Guide to Blockchain Technology

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Bachelor's thesis

Information and Communications Technology

Spring, 2022

Jonne Saajos

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja Viestintätekniikka
Tekijä Jonne Saajos
Työn nimi Opas Lohkoketjuteknologiaan
Ohjaaja Jari Mustajärvi

Tiivistelmä
Vuosi 2022

Opinnäytetyön tavoitteena oli antaa lukijalle kattava peruskäsitys siitä, mikä lohkoketjuteknologian historia on, mitä lohkoketjuteknologia tarkoittaa, mitä teknillisiä ratkaisuja se sisältää ja mihin lohkoketjuja voidaan hyödyntää.

Tietoa opinnäytetyöhön kerättiin useista eri läheistä ja tietoa usein verrattiin monen eri lähteen kautta jotta saatiin luotettava, lähdekriittinen tietokokonaisuus rakennettua. Teknillisiä ratkaisuja ja käyttökohteita kuvattiin paljon esimerkkien kautta jotta myös henkilö jolla on vain vähän kokemusta tietyistä teknillisistä menetelmistä voi saada hyvän peruskäsityksen kokonaiskuvasta ja näiden menetelmien yhteydestä lohkoketjuteknologiaan. Lohkoketjuteknologian käyttökohteita valikoitiin muutamia, perusteina käyttökohteen yleisyys ja mielenkiintoisuus.

Opinnäytetyön lopputulos rakentui hyväksi kokonaisuudeksi lohkoketjuteknologian peruskäsitteitä, ratkaisuja, eri lähestymistapoja, käyttökohteita ja työmarkkinoita ja opinnäytetyön kappaleiden järjestyksestä tuli kokonaisuuden ymmärtämisen kannalta järkevä.

Avainsanat lohkoketjuteknologia, lohkoketju, kryptovaluutta, kryptovaluutat, bitcoin, ethereum, cardano
Sivut 47 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology
Author Jonne Saajos
Subject Guide to Blockchain Technology
Supervisors Jari Mustajärvi

Abstract
Year 2022

The goal of this thesis was to form a good overall picture on the history, purpose and technical methods used in blockchain technology and what blockchains are used for. Data for this thesis was gathered from multiple sources and subjects were often compared through many sources to obtain a reliable, source-critical body of information. Technical solutions and use-cases were often explained through examples to help people with little to no previous experience on the subject understand the overall picture and connections between these technical solutions. There were few blockchain applications that were picked for this thesis on the basis of their prevalence and interest. The result of this thesis was built as a good overall gathering of blockchain basic concepts, solutions, technical approaches, use-cases and labor markets and the order of chapters became logical for a good overall understanding.

Keywords blockchain technology, blockchain, cryptocurrency, cryptocurrencies, bitcoin, ethereum, cardano
Pages 47 pages

Contents

1 Introduction

This thesis is made to be a guide to blockchain technology which can be used by someone with little to no background knowledge in blockchains. Blockchain technology is a fairly complex subject and because it is rather new technology a guide that has gathered the most essential knowledge from several trusted sources would be beneficial for anyone interested in this subject. Cryptocurrencies are a hot topic in modern society and it has gained a lot of interest, not only in private individuals but also in nations and companies. Total cryptocurrency market capitalization grew from Jan. 2020 to Sep. 2021 all time high with growth of almost 15 times, from 200 billion US dollars to 2.9 trillion US dollars. (Coinmarketcap, 2022)

The guide will present a brief introduction and history of blockchain technology; what is a blockchain, what are the benefits of blockchain, when was the first time blockchains were studied and developed, how did modern major cryptocurrencies begin their journey and what obstacles did they have to solve for them to get so massively adopted and accepted amongst the community. The guide will proceed to introduce technical fundamentals of blockchain technology so that the reader can gain a good general understanding of how and why a blockchain functions and for what reasons are particular technological solutions used. The Last parts of this thesis concentrate on comparing major cryptocurrencies technology-wise to further deepen the knowledge of technical aspects and lastly presenting some practical blockchain applications that are already being used or are developed for future implementation, we will also look into some statistics and latest news of blockchain labor markets. The main contents of this thesis are concentrated in purely presenting the technical aspects of blockchains and cryptocurrencies. The thesis will not include any financial advices, political, economical or socioeconomical subjects or speculation of any sort.

The sources for this thesis are a variety of technical reports, white papers, MIT lectures, documentations, books and articles. The data gathered has been observed through multiple sources to ensure a healthily criticized body of information.

2 Purpose and Objectives of Thesis

The purpose of this thesis was to gather and explain the basic concepts and background of blockchain technology and cryptocurrencies. Usually when asked about cryptocurrencies and blockchain technology, people mention Bitcoin but do not have a clear image or understanding on what else there is to it. Cryptocurrencies are often connected to just a digital form of money or uses in illicit acts for example. This thesis aims to give the reader a new perspective on cryptocurrencies via explaining the backgrounds and ultimate goals that different cryptocurrencies have and what breakthroughs there have been after the launch of Bitcoin. In order to reach this goal, the chapters will progress logically in this thesis, always deepening the knowledge base by applying what we have learnt in previous chapters, this way we get to build a sensible whole of the thesis but also help the reader to reach a good general understanding of the big picture. While blockchain technology is technically rather a complex subject and technology is full of new innovations and is developing at a fast pace, it is understandable that people, even in engineering have little to no knowledge on blockchain technology. This is the problem I am trying to solve via providing a blockchain guide that presents the relevant concepts of blockchain systems and what differences and use-cases can there be for different cryptocurrencies and blockchain platforms.

To answer these research questions on how to build an educational whole of a constantly evolving, new technology and cover the very essential parts of these subjects I decided to primarily rely on literature research as a primary source of intel because there was a lot of literature available, from academic research to news articles and books. There is plenty of material on the topic such as on Youtube, but I have decided to not include these as a source because many of these videos are influential and biased or have lightly backed sources. For this topic, literature material was more easily confirmed and can be considered generally more reliable. I have made use of multiple sources per subject to achieve a thorough qualitative analysis of these topics by comparing, analyzing and finally synthesizing the data I have gathered. In some occasions I may have first seeked some perspective from articles (e.g. news or blog posts) of appropriate sources but have then verified these assumptions and posts from more trustworthy sources such as technical or academic papers. This systematic way of researching and source evaluation through literature has made a reliable foundation for the thesis. Secondary source used for this thesis was a MIT lecture instructed by Prof. Gary Gensler who has had a long career in finance and is currently the chair of U.S. Securities and Exchange Commission. This lecture on top of providing

some basic concepts of cryptocurrencies, gave me some good insights of economical challenges of cryptocurrencies in general. Although the theme of this thesis is primarily technical, these kinds of economical perspectives helped me in criticizing some insights more justifiably and gaining even better collective of information.

Blockchain industry also contains many different opportunities for careers, for example entrepreneurship, employment, or research. While this thesis will inevitably leave some open questions, it is expedient to provide enough information on this thesis about blockchain technology to arouse the reader's interest in researching and learning more about this technology. This thesis introduces cryptocurrencies and technologies of three different generations to further build the reader's understanding on how the technological solutions have evolved and for what reasons. Technical solutions that are used in running and developing blockchain systems are presented extensively but comprehensibly. It is essential to have some sort of basic understanding on the technical side of blockchain systems to understand why certain things like decentralization are important and why remodelling of some traditional applications is possible with the use of blockchain systems.

3 History

The blockchain pioneer Bitcoin was initially implemented in 2009, but the roots go beyond that. Already in 1991 a blockchain was described by Stuart Haber and W. Scott Stornetta. Stornetta, who was a physicist, scientific researcher and a notable figure in 1990s cryptographic science and distributed computing. He was the first person to mention blockchain architecture. Stornetta and Haber studied mechanisms on how to create digital time stamps and order recorded files in a secure and unique way so that the files could not be tampered. In 1994, Stornetta and Haber founded a company called "Bellcore". Bellcore provided digital time stamping services with the use of framework "Linked Time Stamping Authority" (TSA). Bellcore is considered to be the first company to provide the services of blockchain. This blockchain technology was however not used and the patent expired in 2004. (W. Scott Stornetta, n.d.)

In 1990s there were multiple attempts to create a digital form of currency.

- Digicash (David Chaum, 1989)

- Mondex (National Westminster bank, 1993)
- Cybercash (Lynch, Melton, Crocker & Winston, 1994)
- E-gold (Gold and Silver reserve, 1996)
- Hashcash (Adam Black, 1997)
- Bit Gold (Nick Szabo, 1998)
- B-Money (Wei Dai, 1998)
- Lucre (Ben Laurie, 1999)

Every project eventually failed due to various of reasons. First of all, none of these digital currencies were adopted by merchants widely enough. Secondly, most of them relied on a central authority and they failed to reach a consensus of the ledger but most importantly none of these projects could solve the puzzle of so-called “double-spend” problem. (Gensler, 2018)

In 2008 developer(s) by a pseudonym “Satoshi Nakamoto” released a whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System”. This whitepaper included the model of a blockchain. This model used and still uses very much the same characteristics as the initial blockchain model developed by Stornetta and Haber. Satoshi Nakamoto also references Wei Dai’s B-Money and Adam Black’s Hashcash in the whitepaper. Satoshi Nakamoto managed to gather all the best of these failed projects together but most notably Satoshi Nakamoto figured a way to solve the “Byzantine generals problem” that essentially disables users from double-spending transactions and thus making the blockchain BFT (Byzantine Fault Tolerant). (Double-Spending) (Gensler, 2018) (Nakamoto, n.d.)

To this day, the true identity of the person or the group behind Bitcoin remains unknown. Satoshi Nakamoto remained active in developing Bitcoin till 2010 and he/them holds around 5% of all the bitcoin supply, which is about 1 million bitcoins. (W. Scott Stornetta, n.d.) (Hayes, 2021)

In 2014, the so-called second generation of blockchain was launched via the blockchain called “Ethereum”. Ethereum was founded by a Russian-Canadian programmer Vitalik Buterin and a English computer scientist Gavin Wood, who is also the creator of Polkadot and Kusama which are multi-chain architecture network protocols that allow arbitrary data to be transferred across blockchains.

Vitalik Buterin, who was only 20 years old at the time Ethereum was launched had background in computer sciences via his father, Dmitry Buterin who was a computer scientist and initially introduced Vitalik to Bitcoin in 2011. At that time, Vitalik began on writing for “Bitcoin Weekly” at a salary of five bitcoins per article. The website of Bitcoin Weekly was shut down due to insufficient revenues but in September 2011, Vitalik Buterin co-founded the “Bitcoin Magazine” where he was a leading writer.

In 2013, Buterin published the first white paper of Ethereum. In Buterin’s mind, the bitcoin needed a scripting language for appication development which was then implemented in the Ethereum blockchain by the name “Smart Contracts”. The Ethereum network went live in July, 2015 and is currently the second biggest blockchain to Bitcoin in total cryptocurrencies market capitalization. ("Vitalik Buterin", n.d.) ("Gavin Wood", n.d.) ("Ethereum", n.d.) (Polkadot Technology, n.d.)

In 2015, one of the Ethereum co-founder Charles Hoskinson, founded a research and development company named Input Output Global (IOG) that is behind the development of a blockchain platform called “Cardano”. Cardano was built to be a “Proof-of-Stake” blockchain in contrary to Bitcoin and Ethereum that uses the “Proof-of-Work” consensus mechanism. Cardano was supposed to be a more secure, low-fee blockchain platform with the same functionalities as Ethereum had via smart contracts. Cardano can be considered as the third generation of blockchain technologies. Cardano is initially trying to solve the problems that Bitcoin and Ethereum has, which are high transaction fees, energy consumption, scalability and interoperability. Cardano has academics and top level engineers developing the project and it is being written in programing language Haskell and it is completely open-source. To this day, IOG has published 128 academic papers on Cardano research. Cardano was initially launched in 2017 but since that it has been critized due to the slow developing pace. Only in 2020 Cardano launched their second phase since the launch that included a staking mechanism that allowed native token holders to stake their tokens (ADA) to passively gain more ADA tokens. The third phase that included smart contract functionality for application development was launched in September 2021. ("Cardano (blockchain platform)", n.d.) (Hussey;Hamacher;& Chipolina, 2021) (Cardano, n.d.)

High transaction fees and the slow speed of transactions of Ethereum has grown in to stage where Ethereum has been forced to develop a major upgrade that will transition its Proof-of-Work

mechanism into a Proof-of-Stake mechanism, this upgrade is planned to be launched in first half of 2022. ("Ethereum", n.d.)

4 Blockchain Introduction

Blockchain is a system, one type of a shared, immutable, append-only database that contains information in blocks. Blocks that store this data are all chained together, thus the name 'Blockchain'. One block includes specific data, typically transaction data and always a signature of itself and the prior block, so every block can be differentiated from each other and the chain stays intact. Because of the nature of blockchain architecture, every block is connected to the previous and to the following block and via cryptographical methods a mutation of single block would alter the whole chain after it. This would be immediately noticed in the network so one should tamper the whole chain to be able to corrupt the blockchain system. Tampering the whole chain would be very impractical which is why blockchains can be considered extremely secure storages.

Blockchains are most often considered as a platform for digital money in a form of DLT (Distributed Ledger Technology) where the transaction data is stored in a block. Blockchain offers many viable options for different use-cases in a modern world such as smart contracts, financial services, supply chains, anti-counterfeiting, digital identities, voting systems and healthcare. (Euromoney Learning, n.d.) (Hayes, 2021) (Blockchain Overview, n.d.) (Gensler, 2018)

Blockchain can be implemented as a public, private, permissioned, hybrid or a sidechain kind of a system. A public blockchain can be accessed by anyone, and anybody can read, write and audit the activities happening in the blockchain network. A public blockchain is typically completely self-governed and it can offer a truly decentralized, democratized and authority-free operations such as Bitcoin network does. (Geroni, 2020) (Seth, 2021)

Private blockchain can be efficient for private businesses, a private blockchain cannot be accessed by just anybody and it can be ran on-premises or behind a corporate firewall. Users need a authentic and verified invitation to join this network. A private blockchain is always governed by someone, e.g. a private business, this blockchain's operator is able to manipulate the whole chain by overriding, editing or deleting entries in the blockchain. (Seth, 2021) (Blockchain Overview, n.d.)

A permissioned blockchain can be useful for companies whose blockchain architecture includes co-operation with other parties, such as a logistics solution built on a blockchain. For a logistics blockchain solution one could permission for example a manufacturer, supplier, carriers, retailers and so on, anyone who has and is accessing the supply chain and needs to store data to the blockchain.

A sidechain is a blockchain that is pegged to a main chain, and the data can be transferred in both directions between these blockchains. The main chain can include multiple sidechains. A sidechain can be created for various of reasons, one being developing purposes. Developers could be working on their products and test them on a "test network" which could be a sidechain to the main chain. Ultimately the vision for sidechains is to make the whole ecosystem of different blockchains seamless by letting the blockchains themselves be independent but providing cross-chain functionality over another. (Side Chain, n.d.)

A hybrid blockchain is something that is in between a public and private blockchain, some blockchains can be be launched as a hybrid blockchain for various of reasons but it can be made completely public and thus totally decentralized and self-governed later on e.g. Cardano. (Cardano Development Flow)

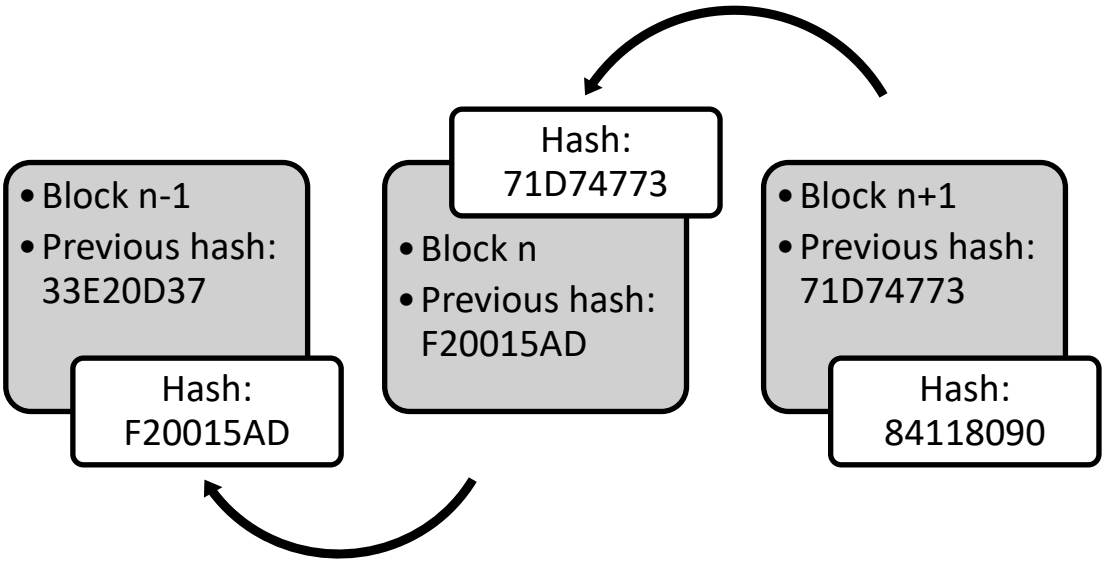
5 Blockchain Technical Fundamentals

As said by Oliver Kattwinkel and Michael Rademacher in their technical report (Kattwinkel & Rademacher, 2020) "a blockchain is not a revolutionary technology but rather a clever combination of three fields: cryptography, decentralization and game theory." Therefore, to understand how a blockchain functions, it is essential to understand the very basic fundamentals on how these three fields are applied in a blockchain technology. This chapter will cover the core parts that blockchain utilizes in making the complex totality function.

5.1 Blockchain

Every block in the blockchain contains a cryptographical hash in a block header that points to the previous block header as shown in Figure 1. This allows the blockchain to be fully linked from the latest block to the first block in the chain which is also called a “genesis block”.

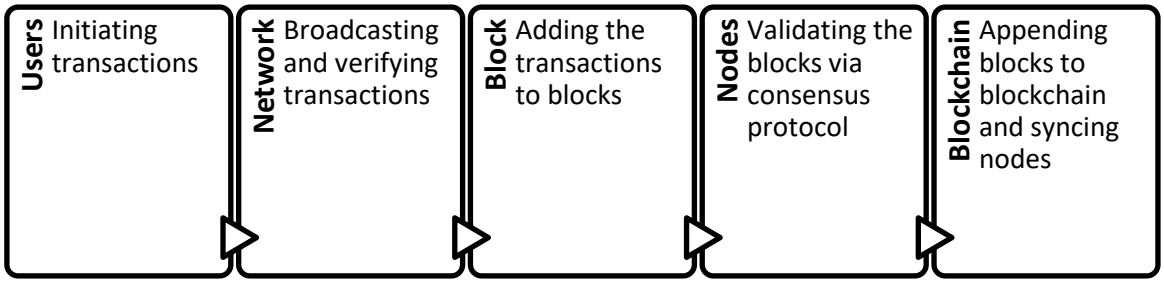
Figure 1. Simplified Blockchain Example



This form of a hash linked list architecture ensures the immutability of the data stored in the blockchain. A manipulation of a block in the middle of chain would alter the header hash and therefore would break the whole hash linked list integrity. To be able to manipulate data in a blockchain, one should alter all the following blocks also and have these validated in the network. Altering data is not so hard but validating them via a consensus becomes very tricky. To be able to validate these tampered blocks, one should typically control over 50 % of the blockchain network so the validation can be agreed via the consensus algorithm. (51% Attack)

Generally a blockchain workflow can be thought in five phases; initiating the transactions, broadcasting and verifying them in the network, building the blocks that include the transactions, validating the block (e.g. mining) and then appending these blocks to the blockchain and syncing the nodes.

Figure 2. Blockchain Workflow Example (Liu, et al., 2019)



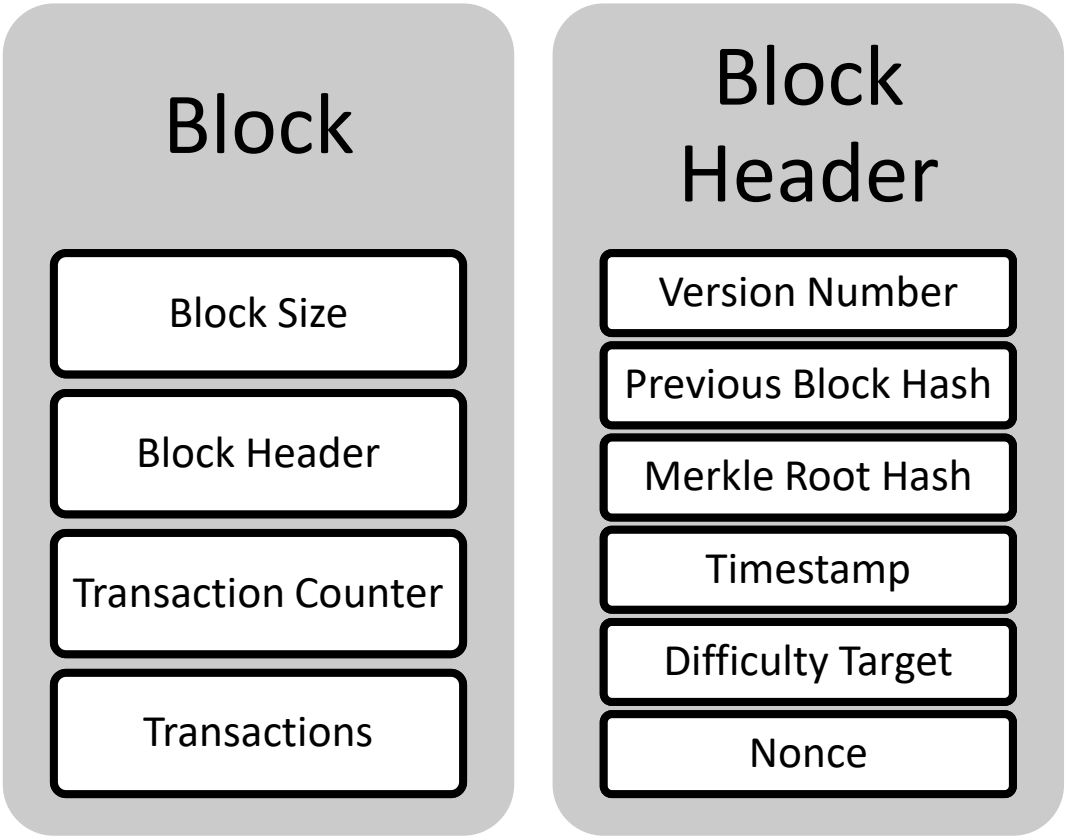
Transactions and broadcasting is most commonly done by a wallet program that can be a “full-node” or a “light-node”. Full-node wallet means that it holds a full copy of the blockchain and thus can be quite big in size, also the syncing can take some time especially on the first run. Another very viable option is to use a light-node wallet which essentially has all the same functionalities as a full-node wallet would but instead of holding the full copy of the blockchain it only keeps the copies of block headers which makes it much more compact and faster syncing. (Wallets)

Once the network has verified the transaction’s validity, the transactions are added to blocks and once added, the network will start validating the blocks via an consensus protocol that could be mining in a case of a PoW (Proof-of-Work) system, such as Bitcoin or Ethereum. Consensus methods are discussed in chapter 5.2.

5.1.1 Block Structure

As we have talked a little bit of what blocks include and what’s their function in the blockchain, here is a more detailed overview of a Bitcoin block and what it specifically store.

Figure 3. Block Structure Example (O'Reilly Media, Inc., 2014)



Summarization of block contents:

- Size of block in bytes
- Block header in a form of hash
- Count of transactions included in the block
- Detailed transactions included in the block

Summarization of block header contents:

- Current protocol version number
- Reference to the previous block's hash
- Merkle root hash of the blocks transactions
- Block creation time in Unix
- Difficulty target used for this blocks creation in PoW algorithm
- Nonce, number that satisfied the PoW algorithm's difficulty target

In essence, this is what a simple block would include. A block can however, depending on the platform, include various other data not mentioned in the example. (O'Reilly Media, Inc., 2014)

5.2 Consensus Mechanism

When it comes to decentralized peer-to-peer networks, a fitting consensus mechanism is a must. In a more traditional software architecture where functionality and data storages are maintained in a centralized server a consensus mechanism is not really needed. A blockchain however needs a functional consensus mechanism to ensure that all the nodes have the same copy of the blockchain. Not only that a appropriate consensus mechanism is a liability for the blockchain, it is required for a blockchain to function as expected. Consensus mechanism has also much to do with the overall security of the blockchain.

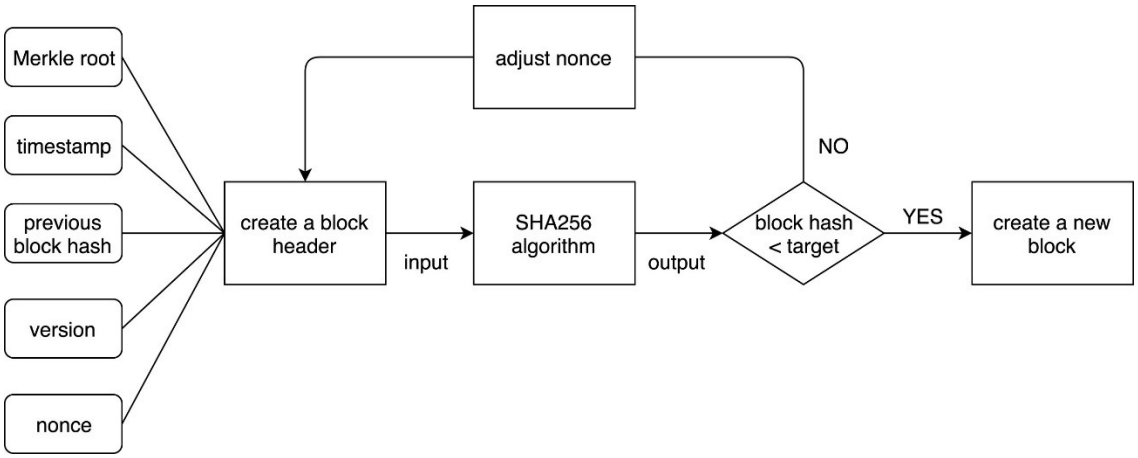
A consensus mechanism first of all needs to be Byzantine fault tolerant which essentially means that nodes have the ability to reach a consensus in a trustless environment. This leads to a topic on tolerancy against malicious actors. If a blockchain's consensus mechanism is built to be Byzantine fault tolerant, it is also tolerant against malicious acts. Generally speaking, vast majority of consensus mechanisms (PoW and PoS) are considered to be 50 % fault tolerant. Anyone who controls over 50 % of the blockchain network can and will make the blockchain centralized and thus has the ability to do malicious acts, such as double-spending. (51% Attack) (Double-Spending) (Zhang & Lee, 2019)

5.2.1 Proof-of-Work

Proof-of-Work consensus mechanism was the first to be used with Bitcoin, thereafter there have been some variations to PoW protocols but the main idea is the same. In PoW models, the consensus is reached via a computational power usage. The worker (also referred as miner) nodes will participate in one type of a competition where each node will have to solve a cryptographical puzzle. Whoever solves the puzzle first, will append a block in the blockchain and is thus rewarded a block reward. This is where the term "mining" comes. In PoW models, as the blockchain and number of nodes grow, the difficulty of the puzzle is also proportionally adjusted. For example, Bitcoin is built to produce a block roughly every 10 minutes, so the difficulty to mine a block is

adjusted so that this interval stays true. Lets see a simplified workflow of a Bitcoin PoW mechanism from figure 4.

Figure 4. Proof-of-Work Example (Zhang & Lee, 2019)



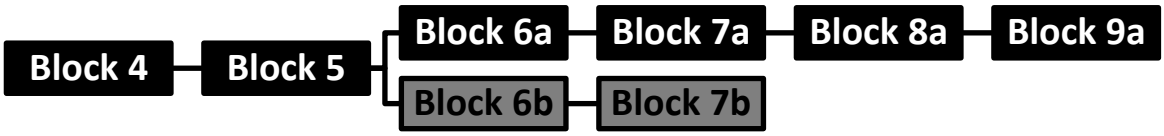
First the metadata is gathered for the block header, and to be noted, we can see there is a nonce included. Nonce is a random number used once, hence the word 'nonce'. Usually the block header also includes the difficulty target for that particular block. Once all the data for a block header is gathered, it is hashed, in Bitcoin, it is hashed with SHA-256. In Bitcoin case the difficulty target represents a number of leading zeroes the block hash must have to be considered as validated. So in simple terms, the proof of work is achieved when enough different nonces are tried so that the block hash starts with the number of leading zeroes defined in the difficulty target. Once this happens, the block is created and appended to the blockchain, and whoever solves this puzzle first, is awarded a block reward as a so-called coinbase transaction. Coinbase transaction is a transaction with no inputs but only amount of bitcoins created as the block reward.

Now from time to time, due to the decentralized nature of blockchain architecture there can be occasions where node's copies of the blockchain are not the same. This may lead to a phenomenon called "forking". Forking means that two miners solve the PoW puzzle almost simultaneously and the blockchain is therefore divided with two candidate blocks that would be extending the main chain. Miners will find the new forked blocks at different times depending on the topological distance to the candidate block propagator so different miners will start mining on top of different blocks. Whichever of these forked blocks gets extended first, will eventually become the main chain because the PoW protocol functions in a way that miners will always prefer the cumulatively most difficult chain or in other words, longest chain. The other blocks will

become “stale blocks”. On major blockchains, forking is quite unusual and if it happens, it is most commonly settled in one block period.

Figure 5 represents a forking incident where block 6a and 6b was mined at the same time. The chain was extended once more to blocks 7a and 7b but block 8a was mined earlier than a block 8b could be found. The network agrees that “chain a” is the longest chain and also cumulatively the most difficult chain and will become the main chain. “Chain b” will be discarded.

Figure 5. Blockchain Fork Example



To be noted on forking incidents and block rewards, blockchains usually have a time period counted in blocks before rewards are released. For example, Bitcoin is using a maturation time of 100 blocks before rewarded coins can be spent. The stale blocks rewards will be lost.

Now we have talked about incidental blockchain forking, but there can also be intentional forking called “hard-fork” or “soft-fork” which can be used for example in updating or upgrading the blockchain protocol. We will talk more about hard forks in later chapters. (O'Reilly Media, Inc, 2014) (Zhang & Lee, 2019)

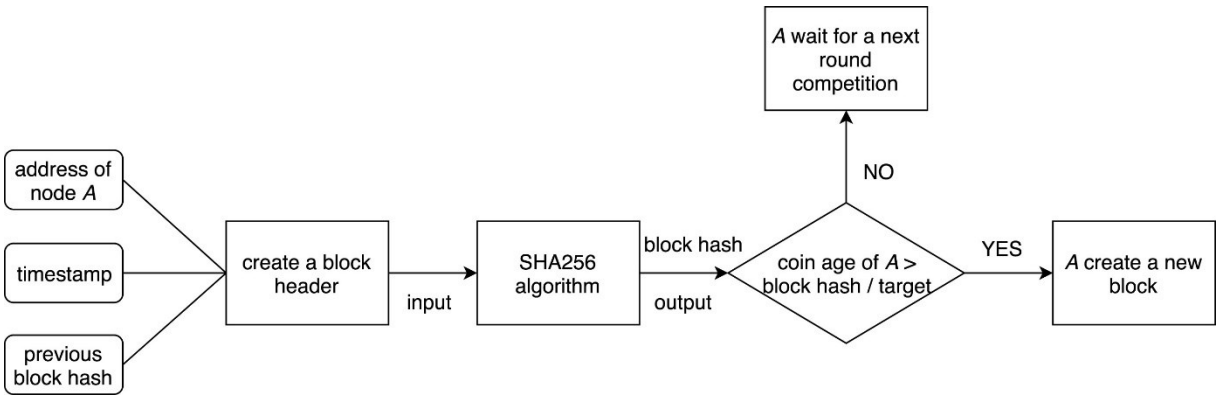
5.2.2 Proof-of-Stake

As we learnt from previous chapter, PoW protocols uses computation power to reach consensus which has been highly criticized due to a possibly huge energy consumption especially amongst major cryptocurrencies like Bitcoin or Ethereum. PoS (Proof-of-Stake) protocols however have a different way to reach consensus and because there is no need to adjust and find a nonce that matches the difficulty target and thus no need for excessive computational power usage, the

energy consumption is a lot lower. PoS protocol uses a way to utilize cryptocurrencies that a user decides to stake in the system. The higher amount staked, the higher the rewards.

We can see from Figure 6 that essentially the procedure of creating a new block follows similar rules, and the main differences is in how the nodes are reaching the consensus. In PoS systems you have a variable “coin age”, coin age is calculated from the total amount of coins staked multiplied by the time staked. So for example, if you stake 5 coins for a 10 days period your coin age will be 50. Once a node creates a block, the coin age will be reseted to zero. (Zhang & Lee, 2019)

Figure 6. Proof-of-Stake Example (Zhang & Lee, 2019)



5.2.3 Energy Efficiency

As we talked about consensus protocols Proof-of-Work and Proof-of-Stake, we came to the conclusion that PoS systems are by far more energy efficient. There are some ways to limit the PoW energy consumption though. For example, Bitcoin miners are heavily using devices called “ASIC” (Application-Specific Intergrated Circuit). These devices are built to have one and only one purpose; solving Bitcoin algorithms. ASIC’s used in Bitcoin try out different nonces for creating a block, and they do it a lot faster than a simple desktop CPU or GPU ever would. This leads to the fact that Bitcoin has an enormous energy consumption. However, since some platforms want to use PoW for several reasons, modern PoW algorithms are made to be ASIC-Resistant. In simple terms, this means that the PoW algorithm will choke if tried to solve via ASIC’s. ASIC-Resistant coins like Ethereum are then mined with GPU’s, and this has actually lead to a rather unexpected phenomenon, that modern GPU’s are out of stock almost everywhere, worldwide.

The PoW algorithm itself can affect a lot in the energy consumption of the consensus protocol and there are several different algorithms used on different PoW cryptocurrencies. The cryptocurrency popularity of course affects a lot in the energy consumption, because when there are more people mining, the difficulty target grows and therefore more computational work is needed to reach the consensus.

To concretize the comparison of PoS and PoW energy consumption, lets compare Cardano's Ouroboros protocol with Bitcoin's PoW. As of January 2022, Bitcoin could consume up to 200,000 GWh/year while Ouroboros would only consume up to 15 MWh/year. On this case, PoS would be 13.3 million times more energy efficient. Not only, that the energy consumption is lower but this affects also the transaction fees. For example, lets take a look on Ethereum and Cardano which are both Smart Contracts platforms but Ethereum is a PoW system as Cardano is a PoS system. (Figure 7) (Tardi, 2021) (Bitcoin - Energy Consumption, 2022) (Costello, 2020)

Figure 7. Ethereum & Cardano Fee Comparison (Messari: Asset Screener, 2022)

Platform	Median Transaction Volume (USD)	Median Fee (USD)
Ethereum (PoW)	324,35	18,43
Cardano (PoS)	348,53	0,203

We can clearly point out, that the transaction volumes are similarly in range but the amount of fees paid on both platforms are radically unequal. This is one of the reasons why Ethereum is planning on upgrading the whole platform to PoS protocol.

5.3 Hard-Fork & Soft-Fork

We talked about incidental forking that may happen if consensus is reached with two or more nodes at the same time. This is usually settled by the next block and long incidental forkings are very rare. There are possibilities to fork the blockchain on purpose though. Terms "hard-fork" and "soft-fork" indicates these situations. Forking on purpose is most commonly due to a network upgrade of some sort, hard-forks being more radical major upgrades that are essentially non-reversible as soft-forks can be considered as minor changes like adding a new transaction type or such.

Hard-forking forks the blockchain into two different chains where the new chain is following new protocol version rules and the old version, still running, following the old rules. Some nodes may follow the old chain for a while, but will soon realize to upgrade their blockchain to an up-to-date version. To be noted, hard-forks require for all nodes to upgrade into the new protocol version due to the fact that these forked chains do not see each other as valid anymore.

A soft-fork typically adds some new features to the blockchain but contrary to hard-forking events, nodes that are still following the pre-fork chain will be able to maintain the consensus on the post-fork chain, they just wont be able to utilize these new features and may not be able to create new blocks. For soft-fork events, as mentioned, not every node needs to upgrade their protocol version but the majority of nodes is enough. (Soft Fork vs. Hard Fork, Differences Explained, n.d.) (Frankenfield, 2021) (Frankenfield, 2021)

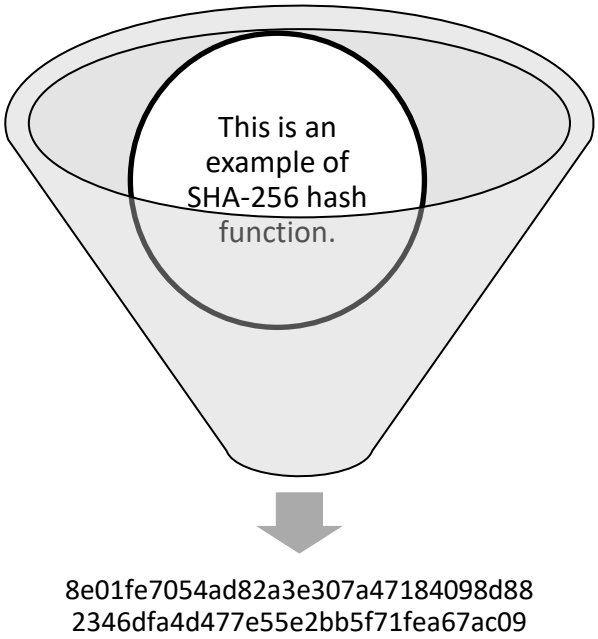
5.4 Cryptography in Blockchain

Cryptography is widely used in blockchain technology thus the buzzword “cryptocurrency”. Cryptographical methods are used to ensure the immutability, security, integrity and provenance of data in the blockchain. Most common cryptographic algorithms used in blockchains are hash functions and asymmetric algorithms.

5.4.1 Hash Functions

Cryptographic hash functions are one of the core features in a blockchain system. Hash functions are used to compress any arbitrary sized data to a fixed-size hash value. Hash functions make the data compressing very efficient but reverting the hashing is mathematically so impractical that the hash functions can be considered as one-way functions. There are several different hash algorithms used in blockchain technology, Bitcoin for example mostly uses SHA-256 (Secure Hash Algorithm) which is part of SHA-2 family. SHA-2 was designed by the United States National Security Agency (NSA) in 2001. SHA-256 algorithm, as name suggests, compresses the data to a 256-bit hash. Different hash algorithms used by major cryptocurrencies are Keccak-256 (Ethereum), BLAKE2 (Cardano) and many more.

Figure 8. SHA-256 Hash Function Example



In blockchain technology, hash functions are the most extensively used cryptographical methods, they are used in hashing various of data such as block headers, merkle trees, generating public keys and addresses, verifying transactions and consensus protocols use it in their algorithms etc. (Turner, 2019)

5.4.2 Public-Key Cryptography

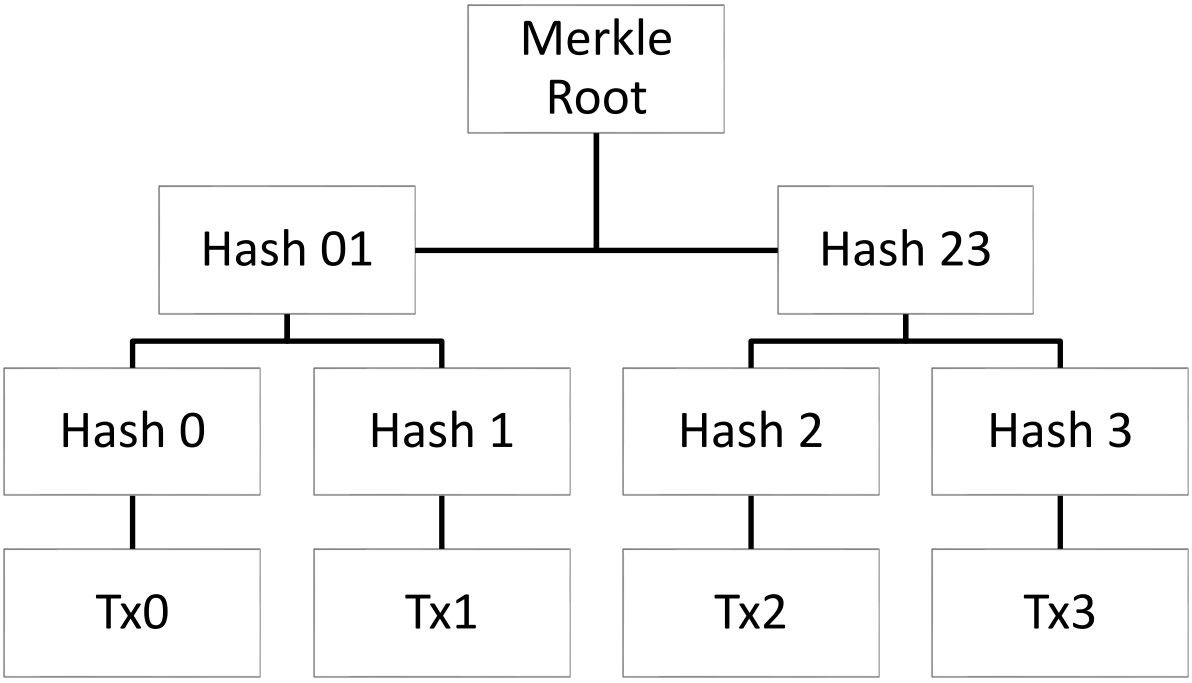
Public-key or asymmetric cryptography uses key pairs of private and public keys. These key pairs can be used for authentication and confidentiality, the private key must be kept safe from others accessing it but the public key can be shared with anyone, trusted or not. Asymmetric algorithm can be used for example in digital signatures or data encryption/decryption.

In simplified manner, in blockchain private keys are used for authenticating outgoing transactions with a digital signature and public keys are used as the receiver addresses. Security-wise, since every transaction is digitally signed with a private key, as long as the private key is kept safe it is basically impossible to commit frauds by modifying a transaction or appearing as someone else. (Poston, 2021)

5.4.3 Merkle Tree

The transactions, as mentioned are stored in blocks but to be more detailed, they are actually stored in a Merkle Tree structure inside the block and only the Merkle Root is stored in the block header. This data structure allows the blocks to be more compact size-wise since only the root hash of the transaction tree is saved. This structure also provides data integrity for the transactions and provides a fast, efficient way to verify transactions. Merkle Tree can be somewhat thought as a hash linked list as a blockchain is in a way but in contrary, you can verify the transactions validity only with one branch instead of needing to download a full copy of the tree. (101 Blockchains, 2020)

Figure 9. Simple Merkle Tree Example (Liu, et al., 2019)

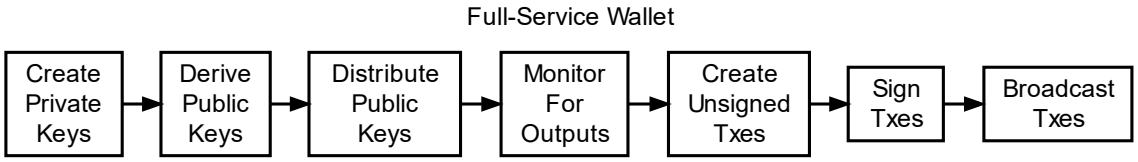


There are some variations of the Merkle Tree in blockchains, for example Ethereum uses a so-called Merkle Patricia Tree which is a bit more complex structure.

5.5 Wallets

Wallet's functionality can be divided in three main fuctions: Public key distribution, signing and network broadcasting. It is possible that not all of these functions are done on a single wallet program but here is an example of a full-service wallet.

Figure 10. Full-Service Wallet (Developers documentation, wallets, n.d.)

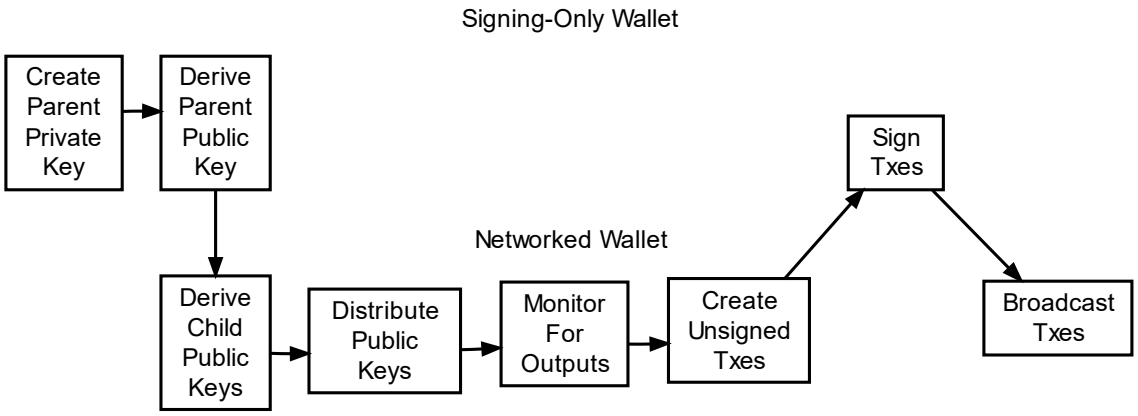


A full-service wallet is capable of creating private keys, deriving public keys from the private keys, distributing these public keys, monitoring for outputs, creating unsigned transactions, signing transactions and broadcasting the transactions to the network.

A full-service wallet is debatably less secure for storing the private keys on the device but this is usually managed by the wallet program to offer encryption of the wallet files that contain these private keys for added security.

As noted earlier, the wallet's functions can be divided to be handled by separate programs. For example in a case extra security is wanted for your private keys, you could generate and store your private keys in a signing-only wallet. Signing-only wallet creates a parent private key and derives a parent public key from it to be used in a networked wallet that would after deriving a child public key from the parent public key handles all the rest of wallets functionality except for signing transcations.

Figure 11. Signing-Only Wallet (Developers documentation, wallets, n.d.)



Another common variants of wallets are offline wallets, hardware wallets and distributing-only wallets. Offline wallets despite the name are, obviously, not completely operable in total offline mode but rather they give extra security by handling the key generation and transaction signing in offline mode. Without going too much in to the details, it can be agreed that an offline wallet provides a very secure way to handle transactions but on the other hand requires a lot of hassle from the user to complete the required processes.

Hardware wallets are devices rather than programs but in essence they function in a similar manner as a signing-only wallet would. Hardware wallets provide improved security but still require some struggle to complete a transaction.

Distributing-only wallets are, as suggested, only used in distributing the public keys to other wallets. These kind of wallets could be used in less secure environments.

5.6 Private – Public key pairs & addresses

One of the core features of blockchain transactions are private-public key pairs that allow users to sign, send and receive funds. The private key can also be seen called as a secret key, which is maybe more appropriate name for it since with the private key you have the full ownership and control over the funds associated with these keys.

As pointed out in previous chapter, wallets are most commonly in charge of generating the private-public key pairs and handling the transaction signing and broadcasting. In modern days, wallet users are rarely handling the private keys themselves but instead are given a seed phrase that encodes as a private key.

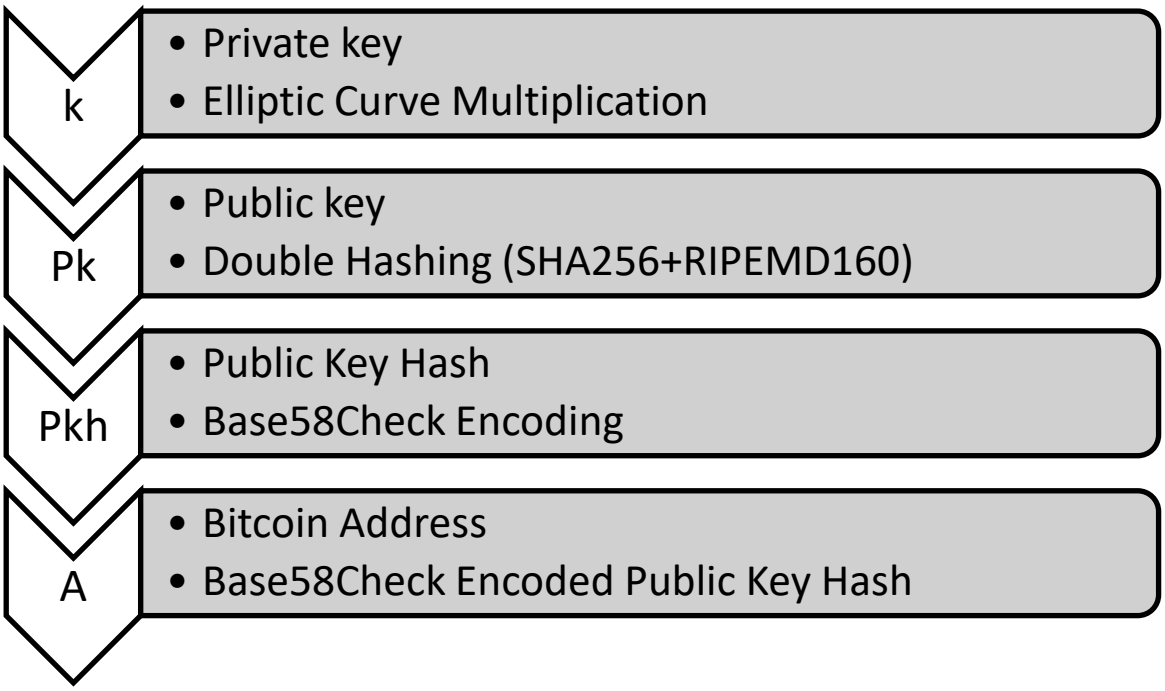
In Bitcoin for example, a private key is simply a random 256-bit number. The public key is irreversibly calculated from the private key, using ECC (Elliptic Curve Cryptography). Bitcoin ECDSA (Elliptic Curve Digital Signature Algorithm) uses pre-defined parameters defined by NIST (National Institute of Standards and Technology) established standard “secp256k1”.

Public key “Pk” derives from the multiplication of private key “k” and a defined, elliptic curve base point “G”

$$Pk = k * G$$

In simple terms, the public key can be considered as your bank account number you would give to others for receiving payments and the private key would be used to verify outgoing payments. Although in Bitcoin, the public key is further hashed into a specific Bitcoin address.

Figure 12. Key pair to Bitcoin address (O'Reilly Media, Inc., 2014)



We can see from above that before getting the final Bitcoin address that is used in receiving funds, the public key is hashed first with SHA256 algorithm and the result is further hashed with RIPEMD160 algorithm. This double hashing produces the bitcoin address, though they are most commonly presented in their encoded forms for convenience.

The Base58Check encoding adds a version prefix to addresses and from this prefix we can identify the address type. There are several types to Bitcoin addresses but the most used are:

- P2PKH (Pay-to-Pubkey Hash) Address, **prefix 1**.
  - Example: **1**7VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem
- P2SH (Pay-to-Script Hash) Address, **prefix 3**
  - Example: **3**EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX

P2PKH Address is the legacy address of bitcoin that is used for transactions, but P2SH addresses are used to achieve some type of conditionality in the transactions. A P2SH address works in a same way as a legacy address would but instead of the address pointing to a public key, it points to a script. The sender does not see this script but can identify it as a P2SH address from the prefix. (O'Reilly Media, Inc., 2014) (Developers documentation, wallets, n.d.)

5.7 Transactions

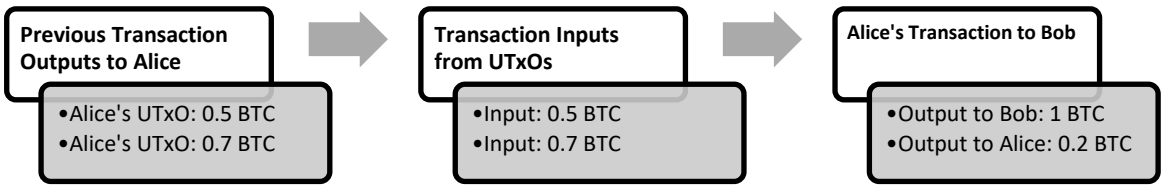
Transactions can be considered as the hearbeat of a blockchain. All the other pieces of blockchain technology ensure that the transactions are validly happening and added to the blockchain. As we saw from earlier chapters, in consensus protocols, the first step is to gather the data that will be stored in a block before creating it. Once a user has created a transaction that has been digitally signed with both parties, the transaction can be broadcasted to the network. Nodes would receive this transaction in different times, and once they have received it, they can start validating it. Once the transaction is validated across almost the full network, it will be added to the block which will then be created and appended to the blockchain. Now, in situations where a node gets another transaction before the previous one has been validated across the network, the pending transaction will enter a so-called “mempool” to wait as a unconfirmed transaction. The mempool is a vital part of the transaction process and it can be used as a meter of one sort to indicate the network congestion. (Wiesflecker, 2020) (Mempool, n.d.)

In blockchain systems, there are two types of transaction models, account/balance and UTxO models. Account based models, used by Ethereum, are similar to what people are used to in traditional banking. The blockchain system keeps track of users account balances and when making transactions these balances are then accordingly moved from one account balance to another. UTxO based models however, differ from the usual in a way that instead of keeping record of the account balances, the system keeps record of the UTxO's and therefore the transactions consists of inputs and outputs of which UTxO's will then be spent accordingly. This is a clever, even though non-intuitive way of recording a ledger. (O'Reilly Media, Inc., 2014) (Frankenfield, 2020)

5.7.1 UTxO Model

UTxO (Unspent Transaction Output) is a part of transaction based models functionality, firstly presented by Bitcoin. UTxO model spends UTxO's (Outputs) as inputs and from these inputs, produces new UTxO's. So it is a continuum of inputs and outputs where the unspent outputs represent user's spendable balance.

Figure 13. UTxO Example (Bitcoin's UTxO Model, n.d.)



Lets break Figure 13 in pieces for better understanding;

1. Alice has received 1.2 BTC in two different outputs. These are two separate UTxO's worth 0.5 BTC and 0.7 BTC.
2. Alice wants to pay Bob 1 BTC. Since the UTxO's are worth 0.5 BTC and 0.7 BTC, she will use both UTxO's as the transaction inputs.
3. Alice creates a transaction with two outputs; 1 BTC to Bob and 0.2 BTC back to herself.

4. Now Bob has an UTxO worth of 1 BTC and Alice has an UTxO worth 0.2 BTC which can then be spent by inputs in upcoming transactions.

To be noted: In real situations, Alice would have to pay some transaction fees, so for example, the transaction to Bob could create outputs of 1 BTC to Bob and 0.19 BTC to Alice which has fees deducted from.

Now, in a case where Alice has one UTxO worth of 100 BTC's and she wants to send Bob only 2 BTC's. The whole 100 BTC's worth UTxO would be spent by a transaction input that would then create outputs of 2 BTC's to Bob and 98 BTC's back to Alice. So in simple terms, UTxO's cannot be divided and must be used as a whole. The "change" will be then sent back as a smaller UTxO.

The transactions in a blockchain can be considered as a chain itself too. Every transaction created will refer to the previous outputs received and every transaction includes inputs and outputs. Since all the transactions are recorded in the public ledger (the blockchain) and are validated and confirmed by the blockchain network, it makes the transactions transparent and irreversible.

Though there are no user-made transactions without inputs in blockchain network, in Bitcoin network, there are so-called "Coinbase Transactions" which are simply the miner rewards, coins that are generated by the system once a block is created. (O'Reilly Media, Inc., 2014) (Bitcoin's UTxO Model, n.d.) (Developers documentation, transactions, n.d.) (Frankenfield, 2020)

5.7.2 EUTxO Model

eUTxO (Extended Unspent Transaction Output) is an innovative model designed and developed by the company IOG which has also developed the Cardano blockchain system. The initial idea was to combine Bitcoin's UTxO model with Ethereum's smart contract ability. UTxO model has several benefits, such as good scalability, privacy and a simple transaction verification but the problem with the basic UTxO model is the turing-incompleteness. Turing completeness in short is a term used in computer sciences that refers to a systems ability in solving any computation problem, usually via a programming language. IOG wanted a way to keep the benefits of the UTxO model but with added flexibility to handle more than just payment transactions. The way they managed to extend the UTxO model was by allowing UTxO's to hold arbitrary data on top of funds and logic

in the form of scripts that'd essentially monitor the transaction for validity. If the script conditions return true, the transaction can be processed and outputs spent.

The benefits of using an extended UTxO model is that it allows smart contracts ability, and maybe most importantly, it allows the fees to be predicted accurately.

(Sanchez, 2021. -a) (Sanchez, 2021. -b) (Przybilla, 2021)

5.8 Smart Contracts

The data that is stored in a block can contain information of various factors such as who, what, when, where, how much or on what conditions. A Blockchain can also include smart contracts which are programs with pre-defined conditions that will be ran automatically when these conditions are met. Smart contracts bring vast amounts of flexibility and diversity to the capabilities of a blockchain. (Smart Contracts, n.d.)

Smart contracts can be used for various of circumstances; financial, healthcare, insurance or whatever type of services that in some way need to have a conditional outcome. Many of the applications that are represented in the later chapters rely on smart contracts. Obviously, smart contracts always need a smart contracts able blockchain system as a backbone. Bitcoin for example has possibilities in adding conditionality in the transactions as scripts but Bitcoin in the core is developed to not be "turing-complete". Ethereum and Cardano in contrary to Bitcoin are turing-complete systems that we'll talk more in their representive chapters.

Smart contracts give the ability to create and process contracts of any sort of complexity without an interfering third party. What makes the smart contracts intriguing is the transparency that they can provide. For an example it is possible to make a contract on exchanging some asset of value with an unknown entity. Funds are locked in the contract and held there until the counterparty fulfills their end of the contract with the goods. If all of the conditions are met, and the assets are verified to be what was agreed by the contract, it can be broadcasted to the network and validated so both parties will receive their goods. Now, in a case where the counterparty never fulfills their end of the contract, the funds would be released and refunded automatically after a pre-defined period of time. Parties never have to actually be in contact with each other but nonetheless can trust that the contract will be solid.

Of course, smart contracts, as they are essentially pieces of program code, written by a person, can include bugs. The blockchain platforms and their smart contracts programming language of choice can, however, have a huge impact on the fault tolerance.

Recap of smart contracts benefits:

- No need for intermediaries
- Documents do not get lost
- Security in terms of hacking
- Process is fast
- Fewer human errors

(Rosic, 2020)

5.9 Blockchain Security

On top of all the cryptographical, technical details that are mostly “hard coded” in the system, a blockchain security is very much about having a big enough, distributed enough, functional P2P (Peer-to-Peer) network up and running. With these reasons, many major platforms are developing their blockchain systems with decentralization as a one of the top priorities. With smaller or non-distributed systems the blockchain will be prone to security threats like 51 % attack. Having someone control over 50 % of the network will lead to the fact that they’d basically have full control of the network and could perform several malicious acts. To be noted, this matter mainly concerns only the public blockchains.

5.9.1 Decentralization

Decentralization in blockchains can be associated with many things from socioeconomics to political economies, but foremost on technological aspect, decentralization makes a truly trustless, provably secure and coherent network possible. Having a truly decentralized peer-to-peer network handling and validating transactions in a trustless environment makes not only fund transactions but also so-called smart contract abilities possible without the need for an interfering third party. These features may make blockchains a viable platform for providing alternatives for

various of societal functions such as digital voting, digital identities, financial systems and thus banking the unbanked etc. We will be talking more about the use-cases and applications in later chapters.

5.9.2 51% Attack

A scenario where someone has gained the control of over 50 % of the network is called a 51% attack. Hypotethically speaking this is possible even in the bigger networks but for example in a blockchain network that uses PoW (Proof-of-Work) consensus algorithm which ultimately requires computing power or hashing power to be exact, over 50 % of the networks hashing power would require a very powerful supercomputer which is practically impossible. In a PoS (Proof-of-Stake) network on the other hand one should own 51 % of the staked cryptocurrency which would be extremely expensive and difficult to obtain. Cardano platform, which is a PoS platform, has >70% of the total token supply staked, which means no exchange even has enough liquidity to provide >50% of the tokens.

A succesful 51% attack can be used for various of malicious acts, such as gaining a mining monopoly in a PoW network and preventing some or all other users from mining, thus gaining all the rewards from mining. There can also be block tampering which can be used for double-spending. (51% Attack, 2021) (Frankenfield, 2021)

5.9.3 Double-Spending

Double-spending is a scenario where a cryptocurrency is spent more than once and the blockchain is tampered in a way that it looks like these transactions never occurred. These scenarios have happened before, and one of the biggest malicious acts was in May, 2018 when a cryptocurrency “Bitcoin Gold” suffered a 51% attack. The attackers were able to double-spend transactions for several days, ending up stealing more than 18 million US dollars worth of Bitcoin Gold. (Frankenfield, 2020)

6 Cryptocurrency Comparison

This chapter introduces, superficially, four different cryptocurrencies; Bitcoin, Ethereum, Cardano and Ergo. These cryptocurrencies have been selected principally because Bitcoin, Ethereum and Cardano can be roughly sperated into three different blockchain generations with their "signature" innovations. Ergo on the other hand, is an interesting blockchain because it includes some properties of all the three previously mentioned blockchains. These four cryptocurrencies should give a good overview on why and how different technical approaches are utilized in different blockchains and how the blockchain technology has evolved from the Bitcoin era.

6.1 Bitcoin

Bitcoin was made to provide an electronic payment system based on cryptographic proof rather than a trust based proof so people would not have to rely on a third party when transacting payments. This kind of decentralized payment system makes completely non-reversible transactions possible and thus lowers the trust required between merchant and customer and therefore reduces the need to gather excessive customer information.

Bitcoin, being the pioneer of modern blockchain technology and cryptocurrencies, created a foundation for other major cryptocurrencies and it has always been the market capitalization leader of all cryptocurrencies. Nonetheless Bitcoin also has flaws, such as enormous energy consumption from the mining process, turing-incompleteness that does not allow smart contracts ability, slow and expensive transactions and high volatility price-wise. These flaws are something that other cryptocurrencies are essentially trying to solve, such as Ethereum providing smart contracts, Cardano provides predictable low fees and low energy consumption with smart contracts ability and so on.

As we have used some examples of Bitcoin's approach to technical functions in blockchain technology, lets remind us of some main points of Bitcoin network;

- Public Blockchain
    - Anyone can participate in sending transactions or become a miner in the blockchain.

- Proof-of-Work
    - Consensus protocol that validates blocks to the blockchain via mining. Proof-of-Work algorithm in Bitcoin is not ASIC-Resistant, which leads to a huge energy consumption.
    - Mining rewards halve every 210,000 block or roughly every four years, which means that the total token supply will be mined in year 2140.
- UTxO Model
    - Transaction model that records unspent outputs of transactions as fund balances. Transactions consists of inputs and outputs that can also include some conditionality, although unable to have smart contracts due to turing-incompleteness.

6.2 Ethereum

Ethereum was designed to bring blockchain technology and cryptocurrencies to a next level via programmability. Ethereum successfully implemented smart contracts ability in their platform and thus begun a new chapter in blockchain era. Programmability in Ethereum has brought many developers to build on top of Ethereum. dApps (Decentralized Applications) that we will look more in-depth in chapter 7.1 have included many innovative ideas that use Ethereum blockchain as their backbone. dApps made by Ethereum have included DeFi (Dezentralized Finance), NFT's (Non-Fungible Tokens), DAO's (Decentralized Autonomous Organizaion), games etc.

As we saw from earlier (Figure 7), Ethereum transaction fees are much higher than a comparable Proof-of-Stake blockchain system. This is because all the dApps running on Ethereum generate more transactions, which then requires more fees to be paid and more mining to happen. Not only that the fees can get expensive, but the energy consumption is also growing. For the time being, in Jan. 2022, the annual energy consumption of Ethereum can be estimated to be up to almost 110 TWh. This is, of course, acknowledged by the Ethereum core developers and there are plans to make a major upgrade from Ethereum to Ethereum 2.0.

Ethereum 2.0 would, among other things, concentrate on introducing a new proof-of-stake consensus algorithm to their network that could by estimate reduce the total energy use by 99.95 %. The merge to an already functional proof-of-stake chain, called the "Beacon Chain" is supposed

to happen in the first half of 2022. (Ethereum Foundation Blog: Ethereum's energy usage will soon decrease by ~99.95%, 2021) (Energy Consumption, 2022) (Gulley, 2021) (Energy Consumption, 2022)

6.3 Cardano

Cardano, the design and development of which begun in 2015 can be categorized as the third generation of blockchain technology. Cardano is trying to work, amongst other things, the problems that lie in Ethereum network, which are the high fees and emissions. As told in Cardano website “The story began in 2015, with a vision of addressing the three strategic challenges facing all blockchain networks: scalability, interoperability, and sustainability.” (Byron - Foundation, n.d.)

IOG (former IOHK) which is the company behind Cardano’s design and development is also behind the Ouroboros proof-of-stake protocol, which is the first provably secure PoS protocol. This proof-of-stake mechanism provides very low energy consumption within the network and makes predictable low transaction fees possible.

Cardano is very fond on making the blockchain development formal and the development is completely based on peer-reviewed academic research. All this research and academic papers are publicly published thus making the Cardano blockchain a massive open-source project. (Cardano, n.d.) (Cardano Roadmap, n.d.)

6.3.1 Cardano Development Flow

The Cardano blockchain network has 5 phases in the roadmap to become a truly decentralized and self-governed network. From the launch in September 2017, Cardano network was federated in the first phase of roadmap but the second phase that was launched in 2020 was all about making the network more decentralized with the help of nodes and node operators or as in Cardano network they’re called stake pools and SPO’s (Stake Pool Operators) This phase was predicted to make the network 50–100 times more decentralized than some other large blockchain networks with nearly 1000 stake pools in the end of this phase. At this time in December 2021, there are over 3000 stake pools operating. The third phase introduced the smart contracts ability in September 2021 which has now in Jan. 2022 brought the first DeFi dApps to the Cardano network.

The upgrades of the fourth phase will take place throughout the year 2022 is about scaling the network to handle all the dApps will be be launching on the network. The last phase of Cardano roadmap is about making the network completely self-sustaining with a voting and treasury system where a network user can vote on the direction of the blockchains future development. (Seth, 2021) (Cardano Roadmap, n.d.)

6.4 Ergo

Ergo is a blockchain project that has a similar approach as Bitcoin did but Ergo can be in a sense considered a modernized version of Bitcoin. Ergo is, as Cardano, using EUTxO model which allows the use of smart contracts in their transactions. Ergo's scripting language "ErgoScript" is based on sigma protocols which are in a very brief description parts of cryptographical proof-of-knowledge. ErgoScript by nature excludes some operations such as infinite loops though it doesn't exclude operations so much to be considered turing-incomplete, which is why it can be used in variety of smart contracts, in a secure way.

Ergo is a Proof-of-Work protocol with the implementation of NiPoPoW's (Non-interactive Proofs of Proof-of-Work) with their consensus algorithm "Autolykos V2". NiPoPoW, without going too much into details, enables the possibility for a computer program to verify an event on a PoW blockchain without actually connecting to the blockchain network. Autolykos algorithm is ASIC-Resistant and also designed to be memory-hard, which basically means that it is possible for ordinary users with lower hashrates to compete with bigger mining farms and earn mining rewards, even with a single gpu desktop computer. (Chepurnoy;Kharin;& Meshkov, 2019) (Non-Interactive Proofs of Proof-of-Work, n.d.)

Ergo, just like Bitcoin but contrary to Ethereum, has a limited supply of tokens. The difference is that Ergo's emission schedule is much shorter than Bitcoins. Ergo's emission schedule will last for 8 years, which means that the full token supply will be mined by 2027. (Basics, n.d.) (Ergo Whitepaper, 2019)

7 Practical Applications

Blockchain technology, after the innovation of smart contracts, has brought many possibilities to extend the original idea of a blockchain, which was by Bitcoin, to be used as a electronic payment system in a decentralized way. dApps and smart contracts provide possibilities in decentralized finance solutions, decentralized autonomous organization systems, digital voting and much more.

7.1 dApps

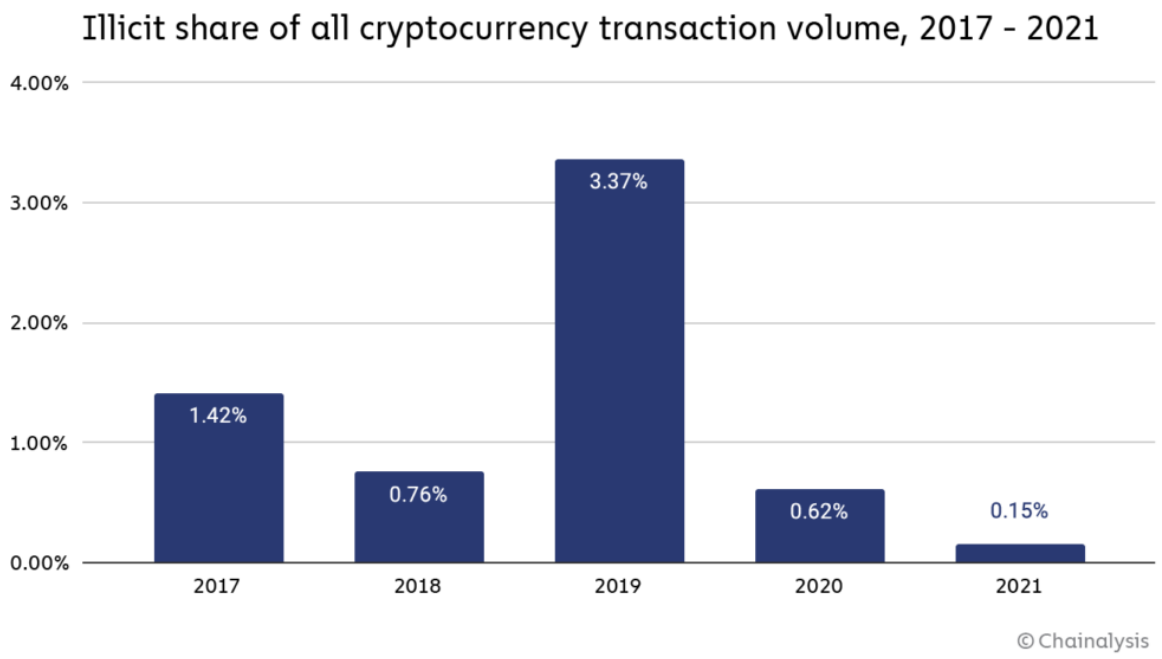
dApps in their simplest sense are just like any other applications, just without a centralized authority. There are basically no restrictions on what applications can be considered a dApp as long as it is decentralized. Blockchains provide this decentralized infrastructure to build on top of, which is why most of the dApps are functioning on-chain. Although there are possibilities to have an application working off-chain, such as some blockchain tracking or data gathering applications. However, these kind of off-chain applications most commonly have a centralized server behind them which is why they can't be really considered as dApps.

dApps have their pros and cons, pros being for example their transparency, coherency and performance. For example, with a decentralized finance solution it is possible to transfer millions of dollars worth of assets on-chain without anyone asking any questions. These transfers can happen almost immediately with very low costs and it can be trusted that the application processes the transfer just like any other transfer. Now on the other hand, these dApps are just like any other applications, programmed by a human being, meaning that bugs may occur and security breaches may happen that can lead to loss of funds. Because of the decentralized nature, there are really no authorities that could refund the user which makes some of the dApps and DeFi solutions questionable at least. Debugging and updating a dApp may also be quite difficult due the nature of blockchains in general. The majority of nodes would need to agree on every update, thus making it more arduous than a regular application update would. Currently, accessing dApps is not as easy as a regular application download would be. For many dApp solutions, a suitable wallet and a browser that supports an external dApp connector is needed. (Cointelegraph: What are dApps?, n.d.)

7.2 Illicit Acts

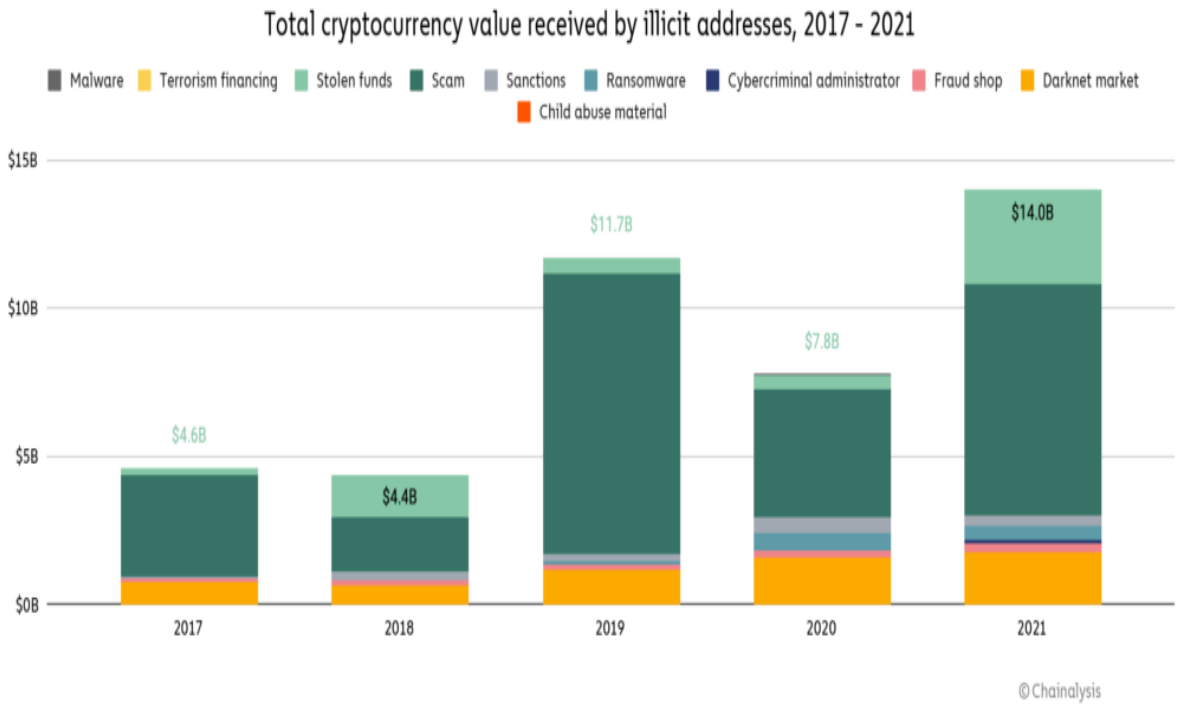
Illicit acts have to be noted when talking about decentralized solutions with no authority of any sort and every transfer essentially happening anonymously. It is true that cryptocurrencies are often connected to the use of illicit acts and there are cases where for example ransomware attackers ask for payments in cryptocurrencies. However, often against the general perception, illicit activities are only a fraction of the total cryptocurrency use (estimately 0.15 % in 2021 as seen in Figure 14).

Figure 14. Chart on Illicit Share of All Cryptocurrency Transaction Volume 2017-2021 (Crypto Crime Trends for 2022, 2022)



This doesn't necessarily mean that the amount of value used to illicit acts in cryptocurrencies is getting smaller but rather that all the legitimate use of cryptocurrencies is expanding as seen in Figure 15.

Figure 15. Chart on Total Cryptocurrency Value Received By Illicit Addresses 2017-2021 (Crypto Crime Trends for 2022, 2022)



Another thing that needs to be pointed out is that most of the cryptocurrency related illicit acts are in matter of fact of scams and stolen funds. Most of the illicit acts happen especially in DeFi protocols, which is not surprising considering the fact that in 2021 DeFi transaction volumes grew by 912 %. (Crypto Crime Trends for 2022, 2022)

7.3 DeFi

DeFi (Decentralized Finance) is an innovative financial solution utilizing the blockchain technology that, in a sense, allows people to be their own bank. DeFi protocols for example lets users to lend cryptocurrencies for interest, borrow funds using cryptocurrencies as collateral, buy insurance, trade derivatives and assets, have a savings account with typically better interest rates as from traditional bank, provide liquidity for earning yield etc.

Currently, Ethereum is by far the market leader in DeFi in terms of TVL (Total Value Locked). By estimate, today in Jan. 2022 Ethereums TVL is around 115 billion US dollars. (Ethereum, 2022)

DeFi is an attractive alternative for holding and managing assets for various of reasons, such as:

- Users hold their own money and assets, no need to transfer their funds to a third party
- Transactions happen fast and fees are low, no matter how big the transaction is
- Interest rates are typically higher than in traditional finance
- Anonymity, DeFi protocols usually don't need to know their customers or gather any user details
- Trustless, DeFi protocols will function as programmed, no chance for human errors or other difficulties
- 24/7, DeFi protocols have no office hours, DeFi operates around the clock, every day of the year
- Bank the unbanked, unbanked people can get access to finance solutions they'd otherwise wouldn't have

(What is DeFi?, n.d.) (DeFi, A comprehensive guide to decentralized finance, n.d.) (Sharma, 2022)

7.4 DAO

DAO (Decentralized Autonomous Organization) is an organization that consists of community members who have authority over any central leadership. DAO's can have wide-variety of purposes such as charities, investments, fundraising, project organization etc.

DAO's have few features that are needed for the complete functionality of the decentralized autonomus organization. DAO's have to have a set of rules that define the operation of a DAO token. DAO tokens can be used by the organization community to for example, vote, use on activities, enable features etc. These tokens are cryptocurrencies of one sort that can be exchanged and thus, will have value, depending of course on the project adoption and popularity.

Projects that let the community decide the development course usually vote via a "governance token". This is in a sense a type of a DAO system used on a development project. There can be "utility tokens" that are then used in allowing user to perform some sort of action for example modify their metaverse plot of land or such. DAO token is really a generalization that would at least have the ability to be used for governance but can also include uses for utility. (Governance Token, n.d.) (What is a decentralized autonomous organization, and how does a DAO work?, n.d.)

(Decentralized Autonomous Organizations (DAOs), n.d.) (Hackl, 2021) (The Different Types of Cryptocurrency Tokens Explained, 2020)

7.5 Web 3.0

Web 3.0 is a term that is about re-decentralizing the web as we know it. Web 3.0 core ideology is to make networks more transparent, trustless, and permissionless; transparent via making the development and softwares open-source; trustless and permissionless via decentralization and removing the need for trusted and governing third parties. Because the decentralization is such a core part of web 3.0, blockchains are commonly seen to have synergies with the future development of web 3.0, as we learnt from DeFi and DAOs for example, these protocols can be seen as fulfilling the ideologies of web 3.0. (Vermaak, 2022) (Fabric Ventures, 2019)

7.6 NFT

NFT's (Non-Fungible Tokens) are tokens, part of a some blockchain network, that can be basically anything digital from pictures to music etc. NFT's can be created pretty much out of anything digital. NFT's, as they are non-fungible, give the NFT owner full ownership of the asset that can not be copied or counterfeited. NFT's have their fingerprint in a blockchain network that can be used for verifying the authenticity. Currently, most of the NFT's in different blockchain networks are digital art and these are distributed and exchanged in the network. In a sense, NFT's can, at this moment, be compared to collectible cards, some very rare and some not. There are many marketplaces for these kind of NFT's, different for different blockchain networks.

There can be a few reasons of why people would want to buy and own NFT's. NFT's could be considered as a store of value or even an investment and some rare NFT's can raise in value over time. Some NFT's can give the owners special memberships to some restricted communities.

As mentioned, currently most of the NFT's are in form of digital art and are considered as collectibles. However, NFT's have the possibility to be used for example as digital identities, passports, driving licenses etc. NFT's can contain on top of the unique fingerprint some metadata that could very possibly be used for such use-cases as different types of digital licenses. NFT's could also be used as Proof-of-Ownership for physical items, even for real estate or cars. Another

interesting feature of NFT's is that they can be fractionalised which would give opportunities to easily and verifiably own fractions of something. (Non-Fungible Tokens (NFT), n.d.) (Clark, 2021) (Sharma, 2021)

7.7 Logistics

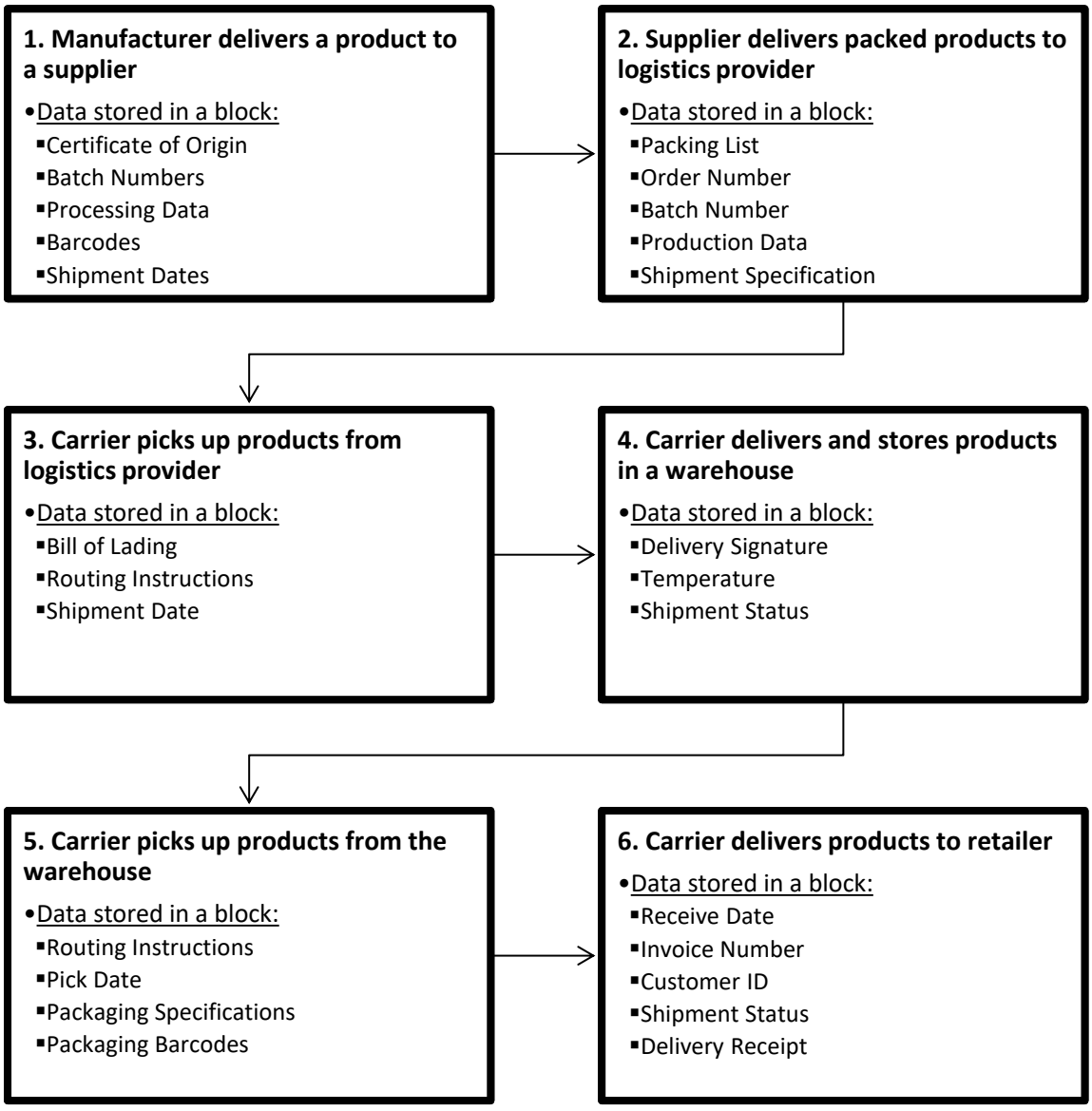
Logistics that may have very complex supply chains and multiple different parties and steps involved in end-to-end process can utilize blockchain technology in multiple areas such as making the supply chain more transparent, faster and thus more efficient, provide better traceability and even in handling the payments to all involved parties. At this moment, logistics supply chain suffer from a lot of manual paperwork, lack of transparency which leads to weak traceability that then leads to various of problems and so on.

Blockchain technology can provide a common platform for all the parties involved in a supply chain which would in one stroke improve pretty much all the problematics that were previously mentioned. Not only that there are a lot of improvements in increased trust, visibility, efficiency, quality etc. Many of the processes can be automated with blockchain and smart contracts, such as payments, transfers of ownership, cargo checks etc. All these things together can reduce transaction costs, possibilities for human errors and slow manual labour.

There are big companies such as DHL, FedEx, Walmart that are either taken or are prototyping these kinds of blockchain related solution implementations in their supply chains. (PwC, n.d.) (Higgins, 2021)

Here is a simple demonstration of how a blockchain could be utilized in a logistics company and how and what information is stored in the blockchain.

Figure 16. Use of a Blockchain in Logistics Example (Globaltranz, 2018)



7.8 Digital Identity

Digital identity is one of the practical applications for blockchain technology. Blockchain based digital identity could be used in many places from IoT devices to vaccination cards. One of the most important use cases would however be people who do not have any kind of identity. There

are by estimate 1.1 billion people around the globe who lack any kind of proof of identity. Lack of identity brings forth different kinds of problems that are for example, enrolling to a school, applying for a job, getting a passport, accessing governmental services etc.

IOG company has taken the lead by signing a partnership with Ethiopia's Ministry of Education in 2021 and will, using Cardano blockchain and a solution named "Atala PRISM", provide digital identity to 5 million students and 750,000 teachers in Ethiopia. This solution will also provide a national attainment recording system that will be able to verify grades, monitor school performance and thus enhance nationwide education etc.

The benefits of a digital identity system is that individuals have more control of the data they want to share. All the information is verifiable, traceable and auditable very quickly via a blockchain solution, the information itself is secured in a blockchain instead of a central data storage and identity thefts become much more difficult. (Cardano Africa, 2021) (Blockchain for Digital Identity and Credentials, n.d.) (Blockchain in Digital Identity, n.d.)

7.9 Digital Voting

Digital voting is a subject with big, critical dilemmas, such as who controls the voting system, how to assure votes are counted correctly, how are votes verified, what if the voting platform crashes etc. Since blockchain is essentially a system that is ran by nodes that are capable of verifying and validating transactions, and by nature, verified data is irreversible and tamper-proof in blockchain, this makes blockchain a propitious platform to achieve digital voting without the previously mentioned problematics. Using a blockchain as a voting platform, even though it could solve all these problems, would still at current state inevitably have an effect in privacy. Since anyone can see the transactions happening in a public blockchain, everyone could also see other people's votes. This may or may not be a problem, depending on the election's nature. However, to achieve the kind of privacy where votes can be verified but are unprovable to others, much more of cryptographical research and work would be needed. As said by Charles Hoskinson (CEO of IOG and founder of Cardano) in a Cointelegraph interview; "If you're just doing a general election where you don't care about privacy, you're counting votes, you can do a billion people. When you want an election where I can verify it, but I can't prove to an outside party that's who I voted for, but at least I know my vote is counted and I want my privacy and I want a paper ballot back up.

And then that's when you get into a situation where you go from billions to thousands, and you have to shard it.". (Kapilkov, 2020)

(Blockchain Voting, n.d.) (Liebkind, 2020) (Kapilkov, 2020)

8 Career in Blockchain Industry

Blockchain technology raises a need for different kinds of experts and developers to work on blockchain industry. Not only are specific blockchain engineers needed for various of tasks but blockchain companies and startups need a lot of support from for example marketing, community management, legal and regulatory counseling, operative support etc. Most of the need for blockchain specialists are especially in finance industry but healthcare, energy and food agriculture industries are also picking up fast.

Research made by Indeed (worldwide employment service) in 2021, pointed out that around one third of regular software developer vacancies were available as remote but specifically on blockchain-related software developers postings almost every second vacancy was available as remote. Also a LinkedIn (worldwide business and employment service) job report made in 2020 showed that the most emerging job was blockchain developer and "Blockchain" was the most in-demand skill out of the top 10 hard skills. These reports can be seen as indicators for a demand that has even made at this point blockchain developers somewhat borderless.

Many big companies like IBM, Cisco, Accenture, Microsoft, Visa and Oracle to name a few are looking for blockchain specialists in their open vacancies. For example IBM had over 400 open vacancies for blockchain-related jobs in 2021 and Cisco and Accenture both had over 200 open vacancies. In addition to big companies, there are also a lot of new startups coming up every year in the blockchain industry. In 2021 venture capitalists invested 33 billion US dollars in blockchain-related startups and most capital was raised in digital asset trading and Web 3.0 focused startups with total deal count being slightly over two thousand.

(Been, 2021) (Pate, 2020) (Melinek, 2022) (The Blockchain Academy, 2021)

9 Conclusion

We have now gained a good overall understanding on where the blockchain ideology started from and how and why Satoshi Nakamoto implemented the Bitcoin that has been a foundation and inspiration to all the blockchains today. We have learnt in-depth how a blockchain works, what are the parts needed to build a functional blockchain and what are the moving parts of a running blockchain; transactions, consensus mechanisms, nodes and how does all this correlate together. We have compared technically different blockchain platforms, we know what different approaches there have been and what innovations have been made along the way to this day. We have a clear picture on what blockchain platforms are, or can be, utilized for and how they can in some occasions affect in the society as we know it. We also gained some insights of the labor markets on blockchain industry and specifically what industries are most interested in exploring utilizement of blockchain systems.

This guide was delimited to provide only the very basic concepts and to give some idea of what can be achieved and built on top of blockchains. Hopefully, this thesis has raised some thoughts and interest to further explore and research blockchain technology and cryptocurrencies because there is still much left unsaid and this technology is evolving at a really fast pace.

References

101 Blockchains. (8.6.2020). *101 Blockchains: Merkle Trees.* https://101blockchains.com/merkle-trees/

Been, E. A. (11.10.2021). *TechRepublic: Cryptocurrency and blockchain jobs listings skyrocket in 2021.* https://www.techrepublic.com/article/listings-for-cryptocurrency-and-blockchain-jobs-skyrocket-in-2021/

Binance Academy: 51% Attack. (18.11.2021). https://academy.binance.com/en/articles/what-is-a-51-percent-attack

Bit2Me Academy: W. Scott Stornetta. (n.d.). https://academy.bit2me.com/en/who-is-w-scott-stornetta/

Bitcoin.org: Developers documentation, transactions. (n.d.). https://developer.bitcoin.org/devguide/transactions.html

Bitcoin.org: Developers documentation, wallets. (n.d.). https://developer.bitcoin.org/devguide/wallets.html

Cardano Africa. (2021). https://africa.cardano.org/

Cardano. (n.d.). https://cardano.org/

Cardano Roadmap. (n.d.). https://roadmap.cardano.org/en/

Cardano Roadmap: 01. Byron - Foundation. (n.d.). https://roadmap.cardano.org/en/byron/

Chainalysis: Crypto Crime Trends for 2022. (6.1.2022). https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

Chepurnoy, A.;Kharin, V.;& Meshkov, D. (6.4.2019). *Autolykos: The Ergo Platform PoW Puzzle.* https://ergoplatform.org/docs/ErgoPow.pdf

Clark, M. (18.8.2021). *The Verge: NFTs, explained*. https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq

Coinbase: What is DeFi? (n.d.). https://www.coinbase.com/learn/crypto-basics/what-is-defi

Coinmarketcap Alexandria: Governance Token. (n.d.). https://coinmarketcap.com/alexandria/glossary/governance-token

Coinmarketcap Alexandria: Mempool. (n.d.). https://coinmarketcap.com/alexandria/glossary/mempool

Coinmarketcap Alexandria: Side Chain. (n.d.). https://coinmarketcap.com/alexandria/glossary/side-chain

Cointelegraph: DeFi, A comprehensive guide to decentralized finance. (n.d.). https://cointelegraph.com/defi-101/defi-a-comprehensive-guide-to-decentralized-finance

Cointelegraph: Soft Fork vs. Hard Fork, Differences Explained. (n.d.). https://cointelegraph.com/blockchain-for-beginners/soft-fork-vs-hard-fork-differences-explained

Cointelegraph: What are dApps? (n.d.). https://cointelegraph.com/defi-101/what-are-dapps-everything-there-is-to-know-about-decentralized-applications

Cointelegraph: What is a decentralized autonomous organization, and how does a DAO work? (n.d.). https://cointelegraph.com/ethereum-for-beginners/what-is-a-decentralized-autonomous-organization-and-how-does-a-dao-work

Consensys: Blockchain in Digital Identity. (n.d.). https://consensys.net/blockchain-use-cases/digital-identity/

Costello, K. (23.3.2020). *From Classic to Hydra: The Implementations of Ouroboros Explained*. IOHK Blog: https://iohk.io/en/blog/posts/2020/03/23/from-classic-to-hydra-the-implementations-of-ouroboros-explained/

Defillama: Ethereum. (25.1.2022). Retrieved 25.1.2022, from https://defillama.com/chain/Ethereum

Digiconomist: Bitcoin - Energy Consumption. (24.1.2022). https://digiconomist.net/bitcoin-energy-consumption

Digiconomist: Ethereum - Energy Consumption. (24.1.2022). https://digiconomist.net/ethereum-energy-consumption

Ergo Platform: Basics. (n.d.). https://ergoplatform.org/en/basics/

Ergo Whitepaper. (14.5.2019). https://ergoplatform.org/docs/whitepaper.pdf

Ethereum Foundation Blog: Ethereum's energy usage will soon decrease by ~99.95%. (18.5.2021). https://blog.ethereum.org/2021/05/18/country-power-no-more/

Ethereum.org: Decentralized Autonomous Organizations (DAOs). (n.d.). https://ethereum.org/en/dao/#what-are-daos

Ethereum.org: Energy Consumption. (23.1.2022). https://ethereum.org/en/energy-consumption/

Ethereum.org: Non-Fungible Tokens (NFT). (n.d.). https://ethereum.org/en/nft/

Euromoney Learning. (n.d.). https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

Fabric Ventures. (31.12.2019). *Medium: What is Web 3.0 & Why It Matters*. https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b

Frankenfield, J. (30.6.2020). *Investopedia: Double-Spending*. https://www.investopedia.com/terms/d/doublespending.asp

Frankenfield, J. (29.11.2020). *Investopedia: UTXO*. https://www.investopedia.com/terms/u/utxo.asp

Frankenfield, J. (25.8.2021). *Investopedia: 51% Attack*. https://www.investopedia.com/terms/1/51-attack.asp

Frankenfield, J. (24.6.2021). *Investopedia: Hard Fork*. https://www.investopedia.com/terms/h/hard-fork.asp

Frankenfield, J. (23.10.2021). *Investopedia: Soft Fork*. https://www.investopedia.com/terms/s/soft-fork.asp

Gensler, G. (2018). *Youtube, MIT OpenCourseWare: MIT 15.S12 Blockchain and Money, Fall 2018*. https://www.youtube.com/playlist?list=PLUl4u3cNGP63UUkfL0onkxF6MYgVa04Fn

Geroni, D. (10.11.2020). *101 Blockchains: Public Blockchain*. https://101blockchains.com/what-is-a-public-blockchain/

Globaltranz. (3.5.2018). *Blockchain Technology in Logistics*. https://www.globaltranz.com/blockchain-technology-transform-logistics/

Gulley, A. (27.4.2021). *Medium: Understanding Ethereum*. https://allan-gulley.medium.com/understanding-ethereum-819c2096b613

Hackl, C. (1.6.2021). *Forbes: What are DAOs*. https://www.forbes.com/sites/cathyhackl/2021/06/01/what-are-daos-and-why-you-should-pay-attention/?sh=57a87e0c7305

Hayes, A. (04.11.2021). *Investopedia: Blockchain Definition*. https://www.investopedia.com/terms/b/blockchain.asp

Hayes, A. (08.12.2021). *Investopedia: Satoshi Nakamoto*. https://www.investopedia.com/terms/s/satoshi-nakamoto.asp

Higgins, M. (8.11.2021). *Forbes: Blockchain in Supply Chain*. https://www.forbes.com/sites/forbestechcouncil/2021/11/08/blockchain-in-supply-chain/?sh=743cbffd4e1a

Hussey, M.;Hamacher, A.;& Chipolina, S. (12.10.2021). *Decrypt: What is Cardano?* https://decrypt.co/resources/cardano

IBM Learn: Blockchain - Smart Contracts. (n.d.). https://www.ibm.com/topics/smart-contracts

IBM Learn: Blockchain Overview. (n.d.). https://www.ibm.com/topics/what-is-blockchain

IBM: Blockchain for Digital Identity and Credentials. (n.d.). https://www.ibm.com/blockchain/identity

Kapilkov, M. (30.10.2020). *Cointelegraph: Future elections could be held on the Cardano blockchain, says Hoskinson.* https://cointelegraph.com/news/future-elections-could-be-held-on-the-cardano-blockchain-says-hoskinson

Kattwinkel, O.;& Rademacher, M. (29.7.2020). *Technical Fundamentals of Blockchain Systems*. https://doi.org/10.18418/978-3-96043-081-0

Liebkind, J. (09.12.2020). *Investopedia: How Blockchain Technology Can Prevent Voter Fraud.* https://www.investopedia.com/news/how-blockchain-technology-can-prevent-voter-fraud/

Liu, Z.;Luong, C.;Wang, W.;Niyato, D.;Wang, P.;Liang, Y.-C.;& Dong, I. (15.3.2019). *A Survey on Applications of Game Theory in Blockchain.* https://arxiv.org/pdf/1902.10865v2.pdf

Lutkevich, B. (2021). *TechTarget: Cryptographic Nonce*. https://www.techtarget.com/searchsecurity/definition/nonce

MakerDAO Blog: The Different Types of Cryptocurrency Tokens Explained. (11.2.2020). https://blog.makerdao.com/the-different-types-of-cryptocurrency-tokens-explained/

Melinek, J. (5.1.2022). *Report: VCs Invested $33B in Crypto and Blockchain Startups in 2021.* Blockworks: https://blockworks.co/report-vcs-invested-33b-in-crypto-and-blockchain-startups-in-2021/

Messari: Asset Screener. (22.1.2022). https://messari.io/screener

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Non-Interactive Proofs of Proof-of-Work. (n.d.). https://nipopows.com/

O'Reilly Media, Inc. (2014). Mastering Bitcoi*n, Chapter 8. Mining and Consensus.* https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

O'Reilly Media, Inc. (2014). Mastering Bitcoin*, Chapter 4. Keys, Addresses, Wallets.* https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch04.html

O'Reilly Media, Inc. (2014). Mastering Bitcoin, *Chapter 5. Transactions.* https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html

O'Reilly Media, Inc. (2014). Mastering Bitcoin, *Chapter 7. The Blockchain.* https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html

Pate, D. L. (13.1.2020). *LinkedIn: The Top Skills Companies Need Most in 2020.* https://www.linkedin.com/business/learning/blog/top-skills-and-courses/the-skills-companies-need-most-in-2020and-how-to-learn-them

Polkadot: Technology. (n.d.). https://polkadot.network/technology/

Poston, H. (9.3.2021). *Infosec: Blockchain and asymmetric cryptography*. https://resources.infosecinstitute.com/topic/blockchain-and-asymmetric-cryptography/

Przybilla, D. (18.12.2021). *Medium: Learning Ergo 101: eUTxO explained*. https://dav009.medium.com/learning-ergo-101-blockchain-paradigm-eutxo-c90b0274cf5e

PwC. (n.d.). *PwC: Blockchain in Logistics.* https://www.pwc.de/de/strategie-organisation-prozesse-systeme/blockchain-in-logistics.pdf

River Financial: Bitcoin's UTxO Model. (n.d.). https://river.com/learn/bitcoins-utxo-model/

Rosic, A. (25.11.2020). *Blockgeeks: Smart Contracts*. https://blockgeeks.com/guides/smart-contracts/

Sanchez, F. (11.3.2021). *IOHK: Cardano's Extended UTxO accounting model (part 1)*. https://iohk.io/en/blog/posts/2021/03/11/cardanos-extended-utxo-accounting-model/

Sanchez, F. (12.3.2021). *IOHK: Cardano's Extended UTxO accounting model (part 2)*. https://iohk.io/en/blog/posts/2021/03/12/cardanos-extended-utxo-accounting-model-part-2/

Seth, S. (29.6.2021). *Investopedia: Public, Private & Premissioned Blockchains*. https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/

Sharma, R. (14.12.2021). *Investopedia: Non-Fungible Token (NFT) Definition*. https://www.investopedia.com/non-fungible-tokens-nft-5115211

Sharma, R. (13.1.2022). *Investopedia: Decentralized Finance (DeFi) Definition*. https://www.investopedia.com/decentralized-finance-defi-5113835

Tardi, C. (22.12.2021). *Investopedia: ASIC Miner*. https://www.investopedia.com/terms/a/asic.asp

The Blockchain Academy. (2021). *The Blockchain Academy.* https://theblockchainacademy.com/wp-content/uploads/sites/6/2021/04/2021-Global-Blockchain-Employment-Report.pdf

Turner, D. M. (29.10.2019). *Cryptomathic: Summary of cryptographic algorithms - according to NIST*. https://www.cryptomathic.com/news-events/blog/summary-of-cryptographic-algorithms-according-to-nist

Vermaak, W. (2022). *Coinmarketcap Alexandria: What is Web 3.0?* https://coinmarketcap.com/alexandria/article/what-is-web-3-0

Vote Australia: Blockchain Voting. (n.d.). https://www.voteaustralia.org.au/blockchain_voting

Wiesflecker, L. (21..12.2020). *Medium: Bitcoin Mempool*. https://medium.com/coinmonks/bitcoin-mempool-simply-explained-7f76be235e85

Cardano (blockchain platform). (n.d.). Wikipedia article https://en.wikipedia.org/wiki/Cardano_(blockchain_platform)

Ethereum. (n.d.). Wikipedia article https://en.wikipedia.org/wiki/Ethereum

Gavin Wood. (n.d.). Wikipedia article https://en.wikipedia.org/wiki/Gavin_Wood

Vitalik Buterin. (n.d.). Wikipedia article https://en.wikipedia.org/wiki/Vitalik_Buterin

Zhang, S.;& Lee, J.-H. (7.8.2019). https://doi.org/10.1016/j.icte.2019.08.001