Blockchain History:

A Comparison of the Three Generations of Blockchain

By

Miroslav Mitráš

Submitted to

Central European University - Private University

Department of Economics and Business

In partial fulfilment of the requirements for the degree of Master in Economic Policy in Global Markets.

Supervisor: Tomy Lee

Vienna, Austria 2021

Abstract

The market capitalization of cryptocurrency market has risen 10 times during last year to highest point of around 2 trillion American dollars. While prices of all cryptocurrencies are rising, Bitcoin's, dominance can reach even 80% of the market capitalization. Is Bitcoin's blockchain technology so advanced that no new cryptocurrency can bring any improvement, or is the dominance on the market caused by first mover advantage? The thesis deals with the comparative analysis of selected cryptocurrencies which represents 3 generations of blockchain technologies Bitcoin, Ethereum and Cardano. The comparison is performed in terms of blockchain technology, consensus algorithms, transactions, decentralization, and historical development. The thesis evaluates the current state and potential of selected cryptocurrencies in terms of prospective investment, but also their possible implementation in various sectors of economy and government.

Market data are used as primary sources. Due to lack of research in this area and pandemic situation secondary sources include various internet book publications, pieces of research but also non-academic sources. This thesis is among the first research papers which points out. the 3rd generation of cryptocurrencies, represented by Cardano, brings faster and cheaper transactions which are more energy efficient. In terms of blockchain technology Cardano provides higher adoption in private, non-governmental and governmental sectors across the board.

Keywords: Blockchain, cryptocurrency, Bitcoin, Ethereum Cardano, smart contract, decentralization, Proof of Work, Proof of Stake

Table of Contents

List of Figures

Tables

List of abbreviations

ADA – Cardano token

BTC – Bitcoin token

dApp – decentralized application

DeFi – decentralized finance

DLT – Distributed ledger technology

ETC – Ethereum Classic

ETH – Ethereum token

NFT – non-fungible token

P2P – peer to peer

PoS – Proof of Stake

PoW – Proof of Work

Introduction

In a world of constant development and daily improvements in technology, would you invest in something what was created in 2009 and cannot be updated? Would you invest in Apple if they would have stopped with development after first iPhone? Most people, when they hear the word "cryptocurrency", they tend to associate it with Bitcoin, and it seems like in cryptocurrency space first mover advantage is enough to dominate the market. Researchers and financial analysts are pointing out issues with Bitcoin such as speed of transactions, centralization of miners, cost of transactions and high energy consumption, but only few researchers are focusing on cryptocurrencies which already solved these issues and offer more possibilities with their blockchain.

The aim of this thesis is to present the history of blockchain technology, cryptocurrencies, and to offer a comparative analysis of 3 generations of blockchain technology which are represented by Bitcoin (BTC), Ethereum (ETH) and Cardano (ADA). The purpose is to demonstrate the development and true potential of second and third generation of blockchain, and to prove that this technology is not just about finance or payments systems, but that it can revolutionize the world we live in. Governments can use blockchain to fight against corruption, get rid of bureaucracy, make faster payments to the people in need. The private sector is able to use blockchain technology in all sectors across the board, from gambling, investment, transportation, supply chain to smart homes, computer programs and phone applications, possibilities are unmeasurable.

The area of 3rd generation of blockchain is highly under-researched, most of the academic studies are written about Bitcoin or cryptocurrency as a payment method, tax frauds or risky

investment. That is why in this thesis is also used non-academic sources, which illustrate the possibilities of blockchain.

In this thesis methods of synthesis and logical analysis of literature and various publications concerning the development of cryptocurrencies and blockchain were used. Using these two methods, I was able to conduct the necessary research, which served as a source of information for comparative analysis which was applied when comparing selected indicators and price movements related to the above cryptocurrencies.

The thesis is divided into 2 main chapters. The first chapter is devoted to the characterization of blockchain and its key features, it continues with a demonstration of different consensus algorithms mainly focusing on Proof of Work and Proof of Stake algorithms and their differences. The next parts are dismantling the tokenization, smart contracts, decentralized applications, and transactions. The next section interprets the evolution of cryptocurrencies, and it also specifies the growth of Bitcoin, Ethereum and Cardano. Their price movements and cryptocurrency cycles are explained in next part. After that, the thesis will focus on cryptocurrency exchanges, wallets, and regulations around the world. The last part focuses on summarizing of comparison of 3 generations of blockchain technologies namely Bitcoin, Ethereum and Cardano it points out main differences between them.

1. Blockchain

The first section of this chapter will clarify the pivotal knowledge about blockchain technology, what key features it contains, and the differences between proof-of-work and proof of stake. The next section will analyze the tokenization of blockchain, decentralization and usage of smart contracts to execute decentralized applications, decentralized finance, and non-fungible tokens. Some of these subsections will contain comparison of Bitcoin, Ethereum and Cardano against each other as examples of blockchain technology in algorithms, tokenization, decentralized applications, transactions, and transactions fees.

1.1 What is blockchain

1.1.1 Characteristics

Distributed ledger technology (DLT) is a term used to describe a technology that allows records to be shared on a computer network. Blockchain is type of DLT, which is based on existing technologies that have been combined in an innovative way to enable the creation of decentralized and distributed records in a peer-to-peer network (i.e., a "user-user" network). For other blockchain properties, transactions are stored in blocks chronologically. Digital signatures guarantee authentication, non-repudiation, and integrity of transactions in distributed ledger technology (National Bank of Slovakia/ NBS).

The blockchain consists of blocks, block is a file that contains data related to the network. The block records all recent transactions that are not yet part of any block. Each time a block is "completed", a path is created to the next block in the blockchain. A block is therefore a permanent warehouse or "book" records which, once entered, cannot be changed, or deleted. Because of that, the block is practically impossible to hack. If it were possible, it would be the same case as if a bank robber got behind the bank counter and stole not only money but also all bank records (Frankenfield, 2020).

The block in the blockchain consists of two parts - head and body. Head consist of number of software version, time, hash of previous block, root hash of Merkle tree, goal of current difficulty, and the own hash number – nonce. The body of the block also consists of two parts: the transaction counter and the transactions themselves. The maximum number of transactions that a block can contain depends on the size of the block and the size of each transaction. Blockchain uses an asymmetric cryptographic mechanism to verify transactions (Zheng et al, 2018). Gupta (2017, p. 14) specifies that

> *each block contains a hash (a digital fingerprint or unique identifier), timestamped batches of recent valid transactions, and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain. The method renders the blockchain tamper-evident, lending to the key attribute of immutability.*

Figure 1 simplifies what Gupta (2017) describes, each of these blocks contains their own hash, they also refer to previous block's hash and hash of transaction. It also helps to clarify the immutability, any change would have to be written in another block and it would have been visible for anyone else, so if transaction is an error or corrupted, a new transaction will be issued and error will be reversed.

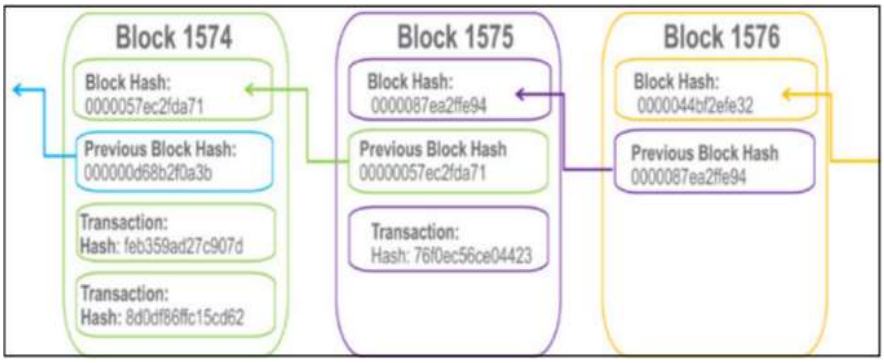

Figure 1 Blockchain stores transaction records in a series of connected blocks *Source: Gupta (2017)*

The so-called "Genesis block" is called the start block or block 0. This block does not contain a reference to any other previous block. The Genesis block is structurally different from other blocks in the system. It is usually verified by the authors or developers of the platform or

cryptocurrencies. The next block in the system already contains a reference to block 0. With the help of a back reference to the previous blocks, it is possible to proceed to this first block at any point in the chain. According to available information, the genesis block on Bitcoin was created in January 2009 and was rewarded with 50 bitcoins, which are, however, unusable (Terracoin, 2019).

1.1.2 Key features of blockchain

In general, according to Zheng et al. (2018) the fundamental properties of blockchain includes decentralization, stability, controllability, and anonymity. Decentralization means that the blockchain transaction is performed between peers in network (P2P) without authentication by a central agency which helps to significantly reduce server costs (development and operating costs) and reduce performance problems at central server. Stability requires that transactions are acknowledged and recorded in blocks distributed throughout the network, it is almost impossible to manipulate transactions since each block must be authenticated by validators (nodes or miners), any falsification could be easily detected. Anonymity brings possibility of communication with other users via automatically generated address, and each user can generate several addresses to prevent identity theft, no private information is used. Controllability improves security, once a transaction in the blockchain network is verified and recorded, users of that block can easily verify and trace previous records through nodes in the distributed network. Every transaction can be tracked in the blockchain.

Figure 2 draws attention to different views on key features of blockchain technology Euromoney.com (2021), underlines that blockchain is programable, and gives chance to smart contracts to execute decentralized application. Moreover, blockchain is distributed and unanimous in validation of transactions and security, which is on the first place.

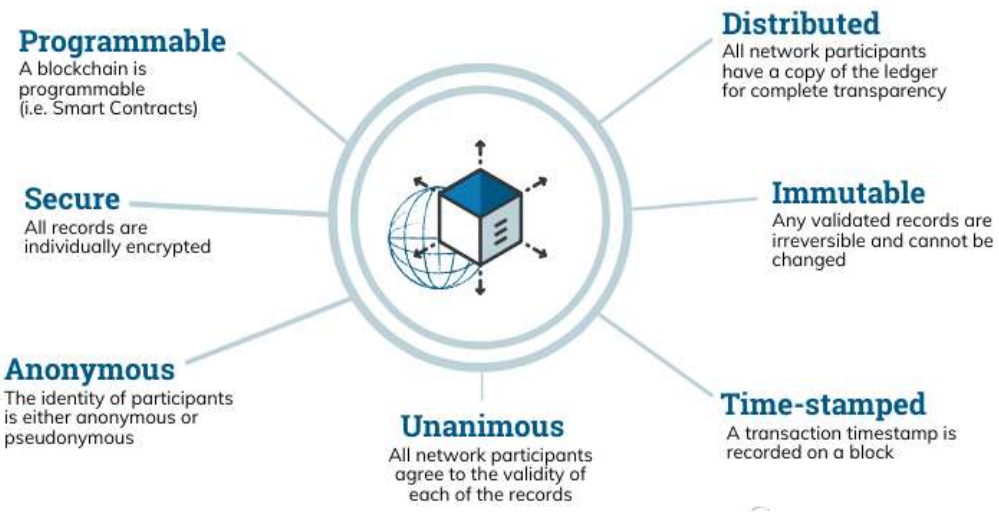

Figure 2 Key features of blockchain, *Source: Euromoney.com*

1.2 Blockchain consensus algorithms

Consensus algorithms are set of rules which are ensuring stability and security of the blockchain technology, on the other hand, also the way how the transactions are authenticated. There are different types of consensus algorithms such as Proof of Work, Proof of Stake, Delegated Proof of Work, Proof of Capacity or Proof of Authority (Zihrli, 2020). This section clarifies the most used consensus algorithms in blockchain, Proof of work and Proof of stake, their pros, and cons and how these algorithms work on Bitcoin, Ethereum and Cardano.

1.2.1 Proof-of-work (PoW)

In blockchain, transactions are not processed one by one, but in blocks of more transactions. Transactions are considered authenticated when the miner adds block to the blockchain (BinanceAcademy, 2020). In a PoW consensus, participants must solve the so-called "cryptographic puzzles" in order to add new blocks to the blockchain. Process of solving algorithms is commonly called "mining" and participants are “miners” (Natarjan et al, 2017).

These "cryptographic puzzles" as Lee (2018) explains consist of previous information recorded on the blockchain and new transactions that will be added to the new block. The complexity of mining increases with each new block added, which means that the PoW mechanism requires

a number of computing devices and techniques, which consumes an enormous amount of electricity.

The extraction of most cryptocurrencies works on the principle of PoW. The most well-known cryptocurrencies used by this system are Bitcoin and Ethereum.

1.2.2 Proof of stake (PoS)

The proof-of-stake (PoS) system works on a different principle than the PoW system. Entities involved in confirming a transaction are validators, not miners, they are not competing between each other, but they are picked randomly to forge the block (AcademyBinance, 2020). As Hill (2020) tells participants can delegate their asset to the stake pool, a place where participants are allocating their asset and they are receiving the rewards for it. People who started the stake pool, and mostly own the highest stake in it are called validators or stake pool leaders, they are receiving rewards and fees for validation of the block.

The Validator's stake is called the pledge chance to validate next block depends on a pledge. The higher the proportion of pledge the higher its chances to validate next block. In PoS, it should be noted that the fees are not high and there are no electricity costs, so in the end it is cheaper (Daniel & Green, 2018).

1.2.3 Differences between Proof of Work and Proof of Stake

Security is pivotal while comparing these two algorithms, both have different approaches to solve this issue. Long range attacks are main questions, in PoW attacker's goal would have been to create new chain of blocks and act maliciously to create or steal more blocks, which would mean bigger rewards for the attacker. Attacker would have to own 51% of all miners, but blocks are created with such big amount of computational power for which is needed big investment to the computational infrastructure and electricity. This is possible just for the country level or the richest people in the world. After all of this, and the recreation of all the

blocks in blockchain, which would have taken more than 100 years, then the user can try to "hack the system", and if it all would go right other validators can just stop the transaction. (Fairweather, 2016).

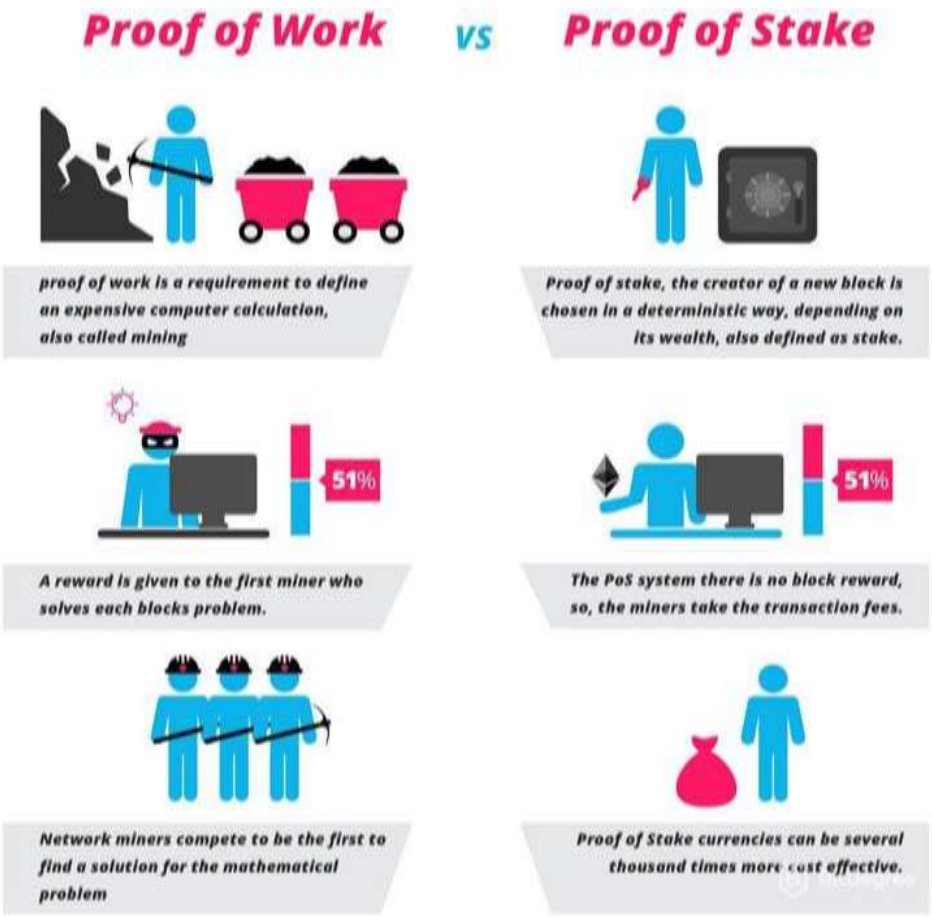

Figure 3 Difference between Proof of work and Proof of stake *Source: Medium.com*

To clarify, as is illustrated above in Figure 3, PoW as mining the gold, it is still getting harder and harder, you need big machines and high energy consumption, but you are still not sure how much gold you will find. PoS is like minting coins, just validators can mint the coin, then add into the blockchain and everyone can use it. If chosen validator will create damaged coin or does not create coin on time this validator will be punished.

Bitdgree (2021) emphasizes that in PoS validators are chosen randomly, no need for competition, very little computational and electricity power is needed, compared to PoW. Here the attacker would have to buy, 51% of all the coins in a market and stake his coins, without

ability to withdraw asset for some amount of time to become a validator. Buying the asset would create asset appreciation, this would make the asset more and more expensive, while buying it. And if the attacker would go through all of this and would be randomly selected to forge next block which would be malicious, other validators will find out, and they will not validate the transactions and attacker will lose all the invested money.

It looks like PoS is making rich people rich, since they are able to buy higher amount of the asset and stake it, but conversely PoW gives bigger chances to rich miners with better computers, software and people who are able to pay higher bill for electricity. PoS stake pools can be limited and after some amount staked, their rewards get reduced, and participants are encouraged to stake their asset in smaller stake pools (McElrath, 2020). However, PoS requires much more programing with higher chance to make mistake in software building the stake pools, rules for validators and users and solving security issues.

All things considered, for creators of an asset is easier to create an online space for using PoW, because of security issues with less coding. Conversely PoS requires much more coding and making sure everything will run smoothly and it is also programmed to punish for attacks. It is much easier to create chain of blocks in PoW, but if everything is prepared well beforehand, than for the users and environment it is much easier to use Proof of Stake rather than Proof of Work. (Rosic, 2020).

Table 1 Proof-of-Work vs Proof of stake

Proof of work	Proof of stake
No asset needed to get started, block rewards	Need to buy asset and stake and asset to start
Uses up so much electricity that it is bad for the environment	Much better for environment, not even 90% of energy needed for PoW
Tested security and decentralization approach	New approaches to security and decentralization
Relatively easy to implement	Harder to implement, high initial investment into the software, easier to run
Big investment to buy special computer hardware, which is needed to mine, high electricity bill for miners	No need for big investments in electricity of computers for validators

Source: Ethereum.org

Table 1 accentuates the differences between PoW and PoS. In earlier stages of blockchain Proof of Work was preferred by most of the people in this sector, but now in 2021 Proof of Stake is on much higher level; offers faster transactions speed and improved security. It is just matter of time until PoS will become the most used algorithm in the blockchain space. However, Bitcoin will always stay the same since it cannot be changed.

1.2.4 Comparison of algorithms

Cardano

Ouroboros protocol provides the same security as Bitcoin's PoW, for a very little impact on environment and electricity consumption. Digiconomist (2021) estimates that in May 2021 Bitcoin's electricity consumption was around 113,000 GWh/per year, if it stays on same consumption level for whole year, it will equal the year electricity consumption of Netherland. Ethereum is also still using PoW and it is estimated that it uses 43,000 GWh/per year or the yearly electricity consumption of Hungary. On the contrary, Ouroboros is using just 0,156 GWh/per year on 100 stake pools, as Costello (2020) highlights. In April 2021, Cardano has around 1,600 stake pools in operation (adapools.org, 2021), which would mean around 0,25 GWh/per year of energy consumption.

I think that with rising price of BTC and ETH and the numbers of transactions still rising, at the end of 2021 electricity consumption of ETH and BTC can even triple from numbers in May 2021.

Latest Hydra update on Ouroboros, has focused on high transaction output, low latency, and minimal storage per node. It enabled Ouroboros to scale horizontal, adding nodes, putting more pressure on hardware and electricity consumption. More nodes (heads of Hydra) will make confirmation of transactions faster, this will allow Cardano blockchain to scale to the levels of global payment systems (Costello, 2020).

Integrity is provided by applying combinatorics and game theory. Ouroboros is secure if 51% of ADA, Cardano token, is staked with trustworthy participants, which is achieved by random selection, and it is being still evolved by thorough security analysis. Protocol rewards participants for the participation in ADA token, for either operating stake pool (nodes) or delegating a stake in ADA (delegators). Ouroboros randomly distributes control over the network to nodes, proportionally, by the size of their stake pool. Every stake pool has one leader/validator, they are rewarded for adding block to the chain (Cardano.org).

Ouroboros sorts time into epochs and slots, 1 epoch lasts 5 days, and 1 slot lasts for 20 seconds, each slot one block is created and added to the blockchain, which translates to 21,600 blocks per one epoch (cardano-foundation.gitbook.io).

Ethereum 2.0/ Ethereum Casper

The start of Ethereum Casper was supposed to happen until end of 2021, it supposed to bring PoS and burning the Ethereum (ETH) tokens, which would mean that ETH would become deflationary asset. Casper would allow anyone who stake at least 32 ETH to become a validators. This person will be chosen to validate the new block proportionally to the staked amount in the stake pool. But for Casper nothing is clear yet, its security and efficiency is still

unproven, we can just guess how it will look like and how it will behave. (BinanceAcademy.org).

Due to this issue, Capital.com (2021) states that Cardano blockchain is far ahead of Ethereum, which has still problems to implement PoW, while Cardano already has hundreds of stake pools and it is an extremely scalable network.

In a comparison of Bitcoin, Ethereum and Cardano helped to demonstrated that PoS is considerably more energy efficient. Cardano's Ouroboros, incentivizes the creation of stake pools, but disincentivizes stake pools with higher investment in it improved decentralization, and security.

On the other hand, PoW, which is used in Bitcoin and Ethereum, incentivizes miners who have better hardware and software, which gives them higher chance to "solve the puzzle" and to receive the reward and fees for authenticating the transactions: PoW gives higher chances to rich miners or makes miners to centralize in miner pools which creates centralization and security threats.

1.3 Tokenization and token standards

1.3.1 Tokenization

The last section portrayed consensus algorithms Proof of work and Proof of stake; it looked at the differences and similarities between them and how these two systems are implemented into the blockchain. The next section outlines tokenization and token standards.

Tokenization was like learning a new language without the syllabus, Token standards gave syllabus to the developers, they allowed blockchain tokens to communicate and transfer knowledge and wealth in easier way, than it was before having. Tokens are already the outcome of how we use the language. This section will differentiate tokenization and token standards,

then talk about standards on Ethereum and native tokens on Cardano. According to Narayan and Tidström (2020, p. 4) tokenization is

> *converting the rights to an asset into a digital token, which facilitates the trading of those assets and permits micropayments. Tokens can represent a wide range of assets and can be transferred without any involvement of centralized entities and can be traded on digital currency exchanges without borders.*

By contrast, Di Angelo and Salzer (2020) illustrate the characteristics of tokens from another point of view as digital asset which can be managed by smart contracts and used withing decentralized applications. Tokens are different from cryptocurrencies, tokens have their own distributed ledger, rather than used for transactions or as a store of value as cryptocurrencies. The features of a token from economic point of view can be found in Sunyaev et. al. (2021, p. 1)

> *a token is a sequence of characters that serves as an identifier for a specific asset (e.g., a personalized usage rights) or asset type (e.g., a cryptocurrency). The abilities to represent assets in form of digital tokens on a decentralized digital platform and to assign ownership of these assets to agents in a fraud-resistant way can help to reduce drawbacks related to trusted third parties.*

The real value of tokenization is pointed out in Tian et al. (2020), where it is underlined that using blockchain and tokenizing valuable assets have higher spectrum of use than most people can imagine, from finance, real estate to energy transition, renewable energy or sectors like infrastructure and intelligent transportation. All of this is thanks to token standards, which helped to create framework blueprint developers. According to Reiff (2020) standards helped to define common rules and made it easier for developers, since they do not need to start from scratch, they can follow the rules of token standards about supply, transactions, and access data of the token standard.

1.3.2 Comparison of tokenization

Ethereum

The most widely used and most general token standard is ERC-20, Di Angelo and Salzer (2020, p. 4) claim that “it provides basic functionality to transfer tokens, as well as allows tokens to be

approved so they can be spent by another on-chain third party". At least six mandatory and three optional functions as well as two events must be implemented to meet the requirements. Another token standard which is explained by Di Angelo and Salzer (2020) is ERC-721, it enables to track ownership of distinguishable assets, non-fungibles (NFTs), compliance of 10 mandatory and 3 optional functions is required. The next important standard is ERC-1150, which provides management of any fungibles and non-fungible tokens in one single contract, and it allows to transfer multiple tokens at once. Compliance of 6 mandatory and 4 optional functions is required.

Cardano

Cardano choses a native token approach, which means that tokens created in Cardano ecosystem are not using smart contracts and another token standard, but they are created on ADA token. "Native token is an accounting system defined as part of the cryptocurrency ledger and enables tokens to be transacted with (tracked, sent and received). This eliminates the need to use custom code or costly smart contracts" (Harrison, 2020).

No need for smart contracts is also highlighted in Vinogradova (2020), because Cardano works as a multi-asset ledger which supports fungible, non-fungible tokens, and mix of both. The author stresses out affordability, where there is no need for gas transfers fees between peers in Cardano Ecosystem as for Ethereum's smart contracts, plus the security is also on higher level and unified process of creating tokens which will reduce mistakes and bugs in the system.

1.4 Decentralization

Previous section formulated tokenization, tokens, and different types of approaches to tokenization for Ethereum and Cardano. The next section depicts the possibilities of created tokens, smart contract which are executing tokens and different types of decentralized application which can be created.

1.4.1 Smart contracts

Tokens are executed and driven via smart contracts, which Tian et al. (2020, p. 6) defines as

> *self-executing and self-enforcing contracts with agreements approved by all parties and written into code" and also "credible transactions through smart contracts are traceable and can be verified without involvement of external third parties or a centralized authority" on the other hand "Terms and conditions are specified, and smart contracts are accessible and visible, thereby bringing transparency, accuracy and trust to involved parties. There is no need for human intervention everything is automated, fast, and secure.*

Sanghavi et al. (2018) highlights that smart contracts are substituting paper contracts, but they are much more secure and transparent while minimizing formalities and are held on decentralized ledger based on blockchain. Ethereum.org (2021) outlines smart contracts as "a vending machine: if you supply it with enough funds and the right selection, you'll get the item you want. And like vending machines, smart contracts can hold funds". Figure 4 portrays graphical representation of smart contract.

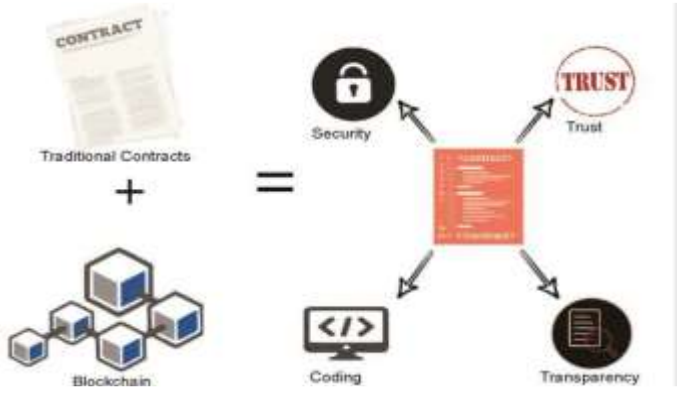

***Figure 4 Graphical representation of smart contract**, Source: Sanghavi et al. 2018.*

1.4.2 Decentralized applications - dApps

Decentralized Applications (dApps) are formulated by Muller et al. (2020, p. 1) as "pieces of software operated by different independent organizations and interact with each other over the Internet to achieve a common business goal". DApp has backend of the application decentralized on peer-to-peer network, while frontend code (interface that people can see) is working and looking just like any other centralized application (Zeichman, 2021).

Features which differentiate dApps from Apps are interpreted in Raval (2020): *Open source* – users have access to the code of the dApps, they can help to improve it, users have also access to their data and dApps are taking internet as a common denominator, not as a closed chain of silos.

Internal currency – dApps will create a token – an appcoin which user will need to use to work within the dApp, such as in Bitcoin miners are paid in transaction fees (user can buy, sell, and send Bitcoin). User can get appcoins from initial signing up or selling their data for advertisements etc...

Decentralized consensus – no trust requirement, nodes/miners approve the transactions; if the block is rightly approved, they get paid if; not they are punished as everywhere in blockchain.

No central point of failure – data is stored across all nodes, if one node fails, other ones will continue, that is why dApp cannot be shut down

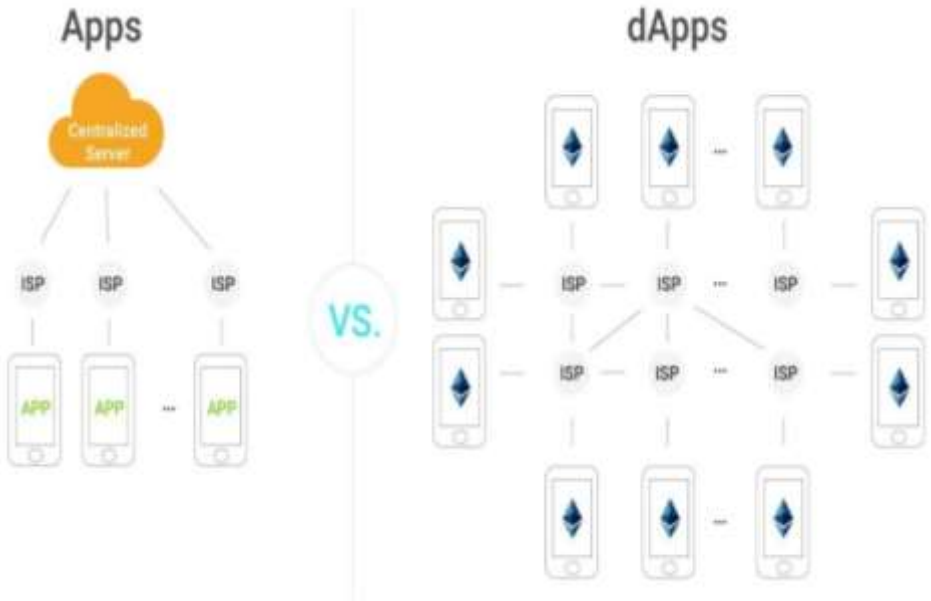

Figure 5 ***Difference between centralized and decentralized applications*** *Source: Hackmoon.com, 2018*

As is shown in Figure 5, there is no central point of failure, instead of central point there are many nodes all around the world which are making sure dApp works without issues and all of these nodes, approve transactions without central point of trust.

Other important benefits of dApps are zero downtime – when a smart contract is deployed on dApps it works automatically; resistance to censorship – no one can block users to work with dApp; complete data integrity – thanks to cryptography data is immutable and indisputable and trustless computation, as we know from smart contracts (Zeichman, 2021).

1.4.3 Decentralized Finance – DeFi

What is the difference between centralized and decentralized finance? Napoletano (2021) portrays DeFi as system which uses blockchain to process the transactions either in fiat or cryptocurrencies. Conversely, Sandner (2021) outlines that DeFi

> *is an umbrella term encompassing the vision of a financial system that functions without any intermediaries, such as banks, insurances, or clearinghouses, and is operated just by the power of smart contracts. DeFi applications strive to fulfill the services of traditional finance (also coined as Centralized Finance, or just CeFi) – but in a completely permissionless, global and transparent manner.*

The Decentralized Finance (DeFi) or Open Finance movement takes that promise a step further. Imagine a global, open alternative to every financial service you use today — savings, loans, trading, insurance and more — accessible to anyone in the world with a smartphone and internet connection (Coelho-Prabhu, 2020).

Table 2 Comparison of DeFi and Traditional finance

DeFi	**Traditional finance**
Person is holding money	Companies holding your money
You control where your money goes and how it is spent	You must trust companies not to mismanage your money, like lend to risky borrowers
Transfers in minutes	Transfers in days
Transactions are anonymous	Activity coupled with your identity
Open to anyone	First need to apply to use services
Market is always open	Employees needs break, not working 24/7
Transparency – anyone can look at data and inspect how system works	You cannot ask to look at financial history of financial institutions

Source: Ethereum.org

Table 2 summarizes differences between Centralized and Decentralized finance. Decentralized finance helps people to own their money, they are in control, transactions are much faster, safer and anonymous. Anyone can check the blockchain data about DeFi company, their investments

and loans, there are no borders for DeFi anyone can make account from any country in the world. As it was shown during the economic crisis in 2008, people are not owning their money, they do not know where their bank is investing it. Conversely, banks want to know everything about the person even to open the account and it is worse when borrowing or lending money (Ethereum.org).

The possibilities of DeFi are outlined in 3rd chapter of this thesis, for example why it is better than centralized finance and some examples from real world of blockchain investing and borrowing.

1.4.4 Non-Fungible tokens - NFTs

This section will draw attention to differences between fungible and non-fungible tokens. Fungible equals to interchangeable, for example 1 Bitcoin for 1 Bitcoin, same with dollars or any other cryptocurrency or currency. Non-fungible is something unique, one of a kind or limited edition, non-fungible tokens, can represent things such as paintings, videos, fan collectibles as pokemon or football player cards etc. (Boscovic 2021, Sharma, 2021). However, Samarbakhsh (2021) points out that "a non-fungible token (NFT) is a digital file with verified identity and ownership", Sharma (2021) elaborates and adds that

> *NFTs are digital representations of assets and have been likened to digital passports because each token contains a unique, non-transferable identity to distinguish it from other tokens. They are also extensible, meaning you can combine one NFT with another to "breed" a third, unique NFT.*

There are many types of NFTs, which are in different prices zones, from 1usd to millions of dollars in ETH[1]. Goldman (2021) underlines the legal point of view on NFTs and characterize them as

[1] More information about markets of non-fungible tokens can be found on a webpage www.nonfungible.com. There you can find market for collectibles, art, game characters or land in online worlds. Prices of NFTs can go as high as thousands of ETH tokens.

intangible or incorporeal personal property – that is, an item that cannot be touched or held but has some level of value assigned to it. Like other personal property, it can, at least in theory, be bought, sold, gifted, bequeathed, mortgaged, used as collateral, and levied.

1.4.5 Comparison of Decentralization

Ethereum

From my chosen blockchains only Ethereum has functional smart contracts on their side, that is why this blockchain is the most used for NFTs, DeFi and dApps and more people are using it, higher market cap and that means higher price for 1 ETH token. Some of the Ethereum DeFi tokens are Aave, Compound and Oasis which are for lending and borrowing cryptocurrencies, another once are 1inch and Uniswap which work as a platform for swapping tokens. For trading and prediction are Polymarket and Augur, for investment Token set and PoolTogether other for payments are Tornado Cash and Sablier and for insurance is Nexus Mutual. On the other hand, almost all NFTs are for sale in ETH token (Ethereum.org, 2021).

Cardano

Smart contracts will arrive on Cardano during the spring of 2021 and with that also dApps, DeFi and NFTs. But at the end of April, Cardano announced the biggest partnership in history of blockchain Cardano Africa deal. In the beginning, 5 million students in Ethiopia will start to use Cardano and Atala prism (system for digital identity) to verify grade and monitor their performance. Cooperation with SingularityNet means investments into young Africans who are working on AI technology and building the future of robotics. Another cooperation will bring 100 000 people in Tanzania fast and cheap internet connection until end of 2021. And finally, Cardano in cooperation with COTI payment system, are preparing fast and free payment system for NGOs in Africa, and they will start with Save the Children in Rwanda, but it will be open for everyone (AfricaCardano.org).

Interoperability has brought decentralized applications and tokenization to the life. Ethereum in 2015 showed the real power of decentralization with their focus on smart contract, which

enabled creation of decentralized applications and platforms for non-fungible tokens. Creation of tokens is also possible on Bitcoin, on the other hand, Ethereum took the approach of token standards and gave software developers blueprint for the creation of either fungible or non-fungible tokens with emphasis on private sector, but it also shows that token standards approach is not as good in security or decentralization as native token approach which was adopted by Cardano. The third generation blockchain gives opportunity to all tokens created in their ecosystem for same security, transaction speed and all other benefits which has the native token of Cardano – ADA.

1.5 Transactions on blockchain

The previous section delineated smart contracts and how they work on dApps, NFTs and DeFi and different strategies of Ethereum and Cardano are deploying decentralized applications. The Next section will illustrate how the transactions on blockchain work and fees users need to pay for transactions on Bitcoin, Ethereum and Cardano.

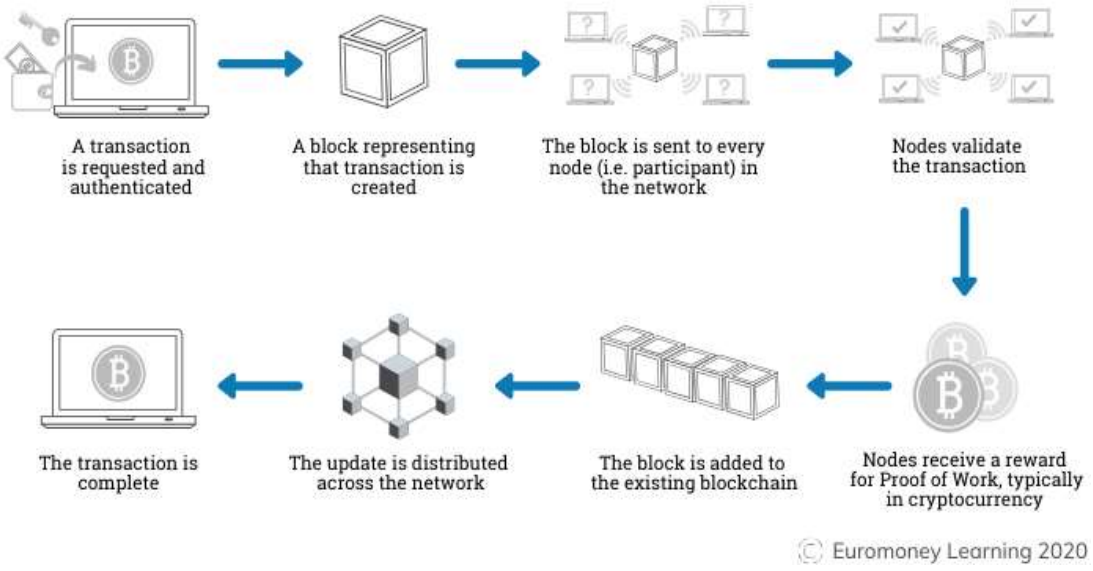

Figure 6 Transaction in blockchain *Source: Euromoney.com*

Figure 6 illustrates how the transactions on blockchain are processed. From requesting the transaction through validation, competition and nodes receiving the reward. The processing of transaction works almost the same on every blockchain the difference is in Proof-of-work and Proof of stake. This picture clarifies how it works on proof of work Bitcoin or Ethereum.

Satoshi Nakamoto (2009, p. 2) the founder of Bitcoin, specified transactions as

> *a chain of digital signatures. Each owner transfers bitcoin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.*

Boscovic (2021) simplifies how cryptography change transactions to series of random numbers which for people without public keys and private keys mean nothing, but people with keys can see the real transaction and they are able to authenticate and authorize the transactions.

Public keys, also called blockchain addresses, are random sequences of letters and numbers, they work like e-mail address, or username on social media accounts. Private key is also sequence of letters and numbers, but they work like passwords to your social media. Using Public and Private key authenticate/signs the transaction. When a transaction is signed, it needs to be authorized/approved before adding to the blockchain (Euromoney.com)

1.5.1 Comparison of Transactions

Specifically on Bitcoin and Ethereum, transactions must be authorized by miners on the blockchain. Miners do not mine transactions; they mine blocks which are collections of transactions. Ethereum is slightly faster than Bitcoin: it normally processes 10-15 transactions per second, while Bitcoin processes 3-5 per second, as a comparison, debit cards (Visa, MasterCard) are capable to process 40,000 transactions per second (Finextra, 2021).

On Cardano authorization is done by the validators/stakepool nodes, who are authorizing the transaction and due to Ouroboros system and Hydra update shifted Cardano's scalability to transaction speed of more than 1,000,000 per second (Costello, 2020).

By contrast, Bitcoin does not have interoperability function, which gives ability to exchange and make use of information sent via transaction, no smart contracts can be created on Bitcoin and that is why there are no dApps, DeFi or NFTs created on Bitcoin, but most of them are on Ethereum, while Cardano acquired this function in March of 2021 (McCall, 2021).

1.5.2 Comparison of transactions fees

Every transaction in blockchain cost fees, but they are calculated differently for Bitcoin, Ethereum and Cardano. In the next section I will explain why there are fees and how to calculate them.

Bitcoin

In Bitcoin, for each mined block miners receive incentives in form of rewards and fees. Anzollini (2019) highlights that in the future, transactions fees will have a pivotal role as an incentive for Bitcoin miners to continue mining. Conway (2021) continues to describe that every bitcoin cycle which is around 210,000 blocks, around 4 years long, this reward is halved, the reward for each block is currently 3,5 BTC, 1 block is mined every 10 minutes.

Every Bitcoin transaction has fixed size of the block 1,000,000 bytes, that is why the most profitable transactions are included in earlier blocks and are authorized first. Fee is measured in Satoshi per byte (1 Satoshi = 10^{-8} BTC). The average size of 1 transaction is 374bytes, the size of transaction is not derived from the amount of BTC in transaction (Anzzolini, 2021). Satoshi per byte depends on demand for transactions but also how long is user able to wait for transaction, exchanges and wallets are let users choose how much they want to pay for transaction. Waiting for authorization of transaction 1 hour can be around 40% cheaper that waiting just 20 minutes. (Buybitcoinworldwde.com, 2021).

As it is portrayed, fees are not high because of higher price of BTC, but when price of BTC is rallying more and more, people want to buy it and therefore high demand for transactions makes price of fees to rise.

The formula for calculation of fees is: Satoshis per byte multiplied by size of transaction in bytes which equals satoshis paid for transaction, for example

100 x 374 = 37 400 Satoshis/Sats

If a user wants to know price of the fee in USD, multiplication of Satoshis with current price of BTC is needed, for example:

1 Satoshi = 10^{-8} BTC, then 37 400 Sats = 0,00037400 BTC, if 1 BTC = 57 000 USD then 0,00037400 BTC x 57000 BTC/USD = 21,318 USD.

Most of the exchanges and wallets will already show users price for transaction in USD and you can just choose how much you are able to pay, it is easy and without the need for calculations.

Ethereum

Ethereum's platform use Gas to refer to the fee which is paid for transaction or execution of smart contract, the price is valued in Gwei, which is small fraction of ETH and it is used to pay miners together with rewards (2 ETH per block) to authorize the transaction. (Zeichman, 2021). As underlined by Tardi (2021) 1 Gwei = 1^{-9}, there are another denomination of ETH, but Gwei is the easiest to use at the moment, another once can be used if price of Ethereum will rise to higher price. Price of fee, same as in Bitcoin, is determined by supply and demand for transactions, but here miners can also decline to process the transaction if it did not meet their expectations (Frankenfield, 2021). Another view is from Tardi (2021) who interprets that Gas

fees are paid to compensate miners for their hardware and power consumption which is needed to process and authenticate the transaction on Ethereum.

Due to this, for simple transactions require 21,000 gas, but for executing smart contracts such as paying for insurance or borrowing money or betting can be even 1,000,000 gas. There is also gas limit per block, just 10,000,000 gas can be in one block of ETH. Gas is given by miners, but people can choose how much they are willing to pay per unit of gas, which is denominated in Gwei. From all of this, the formula for calculating gas price is: Gas consumed multiplied by gas price per unit (Conner, 2019).

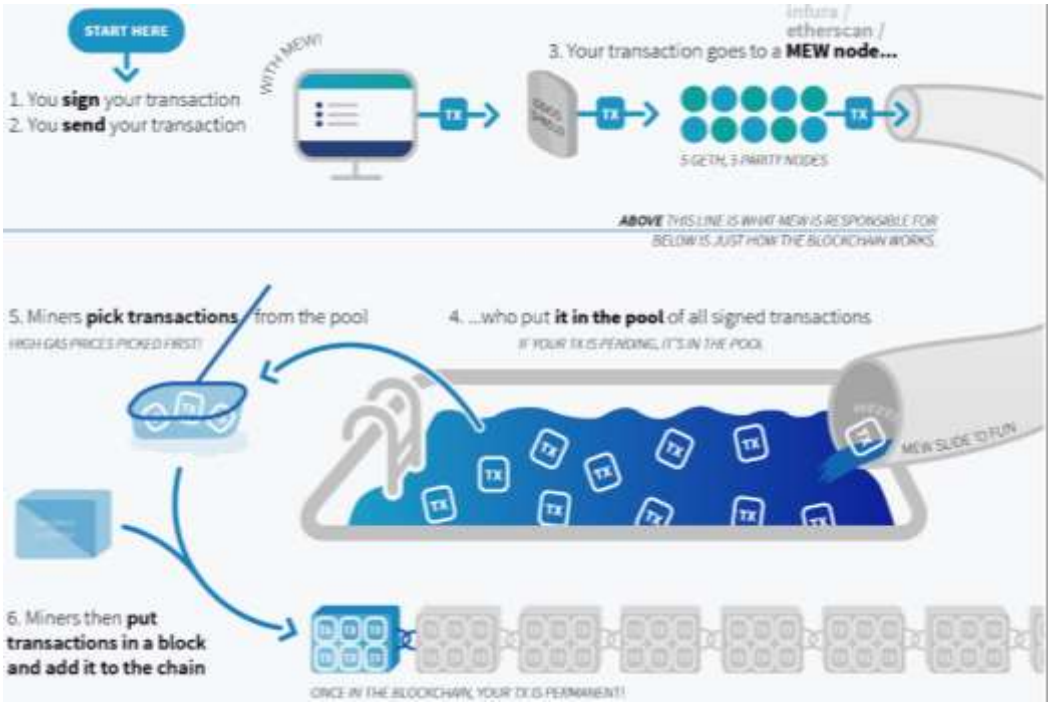

Figure 7 Transaction in Ethereum ecosystem *Source: Medium.com*

How are transactions in Ethereum ecosystem processed and the issue with gas limited is illustrated in Figure 7.The issues with gas limit and transactions prices are highlighted in (Connor 2019), where the price of fees rise because of high gas expenditure, and since for execution of smart contracts you need much more gas than for simple transactions, the higher

creation and usage of tokens for dApps, DeFi, NFTs is making transaction fees on Ethereum platform to rise, even though there can be low level of transactions of ETH. Since users are able to pay for smart contracts execution higher price than for simple transactions, smart contract users will be picked first and if you want to have your simple transaction made fast you have to pay higher price.

Since the Ethereum platform has the highest number of Defi, dApps and NFTs this is becoming a huge issue for Ethereum, which supposed to be solved by Ethereum 2.0, at the end of 2021.

Cardano

Cardano is using fees to cover processing and long-term storage cost of transactions. Here are fees distributed between all stake pool operators who validated the block during the 1 epoch and calculation formula is much easier than in BTC and ETH (Cardano.org, 2020).

The Formula for calculation has two constants or protocol parameters a/b, where parameter *a=0,155381 ADA,* is constant payable fee, not attached to anything and it is still the same. Parameter *b = 0,000043946 ADA/byte* which represents size of 1 byte in transaction, and with larger size larger storage and computational power is needed. The last one is a parameter *s* which represent size of transaction in bytes. Formula for calculation is $a + b \times s$ = transaction fee in ADA (Brunjes, 2017).

For example: If we know that average size of transaction in Cardano is 200 bytes, we can calculate the transaction fee: 0,155381 + 0,000043946 x 200 = 0,1641 ADA.

In Summer of 2021 when smart contracts will be fully functional, it will allow tokens to create dApps, DeFi and NFTs will be possible to make, Cardano will start with a Babel fees. This will allow users to pay fees in any token which is made in Cardano ecosystem or ADA, plus there will be possibility to bundle the transactions together, whether fungible or non-fungible or mixed, to save on transaction fees (Garg, 2021). This upgrade will also bring another

improvement, as Kiaiyas (2021) illustrates that stake pool operator/nodes will be able to create their own exchange rates for tokens created on Cardano ecosystem to ADA, but if exchange rate will be too high, users can change the stake pool.

Transaction speed and fees are essential question for blockchain technologies. It has been shown that PoS algorithm helps Cardano to create incomparably higher speed than Bitcoin or Ethereum can ever reach., as well as Cardano has fees which are just small percentage of the technologies which work on Proof of Work algorithm.

2. Comparative Analysis of Cryptocurrencies

The previous chapter concentrated on the features of blockchain where the main consensus algorithms, decentralization, tokenization, and transactions were used as a comparison between the 3 generations of blockchain technologies. This chapter will focus on evolution of cryptocurrencies, their exchanges, the different types of wallets, as well as on existing regulations around the world.

2.1 History

The emergence of cryptocurrencies is conditioned by the development of the world in which there is a high-speed exchange of information in the digital space. Users use cryptocurrencies worldwide, the mobility of their identity is considerable, and therefore one of the important aspects that are required in the digital environment is the security of transaction movement and security of payment. Thus, at the turn of the centuries, in the global digitized economy, there were doubts as to whether the effective maintenance and improvement of banknotes, which are subject to government oversight, lose their value due to inflation and are difficult to relocate.

The system that would meet the requirements was the introduction of the eCash currency in 1989. The creation of the eCash currency was supported by the owner of the company DigiCash system, David Chaun, a USA resident. The privilege of the eCash currency was encryption, which required the use of private and public keys. It thus created the basis that cryptocurrencies still use today. The main goal was therefore password-protected monetary transactions, which were not affected by a third party, i.e., other natural persons, legal entities, banks, or authorities. The eCash currency was popular among certain entities. After some time and due to inefficiency management, the company DigiCash system disintegrated. However, the asymmetric encryption that the system abounded remained active as a technology (Hulsink, 2003).

In early 1998, Adam Back introduced the HashCash system, Curran and Honan (2005) emphasize the principle of the HashCash system was already developed in 1992 by Cynthia Dwork and Moni Naor, who had previously worked with David Chaun. HashCash worked on the principle of verifying the work performed and was originally used to prevent spam e-mails. Therefore, when sending the e-mail, the sender's computer had to find the numbers specified by the HashCash system, while it took some time to search. This confirmed that the sender was sending one email, not spam.

This technology of verifying the work performed represented another shift in the formation of cryptocurrencies, it later led to the idea of "hashing the blocks" in Proof of Work algorithm by Satoshi Nakamoto.

Another shift in the development of cryptocurrencies was provided by the programmer Wei Dai in 1998, who developed the B-money technology. This technology used verification of work performed in connection without third-party tracking. The results were verified by a community that was connected to the network and the transactions, together with their record, were kept public. Transactions would be considered valid if sent to the network via an asymmetric encryption (Dai, 2018).

The creator of Bitcoin used this idea to create decentralized authentication of transactions by community of miners, who are authenticating the anonymous transaction on public blockchain.

In 1998, Nick Szabo created Bit Gold technology, in which a community of people participated in solving cryptographic tasks, where they published their results on an open record. An important element of this mechanism was the division of the process into smaller processes - time-stamped tasks. As a result of partial technologies and cooperation between these developers, the basic principles of the cryptocurrency protocol were described, i.e., a set of

rules intended for communication between the end points of a communication system (Szabo, 2005).

The use of Blockchain in Bitcoin is illustrated by book of accounts – the ledger. A ledger cryptographically encrypts stored information about the executed transactions of users. All transactions are public and therefore shared with all participants authenticated by miners. That is how Bitcoin avoids "double spending", the double use of a single transaction. For example: if someone has a banknote and a copy of this banknote, they can pay with them if the buyer does not find the copy invalid. However, in the case of Blockchain and Bitcoin, this is not possible, as all transactions are listed in the public ledger (Reiff, 2020).

After the long development, cryptocurrencies have the acquired structure, which is known nowadays, Frankenfield (2020) specifies that

> *A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.*

Royal (2021) stresses that many online shops are starting to accept cryptocurrencies as payment for their goods, companies are creating they own cryptocurrencies or tokens, for which their customers can buy goods from their shops. Conversely, crypto payments are still not mainstream and there is long way to go to be accepted by national banks or law makers. For the time being, it is just special feature, which shops use to attract customers.

Coinmarketcap.com (2021) which is the most referenced price tracking website for cryptocurrencies, records more than 5000 cryptocurrencies in May 2021. Market capitalization of all cryptocurrencies is 2,4 trillion dollars, with Bitcoin accounts for more than 50% of the market.

2.1.1 Comparison of development

Bitcoin

Satoshi Nakamoto (2008), the unknown inventor of BTC, never intended to invent a currency. Satoshi stated in its B12 Communication at the end of 2008 that it had developed an "Electronic Peer-to-Peer Cash System". Its goal was to invent an independent and fully digital cash system. It basically combined already existing principles, such as hash functions, asymmetric cryptography, or a P2P protocol.

Bitcoin is a digital currency that was created in 2009 and is the first decentralized cryptocurrency. As illustrated by Bradh (2020), its creation was preceded by a publication written in 2008, under the pseudonym Satoshi Nakamoto was signed. The author, whose identity is still unknown, states in the Bitcoin white paper that a simple peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without any financial institution.

Nakamoto (2008) argues that online commerce relies almost exclusively on financial institutions that serve as trusted third parties for processing electronic payments. While the system works well enough for most transactions, it still suffers from the internal shortcomings of a trust-based model. The author further argues that an electronic system based on cryptographic trust instead of trust is needed, which will allow any two willing parties to trade directly with each other without the need for a trusted third party. Baldwin (2018) explains that confidence in banks was the lowest during the financial crisis. Bitcoin was conceived in 2008 as an attempt to decrease reliability on government and banks. With Bitcoin, trust does not dissipate, but rather shifts. Confidence shifts from trust in banks or states to trust in algorithms and encryption software.

The solution proposed by Nakamoto (2008) starts with a timestamp server. The timestamp server works by creating a hash for that block of items that must be time-stamped and publicly

available so that everyone can access it. By the item block it is meant the requirements for the transactions to be performed. For example, one item contains the public key of the recipient, the number of Bitcoins and the digital signature of the previous owner. In the case of Bitcoin, as it is portrayed by Panda (2021) hash is a 64-digit hexadecimal number created using the Secure Hash Algorithm 256 (SHA-256), cryptographic hash function from an item block that has been stamped. The author further claims that the timestamp confirms that the data existed in time to reach the hash, in addition, each timestamp contains a previous timestamp in its hash that forms a string, with each timestamp amplifying the previous ones. In this way, a blockchain is created.

Bitcoin works like this until now, nothing can be changed, since its author is unknown, and all the issues which arose with Bitcoin's popularity - slow transaction speed and high fees, centralization of miners, as it was described in the previous chapter - are becoming issues which cannot be solved by anyone.

Bitcoin's code is open source, therefore other developers started to code their own improved clones of Bitcoin, such as LiteCoin, Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond, Bitcoin Atom or Bitcoin Private. All these coins are working on improving the transaction speed, lowering fees and decentralization but none of them is even close to popularity of original Bitcoin (Bazan, 2020).

Bitcoin can store value, or send money to another user in blockchain space, whereas; Ethereum and Cardano have more to offer in terms of tokenization and dApps.

Ethereum

Vitaly Dmitriyevich Buterin came up with a project in 2013 that talked about decentralized blockchain. But compared to Bitcoin, it was a more general use, not just for cryptographically secured financial transactions, but to solve more complex transactions. Buterin attempted to

create a blockchain, with interoperability, the function which gave blockchain understanding of smart contracts. For the first time in history of blockchain users were able to create decentralized applications and their own tokens through Buterin's programing language Solidity in 2015. (Coinmarketcap.com, 2021).

Ethereum has a capability that goes far beyond the pure P2P digital money equivalent of Bitcoin. Simply put, it is very similar to a smartphone operating system on which software applications can be built. The development of the Ethereum program is promoted and supported by the "Ethereum Foundation", a Swiss non-profit organization founded by the founders of Ethereum (Lewis, 2016).

In May 2016, Ethereum ecosystem faced an attack from a hacker who has found a loophole in the system and stole 3,6 million of ETC. Due to this unexpected event, the developers decided to make a radical update or in blockchain language "hard fork", – Tangerine whistle, in 2016 - from block 1 920 000 the Ethereum blockchain split and a new branch was created. Those who accepted these changes continued to Ethereum - ETH, the others remained on the old blockchain branch, which changed its name. at Ethereum Classic - ETC (Güçlütürk, 2018).

Another hard forks which have brought significant changes into the Ethereum ecosystem are Byzantium in 2017, which changed its mining reward from 5 to 3 ETH per block. Constantinople in 2019, started to prepare way for the Proof of Stake on Ethereum blockchain and optimized gas fees. In 2020, Ethereum started with staking for PoS, but it works just in Beta version. Beacon chain genesis set the rules for staking, at the end of 2020. The latest hard fork is announced to happen in July 2021, "London" hard fork will make Ethereum a deflationary asset, with every transaction on Ethereum blockchain, some part of the fee will be destroyed. The biggest hard fork is yet to come at the end of the 2021, Ethereum 2.0 or Casper. It will change Ethereum blockchain from PoW to PoS. this will bring faster and cheaper transactions, solve issue with centralization of miners and Ethereum will become much more

environmentally friendly, using less than 1% energy which is needed now to run the network (Ethereum.org).

Cardano

Cardano was launched in September 2017 by Charles Hoskinson, co-founder of Ethereum. Three organizations are responsible for development of Cardano: IOHK, Cardano foundation and EMURGO, just the third one is a for profit organization, the IHOK is working with academics – PhDs, to produce research based hard forks on Cardano (Conway 2021). The academic approach is also emphasized in Coinbureu.com (2018) which points out that Cardano is cooperating with Tokio Institute of Technology and University of Edinburg, who are working to bring smart contracts on Cardano platform, by using the Haskell coding language, due to its security. Coinmarket.cap (2021) depicts Cardano as Proof of Stake blockchain which has the goal to allow innovators to bring positive change in the world by using their technology, helping to create a society, which is fair, secure and transparent to everyone.

Cardano works with scientist, engineers, and developers to prepare the best updates possible, but first all updates are peer reviewed and improved if possible. Cardano's roadmap started in the autumn of 2017, and it consists of 5 eras. First was the Byron era, it was the beginning and the main target was to build the community, the fundamentals for the Cardano blockchain, and it allowed users to buy and sell ADA token in more than 30 cryptocurrency exchanges. The Shelley era has brought the decentralization – Proof of stake, it allowed users to stake their ADA token and earned interest, but also improved transaction speed, lower fees and help to reduce energy consumption.

The third phase is Goguen era. It brought smart contracts and decentralized applications, in the spring of 2021. Marlowe is the domain which will allow to create smart contracts even for non-programmers, with much easier settings then it is in Ethereum. With regards to sphere of

tokenization, as mentioned in section about Tokenization, Cardano will become a ledger with support for native tokens. Basho era, at the end of 2021 will bring improvements to the ecosystem, most importantly to transactions speed, interoperability, and scalability. The Voltaire era will bring power to the people – governance. People who staked Cardano will be able to participate in voting for improvements or price level of fees, Cardano will become self-sustaining blockchain (Cardano.org, 2021).

In summary, the foundation of cryptocurrencies started in early 1990s with different approaches to create decentralized currency. Bitcoin, the first blockchain based cryptocurrency, as a final version of this approaches was created in 2009 by Satoshi Nakamoto: reached the goal of decentralization and provides fast, cheap, and secure payments anywhere in the world. The second generation has improved the security and transaction speed, but also put spotlight on smart contracts and decentralized application. Next, the 3rd generation of blockchain-based cryptocurrencies understood that improvements are still needed to be made and Cardano has brought improvements across the board.

2.2 Cryptocurrency cycles

2.2.1 Price movement

The most influential events in cryptocurrency history are Bitcoin halvings. With the first approximately 18.5 million BTCs extracted in just ten years since the introduction of the BTC network just 3 million of BTC still remains to be mined. The BTC mining process, which rewards the miners with the BTC piece after successfully authenticating the block, adapts over time. When launched the mining reward was 50 BTC. A few years later (in 2012) it halved - to 25 BTC. In 2016, it halved again - to 12.5 BTC. On 11 May 2020, the remuneration was halved again to 6.25 BTC. Currently miners receive this reward when they succeed in their endeavors (Pantera Capital, 2021).

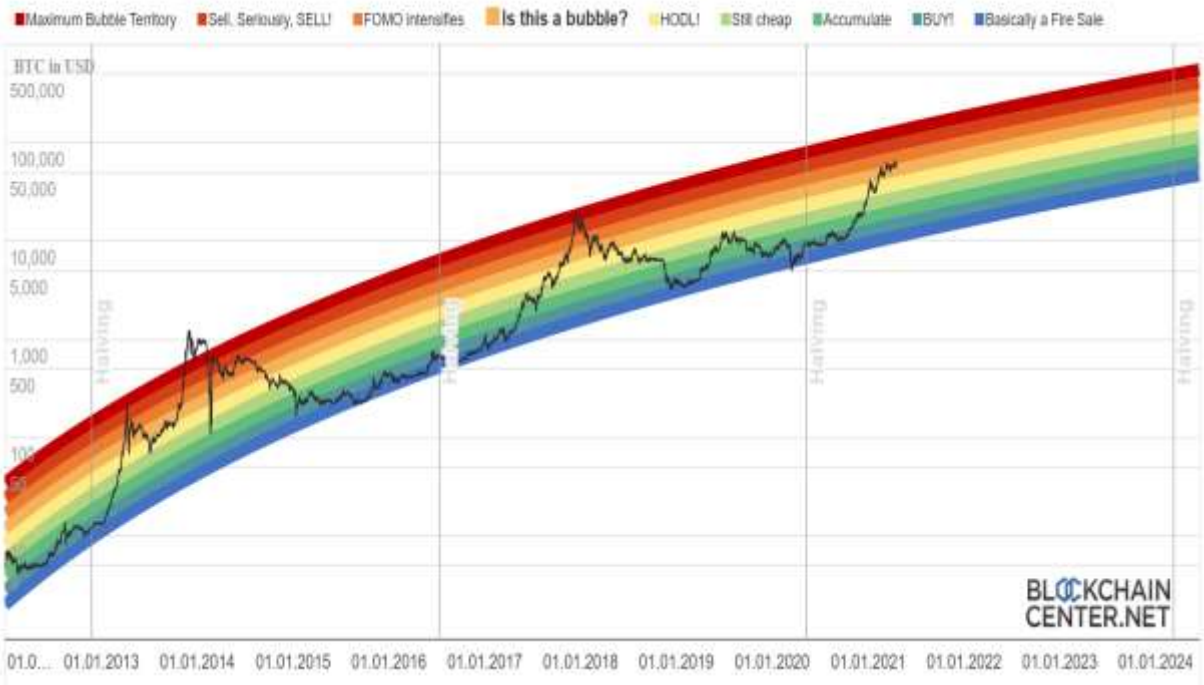

Figure 8 ***Rainbow chart of Bitcoin halvings*** *Source: BlockchainCenter.net*

The development of the price movement of Bitcoin is portrayed in a Figure 8. First halving happened in November of 2012; price went up from the bottom of 12 USD to 1150 USD in December of 2013. Second halving happened in July of 2016 when Bitcoin rallied from the 650USD price to almost 20,000 USD in December of 2017. The last halving happened in May of 2020, and bitcoin bottomed out at 3,200 USD in this cycle (Conway, 2021)

In May of 2021 BTC price is around 60 000 USD with the market cap of 1 trillion USD. From my personal point of view, Satoshi Nakamoto programmed Bitcoin to create cycles, and planned it so until 2140, when last halving will occur. Since the first top of the price happened 1 year and 1 month after the halving and the second top occurred 1 year and 6 months. This would bring us to the top of the cycle in 1 year and 11 months after the halving, which would be in April of 2022, if there is continuation in this pattern.

2.2.2 Altcoin season

Bitcoin is the leader of the cryptocurrency market, and most of the time it has more than 50% of market capitalization. During the top of the Bull run, as it happened in 2013 or in 2017,

Bitcoin had almost 80% of all market capitalization of cryptocurrency market, all other cryptocurrencies, or altcoins, are not moving or falling during this period (Jones, 2021).

But, when Bitcoin's market capitalization falls past 50%, altcoin season is occurring. Top 20 alctoins by market capitalization and then others are having massive gains, in few days their price can rise more than 10x. It is very rare situation, since most of the time when Bitcoin is falling all other coins are following the trend (Moore, 2021).

The next section will look at the price development of Ethereum and Cardano, both of them went through 1 full cycle and they are in the middle of their second cycle in May of 2021.

Ethereum

The biggest altcoin, Ethereum originated in the middle of 2015. During the first year of its operation on the market, it did not take much, because its price was at the level of 1-2 USD. In the middle of 2016, there was a slight increase in interest in the currency, as the price suddenly jumped to the level of approximately USD 10. Until the beginning of 2017, this price did not change much, but then in May 2017, the price reached the level of 400 USD.

After a slight stagnation, the price shot to the level of 1,500 USD per ETH on 9th January 2018, during the Altcoin season. In 2018, much like Bitcoin there was a great fall, until the halving in May 2020, where from the price around 100 USD, is now in May 2021 trading around 4,000 USD/ETH with a market capitalization of 450 bilion USD (Coingecko.2021). The evolution of ETH price can be seen in Figure 9.

Figure 9 **Price movement of Ethereum** *Source: Blockchaincenter.net*

My personal view is that with the new updates ETH price can reach even 20,000 USD at the end of this Bull run, since it will become Proof of Stake blockchain and deflationary update during the summer of 2021 will also add on price.

Cardano

Cardano is one of the biggest altcoins, during the 2021 battling for 3rd place in market capitalization. Its price in the beginning in autumn of 2017 was around 0.1 USD, but then during the altcoin season on 4 of January 2018 Cardano price had risen to 1.33 USD. After the January of 2018 as all cryptocurrencies there was fast decline in price, and until the spring of 2020 Cardano value was between 0.05 and 0.15 USD per coin. But then after the bitcoin halving in May of 2020, it skyrocketed to 2.45 USD now in May of 2021, and it had a market capitalization of 70 billion USD. The price development of Cardano is portrayed in Figure 10.

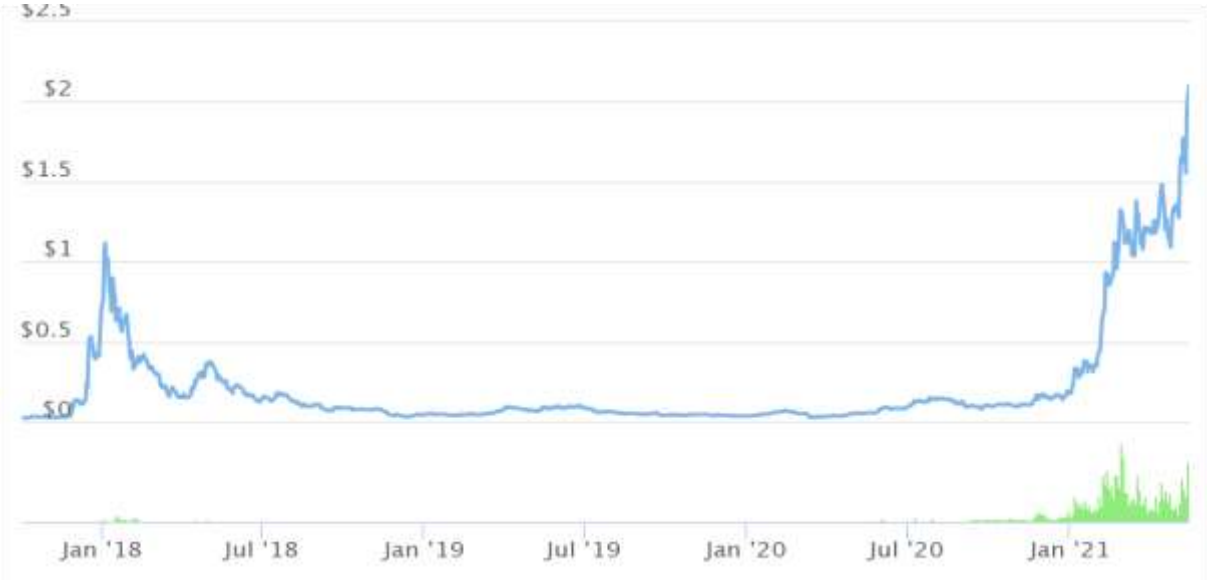

Figure 10 **Cardano price development** Source: Coinmarketcap.com

In my opinion, Cardano can reach 14-15 USD per coin until end of this Bull run, which would mean 450 billion market capitalization. Based on facts, Cardano has 70% of coins staked, big cooperation with countries in Africa are announced, and smart contracts with possibility of building decentralized application are coming during the summer. In the other words, big investments are coming for Cardano. Having proof of stake, much faster transactions speed and lower fees is also talking in Cardano's favor, over the Ethereum or Bitcoin.

Throughout the analysis of prices this thesis has shown that price movement of cryptocurrencies works in cycles. The best time to invest is few weeks before halving, and peeks of cycles have shown that cycles are getting longer by 5 months, first cycle lasted 13 months, next one 18 months, now we are in 3rd one which should peak around 23 months from halving, which would bring us to April of 2022. Due to lengthening of cycles, smaller bear markets, in forms of weeks or months could occur in the future.

2.3 Cryptocurrency Ecosystem

Previous sections portrayed the 3 of the top cryptocurrencies on the market, the next one will highlight places where to buy and sell cryptocurrencies – exchanges and give examples of the best exchanges. For investors it is also good to know places where to earn interest on their holdings, but also how to store cryptocurrencies and what is the safest wallet where you can store it.

2.3.1 Cryptocurrency exchanges

The cryptocurrency market is a new market that was created together with the first cryptocurrency Bitcoin - in 2009. It is a place where various participants meet to buy and sell cryptocurrencies. During first months of its existence Bitcoin was traded just from wallet to wallet, and people have agreed to buy and sell on online forums or social networks. Then first exchanges were created as purely as a place for transactions.

After the 2015, first exchanges which worked as a place to make transactions, but also as a storage of cryptocurrencies (wallets) or investment places, where you can stake or earn percentages on invested cryptocurrencies started to be build, such as Coinbase, Binance, Kraken, Crypto.com (Bitpanda, 2020).

Coinbase

The best for beginners and Bitcoin focused users is Coinbase. If offers an easy-to-use environment, with around 50 cryptocurrencies, with possibility of exchange between each other. Another plus is the possibility of earning cryptocurrencies by learning about them, watching videos and then answering questions, but it is just small amounts 5 to 10 USD, and it occurs just sometimes. The negatives are higher fees around 0.50% spread for buy/sell transaction, limited offer of trade pairs, missing automatic trades, where you can sell and buy at the price you set (Coinbase.com).

Binance

This exchange offers much more trading pairs, more than 360 altcoins and possibilities of trading with many fiat currencies, low fees at 0.10% buy/sell transaction. Deposit is free from bank account and from debit card is 3.5 % fee. Another plus is that Binance is working as a saving and staking platform where you can earn interest on your holdings, interest depends on market capitalization of cryptocurrency. Some beginning cryptocurrencies can earn even 40% interest per year (Houston, 2021). This exchange has its own coin called Binance coin – BNB, which is in top 10 cryptocurrencies by the market capitalization, by staking it, users can earn small amount of beginning cryptocurrencies, which were first launched on Binance, plus monthly interest rate. Crypto loans are also offered on this platform, but you have to use your cryptocurrency holdings as a collateral. Binance also offers futures and margin trading for experience users. The new feature of Binance is cooperation with Visa, the Binance debit card, with which can pay with your crypto from your wallet no need to withdraw to your bank account, if you are holding BNB token, you can earn cashback on your payment with this card, which depends on holding amount (Binance, 2021).

Crypto.com

Another exchange which offers staking or savings to earn interest on crypto on their platform is Crypto.com. It also has low fees such as Binance, but it has much less trading pairs, and webpage and their mobile apps is very complicated for beginners and poor customer service is not helping to solve this situation. Crypto.com also offers debit card, where if you stake their coin – CRO, you can also earn cashback from your payments, trading discount on fees, and for example if you pay with card for Netflix or Amazon prime, the amount will be added to your account in CRO coin (Newberry, 2021).

As other examples of cryptocurrency exchanges are Kraken, Huobi, Bitfinex, Phemex, Poloniex, Kukoin etc. (Coinmarketcap.com, 2021).

Some exchanges offer loans or savings on cryptocurrency assets, but there are also companies which are focusing on these types of products with much higher percentages on investment and lower on loans. Among the best are Celsius.Network, YouHodler.com, Nexo or BlockFi, which are giving user opportunity to gain interest in BTC, ETH, BNB, and other cryptocurrencies, but also stable coins like USDT. On the other hand, good loans for collateral in cryptocurrencies where you can choose percentage of your collateral and lengths of your loans and from this your costs will be calculated.

2.3.2 Cryptocurrency wallet

The wallet is software for managing private keys belonging to a user's addresses and store to cryptocurrency. A cryptocurrency wallet typically allows users to send payments, keep a history of transactions, or keep track of known addresses. There are several types of wallets. Some have great security, but they are difficult to use for daily payments. Others, on the other hand, have weaker security, but are perfect for daily payments. It is recommended using only proven web wallets and having several security methods activated (phone number, mail, password, PIN ...) (Frankenfield, 2021).

The smartphone wallet is very practical, available in the app store and it has the possibility of making payments anytime and anywhere. It is recommended that users do not keep their savings on this wallet, but only small amounts. There is a greater chance of the phone being stolen or lost when compared to desktop computer, so a few levels of security are even more important (Lesser, 2021).

The hardware wallet is the most secure, more expensive solution, good for long-term investors. The saying goes like this, „if you don't have cryptocurrencies on your hardware wallet, you don't really own cryptocurrencies." For hardware wallets, it is recommended to write the private

key on paper or store it somewhere in the physical world and not store it on a mobile phone, computer or device that is online, no personal data of user is used (McNamara, 2021).

The desktop wallet here, the security advantage is that private keys only work directly on user's home computer as the only one, which makes it harder to steal. The huge disadvantage is that if something happens to user's computer, the user will lose his/her cryptocurrencies (Lesser, 2021).

The paper wallet is a wallet on which the private key does not appear anywhere on the online servers. Only you have it in physical-printed form in the form of a QR code. The advantage is the speed of its establishment, financial simplicity, and security against online attacks. The disadvantage if the user carries a wallet with him/her (QR code) is that they can be the target of thieves. If user has one only one copy and lose it, that means loss of all cryptocurrencies irretrievably, so it is better to print several copies and store them safely (Frankenfield, 2021).

This part has shown different cryptocurrency exchanges and evaluated their features, such as offer of trading pairs, savings, or debit cards for payments. It has also focused on cryptocurrency wallets and highlighted their different attributes which should make easier for user to choose between them.

2.4 Regulation of cryptocurrencies

With the rise of cryptocurrencies, countries around the world are increasingly focusing on creating regulatory frameworks. As far as cryptocurrencies are concerned, a set of international rules has yet to be established. Governments around the world have adopted very different approaches to regulating cryptocurrencies. Below we find a list of the most important countries from around the world, the European Union, and their ways of regulating cryptocurrencies.

European Union

Encryption is generally considered legal throughout the EU, but the rules for exchange vary between Member States. Taxes also vary - ranging from 0% to 50% and cryptocurrency subject to capital gains tax. The European Parliament has not yet adopted any specific legislation on cryptocurrencies. Exchanges must be registered with local financial authority and from there they can operate throughout the EU. 5. The AML63 Directive now requires that cryptographic exchanges be monitored by EU rules for money laundering. The exchange of the FIAT currency for cryptocurrencies is not subject to VAT (Communication and Information Resource Centre of the for Administrations, Businesses and Citizens, 2020).

The USA

Although cryptocurrencies are legal in the United States, there does not appear to be a uniform legal approach to them. Laws vary widely from state to state, and it seems that federal laws cannot agree on what a cryptocurrency is. For example, the Financial Crime Enforcement Network (FinCEN, 2013) considers cryptocurrencies to be money transfers, while the IRS66 considers them to be assets. Cryptocurrency exchanges also face great uncertainty regarding regulation. Several different regulators claim jurisdiction and there must still be a coherent approach. The rules are very different. As already mentioned, the US is beginning to take steps to create some bridging regulation on the crypt. The US Treasury has been opened to regulate cryptocurrencies in the fight against crime, and change may be on the horizon (IRS, 2014).

United Kingdom

At present, cryptocurrencies are not considered legal tender, although cryptocurrency exchanges are legal. The potential taxability of a cryptocurrency depends on the activities and stakeholders, although profits or losses from cryptocurrencies are subject to capital gains tax. Cryptocurrency exchanges will need to be registered with the Financial Conduct Authority

(FCA), but some exchanges may apply for an electronic license. Since January 2020, the FCA has now had the power to oversee how cryptocurrencies face the risks of money laundering and terrorist financing (fca.org.uk, 2020)

Russia

Russia has a complex history of cryptocurrencies and now appears to be taking action against its use. In Russia, cryptocurrencies are considered money laundering, and 2019 laws in the country have illegally replaced money laundering. It is still unclear what cryptocurrencies are defined for and how they can be used. New proposals are being made that could allow for the confiscation of cryptocurrencies, and these proposals are said to enter into force shortly. However, it is not clear how the Russian government wants to confiscate cryptocurrencies, especially BTC, which is anonymous and decentralized (Chang, 2019).

China

Unlike most countries on this list, cryptocurrencies are illegal in China. The "People's Bank of China" or PBC (Reuters, 2021) banned financial institutions from handling BTC transactions in 2013. Since 2017, ICOs and domestic cryptocurrency exchanges have also been banned. There have been several solutions in the past, but the government has been ruthlessly trying to stop cryptocurrency in China. While mining was legal (or at least in the gray zone), China is now trying to ban BTC mining. Paradoxically, China mines up to 2/3 of BTCs in total (Aljazeera.com, 2020). China has some of the strictest laws against cryptocurrencies in the world. "At the end of 2019, several exchange offices in China closed as a result of government intervention" (Reuters, 2019)

Australia

Australia has been a much more progressive country in terms of encryption and exchange regulations. There are also legal cryptocurrencies in Australia. BTC and other cryptocurrencies

with similar properties are considered to be public property and are subject to capital gains tax. The Australian Financial Regulatory Authority, AUSTRAC, has developed stricter rules for cryptocurrency exchanges (ato.gov.au, 2020). This is to prevent money laundering and terrorist financing, and the exchange is in principle subject to rules that reflect financial institutions.

India

While the Indian government easily accepted Blockchain, the cryptocurrencies themselves faced more difficult challenges. Cryptocurrencies are not considered legal currency and face the Indian Reserve Bank (RBI) in court after being banned by the bank. To date, however, encryption is not banned in India, but the lawsuit is not over. The future of cryptocurrency and its replacement is still unclear. Although much of the concern about cryptocurrencies in India is related to money laundering and terrorist financing, with administrative regulations, regulators can offer protection and encourage progress (Legal500, 2021).

2.5 Comparison of Blockchain technologies

Almost all previous sections illustrated different important blockchain characteristics. This section will distinguish main differences between the 3 blockchain technologies Bitcoin, Ethereum and Cardano. A summary of these features is depicted in Table 3.

Table 3 Comparison of Bitcoin, Ethereum and Cardano

	Bitcoin	Ethereum	Cardano
Foundation	Satoshi Nakamoto 2009	Vitalik Buterin 2015	Charles Hoskinson 2017
Consensus Algorithm	Proof of work	Proof of work/from 2022 Proof of stake	Proof of stake
Tokenization	No	Token Standards ERC-20, ERC-721, ERC-1150	Native Tokens
Smart contracts	No	Yes	No – starting summer of 2021
Transaction speed	4-7 transactions per/second	14-20 transactions per second	1,000,000 – 2,500,00 transactions per second
Average Transaction fees	14-25 USD	10-25 USD	0,2-0,4 USD
Energy Consumption	100%	38%	0,0000221%

Source: data in this thesis

As presented in Table 3, Bitcoin was founded in 2009 by unknown person pseudonym Satoshi Nakamoto, it works on Proof of work algorithm. Bitcoin does not support creation of tokens neither smart contracts. The average transactions speed is 4-7 transactions per second and the average fee is around 14-25 USD. It needs to be underlined that energy consumption of Bitcoin is now higher than energy consumption of Hungary, on the other hand 70% of electricity comes from renewables.

Ethereum was launched by Vitalik Buterin in 2015, specifically to run smart contracts and create tokens. To create tokens Ethereum uses token standards such as ERC-20 for fungible tokens, ERC-721 – for nonfungible tokens. This made it easier for software developers to create tokens on Ethereum platform. Token standards differ in small parts from ETH token, their transactions speed, or safety can be less effective than ETH token. Ethereum has faster transaction speed than Bitcoin, but fees are almost the same, but ETH experiences a sharp rise in fees due to rising smart contract numbers in 2021. The improvement against Bitcoin can be seen also in energy consumption where Ethereum uses just 38% of BTC's consumption.

Cardano was founded by Charles Hoskinson in 2017, co-founder of Ethereum. Proof of stake was launched in summer of 2020, tokenization in spring of 2021, where Cardano platform is using Native token approach, which means the same security and transaction speed and fees for all tokens created on this platform. Smart contracts will be launched in the summer of 2021 which will bring much more attention of private firms and startups to Cardano. Conversely, Cardano's focus is on national level and non-governmental organizations, with the focus on "changing the world to better place" as highlighted by Hoskinson. Transaction speed, fees and energy consumption are incomparably better than in previous two technologies, and even if Ethereum upgrade to 2.0, Cardano will be still ahead after launching smart contracts on their platform.

Conclusion

This thesis has analyzed three generations of blockchain based cryptocurrencies through comparative analysis of features and different attributes of Bitcoin, Ethereum and Cardano to demonstrate the evolution of blockchain and possibilities which arise with new technology.

With rising prices of cryptocurrencies, the research on the topic increased but most of the research so far focused on Bitcoin, tax frauds or crime and black market activity which is always connected to cryptocurrencies due to anonymity and inability to track payments. The thesis, however focused on possibilities that can bring improvements to private and governmental sectors with different blockchain technologies.

Bitcoin's goodwill, which has developed over the last 12 years, has been strong enough to maintain its market leader position, even though its technology is outdated in comparison to Ethereum and Cardano. Ethereum, which also works on Proof of Work algorithm, as Bitcoin, gained the feature of interoperability, which enabled creation of decentralized applications and tokenization.

The differences between Proof of Work and Proof of Stake such as transaction speed, security, decentralization, tokenization helped to understand that Cardano has improved on all features of Ethereum, let alone Bitcoin.

Decentralization is supported and incentivized in Cardano ecosystem, while in Bitcoin and Ethereum, miners are centralizing and creating room for failure. Energy consumption of Cardano is not even 1% of Ethereum's and 0,01% of Bitcoin since nodes are not competing to authenticate the transactions, but randomly chosen and then controlled by all other nodes.

The third generation of blockchain will provide platforms with samples of already created decentralized applications and token creation is already possible with few clicks of the mouse,

and there is no need for software developers as it is in Ethereum's case. Simultaneously unmeasurable improvements in transaction speed and transaction fees create packages for creation of better and more secure economy, government, and everyday life.

More research is needed with regards to the third generation blockchain and its possibilities for improvements in all spheres of life. Up to now blockchain has not received the well-deserved attention of researchers. Since the world is now fighting the climate change, future research should focus on blockchain technology which helps in this area, and this can bring recognition and popularity to the blockchain technologies.

Policy Recommendations

Blockchain offers an extremely wide application layer and has the potential to completely change the Internet or the global economy. Although this technology may remain misunderstood in the eyes of many investors, users, and financial experts, one thing is certain - the blockchain will be written in bold in the history of modern technologies.

Slovakia is trying to improve digital governance and digital identities of its citizens. After investing more than 1 billion euros from Euro fonds, the system is unreliable, it is hard to use and there has been attack during which data of citizens were stolen. Some people are constraint to use it, for example entrepreneurs or NGO leaders, but they still need to print out papers and bring it to the government office, which somehow misses the point of e-government.

Cardano with Atala PRISM would bring a decentralized identity solution for Slovakia. This will bring secure, decentralized storage of data for citizens and entrepreneurs. Digital government will reduce spending on labor intensive government offices, it will help to avoid corruption, in this way will increase trust in government. This solution will be first time used in Ethiopia, so countries around the world can learn from good example of this African country.

Slovakia has also big issue with land registry and Euro fonds for the farmers. Data of the farmers are misused, someone else is receive money from EU funds without the knowledge of the owner. Conversely, some owners of the land received funds on farmland even though it is just concrete road in the middle of the farmlands.

Writing data in a (public) blockchain is similar to carving it into stone. This is useful, for example, in the case of entries for the land register, which make it possible to eliminate fraud (misappropriation of real estate, misappropriation of financial advances - payment can be included directly in the smart contract) and reduce the total cost of database registration and operation.

Bibliography

Aljazeera. 2019. “China's bitcoin miners have greater production power: research. “ Accessed on 25 May 2021. https://www.aljazeweera.com/ajimpact/china-bitcoin-miners-greater-production-power-research-191211190946896.html

Anzzolini, Damiano and Riguzzi, Fabrizio and Lamma, Evelina. 2019.“ Studying Transaction Fees in the Bitcoin Blockchain with Probabilistic Logic Programming.“ Accessed on 25 April 2021. https://www.researchgate.net/publication/336932135_Studying_Transaction_Fees_in_the_Bitcoin_Blockchain_with_Probabilistic_Logic_Programming

Austrialian Government – Australian taxation office. 2020.“ Tax treatment of cryptocurrencies.“ Accesed on 26 May 2021. https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin

BALDWIN, Jon. 2018. “In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. “ Accessed on 10 May 2021. https://www.nature.com/articles/s41599-018-0065-0

Bazan, Walter. 2020. “How are Bitcoin forks related to Bitcoin? “ Accessed on 5 May 2021. https://www.researchgate.net/publication/343692091_How_are_Bitcoin_forks_related_to_Bitcoin

Bitpanda. 2020. “The difference between a cryptocurrency broker and an exchange.“ Accessed on 15 May 2021. https://www.bitpanda.com/academy/en/lessons/the-difference-between-a-cryptocurrency-broker-and-an-exchange/

AcademyBinance. 2018. “What Is Proof of Work (PoW)? “Accessed on 25 April 2021. https://academy.binance.com/en/articles/proof-of-work-explained

Binance. “Binance.” 2021. Accessed on 14 May 2021. www.binace.com

Bitdegree. 2021. “Proof of Work VS Proof of Stake: Which One Is Better?” Accessed on 16 May 2021. **https://www.bitdegree.org/crypto/tutorials/proof-of-work-vs-proof-of-stake**

Blockchaincenter. 2021. “Bitcoin Rainbow Price Chart.” Accessed on 12 May 2021. https://www.blockchaincenter.net/bitcoin-rainbow-chart/

Blockchaincenter. 2021. “Ethereum Rainbow Price Chart.” Accessed on 12 May 2021. https://www.blockchaincenter.net/ethereum-rainbow-chart/

Boscovic, Dragan. 2021. “How nonfungible tokens work and where they get their value – a cryptocurrency expert explains NFTs.” The Conversation. Accessed on 21 April 2021. https://theconversation.com/how-nonfungible-tokens-work-and-where-they-get-their-value-a-cryptocurrency-expert-explains-nfts-157489

Bradh, Gurbaksh. 2020. “Cryptucurrency: Bitcoins. “ Accessed on 10 May 2021. https://www.researchgate.net/publication/344602840_CRYPTOCURRENCY_BITCOINS

Brunjes, Lars. 2017. “How Cardano's transaction fees work.“ Accessed on 26 April 2021. https://iohk.io/en/blog/posts/2017/10/19/how-cardanos-transaction-fees-work/

Chang, Samantha. 2019. “Russia to Criminalize Bitcoin Use as Money Substitute: Putin to Roll Out Laws.“ Accessed on 24 May 2021. https://www.investopedia.com/news/russia-criminalize-bitcoin-use-money-substitute-putin-roll-out-laws

Capital: Research team. 2020. “Cardano vs Ethereum: which coin should you invest in right now?“ Accessed on 2 May 2021. https://capital.com/cardano-vs-ethereum-which-coin-to-invest-in

Cardano. 2017. „Roadmap.“ Accessed on 6 May 2021. https://roadmap.cardano.org/en/

Cardano Foundation, 2020. „About Cardano.“ Accessed on 7 May 2021. https://cardano-foundation.gitbook.io/stake-pool-course/lessons/introduction/about-cardano

Communication and Information Resource Centre for Administrations, Businesses and Citizens. 2019. “Issues arising from recent judgments of the court of justice of the European union“ Accessed on 20 May 2021. https://circabc.europa.eu/sd/a/a4eb60ae-81f9-4556-9385-6fb4c7b09075/WP%20982%20-%20Case%20C-647%2017.pdf

Coealho-Prabhu, Sid. 2020. “A Beginner’s Guide to Decentralized Finance (DeFi).“ Accessed on 24 April 2021. https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4

Conway, Luke. 2021. “Cardano – ADA.” Accessed on 12 May 2021. https://www.investopedia.com/cardano-definition-4683961

Conway, Luke. 2021. “Bitcoin halving.“ Accessed on 21 May 2021. https://www.investopedia.com/bitcoin-halving-4843769

Coinbureu. 2018. “Deep Dive into Cardano (ADA), The Third Generation Cryptocurrency.“ Accessed on 12 May 2021. https://www.coinbureau.com/education/cardano-ada/

Conner, Eric. 2018. “Understanding Ethereum Gas, Blocks and the Fee Market.” Accessed on 26 April 2021. https://medium.com/@eric.conner/understanding-ethereum-gas-blocks-and-the-fee-market-d5e268bf0a0e

Curran, Kevin and Honan, John. 2005. “Addressing Spam E-Mail Using Hashcast.“ Accessed on 5 May 2021. https://www.researchgate.net/publication/220292210_Addressing_Spam_E-Mail_Using_Hashcast

Coinbase. 2021. “Coinbase.“ Accessed on 20 May 2021. www.coinbase.com

Coingecko. 2021. “Ethereum.“ Accessed on 14 May 2021. https://www.coingecko.com/en/coins/ethereum

Coinmarketcap. 2021. “Cardano.“ Accessed on https://coinmarketcap.com/currencies/cardano/

Coinmarketcap. 2021. “Ethereum.” Accessed on 14 May 2021. https://coinmarketcap.com/currencies/ethereum/

Daniel, George. and Green, Amanda. 2018. “IFRS – Accounting for crypto assets” London: Ernst & Young Global. Accessed on May 16 2021. https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf

Di Angelo, Monika. and Salzer, Gernot. 2020. “Tokens, Types, and Standards: Identification and Utilization in Ethereum.” Accessed on 8 May 2021. https://www.researchgate.net/publication/339843828_Tokens_Types_and_Standards_Identification_and_Utilization_in_Ethereum

Digiconomist. 2021. “Bitcoin energy consumption index.” Accessed on 6 April 2021. https://digiconomist.net/bitcoin-energy-consumption

Digiconomist. 2021. “Ethereum energy consumption index.” Accessed on 6 April 2021. https://digiconomist.net/ethereum-energy-consumption

Dowling, Michael. 2021. “Is non-fungible token pricing driven by cryptocurrencies?” Accessed on 24 April 2021. https://www.researchgate.net/publication/350467773_Is_non-fungible_token_pricing_driven_by_cryptocurrencies

Ethereum. 2021. “The history of Ethereum.” Accessed on 10 May 2021. https://ethereum.org/en/history/

Ethereum. 2021. “Gas and fees.” Accessed on 1 May 2021. https://ethereum.org/en/developers/docs/gas/#top

Ethereum. 2021. “Decentralized finance.” Accessed on 28 April 2021. https://ethereum.org/en/defi/#gatsby-focus-wrapper

Financial Crimes & Enforcement Network. 2013. “Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” Accessed on 15 May 2021

https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering

Frankenfield, Jake. 2021. "Gas (Ethereum)" Accessed on 26 April 2021. https://www.investopedia.com/terms/g/gas-ethereum.asp

Frankenfield, Jake. 2021. "Cryptocurrency" Accessed on 6 May 2021. **https://www.investopedia.com/terms/c/cryptocurrency.asp**

Frankenfield, Jake. 2020. "Paper wallet and other forms of cryptocurrency storage." Accessed on 21 May 2021. https://www.investopedia.com/terms/p/paper-wallet.asp#:~:text=A%20paper%20wallet%20is%20a,other%20forms%20of%20cryptocurrency%20storage.

Fairwaeather, Lewis. 2020. "The problems that Ethereum 2.0, proof of stake aims to solve." Accessed on 8 April 2021. **https://betterprogramming.pub/the-problems-that-ethereum-2-0-proof-of-stake-aims-to-solve-5361c155461a**

Financial Conduct Authority. 2021. "Cryptoassets." Accessed on 22 May 2021. https://www.fca.org.uk/consumers/cryptoassets

Garg, Priyeshu. 2020. "How Cardano will handle native tokens on its platform." Accessed on 6 May 2021. https://cryptoslate.com/how-cardano-will-handle-native-tokens-on-its-platform/

Goh. Brenda. Altuhn, John. 2019. "China wants to ban bitcoin mining" Reuters. Accessed on 21 May 2021. https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4/

Gupta, Manav. 2017. "Blockchain for Dummies." John Willey & Sons Inc. p. 44, ISBN: 9781119545934, Accessed on 23 March 2021. https://www.ibm.com/downloads/cas/D8O9VBAK

Hackmoon. 2018. “What are decentralized applications (dApps)? – Explained with examples.” Accessed on 15 April 2021. https://hackernoon.com/what-are-decentralized-applications-dapps-explained-with-examples-7ff8f2c4a460

Harrison, Tim. 2020. “Native Tokens on Cardano.” Accessed on 11 April 2021 https://iohk.io/en/blog/posts/2020/12/08/native-tokens-on-cardano/

Houston, Rickie. 2021. “The best cryptocurrency exchanges for trading Bitcoin and other assets.” BussinesInsider. Accessed on 5 May 2021. https://www.businessinsider.com/personal-finance/best-crypto-bitcoin-exchanges?r=DE&IR=T

Hulsink, W. 2003. “Death of the cyber sales manager The rise of electronic commerce and the fall of the online micropayments firm Digicash BV.” E-Business Review. III. 82-85. Accessed on 6 May 2021. https://www.researchgate.net/publication/309583839_Death_of_the_cyber_sales_manager_The_rise_of_electronic_commerce_and_the_fall_of_the_online_micropayments_firm_Digicash_BV

Internal Revenue Service. 2004. “IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply.” Accessed on 23 May 2021. https://www.irs.gov/newsroom/irs-virtual-currency-guidance

Jones, Evan. 2021. “Ask CryptoVantage: What is altcoin season? Accessed on 25 April 2021. https://www.cryptovantage.com/news/ask-cryptovantage-what-is-altcoin-season/

Kalisky, Boris. 2018. “Bitcoin a ti druzí - Nepostradatelný průvodce světem kryptoměn.” Praha, IFP publishing. ISBN: ISBN 978-80-87383-71-1. Accessed on 15 May 2021. https://docplayer.cz/111250991-Bitcoin-a-ti-druzi-boris-kalisky-nepostradatelny-pruvodce-svetem-kryptomen-a-jeho.html

Lesser, Jonathan. 2021. “The best cryptowallets 2021.” Accessed on 26 May 2021. https://www.tomsguide.com/news/best-crypto-wallets

Lewis, Anthony. 2016. “A gentle introduction to Ethereum.” Accessed on 5 May 2021 https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/

Lexycology. 2021. “A primer on nfts and intellectual property.” Accessed on 23 April 2021 https://www.lexology.com/library/detail.aspx?g=d96ed012-8789-4e87-bc1d-70ba76569c0f

Moore, Galen. 2021. “Altcoin Season’ Leaves Some Bitcoin Alternatives Frozen.” Accessed on 9 May 2021. https://www.coindesk.com/altcoin-season-defi-web3-ada-algo-zrx

McNamara, Ryan. 2021. “The Best cryptocurrency cryptowallets.” Accessed on 18 May 2021, https://www.benzinga.com/money/best-crypto-wallet/

Muller, Marcel. 2020. “Engineering Trust-aware Decentralized Applications with Distributed Ledgers” Accessed on 28 April 2021. https://www.researchgate.net/publication/347239262_Engineering_Trust-aware_Decentralized_Applications_with_Distributed_Ledgers

McElrath, Bob. 2016. “What is wrong with proof of stake?” Accessed on 16 April 2021. **https://medium.com/@BobMcElrath/whats-wrong-with-proof-of-stake-77d4f370be15**

Nakamoto, Satoshi. 2008, “Bitcoin: A Peer-to-Peer Electronic Cash System.” Accessed on 1 April 2021. https://bitcoin.org/bitcoin.pdf

Napoletano, E. 2021. “Decentralized finance is building new financial system.” Forbes. Accessed on 16 April 2021. https://www.forbes.com/advisor/investing/defi-decentralized-finance/

Narayan, Rumy and Tidström, Annika. 2020. “Tokenizing coopetition in a blockchain for a transition to circular economy.” Accessed on 28 April 2021. https://www.researchgate.net/publication/340380372_Tokenizing_coopetition_in_a_blockchain_for_a_transition_to_circular_economy

Natarajan, Harish and Krause, Solvej Karla and Gradstein, Helen Luskin. 2017. "Distributed Ledger Technology and Blockchain." In Fintech note No.1. Washington: World Bank Group. Accessed on 15 April 2021. http://documents.worldbank.org/curated/en/134831513333483951/Distributed-Ledger-Technology-DLT-and-blockchain-Fintech-note-no-

National Banks of Slovakia, "Technologia distribuovaných záznamov." Accessed on 5 April 2021. https://www.nbs.sk/sk/dohlad-nad-financnym-trhom/fintech/technologia-distribuovanych-zaznamov-dlt

Newberrry, Ema. 2021. "Crypto.com Review: Your One-Stop Crypto Shop." Accessed on 20 May 2021. https://www.fool.com/the-ascent/buying-stocks/cryptocom-review/#:~:text=com's%20Secure%20Website-,Full%20Crypto.com%20review,of%20cryptocurrencies%20at%20affordable%20rates.

Szabo, Nick. 2005. "Bit Gold." Nakamoto Institute. Accessed on May 4 2021. https://nakamotoinstitute.org/bit-gold/

Panda, Sandeep. 2021. "Anatomy and Lifecycle of a Bitcoin Transaction." Accessed on 5 May 2021. https://www.researchgate.net/publication/350995845_Anatomy_and_Lifecycle_of_a_Bitcoin_Transaction/stats

Raval, Siraj. 2021. "Decentralized Applications." O'Reilly. Accessed on 30 April 2021. https://www.oreilly.com/library/view/decentralized-applications/9781491924532/ch01.html

Reiff, Nathan. 2020. "What Is ERC-20 and What Does It Mean for Ethereum?" Investopedia. Accessed on 6 May 2021. https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

Reiff, Nathan. 2020. “How does a block chain prevent double spending of Bitcoins?” Investopedia. Accessedon 8 May 2021. https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp

Reuters. 2021. “China bans financial, payment institutions from cryptocurrency business.” Accessed on 26 May 2021. https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/

Royal, James and Vogt, Kevin. 2021. “What Is Cryptocurrency? Here’s What You Should Know.” Accessed on 28 May 2021. https://www.nerdwallet.com/article/investing/cryptocurrency-7-things-to-know

Rosic, Ameer. 2021. “Proof of Work vs Proof of Stake: Basic Mining Guide.” Accessed on 27 April 2021. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Sandner, Phillip. 2021. “Decentralized finance will change your understanding of financial systems.” Forbes. Accessed on 28 April 2021. https://www.forbes.com/sites/philippsandner/2021/02/22/decentralized-finance-will-change-your-understanding-of-financial-systems/?sh=4fffb0915b52

Sunyaev, Ali. 2020. “Token Economy. Business and Information Systems Engineering.” The international Journal of Wirtschaftsinformatik. Accessed on 2 May 2021. https://www.researchgate.net/publication/349255284_Token_Economy

Samarbashkh, Lale. 2021. “What are NFTs and why are people paying millions for them?” The Conversation. Accessed on 24 April 2021. https://theconversation.com/what-are-nfts-and-why-are-people-paying-millions-for-them-157035

Sharma, Rakesh. 2021. “Non-Fungible Token (NFT) Definition.” Investopedia. Accessed on 6 April 2021. https://www.investopedia.com/non-fungible-tokens-nft-5115211

Sanghavi, Vatsal and Doshi, Ronak and Shah, Devansh and Kanani, Pratik. 2018. "Blockchain Based Asset Tokenization." Accessed on 25 April 2021. https://www.researchgate.net/publication/329044416_Blockchain_Based_Asset_Tokenization/citations

Tardi, Carla. 2021. "Gwei (Ethereum)." Investopedia. Accessed on 3 April 2021. https://www.investopedia.com/terms/g/gwei-ethereum.asp

TerraCoin, 2019. "What is Genesis Block and why Genesis Block is needed?" Accessed on 24 March 2021. https://tecracoin.medium.com/what-is-genesis-block-and-why-genesis-block-is-needed-1b37d4b75e43

TheLegal500. 2021. "The legality of cryptocurrency in India." Accessed on 24 May 2021. https://www.legal500.com/developments/thought-leadership/the-legality-of-cryptocurrency-in-india/

Tian, Yifeng. and Lu, Zheng. and Adriaens, Peter. and Minchin, R. and Caithness, Alastair. and Woo, Junghoon. 2020. "Finance infrastructure through blockchain-based tokenization." Frontiers of Engineering Management. 7. Accessed on 29 April 2021, https://www.researchgate.net/publication/344891648_Finance_infrastructure_through_blockchain-based_tokenization

Vinogoradova, Polina. 2020. "Native tokens on Cardano core principles and points of difference." Accessed on 29 April 2021. https://iohk.io/en/blog/posts/2020/12/09/native-tokens-on-cardano-core-principles-and-points-of-difference/

Wei, Dai. 2018. "B-money," Accessed on 8 May 2021. **https://web.archive.org/web/20180328204908/http://www.weidai.com/bmoney.txt**

Ziechmann K., 2021. "Introduction do dApps." Accessed on 10 May 2021. https://ethereum.org/en/developers/docs/dapps/

Zirhli, Busra. 2020. “Consensus Algorithms in Blockchain.” Accessed on 28 March 2021. https://www.researchgate.net/publication/341626342_Consensus_Algorithms_in_Blockchain

Zheng, Zibin and Xie, Shaoan and Dai, Hong-Ning and Chen, Xiangping and Wang, Huaimin. 2018. “Blockchain challenges and opportunities: a survey.” In *International Journal of Web and Grid Services* Inderscience Publishing. ISSN 1741-1114. Accessed on 3 April 2021. https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey