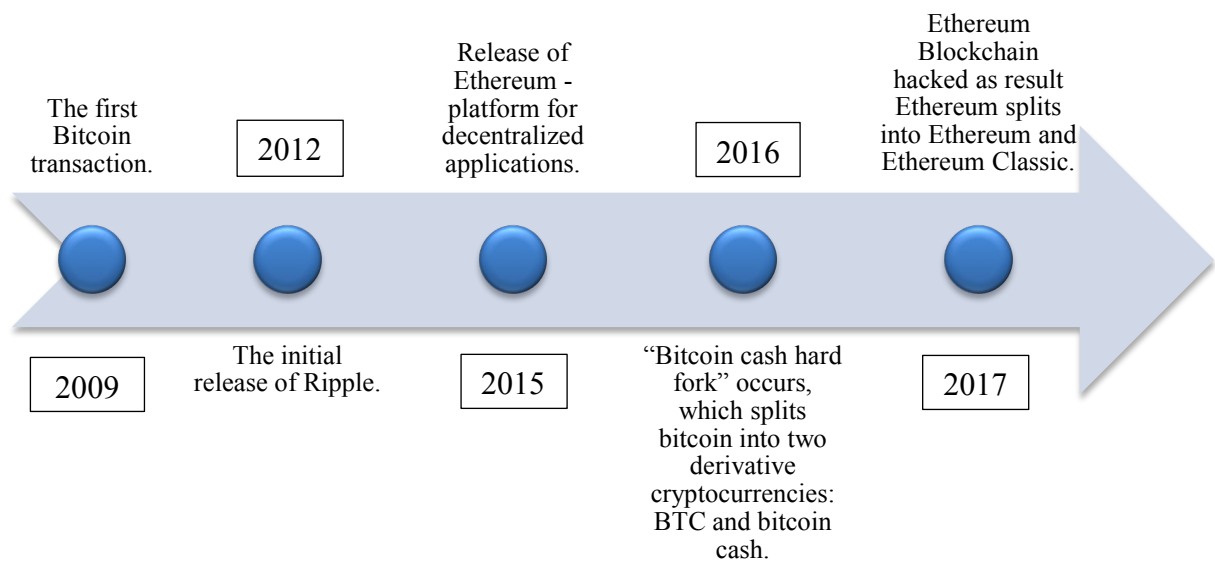


Figure 6: The most significant cryptocurrencies projects events timeline

Source: own processing based on data (Bigmore, 2018)

Over the years, cryptocurrencies broaden the boundaries. As an illustration, Microsoft allows users to buy games using cryptocurrency, Uber in Argentina switches to bitcoin payments, and Swiss railway is among users who accept the currency as well. Moreover, the number of ATMs allowing cryptocurrencies growing daily.

3 REGULATION OF CRYPTOCURRENCY IN THE WORLD

Many steps have been made, since the appearing of Bitcoin as a first digital currency. In many countries, the alternative of creating digital money was perceived positively. A lot of volunteers and individuals who had believed in concept have affected the spreading of cryptocurrencies by providing the simplest infrastructure merely starting use cryptocurrency in the very beginning. As a result, cryptocurrency has gained sufficiently wide distribution and become the subject of interest for worldwide CEOs and government regulators. Thus, these steps have approached the need for intervention of law and regulations. Nevertheless, it's still difficult for many legislators to understand the nature of changes taking place in the outside world. In the context of cryptocurrencies, the biggest misunderstanding remains practical implementation of restrictions towards the crypto economy. For instance, Bitcoin - simply doesn't have any central server which authorities could confiscate. However, they have enough legal authority and various tools to complicate the life of the crypto ecosystem.

I provide a brief overview of facts about opportunities and limitations of cryptocurrencies in selected world regions.

3.1 United States of America

The first case that influenced the shaping of cryptocurrency legality was capturing of Silk Road exchange market by FBI. They have tracked cashflow laundered from the drug sales using the transparency of Bitcoin transactions provided by Blockchain.info resource in 2013. Thus, the situation damaged the image of cryptocurrency and affected the mind of society. However, when FBI get the bitcoins they realized the worth of code lines. Moreover, the certain success of the operation has opened the new way of payment, as Bitcoin less frighten for Governments and law enforcement. In that untypical way, the cryptocurrencies become legalized in the United States (Vigna, 2015).

Nowadays, each American state has different positions towards the regulation of crypto. Some of them ask for a license and proof of the fight against money laundering and illegal money transfers. At the same time, when the ones as Texas and some others on West decided to fall cryptocurrency outside the scope of the legislation, (not required a license) giving more room for the digital community to broaden and grow.

3.2 China

The People's Bank of China banned financial institutions from handling Bitcoin transactions in 2013 and went further by banning domestic cryptocurrency exchanges in 2017. Unsurprisingly, China does not consider cryptocurrencies to be legal tender and the country has a global reputation for hard cryptocurrency regulations. (Cryptocurrency Regulations Around The World, 2018) However, China is actively exploring the Blockchain technology itself and is expected to be widely integrated into sectors such as product traceability, copyright protection, bill verification, precision marketing, energy, and healthcare.

3.3 EU

On October 22, 2015, the European Court of Justice held in his decision that buying or selling cryptocurrencies such a Bitcoin is exempt from value-added-tax (VAT) in all EU Member States. However, the President of the European Central Bank (ECB), Mario Draghi, warned that Bitcoin and other digital currencies are “very risky assets” due to their high volatility and speculative prices. He also stated that digital currencies are not subject to a specific supervisory approach. In addition, in December 2016, the ECB and the Bank of Japan launched a joint research project named “Stella,” which looks at the possible use of distributed ledger technology for financial market infrastructures. (Global Legal Research Directorate Staff, 2018)

Meanwhile, various countries are attempting to work out the best ways to deal with cryptocurrencies. For instance, Germany's ministry of finance would not accept it as an official currency but rather as a “unit of account”, paving the way for a future framework to tax Bitcoin-based transactions. In the Czech Republic, anti-money laundering legislation keeps a close eye on all providers of services related to cryptocurrencies such as exchanges.

So, the EU is actively exploring further cryptocurrency regulations. In February 2018, Mario Draghi added authorities were working with the Single Supervisory Mechanism to develop a way of identifying the financial risks that cryptocurrencies pose. (Cryptocurrency Regulations Around The World, 2018)

3.4 Switzerland

In Switzerland cryptocurrencies and exchanges are legal, and the country has adopted a remarkably progressive stance towards cryptocurrency regulations. The Swiss Federal Tax Administration considers cryptocurrencies to be assets: they are subject to the Swiss wealth tax and must be declared on annual tax returns.

Moving forward, Switzerland's government has indicated that it will continue to work towards a regulatory environment which is friendly to cryptocurrencies. In 2016, the town of Zug, a prominent global cryptocurrency hub, introduced Bitcoin as a way of paying city fees. In January 2018, Swiss Economics Minister Johann Schneider-Ammann stated that he was aiming to make Switzerland "the crypto-nation". Meanwhile, the Swiss Secretary for International Finance, Jörg Gasser, has emphasized the need to promote cryptocurrencies without compromising existing financial standards. (Cryptocurrency Regulations Around The World, 2018)

4 OTHER SIGNIFICANT BLOCKCHAIN APPLICATIONS

A smart contract is another meaningful application of Blockchain technology. Ethereum platform was designed specially to build and run smart contracts. A smart contract allows users to agree on the conditions of cooperation and keep the agreements into Blockchain. When the conditions are done, the contract performs the action. The first part of this chapter reveals the properties of smart contract and its advantages. For better understanding its benefits, the directions of implementation and possible dangers are designed.

After Blockchain and cryptocurrencies were widely reported in the mass media for their massive potential and rise in value, initial coin offerings (ICOs) also became increasingly well known. It was primarily the immense amounts of money raised through ICOs –amounts that continued to grow, in the first quarter of 2018 – that focused, close attention on this topic. (Stacher, 2018) The second part deals with modern types of investment and raising capital that Blockchain technology makes possible.

4.1 Smart contract

A smart contract is a set of computer code between two or more parties that run on the top of a Blockchain and constitutes a set of rules which are agreed upon by the involved parties. When these rules are met, this code executes on its own and provides the output. (Pratap, 2018) The code and the agreements contained therein exist across a distributed, decentralized Blockchain network. Smart contracts allow you to exchange anything of value including money, shares or property without the need for a central authority, legal system, or external enforcement mechanism. They make transactions traceable, transparent and irreversible.

The first smart contract concept was introduced well before any Blockchain technology was even in existence. Smart contracts were first proposed by Nick Szabo in 1994. Szabo is a computer scientist, legal scholar, and cryptographer who is a well-respected academic with research in digital contracts and digital currency. (Swezey, 2017)

A smart contract consists of a value, address, functions, and state. It takes transaction as an input, executes the corresponding code and triggers the output event or another contract (see figure 7). Drawn upon the function logic, implementation states are changes.

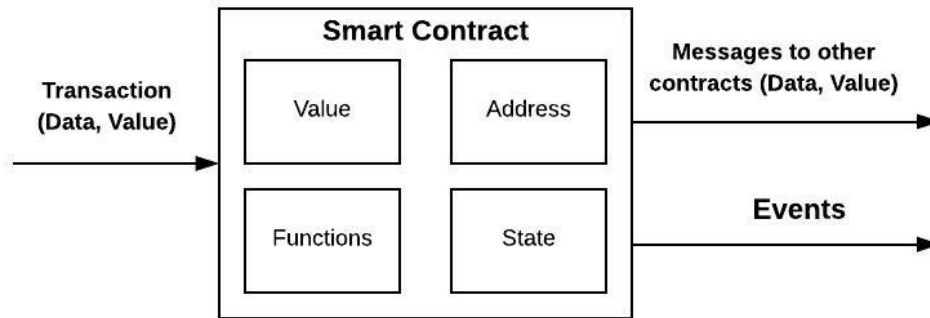


Figure 7: Structure of smart contract

Source: own processing based on data (Bhabendu, 2018)

Smart contract properties:

- Self-executable
- Self-verifiable
- Tamper Proof

These properties are what makes these contracts “smart”.

For a wide range of applications, smart contracts based on Blockchain technology bring next benefits comparing to traditional contracts:

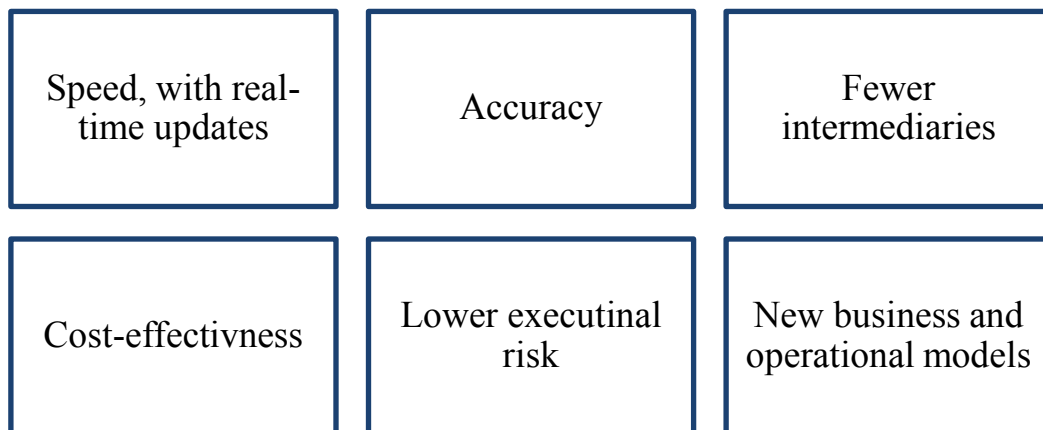


Figure 8: Smart contracts benefits

Source: own processing

To conclude, in a normal world process for getting a court-registered document as a proof, you would need to go to a lawyer or notary first, give them money in turn of their services and wait till you get the document that you need. However, the scenario changes completely with smart contracts. When you run this process with smart contracts, you’d simply get the document of

your need by paying just for that and this will be done without the involvement of any third-party such as the lawyer in this case. Moreover, smart contracts are not limited to only defining the rules around any agreement, but they are also responsible for automatically executing those rules and obligations. Smart contracts are most beneficial in business collaborations in which they are used to agree upon the decided terms set up by the consent of both the parties, but also could bring set of advantages applicable to public sectors organizations. This reduces the risk of fraud and as there is no third-party involved, the costs are reduced too. (Pratap, 2018)

4.1.1 Smart Contracts Use Cases

Smart contracts can be applied in different industries and sectors and bring certain advantages for many industry sectors such as, reducing overhead costs, providing transparency, and saving time. Besides, they are more reliable, secure, efficient and trustworthy compared to paper contracts. (Pratap, 2018)

In this section, the list of the main directions where smart contracts were implemented will be discussed. However, see Chapter 5 to understand the wide potential of Blockchain technology and smart contracts on the level of public institutions and markets.

Insurance

Traditional insurance system takes a lot of time to process a claim. As a result, we have unwanted administrative costs, dissatisfied customers and inefficiency for insurance companies. In the other side, customers are trapped in time constraints for their money.

By using smart contracts in such processes can result in simplifying and streamlining the processes by automatically triggering payment for a claim when certain conditions are met as per the client and company's agreement. Any specific details like the extent of loss due to damage can be kept on a Blockchain and the amount of compensation can be decided accordingly. (Pratap, 2018) Etherics and InsCoin are some of the projects that work hard to provide insurance infrastructure based on Blockchain.

Supply chain

Supply chain management involves the flow of goods and products from the initial stage to the final stage. Being a major part of many industries, proper functioning of a supply chain is crucial for businesses. Supply chain management is not a one-person job to do and thus, there are multiple entities are engaged in supply chain system (such as transport and shipment).

Smart contracts in the supply chain can record ownership rights while the products are transferred through the supply chain. Everyone in the network can track the location of the

product at any given time. The final product can be checked at each stage throughout the delivery process until it reaches the end customer. If an item is lost in the process, smart contracts can be used to detect its location. Also, if any stakeholder fails to meet the contract terms, it would be transparent for the whole system to see. Making supply chain more transparent via smart contracts is helping to smooth out the movement of goods and restore trust in trade. (Pratap, 2018)

Real Estate

Real estate system in the traditional way of involves lots of risks as well as time taking. Let's take an example to better understand the advantage of a smart contract. For instance, you rent or sell your apartment to someone, then you create a smart contract in an existing Blockchain network. Information regarding the property stored in the Blockchain can be viewed, and anyone can access it, but they can't change it. In this way, you can find a buyer without the need for a middleman. The CrowdliToken platform is now the existing use case of Blockchain based smart contracts for trading property.

4.1.2 The danger for smart contracts – The Oracle Protocol

Engineering a Blockchain contract is not like programming a client-server app. One important difference is that data with which the contract interacts, must already be on the Blockchain. Many use cases of smart contracts run into a similar problem – they are seriously limited unless they can interact with the world outside the Blockchain. (Kosinski, 2018) Because of the fact that smart contracts are locked in the Blockchain without access to the external data, Oracle is designed to be the input/output gateway that can collect data from outside. Simply put, an oracle is another contract, which injects data into the Blockchain, allowing other contracts to consume it. The type of data required by smart contracts can include information on price feeds, weather information, and others.

For blockchains to have a sustainable impact on practical applications and various industries, they need to be able to interface accurately and reliably with real-world data. (Curran, 2019) But achieving this with oracles is difficult and presents many challenges. The Oracle has a weakness that is defined as the security, authenticity, and trust conflict between third-party oracles and the trustless execution of smart contracts.

So, Despite the high security of the Blockchain technology, the ecosystem in which Blockchain based applications are built can become the subject of hacking. The Oracle protocol is one of the tempting aims for hackers.

4.2 Initial coin offering as an innovative crowdfunding model

Matching investors with entrepreneurs is one of the core functions of the financial services industry. The process of offering shares in a private corporation to the public for the first time is called an initial public offering (IPO). Growing companies that need capital will frequently use IPO to raise money, while more established firms may use an IPO to allow the owners to exit their ownership by selling shares to the public.

In an initial public offering, the issuer, or company raising capital, have to attract underwriting firms or investment banks to help determine the best type of security to issue, offering price, amount of shares and time frame for the market offering (Chen, 2019). But it's a fact that intermediaries take a good deal of money which startups can't allow themselves. Moreover, taking loans from banks has become more and more difficult, therefore startups began crowdfunding. Crowdfunding is a method for raising money for your business or idea with the collective efforts of other individuals. They can be your family, friends or just about anyone who is willing to back your project in return for a piece of the pie (Varsamis, 2018). Thanks to new crowdfunding platforms, small companies now can access capital using the Internet. Kickstarter and Indiegogo are the best-known platforms which help to match startups with stakeholders. However, even in this scenario the sides can't work directly and have to pay sufficiently high commission fees to online platforms. So, the intermediary is the ultimate arbiter of everything (Tapscott, 2016).

4.2.1 The Blockchain takes the concept of investment further

An initial coin offering is a new source of funding. An ICO is equivalent to an IPO in the investment world. Companies can raise funds in crowdfunding manner by issuing digital tokens and sell them through Blockchain. So, even poorest people can become stock market investors by buying these tokens (in section 4.2.2 you can see more about different types of tokens).

In the Blockchain scenario, ICOs act as fundraisers of sorts. For instance, a company looking to create a new application or service launches an ICO. Next, interested investors buy the offering, either with fiat currency (government-issued money) or with preexisting digital tokens like ether. In exchange for their support, investors receive a new token of specific ICO. Investors hope that the token will perform exceptionally well into the future, providing them with a stellar return on investment. The company holding the ICO uses the investor funds as a tool for achieving its goals, launching its product, or starting its digital currency. ICOs are used by startups to get around the rigorous and regulated capital-raising process required by venture capitalists or banks. (Frankenfield, 2018)

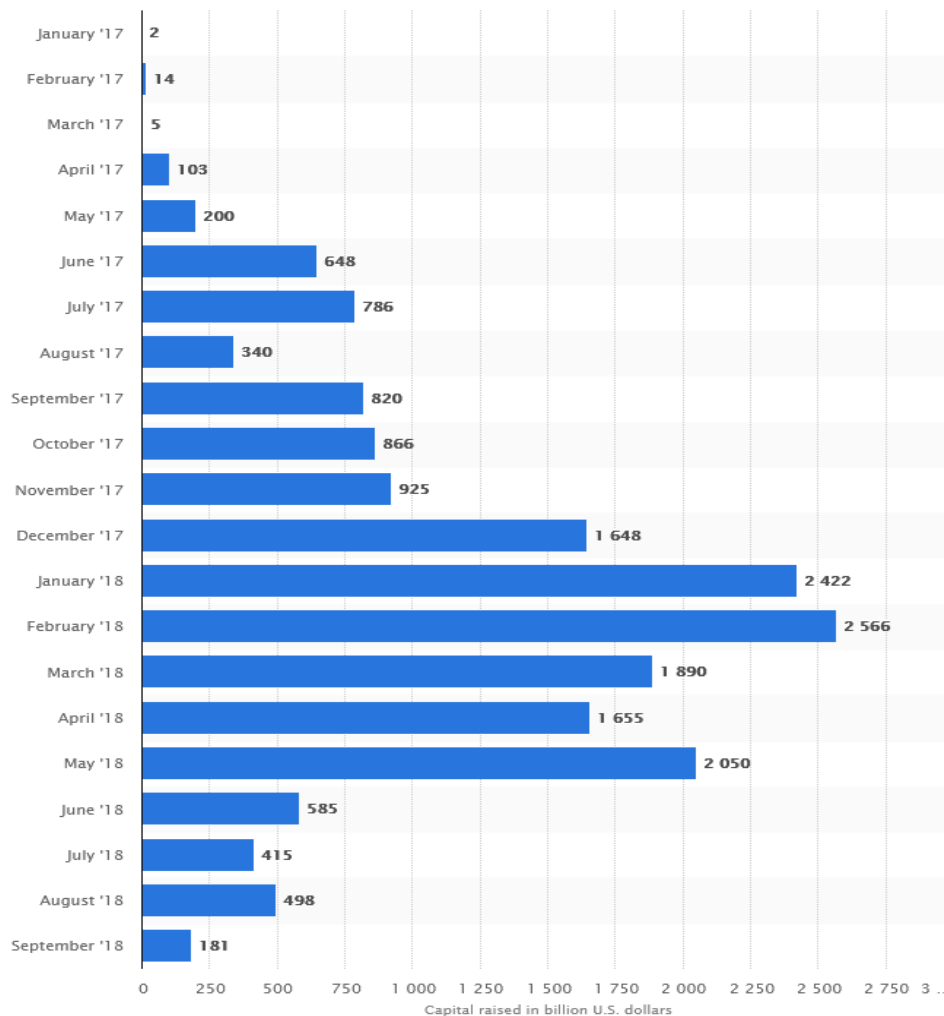


Figure 9: Total funding raised by Blockchain Initial Coin Offerings (ICO) worldwide

Source: (Blockchain ICO projects, 2019)

The statistic chart from statista.com presents the total funding raised by Blockchain initial coin offerings from January 2017 till September 2018. The amount raised by ICOs peaked in February 2018, amounting to 2.6 billion United State dollars (see figure 9). So, the amounts of money accumulated by ICOs at this period proves that initial coin offering becomes an innovative way of raising capital in the 21st century. However, ICOs are largely unregulated therefore the amounts begin declining (see figure 9) from the second part of 2018. The security token offering (STO) comes in replacement, offering legal obligations for investors. Simply put, STO is upgraded ICO, which protects the rights of the investor.

4.2.2 Types of Token

With time many new and different types of Blockchain projects were invented. The creation and growth of Ethereum gave birth to the term “token” which soon became a universal term for all currencies. Token represents a digital asset built on an existing Blockchain. Token classification is quickly becoming one of the most important subjects in Blockchain. It will determine how companies are formed and how assets are traded in the years to come. Depending on the application and functions of different tokens, they were divided into different categories.

Currency token

This is the classic cryptocurrency we referred to earlier (look back to Chapter 2). Bitcoin is an obvious example. These kinds of tokens are meant to be spent on the many and varied daily transactions of life. Nowadays, Overstock, Microsoft, Expedia, and Amazon are among the growing number of retailers who let you buy stuff with Bitcoin. Currency tokens are the best representation of a decentralized online alternative to government-controlled fiat currencies. (Coin Crunch, 2018)

Utility Tokens

These tokens are designed to be used for a purpose, usually within the application/platform for which they are developed. The most common use of a utility token is a payment option for purchases or for running a smart contract within the platform. Utility tokens are released by a company to provide their users with a mechanism to pay for a new company product or service, which has been developed on the Blockchain technology. It is usually beneficial to buy utility tokens during the ICO sale since the tokens during the ICO are offered at a significantly lower price than the market rate.

Security tokens

Security tokens are Blockchain investment products which don't give any ownership in the underlying company, but which do take value from the company. A security token takes its value based on some metric related to the company's performance. As the company thrives, its token gains value and investors can sell for a profit. Security tokens are limited by specific federal laws and rules of stock trading. (Reed, 2019)

Equity Tokens

Equity tokens are, in a very real sense, 21st-century stocks. An equity token represents a share in the underlying company. As with any stock purchase, holders literally own their given

percent of the total enterprise. They are entitled to a portion of the company's profits and a right to vote on its future. The only significant difference between an equity token and a traditional stock is the method of recording ownership. A traditional stock is logged into a database and can be accompanied by a paper certificate. An equity token records corporate ownership on a Blockchain. (Reed, 2019)

5 BLOCKCHAIN AS A POTENTIAL TECHNOLOGY FOR MODERN MARKETS OF ECONOMY

Blockchain's benefits of enhanced security, improved traceability, increased efficiency and speed of transactions could be useful in various industries and sectors. The technology's potential makes many government leaders and CEOs of companies are actively exploring its uses.

5.1 Potential uses of Blockchain technology applying to public sector organizations and markets.

In this section, I design potential directions where Blockchain based applications can be used to improve the functionality of the Public Institutions and Markets.

5.1.1 Banking

Banking remains to be the main area for various Blockchain based smart contract use cases. Any possible asset, such as a fiat currency (legal tender whose value is backed by the government that issued, ex: EUR or USD) or property can be represented in the form of tokens and consequently traded on a Blockchain. ING Dutch multinational Bank one of the financial organizations that exploring Blockchain technology for increasing the quality of their services.

Mortgage services

Mortgage agreements are complex as many details are included in them such as the income of the mortgagee, credit score as well as outgoings. In order to go ahead with mortgage loans, it is extremely necessary to carry out the checks on these details. This process often goes in the hands of intermediaries and third parties which makes it lengthy and troublesome for the lender as well as the loan applier. Using smart contracts in this situation is beneficial due to multiple reasons. The most important being the elimination of the middlemen to avoid any lengthy process and confusion. Moreover, all the details can be stored in one location which is always accessible by both parties. (Pratap, 2018)

Clearing and settlement processes

Banks can also use smart contracts to streamline clearing and settlement processes. The smart contract can take over the onerous administrative task of managing approvals between participants, calculating trade settlement amounts and then transferring the funds automatically

once the transaction embedded within the smart contract has been verified and approved. (Liyanage, 2018)

Delay-tolerant micropayments

Delaying in micropayments can be solved by blockchains too. Blockchain tokens can be used as a replacement for fiat currency to enable payments in environments with limited or intermittent connectivity. All transactions store in a Blockchain during disconnection periods. Bank updates the fiat currency accounts based on the Blockchain entries. (Liyanage, 2018)

5.1.2 Land title registration

As publicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. The smart contract can provide automation, shared access to information such as title deeds and land registry records. (Liyanage, 2018) A decentralized, standardized system for land registration records could reduce the number of intermediaries required, increase trust in the identity of transacting parties, increase process efficiencies, and decrease time and cost to process (White, 2017).

Several countries are undertaking Blockchain based land registry projects. The Republic of Georgia cemented a deal with the Bitfury Group to develop a Blockchain system for property titles that allowing citizens and companies to use a smartphone application to acquire and transfer property titles within a short period of time and at limited cost (Cheng, 2017). Most recently, Sweden announced it was experimenting with a Blockchain application for property titles (What is Blockchain Technology? A Step-by-Step Guide For Beginners, 2019).

5.1.3 Voting

Using Blockchain to record votes in an election is more tamperproof than existing digital and traditional voting methods (Cheng, 2017). For instance, the smart contract can validate voter criteria, log vote to the Blockchain, and initiate specific actions as a result of the majority vote (Liyanage, 2018).

Potential solutions are currently working to blend secure digital identity management, anonymous vote-casting, individualized ballot processes (for example, a vote token), and ballot casting confirmation verifiable by the voter (White, 2017). The BoardRoom is now the existing platform using the concept for voting inside enterprises.

5.1.4 Healthcare

In the healthcare industry, the use cases of Blockchain technology are huge, ranging from digitalizing the medical records to patient matching and identification for distant cooperation.

Electronic Medical Records

Personal health records could be encoded and stored on the Blockchain with a private key which would grant access only to specific individuals (What is Blockchain Technology? A Step-by-Step Guide For Beginners, 2019). Plenty of projects directed on managing personal medical records of patients have been created. Among examples are BitMark, CareChain, HealthCombix, and others.

Population health data access

A smart contract can be used in that system to make the system more reliable and automated. Using Smart contract human can write some term and condition which could be applied once data are collected. Then it will execute these smart contracts and trigger corresponding events. (Bhabendu, 2018) In this area, the most well-known projects are Hyperledger, BlockchainHealth which bring together people and their doctors able to control them distantly.

Patient matching and identification

Blockchain based smart contracts can provide a platform to share patients' information between different organizations It can help in finding donors all around the world and speed up transferring the needful organs, either to deliver necessary medicaments or help in time for sick people (Liyanaage, 2018). Several projects are already in preparation like Hyperledger, Accenture.

5.2 Conditions for Blockchain success

Blockchain technology is still very new. For instance, according to the social survey made in section 6.1 about 40% of humans haven't heard about Blockchain and related applications (see figure 12). Nevertheless, technology has plenty of room to grow and develop, but like any innovation, it's crucial to get initial support at the beginning. Key conditions for Blockchain success are designed.

Educational Institutions and Communities of Talent

Great computer science schools can lead to successful Blockchain innovation ecosystems. The National University of Singapore, ETH Zurich, Stanford University, the University of Toronto, York University and the University of California are among the ones who provide Blockchain program. Highly educated populations are an important factor for innovation to

take root in any given jurisdiction. It's crucial to initiate a national brain gain rather than brain drain. (Tapscott, 2016)

Government Support and Regulatory Environment

One of the most important things that government can do is to be model users of the technology itself. Government initiatives that fund innovation directly will have the highest benefit in the future. China's government is already investing billions of dollars into Blockchain development. Canada in its turn also has put a billion dollars into projects with a Blockchain component, meanwhile, Israel pours in Blockchain startups daily.

Still, governments can help as well as impede innovation. Thus, neither overregulation nor no-regulation is rational. Free for all jurisdictions countries like Ukraine will run into heavy problems. However, banning Bitcoin, ICOs, and cryptocurrency exchanges as many countries do, will hurt innovation for decades. (Tapscott, 2016) Furthermore, the great question is how digital assets should be taxed. So, if the governments provide supportive regulations, it will definitely help Blockchain innovations.

Incubators and Corporate Leadership

Innovation is nurtured in environments established exclusively for this purpose. For instance, in Toronto incubators (such as MaRS or OneEleven) have provided an auspicious climate in which Blockchain entrepreneurship can flourish. Regions with incubators have an automatic advantage over the ones who don't have any. Besides, centers of Blockchain innovation very often have close ties with established business communities. In areas where corporate entities manifest a curiosity and market positioning as innovators, Blockchain developments can especially thrive. (Tapscott, 2016)

6 PUBLIC PERCEPTION OF BLOCKCHAIN TECHNOLOGIES

Awareness of Blockchain technology in society is crucial for its future development. As any innovation needs time to become widely used, at first Blockchain must become publicly known. The biggest thing that people can do for the technology it starts using it. So, in this Chapter, I analyze the attitude of people towards Blockchain and its applications. The second part deals with the analysis of Cryptocurrency trend and shows the reason for general public interest.

6.1 Analysis of social survey towards Blockchain

The social survey aims to gain a better understanding of Blockchain prevalence. The survey reveals how Blockchain based technologies are perceived in 2019. This online survey was carried out via Google forms approximately between 11 February and 1 April 2019. 826 respondents of different ages were surveyed.

What is your gender?

82 ответа

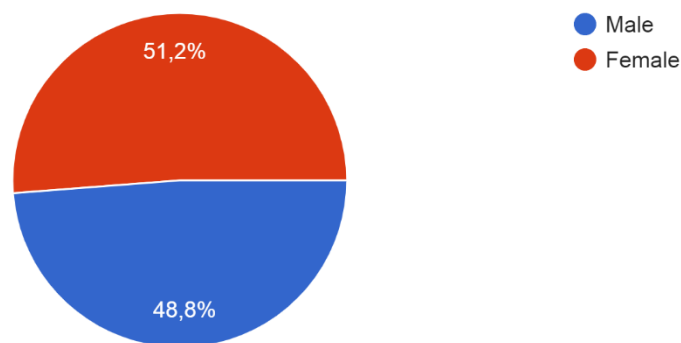


Figure 10: Gender of survey participants

Source: google forms based on own data

The first question was about the gender of the participants. According to the diagram, (see figure 10), the number of men (51,2 %) who took part in the survey is almost equal to the figure that represents the number of women (48,8 %).

How old are you?

82 ответа

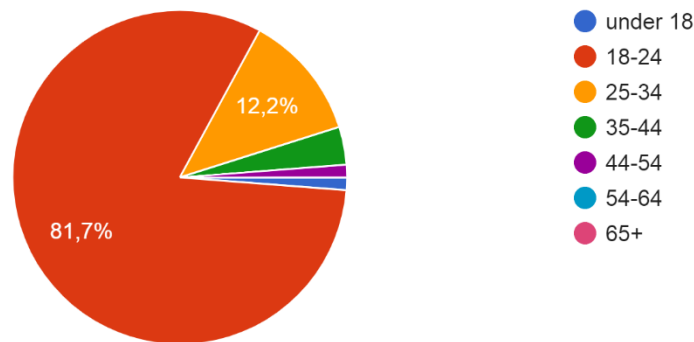


Figure 11: Age of respondents

Source: google forms based on own data

People of different ages have participated in the survey (see figure 11). The majority are students between 18-24 years (81,7%). Then, the young adults (12,2 %) show an interest in the survey about Blockchain based technologies as well. Just a couple of persons (3,7%) from the age 35-44 answer the questions. Besides, some teenagers (1,2%) and 44-54 years old humans (1,2%) give their answers too. To sum up, most of the surveyed people belong to Z generation, the ones who have grown in the era of digitalization with a smartphone in their hands as a basic toy.

Have you ever heard of Blockchain technology?

82 ответа

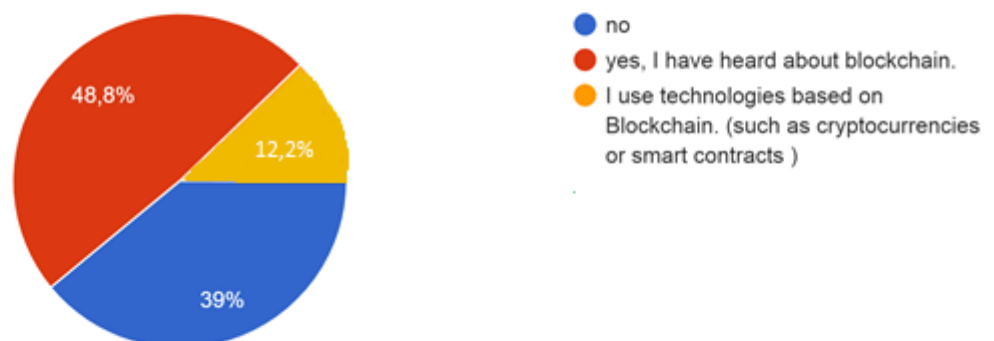


Figure 12: Blockchain technology prevalence

Source: google forms based on own data

Almost half of participants (48,8%) answer that they “I have heard about Blockchain”. Of course, simply having heard of Blockchain, perhaps in the media, is not the same as understanding it or using it. However, around one in ten (12,2%) respond “I use Blockchain based technology”. So, altogether that’s more than 60 % of surveyed are familiar with technology and it’s a good prevalence for the Blockchain.

Would you use Blockchain based technologies for?

826

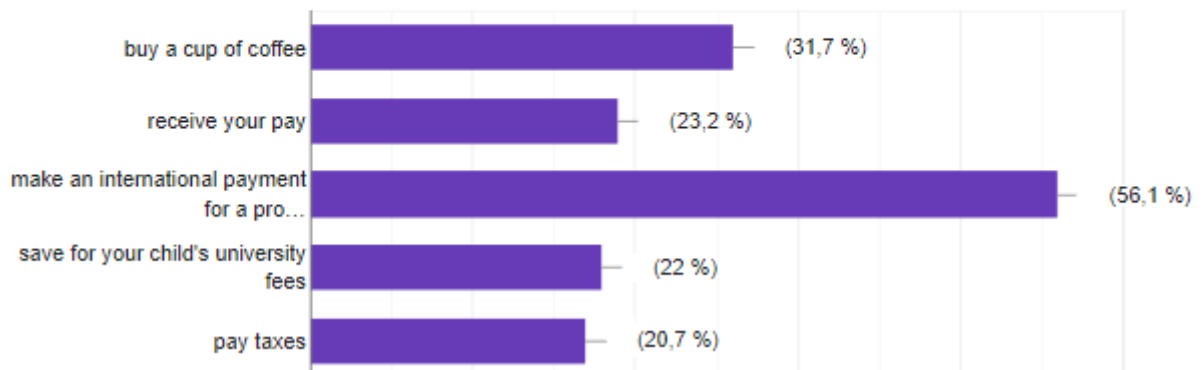


Figure 13: Well-known applications for future users of Blockchain based technologies

Source: google forms based on own data

International payments (56,1%) and small purchasing (31,7%) are the most popular option among respondents. Hence, both are a more suitable solution for cryptocurrencies (such a Bitcoin) – the first application of Blockchain technology. Only 23, 2% of the surveyed people would opt to receive their salary through Blockchain technologies and 20,7% of people would pay taxes relying upon Blockchain. In this case, mentioned above functions are better implemented by smart contracts– another application of Blockchain. For instance, when salary day comes, the smart contract executes on its own and provides the output like transferring of amounts by corresponding smart tokens.

On this basis, I claim that participants do believe in the wide application of Blockchain in form of cryptocurrency as a complement to government-issued money. In other words, they tend to see the prospect of the creation of the new digital currency in that. At the same time, they aren’t so trusting in relation to another significant Blockchain application known as a smart contract. The reason may be the shallow awareness of potential use or lack of hype comparing to cryptocurrency.

6.2 Analysis of Cryptocurrency trend

According to the high ratings of respondents who see cryptocurrency as a promising Blockchain based technology (see figure 13), I provide the chart of a cryptocurrency trend and estimate the reasons for general public interest.

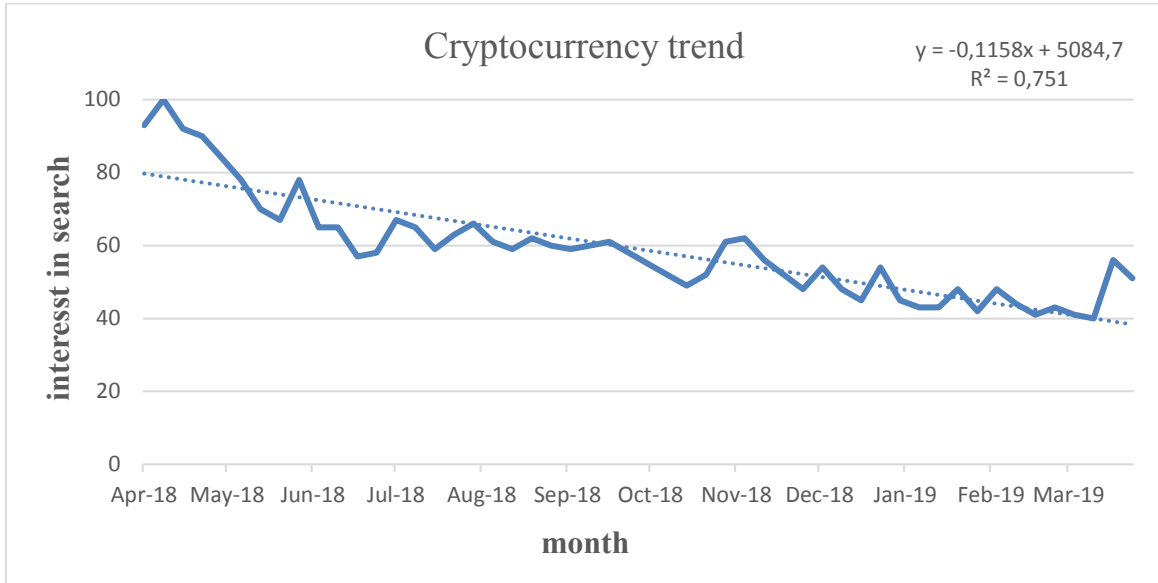


Figure 14: Cryptocurrency trend

Source: own processing

The chart represents the relative interest in the search by keyword "cryptocurrency" in the period between 15 April 2018 and 7 April 2019 (see figure 14). A value of 100 represents the highest popularity of the term.



Figure 15: Bitcoin Price Index

Source: own processing

Figure 15 illustrates the volatility of Bitcoin price in the United State dollars in the same period from April 2018 until April 2019. Consequently, based on the value of the Pearson correlation coefficient 0,858 that shows a significant correlation at the 0,01 level (see figure 16), it becomes obvious that the Cryptocurrency trend and Bitcoin Price Index are significantly dependent. In other words, it means that the Cryptocurrency trend curve gradually falls proportional to Bitcoin price dropping. This points to the fact, people are interested in cryptocurrencies when they can earn on the volatility of cryptocurrencies such as Bitcoin.

| | | Correlations | |
|----------------------|---------------------|--------------------------|-------------------------|
| | | Cryptocurrency _trend | Bitcoin_Price_ Index |
| Cryptocurrency_trend | Pearson Correlation | 1 | ,858** |
| | Sig. (2-tailed) | | ,000 |
| | N | 52 | 52 |
| Bitcoin_Price_Index | Pearson Correlation | ,858** | 1 |
| | Sig. (2-tailed) | ,000 | |
| | N | 52 | 52 |

** . Correlation is significant at the 0.01 level (2-tailed).

Figure 16: Correlation between Cryptocurrency trend and Bitcoin Price Index

Source: own processing

CONCLUSION

The aim of this thesis was to define the concept of Blockchain technology and determine how Blockchain can improve the functionality of modern markets and public institutions. The technology's potential makes many government leaders and CEOs of companies are actively exploring its uses. Blockchain and related applications have a huge capacity to solve existing problems in various industries starting from banking and healthcare and ending with voting and land registrations processes. Blockchain benefits of greater transparency, enhanced security and increased efficiency of transactions have a huge potential to reshape processes of trading real estate, organizing supply chain, providing insurance services, sharing energy resources and many others.

Another objective of this work was to analyze the general public perception of Blockchain technology and its applications. Awareness of Blockchain technology in society is crucial for its future development. As any innovation needs time to become widely used, at first Blockchain must become publicly known. The biggest thing that people can do for technology - start using it. Accordingly to the social survey made in section 6.1, about 60% of the surveyed people are familiar with the technology. Moreover, 12% of them even use the related application based on Blockchain (such as cryptocurrencies or smart contracts) and it is a good prevalence for the Blockchain.

In this work were designed conditions for Blockchain success. Blockchain technology is still very new. However, technology has plenty of room to grow and develop, but like any innovation, it's critical to get initial support at the beginning. Government support, corporate leadership and provision of Blockchain programs by educational institutions, can provide a favorable climate in which Blockchain technology will flourish.

BIBLIOGRAPHY

- BHABENDU, Kumar Mohanta and S Panda SOUMYASHREE, 2018. An Overview of Smart Contract and Use Cases in Blockchain Technology. *ResearchGate* [online]. October 2018 [cit. 2019-04-17]. DOI: 10.1109/ICCCNT.2018.8494045. Available on: https://www.researchgate.net/publication/328581609_An_Overview_of_Smart_Contract_and_Use_Cases_in_Blockchain_Technology
- BIGMORE, Rosemary, 2018. A decade of cryptocurrency: from bitcoin to mining chips. In: *The Telegraph* [online]. [cit. 2019-04-17]. Available on: <https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/>
- BLOCKGENIC, 2018. Different Blockchain Consensus Mechanisms. In: *Hackernoon* [online]. November 24, 2018 [cit. 2019-03-04]. Available on: <https://hackernoon.com/different-blockchain-consensus-mechanisms-d19ea6c3bcd6>
- BUNJAKU, Flamur, 2017. CRYPTOCURRENCIES – ADVANTAGES AND DISADVANTAGES. *Journal of Economic* [online]. [cit. 2019-03-08]. DOI: 336.743:004.031.4. Available on: <http://eprints.ugd.edu.mk/18707/1/Cryptocurrencies.pdf>
- BUTERIN, Vitalik, 2015. State Tree Pruning. In: *Ethereum Blog* [online]. June 26, 2015 [cit. 2019-03-22]. Available on: <https://blog.ethereum.org/2015/06/26/state-tree-pruning/>
- COIN CRUNCH, 2018. Guide to Crypto Token Types. In: *Hackernoon* [online]. [cit. 2019-04-07]. Available on: <https://hackernoon.com/guide-to-crypto-token-types-6ce04edaba72>
- CURRAN, Briann, 2019. What are Oracles? Smart Contracts, Chainlink & “The Oracle Problem”. In: *BLOCKONOMI* [online]. Jan 30, 2019 [cit. 2019-04-18]. Available on: <https://blockonomi.com/oracles-guide/>
- FRANKENFIELD, Jake, 2018. Initial Coin Offering (ICO). In: *Investopedia* [online]. Dec 20, 2018 [cit. 2019-03-29]. Available on: <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>
- FRANKENFIELD, Jake, 2018. Proof of Elapsed Time (Cryptocurrency). In: *Investopedia: Virtual currency* [online]. April 4, 2018 [cit. 2019-03-19]. Available on: <https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp>
- GLOBAL LEGAL RESEARCH DIRECTORATE STAFF, 2018. Regulation of Cryptocurrency Around the World. In: *Library of Congress* [online]. June 2018 [cit. 2019-04-22]. Available on: <https://www.loc.gov/law/help/cryptocurrency/world-survey.php#eu>
- HACKER, Philipp and Chris THOMALE, 2017. Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. *Ssrn* [online]. 30 Nov 2017 [cit. 2019-03-28]. Available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820
- CHENG, Steve, Matthias DAUB and Axel DOMEYER, 2017. Using blockchain to improve data management in the public sector. In: *McKinsey* [online]. February 2017 [cit. 2019-04-19]. Available on: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector>
- CHEN, James, 2019. Initial Public Offering - IPO. In: *Investopedia* [online]. Mar 13, 2019 [cit. 2019-03-29]. Available on: <https://www.investopedia.com/terms/i/ipo.asp>

- KOSINSKI, John R., 2018. Ethereum Oracle Contracts: Setup and Orientation. In: *Developers* [online]. [cit. 2019-04-18]. Available on: <https://www.toptal.com/ethereum/ethereum-oracle-contracts-tutorial-pt1>
- LIYANAGE, Madhusanka, 2018. The Use of Smart Contracts and Challenges. In: *ResearchGate* [online]. [cit. 2019-04-09]. Available on: https://www.researchgate.net/publication/328230865_The_Use_of_Smart_Contracts_and_Challenges
- MASSESSI, Demiro, 2018. Public Vs Private Blockchain In A Nutshell. In: *Medium* [online]. Dec 12, 2018 [cit. 2019-04-16]. Available on: <https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f>
- NAKAMOTO, Satoshi, 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. [cit. 2019-03-19]. Available on: <https://bitcoin.org/bitcoin.pdf>
- OSETSKYI, Victor, 2018. What Is Smart Contracts Blockchain And Its Use Cases in Business. In: *Medium: Existek* [online]. [cit. 2019-04-08]. Available on: <https://medium.com/existek/what-is-smart-contracts-blockchain-and-its-use-cases-in-business-271a6a23cdda>
- PRATAP, Mayank, 2018. Everything You Need to Know About Smart Contracts: A Beginner's Guide. In: *Hackernoon* [online]. Aug 29, 2018 [cit. 2019-03-27]. Available on: <https://hackernoon.com/everything-you-need-to-know-about-smart-contracts-a-beginners-guide-c13cc138378a>
- REED, Eric, 2019. Equity Tokens vs. Security Tokens: What's the Difference? In: *BITCOINMARKETJOURNAL* [online]. [cit. 2019-04-07]. Available on: <https://www.bitcoinmarketjournal.com/equity-token/>
- STACHER, David, 2018. *Regulation of Initial Coin Offering (ICO)*. Master's Thesis. University of Basel. Supervisor Dr. Aleksander Berentsen.
- SWEZEY, Matt, 2017. What is a Smart Contract? In: *Medium* [online]. June 2017 [cit. 2019-04-17]. Available on: <https://medium.com/pactum/what-is-a-smart-contract-10312f4aa7de>
- TAPSCOTT, Don, 2016. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World*. New York: Penguin Books. ISBN 9781101980149.
- THE LINUX FOUNDATION, 2018. Blockchain: Understanding Its Uses and Implications. In: *EdX* [online]. [cit. 2019-03-06]. Available on: <https://www.edx.org/course/understanding-blockchain-and-its-implications>
- TSCHORSCH, Florian and Burn SCHEUERMANN, 2016. *Bitcoin and beyond: A Technical survey on decentralized digital currencies* [online]. [cit. 2019-04-16]. Available on: <https://eprint.iacr.org/2015/464.pdf>
- VARSAMIS, Evan, 2018. What Is the Future of Crowdfunding and ICOs? In: *Forbes* [online]. Mar 27, 2018 [cit. 2019-03-29]. Available on: <https://www.forbes.com/sites/theyec/2018/03/27/what-is-the-future-of-crowdfunding-and-icos/#5fb512687a5a>

VIGNA, Paul and Michael J. CASEY, 2015. *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*. New York: ST. MARTIN'S PRESS. ISBN 978-5-00117-128-7.

WHITE, Mark, Jason KILLMEYER and Bruce CHEW, 2017. *Will blockchain transform the public sector? Blockchain basics for government* [online]. In: Deloitte University Press [cit. 2019-04-19]. Available on:

https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf

XU, Jennifer J., 2016. Are blockchains immune to all malicious attacks? *ResearchGate* [online]. [cit. 2019-04-17]. DOI: 10.1186/s40854-016-0046-5. Available on:

https://www.researchgate.net/publication/311568850_Are_blockchains_immune_to_all_malicious_attacks

Ethereum Development Tutorial, 2017. In: *GitHub* [online]. 19 Oct 2017 [cit. 2019-04-16]. Available on: <https://github.com/ethereumproject/wiki/wiki/Ethereum-Development-Tutorial>

What is Blockchain Technology? A Step-by-Step Guide for Beginners, 2019. In: *Blockgeeks* [online]. March 1, 2019 [cit. 2019-03-18]. Available on: <https://blockgeeks.com/guides/what-is-blockchain-technology/>

Blockchain ICO projects: funds raised worldwide 2017-2018, 2019. In: *Statista* [online]. [cit. 2019-03-29]. Available on: <https://www.statista.com/statistics/804748/worldwide-amount-cryptocurrency-ico-projects/>

Cryptocurrency Regulations Around the World, 2018. In: *ComplyAdvantage* [online]. Nov 1, 2018 [cit. 2019-04-21]. Available on: <https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/>

What is Ethereum (ETH)? In: *Ethos* [online]. [cit. 2019-04-16]. Available on: <https://www.ethos.io/what-is-ethereum/>