Group 49

Blockchain and Distributed Ledger Technologies

Bachelor Project Spring 2020

Sven Daneel and Bjørnar Hoff
INSTITUTE OF TECHNOLOGY – OSLO METROPOLITAN UNIVERSITY
Software Engineering

Institutt for Informasjonsteknologi

Postadresse: Postboks 4 St. Olavs plass, 0130 Oslo
Besøksadresse: Holbergs plass, Oslo

PROSJEKT NR. 49	
TILGJENGELIGHET Åpen	

Bachelorprosjekt

Telefon: 22 45 32 00

HOVEDPROSJEKTETS TITTEL Blockchain and Distributed Ledger Technologies	DATO 25.05.2020 ANTALL SIDER / BILAG 180
PROSJEKTDELTAKERE Sven Daneel (s325867) Bjørnar Hoff (s325858)	INTERN VEILEDER Eva Hadler Vihovde

OPPDRAGSGIVER Oslo Metropolitan University (OsloMet)	KONTAKTPERSON Tulpesh Patel

SAMMENDRAG

Throughout our joint bachelor thesis at Oslo Metropolitan University, we have created a research report that deals with Blockchain and Distributed Ledger Technologies. The thesis contains a broad aspect of components and use-cases of this technology, including speculative opinions about the future potential of this technology. With the use of diagrams, figures, dictionary, tables, and educationally written structure, we aim to provide the reader with the necessary competence to devour all the contents and use their acquired knowledge to make up their own opinions and thoughts about this technology.

3 STIKKORD Blockchain
Distributed Ledger Technologies
Finance

Preface

The current document is a bachelor project submitted to Oslo Metropolitan University (OsloMet) in the spring of 2020. For continuous flow and readability, the report has been optimized for digital reading, while following specified guidelines in cooperation with internal OsloMet supervisors. Within the document, we have embedded various links, enabling the reader to access additional information and definitions as required. It is also possible to print the document and read it in paper format.

In order to provide a bigger and more complete picture of our thesis topic, we also included subjects that were not necessarily part of our field of studies, such as economics, finance, and blockchain. Therefore, we decided to give our thesis an objective research-based approach, intending to clarify and provide readers with a valuable learning experience.

The document is divided into two phases, providing the reader with a continuous and steady learning curve. Knowledge gathered from chapters in phase 1 (Technological Background) is needed to gain further understanding of the topics discussed in phase 2 (Real-World Usage). Structuring the thesis into two distinct phases allows the reader while progressing through the document, to continuously acquire the knowledge needed to attain a deeper understanding of the complex nature of this technology.

The thesis requires some basic knowledge or understanding of computer science or IT. Internal links provide further definitions or clarification regarding specific blockchain terms or unfamiliar words. Links within the document are recognized by a blue underscore. In the dictionary, one can return to the first occurrence of the dictionary-word for a smoother navigation experience and mitigate the frustration of scrolling through the document and guessing the page number one was reading previously.

In the document, footnotes make reference to external sources. These references are formatted within footnotes and listed in a separate reference list at the end of the thesis. Figures and diagrams are either generated by us (in blue) or copied from the internet. Internet sources are listed under an independent reference list for attachments.

The thesis is built with the vision of an intended continuous thread, starting from the beginning and guiding the reader throughout the document. Consequently, we strongly recommend reading the thesis based on its given structure, with phase 1 followed by phase 2. However, we want to highlight essential chapters 3, 5, 8, 14, 15, 16, 18, 19, due to their importance and thought-provoking nature.

Due to the tremendous size of our thesis, we have determined to build the document with defined and numbered headings to our table of contents. This implementation will greatly enhance and aid while navigating through the thesis in PDF format, independently if the reader is using an Apple or Microsoft product. We highly advocate that the reader has activated the navigation route for the table of contents or uses the indexes related to our thesis. If the navigation contents do not automatically appear in PDF format, it has to be activated through switching on bookmarks.

Table of Content

1 Introduction

We decided on blockchain technology as the topic of choice for our thesis. Our goal was to contribute with an understandable paper that would provide readers with extensive knowledge on the subject and grant them the required competency to tackle this exciting subject. To facilitate its content and make abstract concepts easier to understand, we added various illustrations such as drawings and diagrams. Our thesis includes a broad spectrum of topics needed to understand this technology. Furthermore, we also included arguments regarding the potential future development of blockchain technology by examining businesses that currently apply and have experience with this technology and its use-cases.

1.1 Background and Motivation

It was only during our last year at OsloMet that the idea of our thesis project began to materialize. From the very start, we both shared a common interest in blockchain and distributed ledger technologies, a topic we were very interested in and wanted to investigate further.

As a start, we conducted various extensive searches on Google Scholar and platforms that provided free articles, including thesis papers. We soon realized that information was available here and there, but no primary source had attempted to summarize all essential blockchain technological aspects. We also discussed the topic with family, friends, and fellow students, and learned that the general public possessed limited knowledge. As the majority of people we interviewed conveyed some fascination towards the subject, any lack of know-how could not be attributed to a lack of interest. Their biggest obstacle was that they did not know where to find reliable information on the blockchain or distributed ledger technologies to educate themselves.

Based on our findings, we came to the consensus that we wanted to thoroughly research the subject, intending to provide readers with a complete picture of this fast-evolving technology. With an entire ecosystem standing behind the current blockchain movement, we wanted to gather what relevant information was available to us and summarize it in a thesis paper.

An additional important aim with our work was not only to provide a complete picture but to provide readers with easy to understand information, in order for them to make up their own opinions about the subject. Upon reading our thesis, we wish to motivate and enable readers to think and reflect on how they want to approach this new technology.

Our thesis is a research-based document that investigates the current standing and use of blockchain technologies. Our target audiences are individuals and businesses with little previous technical know-how but who are interested in gaining a better understanding of the current technological advancements in our society. We chose to write our thesis paper in English, as it will reach a larger audience. Furthermore, this thesis can subsequently be used for teaching purposes in the blockchain course at OsloMet, starting in the fall of 2020.

1.2 Authors

We are two bachelor students at OsloMet attending the software engineering program. We both commenced our studies at the same time. From the very start, we enjoyed excellent communication and discovered our mutual interest in technological subjects. Having already successfully worked on various projects, we decided to tackle the challenge of blockchain technology, which in many ways is still in its infancy. During our work, we enjoyed ongoing excellent teamwork and maintained high confidence in each other that we both would give our best.

	Sven Daneel is a 24-year-old software engineer at OsloMet. He grew up in Switzerland but decided to relocate to Norway after finishing primary school. He completed his high school degree at Norges Toppidrettsgymnas (school of elite sports) while being an active ice hockey player. Upon completing his bachelor´s, he will commence a full-time job as a full-stack .NET developer at Experis Academy.
Sven Daneel Sven4696@gmail.com 452 05 607	**Author – Oslo Metropolitan University**

	Bjørnar Hoff is a 25-year-old software engineer at OsloMet. He grew up in Eidsvoll, Norway. Before attending OsloMet, he completed a 1-year study in general sports at Innlandet college in Elverum. Upon completing his bachelor's, he plans to commence his master’s in data technologies at NTNU in Trondheim.
Bjørnar Hoff bjornar_hoff@hotmail.no 976 91 932	**Author – Oslo Metropolitan University**

1.3 Contributors

In this chapter, we want to present important players that contributed to the development of our thesis. During the progression of our work, we were in contact with many different people. We are very grateful for all the advice and support they were able to provide, as it helped to improve the quality of our thesis. Here we would like to present those individuals who had the most significant influence on our work.

1.3.1 Employer

Our thesis project is written and evaluated under the supervision of OsloMet, represented by Tulphesh Patel, who leads the upcoming 2020 fall course blockchain project. The faculty which is responsible for our work is “*faklutet for teknologi, kunst og design*(TKD).” This faculty is part of higher education within technical, art, and design. In addition, the faculty provides for research- and development activities in these subjects.

OsloMet became our employer primarily due to their interest in using some of our thesis work as further learning material within the DATA3780 subject (Applied Blockchain-technology project).

1.3.2 Supervisors

	Upon being informed that we needed a supervisor at OsloMet, we immediately sought out Eva. For us, she was the right choice, as we had already attended some of her previous courses and were very impressed by her knowledge and expertise. Besides, former students suggested her to us as being an excellent supervisor for challenging bachelor projects. While working together on our thesis, she always supported our vision and provided us with valuable advice and support. We met frequently, where we discussed the current progress and challenges in our work. Eva was always approachable and available for tips and advice.
Eva Hadler Vihovde evav@oslomet.no 928 88 788	**Intern supervisor – Oslo Metropolitan University**

	Tulpesh was our external thesis supervisor, as he is responsible for the blockchain course at OsloMet. He was both an important and valuable contact for us. Tulpesh was able to provide us with needed feedback both regarding the structure and content of our thesis. He has contributed to the professional layout of our work.
Tulpesh Patel tulpesh.patel@oslomet.no 960 45 890	**Employer and external supervisor – Oslo Metropolitan University**

1.3.3 Sparring Partner

	For the development of our thesis, we were very fortunate to have Jan Henrik from PwC as our sparring partner. He is the director of the cybersecurity department in PwC. We met towards the end of 2019, where we discussed an initial draft of our thesis work. Since then, we have been fortunate to profit from his network connections.
Jan Henrik Schou Straumsheim jan.straumsheim@pwc.com	**Sparring Partner – PricewaterhouseCoopers (PwC)**

1.4 Task & Solution

Our first aim was to give a general overview of the overall technical aspects of blockchain technology and its digital assets. Thus, the information presented in the first phase of our document is mainly to provide readers with a sound background of this technology. In the second part of phase 2 of our thesis, we explain how this technology is currently implemented in our society and its future potential. Thus, the implementation of the project is divided into two consecutive phases, where the subsequent phase is built on the experiences gathered during the previous phase. The overall project is based on blockchain technology and distributed ledger technologies.

1.4.1 Phase 1 - Task

To define what blockchain technology is, its origin and structural architecture, and how it has developed since its first application. Explain current technological advancements and challenges and its innovative and ever-evolving appearances. In order to describe the implementation of this technology, we mainly discuss the top three digital assets currently in use, namely Bitcoin, Ethereum, and XRP.

1.4.1.1 Solution Methods

In this phase of our thesis, we aim to educate the reader by:

- Describing the history and origins of blockchain technology.
- Describing blockchain technology and its network structure, including its main components.
- Presenting block compositions within the blockchain architecture and their function.
- Assessing and comparing 3 unique consensus models regarding the features of their consensus protocols. Show the importance of protocol consensus and sustainability in order to arrive at a high-level conclusion.

- Describing how Ethereum propelled the crypto space into a new paradigm with its innovative use of smart contracts. In addition, evaluate how these smart contracts work and how they are used today.
- Examining the most prominent favorable and unfavorable aspects of Bitcoin, Ethereum, and XRP.
- Presenting potential solutions regarding current shortcomings of blockchain technology and how various blockchain communities plan to address these challenges.

1.4.2 Phase 2 - Task

Based on currently applied use-cases, examine how blockchain technology is implemented and what career fields most frequently use this technology. Speculate on the future usage of blockchain and digital assets, and where we see this technology being adopted by businesses and individuals. Furthermore, we evaluate and discuss the need for the implementation of blockchain technology in a particular scenario.

1.4.2.1 Solution Methods

In this phase of our thesis, we aim to investigate and present to our readers how this technology is currently being implemented, including its future potential.

- Investigate currently existing legal frameworks available for digital assets and blockchain technology.
- Research Facebook's libra project and their impact on the current financial system.
- Study and present the largest companies in the blockchain ecosystem.
- Investigate the need for a blockchain and how to distinguish different types of blockchains.
- Suggest a use-case where this technology most likely can be realized and expected to highly profit.
- Demonstrate future use-cases where the potential beneficial attributes of a blockchain can be harnessed.
- Examine CBDC's (Central Bank Digital Currencies) and the usefulness of a parallel economy built on this technology.
- Challenge the claim of substituting the monetary currency with a digital asset. Evaluate the feasibility of a country having lost faith in their monetary system to switch to a form of digital currency.

1.5 Appendices with a Decentralized Exchange (DEX) Task

At the end of our thesis, we provide a flowchart with a short explanation that shows the dataflow in a Decentralized Exchange (DEX) and how such a DEX could potentially function. The aim is to provide more tech-savvy individuals with a border plate architecture skeleton that can be further developed to a fully functioning application. The reason we could not write and finalize the full application is due to the extensive research needed to write phase-1 and phase-2 and being only 2 thesis authors. Thus, this appendices section is an additional resource for individuals who wish some guidance on DEX based on a hands-on approach. Nonetheless, the main product of our thesis remains phase-1 and phase-2.

1.5.1 Solution Methods

- Suggest possible technologies required for building and utilizing the DEX
- Explain the dataflow and how smart contracts are implemented and used.
- Explain the different data structures and data types needed for this application.
- Display a flowchart representing the application.

1.6 Work Process

This thesis is an OsloMet bachelor project written by 2 attending students, who are the sole authors of this document. Due to Covid-19, the authors faced additional challenges and difficulties during its development as personal meetings and interactions had to be kept to an absolute minimum. Thus, for communication and research sharing, the thesis evolved based on supporting digital tools such as Skype and OneDrive. In addition, supervision from experts and university supervisors was also a challenge, with difficulties in organizing personal meetings.

1.7 Last Words

This document provides important background knowledge, including some in-depth information, for individuals who are interested in and want to understand how Blockchains and Distributed Ledger Technologies operate. Furthermore, this document can be a valuable source of information for students enrolled in DATA 3780, including its professors. In addition, we as authors, decided to write our thesis in English. Thus, this document is also available to an international audience, including international students at OsloMet, with little knowledge of Norwegian.

The task of writing this thesis has been quite extensive, especially as we are only two authors responsible for all research activities, including the write up of the thesis paper. We found many excellent and highly technical papers on the subject and were consequently able to gain a robust understanding of the topic. This led to a steep learning curve for both of us, and we now wish to bring our gathered knowledge and learning experience to our readers.

When writing our thesis, we as authors, had to face many challenges. Not only was the work written under major COVID-19 restrictions, on a subject still under development with much scattered information. In addition, we were only 2 students to tackle a large amount of work ahead. We also wanted our work to reach a more international audience, which made it necessary for us to write a document in English. As a consequence, additional demands and burdens were added to our work, which included wording challenges and an extensive English language review. Both these aspects significantly increased our workload, including the invested time needed to finalize the document. Looking at our final project, we are not only incredibly proud of our work, including its inherent quality. Still, we firmly believe that also our readers will recognize its importance and benefit from the value of this thesis.

Finally, we are aware that blockchain technology has somewhat suffered from a shady reputation. Media information regarding untraceable and illegal money transactions have made many suspicious as to the legitimacy of this technology. Blockchain today has made huge steps towards becoming a legitimate and useful tool, providing never seen opportunities for society. We, therefore, ask our readers to keep an open mind and set aside any potential prejudices they might have regarding this subject. Based on our objective research on the topic, we hope to be able to clean up some existing misconceptions and provide some understanding as to how this technology functions, including its many promising potentials.

Phase 1 – Technological Background

2 History of Blockchain

The very first steps of blockchain technology can be traced back to the second World war around 1940 when decoding and encryption were used to hide sensitive information from one's enemies. Alan Mathison Turing, a highly skilled English mathematician, computer scientist, and cryptanalyst, was asked to decipher the Enigma Machine.[1] An encryption device extensively used by Nazi Germany to protect its military communications. Turning managed to decode the Nazi ciphertext, giving the French and British allies a massive advantage. In the meantime, the Americans were able to decode the Japanese Encryption device. As a result, the government became increasingly aware of these types of devices and their potential. They soon realized that cryptography could facilitate or safeguard certain communication pathways and wanted to make the technology more broadly accessible. Without realizing it, they set the stage for the foundation of blockchain technology.

Until the 1970s, cryptography was primarily used by the military. This quickly changed when the US government decided to harmonize cryptography by publishing applicable encryption standards, called "Data Encryption Standard." Whitfield Diffie and Martin Hellman created the first public-key cryptography, called the "Diffie-Hellman algorithm." The algorithm works by splitting encrypted keys into pairs, a private-key, and a public-key. These keys could be used to both encrypt and decrypt messages. Both men are known as the founder of public-key cryptography, which is essential for the creation of blockchain technology.[2]

During the 1990s, the idea of anonymous digital cash and pseudonymous systems were brought together into a movement, at the end of 1992, from a group called "Cypherpunks." The group was founded by Eric Hughes, Timothy C May, and John Gilmore. "Cypherpunks" considered all governments to be evil and were ideologically opposed to the idea of any government. [3] Consequently, the goal was to use encryption as a tool to protect individual freedom. Notable individuals stemming from the Cyberpunks and their achievements are Julian Assange (founder of WikiLeaks), Bram Cohen (Creator of BitTorrent), Hal Finney (Main author of PGP 2.0), and many more.

[1] Newman, M. H. A. (1955). Alan Mathison Turing, 1912-1954.Retrieved from https://royalsocietypublishing.org/doi/pdf/10.1098/rsbm.1955.0019

[2] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[3] Lopp, J. (2016). Bitcoin and the Rise of the Cypherpunks. Retrieved from https://www.coindesk.com/the-rise-of-the-cypherpunks

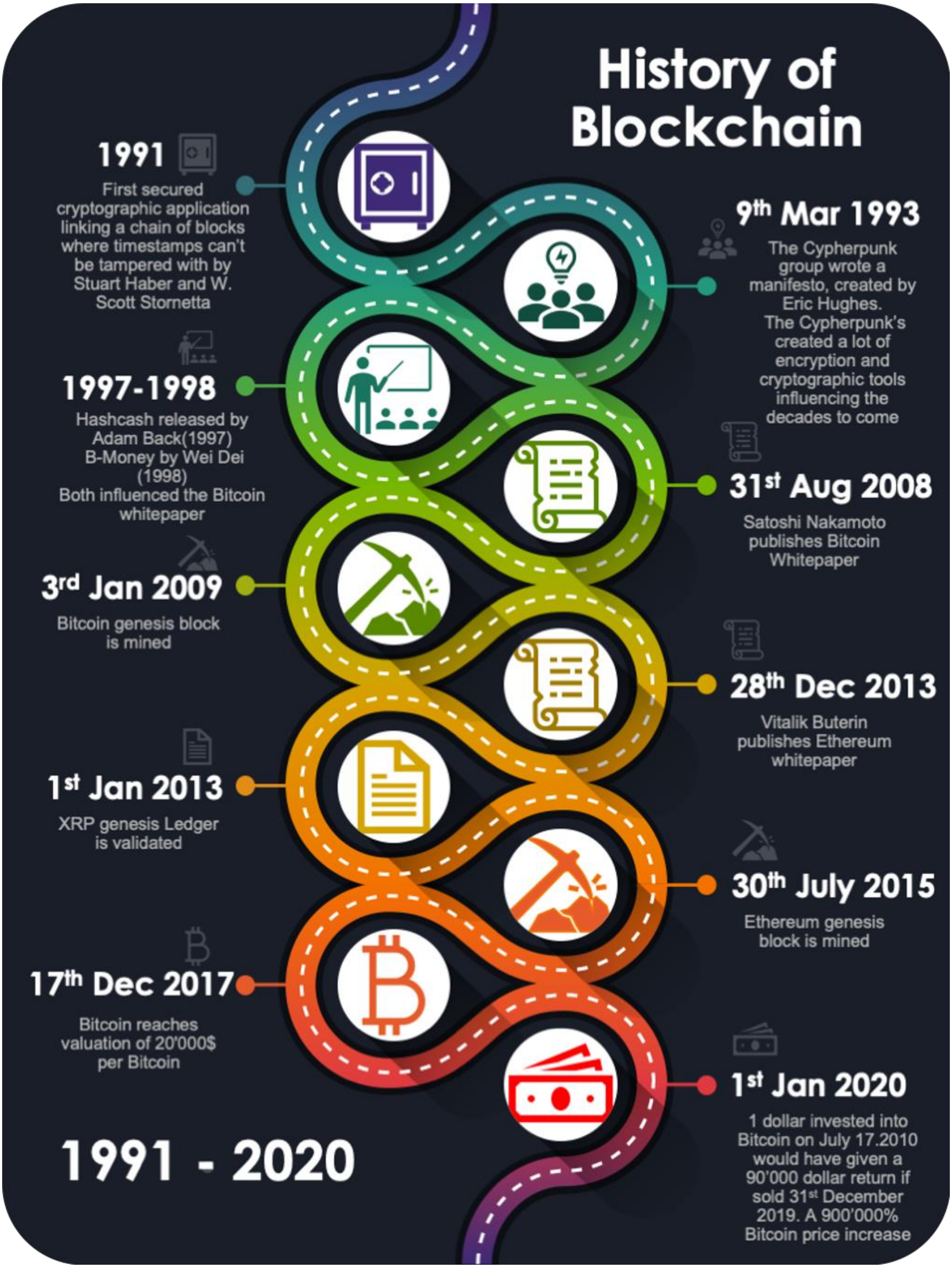
The first secured cryptographic application linking a chain of blocks can be dated back to 1991 by Stuart Haber and W. Scott Stornetta. The aim was to create a network where document timestamps could no longer be tampered with. Shortly thereafter, in 1992, Bayer, Haber, and Stornetta implemented Merkle trees into their system design, which improved the efficiency by grouping several documents into one block. [4]

However, due to the lack of decentralization, these ideas by themselves didn't grab hold. Until a group of individuals or a person on the 31st of August 2008 going by the pseudonym "Satoshi Nakamoto" released "Bitcoin a Peer-to-Peer (P2P) electronic cash system" in 2008. This ingenious invention will forever mark the birth of a decentralized world where one does not need to rely on a third-party/mediator to process transactions, such as a bank.

As the Bitcoin creator "Satoshi Nakomoto" is still unknown, the inspiration and how Bitcoin operates is most likely the result of open-source cryptography researched under the "Cypherpunk" movement. The inspiration for Bitcoin, which was the birth of modern blockchains as we know it today, was taken from b-money and hashcash, also developed by individuals from the "Cyberpunks" revolution. Both projects have directly affected the first blockchain application and its future development. After the release of Bitcoin, developers began to see a huge potential in blockchain and began to explore this technology.

New ideas catapulted the blockchain ecosystem into a hub of innovation, which keeps evolving with its growing community. Below we display a timeline that shows the ideas which influenced the creation of blockchain technology, which origins from the creation of the 2008 Bitcoin whitepaper and influential events that transpired after. We have included a few highlights and main events that we deem worth taking note of and which will be further discussed in this thesis.

[4] Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences Ii* (pp. 329-334). Springer, New York, NY.



History of Blockchain

1991

First secured cryptographic application linking a chain of blocks where timestamps can't be tampered with by Stuart Haber and W. Scott Stornetta

9th Mar 1993

The Cypherpunk group wrote a manifesto, created by Eric Hughes. The Cypherpunk's created a lot of encryption and cryptographic tools influencing the decades to come

1997-1998

Hashcash released by Adam Back(1997) B-Money by Wei Dei (1998) Both influenced the Bitcoin whitepaper

31st Aug 2008

Satoshi Nakamoto publishes Bitcoin Whitepaper

3rd Jan 2009

Bitcoin genesis block is mined

28th Dec 2013

Vitalik Buterin publishes Ethereum whitepaper

1st Jan 2013

XRP genesis Ledger is validated

30th July 2015

Ethereum genesis block is mined

17th Dec 2017

Bitcoin reaches valuation of 20'000$ per Bitcoin

1st Jan 2020

1 dollar invested into Bitcoin on July 17.2010 would have given a 90'000 dollar return if sold 31st December 2019. A 900'000% Bitcoin price increase

1991 - 2020

Figure 1. Blockchain Timeline

3 What is Blockchain

To answer this question, we must first examine where this technology emerged. Interestingly enough, the terminology blockchain did not appear in the bitcoin whitepaper, which is the first application that introduced this technology. The first mention of the blockchain that we could find was an email between the creator of Bitcoin ‘Satoshi Nakomoto’ and Hal Finney (an early Bitcoin developer). In their email exchange, Hal Finney wrote:
“it is mentioned that if a broadcast transaction does not reach all nodes, it is OK, as it will get into the block chain before long.” [5]

Satoshi, in his whitepaper, writes about proof-of-work chains and refers to a chain containing blocks. Therefore, the term blockchain came naturally from the community.

In consecutive chapters within “what is blockchain,” we will define and demonstrate diverse and essential components of a blockchain. Thereby equipping the reader with the necessary insight for understanding all complex factors of this technology.

3.1 Blocks & Ledgers

3.1.1 Block

Blocks represent the building unit where all required data is inserted and bundled together in a specific order. A blockchain consists of many blocks linked together, representing a chain where each block has particular transactions and other data inside it.

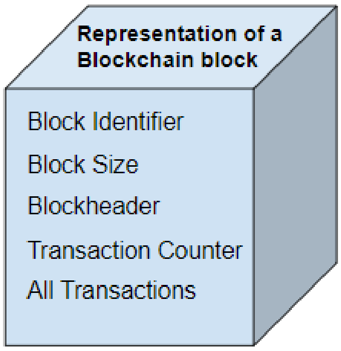


Figure 2. Simplified Block Representation

This is a simplified version of a block for educational purposes; each actual component content of a Bitcoin block will be explained in further detail in chapter 4.

[5] Institute, S. N. (2008). Bitcoin P2P e-cash paper. Retrieved from https://satoshi.nakamotoinstitute.org/emails/cryptography/6/#selection-35.2-37.59

3.1.2 Ledger

A Ledger is very similar to a block, whereas it is a written or computerized record of all transactions that occurred on the network. In essence, the ledger is an item keeping track of fund movements and its attached data contained into individual ledgers that share a link that is connecting other ledgers for a continuous growing documented record of data, which is immutable.

Below we will provide a simplified version of what a Ledger could contain. An example of a real Ledger and its contents can be found in chapter 5.

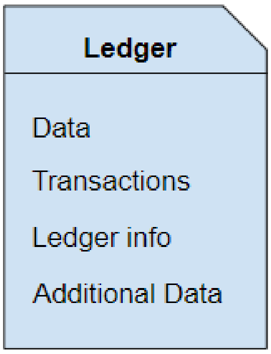


Figure 3. Simplified Ledger Representation

3.2 Nodes

3.2.1 What are Nodes

In the blockchain networks, we often talk about nodes. These nodes can be computers or servers running the digital assets/blockchain software. Nodes can connect with one another and can join and leave the network at any time.

There are two types of nodes in a digital assets network: Full node and lightweight node.[6]

3.2.2 Full Nodes

A Full node connects to a digital assets network. The reason it is called “full node” is that these nodes provide complete validation of each block and transaction that occurs on the network by being checked against consensus-rules.

If any of the transactions do not satisfy these rules, they will get rejected by a “full node” and will not be included in the blockchain.

[6] Asolo, B. (2018). Full Node and Lightweight Node. In. *Mycroptopedia*. Retrieved from https://www.mycryptopedia.com/full-node-lightweight-node/

The main tasks of a full node are:

- Accept transactions and blocks of other full nodes.
- Validate transactions and blocks.

A full node will not approve anything that does not satisfy the rules. A full node possesses a full copy of the entire blockchain history. If a new block joins, this copy will be updated. A network can consist of many full nodes. So, the more full nodes that operate in the network, so the more trustfulness and decentralized the system becomes. [6]

3.2.3 Lightweight Node

A lightweight node verifies transactions in the same way as full nodes. The difference is that a full node requires a full copy of the blockchain to be downloaded. However, a lightweight node only requires to download the 'header' of all blocks in the chain. Therefore, the lightweight node will require less storage and processing power than a full node. These lightweight nodes can be digital wallets or third-party applications that wish to interact with the blockchain but don't want to run the entire history of the network.

Lightweight nodes use a method called SPV (simplified payment verification) for transaction verification. Applying this method, full nodes can accept the lightweight nodes access to the network so lightweight nodes can transmit transactions and notify when a transaction affects them. [6]

The relationship between a full node and a lightweight must exist because if not, a lightweight node could not be able to connect to the network. Lightweight nodes fully trust full nodes that the blockchain contains properly validated blocks and transactions.

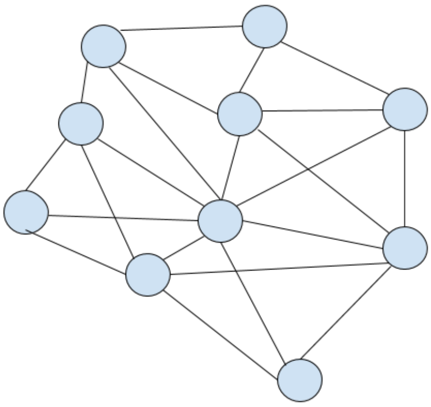


Figure 4. Nodes in a network

3.3 Permissionless vs. Permissioned

3.3.1 Permissionless Blockchain

Bitcoin, Ethereum, and XRP are examples of permissionless blockchains. There are no barriers when it comes to joining the network. Anybody can run a node, access a wallet, and write data into a transaction as well. There aren't any central organizations that you need to report to or ask for permission to access this network.

3.3.2 Permissioned Blockchain

A permissioned blockchain can only authorize a limited set of readers and writers. Here a central entity has full control and decides the attributes of individual peers to participate in the network in order to write and read data from the blockchain.
The most widely recognized permissioned blockchains are Linux foundations Hyperledger Fabric and R3 Corda.

In phase-1, we will mainly focus on and examine permissionless blockchains. However, in phase-2, we will dive into Facebook's libra proposal and take a closer look at permissioned blockchain.

3.4 Problems Satoshi Targeted

Two inherit, main and burdensome problems Satoshi solved are:

- Byzantine fault
- Double spend problem

3.4.1 Byzantine Fault or Byzantine Generals' Problem

A group of generals, each with their own army, surround an enemy castle at different locations. The generals need to agree on whether to attack the castle or retreat. For their action to be successful, they must act simultaneously. It does not matter whether they decide to attack or retreat; the only condition is that they must reach a consensus regarding their decision. As a result, the following requirement must be met: [7]

- Each general must decide to either attack or retreat.
- Upon having decided, their decision cannot be reversed.
- Generals must agree on the same resolution and execute it in a synchronized matter.

[7] Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: the Works of Leslie Lamport* (pp. 203-226).

The prior mention communications problem depends on a few factors being that each general can only communicate with one another through messages relayed through a courier. Ergo the underlying issue of the general byzantine problem is that messages can be either be lost, delayed, or destroyed.

Further complications may arise if a general, for whatever reason, decides to act maliciously and send a fraudulent message, which will lead to total failure of the attack.

If we implement this dilemma in the context of blockchain communication, each general will represent a node in the network. The nodes need to reach an agreement regarding the current valid state of the blockchain. In other words, the majority of network participants of a distributed network have to agree and execute in unison a given action to avoid total system failure.

3.4.2 Double Spend Problem

This is a potential flaw that would make it possible for a digital currency to be spent more than once. Unlike physical cash, a digital token is represented in a digital form and can be duplicated or falsified. [8]

3.5 Centralized vs. Decentralized vs. Distributed

Blockchain technology aims to decentralize the governance structure of the network. In reality, there will always be some sort of central weakness; however, the goal is to reduce centralization as much as possible. The end goal would be to achieve a decentralized system, where nodes in the network do not cluster into more centralized points. We will provide a summary of the current existing networks. Where each blue circle represents a network node, and connecting lines represent communication relations.

3.5.1 Centralized

Most applications use this model today since it applies the client/server architecture. In this architecture, client nodes are directly connected to a central server. Furthermore, clients request access or information from a single server, controlled by a corporation or company.[9] The state of the system is stored on a single computer and managed by a central authority.

[8] Frankenfield, J. (2019). Double-Spending. Retrieved from https://www.investopedia.com/terms/d/doublespending.asp

[9] Hooda, P. Comparison - Centralized, Decentralized and Distributed. Retrieved from https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/

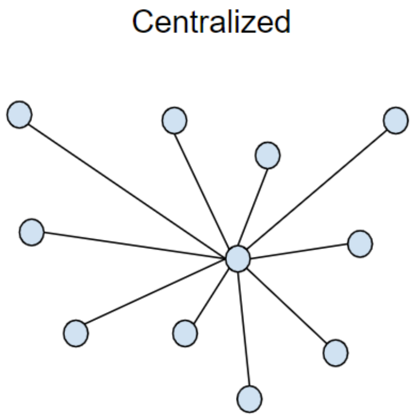


Figure 5. Centralized Network Visualization

PROS	CONS
Simple development and needs less time for developing.	Since the data is owned and controlled by one company or server, errors in the system will bring down the whole network. As a consequence, the system is very dependent on security maintenance and bugs exploitation.
Practical if the data needs to be controlled centrally and is easier to scale up.	Higher security and privacy risks for system users.
Easier to maintain with updates being rapidly performed.	

3.5.2 Decentralized

This model is used in systems that do not want to rely on a central authority that manages the state of the network or the governance structure. Hence, the processing tasks are shared among network participants. Thereby, each governance node on the network has a copy of the entire network data, with each node sharing an identical copy. Furthermore, if a malicious actor tries to make changes or falsify any data, the other nodes on the network will reject these changes as malicious nodes will start to broadcast invalid record versions. This means that each node in the system reaches its own conclusion and shares it with their peers. Collectively they reach an agreement according to governance rules. [10] In a decentralized network, there is no central authority accepting or denying users from participating, transacting, or using the ledger.

[10] Decentralization: A Sampling of Definitions, 1999, p. 13. Retrieved from http://web.undp.org/evaluation/documents/decentralization_working_report.pdf

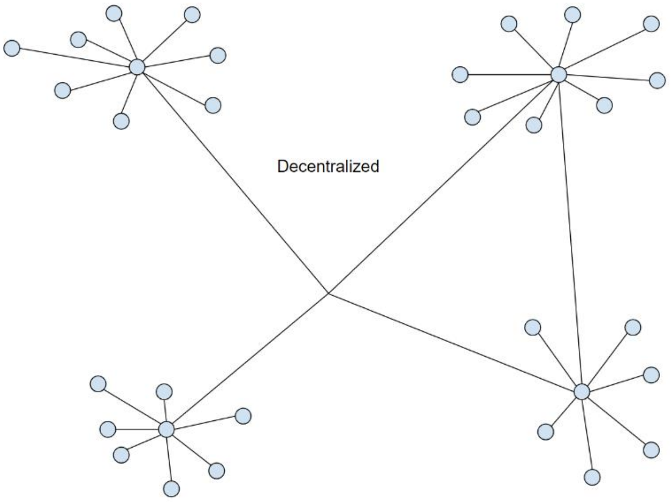


Figure 6. Decentralized Network Visualization

PROS	CONS
High availability across the network since some nodes are always online/available for work.	Due to the more complex decentralized architecture, maintenance costs are higher. Due to nodes acting independently, relying on rules which have to be precise, performance is less consistent when the network is not optimized correctly.
As each node manages its own behavior, there is increased autonomy and control over resources within the network.	As there is no chain of command instructing other nodes to perform specific tasks, the coordination of larger requests becomes increasingly difficult.
It is less likely to fail compared to a centralized system. In the event, some nodes should fail, the impact on the system will not be as consequential as other nodes will still be online able to process transactions or data.	Scaling is a tremendous problematic issue when it comes to a decentralized system. With respect to blockchain, this would represent amounts of transactions the network can process per second.
A decentralized system provides more transparency and accountability to the network and is thus considered increasingly more secure than traditional centralized systems.	

3.5.3 Distributed

This model is similar to a decentralized system in that neither shares a single central owner. In a distributed system, users have equal access to data. The best example of a distributed system is the internet. Distributed systems enable system hardware, software, and data to be shared and coordinated among the network. Distributed can be linked to that the processing and data are shared across multiple nodes, but the decisions may vary from centralized to decentralized. The state of the system is divided over numerous computers across the network. [11]

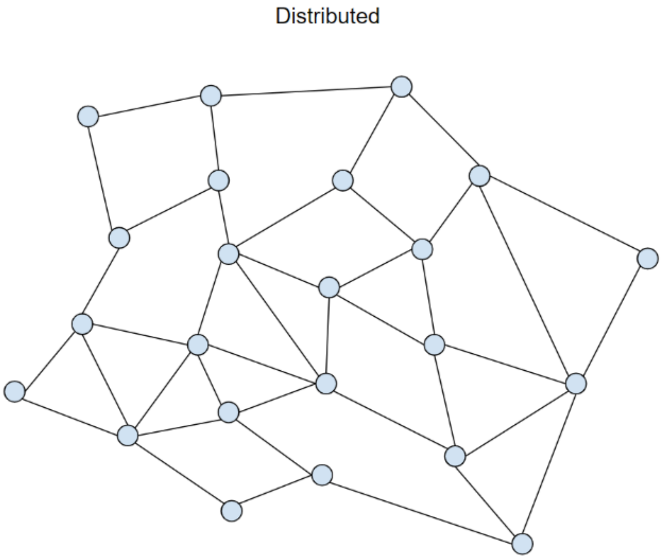


Figure 7. Distributed Network Visualization

PROS	CONS
The architecture of this system promotes resource sharing and good behavioral traits from peer nodes.	As the architecture is more distributed than traditional centralized systems, maintenance costs are higher.
Node failure does not lead to system failure, as active nodes are still available for network communications.	As the network complexity is rather significant, setting up and deploying the distributed system is quite burdensome. This is especially evident when working with separate systems that must work together to achieve reliable results.
Resources can be shared between multiple nodes rather than being restricted to one user or authority.	

[11] distributed systems. (n.d.) *McGraw-Hill Concise Encyclopedia of Engineering*. (2002). Retrieved April 8 2020 from https://encyclopedia2.thefreedictionary.com/distributed+systems

3.5.4 Conclusion Distributed vs. Decentralized Networks

Since both decentralized and distributed systems are very similar, the main difference is that a decentralized system refers to various levels of control. In contrast, a distributed system relates to differences in location.

In the case of a Decentralized and Distributed network, a blockchain consists of both characteristics. Therefore, blockchain is a decentralized and distributed system.

3.6 Blockchain and Distributed Ledger Technologies

While these two terms are used interchangeably, there are distinct differences defining them both.

3.6.1 Distributed Ledger

Distributed ledger flourished from several existing peer-to-peer (P2P) technologies, which were facilitated through the internet like email, file sharing, and other sharing solutions. Furthermore, Distributed Ledger Technology (DLT) is a consensus record with a cryptographic audit trail maintained by a distributed set of computers, which are separated geologically and often referred to as "nodes." These DLT solutions can be decentralized or centralized, depending on the implemented governance structure. [12]
This technology enables system transactions and data to be recorded, shared, and synchronized across a distributed network while being operated by different network participants. As is the case in most blockchain, DLT does not require each node to receive all network information.[12]

3.6.2 Blockchain

Blockchain technology is a data structure used in some implementations of DLT. Blockchain has a shared and replicated ledger history. The history is mutually distributed in a decentralized manner among network governing nodes. In addition, these nodes collectively achieve consensus and agree upon governance structure, and changes applied to the network. Nodes are used for ordering and validating transactions into blocks. These blocks get appended to the chain consisting of previous blocks containing previous transactions. This data structure is considered immutable; therefore, once a block is added to the chain, one can be confident that no one will change the content of the attached block. [12]

[12] WorldBank. Distributed Ledger Technology (DLT) and Blockchain. 2017. Retrieved from. http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

Essentially, blockchain represents a continuously growing list of records. The append-only structure allows data to be added but not removed. As a consequence, a certain degree of database security is maintained.

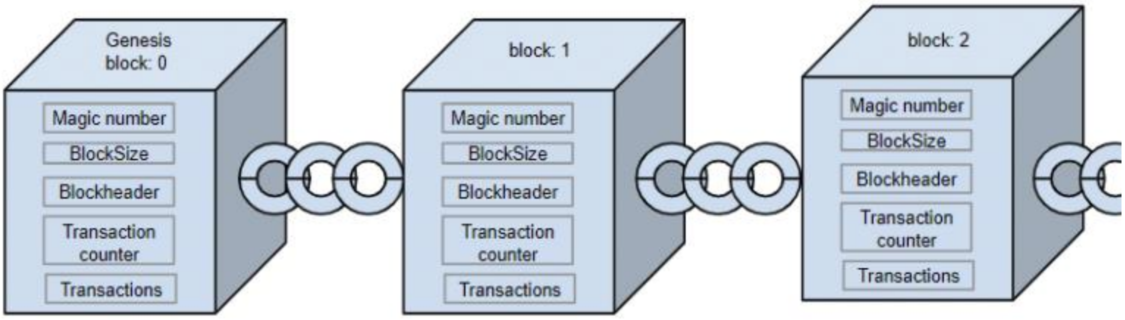


Figure 8. Blockchain visualization

3.6.3 Conclusion Blockchain and Distributed Ledger Architecture

Blockchains and distributed ledgers are very similar but distinct in the way that blockchain technology is an implementation form of a Distributed ledger solution. However, not all Distributed ledger technologies consist of blockchains. In Phase 2 (Real World Usage), we mainly talk about blockchains and their use-case; however, some DLT solutions might also be a viable contender for these topics.

3.7 Transactions

A transaction represents an interaction between two or several parties. [13] In the digital asset world, a transaction is a transfer of digital assets (digital money) between users within the blockchain network. In a business setting, transactions can be a way of recording activities on digital assets. [13]

Transactions can be linked to the trade, purchase, or sale of various items between two or more parties. If we purchase an item in the store, we will get a receipt. We can also follow the transaction through a bank statement confirming that a purchase was performed. In this setting, the bank has control over everything that was bought, including any financial choices made. The banking institution is a centralized system. Thus, the bank has an ultimate say and retains full power over the account. The banking institution is an example of how a centralized system operates. We must trust the banks to keep our money safe.

[13] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

These banks and institutions are intermediaries (middlemen). In a distributed opensource ledger system like Bitcoin, we don’t need to rely on or trust any single body or person. One can send value through the network, without a middleman making decisions to prevent it potentially. Therefore, Bitcoin is censorship-resistance and decentralized.

3.8 Hashing

The basic principles behind blockchain are not complicated. The reason why blockchain seems complicated is due to the digital asset are built on top of this technology. Digital assets, like Bitcoin and many others, have a consensus algorithm that increases complexity. To understand what blockchain is, we need to have basic knowledge about hashing.

Hashing often refers to data of any length injected into an algorithm and receives out a cryptographic fixed-length output. In the Bitcoin example, Bitcoin uses a hashing algorithm called SHA-256. This Is one of several cryptographic hash functions. No matter which size the input is, the output will always have a fixed 256-bits (32 bytes) length. This is visualized and simplified in the two examples below:

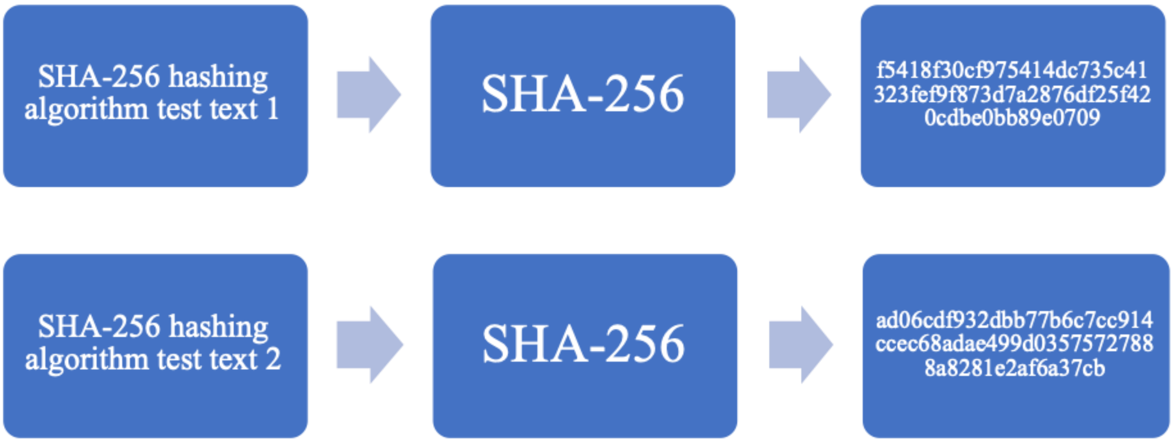

SHA-256 hashing algorithm test text 1
SHA-256
f5418f30cf975414dc735c41323fef9f873d7a2876df25f420cdbe0bb89e0709
SHA-256 hashing algorithm test text 2
SHA-256
ad06cdf932dbb77b6c7cc914ccec68adae499d03575727888a8281e2af6a37cb

Figure 9. SHA-256 hashing visualization

As visualized in the example above, the output of the SHA-256 has a fixed length; however, a small input change will result in a recognizable output change from the SHA-256 hash.
This alteration is consistent whether the transaction is a single word or a complicated transaction with a large amount of data attached.

3.9 Public-key & Private-key Infrastructure

In order to ensure secure money transfer and have complete asset ownership, most blockchains use a public-key and a private-key infrastructure (Asymmetric Cryptography) to secure the digital assets from being stolen. Most blockchains use Elliptic Curve Digital Signature Algorithm (ECDSA) to generate private and public key pairs. An advantage of using this infrastructure is that the algorithm is easy to calculate one direction but extremely difficult to calculate the opposite direction.

3.9.1 Digital Asset Addresses

In order to generate a public key, the system uses a one-way function that inserts the private-key as an input. Therefore, the owner of the public-key can confidently give out their public-key assured that no one would be able to reverse the ECDSA algorithm in order to retrieve the private-key. We will use Bitcoin as an example to illustrate how it works (see figure 8). Alternative blockchains might vary their hashing algorithms but mostly operate the same way.

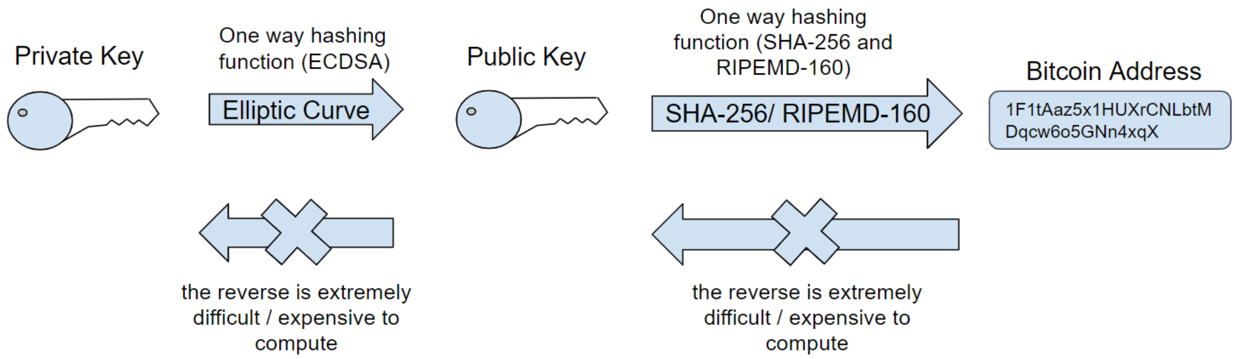

Private Key
One way hashing function (ECDSA)
Elliptic Curve
Public Key
One way hashing function (SHA-256 and RIPEMD-160)
SHA-256/ RIPEMD-160
Bitcoin Address
1F1tAaz5x1HUXrCNLbtM Dqcw6o5GNn4xqX
the reverse is extremely difficult / expensive to compute
the reverse is extremely difficult / expensive to compute

Figure 10. Asymmetric Cryptography, Bitcoin address

Addresses are a string of alphanumeric characters (160bit) that a user can share with anyone from whom they want to receive funds. These addresses are a representation of a public-key. However, to add an additional level of safety, the address will be derived from a one-way hashing function. Thereupon, the public-key is hashed by an SHA-256 algorithm; besides, it is hashed with the RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160).[14] After these two hashes have been successfully implemented, the algorithm produces the Bitcoin address. This is a simplified process for a more detailed explanation click here.

[14] Technical background of version 1 Bitcoin adresses. (2019). In. *Bitcoin Wiki*. Retrieved from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

Bitcoin and many other blockchains addresses appear in digital assets as transactions between two parties, with the addresses signifying the fund recipient and sender.

The private-key gives users control over corresponding digital asset funds. This private-key is used to sign transactions generated by the user. This signature will define ownership and allow users to spend their funds. Therefore, each transaction has a unique digital fingerprint that is established when signing the transaction with its corresponding private-keys. This allows a user to prove that he does, in fact, have ownership over his or her funds.

3.9.2 Digital Signatures

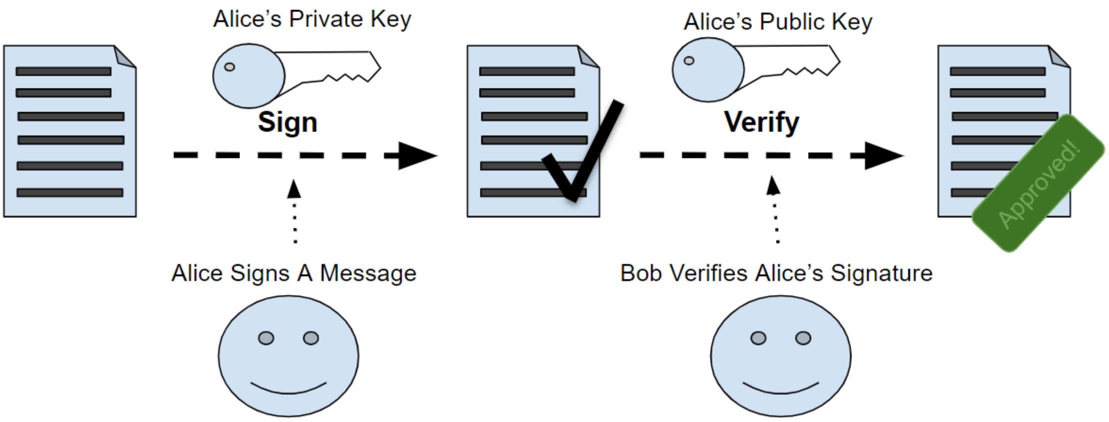


Figure 11. Digital signatures visualization

Digital signatures are essential in any digital asset system, as they verify the authenticity of the transaction. Digital signatures serve as proof of private-key ownership, which authorizes the owner to spend digital assets. Furthermore, individuals can verify with their public-key derived from the private-key, that the transaction is authentic and hasn't been tampered with. Once a transaction has been authorized and signed, it cannot be modified by anyone. [15]

3.10 Digital Assets within Blockchains

Blockchain is the platform that provides digital assets to function. Blockchain is the technology that forms the network, which provides the infrastructure to transact and transferring value or information. Digital assets or cryptocurrencies are tokens used within the network to move value and pay for transactions. Herby digital assets provide the function of a medium of exchange within the blockchain infrastructure.

[15] Paul, E. (2017). What is Digital Signature- How it works, Benefits, Objectives, Concept. Retrieved from https://www.emptrust.com/blog/benefits-of-using-digital-signatures

3.11 Pseudonymity, Anonymous and Transparent

Blockchains can be anonymous where no entity can track network funds and without network participants or nodes being able to trace funds, which is the case of Monero. Monero is a privacy-centric blockchain. In addition, a blockchain can be pseudonymous and transparent like Bitcoin, Ethereum, and XRP. Pseudonymous is the creation of identity. However, the name or personal information is not exposed. The only identity provided by these blockchains is the public address, where one can track all funds on the network. One can look up a specific digital asset lifetime all the way back to its inception, and trace in on the blockchain.

3.12 Divisibility

Digital assets are highly divisible. 1 Bitcoin can be divided into 0.0000001 decimal places, whereas the smallest unit of account is referred to as a satoshi. Other digital assets also share this divisibility quality. However, the amounts of decimal places digital assets can be divided into varies.

3.13 Wallets

A wallet is the backbone of digital assets storage. A user can create an unlimited number of digital wallets to store their digital assets. In order to generate a wallet, users create an ID by writing down a phrase or random words, preferably on paper so as not to be hacked. In the event the computer is destroyed or lost, the user will be required to provide identification through the use of this personalized ID. The ID can be written into a new computer able to run the wallet software, retrieving all originally stored funds in their newly generated wallet.[16]

Wallet software is also responsible for general asset maintenance, creating new addresses, sending, and receiving funds. These wallets may vary from mobile, desktop, hardware, and paper wallets, including many additional convenient options to choose from.

Personally, we highly recommend storing funds in hardware wallets. These types of wallets are also referred to as cold storage wallets, as they are disconnected from the internet, and transactions can be signed without being online. Hardware wallets are small devices that manage to store a variety of digital assets. They are easily transported since they are no bigger than a USB drive.

[16] Bitcoin. (2020) Wallets. Retrieved from https://bitcoin.org/en/wallets-guide#introductions

Figure 12. Hardware Wallet [17]

3.14 Exchanges

So far, digital assets are mostly driven by speculation, as one sells and buys these assets in the hope of some financial gain. These purchases/sales of digital assets are conducted on exchanges. Digital asset exchanges are very similar to traditional financial exchanges; however, so far, they differ from only selling digital assets. Currently, two types of exchanges exist where people can trade digital assets. These are termed centralized and decentralized exchanges. A drawback is that some exchanges are maintained and controlled by companies that must adhere to government regulations. As a consequence, particular countries might decide to ban individual exchanges or digital assets.

3.14.1 Centralized Exchanges

Coinbase, Binance, and Bitmex are examples of centralized exchanges. These are currently the most prominent exchanges on the market since they have a lot of liquidity, including more in-depth order books. A key identifier of a centralized exchange is that they control private and public keys, and according to these centralized exchanges, store assets safely. Therefore, the user's funds are not controlled by the individual but by the exchange. However, these exchanges are targets for hackers, as they have been hacked in the past.

[17] Ledger (Producer). (2020). Ledger Nano X. Retrieved from https://cdn.shopify.com/s/files/1/2974/4858/products/ledger-nano-x-stand-up_grande_7a016731-824a-4d00-acec-40acfdfed9dc_large.png?v=1573828954

As a consequence, investors have lost all their crypto, while thinking the exchange would have safely stored their funds.[18] Most of these centralized exchanges adhere to government regulations and therefore implement Know Your Customer (KYC) [19] and Anti Money Laundering (AML) [20] policies. Each user of these platforms must upload verification like passport, driver's license, or various other identification documents.

3.14.2 Decentralized Exchanges

IDEX, Binance DEX are examples of decentralized exchanges. Here the private keys are held by the users. Conversions between digital assets on decentralized exchanges are handled by smart contracts, which will be further explained in the Ethereum chapter. Smart contracts provide mechanisms needed for directly matching buyers with sellers. The drawbacks here are that these exchanges provide little liquidity and user traffic. This leads to a slower and lagging user experience, which most people don't want to put up with.

As user experience regarding centralized exchange is easier and more developed, most users are comfortable using these types of exchanges. This will likely change as the industry matures, and decentralized exchanges become faster and more scalable.

3.15 Immutable

All transactions and data written into the blockchain are permanent. If person A purchases an item from person B, the transaction is stored permanently and immutably on the public blockchain. There is no way one can retrieve the transaction or change any of the data within a block once it has been confirmed. This permanent feature provides enhanced certainty, that once data is stored on the blockchain, it will remain there insusceptible to change as long as the blockchain remains operational. Furthermore, users of the blockchain can be sure that their wealth and information cannot be tampered with. This assurance is generally provided to users by middlemen (like banks).

Immutability is provided by the system's architecture and by using the SHA-256 hashing function. Each block appended to a given blockchain must contain the previous hash of the previous block. They are thereby creating a chain where the link between each block is the previous hash. Thus creating a tamper-proof network, which does not allow any entity to change data within a block without changing all subsequent blocks previous hash references.

[18] Hackernoon. (2019). Centralized vs Decentralized Cryptocurrency exchanges. Retrieved from. https://hackernoon.com/centralized-vs-decentralized-cryptocurrency-exchanges-explained-simply-639411ecb452

[19] PwC. (2013). [PDF]. Know Your Customer: Quick Reference Guide. Retrieved from https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf

[20] Finra. Anti-Money Laundering (AML). Retrieved from https://www.finra.org/rules-guidance/key-topics/aml

The proof-of-work is also designed to slow down the process of calculating new blocks, thereby slowing down the process to change all the consecutive blocks(details will be explained later). Changing any data within a block will make the previous hash reference unrecognizable and incorrect with the subsequent block's history. The other nodes on the network will notice this alteration, as they will not share the same blockchain history. As a consequence, nodes will reject the changes made.

3.16 Blockchain 1.0 vs. 2.0 vs. 3.0

Blockchains have evolved very rapidly since their first application, which was Bitcoin, due to the permissionless nature of blockchain and allowing free thinkers to experiment and implement new ideas. Therefore, blockchains can be categorized into three generations.

3.16.1 Blockchain 1.0

Bitcoin introduced first-generation blockchains in 2008, which enables scattered people around the world to transfer value without trusting or knowing each other. Individuals quickly discovered the potential of this technology. They saw that the underlying technology had a more general application beyond digital currencies in its capacity to function as a distributed ledger tracking and recording the exchange of any forms of value. [21]

3.16.2 Blockchain 2.0

After a few years in 2013, the second generation of blockchains emerged, designed as a network on which developers were able to create an application. Essentially this was the beginning of the evolution into a distributed virtual computer. Ethereum made this possible with the introduction of smart-contracts functionality, thereby providing a decentralized Turing-complete virtual machine that can execute computer programs using a global network of nodes. The crucial contribution of Ethereum as the second generation of blockchain technology was that it functioned to extend the capacity of the technology from primarily being a database supporting Bitcoin to becoming more of a general platform in order to run decentralized applications and smart contracts. [21]

[21] Bitcoinik. (2019). Blockchain Version 1.0, 2.0, 3.0 And Future. Retrieved from https://bitcoinik.com/blockchain-evolution-1-0-to-3-0/

3.16.3 Blockchain 3.0

The existing second-generation blockchains infrastructures are not efficient enough to handle global usage or large-scale adoption of any applications. Therefore, highlighting the need for a more scalable solution. Third generation blockchains are trying to solve the inefficiency in current second-generation blockchains, and they are currently under development (IOTA, HashGraph, EOS, Lightning Network, Ethereum 2.0). One promising mathematical function implemented in some third-generation blockchains is Directed Acyclic Graph (DAG) . [22]

Scalability remains the most crucial development need for blockchains, and this issue is what blockchain 3.0 is trying to solve.

If a blockchain aims to evolve into a 3.0 model, the aim is to be: [23]

- Scalable, handling equivalent of transactions per second (TPS) as other payment networks like visa (65’000+ TPS)[24]
- Cheap, transaction costs need to be minuscule or non-existent.
- Energy-efficient, these blockchains cannot consume a large quantity of electricity.
- Interoperable, blockchains can easily communicate and transact across other blockchains or platforms.
- User-friendly, mainstream users will no longer need to understand the underlying technology to interact with the blockchain.

These third-generation blockchains aim to help usher in the next generation of the Internet, Decentralized Web, or Web 3.0.

[22] Technopedia. Directed Acyclic Graph (DAG) Retrieved from https://www.techopedia.com/definition/5739/directed-acyclic-graph-dag

[23] Technologies, S. (2018). Blockchain 3.0 & The Future of the Decentralized. Retrieved from https://medium.com/@saratechnologiesinc/blockchain-3-0-the-future-of-the-decentralized-internet-63ba199e2a5

[24] VISA Fact Sheet. (2019). Retrieved from VISA: https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-fact-sheet-july-2019.pdf

3.17 Conclusion What is Blockchain

A Blockchain is a peer-to-peer distributed network that is persistent, transparent public append-only ledger, whereas once data is stored on the blockchain, it cannot be erased or altered. The blockchain appends blocks/ledgers through a mechanism for creating consensus between scattered or distributed set of nodes/validators which do not need to trust each other; they only need to trust the mechanism by which their consensus has arrived at. Furthermore, these nodes/validators dictate network governance. The network ensures safety by using various hashing algorithms and encryption. Funds are transferred across the network by administrating public- and private keys for each wallet created on the network. While public keys are used for received funds, private keys ensure the integrity and make it possible to send and sign transactions.

Depending on the architectural structure of the blockchain, the system can be transparent, and funds can be traceable since their inception, encryption enables a pseudonymous nature, whereas identities are created on the blockchain with addresses. In addition, blockchains can be completely private and anonymous, whereas no entity can trace and see contents of any transaction on the network. Most blockchains associate some form of a digital asset in order to facilitate the actual transfer of value, whereas the blockchain serves as the road or railway through which the value is transferred. The permissionless and innovative nature of blockchain technology allows the technology to evolve and develop at a rapid pace; therefore, establishing giant leaps in improvements and innovative approaches to elevate the technology and its utilization.

4 Blockchain Data Structure Architecture

Blockchain is a public distributed ledger that consists of a chain of blocks that contain information. Each block has a unique hash attributed to itself and linked together by linking to the previous block's hash. This technique creates an immutable ledger that stores only one public official version of all the information stored on the blockchain. Therefore, once data is stored on a blockchain, it becomes almost impossible to revert or change some data inside the block. [25]

This technique establishes a layer of security to a blockchain that is hard to match. If one tried to change some data inside the block, the current hash of the block would change.
Consequently, the link between the blocks would not be correct since the preceding block would have a different previous hash. Still, this technique isn't enough to secure the blockchain. Computers today could calculate millions of hashes per second and recalculate all the hashes of previous or preceding blocks and make a version of the blockchain valid again.

To mitigate this, Satoshi implemented proof-of-work; this is a mechanism to slow down the creation of new blocks. In the event of Bitcoin, it requires an average of 10 minutes to add a new block to the chain. This mechanism is designed to prevent an attacker from tampering with these blocks because if you tamper with one block, you will have to calculate the proof-of-work for all subsequent blocks. The security aspect of a blockchain comes from the use of hashing and proof-of-work puzzle. There is another way blockchains secure themselves, by having nodes and miners distributed around the world, rather than using a central entity to manage the chain, blockchains use a peer-to-peer network. [25]

A grid of nodes creates a shared, decentralized network that communicates with each other and validates new blocks added to the chain. Hence, establishing consensus agreeing upon what blocks are valid and which aren't. Successfully tampering with a blockchain would require one to tamper with all the blocks in the chain, recalculate the proof-of-work for each block and take control of more than 50% of the peer-to-peer network. Only then will the tampered block be accepted by everyone else. [25]

[25] Bitcoin. (2020). Blockchain. Retrieved from https://bitcoin.org/en/developer-reference#block-chain

4.1 Block Components

This is a visual representation of a Bitcoin block and the data contained inside each mined block: [26]

Field	Description	Size
Magic number	In Bitcoin's case, the value is always: 0xD9B4BEF9. This number is used to identify themselves as a blockchain block.	4 bytes
Blocksize	The number of bytes following up to the end of the block. (storage size of the block)	4 bytes
Blockheader	Consist of 6 items (see table below).	80 bytes
Transaction counter	A positive integer (positive number) representing the number of transactions included in the block.	1-9 bytes
Transactions	A list of transactions	Varies from the number of transactions

This is a visual representation of the content inside the Block header: [26]

Field	Description	Size
Version	The current version which the Bitcoin block is on.	4 bytes
hashPrevBlock	A 256-bit hash of the previous block header data.	32 bytes
hashMerkleRoot	The 256-bit hash of all the transactions in the current block. Use the Merkle tree data structure to get this Merkle root hash.	32 bytes

[26] Block. (2019). In *Bitcoin* Wiki. Retrieved from https://en.bitcoin.it/wiki/Block?fbclid=IwAR3HH6Bd0W-pZz82TSVXwjZE5_PJ-peDGS5JnDJJGy2juVBmQFRAW9q5SjU

Time	Current time the block is mined as a timestamp in seconds since 01.01.1970 00:00 UTC.	4 bytes
nBits/Target	It provides the difficulty level of the current block. This is used when miners guess the nonce and hash of the block header data, and miners have to guess a hash that is below or equal to the Target in order to mine the next block.	4 bytes
Nonce	32-bit number, which starts at 0.	4 bytes

4.2 Merkle Tree and Merkle Root

Merkle trees are data structures, where the validity of the content is easily verified. This data structure is particularly useful and is applied in DLT. It is burdensome to verify every single transaction on the network and which would require exponentially more resources to verify all these transactions.[27]

Merkle tree uses hash functions to authenticate the legitimacy of transactions. For example, we have four transactions (ABCD), with each having its own unique hash value. We group them as AB and CD, resulting in a unique hash value for both. Now we merge AB and CD to ABCD and create a new unique hash value at the top of the tree, called a Merkle root. This structure carries the advantage that if we change a single bit in any of our four transactions, the Merkle root will be unrecognizable. As a result, we have a secure and scalable solution for verifying grouped transactions together.

[27] Merkle Tree. *Brilliant.org*. Retrieved 16:42, February 14, 2020, from https://brilliant.org/wiki/merkle-tree/

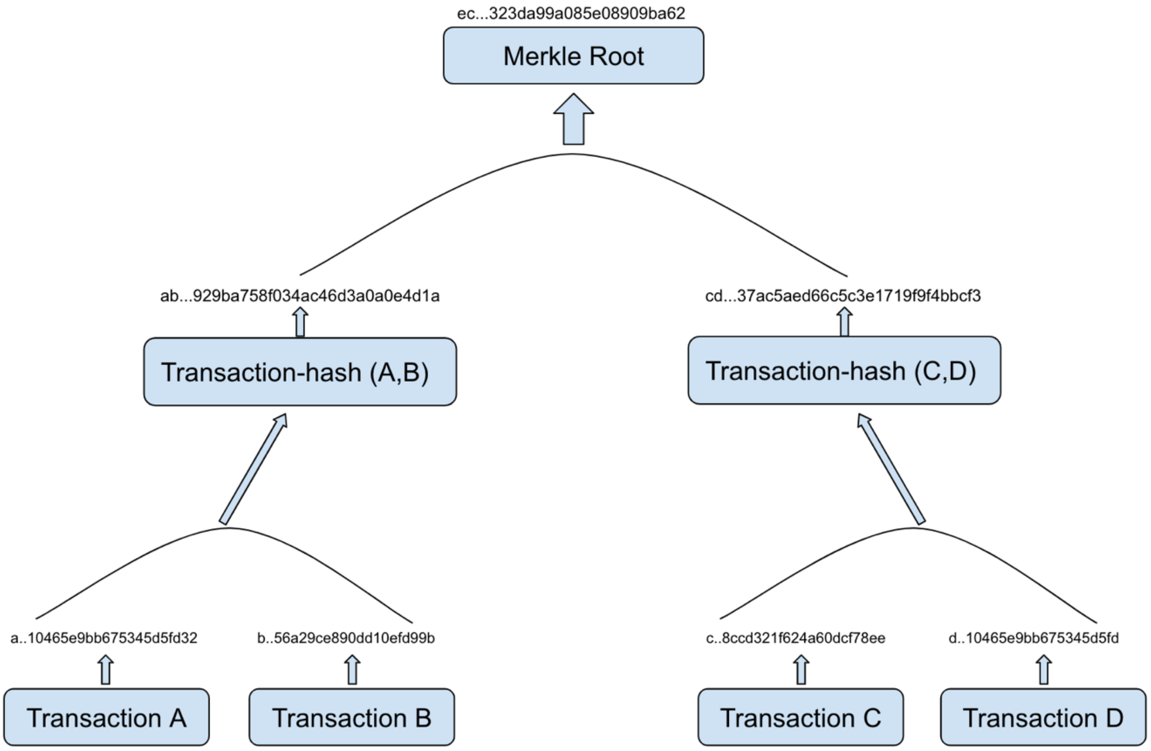


Figure 13. Merkle tree visualization

4.3 Blockchains without Blocks

Directed Acyclic Graph (DAG) is a data structure where information flows solely into one direction. Within a DAG network, there are no miners and no blocks. Users on the network confirm transactions by confirming previous transactions with each new transaction, or resolve conformations differently depending on the digital asset, however, they all share that the data is stored in an individual transaction and not in blocks. This mechanism is very promising since the more new transactions users make, the more available conformations transactions can be confirmed. Thereby positively effecting scaling if more users join the network. [28]

[28] Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018, December). A comparative analysis of DAG-based blockchain architectures. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 27-34). IEEE.

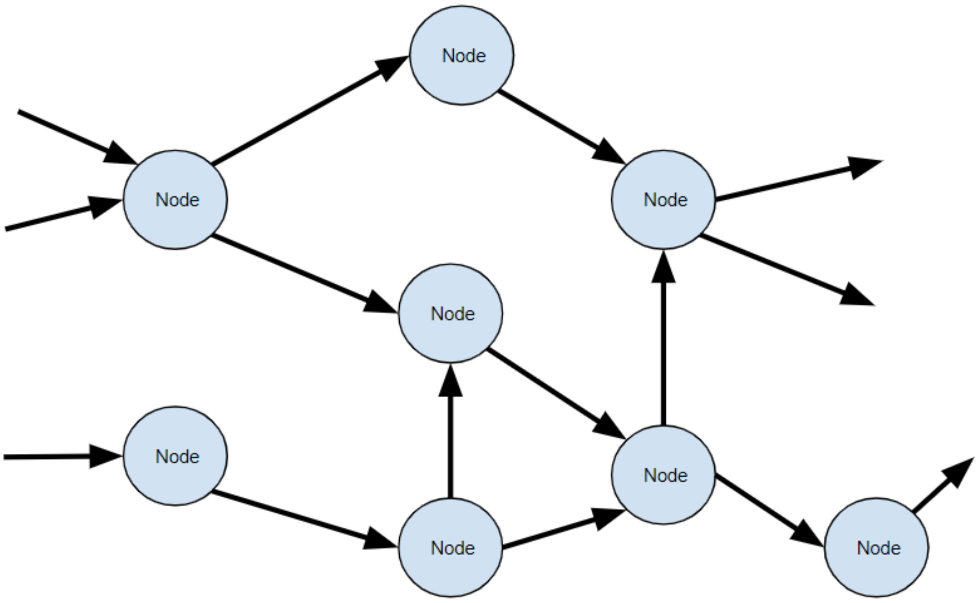


Figure 14. DAG Visualization

Each individual node represents a transaction. By comparing blockchain to DAG, the blockchain can be described as a linked list and the DAG as a tree branching out from one transaction to another and so forth.

4.3.1 Conclusion Directed Acyclic Graph

Several Distributed ledger technologies are adopting the DAG architecture structure. Furthermore, while some blockchains struggle to overcome the scalability issue, others have decided to get rid of the whole blockchain notion with blocks and implement a new data structure that potentially offers greater scalability and speed. However, these DLT solutions are relatively new and require proving their technology at scale. Therefore, the maturity of the DAG data structure will provide more certainty of its benefits and drawbacks over time.

5 Consensus Models

5.1 Proof-of-Work

Proof-of-work (PoW) is a consensus model/mechanism proposed by Satoshi Nakamoto in the Bitcoin white paper. Satoshi decided to implement the use of Hashcash, which is the proof-of-work system used to limit email spam and denial-of-service attacks as part of the mining algorithm. Hashcash was first proposed by Adam Back back in 1997.[29] The PoW mechanism is designed to slow down the creation of new blocks added to the network by Miners, which are computer hardware to calculate a cryptographic solution. Once a miner finds the solution, the block is appended to the chain, the miner receives the Bitcoin rewards in addition to all transaction fees in that block. Here we will provide a high-level overview of the mining process and the PoW consensus algorithm.

5.1.1 Mining and Validation of Transactions

Mining is a competitive process and activity for high-powered computers that solve math problems, also called "proof-of-work." Miners get paid for their work through the validation of transactions. By verifying transactions, mining processes, and activities performed by these high powered computers help to prevent "double-spending." [30]

The miner intends to calculate a specific SHA-256 hash that has to be below or equal to the current target. The target is set by the network for the miner to add the next block to the chain. All data required by the computer to calculate this block header hash(BH-hash) are inside the block header. The version and hashPrevBlock can't be manipulated for calculating a new hash. These two values are inalterable. The timestamp, on the other hand, changes every second, which is crucial for calculating hashes of the block header. Mining requires computers to guess the nonce a 32-bit integer randomly. Therefore the nonce can be any value between 0 and 4,3 billion.

Since there is a possibility that none of these nonces will produce a valid BH-hash that is lower or equal to the set target, additional mechanisms must be present to prevent this. The hashMerkleRoot (hash-MR) is decisive in this process due to large mining pools having the ability to calculate trillions of BH-hashes per second, which would render the nonce useless. In this scenario, the mining pool would compute all possible nonces without coming up with a valid BH-hash; Instead of just waiting until another second has passed, an option is to replace some transactions inside the block, which will, therefore, alter the hash-MR.

[29] Back, A. (2002). Hashcash-a denial of service counter-measure.
[30] Fortney, L. (2019). Bitcoin Mining, Explained. Retrieved from https://www.investopedia.com/terms/b/bitcoin-mining.asp

Thus, the mining pool can iterate through all possible nonces repeatedly without having to waste any resources or time.

The target/nBit is a 32-byte integer. Bitcoin uses SHA-256 as the hashing function for comparing this hash with the target. But the storage space for this target number is 4 bytes. For this, to manifest, we write out this number in a "compact" format. [31]

Example with Bitcoin and use of target:
let's take block Number 613985 of Bitcoin. Here the Bits is 387,124,344 for this to be represented into a 256-bit hash we need to do some refactoring.
First, we write the number into the hexadecimal form, which corresponds to 17130c78.
The bits can be represented as either the number or the hexadecimal version depending on the block explorer and which option seems more user-friendly. To write this number into a hexadecimal 256-bit hash, we need the hexadecimal 256-bit representation of this number.

We divide the 4-byte string 17130c78 into 1 byte each, like this: 17 13 0c 78.

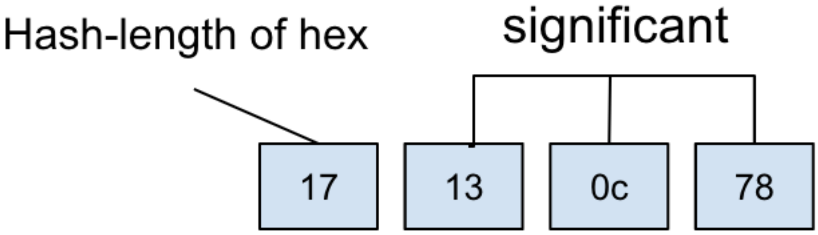


Figure 15. Divided 4-byte string into 1 byte each

Now the first byte (17) indicates the number of bytes set aside for the significant portion and preceding bytes, and this will be the length in hexadecimal form: $1 \times 16^1 + 7 \times 16^0 = 23$
This number indicates how much space is provided for the representation – significant (Mantissa). 13 0c 78 is the "significant" portion.

[31] Bitcoin. (2020). Target nBits. Retrieved from https://bitcoin.org/en/developer-reference#target-nbits

So, the 23-byte portion of the string is made up like this:

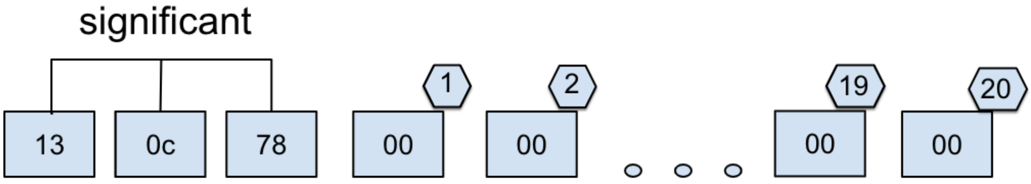


Figure 16. 23-byte portion

For this representation to be able to be comparable to an SHA-256 hash, we need to add the rest of 00-byte pairs in front of this hexadecimal representation of the target, in order to compare the SHA-256 block header hash to this derived target.

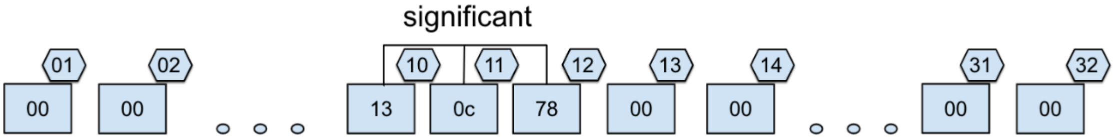


Figure 17. Target comparable to a block header hash

This target representation is now complete and can be compared to the block header hash. If the block header hash is either lower or equal to the target threshold, the miner is allowed to add a new block to the blockchain after all the nodes have verified that no malicious actions were undertaken.

To keep the network in balance, every 2016 block, the difficulty is evaluated. The proof-of-work mechanism is designed so that in an interval of 10 minutes, multiplied with 2016 blocks should equate to two weeks.
If the creation of these 2016 blocks takes

- More than two weeks, the difficulty of mining blocks is too hard and is adjusted to an easier target. Lower difficulty means a smaller target number. Therefore, fewer possible guesses can be performed.
- Less than two weeks, the difficulty for mining blocks is too easy and is adjusted higher. Greater difficulty means a higher target number, which equates to more possible guesses that can be correct.

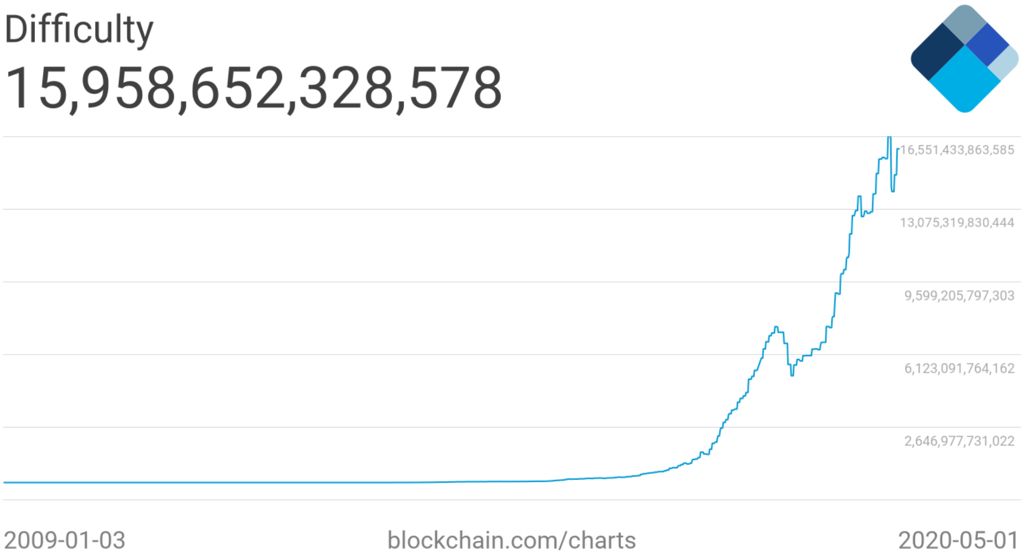


Figure 18. Mining Difficulty - A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners. [32]

To summarize, the proof-of-work algorithm is designed to slow down the creation of new blocks to about 10 minutes per block. In addition, miners around the world to try to guess a specific number below or equal to a target threshold.

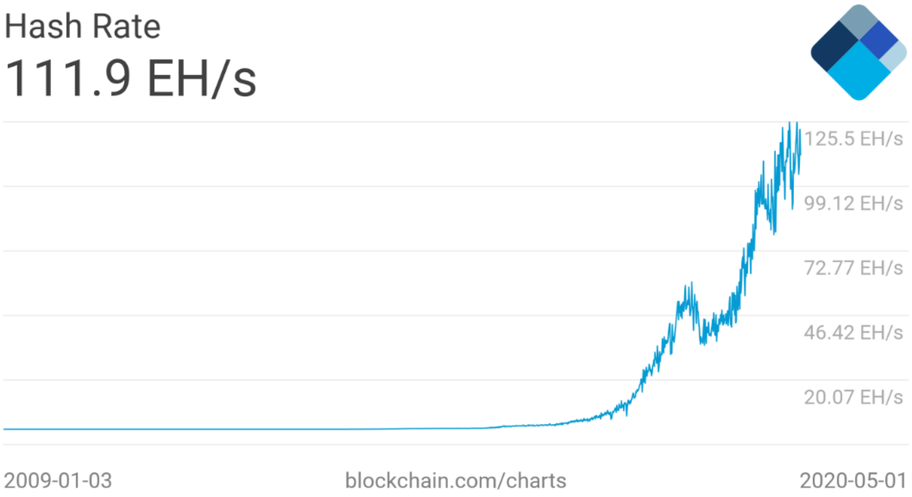


Figure 19. Hash Rate- The estimated number of exa hashes per second (quintillions of hashes per second) the Bitcoin network is performing. [33]

[32] Blockchain (Producer). (2020). Network Difficulty. Retrieved from https://www.blockchain.com/charts/difficulty?timespan=all

[33] Blockchain (Producer). (2020). Hash Rate. Retrieved from https://www.blockchain.com/charts/hash-rate?timespan=all

5.1.2 Mining Hardware

Over the years, miners have used various types of to mine Bitcoin. Here we will look at the mining history of Bitcoin and look at the different hardware used.

5.1.2.1 Central Processing Unit (CPU)

In the early days of Bitcoin, the majority of miners used their laptops to mine Bitcoin without any issues. They use their personal CPU and calculate hashes in hopes of the next block reward. The introduction of GPU mining consequently made it financially unwise to continue mining Bitcoin with CPU, thus highly favoring the use of GPU mining.

5.1.2.2 Graphics Processing Unit (GPU)

The introduction of GPU mining raised the hash rate of the network to such a degree that the number of Bitcoin produced by CPU mining became lower than the operational cost. Therefore, rendering CPU mining obsolete. Since there is a monetary gain in mining, it didn't take long to have technological advances in mining.

5.1.2.3 Field-programmable Gate Array (FPGA)

FPGA's contain logical and programmable units called "logic blocks" and a hierarchy of reconfigurable interconnects which allow blocks to be "wired together." This can be compared to many logic gates that are inter-wired in different configurations. These logic blocks can be configured in a way to perform complicated combinational functions or straightforward logic gates like AND and XOR. In most FPGAs, the memory elements are included inside the logic blocks, which can be plain flip-flops or more complete blocks of memory.[34]

5.1.2.4 Application-specific Integrated Circuit (ASIC)

ASIC's is a microchip designed and manufactured to fulfill a specific purpose rather than employed for general purposes. Today ACIS's are at the forefront of mining and have a substantial advantage when it comes to calculating hashes. They are also way more energy-efficient than previously used solutions. [35]

[34] FPGA. (2015). In *BitcoinWiki*. Retrieved from https://en.bitcoin.it/wiki/FPGA

[35] Smith, M. J. S. (1997). *Application-specific integrated circuits* (Vol. 7, pp. 1-1). Reading, MA: Addison-Wesley.

5.1.2.5 Conclusion Mining Hardware

Mining undergoes continuous innovation with the aim to strive for the cheapest solution required to process hash calculations. The downside is that the average person can't afford the ASIC mining rigs, as it is vastly more expensive and only designed for a single purpose. Thus, an increase in mining centralization can be expected, and if there isn't a viable and affordable solution on the market for the average person, we can only assume that this trend will continue.

5.1.3 Mining Pools

Mining pools are the pooling of resources by miners.[36] They are designed to share their resources over the network in order for the next block to be mined faster. If the resources are large enough, the chance of extracting a future block increase. Through "pooling," rewards are split according to the ratio of mining power contributed.

The birth of mining pools transpired when the algorithm became too difficult for individuals miners to keep up with, due to the increased demand of the network. It could take several months or years for an individual to resolve a mathematical problem related to mining blocks. Therefore, sharing computing power through the system will more quickly generate blocks and receive a portion of the block reward. [36]

When joining a mining pool, it is essential to find the "right" one.
On the internet, there are many different mining pools, and most pools are located in countries where the supply of cheap energy costs is the highest. Each miner aims to gain a maximum of profit for each block that is mined.
In order to find and select the "right" pool, we must consider the stability of the pool, the percentage fee that the mining pool takes, how often a block is mined, and the reward method used by the pool. [37]

[36] Eyal, I., & Sirer, E. G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436-454). Springer, Berlin, Heidelberg.
[37] Karamat, S. (2018). What is a mining pool? Retrieved from https://coinrivet.com/guides/what-is-cryptocurrency-mining/what-is-a-mining-pool/

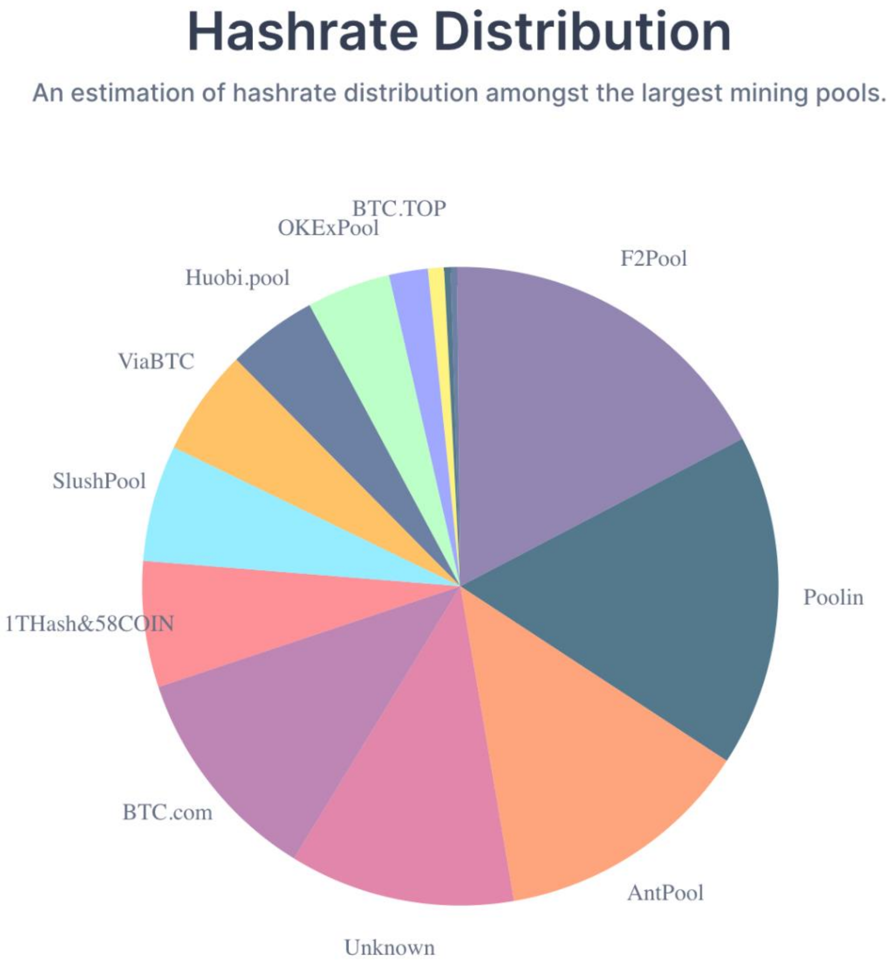


Figure 20. Hashrate Distribution [38]

5.1.4 51% Attack or Majority of the Hash Rate

"*The intention is to make 51% attacks extremely expensive so that even a majority of validators working together cannot roll back finalized block without undertaking an extremely large economic loss – a loss so large that a successful attack would likely on net increase the price of the underlying cryptocurrency*" [39] – Vitalik Buterin

Here we will provide an overview of the 51% attack and explain what I could do and what I couldn't do if I managed to obtain the majority of the hashing power:

[38] Blockchain (Producer). (01/05/2020). Hashrate Distribution. Retrieved from https://www.blockchain.com/pools?timespan=24hours
[39] Buterin, V. (2017). Minimal Slashing Conditions. Retrieved from https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c

The 51% attack is a very misunderstood and easily confused subject. We will clear up some misunderstandings and elaborate on what 51% actually means and what it can do. When referring to a 51% attack, the focus is around owning more than 50% of the hash rate of the proof-of-work digital asset. This will give the attacker added influence over the network since they own more than half of the hashing power needed to validate new blocks.

In any proof-of-work digital asset, there is a primary rule regarding conflicts of truth, when Bitcoin is presented with two conflicting versions of newly mined blocks. In that case, the network will choose the longest chain; this means the network which has more hashing power over time. If probabilistically, one has more hashing power over time, these miners will confirm more blocks than other pools or miners that have less hashing power. Less hashing power means that one can't calculate as many hashes required to guess the right hash. In order to keep the network safe and decentralized, this rule is a fundamental aspect of a proof-of-work blockchain.[40]

Still, the rule regarding the selection of the most extended chain can be exploited by groups that own a majority (51%) of hashing power. What this means is that if I managed to achieve a 51% hash rate ownership, I would be able to mine blocks faster than the rest of the network.

In the event of a 51% attack, the whole network would theoretically become useless, and the aspects that make Bitcoin or other proof-of-work digital assets unique will be rendered false. This could result in a rapid price and trust decline in the network.

In a sense, a 51% or majority attack is suicide. If someone already has a lot of ownership and is invested in the network, doing anything malicious such as trying to censor and double-spend would kill profitability. Thus, people won't trust the system anymore and will capitulate. It would require billions of dollars to try to gain a 51% majority in the Bitcoin blockchain network. Doing anything remotely malicious will thus only end up hurting oneself economically. [40]

5.1.5 What I Can Do With a 51% Attack

Once I have obtained the majority of hashing power, I can now start mining for myself. This means I will mine blocks for myself without announcing them to the network of nodes. Meanwhile, I spend my digital assets in the public network, such as buying a house or car, and so forth. Keep in mind that I am mining for myself without announcing my version of the blockchain, but the network keeps on validation blocks and adding new blocks. However, I am mining my own version of the blockchain privately and not including those transactions I made on the public chain.

[40] Weaknesses. (2018). *Attacker has a lot of computing power*. ln *BitcoinWiki*. Retrieved from https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

After some time, based on my more substantial hashing power, I will have mined more blocks than the public blockchain. After I have waited long enough, I can decide to announce my version of the blockchain to the network of nodes. Thanks to the fact that proof-of-work systems resolve conflicts of interest by choosing the longest chain, my version will be accepted as the real version since it has the longest chain. My version will become the actual state of the blockchain. Consequently, all those digital assets that I acquired goods for won't be included in the transaction history of the blockchain. I get to keep all the items that I purchased and still have all my digital assets in my wallet, which were initially used to buy these items. Thus, I can double-spend my digital asset.

An intriguing part of a blockchain is that it is supposed to be censorship-resistant. Nevertheless, once I have acquired the majority of hashing power, I am now able to block certain transactions I don't agree with and block specific addresses on the network. Hence, I could censor particular organizations or people.

By possessing 51% of the network, I can start putting other miners out of business as I have most of the hashing power and can mine blocks faster. I will be able to collect all future block rewards and transaction fees. As a result, I would increase my monopoly on the network and more quickly gain additional percentages. All other miners would stop being profitable as they must spend money on hardware and electricity without collecting the block rewards. By continuing their operation, they will head into a monetary loss.

5.1.6 What I Cannot Do With a 51% Attack

A 51% majority sounds very scary, but in practice, it does not have as much power or control over the network or other people's Bitcoin as one might predict. I will not be able to reverse other people's transactions. Furthermore, I will not be able to prevent transactions from being sent, but I will be able to let those transactions stay unconfirmed by the miners. I will not be able to change consensus rules by having the majority of hashing power. Thereby being rendered unfeasible to create any additional coins out of thin air, neither will I have the ability to change the mining reward for each block.

5.1.7 Conclusion 51% Attack

Even though this flaw could theoretically happen, it is very improbable that it will occur. The main reason being that there is no monetary incentive to try to gain the upper hand with a 51% attack on the network. The only motive we could consider would be to destroy the system and make Bitcoin or other proof-of-work blockchains less trustworthy. However, since there is a monopoly in mining pools concentrated in China, the possibility exists that the Chinese government might disapprove of Bitcoin and decides to take control of the Chinese mining pools. This would result in China controlling over 51% of Bitcoin mining and a situation that could potentially destroy the network.

5.2 Proof-of-Stake

Proof-of-stake is a consensus model that was introduced back in 2011. This model aims to create a consensus of the blockchain identical as described for “proof-of-work.” The only difference is its procedures. In proof-of-stake, the term “mining” is not used in the same way as in proof-of-work. Users that validate blocks are referred to as “forgers.” [41]

Users who want to join the forging process must insert a designated amount of coins (stake) into the network. The amount will determine whether your chance is large or small to become the node in the network, thereby validating the next block. A more substantial number of coins inserted in the network equates to a significant increase in a given a chance to validate. [41]

A relatively easy implementation of the PoS algorithm requires the miner mining the next block to sign it with their private key to the address holding their coins, where the block is valid if the hashing algorithm sha256 is equal to the equation [45]:

$$\text{sha256}(PreviousHash + Address + Timestamp) \leq 2^{256} * \frac{Balance}{Difficulty}$$

Where PreviousHash is the hash of the previous block in the chain, Address is the signer’s address with the balance, and Timestamp is the current Unix time in seconds after 1. January 1970 and Difficulty is an adjustable parameter to regulate the frequency of successful signatures. Examining this algorithm, it has the necessarily required properties so that every miner has some random chance per second of successfully mining the next block. The only variable that would increase the miner success rate of discovering the next block would be the balance. Therefore, if one has twice the balance amount looked up for this operation, the chance of mining the next block is double as high. [45]

In order to prevent the wealthiest nodes in the network always acquiring the opportunity to be selected for rewards, PoS has created mechanisms to counter this dilemma. The two most well-known methods are Randomized block selection and coinage selection.

[41] Proof of Stake Explained. (n.d). Retrieved from Binance Academy: https://www.binance.vision/blockchain/proof-of-stake-explained

5.2.1 Randomized Block Selection

In randomized block selection, the proof-of-stake validators is selected by looking for a combination of the lowest hash value and the largest “stake” invested. Since the size of the stake is public to everyone, the next forger may usually be predicted by other nodes on the network. [42]

5.2.2 Coin Age Selection

In order to forge the next block, this method selects the next node based on the “coinage” of the stake, to forge the next block. The way this is calculated is:

$$Number\ of\ days\ staked * Number\ of\ coins\ staked$$

Once a node has forged a new block, the coinage is reset to zero. Upon reset, you must wait a certain amount of time before forging a new block. The coins must be held for at least 30 days before they can compete for a new block. The user is assigned to forge the next block within 90 days. This structure prevents the most significant and oldest stakes from dominating the network. This mechanism promotes a robust and decentralized forging network. [42]

5.2.3 Advantages and Weaknesses of Proof-of-Stake

The implementation of “proof-of-stake” (PoS) is still new and will, therefore, have both positive and negative aspects. First of all, the PoS method is much more energy-saving than proof-of-work (PoW). PoS will also be more decentralized because rewards are linear with respect to the amount of stake. Therefore, creating no extra edge to join a pool (more decentralized).
By owning 51% of the entire stake, PoS security will increase as you will dominate the network. Still, attaining 51% ownership will be very expensive and thus not profitable.

Proof-of-stake has eliminated problems associated with energy-intensive mining. Still, two theoretical concerns were quickly discovered. The problem with “nothing at stake” and “long-range attack.” [43]

[42] Ray, S. (2017). What is Proof of Stake. Retrieved from https://hackernoon.com/what-is-proof-of-stake-8e0433018256

[43] Martinez, J. (2018). Understanding Proof of Stake: The Nothing at Stake Theory. Retrieved from https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

5.2.3.1 Nothing at Stake

In the event of a fork, the optimal strategy for any miner is to mine on every chain, so that the miner receives their reward no matter which fork remains successful. [44] An attacker may be able to send a transaction in exchange for another cryptocurrency. When the attacker gets the currency, the attacker can start a fork of the blockchain from one block behind the transaction and send the money to themselves instead. This will cause the attacker's fork to win because everyone else is mining on both. [45]

5.2.3.2 Long-range Attack

Another dilemma that is burdensome is the issue of so-called "long-range attacks." This malicious attack attempts a miner to start a fork far behind the main chain. The aim is for the attack to find an account that has no stake at the current block but has a larger stake in a previously mined block. Therefore, the attacker can now create forks from the past blocks that can overtake the current main-chain with a (previous) majority stake. This can be achieved form compromising the private keys of older accounts, which no longer have any stake for the moment but had a significant stake in the network at previous stages inside the chain history. This issue can generally be solved with timestamping, but exceptional corner cases do tend to appear in cover complicated designs. [45] [46]

[44] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297-315). Springer, Cham.

[45] Ray, J. (2018). Problems. *Proof of Stake.* Retrieved from https://github.com/ethereum/wiki/wiki/Problems

[46] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297-315). Springer, Cham.

5.3 XRP Ledger Consensus Protocol

The XRP ledger consensus protocol is quite different from the PoW and PoS approach. In this protocol, there isn't any mining involved or the staking of digital assets. Here we provide a high-level overview of this consensus protocol. In both Ethereum and Bitcoin, we often mention and talk about blocks. Regarding XRP, we refer to each element added to the chain as a ledger. Each time a new ledger gets added to the chain, it receives two unique identifiers. One identifier is the ledger index, which becomes incremented by one digit each time a ledger is attached. The other identifier is the ledger hash, which is referred to as a unique hash or fingerprint with respect to the ledger's content. [47]
A unique feature of XRP is that every time a transaction is sent through the network, a portion of XRP is burned. This is referred to as a transaction cost. This process is implemented in order to protect the XRP ledger from spam and denial-of-service attacks.

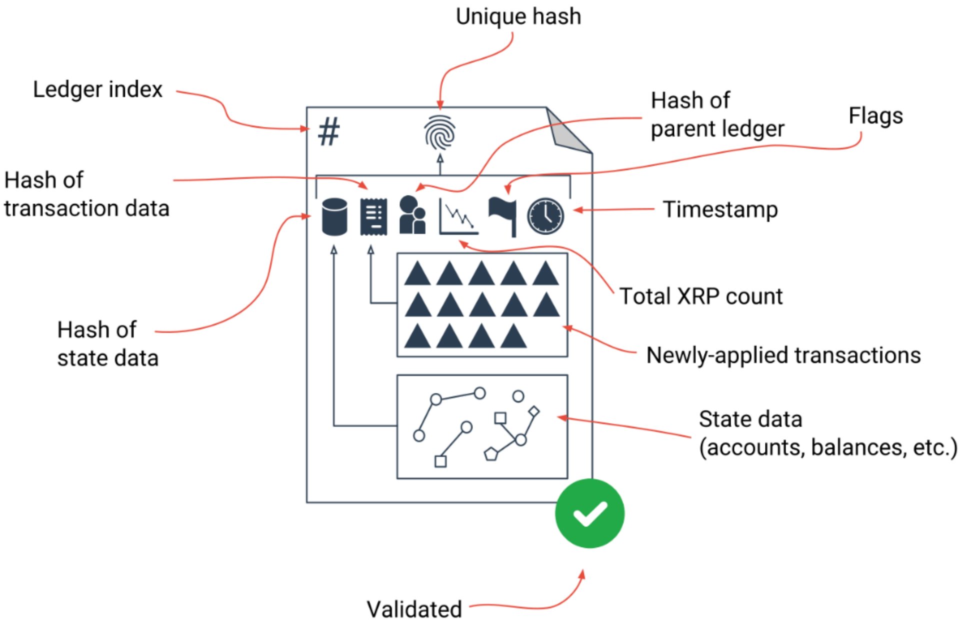


Figure 21. XRP Ledger Elements [48]

This consensus protocol is highly energy-efficient and scalable, reaching up to 1'500 Transactions Per Second (TPS) on-chain and can scale up to 65'000 TPS off-chain, according to Ripple and settles a ledger on average every 3 seconds. [49]

[47] Cohen, D., Schwartz, D., & Britto, A. (n.d). Consensus. Retrieved from https://xrpl.org/consensus.html
[48] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/anatomy-of-a-ledger-complete.png
[49] Ripple. (2020). XRP. Retrieved from https://ripple.com/xrp

The XRP ledger consists of many independent ledger servers (usually running rippled) that accept and process transactions. Servers can be divided into two types of primary servers, Validators and Tracking servers. The primary function of the tracking servers includes the distribution of client transactions and answering queries about the ledger.

"Strictly speaking, validators are a subset of tracking servers. They provide the same features and additionally send "validation" messages. Tracking servers may be further categorized by whether they keep full vs. partial ledger history."[47]

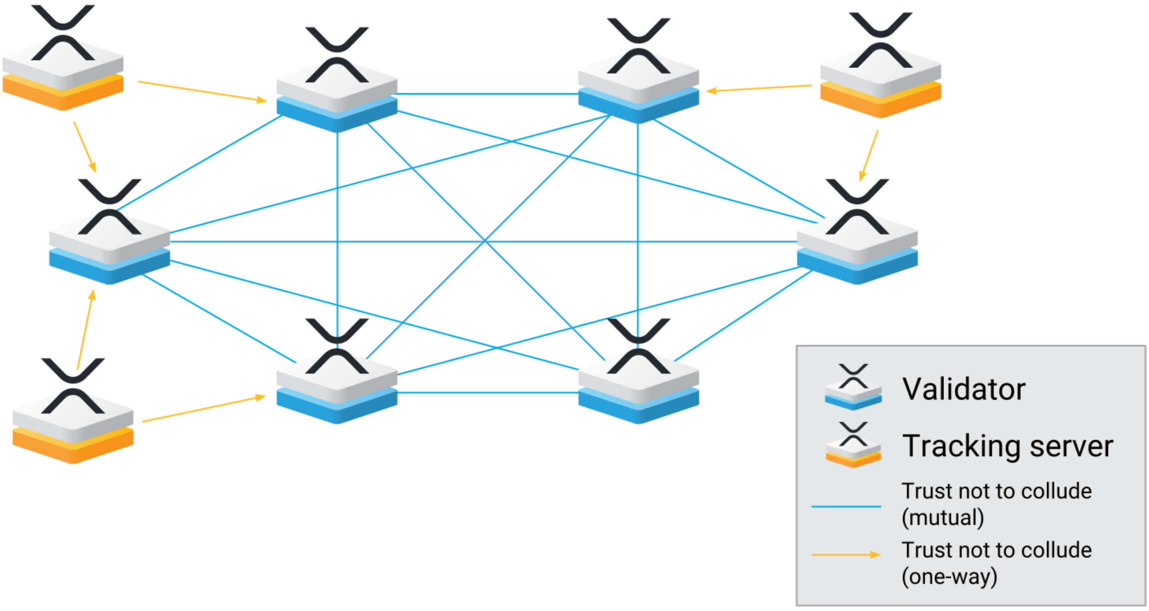


Figure 22. Participants in the XRP Ledger Protocol [50]

These servers share within the network all candidate transaction information. Based on an established common consensus, validators agree on a specific amount of required transactions that must be included in the next ledger version. The agreement is an iterative process where servers deliver proposals or sets of candidate transactions. Servers communicate and update recommendations until a supermajority of chosen validators agrees on the same set of candidate transactions.

"Transactions fail to pass a round of consensus when the percentage of peers recognizing the transaction falls below a threshold. Each round is an iterative process. At the start of the first round, at least 50% of peers must agree. The final threshold for a consensus round is 80% agreement. These specific values are subject to change.". [47]

[50] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/xrp-ledger-network.png

During consensus, each server evaluates proposals form a specific set of servers. These are known as the server's trusted validators or Unique Node List (UNL).

"Each server defines its own trusted validators, but the consistency of the network depends on different servers choosing lists that have a high degree of overlap. For this reason, Ripple publishes a list of recommended validators.". [47]

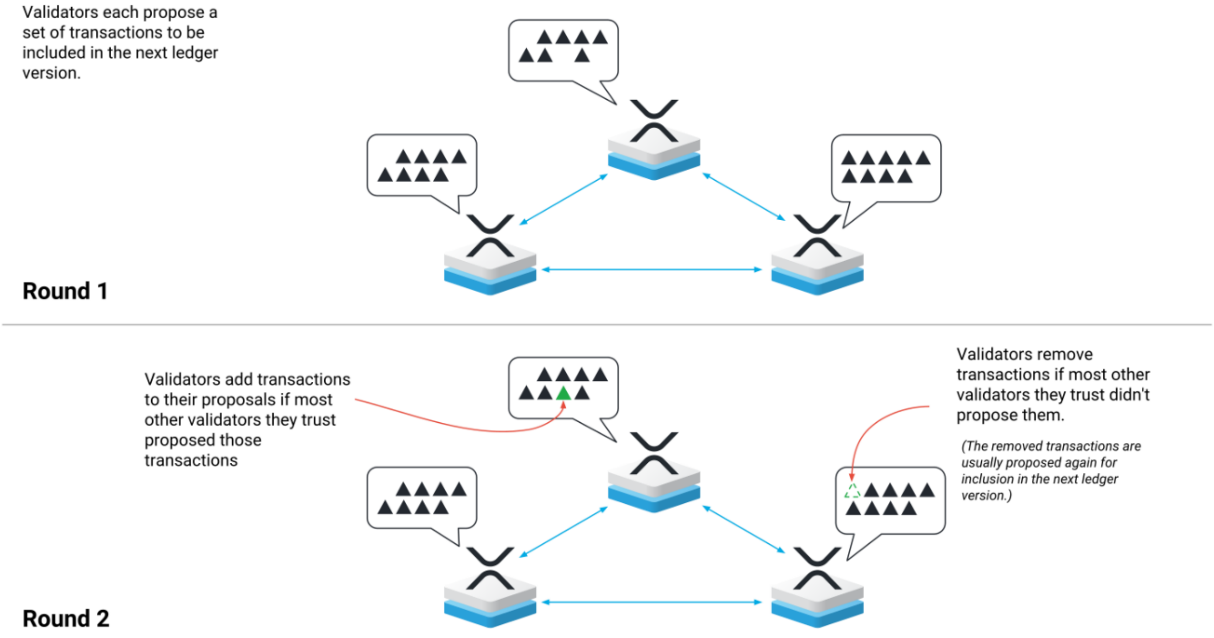

Validators each propose a set of transactions to be included in the next ledger version.
Round 1
Validators add transactions to their proposals if most other validators they trust proposed those transactions
Validators remove transactions if most other validators they trust didn't propose them.
(The removed transactions are usually proposed again for inclusion in the next ledger version.)
Round 2

Figure 23. Validators Propose and Revise Transaction Sets [51]

5.3.1 Consensus Rounds

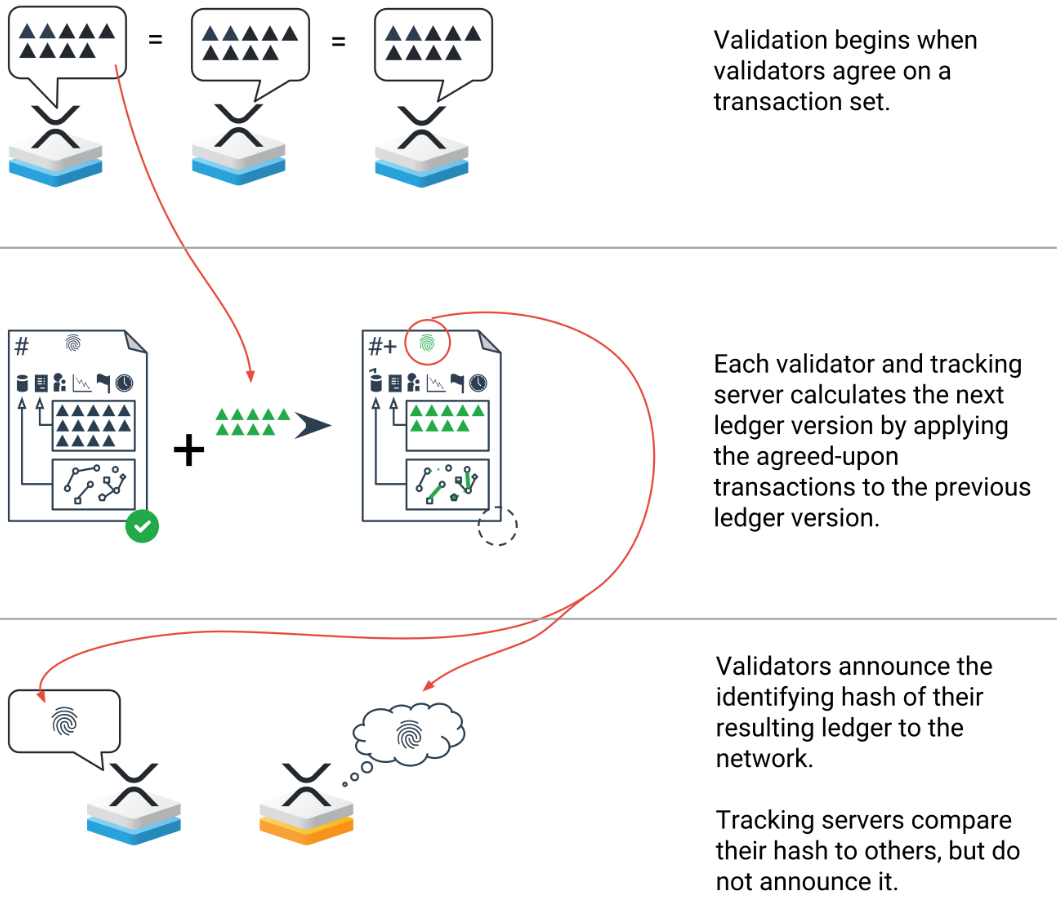
A consensus round is an attempt to agree on a group of transactions so that these transactions can be processed. Trusted validators serve as a subset of the network, which, when taken collectively, are "trusted" not to conspire to defraud the proposed server evaluation. This interpretation of "trust" does not require each individual chosen validator to be trusted. Instead, validators are determined based on the expectation that they will not cooperate in a coordinated effort to falsify data forwarded to the network. Contender transactions that aren't embodied in the mutually agreed proposal remain candidate transactions. These may be reconsidered in the next ledger version.

[51] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-rounds.png

5.3.2 Validation

The validation process is the second stage of the overall consensus procedure, and it verifies that all servers were provided with identical results upon declaring a ledger as the finalized version. Under rare conditions, the first consensus stage can fail; Based on the validation process, confirmation of failure can be forwarded and recognized by servers in the network which act appropriately. Validation can be divided into roughly two components:

- A calculation step, where the resulting ledger version is calculated from a mutually agreed portion of the transaction set.
- A comparison step, where findings are compared in order to assert a ledger version based on enough trusted validators reaching an agreement.



Validation begins when validators agree on a transaction set.

Each validator and tracking server calculates the next ledger version by applying the agreed-upon transactions to the previous ledger version.

Validators announce the identifying hash of their resulting ledger to the network.

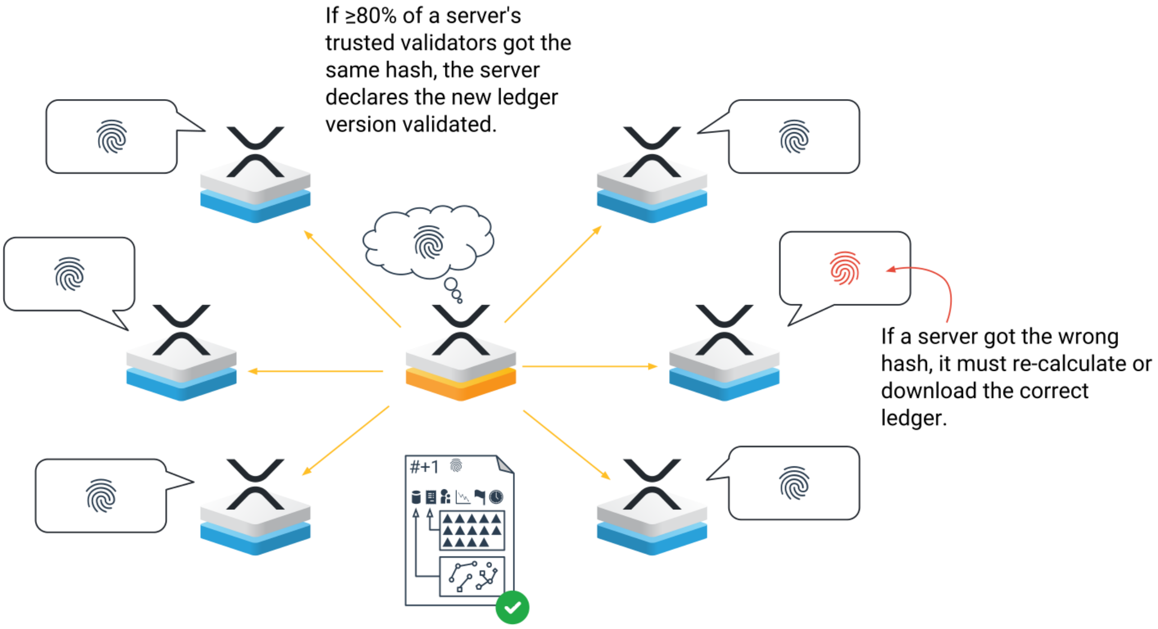
Tracking servers compare their hash to others, but do not announce it.

Figure 24. An XRP Ledger Server Calculates a Ledger Validation [52]

[52] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-calculate-validation.png

5.3.3 Compare Results

Validators each relay their findings in the form of a signed message containing the hash of the computed ledger version. These messages, termed validations, allow each server to compare the ledger it computed with those of its peers.



If ≥80% of a server's trusted validators got the same hash, the server declares the new ledger version validated.
If a server got the wrong hash, it must re-calculate or download the correct ledger.
#+1

Figure 25. Ledger is Validated When Supermajority of Peers Calculate the Same Result [53]

Servers in the network perceive a ledger instance as validated and final when a supermajority (80%) of the peers on the network have endorsed and broadcast an identical validation hash to the network. If the network fails to achieve supermajority consensus, this might be due to too large transaction volume or network latency preventing the consensus process from producing dependable proposals. If this is the case, servers repeat the consensus process until a supermajority is achieved.

5.4 Consensus Rule Changes

In order to diminish bugs and ensure optimal software efficiency, it requires software to be updated and modified on an ongoing basis. Digital assets aren't any different, and these upgrades are called either soft forks and hard forks. Since digital assets are decentralized distributed networks, where all nodes must cooperate to achieve consensus, applicable rules are enforced referred to as a protocol. The majority of these forks are implemented in order to make changes or adaptions to these protocols.

[53] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-declare-validation.png

5.4.1 Soft Fork

A soft fork is a modification to an existing protocol that is backward compatible, which means that all the older version nodes are still able to accept and validate new blocks and process transactions as long as the old protocol doesn't violate the updated rules. [54]

For example, if a soft fork occurs and the new rule is implemented to decrease the block size from 2 MB to 1 MB. The older nodes will still be able to confirm and validated new blocks as long as their size doesn't exceed 1 MB, although they will reject blocks that are larger than one MB and therefore have an incentive to upgrade to the newer version.
A soft fork example is the proposed upgrade Segregated Witness (SegWit) protocol change.

5.4.2 Hard Fork

A hard fork drastically modifies an existing protocol by altering protocol rules. Consequently, all nodes run the previous protocol version needed to validated transactions and add new blocks to the chain that are disabled. Hard forks can be well planned and approved by the community or instead controversial.[54] Controversial means that there is a disagreement in the community leading to a split in the chain and resulting in two independent blockchains. In contrast, planned hard forks would be discussed within the community, with a majority of nodes being upgraded to a new protocol rendering the old version obsolete.

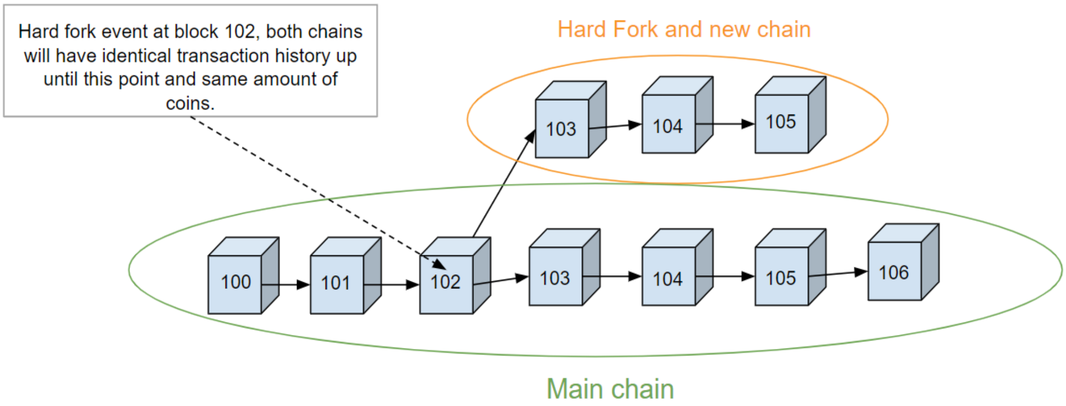

Hard fork event at block 102, both chains will have identical transaction history up until this point and same amount of coins.
Hard Fork and new chain
103
104
105
100
101
102
103
104
105
106
Main chain

Figure 26. Hard fork visualization

A hard fork based upon a common original blockchain will result in both the old and new protocol version having an identical blockchain transaction history up until the blockchain split. Thereafter, these two independent blockchains will each have their own transaction history. An example of this is the hard fork, which leads to the creation of Bitcoin Cash. So, Bitcoin Cash has the same transaction history and amount of coins as Bitcoin when it went through the hard fork.

[54] Hards Forks and Soft Forks. (n.d). Retrieved from Binance Academy: https://www.binance.vision/blockchain/hard-forks-and-soft-forks

5.5 Conclusion Consensus Protocols

Through analyzing the different consensus protocols, we have come to a few conclusions and discovered interesting attributes.

5.5.1 Stakeholders

Any system or, in this case, a consensus algorithm will have stakeholders. These stakeholders will obtain value from a system, as the system will solve their potential problems and continue to function. We will divide these stakeholders into the following two categories.

5.5.1.1 Natural Stakeholder

These are the people who have a core problem in which the system is designed to solve. They are the ones paying the system's fees. Within these digital asset ecosystems, the natural stakeholders are the people who seek means of exchange or a store of value.

5.5.1.2 Forced Stakeholder

These stakeholders are required for a system to function, as they solely provide value because the design of the system design requires them. Forced stakeholders extract value from the system and represent remaining friction inside the system. These forced stakeholders are the miners in the PoW consensus model. The only value miners bring to the system is by allowing the system to function.

5.5.2 Relationship Between These Two Stakeholders

Incentives and interests between the two described stakeholders do not align. A natural stakeholder requires the system to be secure, reliable, and wants to transact as cheaply as possible. In contrast, the forced stakeholder profits from the natural stakeholder and system, as they want fees to be as high as possible to gain maximum profit. So, in PoW, the forced stakeholder prefers the block reward and the transaction fees to be as high as they can while keeping the system as useful as possible for the natural stakeholder. This situation will create a conflict of interest between the two stakeholders.

Proof-of-work consensus algorithm:

- Security is derived from the cost needed to replicate the chain. Honest participants must pay these costs.
- Money exits the system to pay for electricity and to distribute mining profits.
- The value must come from natural stake holders.
- A loss in value can result in a loss of security, as miners are dependent on the system's value. If miners capitulate, the system’s security is reduced.

Proof-of-Stake consensus algorithm:

- Stakers lock up a volatile asset
- If they mess up, forgers risk losing their assets.
- Messing up and justifying the risk of losing assets must be countered by expected significant returns.

5.5.3 Incentives are Expensive

Incentives tax natural stakeholders and add forced stakeholders to the system. In order to keep security high, these incentives force stakeholders to pay more money than attackers are willing to pay. Furthermore, incentives create misalignments between natural and forced stakeholders.

Consensus is all about agreeing on a certain set of transactions, which are added into a block appended to the chain. How the system achieves consensus varies from PoW, PoS, XRPL, and other consensus options.

When removing incentives aimed at attacking the system, one will no longer be able to double spend and choose which transactions are to be included in the next block. When trying to undertake something malicious, the attacker only gets one opportunity, after which he will be excluded from the system. So why bother when there aren't any incentives to attack the system. As a result, stakeholders get what they want:
When removing incentives to attack the system, one cannot double-spend, cannot choose which transactions are included in the next block; you only get one shot, and then you are excluded if you try to do something malicious. So why bother when there aren't any incentives to do so. Therefore, stakeholder receives what they want:

- Minimal risk to the system
- Minimal drama and conflicts
- Minimal cost
- Maximum fairness

Each individual network node relies solely on the system's incentive structure to break ties among equally acceptable ways to achieve forward progress. Stakeholders require only a resolution of the double-spend problem among equally acceptable transactions. These transactions should have minimal cost, drama, and fairness. It does not require millions of dollars in incentives to achieve a double-spend resolution. Objectively identifying good ways to make progress and validate transactions is all that is necessary to achieve consensus.

5.5.4 Good & Bad Actors

We believe that good actors wanting to make the system stronger will accumulate if there are no artificial incentives barriers. Therefore, a miner or validator will only try to make the system more robust, if their interest is to do so and they have no ulterior motive. However, bad actors will naturally leave the system if there aren't any incentives other than to make the system better.

5.5.5 Natural vs. Artificial Incentives

5.5.5.1 Artificial Incentives

Artificial incentives lead towards centralization as people who take advantage of those incentives tend to look similar. These people dilute the power of natural stakeholders as they have to work through forced stakeholders who have different incentives. Furthermore, artificial incentives are a tax on natural stakeholders and represent friction left in the system. In addition, they burden natural stakeholders by bringing these forced stakeholders into the system. The reason being that forced stakeholders want artificial incentives to maximize system friction, thereby boosting revenue.

5.5.5.2 Natural or No Incentives

Natural incentives decentralize the network because the only reason to participate is to make the system more secure, robust, and reliable. There is nothing else to take from the system. These natural incentives do not bring artificial stakeholders to the network. Furthermore, natural incentives do not tax natural stakeholders. A system with natural incentives provides benefits of low fees, as no forced stakeholders are paid for calculating PoW or locking up funds in PoS. Rapid transactions and block confirmations are possible because everyone is aware of who the consensus participants are. Consequently, validators do not need to worry about someone mining for themselves or trying to defraud the system. As there is no reward for mining the next block, this objectively leads to no caring with respect to who might mine the next block in the chain.

5.5.6 Final Thoughts

We believe that natural or no incentives can be viewed as superior models regarding the protocol consensus necessary to scale and achieve maximum fairness between validators and stakeholders. Furthermore, without incentives present the natural stakeholders that use the system are provided with fast, low fees, and reliable payments which do not stay unconfirmed. These benefits will naturally draw in the most extensive user base, as most people using a system do not care or understand the consensus protocol or blockchain politics. They will naturally flock towards the system, which provides them with the best price and fastest transactions.

6 Ethereum

After Satoshi Nakamoto launched Bitcoin in 2008, developers and magazines began to look closer at this technology. In one of the magazines called Bitcoin Magazine, a young man wrote articles about this innovative space. This boy was called Vitalik Buterin. Vitalik is a Russian-Canadian computer scientist. He is known as co-founder of the Ethereum platform. [55]

When Bitcoin was released, Vitalik saw firsthand how the blockchain ecosystem took shape, and he noticed a common problem among blockchain projects. Many developers were forced to create their own blockchain. Vitalik wanted to create a single blockchain enabling anyone to create their own decentralized application. Just like the internet, where anyone can create their own website to be uploaded and available on a common internet. He solved this by creating Ethereum. Vitalik published Ethereum whitepaper the first time in November 2013, and Ethereum was launched on July 30th, 2015. [55]

Ethereum has as cryptocurrency called Ether (ETH), which is currently the second-largest cryptocurrency on the market. ETH is a digital currency with many of the same functionalities as Bitcoin. It allows for worldwide transactions, requiring only a short period of time. ETH is not controlled by any central cooperation or entity; therefore, it is decentralized. It is worth noting that most blockchains start centralized, but as they evolve and grow, they become increasingly decentralized. ETH does not have an overall cap, but the annual issuance capped at 18,000,000 ETH per year. With an annual issuance of 18 million ETH per year, relative inflation decreases every year. [55]

Ethereum´s blockchain differs slightly from other blockchains. ETH is programmable, which means users can create their own decentralized application on Ethereum. These decentralized applications are called Dapps (decentralized applications). [56]
As long as the decentralized application is "uploaded" to Ethereum, it runs precisely as originally programmed.
All over the world, people are working on developing Ethereum. Developers create thousands of applications on Ethereum. These can be applications such as games, platforms for decentralized currency exchange, financial applications, and much more.[56]

[55] Buterin, V. (2013). Ethereum white paper. *GitHub repository*, *1*, 22-23.
[56] What is Ethereum? (2020). Retrieved from Ethereum: https://ethereum.org/what-is-ethereum/

6.1 What is Gas?

As mentioned earlier, Ether (ETH) is the fuel of the network. For every instruction conducted in the form of transaction, or some other action performed on the blockchain. Each of these methods requires a certain amount of gas to be paid for the program to run.
This payment is calculated in gas, and gas is paid in ETH. [57]
We can compare this system to our system by measuring electricity in our houses. We use kilowatts (kW), and Ethereum uses gas.

When a solidity contract compiles, it gets converted into a sequence of operation codes. This sequence is also known as opcodes. All of the opcodes and their description are listed up in Ethereum Yellow Paper. Each transaction requires a different amount of gas to complete. When sending one simple transaction from one to another requires a minimum of 21,000 gas cost.
This type of fee is called the TX fee (Transaction fee). This fee is calculated as follows:

$$gas\ limit * gas\ price$$

Any third party does not collect this fee, and it is the reward for all the miners for the work they contribute to securing the network.

6.1.1 Gas Limit

The gas limit is a maximum limit of how much you want to spend on each transaction. This depends on how much code you want to run on the blockchain. If you set a lower limit for the gas limit than it costs to run the code, the transaction will not be approved, and an error will occur. An error called: "Out of gas" error. [57]
Unused gas is refunded back to the user if the limit is set higher than the transaction cost.

6.1.2 Gas Price

The gas price is the total amount you are willing to pay for every unit of gas. Usually, this is measured in “Gwei.” Gwei stands for gigawei, and it is a unit for ether.

$$1{,}000{,}000{,}000\ Gwei = 1\ ETH$$

[57] Base, K. (2019). What is gas? Retrieved from https://support.mycrypto.com/general-knowledge/ethereum-blockchain/what-is-gas

The higher the gas price, the higher the chances that the transaction will be included in the next block. You can find the current gas price here. The reason that higher gas prices will give you a higher chance to get included in the next block is that miners select transactions with the highest gas price to get the highest reward.[58]

6.2 Smart Contracts

Smart contracts were first introduced in early 1990 by a cryptographer, computer scientist, and lawyer named Nick Szabo. Nick Szabo defines contracts as:

"A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are "smarter" than their paper-based ancestors. ". [59]

Smart contracts are based on if-then conditions and actions. They are turning complete, which means that one can program any logic into these smart contracts.
A smart contract is a computer program (script) that allows you to run sets of codes without the involvement of a third party. This agreement is documented on the Ethereum blockchain, which is self-verifiable in the form of data code. That means that the code is in a public "database" and cannot be changed. A smart contract consists of the value, address, functions, and state.[60]
Smart contracts are executed when a transaction(e.g. ETH transfer) has the same address as the function inside the smart contract. The logic that runs depends on how the logic is implemented when the smart contract was created.

An example of how a smart contract can be used:
If Bob wants to buy Alice´s boat, the agreement between Alice and Bob is stored on Ethereum blockchain using a smart contract. The deal would look like: "When Bob pays Alice 200ETH, then Bob will receive ownership of the boat."

[58] district0x. What is Gas. Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-gas/
[59] Szabo, N. (2018). Smart Contracts: Building Blocks for Digital Markets.
[60] Bahga, A., & Madisetti, V.K. (2016). Blockchain Platform for Industrial Internet of Things

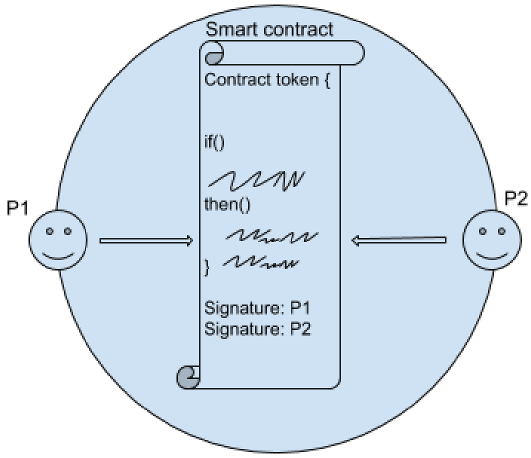


Figure 27. Simple Visualization of Smart Contract

In contrast to a blockchain-based smart contract, agreements are, for the most part, done with the involvement of various 3rd parties, including their applicable fees (e.g. lawyers, house brokers, and the banks). This is just one example of the logic and how smart contracts can be created and used. Smart contracts are self-verifiable, self-executable, and tamper-proof.

6.3 The Life Cycle of Smart Contracts

Smart contracts are developed in the Solidity programming language. Solidity is a high-level programming language for implementing smart contracts, similar to C++ and JavaScript. [61] Everyone can create their own smart contract. A smart contract consists of various "classes" containing fields and methods. If you want to deploy your smart contract to Ethereum's blockchain, you need to compile solidity code to the EVM (Ethereum virtual machine) bytecode. The EVM bytecode is then sent to the Ethereum network in the form of a transaction.

In order to invoke methods in a contract, you have to send a transaction with the smart contract address. Contracts can only run once a transaction has been called. [62]

In smart contracts, there are two types of accounts, externally owned accounts (EOA) which are owned by the users private key, and contract accounts, that are controlled by their contract code. [59] Contracts never run without a call of a transaction, which means it will never "run in the background" or on their own accord. Contracts can be a chain of executions, where one contract calls another contract, and so on. But the first execution will always have to be called by a transaction from an externally owned account.

[61] Solidity. (n.d). *Documentation*. Retrieved from Solidity: https://solidity.readthedocs.io/en/v0.6.2/
[62] Antonopoulos, A. M., & Nugent, T. (2020). Ethereum Book. Retrieved from https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc#what-is-a-smart-contract

A created contract cannot be changed but deleted by executing an EVM opcode called "SELF-DESTRUCT." This opcode costs a certain amount of gas. Every transaction uses this gas as a "payment" mechanism. Gas is a unit of computation and expressed in Ether. The sender of the transaction pays a required gas cost. If a contract provides for an opcode option, the smart contract cannot be deleted (more on opcodes and gas later). [63]
Since blockchains are immutable, you can only remove existing code and states from its address. You can never remove the transaction history of a smart contract. [62]
All transactions are atomic, which means that they execute in their entirety, regardless of how many contracts they call and what they do. [62]

6.4 What is EVM (Ethereum Virtual Machine)

EVM is designed to be the infrastructure for smart contracts based on Ethereum. EVM runs as a sandbox environment and is responsible for executing contract bytecode. The figure below shows how this works.

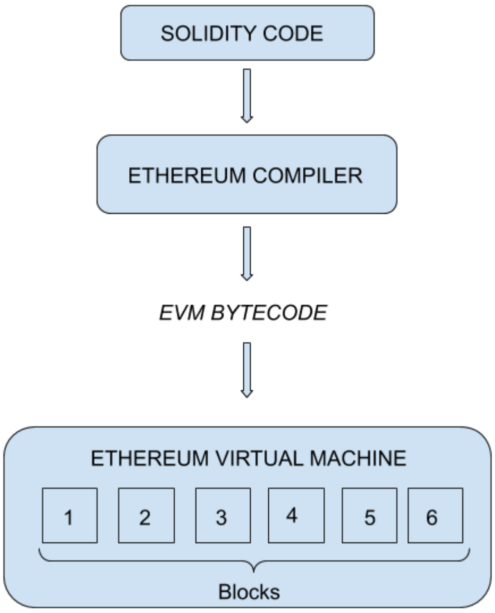


Figure 28. Ethereum Virtual Machine

[63] Sillaber, Christian & Waltl, Bernhard. (2017). Life Cycle of Smart Contracts in Blockchain Ecosystems. Datenschutz und Datensicherheit - DuD. 41. 497-500. 10.1007/s11623-017-0819-7.

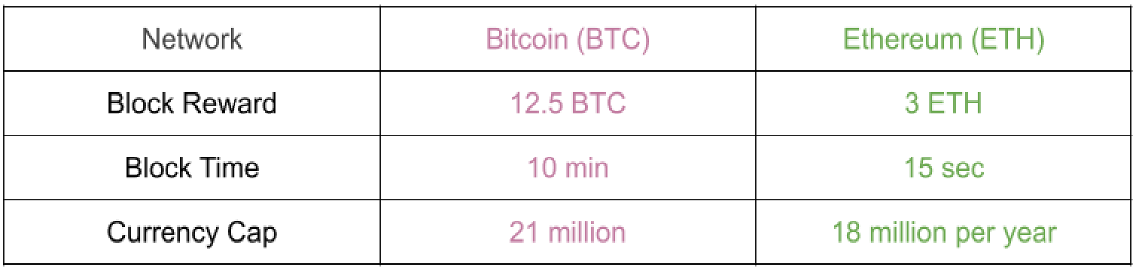
The EVM bytecode is in its entirety isolated from the filesystem, network, or any host computer processes. This architect structure provides excellent security from hackers and attackers who wish to steal some data on the computer that the person is using. All nodes run the EVM, which allows these nodes to agree on how to execute given instructions and execute code in a trustless ecosystem. For every instruction implemented in the EVM, miners must validate and execute every transaction. Therefore, you have to pay (**gas**) for the computation, irrespective if it fails or succeeds. [64]

6.5 Ethereum Mining

Ethereum mining is almost like Bitcoin mining: computers that validate transactions through proof-of-work. Bitcoin miners collect their reward in Bitcoin, Ethereum miners get paid in Ether.

Ether is not only a digital currency like Bitcoin, and ether is more like a digital commodity. To run applications on Ethereum blockchain, you need Ether, just like you need gasoline to fuel your car. Just like we mentioned earlier in this topic, ether powers smart contracts, generating tokens, running Dapps, making payments, etc. That’s why ether is called programmable money. [65]

This table presents block reward, block time, and currency cap in Bitcoin mining and Ethereum mining.



Network	Bitcoin (BTC)	Ethereum (ETH)
Block Reward	12.5 BTC	3 ETH
Block Time	10 min	15 sec
Currency Cap	21 million	18 million per year

Figure 29. Mining table

[64] What is the «Unstoppable World Computer»?. (n.d) Retrieved from Bitrates: https://www.bitrates.com/guides/ethereum/what-is-the-unstoppable-world-computer

[65] district0x. Ethereum vs. Ether. Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-gas/

6.6 Ethereum Tokens

Tokens are a concept within Ethereum that can be a bit complicated. Applications (Dapps) created on the Ethereum blockchain have their cryptocurrency or 'tokens.' For users to use the applications on the blockchain, they have to use the application's token. The analogy can be compared to renting an item. The Ethereum blockchain acts as the landlord and can rent out its security and blockchain features to other people who wish to create their own digital asset without creating a separate blockchain. The issuer of this new token will, therefore, have to pay Ethereum in gas to rent the platform. This token may represent something specific in a given ecosystem. This can be anything of value, such as voting rights, economic value, etc. It is essential to understand that a token is not limited to one particular role. [66]

An example of how a token works:

If you imagine an arcade with many different arcade games, in this game hall, you have to exchange money to get back coins that can be used on the various machines. When these coins inserted into the device, you are allowed to play the game specified on the machine.

The tokens work in precisely the same way. Tokens are the entry value to use the application on the blockchain.

Tokens are often issued through a crowd sale called ICO (initial coin offering).

6.7 ICO (Initial Coin Offering)

ICO is crowdfunding for blockchain projects. In an ICO, cryptocurrencies are sold in the form of "tokens" to early investors and speculators before they are listed on a broader marketplace. When participating ICO, caution is advised because it is a high-risk investment. The most important thing when participating in an ICO is to do essential research about the company and team members, value of the project, use-case, and apparent need for this token to exist and whitepaper.

An ICO has achieved its goal when it soft cap (minimal amount required) is reached. The ICO also has a hard cap (maximum accepted amount).

If the ICO doesn't reach a soft cap, the funds are often returned to the investors. [67]

[66] district0x. The Role of Tokens. Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-gas/

[67] Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business*, *100*, 64-75.

Most tokens out there today came about through an ICO with nothing else than a whitepaper explaining their project and explaining their vision. 2017 was a vast ICO craze where a lot of projects raised enormous amounts of money without any concrete business plan, or they were outright scams. Most ICO's failed hard as they either exited and abandoned investors without notice. This was made possible cause there wasn't any regulation or guidelines for these ICO's anyone could create a webpage copy an existing tokens code or and write lofty promises for substantial monetary gains if they bought their token. Alternatively, they mismanaged their funds by celebrating and wasting unnecessary money. In 2018 there was a considerable decline in the overall crypto market, and most ICO's vanished.
The greatest ICO's was EOS, which raised an astonishing 4 billion dollars, which is an insane amount of money compared to more traditional fund-raising methods. [68]

6.8 ERC-20 Token

This standard is implemented to make it easier for developers to create tokens upon the Ethereum blockchain and creates a standard interface that allows any tokens on Ethereum to be reused by applications like wallets or decentralized exchanges. There are specific rules and methods one most follow for the token to be accepted as an ERC-20 token. [69] These tokens are written in solidity and deployed on Ethereum in the form of a smart contract. The ERC-20 standard provides basic functionality to transfer tokens and allow 3rd parties to spend tokens on behalf of the token holder. [70]

[68] Nonninger, L. (2018). Block.One just raised aq $4 billion ICO Retrieved from https://www.businessinsider.com/blockone-raises-4-billion-ico-2018-6?r=US&IR=T

[69] Vogelsteller, F., & Buterin, V. (2019). EIP20: ERC-20 Token Standars. Retrieved from https://eips.ethereum.org/EIPS/eip-20

[70] district0x. What is an ERC20 Token? Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-an-erc20-token/

7 XRP

XRP is very interesting since it has been around since 1. January 2013 and has continuously been among the top coins for this period. XRP:

- Operates very differently compared to Bitcoin and Ethereum
- Have no mining or blockchain or native assets that are released during a specific time interval.
- Have no blocks but ledgers that work similarly.
- Use different consensus algorithms that consist of validators securing the network.
- Can handle 1'500 TPS on-chain and scale up to 65'000 TPS through payment channels and settles on average between 3-4 seconds. [49]
- Have its coins pre-mined to a total of 100'000'000'000 XPR
- One XRP can be divided into six decimal points, and the smallest donation is called drops (0,000001 Drops)

A polarizing difference between XRP and Bitcoin or Ethereum is that XRP is deflationary while the other two are inflationary. As a deflationary setting burns XRP every time someone sends a transaction, it will prevent spam attacks and protect the network. [71]

We cannot discuss XRP without mentioning Ripple. Ripple is a software development company that was founded after the creation of XRP. The majority of XRP was gifted to Ripple (80 billion XRP).[72] Thus, it is worth noting that the creators of XRP are also involved in the Ripple company. We will discuss Ripple and its mission more in the second document phase.

It is worth knowing the difference between the XRP digital asset and the XRP Ledger.

XRP:

" XRP is a cryptocurrency, a digital asset that lives on a public ledger that can be transferred using digitally signed transactions." [73]

XRP Ledger:

" XRP Ledger is the public ledger that XRP is native on. It supports a decentralized exchange for other assets, fast payments, and so on." [73]

[71] Transaction Cost. (n.d) Retrieved from XRP Ledger: https://xrpl.org/transaction-cost.html

[72] XRP Distribution. (2015). Retrieved from Ripple Labs: https://web.archive.org/web/20150806120942/https:/www.ripplelabs.com/xrp-distribution/

[73] Quora. David Schwartz. Retrieved from. https://www.quora.com/What-is-the-difference-between-XRP-XRP-Ledger-and-Ripple?share=1

7.1 The Burn Rate & Calculations

As mentioned earlier, in order to secure the network, each transaction destroys a small portion of XRP. Some people speculate that the primary purpose behind this mechanism is to impact the price of XRP, rather than securing the network. Let's take a closer look:

The minimum transaction cost for a standard transaction is 0.000010 XRP (10 drops).
Ripple's API requires all XRP amounts to be specified in drops of XRP. [71]

$$1\ XRP = 100000\ drops$$
$$1\ \text{"}drop\text{"}\ of\ XRP = 0.000001\ \mathrm{XRP}$$

It is crucial to have an overview of the potential daily amount of burned XRP. Below you will see how this can be calculated:

$$Maximum\ transactions\ per\ second = 1500$$
$$Minimum\ transaction\ cost = 10\ drops$$
$$1\ day\ (24\ hours) = 86400\ seconds$$

$$1500tps * 10\ drops * 86400sec = 1.296\ billions\ drops\ per\ day$$
$$1.296\ billions\ drops\ per\ day = 1296\ XRP\ burned\ per\ day\ at\ maxium\ capacity$$

To destroy 1% of the total supply XRP (around 1 billion XRP), it would take approximately 2113 years to burn 1% at the current TPS threshold. Based on this calculation, we can conclude that the expected burning rate will not affect the coin price. [71] Still, if XRP scales up, enabling more transactions per second or increases its transaction cost, the overall burn rate will increase and make XRP a more scarce asset.

7.2 Decentralized Exchange

An exciting feature that is built into the XRP Ledger is the Decentralized exchange. Orders in which currencies are traded are called “Offers.” Offers can be transacted with issued currencies through the use of native XRP, or issued currencies with each other. In addition, issued currencies that possess the same currency code but are not necessarily issued by the same issuer.

This feature makes it possible to issue any asset or currency upon the XRP Ledger, which will be backed by XRP. Thus, one can trade assets fast, secure, and cheap by utilizing XRP features. This build-in Decentralized exchange will allow a business to leverage the benefits of XRP and create new business models. Furthermore, this will allow a business to issue different assets on top of the ledger.

7.3 Interledger Protocol

Stefan Thomas and Evan Schwartz created the Interledger protocol. Both at the time, employees at ripple. [74]

To grasp how interoperability between ledgers can process value exchanges efficiently and quickly, it is vital to understand the interledger protocol. To understand the interledger protocol, the best way is to divide this term into **inter** and **ledger**.

Inter refers to an event that occurs in between or among other events. A corresponding term often used is the word "international," which indicates the involvement of more than one country or events that transpire between various countries.

A **ledger** "*is the principal book or computer file for recording and totaling economic transactions.*" [75]

If we combine these words, we know that this is about registered transactions between two systems. Interledger protocol is a system that accepts multiple payment systems to communicate with each other. This protocol is not owned by any third party, blockchain, company, or currency. The goal of this protocol is to be the rail of connecting any value being a commodity like gold or silver or cryptocurrencies quickly.

7.3.1 So, What Can This Protocol be Used For?

A sufficient advantage of the interledger protocol is by applying it to value transfers between incompatible ledgers or networks which wish to communicate with each other. Its aim is to become a standard for any transaction between two unique payment networks or ledgers. It is thereby removing intermediaries and central authorities from the system. The notion of packetizing money and creating a standard gateway in which value can move across ledgers is compelling and exciting. [74]

The technology of the internet allows us to communicate worldwide in only a few seconds. Data packets can be sent through TCP / IP, broadcasting to everyone. As a consequence, this speed and simplicity should also be feasible when sending money or value between two people. Interledger protocol can easily be used to solve this problem. Thus, interledger is an open-source protocol that can send payments across different ledgers. To ensure that nothing is lost during a transaction, protocols include standardized message packets and address formats. [76]

[74] Thomas, S., & Schwartz, E. (2015). A protocol for interledger payments. URL https://interledger. org/interledger. pdf.
[75] Wikipedia. (2020). Ledger. Retrieved from https://en.wikipedia.org/wiki/Ledger
[76] Interledger Architecture. (n.d). Retrieved from Interledger: https://interledger.org/rfcs/0001-interledger-architecture/

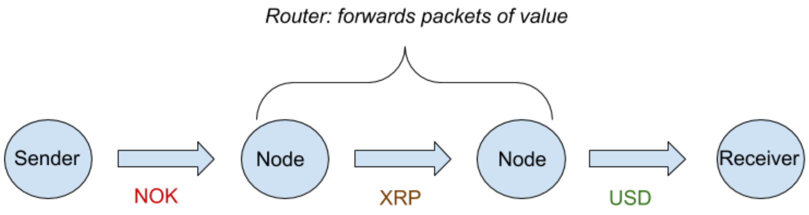


Figure 30. Interlegder transaction

7.3.2 How Does Interledger Work?

The interledger protocol has a set of specific rules, which nodes must comply with when sending value over the interledger network. ILP is a request/response protocol. This protocol has several versions. Currently, the ILPv4 protocol version is used. ILPv4 has three different package types: **prepare**, **fulfill,** and **reject**.

The sender sends a **prepared** packet as a request to the router (node). The router forwards the package to the receiver. The receiver responds to the package either by accepting (**fulfill)** or rejecting (**reject)** the package. The packet with the information given by the receiver returns again via the router to the sender. If a **fulfill** package is returned to the sender, the sender knows that the transaction has been approved by the receiver. The sender can now send the remaining **prepared** packets until the transaction content has been fully received. [77]

[77] Interledger Overview. (n.d). Retrieved from Interledger: https://interledger.org/overview.html

8 Positive and Negative Aspects of Blockchain

By objectively examining blockchains such as Bitcoin, Ethereum, and XRP and describing their strengths and weaknesses is vital to continue the blockchain innovation space. We will, therefore, describe some shortcomings and virtues to these networks without being biased or solely focus on their positive or negative qualities. We present our own opinions and conclusions based on our research and know-how regarding these blockchain technologies.

8.1 Bitcoin

8.1.1 Favorable Aspects

Security:

Through the process of mining, the network prevents malicious actors from gaining control over the network. The Hashing power of this network is astounding and keeps on growing, thus leading to an incredibly secure protocol. To this day, no one has achieved to hack or deceive Bitcoin, even though if successfully hacked, the reward would be in the hundreds of billions of dollars. Consequently, this network is one of the most secure systems on the planet.[33]

Censorship Resistant:

The decentralized and permissionless nature of Bitcoin allows any candidate to use this network without having to request permission from any given entity. Especially for people living in oppressed governments or dictatorships, these fundamental qualities can be especially powerful, providing valuable advantages. Once a Bitcoin transaction is sent, there isn't an entity on this planet that can stop or censor the person or its transaction unless miners decide not to validate the transaction. The censorship feature is also included in Ethereum and XRP.

Decentralizing Power:

Since the introduction of Bitcoin, a pandora's box has been opened, generating many questions, including prejudices against these types of networks. It is, therefore important to put the spotlight on the centralization vs. decentralization concept and make it more understandable and acceptable to the general public. In a developing world of digitization and data-privacy, Bitcoin brings essential discussion points to the table. The whole concept of programmable money challenges the status quo of some world powers. The idea of an increase or returning power to the individual can seem very threatening to some greedy corporations or conservative establishments, which solely have ongoing profit as their primary aim.

8.1.2 Disadvantageous Aspects

Energy Consumption:

One of the most concerning aspects is the energy consumption needed for guessing hashes. Bitcoin requires an astonishing amount of electricity to keep it´s network secure. Even though lots of miners use renewable energy sources to sustain their business model, we believe that if the network continues to grow and security must be maintained, the high energy requirement cannot be supported in the long term. We would need to see a decrease in the high energy dependency of Bitcoin or some solution addressing this issue.[78]

Lack of Standardized Policy Refunds:

Users affected by fraud cant request a refund through Bitcoin. This decentralized network structure makes it hard for any single party to fix problems between users. Responsibility is thereby solely dependent on the network user. Compensation is not possible when using these decentralized networks. However, when using centralized exchanges, one might be compensated for losses by hacks or mistakes committed by the exchange affecting the user. The lack of reassurance if money is lost or stolen is quite significant, and therefore, this issue is a remaining one and will be hard to tackle.

8.1.3 Personal Reflections

Relationship between Mining and Security:

Depending on the circumstances, this correlation is both negative and positive. In the event that the price of Bitcoin rises and the profitability of mining Bitcoin skyrockets, more miners will jump into the industry, creating an overall more secure network. On the other hand, if prices decline, it becomes less profitable to add new blocks. The result will be an increase in miners who capitulate. Due to geolocation and high electricity costs, certain miners will run into a negative monetary situation leading to a decline in total hashing and a less secure network. The monetary incentive to keep the safety of the network growing can be a double-sided sword, as it can lead to enormous fluctuations in the secure stability of the network. If miners don't see any monetary gain while mining, they will decide not to continue. This type of correlation is also seen in Ethereum and other proof-of-work digital assets.

8.2 Ethereum

8.2.1 Favorable Aspects

Ethereum also has a censorship-resistant feature (see Bitcoin censorship-resistant)

Decentralized Applications:
By creating an open-source autonomous application, will allow these applications to behave the same way every time they are run. Thus, the ability of the smart contract to act the same way every time is very beneficial to developers and will lead to creative ideas and business models that haven't even been conceived previously. In an increasing landscape where corporations sell your data for advertisement purposes, it will allow decentralized applications to shine and offer unique propositions. In a not too distant future, someone might come up with a social media app that lets users control and sell their own data, thereby allowing the user to collect applicable funds instead of some cooperation. In this scenario, the power is given back to the individual, creating a future where the individual earns money by selling his or her sensitive data or content.

Open Source and a Strong Development Team:
Open-source codes are essential for building trust and, consequently, safety into blockchain networks. In an open-source project setting, no single authority owns or controls processes, or is able to sell the software. Programmers do not work under a contract with the aim of building a required solution for someone. As they want to use the product they are building, the motivation will be more significant to develop a superior product. The motivated and credible development team aims to create an Ethereum platform with the highest potential. In the past, challenging Decentralized Autonmous Organisation (DAO) hack and Denial-of-Service (DoS) attacks were successfully solved by the team.

8.2.2 Disadvantageous Aspects

Ethereum also has a lack of standardized policy refunds (see Bitcoin lack of standardized policy refunds).

Energy Consumption:
As with Bitcoin, Ethereum relies on the same proof-of-work consensus model, which requires energy but far less than Bitcoin. This energy dilemma has led Ethereum to migrate from their current consensus model to a different approach called proof-of-stake. The switch to proof-of-stake will take some time. In addition, as current projects hosted by Ethereum rely on the ongoing functionality of the network, a switch must be protected against errors.[78]

[78] Leopold, S. J., & Englesson, N. (2017). How Eco friendly is our money and is there an alternative? Retrieved from http://papers.netrogenic.com/sid/eco-friendly-money.pdf

Storage:
As with most blockchains, storage is a constant challenge that needs to be taken into consideration if wanting to scale up the underlying chain required for blockchain to be used worldwide. Ethereum wants to be a world supercomputer used by anyone able to run its application, a situation that raises concerns regarding data storage. Currently, smart contracts live on the main chain, storage space with all its applications, contract states, and transactions will increase significantly. The larger the blockchain, the more powerful computers will be needed to run an entire node. This could lead to a situation where only a select few users are able to afford the running of a full node, thereby increasing node centralization. However, we remain optimistic that this problem will be combated since the potential for data storage capacity has grown tremendously over the last decade. [78]

8.2.3 Personal Reflections

Deliver or Wither:
Since 2016 Ethereum has proposed several scaling solutions but has not been able to provide for ways on how to implement them. 2020 is the suggested year, where we will see some of these scaling solutions being implemented. Ethereum is currently the king of decentralized applications. However, other projects like Cardano, EOS, Tron have been catching up and claim to be more scalable than Ethereum. The first-mover advantage of Ethereum won't last forever, and projects will move their decentralized applications to other blockchains if their needs aren't satisfied. Only time will tell if Ethereum will come through on their promise and remain the king of the castle.

8.3 XRP

8.3.1 Favorable Aspects

XRP also has a censorship-resistant feature (see Bitcoin censorship-resistant)

Secure:
The XRP consensus protocol is very reliable and addresses some of the shortcomings regarding proof-of-work. The feared 51% attack isn't possible in this consensus. In addition, to achieve consensus, a supermajority of over 80% must be obtained for transactions to be agreed upon or network updates to go through.

Fast, Cheap, and Energy-efficient:
When it comes to transaction speed, XRP is a leader in this respect with an impressive settling speed of 3-4 seconds per transaction. Furthermore, sending transactions with XRP is incredibly cheap. As an example, a given transaction, moved 7'337'553 USD and paid a fee of 0.000012 XRP (0.000004 USD). Another great benefit of this network is the minuscule amount of electricity needed to power the system. At the end of this chapter, a study from Stanford and Stockholm university comparing the electricity consumption of Bitcoin, Ethereum, and XRP will be presented.

Decentralized:

Since the XRP consensus protocol doesn't rely on mining, there aren't any centralization mining pool issues. Here we will examine the unique node list (UNL). On the UNL, out of 35 validators ripple runs six; this equates to having control over 17.1 % of validators on the UNL network. As this percentage is not very large, the XRP ledger consensus protocol is relatively decentralized compared to Bitcoin and Ethereum (based on the 18th of May 2020 statistics).[79]

8.3.2 Disadvantageous Aspects

XRP also has a lack of standardized policy refunds (see Bitcoin lack of standardized policy refunds).

XRP Distribution:

Ripple owns an extraordinary 55,86 billion XRP.[80] This concentration of wealth amounts to more than 50% of the entire XRP supply. Still, Ripple has implemented procedures that ensure that they cannot dump all their XRP on the open market at one time. A situation that would suffocate the market including its asset price. They have locked up the majority of their XRP (49,5 billion) in cryptographically secured escrow contracts. This contract grants Ripple 1 billion XRP per month that can be used to fund operations or make strategic partnerships. The amount of XRP leftover from the 1 billion granted is put back into an escrow contract and prolonged for another five years. Depending on the amount returned into escrow contact, it ensures a calculated distribution of XRP throughout five years or beyond. Even though this is a smart approach, one cannot deny that Ripple, in a matter of monetary XRP distributions, retains a monopoly. Nevertheless, Ripple aspires to expand its ecosystem and see that XRP thrives on the open market. The ambition of Ripple is, therefore, to have XRP widely used and distributed. Only time will tell if and how this trend will continue to be possible.

8.3.3 Personal Reflections

Working with the System not Against it:

In contrast to Bitcoin, with its aim to circumvent or make banks obsolete, Ripple works with governments and regulators around the world to make XRP regulatory compliant. Ripple does not want to disrupt the current monetary system but rather make it more efficient. We find this approach to be very smart, as we don't foresee banks or governments disappear as current service providers or give up their powerful hold on the market.

[79] Validator Registry. Retrieved 17 February 2020 from XRP Charts: https://xrpcharts.ripple.com/#/validators

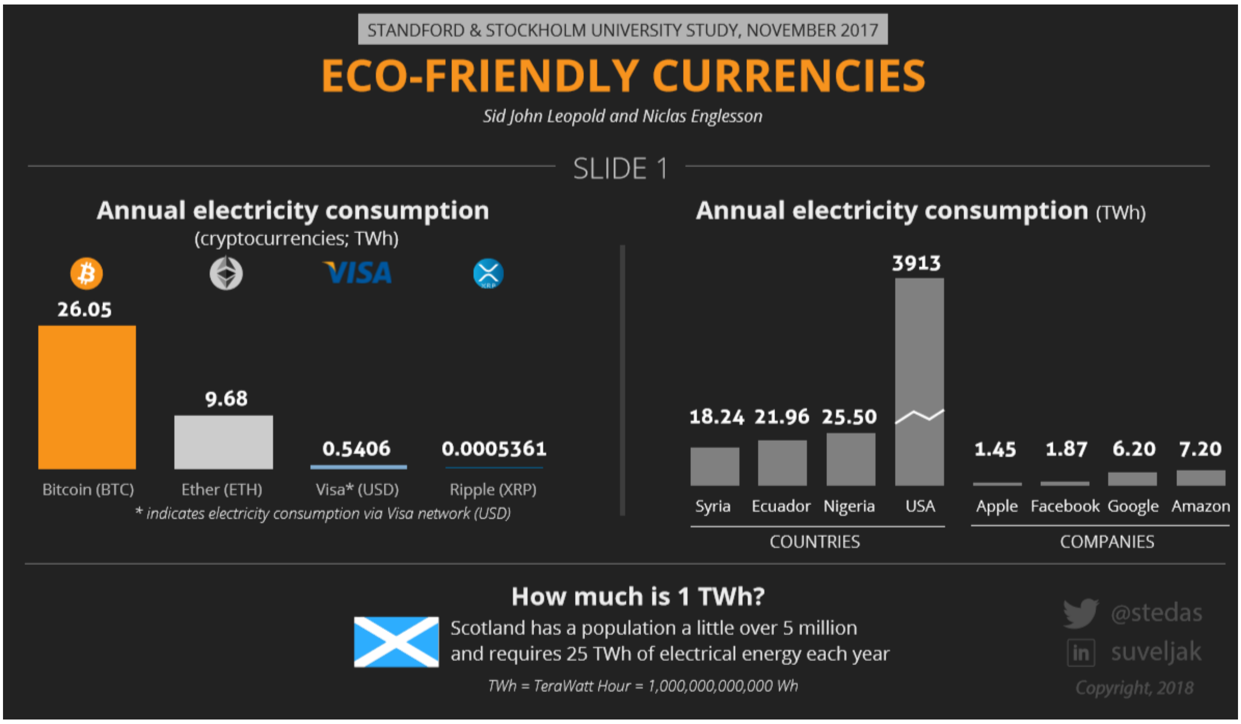
[80] Market Performance. Retrieved 19 May 2020 from Ripple: https://ripple.com/xrp/market-performance

8.4 Final Thoughts

All three blockchains have their distinct benefits and disadvantages. We do not believe that one single digital asset will end up ruling them all. They will continue to carve out specialized niches within the market to attract users. How these and other digital assets compete amongst each other for different use-cases will be explained in phase 2.

In the following chapters, we compare Bitcoin, Ethereum, and XRP amounts of transactions per second, energy consumption, transaction fee, and transaction speed with one another.

8.4.1 Electricity



STANDFORD & STOCKHOLM UNIVERSITY STUDY, NOVEMBER 2017

ECO-FRIENDLY CURRENCIES

Sid John Leopold and Niclas Englesson

SLIDE 1

How much is 1 TWh?

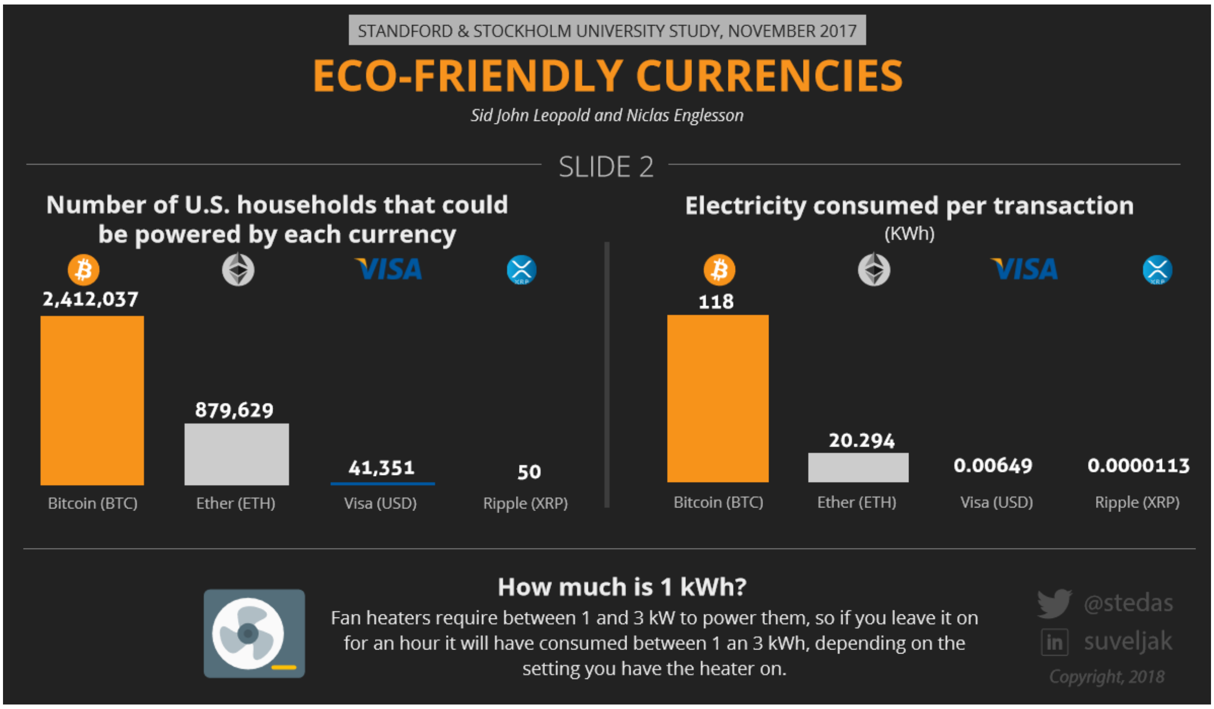
Scotland has a population a little over 5 million and requires 25 TWh of electrical energy each year

TWh = TeraWatt Hour = 1,000,000,000,000 Wh

Copyright, 2018

Figure 31. Electricity consumption [81]

[81] Leopold, S. J., & Englesson, N. (Producer). (2017). Eco-Friendly Currencies. Retrieved from https://www.stedas.hr/ripple/Eco-friendly-cryptocurrency.pdf



STANDFORD & STOCKHOLM UNIVERSITY STUDY, NOVEMBER 2017

ECO-FRIENDLY CURRENCIES

Sid John Leopold and Niclas Englesson

SLIDE 2

Number of U.S. households that could be powered by each currency

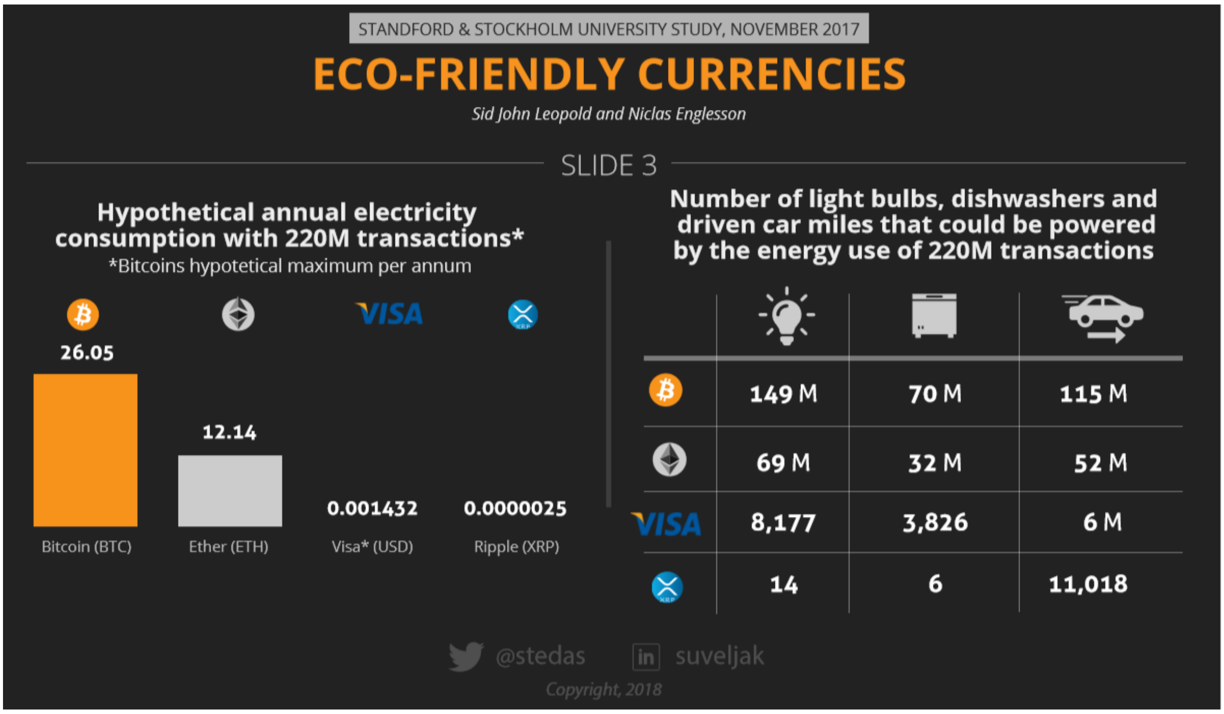
Electricity consumed per transaction (KWh)

How much is 1 kWh?

Fan heaters require between 1 and 3 kW to power them, so if you leave it on for an hour it will have consumed between 1 an 3 kWh, depending on the setting you have the heater on.

@stedas
suveljak
Copyright, 2018

Figure 32. Electricity consumed and households that could be powered by currencies [81]



STANDFORD & STOCKHOLM UNIVERSITY STUDY, NOVEMBER 2017

ECO-FRIENDLY CURRENCIES

Sid John Leopold and Niclas Englesson

SLIDE 3

Hypothetical annual electricity consumption with 220M transactions*

*Bitcoins hypotetical maximum per annum

Number of light bulbs, dishwashers and driven car miles that could be powered by the energy use of 220M transactions

	💡	▭	🚗
₿	149 M	70 M	115 M
Ξ	69 M	32 M	52 M
VISA	8,177	3,826	6 M
✕	14	6	11,018

@stedas
suveljak
Copyright, 2018

Figure 33. Electricity consumption overview [81]

8.4.2 Conclusion of Electricity

The proof-of-work consensus protocol is very energy-intensive, so keeping the network up and running consumes a lot of power. It is worth noting that back in 2017 when this study was published coincides with a significant increase in Bitcoin attention and price. Even if most of the energy used is renewable, energy requirements will most likely increase as the network picks up inactivity and is more widely used. The fact that in November 2017, Bitcoin required more power than some countries is absolutely unacceptable. In order to achieve consensus, more energy-efficient options or sources should be found. Means to decrease electricity dependency would require alternative energy solutions. This would especially be the case for proof-of-work, which depends highly on electricity and would thus not be sustainable. Currently, only a few alternatives have been suggested. Using Bitcoin and Ethereum should ensure that a healthy environment can be maintained.

8.4.3 Scalability (TPS)

Blockchain	Max. Transactions per second (TPS)
Bitcoin[82]	7
Ethereum[49]	15
XRP[49]	1’500
Visa[24]	65’000

Figure 34. Scalability

8.4.3.1 Conclusion Scalability

These TPS are derived from the scalability of the underlying layer-1 blockchain and do not account or consider any implementations or augmentations of layer-2 solutions like payment channels etc.

Thereby we can conclude that none of these layer-1 blockchains can match or compete with existing payment networks. However, there is currently a lot of innovation and development focused on these scaling limitations. Consequently, these numbers will not stay stagnant and increase in time just as early internet bandwidth was highly inefficient in the early days of the internet. Furthermore, we believe breakthroughs and new approaches towards lifting the current bottleneck of these TPS will eventually increase and be able to match or exceed conventional payment networks.

[82] Scalability. (2019). In *BItcoinWiki*. Retrieved from https://en.bitcoin.it/wiki/Scalability

8.4.4 Average Transaction Fee

8.4.4.1 Bitcoin

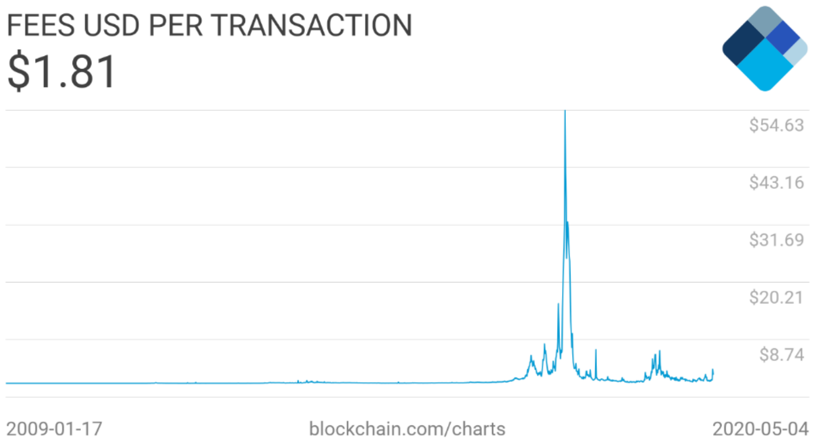


Figure 35. Fees USD per Transaction [83]

8.4.4.2 Ethereum

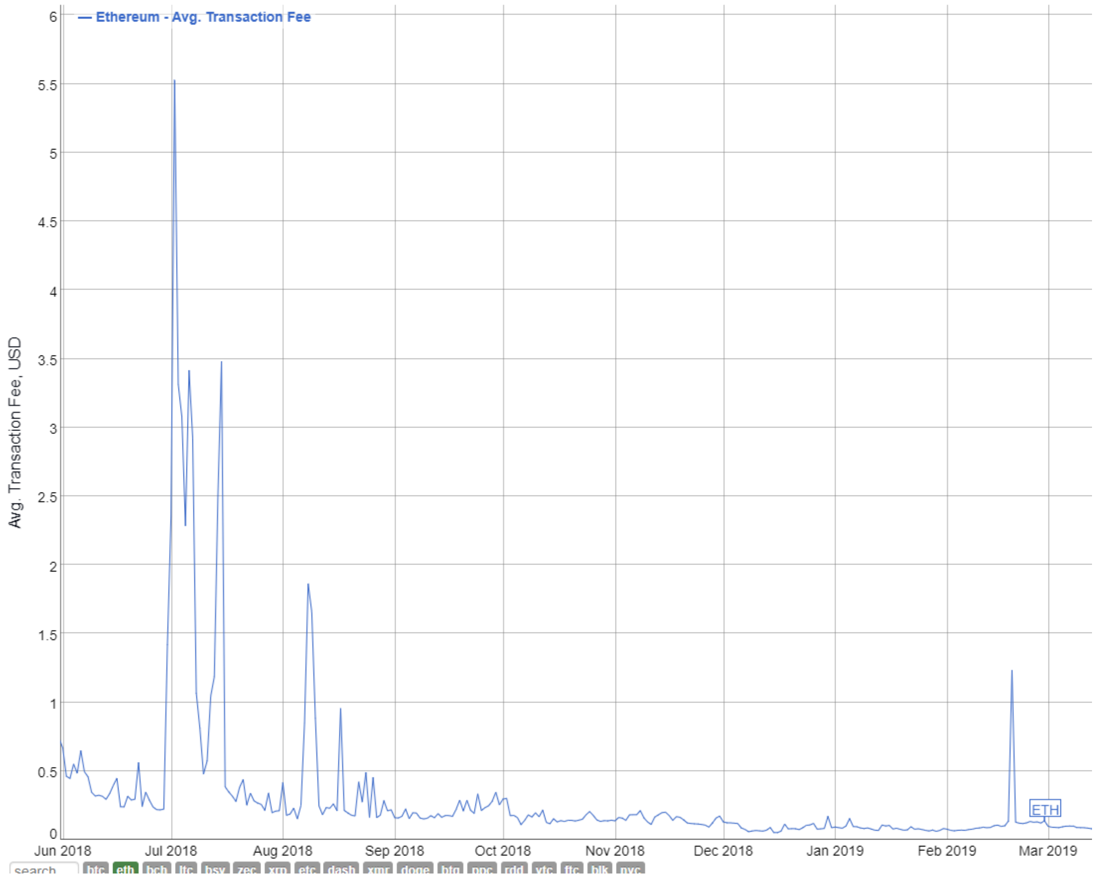
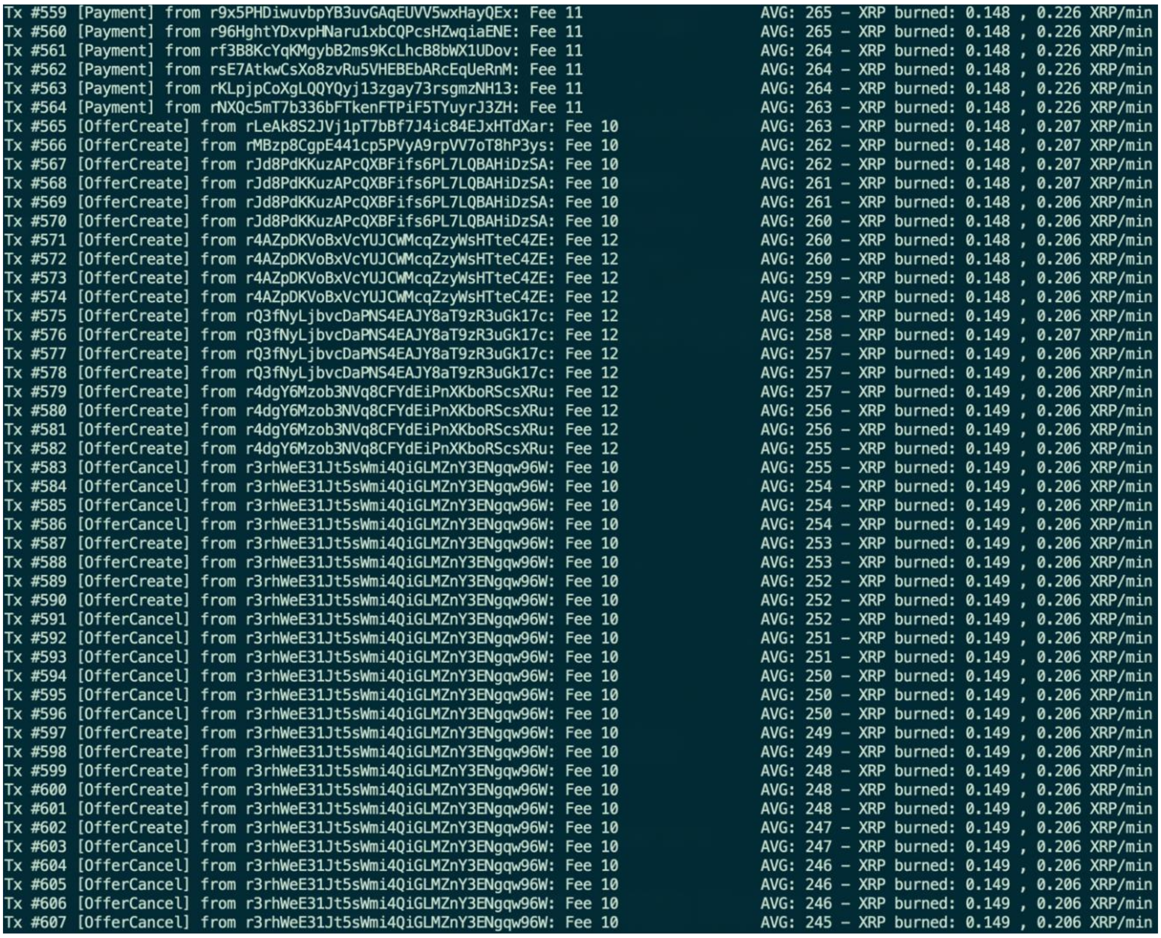


Figure 36. Average Transaction Fee Ethereum [84]

[83] Blockchain (Producer). (2020). Fees Per Transaction (USD). Retrieved from https://www.blockchain.com/charts/cost-per-transaction?timespan=all

8.4.4.3 XRP

We could not find a reliable source regarding the average XRP transaction fee. We, therefore, created a script that listens to the XRPL and subscribes to all transaction streams. Thus, based on the live information, the XRP fee is around 12 drops. At an XRP price of 20 cents per XRP, this would be equivalent to 0.0000024 cents.



```
Tx #559 [Payment] from r9x5PHDiwuvbpYB3uvGAqEUVV5wxHayQEx: Fee 11                    AVG: 265 - XRP burned: 0.148 , 0.226 XRP/min
Tx #560 [Payment] from r96HghtYDxvpHNaru1xbCQPcsHZwqiaENE: Fee 11                    AVG: 265 - XRP burned: 0.148 , 0.226 XRP/min
Tx #561 [Payment] from rf3B8KcYqKMgybB2ms9KcLhcB8bWX1UDov: Fee 11                    AVG: 264 - XRP burned: 0.148 , 0.226 XRP/min
Tx #562 [Payment] from rsE7AtkwCsXo8zvRu5VHEBEbARcEqUeRnM: Fee 11                    AVG: 264 - XRP burned: 0.148 , 0.226 XRP/min
Tx #563 [Payment] from rKLpjpCoXgLQQYQyj13zgay73rsgmzNH13: Fee 11                    AVG: 264 - XRP burned: 0.148 , 0.226 XRP/min
Tx #564 [Payment] from rNXQc5mT7b336bFTkenFTPiF5TYuyrJ3ZH: Fee 11                    AVG: 263 - XRP burned: 0.148 , 0.226 XRP/min
Tx #565 [OfferCreate] from rLeAk8S2JVj1pT7bBf7J4ic84EJxHTdXar: Fee 10                AVG: 263 - XRP burned: 0.148 , 0.207 XRP/min
Tx #566 [OfferCreate] from rMBzp8CgpE441cp5PVyA9rpVV7oT8hP3ys: Fee 10                AVG: 262 - XRP burned: 0.148 , 0.207 XRP/min
Tx #567 [OfferCreate] from rJd8PdKKuzAPcQXBFifs6PL7LQBAHiDzSA: Fee 10                AVG: 262 - XRP burned: 0.148 , 0.207 XRP/min
Tx #568 [OfferCreate] from rJd8PdKKuzAPcQXBFifs6PL7LQBAHiDzSA: Fee 10                AVG: 261 - XRP burned: 0.148 , 0.207 XRP/min
Tx #569 [OfferCreate] from rJd8PdKKuzAPcQXBFifs6PL7LQBAHiDzSA: Fee 10                AVG: 261 - XRP burned: 0.148 , 0.206 XRP/min
Tx #570 [OfferCreate] from rJd8PdKKuzAPcQXBFifs6PL7LQBAHiDzSA: Fee 10                AVG: 260 - XRP burned: 0.148 , 0.206 XRP/min
Tx #571 [OfferCreate] from r4AZpDKVoBxVcYUJCWMcqZzyWsHTteC4ZE: Fee 12                AVG: 260 - XRP burned: 0.148 , 0.206 XRP/min
Tx #572 [OfferCreate] from r4AZpDKVoBxVcYUJCWMcqZzyWsHTteC4ZE: Fee 12                AVG: 260 - XRP burned: 0.148 , 0.206 XRP/min
Tx #573 [OfferCreate] from r4AZpDKVoBxVcYUJCWMcqZzyWsHTteC4ZE: Fee 12                AVG: 259 - XRP burned: 0.148 , 0.206 XRP/min
Tx #574 [OfferCreate] from r4AZpDKVoBxVcYUJCWMcqZzyWsHTteC4ZE: Fee 12                AVG: 259 - XRP burned: 0.148 , 0.206 XRP/min
Tx #575 [OfferCreate] from rQ3fNyLjbvcDaPNS4EAJY8aT9zR3uGk17c: Fee 12                AVG: 258 - XRP burned: 0.149 , 0.206 XRP/min
Tx #576 [OfferCreate] from rQ3fNyLjbvcDaPNS4EAJY8aT9zR3uGk17c: Fee 12                AVG: 258 - XRP burned: 0.149 , 0.207 XRP/min
Tx #577 [OfferCreate] from rQ3fNyLjbvcDaPNS4EAJY8aT9zR3uGk17c: Fee 12                AVG: 257 - XRP burned: 0.149 , 0.206 XRP/min
Tx #578 [OfferCreate] from rQ3fNyLjbvcDaPNS4EAJY8aT9zR3uGk17c: Fee 12                AVG: 257 - XRP burned: 0.149 , 0.206 XRP/min
Tx #579 [OfferCreate] from r4dgY6Mzob3NVq8CFYdEiPnXKboRScsXRu: Fee 12                AVG: 257 - XRP burned: 0.149 , 0.206 XRP/min
Tx #580 [OfferCreate] from r4dgY6Mzob3NVq8CFYdEiPnXKboRScsXRu: Fee 12                AVG: 256 - XRP burned: 0.149 , 0.206 XRP/min
Tx #581 [OfferCreate] from r4dgY6Mzob3NVq8CFYdEiPnXKboRScsXRu: Fee 12                AVG: 256 - XRP burned: 0.149 , 0.206 XRP/min
Tx #582 [OfferCreate] from r4dgY6Mzob3NVq8CFYdEiPnXKboRScsXRu: Fee 12                AVG: 255 - XRP burned: 0.149 , 0.206 XRP/min
Tx #583 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 255 - XRP burned: 0.149 , 0.206 XRP/min
Tx #584 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 254 - XRP burned: 0.149 , 0.206 XRP/min
Tx #585 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 254 - XRP burned: 0.149 , 0.206 XRP/min
Tx #586 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 254 - XRP burned: 0.149 , 0.206 XRP/min
Tx #587 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 253 - XRP burned: 0.149 , 0.206 XRP/min
Tx #588 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 253 - XRP burned: 0.149 , 0.206 XRP/min
Tx #589 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 252 - XRP burned: 0.149 , 0.206 XRP/min
Tx #590 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 252 - XRP burned: 0.149 , 0.206 XRP/min
Tx #591 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 252 - XRP burned: 0.149 , 0.206 XRP/min
Tx #592 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 251 - XRP burned: 0.149 , 0.206 XRP/min
Tx #593 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 251 - XRP burned: 0.149 , 0.206 XRP/min
Tx #594 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 250 - XRP burned: 0.149 , 0.206 XRP/min
Tx #595 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 250 - XRP burned: 0.149 , 0.206 XRP/min
Tx #596 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 250 - XRP burned: 0.149 , 0.206 XRP/min
Tx #597 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 249 - XRP burned: 0.149 , 0.206 XRP/min
Tx #598 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 249 - XRP burned: 0.149 , 0.206 XRP/min
Tx #599 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 248 - XRP burned: 0.149 , 0.206 XRP/min
Tx #600 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 248 - XRP burned: 0.149 , 0.206 XRP/min
Tx #601 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 248 - XRP burned: 0.149 , 0.206 XRP/min
Tx #602 [OfferCreate] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 247 - XRP burned: 0.149 , 0.206 XRP/min
Tx #603 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 247 - XRP burned: 0.149 , 0.206 XRP/min
Tx #604 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 246 - XRP burned: 0.149 , 0.206 XRP/min
Tx #605 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 246 - XRP burned: 0.149 , 0.206 XRP/min
Tx #606 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 246 - XRP burned: 0.149 , 0.206 XRP/min
Tx #607 [OfferCancel] from r3rhWeE31Jt5sWmi4QiGLMZnY3ENgqw96W: Fee 10                AVG: 245 - XRP burned: 0.149 , 0.206 XRP/min
```

Figure 37. Average XRP transaction fee

8.4.4.4 Conclusion Average Transaction Fee

Comparing the average transaction fee of these blockchains highlights the ineptitude of the current financial system to challenge these decentralized payments networks. Try sending millions or in this transaction over a billion dollars through the current financial system and paying a transaction fee anywhere between 0.0000024 cents – 2 Dollars, which is highly improbable in the applicable corresponding banking system.

[84] Bitinfocharts. (Producer). Ethereum average transaction fee. Retrieved from. https://bitinfocharts.com/comparison/ethereum-transactionfees.html

8.4.5 Transaction Speed (On-Chain)

Since both Bitcoin and Ethereum run PoW, one cannot conclude a transaction to be finalized after only one block is added to the chain. Arguments exist regarding how many blocks need to be appended to a block prior to having a final chain. In order to ensure that a transaction and block are confirmed and finalized, we will use at least six blocks.[85]

8.4.5.1 Bitcoin

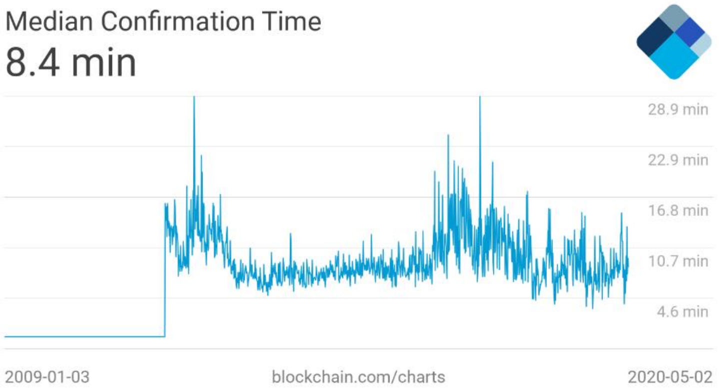


Figure 38. Median Confirmation Time [86]

8.4.5.2 Ethereum

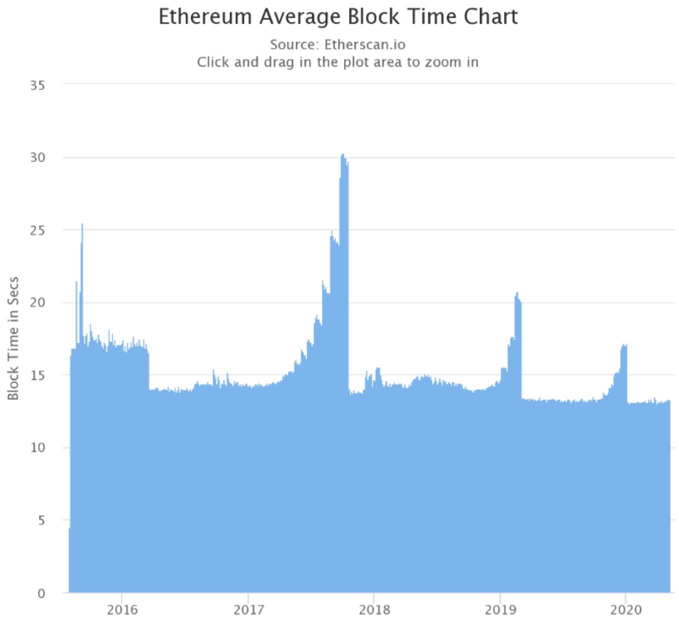


Figure 39. Ethereum Average Block Time Chart [87]

[85] BitcoinWiki. (2018) Conformation. Retrieved from https://en.bitcoin.it/wiki/Confirmation
[86] Blockchain (Producer). (2020). Median Confirmation Time. Retrieved from https://www.blockchain.com/charts/median-confirmation-time?timespan=2years

8.4.5.3 XRP

Since there are not any conflicts of an XRP ledger being split into 2, XRP close time can be regarded as final after one ledger has been added to the chain. Therefore, we can consider a ledger confirmed and final as soon as it is added to the chain. The XRP average close time is between 3-4 seconds.[88]

8.4.5.4 Conclusion Block Conformations

Blockchain	Final transaction speed
Bitcoin	60 min
Ethereum	1 min 30 seconds
XRP	3-4 seconds

Figure 40. Transaction speed table

8.5 Conclusion

Currently, Bitcoin and Ethereum cannot handle the Transactions per second (TPS) needed to unleash their full potential. However, both of these communities have brilliant programmers and entrepreneurs developing the projects. Furthermore, both Ethereum and Bitcoin have proposed various scaling solutions to increase current network capacity and address other relevant issues. We will examine these solutions in the next chapter.

[87] Etherscan. (Producer). (2020). Ethereum Average Block Time Chart. Retrieved from https://etherscan.io/chart/blocktime
[88] Market Performance. (n.d). *XRP Market Metrics*. Retrieved from https://ripple.com/xrp/market-performance/

9 Solutions for Scaling

Bitcoin and Ethereum both aim to be globally used and implemented into various businesses or used by everyday people. For this to be feasible, we must address the severe scaling limitations existing currently, if these networks want to achieve global adoption.
The most promising scaling solutions are presented below for both Bitcoin and Ethereum.

9.1 Bitcoin

Since Bitcoin uses the proof-of-work consensus model, few issues arise regarding scaling and transaction speed. On average, a new block is appended approximately every 10 minutes. Consequently, this amount of time would be needed for a transaction to be included in the next block. In order to ensure that a confirmed network transaction causes no conflict of interest with other blocks, it is wise to wait until a few subsequent blocks have been added.

Six block confirmation is a safe assumption that no conflict of interest exists with applicable miners, and the added blocks are immutable. With the six-block requirement, an emerging issue arises regarding the speed of transactions and the usability of the system.

Here are some scaling solutions which are currently being worked on or being adopted to increase the network capacity of Bitcoin.

9.1.1 Segregated Witness (SegWit)

SegWit is a Bitcoin network soft fork upgrade implemented on the 23rd. Of August 2017. The aim was to increase block capability by separating the “witness” from the lists of inputs. This witness data is required to check for transaction validity but not required for the determination of transaction effects. SegWit also addresses the transaction malleability. As a signature does not cover all transacted data, this weakness was discovered upon signing the transaction. Consequently, a network node could alter the transaction in such a way that the hash would become invalid. As the change only affects the hash of the transaction while keeping transaction output unaltered, it will still allow for Bitcoin to be transferred to the intended recipient. [89]

9.1.1.1 Challenges

As with any soft fork, the upgrade to a new protocol version is voluntary. Therefore, an update will take time until a majority of network nodes have agreed on adopting the proposed changes.

[89] Segregated Witness Proposal. (2018). *GitHub repository, Bitcoin/bips/BIP 141.* Retrieved from https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

9.1.2 Lightning Network (LN)

The Lightning Network is a layer-2 scaling solution. This type of solution is not directly implemented onto the blockchain but moved off-chain.[90] The Lightning Network is still in its early development stages and thus not ready for everyday use. The solution is not solely applicable to Bitcoin but can also be implemented by other blockchains. As the Lightning Network eliminates the need to broadcast every transaction to the network and wait for block confirmations, it offers Bitcoin a mean for cheaper and faster transactions.[90]

Payment channels are essential for the Lightning Network functioning. These channels allow two or more participants to transact fast and frequently off-chain, but they settle the final verdict into an on-chain transaction. Payment channels are the transaction pathway through which the LN transfers value.[90]
In this example, we will use Alice (A) and Starbucks (S) to explain the process of using the lightning network and how it works.

Alice wants to buy coffee at Starbucks, but the on-chain transaction fee is too high and takes too long to conduct their business. Thus, the coffee will be cold before the transaction is confirmed. To solve this problem, they decide to use the lightning network. They open a payment channel on the public blockchain and deposit their funds into a two-party, multi-signature "channel" Bitcoin address.[90] This wallet functions like a deposit safe. Once Alice and Starbucks have deposited their Bitcoin into the multi-signature wallet (here only Alice deposits funds), they can create an open transaction and broadcast it to the network. Once this is broadcasted, they can now start sending transactions, without every time transacting on the public network. These transactions between these two players are called commitment transactions.[90]

Commitment transactions divide applicable funds between both parties and act like IOU's. Payment will be paid out once the channel has closed. In commitment transactions, both parties can credit or debit funds from their accounts until one party runs out of funds in the payment channel. Their balances will be updated off-chain. If they decide to close the payment channel, then the latest verified transaction will be broadcast to the network in a single on-chain transaction. Thus they avoid settling various personal transactions on-chain while paying on-chain fees and waiting for block confirmations. [91]

[90] Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.
[91] LND Overview and Developer Guide. (n.d). Retrieved from Lightning Network Developers: https://dev.lightning.community/overview/

9.1.2.1 Multihop Payments

Here we will use Alice (A), Bob (B), Carol (C), and Dave (D).

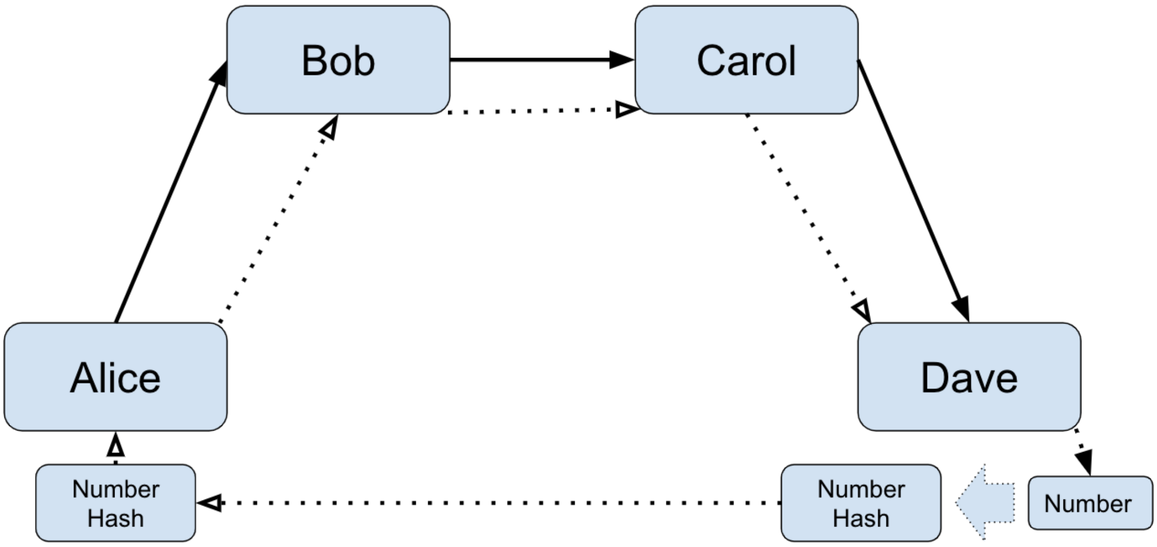


Figure 41. Visualization of multihop payments

Single payment channels work fine as long as you have a relationship with the counterparty. However, in an everyday scenario, one does not always know or have a payment channel open with the desired business entity. To solve this, the lightning network can move funds from Person A to person D, even though no open payment channel between them exists. This will only work if person A has another payment channel open with Person B, which has an open payment channel with Person D through a connection from person C. Nevertheless, this transaction will only go through if the amount of value sent does not exceed the amount locked up in these open payment channels.[91]

For this to work, the following steps occur. Alice notifies Dave that she wants to send him money. If Dave wants to accept this money, he will produce a random number and hashes it. Furthermore, he sends this hash to Alice. Alice will create a Hash Time-locked Contract (HTLC) [90] with Bob. This means that Alice tells Bob: “I will pay you if you can find me the number of the hash in a particular amount of time.” Primarily only Bob can redeem the money with knowledge of the number, and if the time expires, he can no longer redeem the funds. This HTLC allows Alice to produce a conditional promise to Bob while ensuring that her funds will not accidentally be lost if Bob never learns the number. [91]

Bob will do the same to Carol since he can only redeem the Bitcoin if he discovers the number of the hash. Carol will produce another HTLC with Dave. However, Dave does possess the knowledge regarding the corresponding number from the hash. If Dave wants to collect the funds, he will reveal the number to Carol, and she will show the number to Bob, and he will reveal the number to Alice. Throughout this process, all involved persons in the chain can collect their Bitcoin, and Alice successfully moved her money to Dave without having a direct open payment channel.

Now everyone can move forward since they all have a guaranteed way to pull their funds by broadcasting the HTLC's to the Bitcoin network (on-chain). An alternative exists for this transaction not to be on-chain. Since Alice is sure that Bob can redeem his funds because he knows the number, she will tell Bob, "I will pay you regardless of the number." Bob does the same with Carol, and she does this same with Dave. Thereby completing the circle and Bob and Carol collect their fees for sending the money from Alice to Dave without creating an on-chain transaction.[91]

In conclusion, the Lightning network is a useful way to settle microtransactions or small value payments between two or more parties. The payment should be fast and cheap whilst not compromising any security aspect. Thus, funds can only be released inside the payment channel after it has been closed. The drawback is that when implementing a payment channel, Bitcoin is locked up in the channel. Consequently, one cannot perform a subsequent transaction if the payment channel gateway transaction value exceeds payment channels funds.

9.1.3 Bitcoin Cash (BCH)

Bitcoin Cash originated from a dispute within the Bitcoin community. Whereas one side favored the scaling solution SegWit, the other side of the community favored an increase in the block size of mined blocks. This controversy ultimately led to a hard fork in the Bitcoin network and thereby creating Bitcoin Cash. This hard fork took place on the 1. August 2017.[92]

The main reasoning behind this hard fork was to increase the block size from 1 Mb to 32Mb, which would allow for more transactions being included in each consecutive mined block. [92] Consequently, more storage space would be needed to run a full node, including its Bitcoin Cash transaction history. It is worth remembering that up until the creation of the hard fork Bitcoin Cash, Bitcoin and Bitcoin Cash had identical block records with an identical total supply of coins (each with 21 million).

[92] Webb, N. (2018). A Fork in the Blockchain: Income Tax and the Bitcoin/Bitcoin Cash Hard Fork. *North Carolina Journal of Law & Technology*, *19*(4), 283.

Since one of the great virtues of a decentralized network like Bitcoin is that both communities were able to solve this dispute by creating or continuing with their version of what they believe to be beneficial to the broader community. This freedom of ideas and creativity is an undeniable strength in decentralized networks.

However, this hard fork does highlight some concerning issues. The alluring situation of having an asset that cannot be duplicated, thus preventing an increase in its total supply, means that only 21 million Bitcoin will ever be available on the market. Still, when splitting the Bitcoin chain, new or additional digital assets are produced in the form of Bitcoin cash or another hard fork. Thereby, one still possesses the original Bitcoin and is at the same time awarded with the hard fork Bitcoin Cash.

When creating a new hard fork, the network awards Bitcoin holders with a 1:1 Bitcoin/hard fork ratio. Thus by having 10 Bitcoin, I will have after the fork 10 Bitcoin cash. Since Bitcoin cash also has trading value on the open market, one will essentially be awarded “Free Money” from this hard fork. Thus, no additional Bitcoin will be created. Instead, alternative hard fork versions will provide Bitcoin holders with additional currency.

9.1.4 Conclusion Bitcoin Scaling Solutions

Bitcoin has proposed various scaling solutions that might help the network process more transactions and become faster. However, none of these solutions fix the underlying issues originating from the expensive PoW consensus protocol. We wish to see Bitcoin succeed with their mission and provide their services. Nonetheless, we came to the conclusion that these scaling solutions are meaningless; if not, the underlying architecture is changed. Changing consensus protocol is an arduous task, and since Bitcoin is the largest digital asset currently on the market, all changes and updates have to be tested and error-free. Bitcoin has a long and bumpy road ahead of itself, but it has only existed for 11 years. We hope to see more scaling solutions for Bitcoin, which will alter or decrease dependence on electricity.

9.2 Ethereum

In late 2017, the need for scaling solutions was apparent when crypto kitties (a decentralized application on top of Ethereum) clogged up the whole network and slowed down transaction confirmations, thus skyrocketing fees. If Ethereum wants to prevail and be the backbone of decentralized applications (dapps), it will need to scale from its current form drastically. Ethereum's developers have discussed among themselves the option to abandon the proof-of-work consensus model and switch to proof-of-stake.

To increase block sizes so each node can validate more transactions would require more data storage means, which would not be a viable and long term solution for the Ethereum community, as this could lead to an increase in centralized network nodes. An increase in storage capacity would require better and more expensive hardware, not manageable by most computers, and unaffordable by average network participants.
A consequence of indefinitely increasing block size would result in an ongoing challenge to keep up with data storage requirements, which could lead to a centralization of miners and nodes.

Here we will present some of the most promising scaling solutions for Ethereum proposed by the community and how they will affect the scaling dilemma. By implementing some of these scaling solutions, Ethereum wishes to transition from a second-generation blockchain to a third-generation blockchain and upgrading to Ethereum 2.0, a term used to describe a series of potential updates of Ethereum.

9.2.1 Layer-1 Solutions (on-chain)

9.2.1.1 Casper

Casper is a layer-1 solution and aims to be a smart contract which will implement and monitor proof-of-Stake.

Casper is a protocol change from the current implementation of PoW to PoS. The implementation of Casper is based on the same application as proof-of-stake. As it is more efficient, secure, and scalable, Ethereum wants to transition from proof-of-work to proof-of-stake. The big difference between Casper and many other proof-of-stake algorithms is that you, as a validator, will lose your stacked funds if you try to mess with the network. Casper is an implementation that solves fundamental algorithm problems in proof-of-stake, with the problem also called "nothing at stake" (read more about proof-of-stake).

9.2.2 Layer-2 Solutions (off-chain)

It is very difficult to upgrade existing blockchains to handle higher levels of throughput on-chain transactions while maintaining current security and decentralization levels. Layer-2 solutions solve this issue by moving some computations off-chain based on reasons such as saving computing resources, privacy, obtaining lower latency, and so on.

By utilizing layer-2 solutions, the original blockchain will still be the ultimate judge in the event of any disputes.

9.2.2.1 State Channels

State channels enable a sender to make off-chain payments while being backed by an on-chain token deposit. When making a payment, the sender signs a proof of balance to the receiver. These balance proofs can be compared to digital checks but cannot exceed the number of tokens held in the deposit on-chain. State channels are similar to payment channels but differ because Ethereum also handles states, not only transactions like in Bitcoin's payment channel. [93]

State channels enable a sender to make off-chain payments while being backed by an on-chain token deposit. When making a payment, the sender signs a proof of balance to the receiver. These balance proofs can be compared to digital checks but cannot exceed the number of tokens held in the deposit on-chain. State channels are similar to payment channels but differ because Ethereum also handles states, not only transactions like in Bitcoin's payment channel. [93]

9.2.2.2 Challenges

One considerable disadvantage of these state channels is that one needs to lock up a certain amount of tokens in order to facilitate transactions. Consequently, if not all tokens are used in the transaction, leftover tokens will remain idle deposited on-chain. This challenge is mitigated by not having to create a payment channel with everyone on the network, but instead, use alternative payment routes by involving other network participants (see XXX). A drawback to this solution would be a potential increase in centralization, as hub users with many open payment channels can end up providing preferred network payment channels.

[93] Stark, J. (2018). Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit. Retrieved from https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

9.2.3 Raiden Network

The Raiden network aims to bring fast, cheap, and scalable transactions on the Ethereum network. The Raiden network is based on the implementation of the state channels in Ethereum. It is very similar to the lightning network. By utilizing state channels technology, it facilitates token transfers without the need for global consensus by using digitally signed, and hash-locked transfers called balance proofs. Balance proof is a binging agreement enforced by the Ethereum blockchain. Raiden Network is used primarily for ERC-20 tokens, which is a standard token protocol for tokens issued on the Ethereum blockchain. [94]

Like the lightning network, two people do not need to have an open payment channel with each other if there is at least one route through a network of channels that connects the two parties.

9.2.4 Sharding

Currently, the nodes of the Ethereum network process all transactions that go through the network sequentially. This provides excellent security and decentralization, but it limits the throughput of the system and, thus, effects scaling.

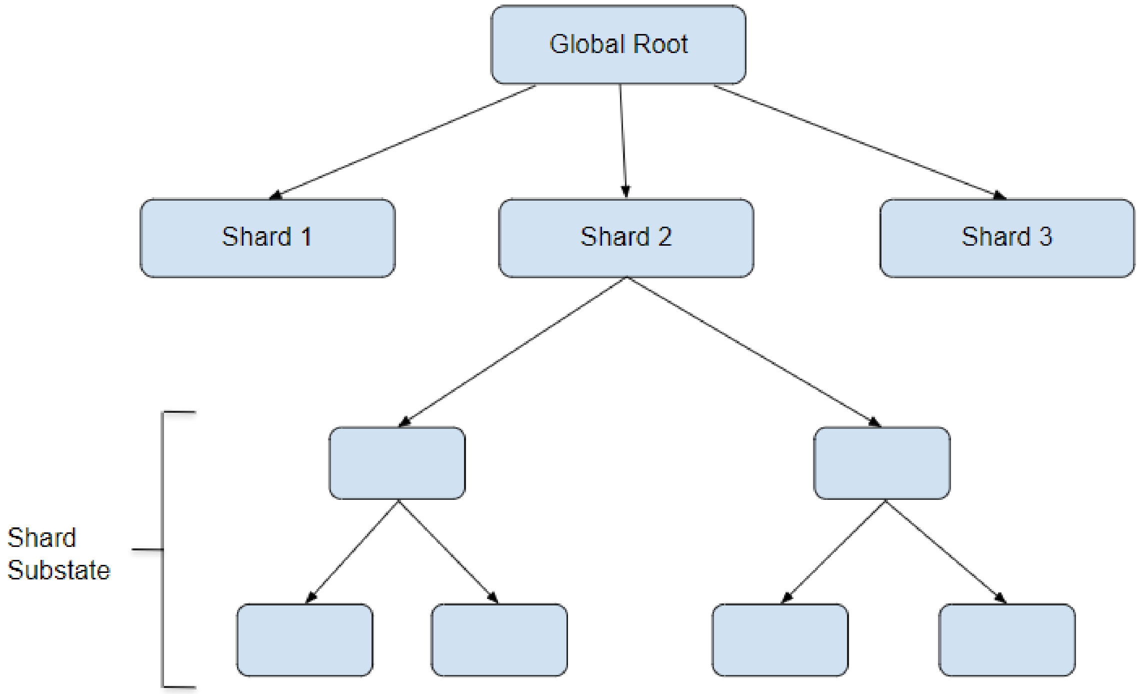


Figure 42. Visualization of Sharding where nodes are pictured as Global Root

[94] What is the Raiden Network. (2018). Retrieved from Raiden Network: https://raiden.network/101.html

A solution to tackle the scaling problem is sharding. Sharding is no new concept, as its principles are used in software database development. Sharding aims to parallelize and share network node efforts. Instead of each node containing the entire Ethereum state, the state can be divided into shards. Each shard will contain an independent piece of the state, including its transaction history.

As a consequence, an individual shard does not have to process every required Ethereum network operation, but operations can be divided between different network shards. In the scaling solution, shards can also be nested into each other; thus, a shard can contain several sub-shards. Every node must only validate shard transactions to whom they are connected. [95]

9.2.4.1 Challenges

Sharding is not a viable solution for Ethereum until they shift from the proof-of-work consensus because you cannot stop a miner from applying their work to a given shard. Thereby the computational power needed to take of a shard is very small. Thus proof-of-stake is a requirement for sharding to become a reality. Ethereum wants to solve this problem with random sampling in PoS. This mechanism enforces that validators cannot choose which shard they wish to work on, and a validator does not know beforehand which shard it will work on, which is solved by a reshuffling of the shards.

Cross shard communication remains a problem. Handling a transaction within one shard presents no significant obstacles. However, the situation becomes more complicated once a shard A address wants to send a transaction to a different shard B address. In order to tackle this communication issue, a protocol upgrade would have to be undertaken, or a new protocol must be implemented.

9.2.4.2 Conclusion Sharding

By dividing blockchain state into smaller shard pieces will allow network responsibilities to be divided among individual shards. The sequential node validation mode will be switched to a parallel or shared validation mode. This can lead to an increase in potential node transaction throughputs on the network. However, cross-communication is an issue that needs to be resolved before this can become a realistic scaling solution for Ethereum or other applicable blockchains. Currently, Ethereum still runs a PoW consensus, which renders the sharding solution impractical and dangerous. PoS is only a first step towards realizing Sharding.

[95] Jordan, R. (2018). How to Scale Ethereum: Sharding Explained. Retrieved from https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce

9.2.5 Plasma

Conceived on the 11th of August 2017, the idea behind plasma was the construction of nested blockchains. The state of these child blockchains is committed to the root chain (Ethereum). There is not any limit to how many child blockchains a child can have, which significantly improves scalability. Plasma will be enforced by a smart contract that dictates the rules of the implementation. [96]

Plasma is fraud-proof. If an incorrect state is committed, anyone else can submit evidence to a parent/root chain and disagree. There is a hierarchy order, whereas the main chain acts as the final judge and can resolve disputes between child blockchains. If the conflicts are minor, the parent blockchain might also be able to determine the dispute. [96]

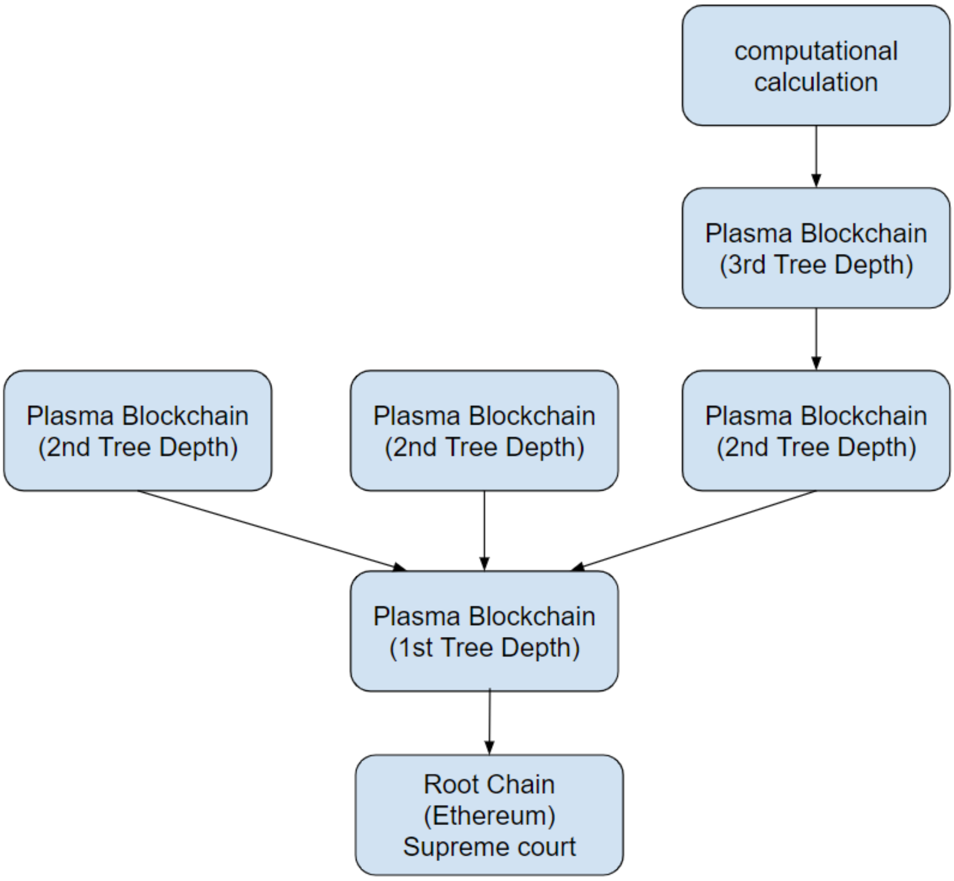

computational calculation
Plasma Blockchain (3rd Tree Depth)
Plasma Blockchain (2nd Tree Depth)
Plasma Blockchain (2nd Tree Depth)
Plasma Blockchain (2nd Tree Depth)
Plasma Blockchain (1st Tree Depth)
Root Chain (Ethereum) Supreme court

Figure 43. Visualization of Plasma

A goal is trust minimization so that the activity in this child blockchains should be as untrusted as possible.

[96] Buterin, V., & Poon, J. (2017). Plasma: Scalable Autonomous Smart Contracts. Retrieved from https://plasma.io/plasma-deprecated.pdf

You can upload a public code to the public Ethereum network and thus allow the creation of a private network that is enforceable from the main chain and creates high scalability for the Decentralized application. [96]

The way plasma enforces these child blockchains is to commit to the root chain periodically. This mechanism can be compared to a court system, whereas the higher up one goes inside the chain of blockchains, the more significant the power of enforceability and final say they have. The Ethereum main chain is the supreme court and administers different responsibilities to the child blockchain. Another great benefit is that you can map out the computation of any given task into a child blockchain, which also maps out operations into their child blockchains, and then you reduce it back down to get the results. This technique is called a map-reduce and is a well-established feature in distributed computing. [96]

9.2.5.1 Conclusion Plasma

Plasma is a desirable scaling solution not only for transactions but also for smart contracts and the way they behave and administer enforceability. The enforceability of the public network allows these private parties and private blockchains to communicate and interact with each other in a trustworthy matter.

9.2.6 Conclusion Ethereum Scaling Solutions

Ethereum has many answers regarding scalability. These scaling solutions have been in development for a while now, and do not guarantee that they will work. Nevertheless, Ethereum has a large community base and brilliant programmers, contributing a lot of time and effort to levitate Ethereum to new levels and achieve greatness. Only time will tell which of these solutions eventually do get implemented and create growth within the network and which will remain research.

Phase 2 – Real-World Usage

10 Today's Monetary System & Digital Currencies

Money is a belief system; the only thing giving any fiat currency value is trust. The trust any individual or business will bestow on a currency will always be based on a mutual acceptance or agreement that a suggested currency has ongoing value, also in the future. Blockchain and DLT solutions aim to circumvent or aid the current legacy system, depending on the digital asset. Blockchain is all about trust. Money is all about trust. We believe that digital assets will play a role in the upcoming decade regarding the monetary system, moving value around the world, and the tokenization of everything.

From the beginning of blockchain technology, it has so far influenced the financial sector to a large extent, through cryptocurrency. A few digital assets have already entered into agreements with banks and other participants to develop payment services and systems based on this technology.

The Digital asset space has only been around for 11 years. Therefore, meaning we are only at the start of this digital revolution. We are comparing this technology to the early internet, which ARPANET adopted TCP/IP on 1st January 1983[97], we would find ourselves amid the 1995s, the pre era of the 2001 internet bubble. Comparing these two very similar technologies, the internet stands for the transfer of information across the globe, while digital assets represent the transfer of value around the world. We can conclude that we haven't even scratched the surface of this technology, including its future potential. New ideas and cases will emerge that we haven't yet imagined. We are very fortunate to live in this very exciting age of digital asset opportunities.

What if anyone could digitize any value and sell it to any other person in this world?
This is a promise that the future of Distributed ledger technology could deliver. Nodes secure the network, and a decentralized transaction ledger dictates ownership of assets. Encryption assures safety. There are a few hurdles and obstacles that need to be overcome for this technology to thrive and innovation to flourish. We will take a closer look at the possibilities of this technology and come up with our thoughts about future use-cases. One of these challenges is regulations; this is the next chapter of this paper.

[97] Andrews, E. (2019). Who Invented the internet? Retrieved from https://www.history.com/news/who-invented-the-internet

11 Regulation

In this chapter, we look more closely at the regulatory aspects governing the utilization of digital assets. In a rather short time, blockchain technology has evolved to become a potential asset/resource able to meet needs from the financial sector, healthcare sector, capital or energy market, including many other potential industries. As a consequence, digital assets are here to stay. For its use to be efficiently integrated and accepted in everyday life, its technology must become increasingly regulated.

As might be expected, technological regulations might differ significantly between national borders. Due to the fact that blockchain technology is worldwide accessible through the internet, one might predict with some confidence that its technology will not have its best standing in countries with strict internet laws. As a consequence, it is to be expected that blockchain companies will move to places where they profit from the most favorable regulatory settings. We will discuss those regulations we expect to be most imperative while looking at a selection of examples from different countries.

11.1 Global-Regulation

With respect to blockchain technology, the most favorable setting would be to have digital asset regulations that would be valid globally. The Financial Action Task Force (FATF) is an organization that has already taken on this task, with its aim to create a comprehensive framework/guidance for digital assets regulations.

11.1.1 What is FATF?

The FATF is an intergovernmental body established in 1989 by the G7 countries and consists of 37-member countries. Their main job is to address international concerns regarding potential threats to the integrity of the international financial system such as an abuse of the financial system, money laundering and others. [98]

FATF member countries are evaluated in accordance with FATF's recommendations, which are also referred to as "mutual evaluations" (read more about mutual evaluations here).

In June 2019, the FATF published their guidelines on cryptocurrency management. Consequently, two new terms were added: virtual assets (VAs) and virtual asset service providers (VASPs). Their definitions are directly quoted from the FATF publication:

*“**A virtual asset** is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.*

[98] FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Virtual asset service provider *means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:*

i) exchange between virtual assets and fiat currencies;
ii) exchange between one or more forms of virtual assets;
iii) transfer1 of virtual assets;
iv) safekeeping and/or administration of virtual assets or instruments enabling
control over virtual assets; and
v) participation in and provision of financial services related to an issuer's offer
and/or sale of a virtual asset. " . [98]

The essential regulations are recommendation 15 and 16 from the FATF publication, aimed at preventing money laundering, including other unchecked activities while executing anonymous blockchain transactions. FATF member countries are required to implement and apply those regulations used for bank transfers. [98] Thus, these recommendations are called "travel rules." These "travel rules" are VASPs, including crypto exchanges, to exchange information about their customers when crypto-currency transactions are made.

Through this organization, the world will be able to collaborate on the implementation and development of blockchain technology. As a consequence, it is important that countries do not ban cryptocurrencies and the usage of blockchain, but rather associate with FATF and adopt its recommendations on how to use this technology, making it globally acceptable.

As already mentioned, blockchain startup companies relocate based on given regulatory frameworks. In Switzerland, more specifically, the canton of Zug is currently the leading spot where most blockchain startups are taking place. We will look at why Zug, from a regulatory perspective, presents itself as the most valuable place for blockchain startups.

11.2 Zug, Switzerland – A Big Hub or Crypto Startups?

Zug is one of 26 cantons in Switzerland with Zug as its main city with approximately 30000 inhabitants. Zug canton is a low tax region charging only 14% corporation tax. Zug is ranked as having one of the fastest-growing crypto communities worldwide and thus often referred to as the "Crypto Valley." Back in 2014, Zug accepted digital currency as a payment solution, including Bitcoin for payments of small fees. At that time, Zug was actually one of the first cities to accept this alternative mode of payment. It was a clear strategic choice in order to gain and attract other blockchain-focused businesses. [99]

[99] Zug. (2019). ln *Bitcoin Wiki.* Retrieved from https://en.bitcoinwiki.org/wiki/Zug

In addition, the government of Zug is very open for negotiations providing great flexibility, which makes it very beneficial and comfortable for startups. Based on this mindset, Zug has managed to bring together many of today's largest crypto companies. Here some examples: Ethereum foundation, Bitfinex, Cardano Foundation, Bitmain, and many more.

In order to keep track and provide support to established cryptocurrency businesses, the government of Zug decided to found the "Crypto Valley Association." It is an independent, government-supported association, established so as to take full advantage of Switzerland's strengths to build the world's leading ecosystem on blockchain and cryptographic technologies. [100]

The association holds an annual conference, called the "Crypto Valley Conference." This conference is the largest and most popular within the blockchain industry. Here, developers, investors, state representatives, and many other blockchain stakeholders are able to exchange ideas and shape the future of this technology.

11.2.1 Cryptocurrency Regulation in Zug, Switzerland

In Switzerland, a digital asset is considered to be part of digital ownership. Consequently, in an exchange process, digital asset acts as currency, making it exempt from laws governing security regulations. This freedom makes it much easier for digital asset developers and application users.[99]

In Switzerland, digital asset exchanges are covered by AML (Anti Money Laundering) and KYC (Know Your Customer) policy. Exchange-users have to be registered and provide proof of identity. In addition, any exchange platform must be in a self-regulated organization or have an applicable license issued by the Swiss Financial Supervisory Authority (FINMA). [99]

11.2.1.1 What is FINMA?

In Switzerland, FINMA (Swiss Financial market Supervisory Authority) is the independent financial-market regulator. Its mandate is to supervise banks, insurance companies, exchanges, including many other relevant financial institutions. They are responsible for ensuring that the efficiency of the Swiss financial market is maintained. In February 2018, FINMA published regulatory framework guidelines applied to Initial Coin Offerings (ICO). In this guideline, they define three types of existing token based on function. [101]

[100] Our Story. (n.d). Retrieved from Crypto Valley: https://cryptovalley.swiss/about-the-association/
[101] FINMA publishes ICO guidelines. (2018). Retrieved from FINMA: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

Payment token: Similar to digital assets, these are tokens that are made to be used for payment purposes at this time or in the future.

Utility token: Tokens that provide digital access to an application or service on a blockchain infrastructure.

Asset token: Similar to bonds, equities and derivatives in their economic function. Represents a credit right to the issuer.

11.3 Singapore

Over the past few years, there has been an increase in the number of ICO's (initial coin offering) in Singapore. As a consequence, the Monetary Authority of Singapore (MAS) decided that all digital token regulations should be under their governance. In the event that a digital asset is considered to be a "security," then they would be regulated under security laws. [102]

In early 2020, Singapore's Payment Services Act (PSA) released a service called Digital Payment Token (DPT). Under the Anti-money Laundering (AML) and Counter-terrorist-financing (CTF) rules, DPT services cover all crypto businesses and exchanges in Singapore.[103]

In late 2019 and in order to align with FATF, MAS made some changes to PSA regarding digital assets. As before, crypto companies are required to register and apply for a license to operate under Singapore´s jurisdiction.

As already mentioned, the FATF framework, with its recommendations, is highly appreciated by many nations. Thus, many of them start to collaborate with FATF by introducing their guidelines. As the head of the AML group, Malcolm Wright stated that he firmly believes that in the near future MAS will be ready to implement FATF recommendations. [102]

[102] Monetary Authority of Singapore. (2019). A GUIDE TO DIGITAL TOKEN OFFERINGS [PDF FILE]. Retrieved from https://www.mas.gov.sg/-/media/MAS/Sectors/Guidance/Guide-to-Digital-Tokens-Offering---23-Dec-2019.pdf

[103] Allison, I. (2020). Singapore Announces New AML Rules for Crypto Businesses. Retrieved from https://www.coindesk.com/singapore-announces-new-aml-rules-for-crypto-businesses

11.4 China

In early 2013, China's central bank (People's Bank of China (PBOC)) announced that Bitcoin was not a valid circulating currency. Thus, banks and payment institutions were banned from trading Bitcoin or using it as payments for services and sales. Since 2014, PBOC has been speculating whether to accept the use of digital currency. As a consequence, an institution called the Institute of Digital Money was set up by PBOC.
The plan of Yi Gang (governor of PBOC) was not to create a viral currency like Bitcoin or Facebook's Libra but to digitize existing cash (existing monetary basis). Thus, retail banks and fintech companies can handle payments, deposits, etc. as usual, with the new digital currency helping payments to be more efficient.

In September 2017, seven central government regulators (PBOC, Cyberspace Administration of China (CAC), Ministry of Industry and Information Technology (MIIT), State Aministration for Industry and Commerce (SAIC), China Banking Regulatory Commission (CBRC), China Securities Regulatory Commission (CSRC), and China Insurance Regulatory Comission (CIRC)) issued an Announcement on Preventing Financial Risks relating to Fundraising through Token Offerings. The announcement was driven by the need to maintain financial stability through prohibit fundraising activities such as initial coin offerings, which banned initial coin offerings (ICOs) in China. [104]

China wants to be the first country in the world to implement digital currency in its central bank. PBOC has not yet released a launch date, but China is a country already well underway as a cashless society. To pay for goods and services, Chinese residents (especially in metropolitan areas) already use AliPay and WeChat, which link directly to personal bank accounts. Regarding payments and transfers, Chinese are also accustomed to using QR codes, making a switch to digital currency transfers between digital wallets easier.

Even though the PBOC has not revealed the technology behind their digital currency, the term “blockchain” is a well-known and popular term in China. It is to be expected that the PBOC has little interest in "losing" control of database management (transactions, etc.) through blockchain but might prefer to use a "private, permissioned" based blockchain.

[104] Zhang, L. (2017). China: Regulators Ban Companies from Raising Money Through Virtual Currencies. Retrieved from https://www.loc.gov/law/foreign-news/article/china-regulators-ban-companies-from-raising-money-through-virtual-currencies/

11.5 Norway

In 2013 and 2018, the Norwegian Financial Supervisory Authority issued some cryptocurrency warnings, which also included initial coin offerings (ICOs). These warnings originated from ESMA (European Supervisory Authority).[105]

As long as the 2012 Norwegian ethical guidelines are maintained, the Central Bank of Norway does not prohibit the investment, sale, and purchase of digital assets. [106]

According to Norwegian tax authorities, Bitcoins and other cryptocurrencies are treated as capital property. All purchases, investments, wealth, and sales of virtual currencies must be included in a tax return. [107]

In 2015, the European Union Court of Justice decided that cryptocurrencies were to be exempt from value-added-tax (VAT). This led the Finance Department of Norway to address the VAT issue concerning digital assets, which resulted in a 2017 decision exempting digital asset sales from VAT. [108]

[105] Press Release, Finanstilsynet, Finanstilsynet advarer forbrukere om kryptovaluta [Financial Supervisory Authority Warns Users on Cryptocurrencies] (Feb. 28, 2018). Retrieved from https://www.finanstilsynet.no/markedsadvarsler/2018/finanstilsynetadvarer-forbrukere-om-kryptovaluta/

[106] Norges Bank [Central bank of Norway]. Utfyllende Etiske Regler for Ansatte i Norges sentralbankvirksomhet [Additional Ethical Rules for Employees of Norway's Central Bank] (28. Nov 2018). Retrieved from https://www.norges-bank.no/tema/Om-Norges-Bank/samfunnsoppdrag/Lover-regelverk/Utfyllende-etiske-regler/

[107] Skatteetaten [The Norwegian Tax Administration] (2020). Kjøp av virtuell valuta. [Purchase of virtual currency] Retrieved from https://www.skatteetaten.no/person/skatt/hjelp-til-riktig-skatt/aksjer-og-verdipapirer/om/virtuell-valuta/kjop/

[108] Skatteetaten. [The Norwegian Tax Administration] (2020). Tax and VAT relating to Bitcoin and other virtual currencies. Retrieved from https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies/

11.6 USA

11.6.1 Token Taxonomy Act of 2019

For several years, the United States has issued various regulations on blockchain technology, with some variability according to individual states. Still, overall these regulations were seen as being relatively strict. This resulted in Blockchain companies emigrating to countries like Malta and Switzerland, where regulations were more adapted to this new technology.

US congress representatives viewed this as an emerging problem and were dedicated to making appropriate adaptations in order to persuade companies to move to the US as compared to other countries. As a consequence, in 2019, congress representatives come up with a bill called the "Token Taxonomy Act." [109]

The bill is based on previous provisions and is intended to be a fine-tuning of the Securities Act of 1933 and the Securities Exchange Act of 1934.

The bill was based on previous provisions with an added fine-tuning of the 1933 Securities Act and the 1934 Securities Exchange Act. What was special about this new bill was its inclusion of a new term: "digital token." The aim was to create a level playing field for all 50 states by replacing state laws that say something about “digital tokens.” [110]

As stated by Congressman Warren Davidson, the “Token Taxonomy Act” is the key to unlocking blockchain technology in America. This bill was an important step forward, with the US being able to compete against other crypto-friendly international jurisdictions.

11.6.2 US Congress – 32 Crypto and Blockchain Bills

Mostly due to facebook’s project Libra, the interest in blockchain technology and digital assets has significantly expanded. From 2019 until April 2020 US Senators and Members of the House of Representatives have introduced a total of 32 bills regarding blockchain technology and digital assets. [111]

[109] Tiwari, A. (2019). All you Need to Know about the Token Taxonomy Act. Retrieved from https://btcmanager.com/all-you-need-to-know-about-the-token-taxonomy-act/

[110] GPO (Authenticated U.S. Government Information). H.R.2144 - Token Taxonomy Act of 2019. Published April 9, 2019 [PDF FILE]

[111] Brett, J. (2020). Congress Has Now Introduced 32 Crypto And Blockchain Bills. Retrieved from https://www.forbes.com/sites/jasonbrett/2020/04/28/congress-has-introduced-32-crypto-and-blockchain-bills-for-consideration-in-2019-2020/?fbclid=IwAR3dh5z4Q9e8njGWxVeKHrkXphEqNL7bv9wVb-0kg3RFnYgn0haqZ6PwN54

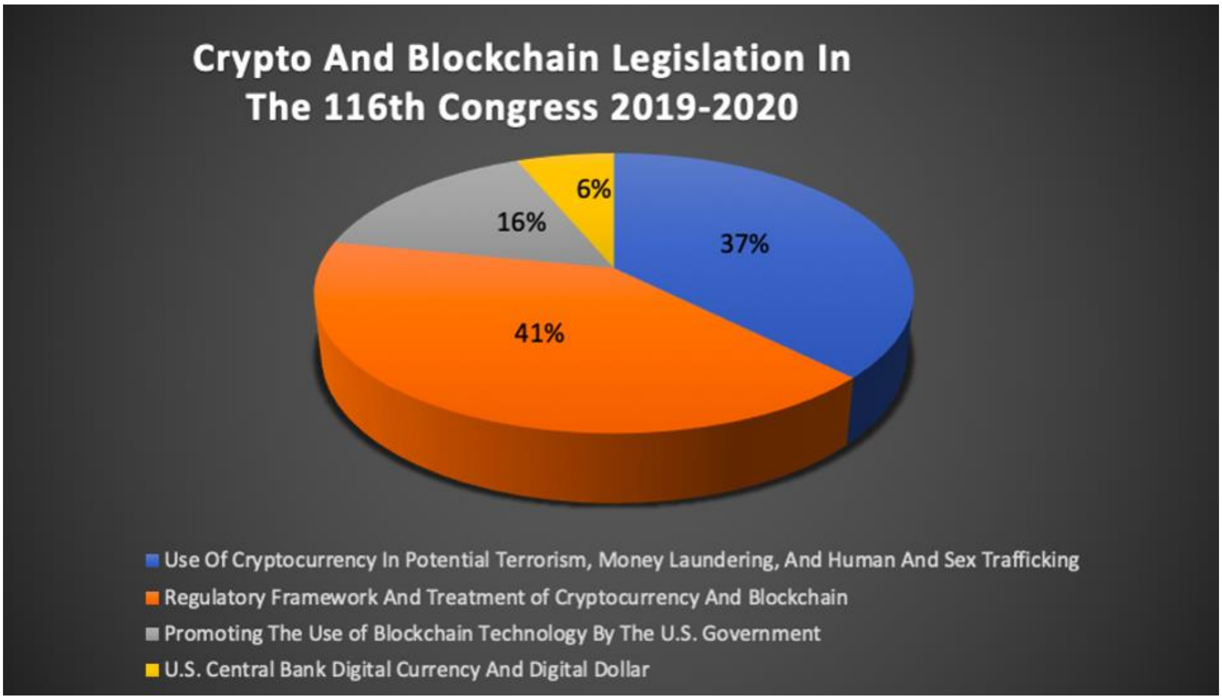


Figure 44. Blockchain Legislation [111]

A total of 13 bills define the regulatory framework and handling of blockchain technology and digital assets. 12 bills address the use of digital assets in the event of terrorism, money laundering, including human sex trafficking. 5 bills address the use of blockchain technology by the US government. [111]

The last two bills introduced the terms ‘Digital Dollar’ and ‘Central Bank Digital Currencies’, with the aim to provide economic stability by focusing on faster delivery of stimulus benefits to Americans due to consequences experienced by the COVID-19 virus. [111]

The COVID-19 virus has actually accelerated the development of the Central Bank Digital Currency initiative, which will be further discussed later in this document. Evidently, the majority of these bills include regulator frameworks regarding the handling of blockchain technology and digital assets. This confirms that lawmakers are increasingly acknowledging the potential and usefulness of blockchain technology and digital assets.

11.7 Conclusion Regulation

Based on an understanding of how different countries start to establish different guidelines aimed at regulating this technology, it makes one realize its rapid increased interest and development. Across borders, countries operate according to different rules and requirements needed to implement blockchain technology. From month to month, significant changes in various guidelines can be observed. Thus, from a regulatory perspective, it is almost impossible to stay current on all ongoing updates and developments.

In summary, we believe that this technology needs and would highly profit from a global regulation. As a consequence, transactions of any value could be transferred around the world both safely and in a matter of seconds. If different countries have different guidelines, it will significantly hamper the innovation of this technology. Besides, companies with high potential will prefer to relocate to countries with less strict requirements able to support their business vision.

We believe that the introduction of project Libra has opened lawmakers' eyes according to this technology. We will see that blockchain and cryptocurrency will grow more prominent around the world, which will affect the legislative volume and hopefully provide more regulatory clarity regarding the blockchain ecosystem.

12 Facebook and Libra

Figure 45. Libra [112]

On the 18th of June 2019, Facebook shocked the world by releasing its whitepaper, which outlines their grand ambitions to bank the unbanked. The Libra association is responsible for this development, and it is headquartered in Switzerland.[115] As expected, their overconfident approach to just release this bombshell, in a sense circumventing central banks around the world by creating their currency, was, therefore, met by increasing regulatory scrutiny. This ultimately led to the co-creator of Libra David Markus testifying before congress on the 16th of July 2019 and explained their intentions and ambitions.[113]

Libra started with titans in the payments industry, backing them like PayPal, Visa, Mastercard, and Stripe; other prominent players include eBay, Spotify, Uber, and Coinbase. The Libra association is composed of these entities acting as validator nodes. Shortly after the massive backlash from regulators around the globe and few countries outright planning to block libra like France, Germany, Italy, Spain, and the Netherlands[114]. The aftermath of all this pushback from governments and banks lead to a few starting partners to jump ship. These include PayPal on the 4th of October and eBay, Mastercard, Visa, and Stripe followed suit on the 11th of October 2019.[115]

[112] Wikipedia (Producer). (2020) Libra. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/4/4b/Libra_logo.svg/2880px-Libra_logo.svg.png

[113] David, M. (2019). HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS. Retrieved from https://www.banking.senate.gov/imo/media/doc/Marcus%20Testimony%207-16-19.pdf?utm_campaign=BitDigest&utm_medium=email&utm_source=Revue+newsletter

[114] Meyer, B. S. (2019). Facebook's Libra faces eurozone backlash. Retrieved from Politico: https://www.politico.eu/article/facebook-libra-faces-eurozone-backlash/

[115] Feiner, L. (2019). Facebook's libra cryptocurrency coalition is falling apart as eBay, Visa, Mastercard and Stripe jump ship. Retrieved from CNBC: https://www.cnbc.com/2019/10/11/ebay-drops-out-of-facebook-libra-cryptocurrency-one-week-after-paypal.html

12.1 Vision

According to Facebook, 1.7 billion people are excluded from financial services around the world.[116] This, in itself, is unacceptable in today's day and age. People around the world can connect to the internet and make use of this vast network of knowledge and information with only a 40$ smartphone. [116] Libra aims to help all these forgotten people to be included in this financial system. Libra wants to enable a single global payment system and connect all these people that are excluded from using our monetary system and joining them using the infrastructure of their system and the internet and leveraging blockchain technology.

12.2 Consensus

Libra has decided to use the Byzantine Fault Tolerant (BFT) consensus(see here). It is thereby providing further evidence that PoW is not a sustainable and long term solution. The security of BFT tolerance primarily depends on the quality of the validator nodes on the network. [116]

12.3 Governance

The libra blockchain and the libra reserves require a governing body that requires a neutral governing body. This is why the Libra association is headquartered in Geneva, Switzerland, which has a great history of being neutral during their existence, and they have a positive stance and regulation of digital assets and blockchains. The Libra association, an independent not-for-profit membership organization, is embodied by the founding partners who want to join the libra project and are partners. Initially, only the founding members will be allowed to run nodes on the network and be the securing governance over Libra. Libra aims to become more permissionless when the network matures and evolves. [116]

The association is governed by the Libra Association Council, which is comprised of one representative per validator node. Together they make decisions about the network and the libra reserves. Each validator node represents a member of the libra association. A member's voter weight in the council is the same as the voting weight described in the consensus protocol. [117]

[116] An Introduction to Libra. (n.d). Retrieved from The Libra Association: https://libra.org/en-US/white-paper/

12.4 Intendent Libra Token

Libra believes the world deserves a global digital currency that combines the attributes of the world's best currencies: stability, wide, universal acceptance, low inflation, and fungibility.[116] The current existing blockchain projects are plagued with extreme volatility. Libra desires to create a stable coin that is backed by a basket of currencies and other low inflation assets. [117] Through these reserves, each Libra coin will be fully supported by a set of stable and liquid assets. These reserve assets are a collection of low-volatility assets, including cash and government securities from stable and reputable central banks.[117] Since Libras value is linked to a basket of currencies, and there might arise a few fluctuations in Libras value, in order to mitigate high volatility, multiple currencies will be include, which is considered most stable. The Libra association manages the reserves.

The Libra association is also responsible for creating new coins and burning coins if they see the need for this. [117] This relationship between the association and the control of issuing currencies is a drawback regarding decentralization. Therefore, one entity is responsible for the creation of money. The technical white paper claims there isn't any worry about inflation or debasing of the currency value since they are only allowed to print more libra coins if there has been an equivalent deposit of amount in the reserves. [117]

The libra token and blockchain is written in the programming language Move, which is an executable byte language used to implement custom transactions and smart contracts. This language was created specifically for the Libra blockchain. [117] The libra token has chosen to use some of the Ethereum features as well. These include the state of the network and smart contracts, and they also make use of Merkle trees.

12.5 Updated April 2020 Libra Token

The above described Libra token was the first approach of Libra, however, due to severe backlash from governments around the world and central banks, Libra decided to abandon their ambitions to create a digital asset-backed by a basket of currencies. The new proposed changes will, therefore, only peg the libra digital asset to a single fiat currency. Thereby complementing various fiat currencies and not competing with various central banks around the world. Libra's main concern was to interfere with monetary sovereignty and monetary policy if the network was allowed to reach a significant scale and usage. Thus libra will create various Libra tokens pegged to fiat currencies, essentially creating stable coins. [117]

[117] The Libra Blockchain. (2019). Retrieved from Libra: https://developers.libra.org/docs/assets/papers/the-libra-blockchain/2019-09-26.pdf

12.6 Our Take and Input

Since Facebook doesn’t have an excellent reputation regarding data privacy, its stablecoin project is quite concerning to many governments around the world and us. However, it isn’t sure Facebook will launch its project with all these big names pulling out and have until now only a whitepaper and not actual blockchain or test version released.

This push from Facebook has had some positive effects on the crypto industry. First of all, the involvement of Facebook in blockchain has given immense legitimization towards the ecosystem. Hence, one of the largest companies on the planet is already getting involved in this space. Furthermore, digital assets have remained mostly unregulated in the majority of countries, leading to increased pressure towards global regulators to take this space seriously and draft legislation accordingly.

Most people do not trust Facebook concerning privacy. Therefore, we speculate that the majority of people on the platform will not trust Facebook to handle their money. However, if Facebook decided to opensource the code base and make this blockchain permissionless and decentralized, there might still be hope for their vision to succeed. Furthermore, we have concluded that this stablecoin is not a Bitcoin or digital asset killer. This is a stablecoin and tied to government back fiat currencies. We have to trust Facebook and the currencies in the basket, which doesn’t eliminate the middleman but makes Facebook the all mighty god of money.

Another significant liability is the censor aspect of Facebook. Most of us are familiar with the blacklisting of the user who posts “hate speech” and disobeys the guidelines, thereby being censored from using the platform. The potential is enormous for Facebook to gain millions, if not billions of users, for their libra currency. What happens when Facebook decides to censor people’s money when they disagree with the person’s views and opinions. This is a scary situation for anybody thinking they are using a decentralized digital asset. It remains to be seen how Facebook will address this issue and how involved they will be in the governance of the network.

This ability of the Libra association to mint new coins might scare the legacy system. Most countries on the globe have a central bank that regulates the monetary policy of their country and dictates the inflow of new currency into the ecosystem. Facebook has 2.5 billion users, which would potentially make them the largest central bank in the world. Furthermore, it would undermine other government's ability to issue currency, and therefore, we conclude that most banks and governments deem Facebook a threat. Taking into consideration that Facebook also owns what’s app and Instagram, which would logically also implement the libra token into its platform after it is successfully trialed and tested. Thus, giving the token immense exposure around the world, which cannot be compared to a single country or entity. This amount of power granted to a cooperation that is known for exploiting users and their data is quite concerning.

As of the new updates(April 2020), we seem to have been correct regarding the concerns of the legacy system and did not allow Libra to exist in its intended environment. Libra has now shifted towards stable coins pegged to a single fiat currency and, therefore, no longer poses a threat to various governments or central banks around the world. [117]

We don't think Libra is a real digital asset but an imposter in order to gain relevance for a company that has lost the trust of most of its userbase. Since digital assets and blockchains are all about trust, this approach of Facebook to create libra is a genius move to regain some of the trust they have lost over the years. If this tactic will work remains to be seen, but we remain skeptical of anything, Facebook says or claims to be true. We all have heard mark Zuckerberg lying to congress and telling them they don't track and misuse our data. Calling early users of Facebook "dumb fucks" for handing over their data isn't a smart move of Zuckerberg. [118] Only the future will confirm how many "dumb fucks" handover their financial data to Facebook as well.

[118] Orlowski, A. (2010). Facebook founder called trusting users dumb f*cks. Retrieved from The Register: https://www.theregister.co.uk/2010/05/14/facebook_trust_dumb/

13 Largest Blockchain Companies

As mentioned above, blockchain technology and digital assets still are in their infancy and are slowly maturing. However, just because this is a new ecosystem doesn’t necessarily mean that companies and businesses aren’t taking advantage of this new digital transformation. Here we will examine the most prominent names and their ambitions.

13.1 Binance/Coinbase

Both these two companies provide digital asset exchanges. They offer a variety of services for customers to sell and buy digital assets. We will present a short history of both companies and their individual business offerings.

13.1.1 Coinbase

Figure 46. Coinbase [119]

Coinbase was founded in June of 2012 by Brian Armstrong and Fred Ehrsam. The company is based in San Francisco, California.[120] They operate two main platforms, Coinbase and Coinbase pro. The first version is very user-friendly and allows customers to buy and sell digital assets easily; the latter is a more professional trading exchange.

Coinbase aims at being the most trusted crypto custody provider for both retail and institutional-grade customers. They also focus on being a very user-friendly platform. In 2019, Coinbase had approximately 1,123 employees worldwide., offering their services in 32 countries. In 2017, the total revenue was over 1 billion dollars.[121] This is an astonishing amount for a company that deals with digital assets. Coinbase is very dominant in the USA. As it is a private company, we are unable to pin down their valuation accurately. According to Forbes's top 10 FinTech US companies, valuation in 2020 was set at 8.1 billion dollars. [122]

[119] Wikipedia (Producer). (2020). Coinbase. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/1/1a/Coinbase.svg/2880px-Coinbase.svg.png

[120] About Coinbase. Retrieved from https://www.coinbase.com/about

[121] Chaparro, F. (2018). Bitcoin exchange Coinbase reportedly made more than $1 billion in revenues last year. Retrieved from https://www.businessinsider.com/coinbase-reportedly-made-more-than-1-billion-in-revenues-last-year-2018-1?r=US&IR=T

[122] Kauflin, J. (2020). The 10 Biggest Fintech Companies In America 2020. Retrieved from https://www.forbes.com/sites/jeffkauflin/2020/02/12/the-10-biggest-fintech-companies-in-america-2020/#289949fa1259

13.1.2 Binance

Figure 47. Binance [123]

Binance was founded in 2017 by Changpeng Zhao and Yi He in China.[124] The exchange is based in Malta, but services are available in most countries around the globe. Binance came up with a smart approach by creating its own token called Binance coin (BNB). This coin has real utility since when using the exchange, it gives certain advantages or use-cases. For example, a use-case converts a tiny amount of a particular digital asset into BNB, which cannot be traded as digital assets have too low a value. Another example of BNB utility is when trading on the Binance platform, trade transaction fees are reduced when using the BNB token.

Even though Binance is relatively new, it has expanded very aggressively and managed in a short amount of time to become one of the largest exchanges. During the time period between launch until 30th September 2019, the company has managed to accumulate an astounding 1 billion dollars in cumulative profits Since Binance is a private company, we were not able to access a reliable source providing an exact company capital account including profit margins.

Binance is a fast-growing company with a global presence in the US, Asia, Europe, and expanding into Africa. This is quite impressive, considering the company is barely three years old.

13.2 Bitmain

Bitmain was founded in 2013 by Jihan Wu and Micree Zhan and is based in Beijing, China. [125] The company's primary business model is mining and selling mining hardware. They are a large distributor of the ASIC miners. Since the company has been involved in Bitcoin and other proof-of-work crypto mining assets from the very beginning, they have quite a monopoly in mining. Currently, they publicly own two of the largest mining pools in existence, Antpool, and BTC.com.

[123] Wikipedia (Producer). (2020). Coinbase. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/1/12/Binance_logo.svg/2880px-Binance_logo.svg.png

[124] Binance Overview. (n.d). Retrieved from Crunchbase: https://www.crunchbase.com/organization/binance#section-overview

[125] Bitmain (2020). ln *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Bitmain

Combined, they alone control approximately 25% of the total hashing power of Bitcoin (see figure 18). This is quite a lot when considering that one single company publicly controls 25% of the network.

By operating in China, they might have additional mining pools that have not been publicly disclosed. Thus, they might have an even more significant stake in Bitcoin.

Figure 48. Bitcoin Mining Rigs. Source: REUTERS/Jemima Kelly/File Photo [126]

Bitmain is a large company in the blockchain industry. In 2018 they had a large pool of employees with as high as 3000 members. However, the decline in the overall crypto price forced Bitmain to lay off almost half of its staff to save costs. [125]

U.S hedge fund Coatue Management and Singapore government-back investment fund EDBI estimated Bitmain to be worth 14 billion dollars. Therefore, to this day, Bitmain remains one of the largest players in the blockchain ecosystem. [127]

[126] Madore, P. H. (Producer). (2019). Bitcoin Mining Giant Bitmain Launches New Chip, Hints at New Miners. Retrieved from https://www.ccn.com/wp-content/uploads/2018/11/bitmain.jpg
[127] Forbes. Bitmain. 2018. Retrieved from. https://www.forbes.com/sites/pamelaambler/2018/08/17/all-you-need-to-know-about-crypto-mining-phemon-bitmain/#4c76f67b580f

13.3 Ripple

Figure 49. Ripple [128]

Ryan Fugger conceived Ripple back in 2004 way before Bitcoin white paper was released. The intent was to create a monetary system that was decentralized and could empower individuals and communities by creating their own currency. [129] Ripple, the company, was founded in 2012 by Chris Larsen and Jed McCaleb and was initially named OpenCoin and rebranded in 2015 to Ripple Labs and later to just Ripple. They specialize in computer software primarily aimed at banks, financial institutions, and other payment companies which wish to send money across borders, instantly, reliably, and for a fraction of a penny. [130]They aim to provide a frictionless experience when submitting money around the globe and want to realize their vision of creating an internet-of-value; more of this in the next chapter.

Ripple currently has 9 offices around the world, among them San Francisco, New York, London, India, Singapore, Sao Paulo, Dubai and beyond. [130] They have more than 350 employees spread around the globe and have over 300 customers. Big names like Santander, MoneyGram, and SBI Remit use their software to enable faster, cheaper and more reliable payments. [130]

David Schwartz, Arthur Britto, and Jed McCaleb were also the creators of the digital asset XRP and OpenCoin at the time were gifted a large amount of XRP (80%) to build upon the network and expand the ecosystem. [129] In a Series C funding round by Tetragon, SBI Holdings, and Route 66, they invested 200 million dollars into Ripple and thereby valuation the company at 10 Billion dollars. It is worth noting that this is ripple stock and not XRP. Ripple also owns a large amount of XRP to this day and use it strategically for funding and partnerships and so forth. It is quite impressive in which monetary situation this company resides in considering it is very young and still considered a start-up.

[128] Wikipedia (Producer). (2020). Ripple. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/8/88/Ripple_logo.svg/2880px-Ripple_logo.svg.png
[129] RippleLabs. (2019). Ln *BitcoinWiki.* Retrieved from https://en.bitcoinwiki.org/wiki/Ripple_(company)
[130] Our Company. (2020). Retrieved from Ripple: https://ripple.com/company

13.4 Conclusion Companies

Even though the blockchain ecosystem is relatively new and hasn’t had time to sufficiently mature compared with other technologies, a lot of money has been invested in these companies. This proves that the market has a great interest in this technology and estimates it to have promising potentials, and should thus be taken seriously. In the next chapter, we will examine whether blockchain could be necessary or an irrelevant business model.

14 Do You Need a Blockchain?

Since this technology is very hyped up and taunted as the solution to every problem regarding databases and storing information. Here we will provide critical analysis of the drawbacks and ask ourselves; do we need a blockchain for this.

Below we have created a flow chart that provides the decision process of adopting a blockchain, and what type of blockchain is most suited for the business model. We have concluded that in most cases, there isn’t a need to incorporate a blockchain. However, the technology does leverage certain advantages, and therefore we have created a flow of questions that determinates the appropriate blockchain recommended.

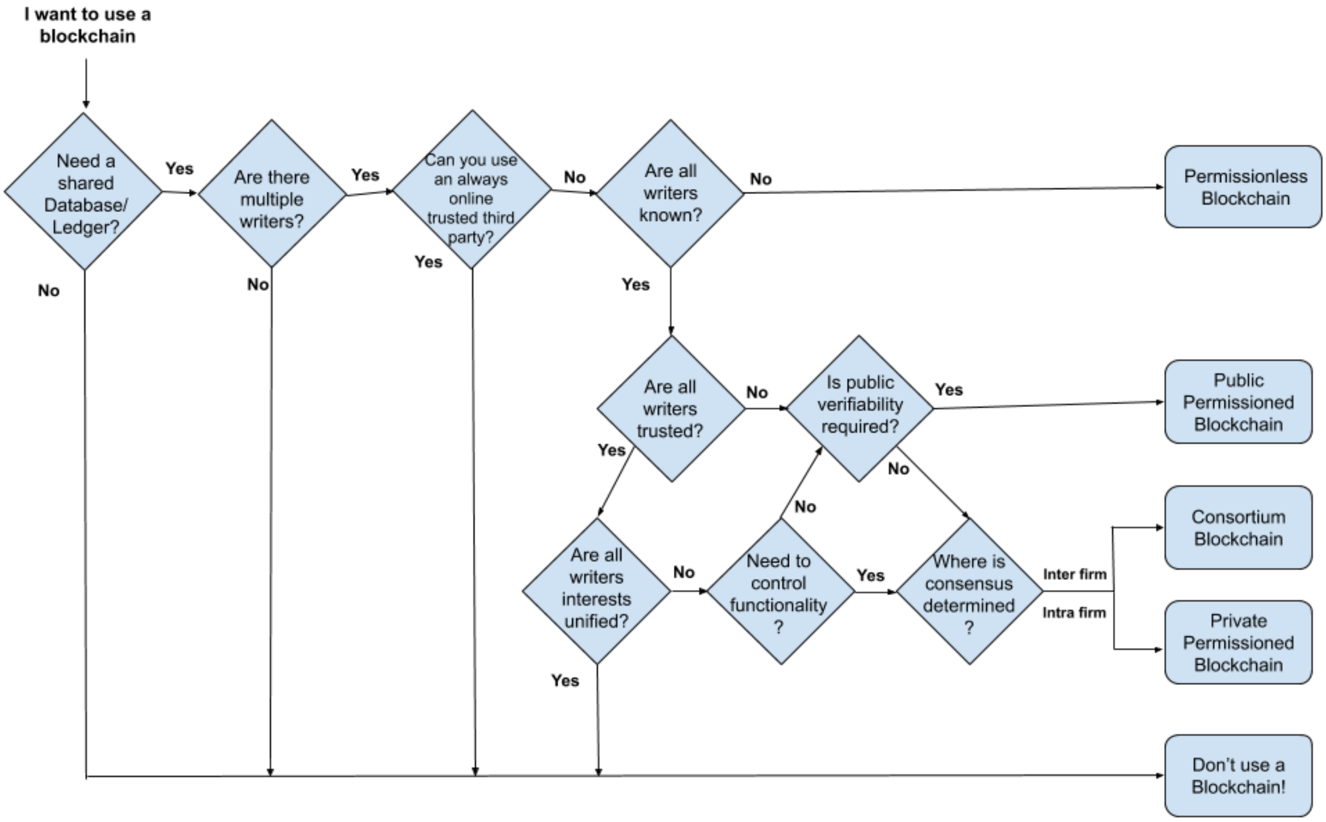

I want to use a blockchain
Need a shared Database/ Ledger?
Yes
No
Are there multiple writers?
Yes
No
Can you use an always online trusted third party?
No
Yes
Are all writers known?
No
Yes
Permissionless Blockchain
Are all writers trusted?
No
Yes
Is public verifiability required?
Yes
No
Public Permissioned Blockchain
Are all writers interests unified?
No
Yes
Need to control functionality ?
No
Yes
Where is consensus determined ?
Inter firm
Intra firm
Consortium Blockchain
Private Permissioned Blockchain
Don’t use a Blockchain!

Figure 50. Flow Chart – Blockchain need

If these terms are unclear read the explanation here again: Permissioned/Permissionless:

14.1 Consortium Blockchain

These blockchains are in the middle of public and private blockchains, combining elements of both. One noticeable difference is that instead of being open source where everyone can see and write to the chain, or private where only one single entity governs consensus rules, a consortium blockchain is governed by a handful of equally-powerful parties functioning as validators of the network.

14.2 Private Blockchain

These blockchains establish rules, dictating who can see and write to the chain. Private blockchains can still be distributed but are not decentralized. Enterprise businesses are the most likely candidates who wish to make use of private blockchains.

14.3 Inter

Inter is a common prefix, which, in our case, is used to describe the consensus determination that *occurs between or among groups* considering adopting blockchain technology.

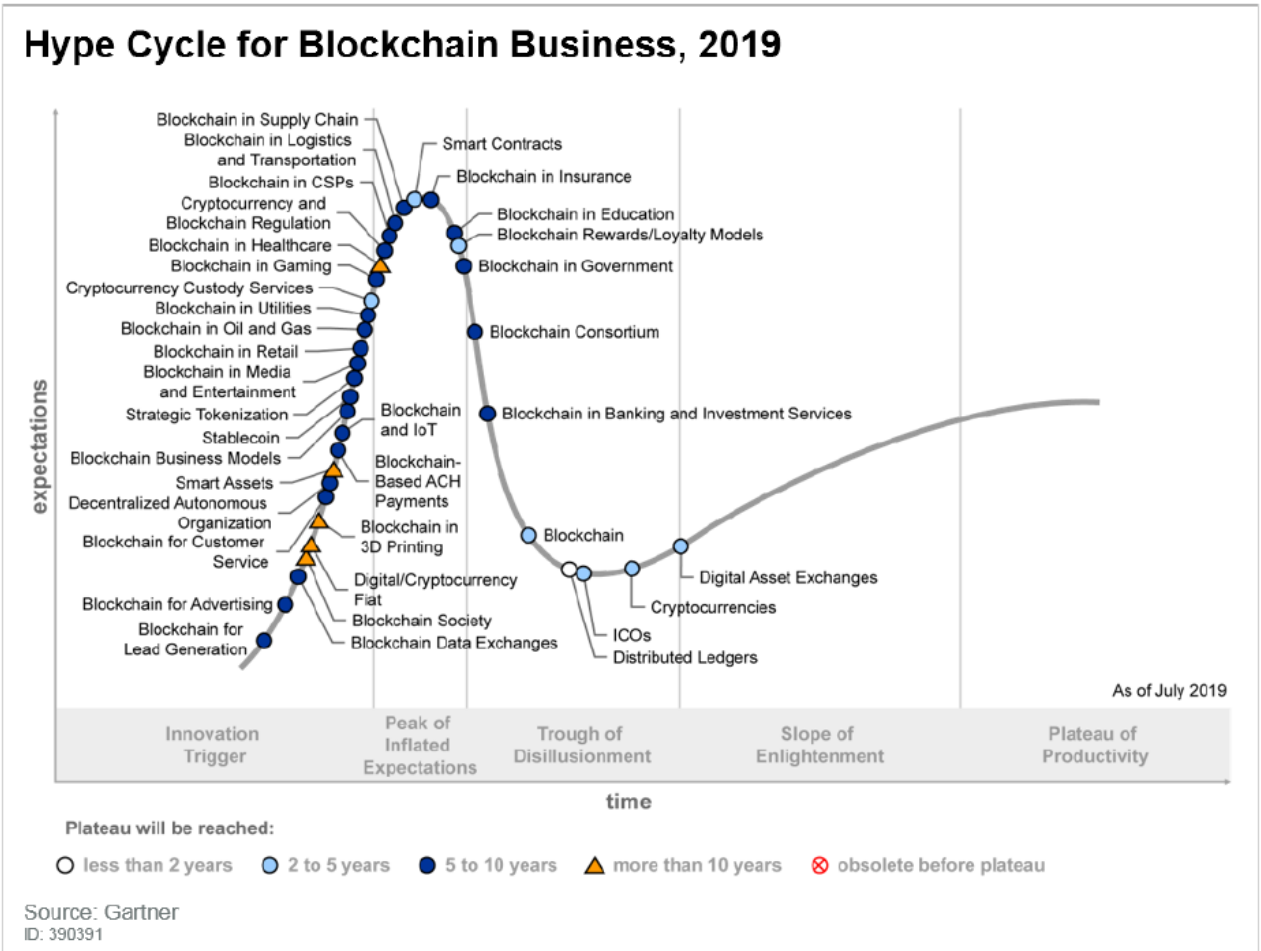
14.4 Intra

Intra is a common prefix, which, in our case, is used to describe the consensus determination that *occurs within or inside* the company or business looking to adopt blockchain technology.

We have now established that a blockchain is not the end-all solution for most use-cases, and we have provided a distinct process to discover the type of blockchain best suited for one's needs. Furthermore, in the real business world, there are cases where an opensource permissionless blockchain is most useful, and we will present a solution in the next chapter.

15 Current Use-Cases

In this section, we will provide an overview of a select few use-cases where blockchain is used in real life and solves real-world problems. There are conflicting results here since there are a lot of ideas and small case usages of blockchain technology. Still, we are interested in medium to extensive scale usage of blockchain technology to solve problems specifically in need of a decentralized solution.
We will examine and give an overview of how the companies or business sectors are using blockchain technology to solve issues.



Source: Gartner
ID: 390391

Figure 51. Hype Cycle Blockchain Business [131]

The above graph provides Gartner´s prediction regarding the current position of blockchain industries, including their future expectation concerning productivity implementation. By studying a few of these industries, we concluded that the most profound impact on blockchain sectors, implementing blockchain solutions, is the financial sector and the supply chain industry. As our document is already quite extensive, we decided to only focus on analyzing the most impacting industry, which is the financial sector.

[131] Gartner (Producer). (2019). Gartner’s Hype Cycle for Blockchain Business. Retrieved from https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/Blockchain-HC-2019.png

15.1 Financial Sector

Arguably the most substantial potential future growth of blockchain technology is in the financial sector, which influences and dictates world economics. Since digital assets potentially represent a form of currency or store of value. Thereby, it is not surprising that until today the largest and most developed use-case resides inside the heart of the monetary system, which is the financial sector.

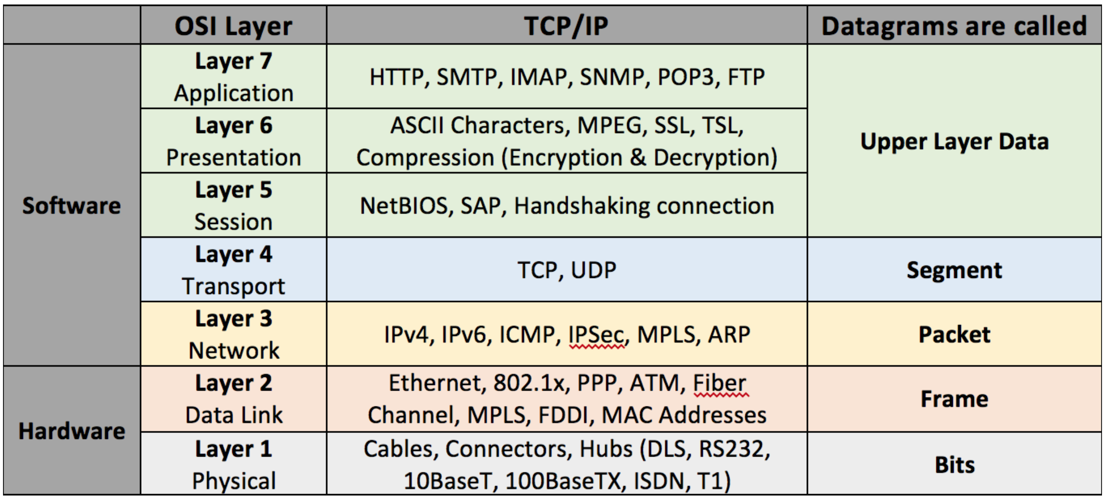
Interestingly enough, even though most blockchain advocates prefer the notion of distributing or circumventing the current monetary system and replacing all intermediaries in the effected ecosystems, one company has chosen to approach this a little differently, and they are Ripple.

Ripple does not only leverage the advantages of blockchain technology; however, they make use of a digital asset XRP. We will analyze their use-case and implications below.

15.1.1 Ripple & Internet-of-Value

We previously described the relationship between Ripple and XRP. Here we outline the internet-of-value concept and how Ripple contributes to this vision. As many of us depend on readily available internet infrastructure, most of us are familiar with its information system. But what is actually the internet, and how does the internet-of-value come into play? The next chapter gives an overview of how the internet is set up and how it correlates with the internet-of-value. Using XRP as a digital asset example, we will look at its implementation and use-case.

15.1.1.1 Internet-of-Value



	OSI Layer	TCP/IP	Datagrams are called
Software	**Layer 7** Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	**Upper Layer Data**
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	**Segment**
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	**Packet**
Hardware	**Layer 2** Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	**Frame**
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	**Bits**

Figure 52. OSI Model [132]

[132] Hameda, A. (Producer). (2017). OSI Model. Retrieved from https://abdulazizhameda.files.wordpress.com/2017/02/osi-model-table.png?w=1166

The figure shows the Open Systems Interconnection model (OSI model). This model aims at standardizing the communication aspects of a computing system or telecommunication. As shown in the figure, interoperability is essential in this process, which is achieved by implementing standardized communication protocols.[133] We can divide the OSI model into seven parts:

OSI Layer	Description
Layer 7 **Application**	The Application layer ensures the supplement of network services to the end-user applications. Network services are typical protocols that work with user data.
Layer 6 **Presentation**	The presentation layer is responsible for syntax processing of message data such as format conversions and encryption/decryption, if necessary, by the application layer.
Layer 5 **Session**	The Session layer manages the sequence and the flow of events that initiate and tear down network connections.
Layer 4 **Transport**	The Transport layer ensures the delivery of data across network connections.
Layer 3 **Network**	The network layer is responsible for packet forwarding, including routing through intermediate routers.
Layer 2 **Data Link**	Once obtaining the data from the physical layer, the data layer is responsible for checking physical transmission errors and packages bits into data "frames."
Layer 1 **Physical**	This part is responsible for the transmission of digital data (bits) from the physical layer of the sending device over a specific protocol to the receiving device. It is usually transmitted using electric voltages, radio frequencies, etc.

[133] Bora, G., Bora, S., Singh, S., & Arsalan, S. M. (2014). OSI reference model: An overview. *International Journal of Computer Trends and Technology (IJCTT)*, *7*(4), 214-218.

This internet represents the flow of data or information across the globe. To put it slightly, the internet is a bunch of agreed-upon protocols and rules, which one can share and move data. Now that a high-level overview of how the internet is set up and operates has been provided, the relevance of an internet-of-value emerges. Here its “value” represents the flow of currency. However, money does not move with the same ease, as seen with the above-standardized protocols. This is where the crucial importance and requirement for an internet-of-value and Ripple comes into play.

Ripple aims to create a global internet of value, where money moves with the ease and efficiency that information spreads across the globe using the internet. To facilitate the reality of these notions, Ripple created the Interledger protocol. [134] This protocol provides for a standard of transfer between ledgers, thereby creating a new standard for interoperability between ledgers. The transfer value can be anything from commodity or cryptocurrency, including any other type of asset. The next challenge is how to most efficiently and safely transmit these values between two parties. Essential virtues being speed, reliability, cost, and scalability. Ripple strongly believes that XRP is perfectly designed to carry these responsibilities as well as able to fulfill these requirements. The proposed combo of interledger protocol and XRP is thus a very effective solution towards realizing the internet-of-value.

With these ideas, Ripple has grand ambitions that will take time to realize and will not happen overnight. The implementation of these goals is a gradual process with many hurdles and challenges along the way. Next, we will evaluate how Ripple is already providing real utility in remittance services around the globe.

15.1.1.2 XRP and On-demand liquidity(ODL)

Domestic payments have a strong foundation in most countries already and happen near instantly. However, one significant friction point still exists in international transfers. Especially remittances of people working overseas and need to send money home to help support families and friends.

[134] Thomas, S., & Scwartz, E. A Protocol for Interledger Payments. Retrieved from https://interledger.org/interledger.pdf

15.1.2 Legacy Financial System

Swift (Society for Worldwide Interbank Financial Telecommunication) provides a messaging network that enables financial institutions worldwide to send and receive transaction information in a secure, standardized, and reliable environment. This Company was founded in 1973. [135]
They provide services with 200+ countries and have 11’000+ partner institutions that are connected to the SWIFT network. No doubt they are a behemoth in this industry and have been around a very long time. With their standard for moving both domestic and international money around in the world, SWIFT currently holds the largest market share. [136] [135]

SWIFT itself does not facilitate the transferring of funds between banks but sends money based on payment orders that are settled between accounts of respective institutions implementing the transfer. [135]

To understand the process needed to move money across borders, the relationship between Nostro and Vostro bank accounts must be understood. When used, these terms actually address and represent the same type of account. For accounting purposes and applied bank transactions, the one bank A will thus name the account “Nostro” while in the other Bank B will give it the name “Vostro.”

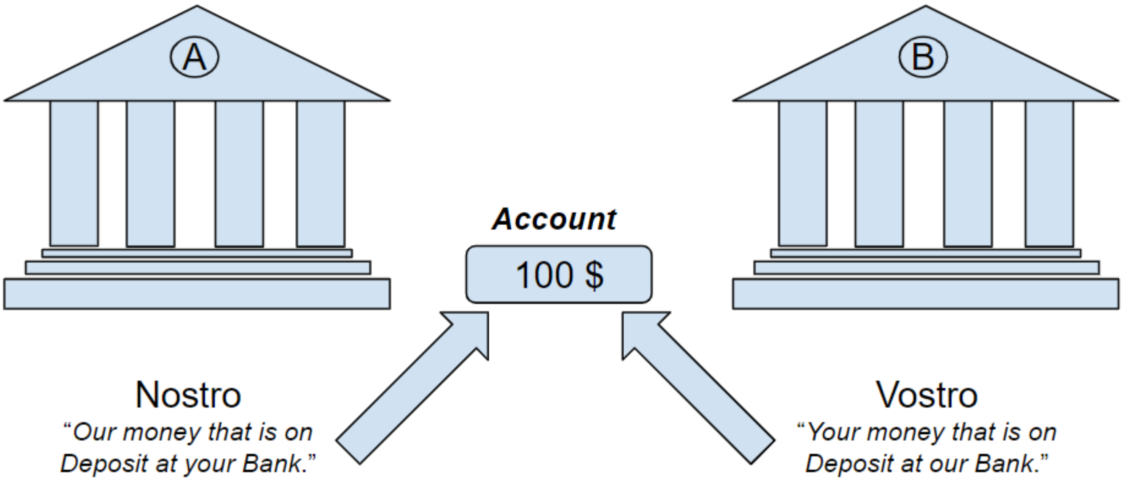

A
B
Account
100 $
Nostro
“Our money that is on Deposit at your Bank.”
Vostro
“Your money that is on Deposit at our Bank.”

Figure 53. Nostro/Vostro in Banking

[135] Swift. (2020). ln *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication
[136] Messaging and Standars. Retrieved from Swift: https://www.swift.com/about-us/discover-swift/messaging-standards

15.1.2.1 Nostro (our)

A “Nostro” account is a reference used by bank A to make reference to an “our account” of which the counterpart account is held by bank B. This means that the money held by bank B holds money on behalf of bank A. Establishing these types of accounts are standard procedures used in international banking relationships.
These accounts are designed to simplify the process of settling Fiat currencies and foreign trade transactions. Nostro accounts are different from standard deposit bank accounts, in that financial institutions usually hold them, and they are denominated in corresponding foreign currencies. [137]

15.1.2.2 Vostro (yours)

A Vostro account is a reference made by bank B to make reference to “their account,” where bank A has deposited money in an account of bank B. Thus, the Vostro account is a record of money owed or maintained by an external third party. Apart from banks, these types of accounts can also be held by companies or individuals. [137]

For example, if a Norwegian business company wants to conduct business in Switzerland, a Nostro account would be opened in Norway with a corresponding Vostro account in a compliant Swiss bank. The Vostro account would be denominated in Swiss Francs (CHF).

15.1.2.3 Conclusion Nostro Vostro

These terms are used to describe a given bank account, which is simultaneously managed by two separate banks, usually in an international setting. One bank owns the money (Nostro account) while the other bank only holds the money from the owner bank (Vostro account). Both banks keep ongoing records of the amount of money being stored on behalf of the other bank.

Even with this type of account set-up, an international transaction or payment still requires between 2-5 business days (weekends excluded).[138] [139] As a consequence, the ability of rapidly sending money to family members will again take an aggravating amount of time. In addition, transactions carry the burden of additional costs, and family members at the receiving side must hold a personal bank account. For individuals living in some non-industrialized countries, this can be quite an impossible task.

[137] Maverick, J. B. (2019). Nostro Account vs. Vostro Account: What's the Difference? Retrieved from https://www.investopedia.com/ask/answers/051815/what-difference-between-nostro-and-vostro-account.asp
[138] HSBC. (2020). International Payments. Retrieved from https://www.hsbc.co.uk/international/money-transfer/
[139] Barclays. What are the timescales for sending international payments? Retrieved from https://ask.barclayswealth.com/help/ukprivatebank/wealth-online/payments/payment-timescales

Western Union is another company that allows for worldwide money transfers. Transactions with this company have several drawbacks. For one, their transaction fees are quite high as they charge outrageous amounts of fees depending on the country of delivery.[140] [141] Some transactions have to go through the US dollar prior to being converted to the local currency, adding additional exchange costs (for example, the South African Rand). Based on personal experience and illegal activities, banks in the receiving country do not pay out the original amount of money that was sent (Banks in Mali and Ivory Coast).

As we established, international payments are quite expensive and slow when comparing them to the movement of data across the internet. Furthermore, in the corresponding banking system, each bank will charge some fees to move money across its network. It is leading to an increase in friction in the system and more costs.

15.1.3 The On-Demand liquidity(ODL) Approach

Here an example. As a business located in the US, they would want to send funds to their business partner in Mexico. The traditional way of doing this would be to create a Nostro/Vostro account. The US business partner can now deposit a certain amount of funds in the corresponding Mexican Vostro account (in local currency) while retaining ongoing access to the account´s balance history (debit & credits). Within this setting, a risk exists for the foreign exchange rate to decline. In the event that the fiat currency loses value, the Vostro account will decrease in value compared to the domestic currency that was initially deposited. It is crucial to understand the Nostro/Vostro architecture type in order to move forward.

Ripple envisions a world where money moves just as fast and cheap as information currently travels through the internet. In order to realize the idea of an internet-of-value, Ripple will build partnerships with banks and payment providers all around the world. On-Demand liquidity (ODL) is a Ripple product, enabling customers to gain access to markets previously untapped and excluded from the Nostro & Vostro relationship account. We will now describe how on-demand liquidity works and how it affects the relationship between banks.

[140] TransferWise. (2018). Western Union money transfer fees: A full overview. Retrieved from https://transferwise.com/us/blog/western-union-fees

[141] WesternUnion. (Producer) Fee Table. Retrieved from https://www.westernunion.com/content/dam/wu/EU/EN/feeTableRetailEN-ES.PDF

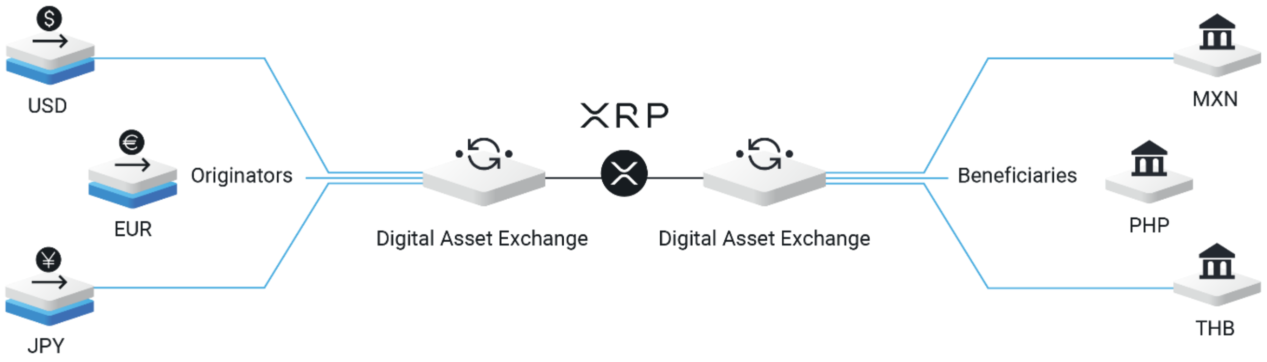


Figure 54. On-demand Liquidity [142]

15.1.3.1 This New Approach Would be Conducted as Follows

As a US bank and Ripple partner, I would want to send funds 100$ (USD) to my business partner and Ripple partner in Mexico. Two crucial components are that there needs to be two regulated digital exchanges present, one in the US and the other in Mexico. Furthermore, I would now purchase XRP on the US exchange and get a certain amount of XRP; for this experiment, we will peg 1 XRP to 1 $. So, I would purchase 100 XRP and send those 100 XRP to the ripple partnered Mexican exchange. This process is very fast around 3 seconds, transparent since it travels over the open XRP ledger, and it would be very cheap at fractions of a penny. Now that I have my XRP deposited on the Mexican exchange, the exchange will sell those XRP for their local fiat currency, which is the Mexican peso (MXN) in this situation.

Thereupon the funds will be transferred to the desired destination account. This whole process is predetermined, which means that the sender and the receiver of the transaction would know the exact transfer time and fees included in the transaction before it is executed.

Notice how the On-Demand Liquidity (ODL) approach operates differently from Nostro/Vostro accounts. With ODL, there is no need for pre-holding currency funds in a destination account. As a consequence, the risk with respect to local currency fluctuations carrying inflationary risks can be excluded. Thus, businesses can expand more rapidly and with less risk into new emerging markets. They will have one less worry when moving their money and investments around the world.

Even though an ODL system sounds very promising, there are still many hurdles that need to be resolved, primarily applicable regulations. Banks will not hold on their books any digital assets or perform transactions without clear rules and regulations.

[142] Ripple (Producer). (2020). On-demand liquidity. Retrieved from https://ripple.com/wp-content/uploads/2019/09/XRP-Graphic.png

Thus, the importance and use of an ODL solution will grow as applicable laws will gradually be defined and set in stone. Nonetheless, there are individual customers in specific corridors (country “railroads”) that already use the ODL feature to help save cost, while offering a superior user experience for their customers.

15.1.4 RippleNet

RippleNet was born out of a vision to realize the prospect of an internet-of-value. Customer demands are changing, and current infrastructures do not provide for acceptable low-cost means for cross border payments. Customers increasingly demand easy, safe, and best price transactions to be executed in real-time. However, today's cross border payments fall short of these expectations. The situation can mostly be blamed on today's infrastructure with its centralized networks and its legacy technology with different payment rails.

As a decentralized network, RippleNet wants to address these frictions. The vision ist to enable a frictionless global payment experience by combining diverse payment players into one ecosystem.

Ripplenet recognizes two types of network participants, namely network user and network members.

15.1.4.1 Network Users

- Corporates
- Small and medium-sized enterprises (SMEs)
- Small banks
- Payment providers who only send payments

To access the RippleNet network, users are benefited with a standardized Application Programming Interfaces (API). As a result, the user gains on-demand global access across the network in real-time, thereby gaining end-to-end visibility regarding his or her payment status.

15.1.4.2 Network Members

Network members are banks and payment providers. As they process payments and are considered main liquidity sources, they serve as the foundation of the network. Payments are processed through:

- A real-time settlement with a bidirectional messaging system.
- Pre-validation of transactions.
- Rich data attachements for every payment.
- Payment certainty by pre-disclosue of information prior to any transaction.

In addition, network members can source liquidity through ODL, as described above.

15.1.4.3 Conclusion RippleNet

RippleNet is solving the inefficiency of today's global network by creating consistency across the network through standardizing governance, applicable rules, its technology, and API. RippleNet ensures real-time fund settlements and bidirectional messaging. Funds moved across the network are guaranteed and low cost. The creation of RippleNet is the first step towards realizing an internet-of-value. We strongly believe that this network effect will thrive as more banks and payment providers become convinced of its advantages and join RippleNet.

15.1.5 MoneyGram & Real Use-Case For Digital Assets

One large customer who uses ripple's blockchain solution and the digital asset XRP is MoneyGram. They are an American company money transfer company based in Dallas, Texas.[143] In 2014, MoneyGram was the second largest provider of money transfers in the world. The company engages in 200 countries around the world. [143]
They are the most significant customer who uses the ODL feature is Moneygram. CEO of MoneyGram Alex Homes has said in an interview conference at Swell November 2019, that they in 4 months have scaled up to 10% of their Mexican peso corridor to use XRP and plan to expand into three more corridors. [144] XRP is used to facilitate foreign exchange trading. Furthermore, in MoneyGram's 10-k filing with the security and exchange commission, they labeled the income generate by XRP as an indefinite-lived intangible asset. This illustrates the usage of blockchain and the digital asset XRP, and it is a remarkable accomplishment in the financial sector.

15.1.6 Conclusion Financial Sector

The way XRP use-case facilitates secure, fast, and reliable international payments will only accelerate its importance as the world market continues to expand. A business will continue to offer and exchange global products, which requires the ability for people to send money across the globe. Consequently, we believe that the demand for low-cost and real-time transactions will only continue to increase. We have observed companies leveraging XRP and ODL so as to expand into new international territories without having to pre-fund accounts and end up with capitals being tied up in partnership countries, exposing them to the risk of currency fluctuation.

[143] Dallasnews. (2010). MoneyGram chooses downtown Dallas for new headquarters. Retrieved from https://www.dallasnews.com/news/2010/09/24/moneygram-chooses-downtown-dallas-for-new-headquarters/
[144] *MoneyGram and Ripple discuss XRP*. (2019). Paper presented at the Swell Conference. https://www.youtube.com/watch?v=yrezhEfUt4E

Businesses will thrive under the provision of the best services. We believe that Ripple can present businesses with an improved and superior financial setting than the legacy system currently is able to provide. In contrast to alternative networks, Ripple has no intent to circumvent the current financial system but aims to work with banks and governments to create ameliorated alternatives on how to move money. We foresee that the internet-of-value will go through giant leaps regarding overall business transactions and global commerce. We look forward to witnessing its development, as events unfold once the financial system operates autonomously and reliably without friction. Finally, money can move across the internet as quickly and cheaply as any information.

16 Future Use-Cases

Future use-cases are essential components for the development of blockchain technology. We may not be able to predict how future systems or applications will evolve, but we can speculate about what sectors most likely will profit from this technology and where we believe this technology has enormous potential.

Blockchain technology is still in its infancy, prediction regarding its potential will thus mainly be based on speculations. As those who experienced the start-up phase of the internet, only a negligible percentage was probably able to envision actual future use-cases, the importance of its worldwide expansion, including how it was going to affect all our lives.

Characteristic features of blockchain technology are transparency, traceability, security, immutability, censorship-resistance, decentralized governance, and automation. Such innovative technology could be instrumental within many different types of sectors. Below we present various industries as future use-cases of blockchain technology.

16.1 Financial Sector

Through the use of a centralized corporate database and lack of financial interoperability, blockchain has the potential to change current trading, settlement, and managerial activities. We have already discussed current use-cases in the financial sector, and we believe that blockchain technology will have the most significant impact in this sector.

Banking and financial services often struggle with slow payments, security problems, and limited transparency. Thanks to blockchain technology, these limitations can be addressed by implementing transparent management systems, more efficient business models, higher liquidity, lower cost, and faster-executed transactions.

We strongly believe that the way Ripple expects to tackle current limitations through the development of improved technology will significantly assist the financial sector in enhancing its existing system.

16.1.1 Banking The Unbanked

Due to multiple layers of intermediation, the existing banking system is often both complex and slow. Blockchain provides secure means for sending digital assets without the involvement of additional third parties deducting fees and slowing down the payment process.

In this respect, a very important limiting factor one must consider is that an estimated 1.7 billion individuals in the world are unbanked. This means that these people do not have- or will not be able to acquire a checking or savings account. [116] [145]

Even though unbanked individuals do not possess a bank account, it is estimated that two-thirds of them own a mobile phone, which would enable them access to various financial services.[145] Currently, unbanked people are unable to participate in the global economy and are excluded from services we in most industrialized countries take for granted. With the opportunity of blockchain and digital assets, we believe that unbanked people can be included in the global financial system. Mobile wallets can store digital assets or stable coins, enabling users to transact services. Anyone with a device connected to the internet can create multiple wallets to store personal income, either by government-backed fiat currencies or public permissionless digital assets. An additional aspect and potential advantages are that in some countries, people do not trust their government-controlled banks. Instead, they prefer to store personal value in non-governmental digital assets.

Whether unbanked individuals choose an independent or government-backed currency is irrelevant. The critical issue here is that unbanked people can store wealth and have the opportunity to interact and contribute to the local as well as a global economy. Gross Domestic Product (GDP) is measured based on the amount of purchased local goods and services. In some countries, financially poor individuals are not included in this equation, which might grossly underestimate the true potential of their financial contribution. By including these “outsiders” in the local and global financial system would significantly improve the GDP of these countries.

16.2 Healthcare Sector

Currently, no satisfactory or secure solutions exist for sharing information between different interest groups in the healthcare system, such as healthcare personnel, pharma companies, patient advocates, and researchers. Health-related data is considered sensitive data that is strictly regulated by applicable data protection laws (GDPR is applicable in the EU). Information usually shared between health sectors include details regarding patient health history, diagnostic tools and processes, medical interventions, and treatment outcome.

Better collaboration between healthcare providers and applicable interest groups can only improve potential treatment options and disease outcomes. Finally, the importance of ensuring a cost-effective healthcare system cannot be ignored.

[145] TheWorldBank. (2018). Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows [Press release]. Retrieved from https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows

The current COVID-19 epidemic emphasizes the need for a decentralized open-source database, where medical professionals and policymakers share and have access to global statistics and information required for decision making. A decentralized open-source database would allow afflicted countries to enter required data regarding the effectiveness of policy implementations and treatment outcomes, including the ongoing development of the epidemic. Granting all respective players contribute relevant data promptly would significantly improve the management of an epidemic both by combating the disease as well as keeping the death toll as low as possible. Such global data-sharing initiatives would not only be restricted to pandemics but could also support important international research activities in the health sector.

A substantial hurdle that must be taken into consideration when sharing health-related data is the anonymity and protection of patient information. The European Union released a new General Data Protection Regulation (GDPR) law, which came into effect in May 2018. Under this law, health-related data is considered sensitive data and, therefore, especially protected against unlawful access and distribution. The law also states that any personal health-related data can only be shared with other researchers or interest groups if the patient has given his or her written approval. How relevant this law is can be recognized when, according to data from the Protenus Breach Barometer, around 1.13 million patient records were compromised in 110 healthcare data breaches in the first quarter of 2018. [146]

The healthcare sector has traditionally followed the technology, rather than led it. Blockchain technology can be crucial to creating a decentralized system that keeps electronic health records safe. The aim must be to adhere to GDPR standardElectronic health records on blockchain will maintain the interoperability of sharing data between different interest groups. This requires that for health information to be standardizing, making data transfer, and sharing more accessible and more efficient. In addition, blockchain will be able to include patients in their decision regarding which data should be shared or rejected and which data must be changed or corrected.

Daily, large amounts of data are collected in the health sector. Thus, data storage requirements are expected to be very large. A centralized database would be considered very vulnerable. In addition, many countries will not accept either by law or due to safety and managerial concerns that patient data are stored outside their country. Consequently, health organizations have used hybrid storage systems to handle storage requirements. Here we see massive potential for blockchain technology to improve and increase the cost-effectiveness of today's data storage system.

[146] Donovan, F. (2018). 1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018. Retrieved from https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018

16.3 Tokenization of Everything

Tokenization is the process of converting on a blockchain the right of an asset into a digital token. At first glance, this step might seem unnecessary. However, when diving further into the use-case and the reasoning behind it will reveal an intriguing opportunity for investors, including middle to lower-income households. The argument behind it is that with the presence of more worldly assets being tokenized, thus entering the digital arena, will have an increase of assets being more liquid and readily available.

For example, Alice has 1000 dollars to invest in either real estate or high-end art. Based on today’s market, she will have great difficulties gaining access to these specialized and often closed retailers. On the other hand, once a painting or real estate becomes tokenized, new opportunities open up to Alice. The process would be as follows. An art-house decides to tokenize one of their Picasso paintings. The painting´s worth is estimated to be 1 million US dollars. As the painting is tokenized, 1 million tokens are generated (= 1 million US dollars), with 1 dollar representing a 0.0001 % stake on the Picasso picture. Alice can now store her wealth into a high-end art piece she deems worthy of her investment, and that she believes will over time generate returns. By investing 1000 dollars in the Picasso picture, she could claim a 0.001% drawing ownership.

The process of asset tokenization can be expanded to include many different asset classes. This will give individuals with average earnings a chance to invest in products usually reserved for wealthy households or institutional investors. In addition to being labeled as security tokens, on-chain tokens produce an immutable record of ownership. In many ways, these tokens resemble traditional securities (like stocks) digitally traded in today's market. By removing mediators and embedding both executions and legalities into smart contract code, will augment tokens ease of divisibility and lower cost of global ownership transfers.

We believe that in the future, many assets will be tokenized. Hence, many new markets will emerge that were previously inaccessible due to illiquidity and the condition of under-utilized markets. Unfortunately, currently, many hurdles put constraints on the implementation of this idea, legal frameworks, and ownership exchange rights being the main adversaries.

16.4 Social Media Sector

In today’s society, social media is one of the most popular internet platforms, used by most people who have access to the internet through telephone, computer, or some other electronic device. Worldwide platforms being used on a daily basis by a large number of people end up collecting a colossal amount of data. The collected information includes everything from personalized data to what the individual does on the platform and even to some contexts what one does outside the platform. All this data is stored in centralized databases.

Most social media platforms have business models that offer users various services free of charge. As a trade-off for these services, platforms sell website advertising space to companies or individual businesses, which are uploaded for users to see and for companies to get additional visibility.

We believe that in the future, social media platforms will be developed based on blockchain technology. This is because users want to retain control of their own data. Data stored and handled by a third party will, by many users, always be viewed as a risk. Based on lengthy and strict data protection laws and guidelines, personal data has become increasingly protected against fraudulent use. Still, for many users, third-party data handling will always remain a matter of concern and will never be an ideal solution.

Thanks to blockchain-based social media platforms, users will retain control over their data. As a consequence, the user alone can decide whether to share, change, or delete their data. In addition, the user will be rewarded for sharing his or her personal data and not a given third party data holder

16.5 Supply Chain Sector

Traditionally there is a lot of communication and planning involved in Supply Chain Management (SCM). The future demand for any given product is estimated based on its past and current demand. Relevant information on product demand is continuously forwarded to shareholders in the hope that they will respond appropriately to ongoing fluctuations in the market.

16.5.1 IBM and Food Trust

The core value proposition is trust here; the customer wants to trust that the purchased item originates from a reliable source that does not use slave labor or child labor to produce these products. Moreover, the product is safe to consume and is not artificially inflated with chemicals. Trust is the core here, and what better way to facilitate trust than to put this food supply chain onto an immutable, transparent, and public ledger where anyone can verify the origins of the products. This is where the blockchain solution comes into play. IBM has created a platform for this lack of accountability in the food industry. [147]

With regard to any Supply Chain Management (SCM), a core-value-proposition is trust. In other words, the customer expects that purchased items originate from a reliable source. For example, the consumer trusts that no child labor, toxic, or contaminated substances are used to produce a product. In the case of foods, the customer trusts that purchased food items are safe for consumption and void of unwanted artificial or harmful chemicals. Still, apart from trust offered by consumers, they are not able to actually verify the truth of these claims.

[147] IMB. (2019) IBM Food Trust. Retrieved from https://www.ibm.com/blockchain/solutions/food-trust

A better way would be to have one´s trust confirmed, such as having the SCM loaded onto an immutable, transparent, and public ledger, where anyone can verify the origin and sound condition of a product. This is where the blockchain solution comes into play. IBM has already developed such a platform for the food industry. [147]

The IBM solution provides authorized users access to their food supply chain. Accessible data encompasses applicable food production by various farms and its distribution to various retail stores. As an option, authorized users can add themselves to the food chain statistics by documenting ongoing product consumption. A complete history regarding the location of selected food items along with applicable detailed information (e.g. production certifications, quality test results, transport temperatures) is available in seconds. IMB has decided to build the food-trust-platform on top of the Hyperledger Fabric, which is a permissioned blockchain. Depending on access level granted, selective data from the supply chain can be exported by the user, who can display the data according to use. [147]

We believe that blockchain supply-chain-solutions are inevitable and will be incorporated into existing market infrastructure. Benefits offered by blockchain technology are essential in order for these industries to increase trust in their products. The ability to maintain good health with increasing age is an ambition shared by all human beings. Thus, ensuring a healthy lifestyle and knowing what these requirements entail, has given rise to one of the most successful businesses of today. People want to know the origin of their foods, under what conditions they were manufactured (people and animals), how they were handled, packaged, transported to the retailer, and finally, its expected shelf life. Blockchain solutions can significantly contribute to making all this information readily available to all potential stakeholders. This favorable setting, based on mutual trust, will result in improved collaboration between food providers and their consumers.

Even though we used the food supply chain as an example, blockchain solutions can also be used in other settings, where the need to exchange information in a supply chain is crucial in order to guarantee the ongoing success of a given entity.

16.6 Charities

Charities are nonprofits organizations that support free of charge individuals, groups of people, or organizations in need of support. The aim of a charity is usually very clearly defined, but they can differ both in terms of size, the target group they want to support (e.g. people, animals, nature), and the geographical areas they cover (national versus international charities). The main features they all have in common are that they are on the constant lookout for donors willing to financially support their charity work while ensuring their finances are managed in such a way as not to end up in any debts.

Charities use their accumulated funds to help people, animals, or situations in need. Unfortunately, charities have also been found to be corrupt. Money is not only invested based on charity by laws but fraudulently used to enrich members of their charity personally.

A problem of financial systems used by charities and many other similar organizations is that they operate on closed systems. The ability of donors to track- and monitor how charities invest their financial contributions are almost nonexistent. Consequently, financial charity supporters have almost no means to verify whether their money was honestly spent. This uncertainty can be mitigated through blockchain charity solutions. Based on this solution, charity management and their financial contributors can create network wallets. These wallets record all individually invested funds, including any executed transactions. Thus, a traceable and immutable financial history is built on blockchain charities.

Blockchain technology can provide for full-scale transparency and untampered documentation regarding cash flow. This will help to protect the system from fraudulent spending. Through system automation and transparency movement of donor funds, blockchain technology can help restore the lost credibility of many current charities.

In 2018, Binance created the not-for-profit Binance Charity Foundation. The charity was founded on a blockchain-based, transparent, decentralized donation system. This system must have been quite successful, as they were able in January 2020 to launch a charity project to help the Austrian government overcome the current eco-catastrophe.

We believe that this type of blockchain solution platform is revolutionary and will be highly attractive to organizations that want their financial processes to be transparent, traceable, unchangeable, and reliable. Such a system will install superior trust in donors, thereby greatly facilitate donor recruiting efforts. We, therefore, believe that more charity organizations will adopt these types of platforms in the future.

16.7 Voting and identity management

Voting blockchain companies are exploring the potential of online voting solutions. Citizens wanting to cast their vote are required to show up at voting stations physically, or in some countries have the option to vote by post. In any democratic system, the goal is to have as many citizens as possible to participate in an election. Thus, an inefficient voting system that creates unnecessary hurdles and discourages voters from voting should be avoided at all costs. Due to a lack of general transparency, including how voting results are analyzed and reported, often add additional serious legitimacy concerns. As a consequence, ballot accuracy is a constant topic for debate, that in the worst case, can lead to political unrest.

Many voters have frequently asked themselves: How can I be sure that ballot results are correct and legitimate? Did the vote-counting machine fail, and if so, did anybody notice? Was my vote correctly registered, or did it end up in the wrong ballot box? These are all serious concerns that could be avoided with a system proof voting system.

We live in a society where almost everything can be handled online, as long as one is connected to the internet. This opens up to potential novel opportunities with the aim of improving the current voting system. As soon as credible and proper systems are in place, blockchain technology could revolutionize the current voting system.

Figure 55. Online Voting [148]

Through a peer-to-peer blockchain network, each vote would be recorded and linked to a specific individual on the distributed ledger. The identity of each voter will be completely anonymous, as they will be hidden behind an encrypted key.

As a consequence, network users can access the ledger and view and verify voting documents. In addition, checks regarding potential discrepancies can be performed so as to protect against fraud or other system malfunctioning.

Blockchain technology is immutable, making the ledger permanent and unchangeable. This ensures that no votes can be changed, removed or added without being noticed. As a consequence, also fraudulent manipulations will be documented on the ledger and consequently exposed. By encrypted blockchain technology, creating a transparent and secure voting system, the fear of manipulated ballot results can be put to rest.

Blockchain solutions add crucial additional protection against potential hacking activities. Blockchain is a decentralized network, which means that votes are not stored on a centralized database but are distributed over a larger public network. This makes it extremely difficult for hackers to introduce block changes (add or remove information) as they have to hack a given block. As described in section 1, this is an almost impossible task to perform.

Last but not least, we firmly believe that a voting system that allows voters to cast their votes through solely activating a ballot-app would encourage more voters to participate in an election. In addition, the ability to subsequently check any casted votes would significantly increase the trust towards the entire voting process. These are all auspicious aspects to look forward to.

[148] Sentiman. (2018). E-Voting and Blockchain. Retrieved from https://www.sentiman.io/wp-content/uploads/2018/08/e-voting-and-blockchain-1.png

16.8 Media and Journalism Sector

In the age of disinformation and outright fake news, trust has become a growing scarce resource of increasing value for both large media and independent journalism. Today's information industry is increasingly plagued by its dubious reputation. The general public is fearing the spread of false information with little or no accountability. A huge step in the right direction would be for journalists to regain some of the trust that has currently been lost.

Blockchain-solution could be a course by which to rebuild this trust. The inherit open source, and immutability aspects of blockchain provide for a new form of information-based transparency. Journalists can store all their published articles on the blockchain, as well as include their sources used to write these articles. This will allow the public the opportunity to back-check references. Also, any corrections or even retractions made on published articles will be documented on an ongoing basis. Thus, journalists have the opportunity to update articles based on newly available information while simultaneously updating their followers or readers.

As a consequence, journalists might be increasingly inclined to conduct well-researched articles and abstain from clickbait or misleading titles. As an added incentive, independent journalists who follow quality publishing rules, by basing claims on sound research, could be rewarded by the public with applicable reliability scores. In contrast, journalists spreading misinformation is “punished” with lower scores and therefore deemed less trustworthy.

Blockchain infrastructure can also be used to set up a system where good quality journalism reaps some type of financial benefit. With this concept, the reader pays the author of the article in micropayments. It can be viewed as a type of subscription model, where the reader pays for specific articles of interest, or time spent reading an article. This is very different from the current time-limiting subscription model. As writers receive micropayments based on streaming time and content, they will most probably be increasingly motivated to provide for good quality news content.

16.9 Conclusion Future Use-Cases

After discussing different types of use-cases, it becomes evident that a central challenge to address is the need to increase the general public trust. Trust is granted mainly with an increase in transparency, which is primarily based on access to traceable information. Implementation of these use-cases far exceeds any potential financial benefits but also extends into additional important sectors such as politics, humanitarian aid, social issues, and scientific progress. Blockchain-technology or Distributed Ledger Technologies (DLT) can offer solutions that can help to fulfill many of these requirements. Therefore, our suggested future use-cases deserve to be considered promising future tools aimed at serving the general public. Still, it is extremely difficult to predict where technological advancements will lead us. In the next chapter, we will discuss how rapidly evolving use-cases will be implemented in the upcoming years. In most of these use-cases, we have argued with the virtues of a blockchain; however, since DLT operates similarly, distributed ledger technologies can feasible solution and possibly be used in future use-cases depending on the architecture and implementation.

17 Central Bank Digital Currencies

Through following monetary policy and regulations of commercial banks and financial services, the central bank is responsible for the prevention of hyperinflation, the maintenance of financial stability, and the stability of their national currency.

Based on the technological introduction of permissionless open-source blockchains, such as Ethereum and Bitcoin, policymakers and central bankers have evaluated the feasibility for central banks to issue digital currencies, also known as Central Bank Digital Currency (CBDC). In January 2019, Barontini and Holden did a survey in order to estimate how many nations had currently evaluated the option of implementing a CBDC. Based on the survey, 70 percent of responders had already experimented with this technology or trialed proof-of-concept.[149]

What does CBDC actually stand for, and what does it entail? Currently, the CBDC is not a well-defined term. The International Monetary Fund (IMF) has given it the following definition: *"CBDC is a new form of money, issued digitally by the central bank and intended to serve as legal tender."* [150]

Thus, after fiat-currency, a CBDC might be the next stage in monetary innovation, with its medium being significantly different from other forms of currencies currently issued by central banks (cash and reserve balances). As defined by the IMF, CBDC must not necessarily have a physical form, but should still be widely available to citizens of a country. Usually, retail payments are only available to some institutions, most often banks with accounts at a central bank. In contrast, CBDC's are designed to make retail payments much more accessible. [150]

Globally, the way payments are handled changed drastically over the last ten years. Due to more online payments with an increase in the use of credit cards, cash payments have fallen sharply both in Europe and the US. Due to fiat currency hyperinflation in countries such as Argentina and Venezuela, people have already started to use alternative digital payment modes like Bitcoin. This topic will be discussed further in the next chapter.

With the current ongoing significant shift in how we define and use money, central banks have started to realize that they must remain flexible and adapt in order to keep up with fast-evolving digital technology.

[149] Barontini, C., & Holden, H. (2019). Proceeding with caution-a survey on central bank digital currency. *Proceeding with Caution-A Survey on Central Bank Digital Currency (January 8, 2019). BIS Paper*, (101).
[150] Griffoli, M. T. M., Peria, M. M. S. M., Agur, M. I., Ari, M. A., Kiff, M. J., Popescu, M. A., & Rochon, M. C. (2018). *Casting Light on Central Bank Digital Currencies*. International Monetary Fund.

Central banks have started to realize that if private issuers gain control over a majority of a country's payments, they will lose the ability to implement and conduct sound monetary policies. It is, therefore, crucial that central banks understand the economic impact of introducing their issued CBDC.

In its current form, digital assets are not perfect, but we expect their role to impact the global economy increasingly. Due to individuals being able to move and use value without relying on fiat currency, digital assets challenge the pillars of our current financial system.

The first bank to publish a CBDC framework was the Bank of England. Still, the central bank of Sweden (Riksbank) is the institution that has come closest to implementing CBDC solutions. In 2020, with the aim to introduce CBDC and make it available to the general public, technical solution tests based on Distributed Ledger Technology were started. An initiative that was named e-krona. [151]

With the Riksbank currently having the lead on CBCD development and is close to its actual implementation, we will take a closer look at the 2020 e-krona project.

17.1 The Central Bank of Sweden: e-krona Project

The e-krona project is a joint venture between the Central Bank of Sweden (Riksbank) and the country's political decision-makers. In collaboration with Accenture, an innovative technology company, they strive to build an e-krona platform. The aim of this platform is to create a simple, user-friendly digital token that meets all required safety and performance standards.

Its development will be implemented in an isolated test environment. Test users retain their e-krona in a digital wallet, where they can initiate transfers or make payments by using personal wearables such as smartwatches, credit cards, various apps, etc. The access and use of e-kronor will be available 24/7, with payments being immediately processed and settled. The project, with its functionalities, is expected to be completed in February 2021. [151]

The e-krona CBDC network will be responsible for its implementation, whose infrastructure is parallel to the current payment system. Only the Riksbank will have the mandate to issue an e-kronor. Thus, e-kronor tokens cannot be forged or copied but enable immediate, peer-to-peer payments. The nodes in the CBDC network will be responsible for securing, validating, and forwarding conducted transactions, with only valid network transactions being documented. [151]

[151] Riksbank, S. (2020). The Riksbank to test technical solution for the e-krona. Retrieved from https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2020/the-riksbank-to-test-technical-solution-for-the-e-krona/

Figure 56 shows an illustration of the e-krona conceptual architecture pilot.

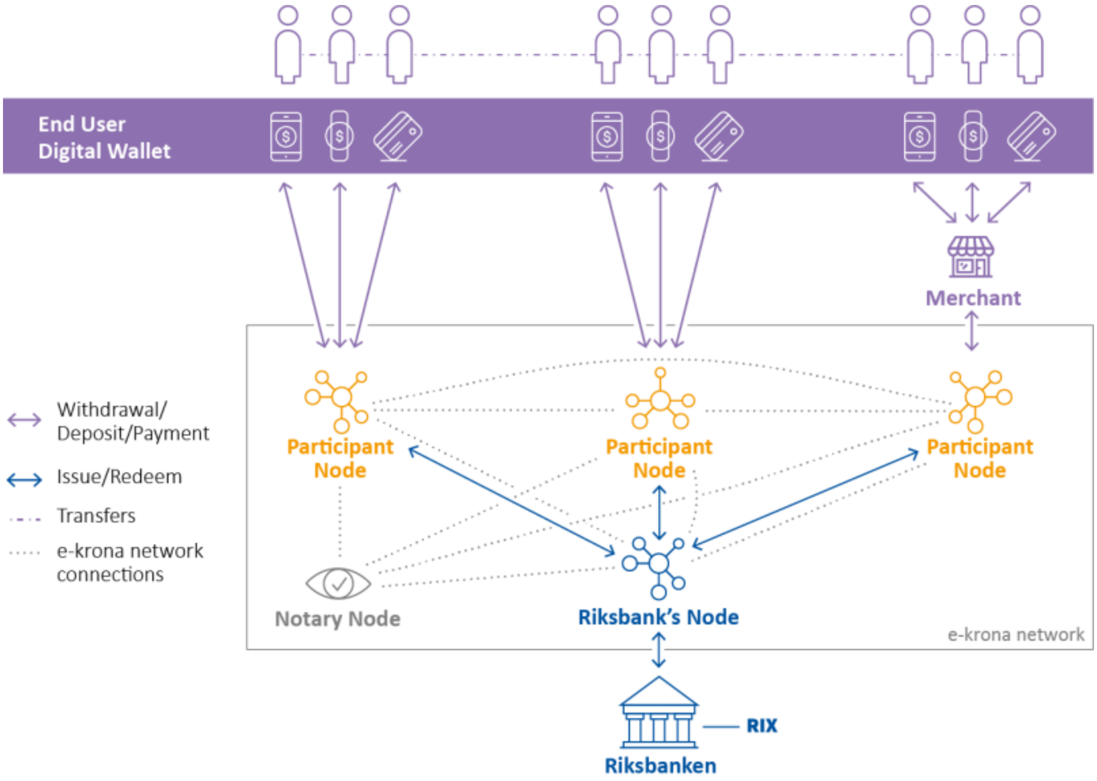


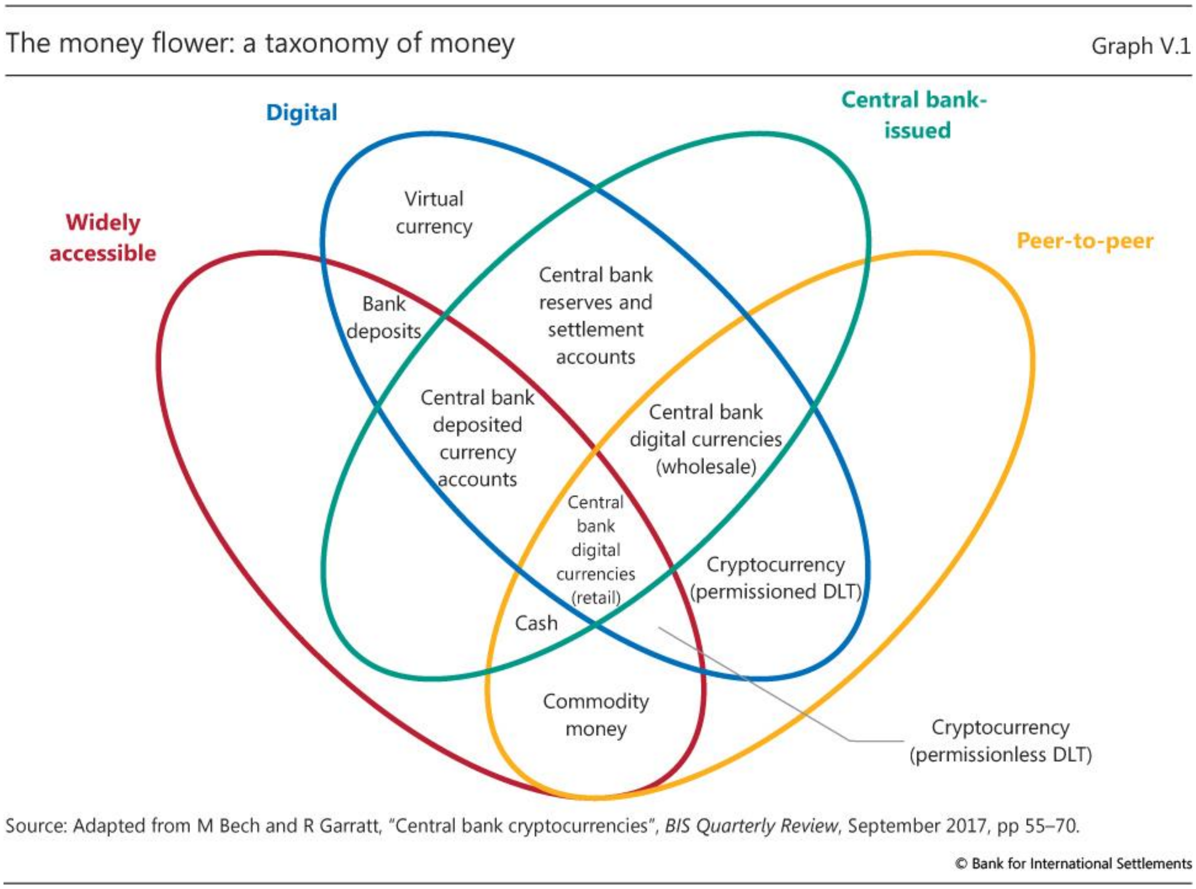
Figure 56. A conceptual architecture for the e-krona pilot [152]

The e-krona platform is built on Corda's open-source blockchain solution used by businesses. The Corda platform differs from ordinary blockchains in that it is not as energy-intensive as many other blockchains. It has a private and permissioned architecture and is only accessible to Riksbank approved members and users. As a consequence, the e-krona and Corda's blockchain are considered a private permissioned blockchain.

[152] Accenture (Producer). (2020). Conceptual architecture for the e-krona pilot. Retrieved from https://www.riksbank.se/imagevault/publishedmedia/327ame3mfehgr0qvkg30/Riksbankens-e-krona_ENG.png

17.2 CBDC Taxonomy

The Venn diagram “The money flower” forms the basis needed to categorize the taxonomy of Central Bank Digital Currencies (CBDC). Several central banks working with CBDC technology utilize the “Money Flower” diagram as help to describe the inherent properties of CBDC in relation to other forms of money. In 2017, Bech and Garratt created the Venn diagram, which illustrates four critical features of money; accessibility, technology, issuer (central bank, commercial banks, etc.), and payment transfer mechanism.[153]


The money flower: a taxonomy of money

Graph V.1

Digital
Central bank-issued
Widely accessible
Peer-to-peer
Virtual currency
Bank deposits
Central bank reserves and settlement accounts
Central bank deposited currency accounts
Central bank digital currencies (wholesale)
Central bank digital currencies (retail)
Cryptocurrency (permissioned DLT)
Cash
Commodity money
Cryptocurrency (permissionless DLT)

Source: Adapted from M Bech and R Garratt, “Central bank cryptocurrencies”, *BIS Quarterly Review*, September 2017, pp 55–70.

© Bank for International Settlements

Figure 57. The Money Flower [154]

[153] Bech, M. L., & Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review September*.

[154] Bech, M. L., & Garratt, R. (Producer). (2017). Central Bank Cryptocurrencies. Retrieved from https://www.bis.org/publ/arpdf/ar2018e/images/graph-V1.jpg

17.3 Pros and Cons of Central Bank Digital Currencies

There are many positive and negative aspects when considering the implementation of Central Bank Digital Currencies (CBDC). In the table below, we selected two properties we believe to be the most important or critical factors. "*Each country will have to weigh the pros and cons of the case for CBDC depending on its particular circumstances.*" [155] [156]

PROS	CONS
A more efficient payment system It reduces transaction time and cost. Provides unbanked citizens from impoverished nations access to a payment system that does not require having a bank account	**Increased cost and a loss in reputation for central banks** The provision of CBDC can be costly, requiring the implementation of a payment value chain, building wallets, monitoring transactions, and maintaining technology. Failure to successfully realize these functions significantly jeopardizes and undermine the reputation of the central bank
Enhanced monetary policy Allows for the direct implementation of required or adapted monetary policies. Allows for an internal competition between permissionless digital assets in order to improve financial inefficiencies	**Centralization** Banks most likely won't issue permissionless CBDC's. Therefore, the amount of control over the currencies of the people is concerning. The Banks could freeze, delete, and stop any payments being internal or international without question by a press of the button as long as the payment is with the CBDC.

[155] Adrian, T., & Griffoli, T. M. (2019). Central Bank Digital Currencies Retrieved from https://blogs.imf.org/2019/12/12/central-bank-digital-currencies-4-questions-and-answers/

[156] Zhang, T. (2020). Deputy Managing Director Tao Zhang's Keynote Address on Central Bank Digital Currency. Retrieved from https://www.imf.org/en/News/Articles/2020/03/19/sp031920-deputy-managing-director-tao-zhangs-keynote-address-on-central-bank-digital-currency

17.4 Central Bank Digital Currency Conclusion

We are currently at the very early developmental stages regarding the implementation of Central Bank Digital Currencies (CBDC). Still, we observe that increasingly more banks realize the opportunities provided by this new technology.

Ironically enough, the very unfortunate and challenging 2020 COVID-19 worldwide pandemic might have given this technology an unexpected boost. On the 3rd of April 2020, the Bank of International Settlements (BIS) published a report with the title, “COVID-19, cash, and the future of payments”. The report was written in connection with the fear that the COVID-19 virus could be transmitted through the exchange of banknotes and coins. [157]

The report referred to a recent study by Neeltje van Doremalen et al., who showed that surface characteristics could significantly influence potential viral survival time. She found that COVID-19 could survive up to 3 hours in the air, 24 hours on cardboard, and even longer on hard surfaces. [158]

Even though the report concludes that there is a low risk of the virus being transmitted through banknotes, it has made many banks, including citizens around the world aware of its potential infection risk. This situation might have stimulated banks to come up with new ways to digitize their currency through their own CBDC. We believe that such a pandemic could help change solutions for today's system by digitizing its fiat currency more efficiently.

[157] Auer, R., Cornelli, G., & Frost, J. (2020). Covid-19, cash, and the future of payments. ISSN:2708-0420. Retrieved from https://www.bis.org/publ/bisbull03.pdf

[158] van Doremalen, N, T Bushmaker, D Morris, M Holbrook, A Gamble, B Williamson, A Tamin, J Harcourt, N Thornburg, S Gerber, J Lloyd-Smith, E de Wit and V Munster (2020): “Aerosol and surface stability of SARSCoV-2 as compared with SARS-CoV-1”, NEJM.org, March.

18 Digital Assets: The Substitute for Failed Monetary Policies

Since we forecast that the financial system and money itself will be most affected in the upcoming changes in blockchain technology, we will provide our own opinions on how the current monetary systems failures will set in motion a gradual shift towards a more decentralized digital finance architecture.

In our last chapter, we will attempt to present our findings and speculate on the future of the financial system. Mainly we will examine struggling or highly corrupt nations, meaning the governments restricting the free will of the people or nations resembling dictatorships. We will display our interpretation of the current monetary policies and how they will impact the future adoption of digital assets in free-falling economies. One key factor that we believe will contribute to individuals adopting digital assets as a means of payment or storing their earned value is inflation and purchasing power.

18.1 Purchasing Power

Purchasing power is the value of a unit quantity of currency needed to purchase a given amount of goods and services. In other words, it represents the actual value of money and how many "things" I am able to buy with it at a given time point. Gold is a prime example of a "currency" that has proven its stable and durable purchasing power over centuries. Its stability is largely based on its limited resource retaining a constant worldwide supply over decades. For this reason, some countries and banks have decided to store their wealth in gold rather than fiat currencies, which are much more prone to inflation.

18.2 Inflation

Inflation is a financial instrument, measured in percentages, that defines the sustained increase in the general price level of the economy. Inflation can be experienced through an increase in the cost of living as the price of goods and services rise. Thus, inflation results in the devaluation of local currencies, which are inflated. As a consequence, the value of money is decreased, which again negatively affects purchasing power. Inflation is the reason why the purchasing power of money from even some years ago is better than it is today. Thus, as prices of goods and services rise, the same amount of money will purchase a smaller quantity of products or services.[159]

[159] Chen, J. (2020). Inflation. Retrieved from https://www.investopedia.com/terms/i/inflation.asp

Inflation can be divided into two sub-categories: Cost-push and Demand-pull inflation.

18.2.1 Cost-push Inflation

Cost-push inflation is a rise in item or service price, caused by an increase in production costs, such as an increase in labor costs, costs needed to extract and produce raw materials, such as higher oil prices. [159]

18.2.2 Demand-pull Inflation

Demand-pull inflation is the result of rising prices due to an increase in customer demand, while supply can't keep up the rising demands. This results in an economic supply-demand gap, where the demand outgrows the supply. As a consequence, prices must be adjusted in order to mitigate this relationship. [159]

In our thesis, we focus on demand-pull inflation. We discuss how the printing of currency by the central banks affects the overall money supply and, consequently, the risk of inflation.

The system of monetary expansion is inherently inflationary, as the act of expanding the money supply in the economy without a proportional expansion of goods and services will always debase a currency. This is clearly shown when comparing the money supply of the USD vs. the purchasing power of the dollar. We can see that there is a defined inverse relationship.

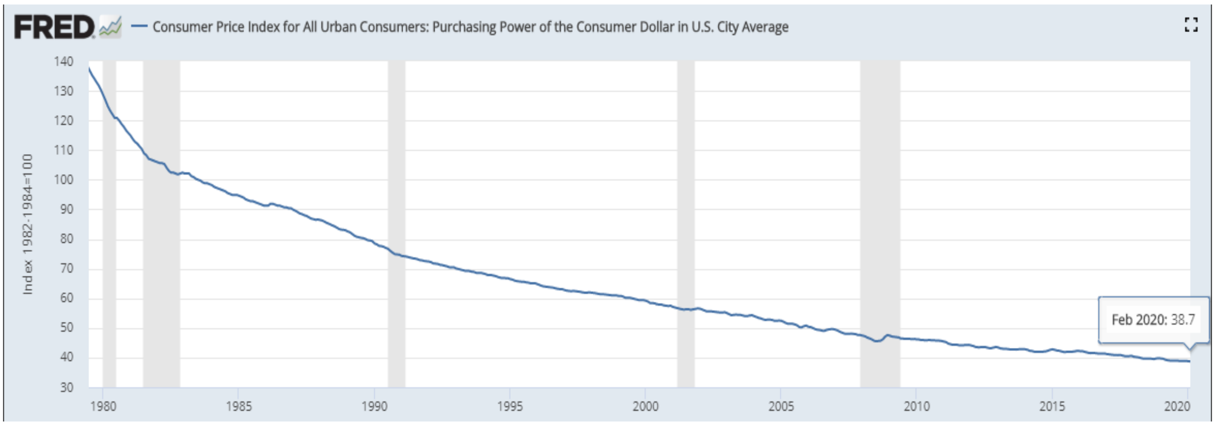


Figure 58. The purchasing power of the consumer dollar in the US [160]

[160] U.S. Bureau of Labor Statistics, Consumer Price Index for All Urban Consumers: Purchasing Power of the Consumer Dollar in U.S. City Average [CUUR0000SA0R], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/CUUR0000SA0R, April 7, 2020.

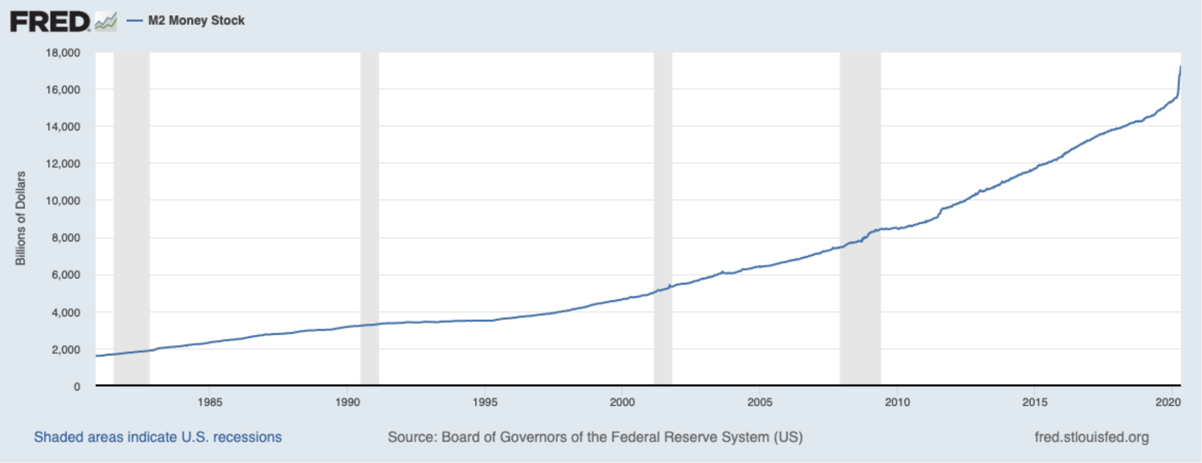


Figure 59. M2 Money stock [161]

M2 Money stock:
"includes a broader set of financial assets held principally by households. M2 consists of M1(currency outside the U.S Treasury, Federal Reserve Banks, and the vaults of depository institutions; traveler's checks of nonbank issuers; demand deposits; and other checkable deposits)[162] *plus saving deposits, small-domination time deposits, and balances in retail money market mutual funds."*[161]

18.3 The Law of Supply and Demand

For the determination of item or service prices, the relationship between supply and demand is a well-established economics model. In an open market, the price of any commodity is determined through the ongoing interactions between supply and demand. The price tends to bid up when customers want to purchase more products than are readily available on the market. Thus, as demand exceeds market-supply, the price will rise to justify the gap. In contrast, if buyers decide to purchase fewer products, the market will create a surplus that tends to bid the price down. A demand that falls short of supply will, therefore, decrease the price of the product.

This correlation is defined as core-of-price-discovery. Many countries depend and expand their wealth by exporting various goods and services. Importing countries are able to buy these products based on the currency power of the exporting country. As a consequence, some central banks try to control or manipulate the price of their goods by printing money.

[161] Board of Governors of the Federal Reserve System (US), M2 Money Stock [M2], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/M2, April 7, 2020.
[162] Board of Governors of the Federal Reserve System (US), M1 Money Stock [M1], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/M1, April 7, 2020.

This will expand the local money supply, which will inflate the value of their currency, making products less expensive for customers wanting to import these products. [163]

In regard to digital assets and other forms of money, there are distinct differences.

18.4 Money

Money is a funny subject; our whole lives revolve around money. We work for it, devote our early years to learn and educate our self to find a job that provides us with income, after that, work in a company or create a business to earn more money. Our whole lives are aimed to amass enough wealth to live life the way we deem worthy. Nonetheless, we do not learn about money from the school system, what money is, how it is created, and who controls it. Ironically, we devote most of our lives to something that is so little understood by the everyday person, or maybe this was intentional. However, we aim to provide an overview of what money is and how it has been used and the properties of money.[164]

Money has been around for thousands of years, evolving from scares products like livestock, sugar, and other various goods which were redeemed for favors or accepted as a payment method towards coins consisting of rare materials like bronze, silver, and gold. One form of currency stands out and has proven itself for thousands of years and is still widely used today for individuals storing their wealth, and this commodity is gold, silver, and bronze. Currency has evolved and transformed during human history. However, most of these monetary commodities share distinct properties that qualify these as money. Next, we will examine these properties which we deem necessary for something to be considered as money:

18.4.1 Store of Value

People can save and store their earned form of money and save it for later to purchase something. My type of currency will hold its value until one decides to spend it. However, some money is prone to inflation, which erodes the purchasing power of that money of a certain period, depending on the inflation percentage.

18.4.2 Unit of Account

A measuring method for a unit of account. It provides a common base for prices. For example, dollars and cents, weight of gold or other units of measurements to quote prices in.

[163] Supply and Demand. (2019). In *Encyclopedia Britannica*: The Editors of Encyclopedia Britannica.Retrieved from https://www.britannica.com/topic/supply-and-demand
[164] St. Louis federal reserve bank. *Functions of Money* [Retrieved from https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money

18.4.3 Medium of Exchange

The form of money is widely accepted as a method of payment. It can be exchanged between parties with ease and is accepted in most stores or countries which one wishes to purchase items from.

These are the base essentials for any good to be considered as money, but there are a lot of items that could be deemed money under these circumstances. Therefore, it is wise to differentiate between "good" and "bad" money. Here money with these characteristics will prevail over other forms of currency, which might lack or not wholly live up to these requirements. These are:

Property:	Definition	"Good" Money of this property	"Bad" Money of this property
Durability	Able to exist for a long time without significant deterioration in quality or value.	Gold	Livestock
Portability	The quality of being able to move the item with ease.	Digital Assets	Gold
Divisibility	Capable of being divided easily and volume.	Fiat currency/Digital Assets	Gold
Uniformity	Always having the same form, manner, or degree, not varying in appearance.	Gold	Livestock
Limited supply	A limited supply of the item can't quickly produce more or exist more.	Gold/Digital Assets	Fiat currency
Acceptability	Capable of being accepted by a variety of individuals around the globe.	Fiat Currency/Gold	Digital Assets
Cognizable	Being able to recognize the form of currency easily.	Fiat Currency/Gold	Digital Assets
Non-counterfeit ability	Not being capable to counterfeit the item and pay with fake goods.	Gold	Fiat currency/Digital Asset

Perfect money does not exist, and each monetary currency has advantages and drawbacks. The best-proven currency thus far is Gold. Because of its characteristics, it has been the dominant choice of currency throughout history.

18.5 The Most Common Form of Currency Today

Through the ages, money has gone through drastic changes from traditionally being transacted through the use of coins to being an electronic bank statement on some business accounts. When looking at the evolution of today's money, we will describe different settings.

During the 20th century, all banknotes issued by the US federal reserve were redeemable in gold. In other words, all issued money or currency made available on the market was backed by a fungible asset such as gold or silver. This system is referred to as the Bretton Woods Agreement, which was implemented during the second world war in 1944.[165] However, in 1971 President Nixon announced that the US dollar would no longer be redeemable in gold[166]. From that day on, the US dollar was endowed as a fiat currency. Today the US dollar has a critical international status, as crude oil is quoted and traded in US dollars, forcing countries who sell or buy crude oil to operate with this currency. As a consequence, the US dollar becomes the national reserve currency of the world.[167]

18.5.1 Fiat Currency

It is money that does not possess any intrinsic value, as it is not backed by fungible assets. Its value is derived from being declared “legal tender”- where a country's government issuing the currency defines it as an acceptable form of payment, legal tender for all debts, public and private.[164]. In essence, the asset has value because the government tells us it has. Therefore, the value of any fiat currency is based on trust people bestow on their government that its currency indeed possesses the proposed value.

[165] Chen, J. (2019). Bretton Woods Agreement and System. Retrieved from https://www.investopedia.com/terms/b/brettonwoodsagreement.asp

[166] Sandra, G. (2013). Nixon ends convertibility of US dollars to gold and announces wage/price controls. Retrieved from. https://www.federalreservehistory.org/essays/gold_convertibility_ends

[167] Farley, A. (2019). Understanding the Correlation of Oil and Currency. Retrieved from https://www.investopedia.com/articles/forex/092415/oil-currencies-understanding-their-correlation.asp

18.6 Consequences When Trust is Lost

Earlier, we strongly argued that money is a belief system. Thus, the real value of fiat currency is solely based on the belief, and trust people in a society bestow on their currency. However, this trust can be misused and exploited for the benefit of a few. Once this trust has been lost, it will be extremely challenging for any government to regain people's confidence. In these circumstances, individuals will most probably search for alternative methods and ways to store and transact their wealth, excluding any involvement of those who betrayed their trust. Thereby paving the path of irreversible change in human's understanding of money, currency, and governance structure of the monetary system.

Once people of a nation have lost trust in their government, and the currency issued from its central bank, the value of that currency will spiral downwards. Throughout history, this type of scenario has played out many times, with catastrophic consequences for those people involved who invested their life savings in the country's fiat currency. As everything revolves around commerce, the entire economy is consequently in freefall.

This development is known as hyperinflation, which occurs when inflation is taken to the extreme, and prices of goods and services rise dramatically. Money loses its value so rapidly that nobody wants to use or accept it as a medium of exchange. Essential trust needed to keep the economy going is lost as people find no value in money as an acceptable form of currency. [168]

18.6.1 Hyperinflation: Germany after 1st World War 1923

The cause and devastating effects of hyperinflation are perfectly illustrated in Germany after the first world war. War leaves behind devastation, uncertainty about the future, and widespread misery. In 1923, German citizens were striking because French troops were occupying the Ruhr part of Germany. The Weimar government decided to support the strike by continuing to pay striking workers. In order to support these strikers, the central banks in Germany started to print paper notes, a policy the government had been using intermittently since 1921 to help with economic conditions.[169] However, this scenario was created due to central banks in Germany printing paper notes to help with the economic conditions. The government economists were skeptical and sounded alarmed, afraid of the potential consequences of banks printing money as if there was no tomorrow. However, the central bank reassured that these measures were only temporary and insisted that these steps were necessary.[169]

[168] Kenton, W. (2020). Hyperinflation. Retrieved from https://www.investopedia.com/terms/h/hyperinflation.asp
[169] Llewellyn, J., & Thompson, S. (2019). The hyperinflation of 1923. Retrieved from https://alphahistory.com/weimarrepublic/1923-hyperinflation/

In this case, the demand for money far exceeded its supply. Therefore, the banks and governments decided to expand the money supply and pump newly printed currency into the economic system to try to save the economy. Obviously, this was a terrible idea, thereby massively devaluating the base currency and robbing the people of their purchasing power. Throughout 1923, the crisis was at its peak with the money printing machine printing into overdrive. As these new banknotes came into circulation, with the devastating result that each Reichsmark´s purchasing power was decreased.[169]

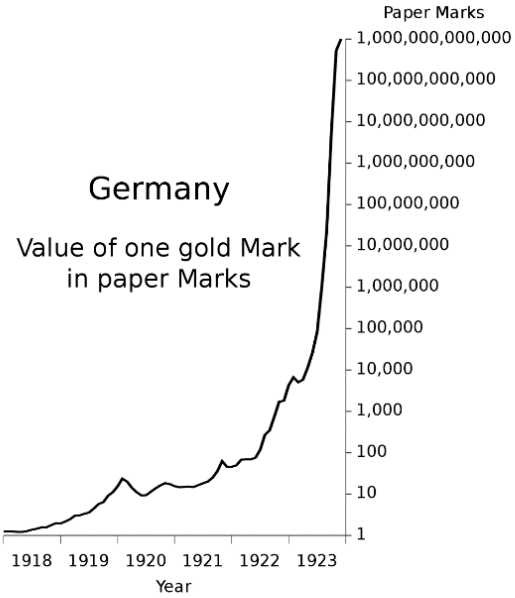


Figure 60. Hyperinflation in 1923 Germany after 1st world war [170]

18.6.1.1 Conclusion Hyperinflation Germany

Printing currency like there is no tomorrow is not a viable long-term solution. It only negatively affects the economy and its citizens of that country in an unimaginable way. This can only be fully understood if one had to live through such a situation. The biggest loser in these kinds of scenarios are, unfortunately, people in the lower to the middle-class economic sector, who have their wealth saved up in investment funds and pension rents.

Still, the situation as it was played out in Germany is not really applicable to our present-day. The internet was not yet conceived or what we today consider part of modern society and living. In addition, there were no digital ways of creating currency or the digital economy, which we have become accustomed to. We will examine a more current scenario taking place in Venezuela, creating economic and social horrors for individuals living in that country.

[170] Logarithmic chart of German Hyperinflation. Based on the values in Table IV (page 441) of The Economics of Inflation by Costantino Bresciani-Turroni, published 1937. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/4/4f/Germany_Hyperinflation.svg/1920px-Germany_Hyperinflation.svg.png

18.6.2 Hyperinflation: Venezuela

In 2018 Venezuela had the most share of oil reserves in the world and was considered one of the wealthiest countries in South America.[171] [172] However, during the same time period, Venezuela was experiencing a high percentage of increases in inflation rates. Furthermore, in 2020 the IMF provides data that states that Venezuela has a whopping 65’000 % inflation rate.[173] This inflation rate is long past average inflation and is devastating for Venezuela citizens.

On the contrary to the German hyperinflation, digital assets weren’t invented yet. We thought it would be interesting to analyze the digital assets space and usage of digital assets in Venezuela under these extreme circumstances and try to find some useful information. Here is our conclusion:

18.6.2.1 Digital Assets in Venezuela

Interestingly enough, the country has issued its own supposed oil-backed cryptocurrency called the Petro on the 15th of March 2018. [174] However, upon further research, we remain skeptical towards this step and has not shown a lot of promise form the inception until 2020. President Trump has gone as far as to banned U.S purchases of the Petro. [175]

We have not found any reliable data on how many citizens of Venezuela are actively using this cryptocurrency. However, there exists evidence on the Bitcoin usage inside the country.

[171] OPEC Share of World Crude Oil Reserves. (2018). Retrieved from https://www.opec.org/opec_web/en/data_graphs/330.htm

[172] J.Kiger, P. (2019). How Venezuela Fell From the Richest Country in South America into Crisis. Retrieved from https://www.history.com/news/venezuela-chavez-maduro-crisis

[173] IMF. Inflation rate, average consumer prices. Retrieved from https://www.imf.org/external/datamapper/PCPIPCH@WEO/WEOWORLD/VEN

[174] Petro Whitepaper. (2018). [PDF] Retrieved from https://www.petro.gob.ve/files/petro-whitepaper-english.pdf

[175] Bloomberg. (2018). President Trump Bans U.S. Citizens From Buying Venezuelan Cryptocurrency Petro. Retrieved from https://fortune.com/2018/03/19/donald-trump-cryptocurrency-venezuela/

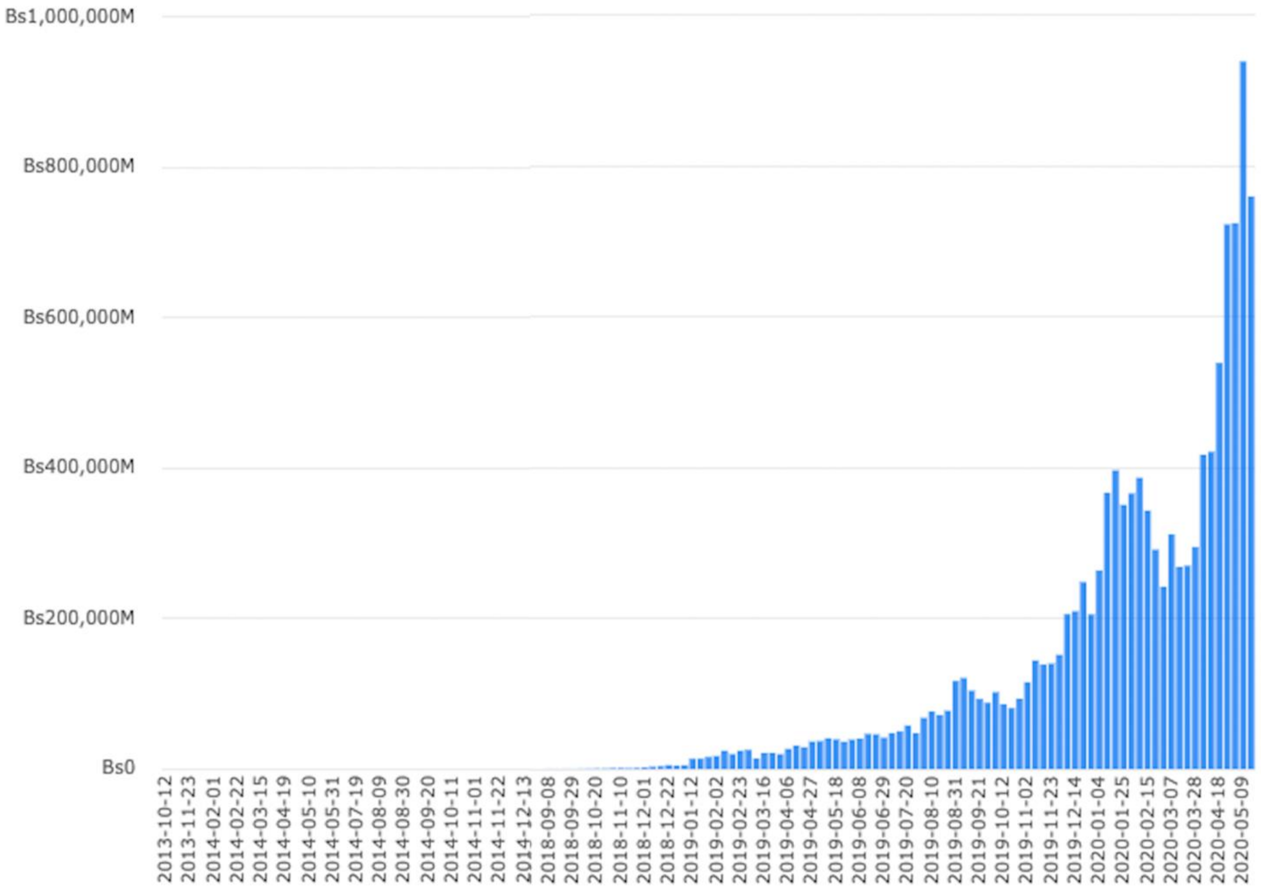


Figure 61. Bitcoin volume in Venezuela [176]

Even though digital assets are extremely volatile and can lose a lot of their value, compared to hyperinflation, digital assets are not equally volatile and more stable. Therefore, we believe some educated citizens in countries which are losing their purchasing power daily and do not have the resources to buy gold or other more stable currencies, will gradually find themselves leaning towards the digital assets market. Here, the permissionless and decentralized nature is very appealing for individuals that do not trust their governments or banks and want to send money to their families or store the little wealth they have left.

However, since Bitcoin is not private by design, we suspect that individuals in Venezuela who do not wish that the government is tracking them and want to send money privately will pivot to more privacy coins like Monera, Dash.

[176] Coindance (2020). Venezuela Local Bitcoins Volume. [April 9th, 2020] Retrieved from https://coin.dance/volume/localbitcoins/VES

We believe that in authoritarian and suppressive regimes, individuals will naturally try to get out of this corrupt system and try to access a different financial way of sending money and keeping their money safe. Therefore, we believe that digital asset adoption will flourish in countries which do not have a strong economic foothold, high inflation rate which devalues savings and wealth of the average citizen and corrupt and oppressive government which spy on all citizens and dictate aspects of their lives.

In most developed economies, this idea of using a digital asset is absurd and ridiculous. However, in less developed countries where citizens might not have access to bank accounts and have no real solution to store currency, they might adapt and be open to this idea of using digital assets.

18.7 Conclusion Digital Assets a Substitute For Failed Monetary Systems

In our current financial system, money is debt, and debt is money. Such a system works well for banks, as they earn interest and make a profit of indebted individuals, businesses, even countries. How can a constant accumulation of debt be sustainable, as the whole point is to eventually have to pay back one's debt, including interest? These questions are difficult to answer and cannot be resolved here. But what we can expect that indebted governments or individuals who live paycheck by paycheck realize that their income dwindles, as goods and services become more expensive, will become seriously fed up. No one wants to be enslaved by their personal debts. People are already looking for alternatives, even though not many are currently in existence. Depending on personal exposure, some have started to gravitate towards digital asset solutions.

An important aspect to understand is how the dynamic of supply and demand play out differently between digital assets and currency. As described earlier, when the money supply is low, banks can print additional currency. This will expand the available currency supply, which carries with it the risk of inflation. In contrast, digital assets can be created infinite amounts. Thus, once all digital assets have been released into the network, no more additional assets will be available for subsequent releases. Due to the digital asset code dictating a finite total supply of assets, will annul any future potential risk of inflation.

In contrast to fiat currencies, some digital assets can implement a predictable and controlled inflation rate, which is programmed by the given network. This is achieved by an algorithm that mathematically calculates the amount of digital assets to be released into the network at any given time. As a consequence, inflation rates occur in a controlled and predictable manner. It is important to understand that the release of digital assets is not controlled by a bank or a centralized entity but solely based on the decentralized architecture of the blockchain. Money printed by greedy bankers does often not align with priorities set by common people. In contrast, digital assets do not operate based on personal gain. Its value is solely controlled by mathematics and governed by network laws translated into computer codes.

Like the value of gold that remains quite stable due to limited supplies, digital assets with its fixed supply will operate and be governed by similar supply and demand laws. As digital assets are leased on the market in a predictable manner, its supply increases only up until all assets have been released in the network. Compared to gold being a scarce commodity with finite amounts, digital assets function in this respect even better as their finite amount is given and immutable, while the future potential gold supplies remain unknown. As a consequence, digital assets become more valuable over time, as more people want to share a finite amount of assets. In other words, more people must share the cake, which makes supply increasingly scarce, and the digital asset more valuable.

Based on its current reputation, digital assets lack many characteristics that are used to describe "good" money. Currently, ongoing fluctuations in price discovery is a matter of concern for many people contemplating viewing digital assets as a currency. We believe that these fluctuations will markedly decrease and become much less prone once the industry matures, and more people use digital assets. This relationship can be well demonstrated when comparing digital assets to gold. Today gold's market cap is worth approximately 10,6 trillion [177] at a price of 55'769 Dollars per kg[178]in order to effect this huge volume of wealth resulting in noticeable price fluctuations, preposterous large amounts of money would have to be pumped into the system. The total wealth of digital assets as of May 17th is 267 billion dollars [179] , which only a minuscule percentage when compared to gold. Thus, much smaller amounts of money injections or withdrawals will result in high price fluctuations.

We believe that digital assets and blockchain technology will one day be deemed just as valuable as any form of currency. In contrast, the digital asset holder will be free of banks and do not have to worry that hyperinflation might devour most of their savings even though there is still a long way to go with many hurdles to overcome. But we remain open-minded and keep an eye out on the future developments and implementations of blockchain technology and digital assets.

As we have seen in this chapter, digital assets carry significant potentials for people to become more financially independent, as well as provide businesses and governments with tools making them more transparent, enabling them to gain the trust of their customers increasingly. In summary, it is still too early to tell if digital assets deserve the same status as money. But digital assets have only existed for 11 years, which is a minuscule speck of time when compared to the history of money.

[177] World Gold Council. How much gold has been mined?. Retrieved from https://www.gold.org/about-gold/gold-supply/gold-mining/how-much-gold
[178] Goldprice. (14th May 2020) Retrieved from https://goldprice.org
[179] Coinmarketcap. (14th May 2020. Retrieved from https://coinmarketcap.com

19 Summary & Conclusion

A blockchain is a persistent, publicly transparent, append-only ledger, peer-to-peer network. Once data is stored on the blockchain network, it cannot be changed or altered. Blockchain technology works by appending blocks/ledgers through employing a mechanism that creates consensus between scattered or distributed sets of nodes/validators. These nodes/validators do not need to trust each other, and they only need to trust the mechanism through which consensus was achieved. Furthermore, these nodes/validators dictate network governance. The network ensures safety and protection through cryptographic hash functions and encryption. The value sent or transmitted through the network must not exclusively be of monetary worth, but can be anything from a business agreement to information regarding processes of a given system.

Currently, newer implementations of Distributed Ledger Technologies (DLTs) are trying to circumvent the usage of blocks in an appendable chain. Instead of blocks, these DLTs experiment with new Directed Acyclic Graph (DAG) data structures that would eliminate the need for mining, staking, and blocks all together. In DAGs, transaction information is stored in each individual transaction and not bundled together into containers like blocks/ledgers. Even though this mechanism is similar to blockchain, the aim is to achieve a single source of truth with a decentralized distributed system based on a topological order. Some of these projects seem very exciting and are at the cutting edge of innovation and research. Nonetheless, these distributed ledger solutions need to prove their efficiency and alleged superiority over contender blockchains.

Regarding consensus models, we have come to the conclusion that in order for a blockchain to be recognized as a viable solution for businesses or individuals around the globe it has to be; sustainable in the long term with respect to energy consumption, able to align the interest between network members (miners/validators) and network users. Thus, incentives of both forced and natural stakeholders need to align in order to achieve the most suitable and safe network. Furthermore, the network has to allow for a scalable payment system that matches or exceeds existing payment networks, such as Visa or MasterCard. In addition, executed transaction time needs to be fast and reliable. Thus, if the underlying proof-of-work consensus architecture remains in place, PoW can be excluded as a sustainable long term consensus model.

We believe that smart contracts will play a decisive role in the upcoming decade, with respect to legal and business contracts that require extensive layers of intermediates to be executed. Due to their autonomous, self-verifying, and tamper-proof nature, smart contracts will naturally prevail and supplant antiquated ways of conducting business. Furthermore, by reducing the relationship of intermediaries, new applications can emerge based on brilliant applications bringing customer demands and data storage security back to the forefront.

Even though digital assets and their ecosystem is considered by some to be sketchy, illegal or just a fad, this assumption should wither away when presented with the hard facts that large industries have already been experimenting with this technology for years and more will assemble. The ecosystem is quite young, standing tall with just 11 years of age.

However, it has attracted a large and diverse worldwide crowd consisting of different interest groups, who have built business models and applications within this ecosystem.

Crucial puzzle pieces missing are harmonized global regulations and standardized procedures for conducting or founding blockchain businesses. As a consequence, we believe the implementation of global regulations is the cataclysm for blockchain adoption and various blockchain use-cases. Facebook's ambiguous libra project has directly contributed to the acceleration of the blockchain industry maturity, changing the perspective viewpoint of this technology. Thus, the anticipated scare by the initial libra whitepaper, resulted in increased awareness by regulators, central banks, and governments around the globe to accelerate regulatory policy developments of digital assets and blockchain technology. This has positively affected the industry as a whole, by recognizing the importance to safeguard innovation while at the same time, provide for a viable developmental framework.

As Sweden is planning to go live with a Central Bank Digital Currency (CBDC) in 2021, and other countries like China have been developing their digital central bank stablecoin for years, we expect CBDC's to become a reality in the impending years. Furthermore, the competitive nature of nations and the current COVID-19 pandemic ramifications will lead to accelerated improvements within CBDC's, as cash becomes increasingly obsolete, and the favorable ease of digital transactions is expanding.

In the upcoming years, we expect distributed ledger technologies to leave the largest footprint in the financial sector. This will especially be the case for international payments and DBDC's. The outdated architectural design with Nostro/Vostro accounts, and their liabilities stemming from antiquated psychology, needs to be reevaluated. Attitudes from various financial behemoths are changing, and they are switching from the mindset that digital currencies are exclusively used by criminals and for money laundering purposes, to recognize that there are substantial benefits with an interoperable, fast, secure, transparent new financial system.

In real business operations, the current largest use-case of digital assets is the internet-of-value. This vision was set in motion by Ripple while using the digital asset XRP. We believe that XRP and other utility-driven digital assets will usher in a new era of digital asset pricing, where the underlying value will be determined by the actual use-case and their real-world impact. As a consequence, these digital assets distance themselves from most current ones on the market that are purely fueled by speculators and traders around the world. The current COVID-19 pandemic especially highlights flaws and frictions regarding correspondent banking systems with their requirements for pre-funding Nostro/Vostro accounts around the world. To date, this is the standardized banking institution, implemented and maintained by SWIFT.

However, expensive, slow, and unreliable payments will become increasingly unacceptable as we as a society move into a more digitized and autonomous world.

Only time will tell if some of our suggested future use-cases will come to fruition. However, we remain optimistic that blockchain offers great benefits for users, businesses, or applications that demand transparency, traceability, security, immutability, censorship resistance, decentralized governance, and automation. What all these qualities lastly boil down to is trust. Trust is most likely the commodity where blockchain has one of its greatest advantages over current systems with comparable services, thereby ensuring its sustainability in the long run. Some of these beneficial qualities might be the missing piece required for a start-up or company to create the next revolutionary app, system, or service to give people access to new opportunities, potentially making their lives easier. Data is the new oil, thereby captivating the attention of entrepreneurs. As more individuals become aware of data protection and data misuse, this will naturally draw users to decentralized solutions where the individual is the administrator retaining the full power of their data.

We foresee that digital assets and distributed ledger technologies (DLT´s) will continue to evolve based on two pathways:

1. In the first pathway, digital assets or DLT's would overthrow or disrupt most existing infrastructures like governments and banks. In most industrialized countries, this pathway is rather unlikely but could be triumphantly successful in countries that are corrupt or impoverished with its higher percentage of unbanked citizens. Irresponsible and greedy actions undertaken from nefarious central banks leads to expanded inflation and worst-case hyperinflation, resulting in the devaluing of the underlying currency. This will rob people from their purchasing power and significantly increase the risk of poverty. Consequently, people will lose trust in the local banking system and seek other means to protect their wealth and the future financial safety of their families. This could lead them towards open-source and permissionless digital assets, independent from the ruling untrustworthy banks and governments. This scenario is very idealistic and stems from a more libertarian view, but probably unlikely to materialize, due to the stronghold of most governments over their citizens and their adamant reluctance to let go of their seized power. It is clear, and these governments might be skeptical against any external invasion that could threaten the prevailing establishment favoring its ruling party.

2. The second pathway envisions a more mature and sensible approach with the aim to educate industry leaders regarding the benefits of this technology and its use-cases. This would augment the current legacy system and bring peace and prosperity among all actors involved. For an autonomous and fair system to be implemented, cooperation and interoperability are required. Therefore, we believe that societies with both regulatory compliant businesses and digital assets that work with the system rather than against it, will prosper among governments and maximize their development.

This will allow this technology and its use-cases to prove their worth and eventually lead to its increased implementation and fuel the transition from speculative crime associate ridden reputation towards an open, transparent system utility-driven system.

Now, after having read our work and acquired a deeper understanding of how distributed ledger technologies and blockchains could potentially shape our future. We encourage the reader to be active and try to initiate discussions and clear up misconceptions within their circle of friends or family, in order to familiarize and bring this technology into society's consciousness. The reader has now been equipped with the required knowledge to discuss blockchain and digital assets on a high-level, while hopefully be intrigued and thus motivated to inquire more information about its technology and future use-cases.

Last but not least, this technology is certainly not a fad or a phase that will be here one year and gone the next. We don’t have all the answers and solutions as to how, when, and to what extent this technology will thrive and be used. These questions will only be accurately answered in the upcoming years. We, as authors of this thesis, look forward to witnessing the future unfolding of blockchain and distributed ledger technologies, including its many promising potentials.

20 Appendices

20.1 Decentralized Exchange

Below we created a flowchart that illustrates the implementation of a Decentralized Exchange (DEX), which demonstrates the use and dataflow by users interacting with the DEX. We provided the exchange with two smart contracts, Token and Exchange smart contracts. Where the token smart contract is used for creating a standardized ERC-20 token on top of the Ethereum blockchain. The Exchange smart contract handles all the functionality of the Decentralized Exchange (buying, selling, depositing, withdrawing etc..).

20.1.1 Technology Used for Flowchart

- **Solidity:** is an object-oriented programming language written for smart contracts and is used to implement smart contracts on various blockchain platforms, especially Ethereum.
- **React:** is a JavaScript library for building user interfaces. Especially useful for single-page applications with its state that can track ongoing changes.
- **Redux:** This is a predictable state container for JavaScript applications, especially useful cause each change in the state creates a new state object where one can track all changes.

20.1.2 Redux Flow

- **Redux state store:** Holds application state contains all states of the application, and when changes are undertaken, the state is copied, and new changes are injected into the newly copied state object.
- **Interactions:** a streamlined approach to managing the redux action creators and reducers.
- **Actions:** are payloads of information that send data from the application to the store.
- **Reducers:** specify how the application’s state changes in response to the actions sent to the store.
- **Selectors:** format and select specified data in order to display the applied changes back to the application for the user to see the interaction taking effect.

20.1.3 Smart Contracts

The first box in the smart contracts represents attributes and variables declared. The second box represents functions and constructors used for the function of the DEX.

20.1.4 Structures

- **Address:** Are a 20byte (size of Ethereum address) placeholder for addresses used in blockchains.
- **Uint256:** Unsigned Integer of 256 bit which cannot be a negative number
- **Mapping:** is a reference type as an array that takes two arguments key and value. It can be compared to other programming languages such as Javas Abstract Map.
- **Event:** it is an inheritable member of a contract. An event is emitted; it stores the arguments passed in transaction logs.
- **Struct:** these are used to represent a record. These can be customizable and store different king of datatypes.
- **+:** is a public modifier, which means that anyone can call these functions from the smart contract and are public to everyone.
- **- :** is an internal modifier that can only be accessed within the given smart contract and is an internal declaration.
- **Payable:** This is an identifier which allows the function to handle actual Ethereum tokens (ETH)

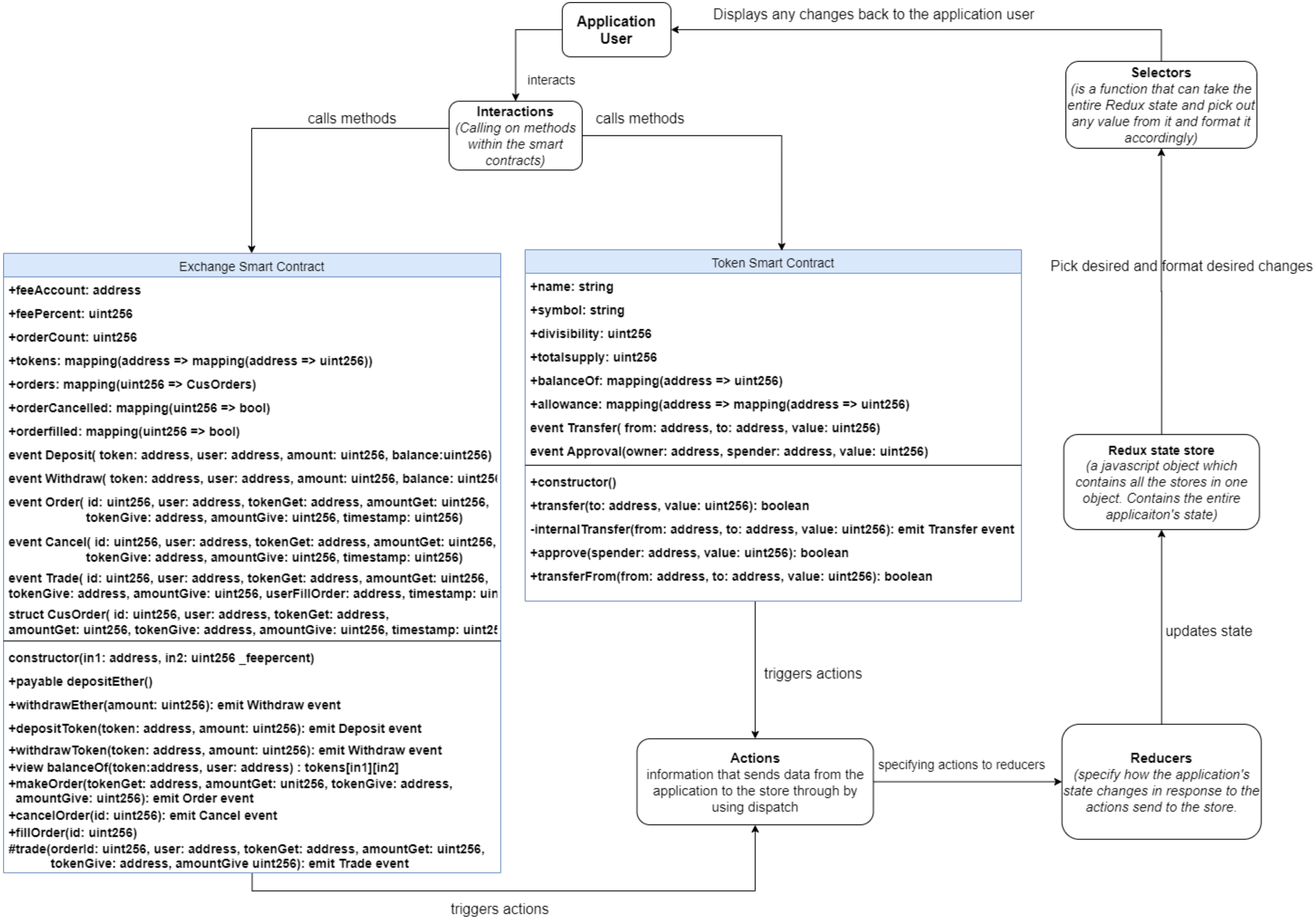
20.1.5 Example of DEX Usage

An application user (Alice) wants to interact with the DEX he wishes to Deposit some Ethereum on the DEX in order to buy the newly created digital asset. Alice now triggers an interaction with the exchange where the interactions.js file contains all possible interactions available with the DEX, in addition, the interaction.js file dispatches the action (the only way to trigger state changes) undertaken and sends the information to Action.js.

Here Action.js contains all possible actions available and specifies the action to the reducers.js file. Thereupon the reducer.js file is responsible for applying the desired changes in response from the action.js to the state object.

As the state object is now altered, the redux state store creates a new state object with the newly applied changes in that state object. Important to note, we don’t mutate the state but rather create a copy with the new changes in order to keep track of changes undertaken to the state object efficiently.

Finally, the state has been updated, and the desired changes have been altered, now the selectors.js file is responsible for selecting the desired data from the whole state object and displays it back to the Application user. Throughout this process, there is a continuous flow of data and steps necessary for the end-user to see changes in real-time and autonomous handling of interactions occurring between the application user and the DEX.


Application User
interacts
Interactions
(Calling on methods within the smart contracts)
calls methods
calls methods
Exchange Smart Contract
+feeAccount: address
+feePercent: uint256
+orderCount: uint256
+tokens: mapping(address => mapping(address => uint256))
+orders: mapping(uint256 => CusOrders)
+orderCancelled: mapping(uint256 => bool)
+orderfilled: mapping(uint256 => bool)
event Deposit(token: address, user: address, amount: uint256, balance:uint256)
event Withdraw(token: address, user: address, amount: uint256, balance: uint25
event Order(id: uint256, user: address, tokenGet: address, amountGet: uint256, tokenGive: address, amountGive: uint256, timestamp: uint256)
event Cancel(id: uint256, user: address, tokenGet: address, amountGet: uint256, tokenGive: address, amountGive: uint256, timestamp: uint256)
event Trade(id: uint256, user: address, tokenGet: address, amountGet: uint256, tokenGive: address, amountGive: uint256, userFillOrder: address, timestamp: uin
struct CusOrder(id: uint256, user: address, tokenGet: address, amountGet: uint256, tokenGive: address, amountGive: uint256, timestamp: uint2
constructor(in1: address, in2: uint256 _feepercent)
+payable depositEther()
+withdrawEther(amount: uint256): emit Withdraw event
+depositToken(token: address, amount: uint256): emit Deposit event
+withdrawToken(token: address, amount: uint256): emit Withdraw event
+view balanceOf(token:address, user: address) : tokens[in1][in2]
+makeOrder(tokenGet: address, amountGet: unit256, tokenGive: address, amountGive: uint256): emit Order event
+cancelOrder(id: uint256): emit Cancel event
+fillOrder(id: uint256)
#trade(orderId: uint256, user: address, tokenGet: address, amountGet: uint256, tokenGive: address, amountGive uint256): emit Trade event
Token Smart Contract
+name: string
+symbol: string
+divisibility: uint256
+totalsupply: uint256
+balanceOf: mapping(address => uint256)
+allowance: mapping(address => mapping(address => uint256)
event Transfer(from: address, to: address, value: uint256)
event Approval(owner: address, spender: address, value: uint256)
+constructor()
+transfer(to: address, value: uint256): boolean
-internalTransfer(from: address, to: address, value: uint256): emit Transfer event
+approve(spender: address, value: uint256): boolean
+transferFrom(from: address, to: address, value: uint256): boolean
triggers actions
triggers actions
Actions
information that sends data from the application to the store through by using dispatch
specifying actions to reducers
Reducers
(specify how the application's state changes in response to the actions send to the store.
updates state
Redux state store
(a javascript object which contains all the stores in one object. Contains the entire applicaiton's state)
Pick desired and format desired changes
Selectors
(is a function that can take the entire Redux state and pick out any value from it and format it accordingly)
Displays any changes back to the application user

20.2 Dictionary

Asymmetric Cryptography: is a cryptographic system that uses pairs of keys. Public keys, which may be disseminated widely, and private keys that are only known to the owner.

Anti Money Laundering (AML): Sets of regulations, laws, and procedures to prevent criminals from disguising illegally obtained funds as legitimate income.

Bit/Byte: A computer works only with 0 and 1 operations. One Bit can only store 0 or 1. One byte is a collection of 8bits.

Blocks: A container data structure. A block can contain any kind of information and these blocks evolves into a chain of blocks (blockchain). In the Bitcoin world, these blocks contains often more than 500 transactions.

Block explorer: This is an explorer that can look up information in a blockchain and find all the information contained inside that block or specific transaction.

Block reward: When the miner successfully validates a new block, they get rewarded with a specific amount of digital assets regarding network rules of how many digital assets are released during each block mined.

B-Money: Anonymous, distributed electronic cash system created under the cypherpunk revolution. Satoshi Nakamoto referenced b-money in the Bitcoin whitepaper.

Candidate transactions: Transactions that have not been included yet in the proposal and remain contender transactions until they are included in the next round.

Censorship Resistance:. Being able to resist suppression of speech, communication, or other information on the basis that such material is considered objectionable, harmful, sensitive, or inconvenient to the entity using censorship. Cannot censor certain opinions or in blockchain, censor other miner, nodes or transactions.

Chain: This is a reference to the whole blockchain instance of blocks
linked together by previous hashes, and therefore the terminology is a chain.

Cryptocurrency: Is a digital or virtual currency that is secured by cryptography. Often decentralized networks based on blockchain technology commonly referred to as digital assets..

Consensus: A way for the blockchain system to collectively come to an agreement of the state of the blockchain and what transactions are included in the blocks.

Consensus models: A method for a blockchain to reach an agreement of the state of the network. Including transactions and who owns how much of which asset.

Consensus rules: The network predefines these rules. In the Bitcoin network, these rules can be:
- Transactions and blocks must be in the correct format
- Transactions output cannot be double-spending
- Blocks may only release a certain number of Bitcoin as a block reward

Data packets: Formatted data units represented in a container that travels along a given network path.

Decentralized autonomous organization(DAO): Is an organization represented by rules encoded as a computer program. It is transparent and controlled by shareholders and not influenced by a central government.

Decentralized: This is a process that activities are distributed or delegated away from a central group.

Decentralized applications (DAPPS): A digital application or computer program that runs on a distributed computing system instead of a single computer. Its not controlled by a single authority.

Denial-of-service (DoS): this is a cyber-attack where the penetrator seeks to make the machine or network resource unavailable to its indented users by temporarily or indefinitely disrupting services of a host connected to the internet.

Digital Asset: This is a more institutional and professional terminology for cryptocurrency. Consequently, a digital assets mostly combines the transfer and tracking of value sent through a network of a blockchain.

Distributed: Something that is shared among multiple systems, also often in different locations.

Distributed Ledger Technology (DLT): The technological infrastructure and protocols that allow simultaneous access, validation, and record updating in an immutable manner across a network spread across multiple entities or locations.

Double spending: When someone in the network tries to spend the same digital asset twice.

Elliptic Curve Digital Signature: One type of cryptography algorithms that ensures that funds can only be spent by the right owner. Including private key, public key, and signatures.

Escrow agreements (contracts): A agreement between two parties where a third party holds and regulates payment of the funds until specified conditions are met.

Externally Owned Account (EOA): A account controlled by a private key. If you own that private key, you have the ability to send ether (Ethereum's currency) and a message from the account.

Fiat currency: Is a government-issued currency that is not backed by a physical commodity (such as gold and silver).

Forgers: In the proof-of-stake consensus model, users who validate transactions and creates new blocks are referred to as forgers (not miners).

Forking: A condition where the state of the blockchain diverges into different chains, where one chain operates by different rules than the other.

Hash: This is a mathematical function that takes in an input and generates a deterministic output. These functions are unpredictable and one-way functions, in the sense that if you want to retrieve the input from the output, it is extremely difficult or impossible.

Hashcash: System to limit denial-of-service attacks and email spam created under the cypherpunk revolution. Satoshi Nakamoto referenced hashcash in the Bitcoin whitepaper.

Hashing power/hash rate: the number of hashes that can be calculated per second to try to solve the proof-of-work consensus.

Hash Timelocked Contract (HTLC): This is a type of smart contract. Recipients of a transaction have to acknowledge payments by creating cryptographic proof within a certain timeframe.

Header: Supplemental data placed at the beginning of a block of data being stored or transmitted withing the applied block.

Hexadecimal: Is a numeral system (16 symbols, base 16) like decimal (10 symbols, base 10). Hexadecimal uses decimal, plus six extra symbols.
Decimal: 0,1,2,3,4,5,6,7,8,9
Hexadecimal: 0,1,2,3,4,5,6,7,8,9,A(10),B(11),C(12),D(13),E(14),F(15)

Immutable: This is an object whose state CANNOT be modified after it is created.

IOU: This is a document that acknowledges a debt owed.

Know Your Customer (KYC): A guideline for professionals verify the identity, suitability, and risk involved with maintaining a business relationship.

Layer-1 (on-chain): is a term to describe the actual first layer protocol of the blockchain, which all nodes validate.

Layer-2 (off-chain): is a term to describe developments for blockchain technology that are built on top of the existing "layer 1" infrastructure. It is also referred to as off-chain" solutions

Ledger: A data structure which contains and various transactions and useful data, keeps track of accounts and transferred value, can also include state changes and so forth. Similar to blocks in blockhchains.

Liquidity: Describes the company's ability to convert its assets to cash in order to pay liabilities and the company's purchasing power.

Microtransactions: Refers to any digital currency transaction that is relatively small in value.

Merkle trees: A data structure represented in a tree where every leaf node is labeled with the cryptographic hash of a data block, and every non-leaf node is marked with the cryptographic hash in the labels of its child nodes.

Miners: Miners are hardware equipment used to solve the proof-of-work consensus. Miners can also be referred to as people involved in this mining process.

Mining pools: A gathering of resources to combine the hashing power into one mining entity that tries to mine the next block and distributes the reward and charges fees to be part of the mining pool.

Multi-signature: Refers to requiring more than one key to authorize a transaction. Analogy: On the house door, you may have multiple locks requiring different keys. Only with all of the keys, you can open the door and get access.

nBits/Target: Refers to the *target.* Target is a 256-bit unsigned integer (number) which a header hash must be equal to or below for this header to be part of a valid block added to the blockchain.

Node: Nodes can be any kind of devices (mostly computers, or even bigger servers). It is a point in the network where a transaction or message can be created, received, or transmitted. Nodes are connected to each other and constantly exchange the latest blockchain data.

Nonce: Nonce is an arbitrary number that can be used just once in a cryptographic communication. A 32-bit number which miners change to guess a hash which is lower than the target of the blockchain system to mine and append the next block in the chain.

Opcode: Is a portion of a machine language instruction that specifies the operation to be performed. It tells the computer to do something.

Opensource: is a decentralized software-development model that encourages open collaboration.

Payment channels: is a class of techniques designed to allow users to make multiple transactions without committing all of the transactions to the blockchain.

Payment orders: Payment orders are post-contract instruments often used to pay fee agreements to agents and usually contain conditions for the payment to be met, such as successful completion of contract requirements.

Peers: A member of the network which has equal status to all other members and shares the same responsibilities and has equal worth or quality.

Peer-to-peer (P2P): can be computing or networking systems, which is a distributed application architecture that partitions tasks or workloads between peers. These peers are equally privileged, equivalent participants in the application.

Private-key: This is part of asymmetric cryptography; this key is the first step to generate public keys with Elliptic curve functions and is used to sign transactions. Furthermore, it is used to prove ownership of funds and should be kept secret and not shared with anyone else but the owner.

Proof-of-Work (PoW): This is a consensus mechanism and the underlying consensus model of Bitcoin. It is preventing denial of service attacks by requiring some kind of work from the users, usually computer processing (mining).

Proof-of-Stake (PoS): This is a consensus mechanism based on the pseudo-random selection process to select the next block. Combination of factors that include staking age, node's wealth, and randomization.

Public-key: This is part of asymmetric cryptography, and the public key ensures that the owner of that address can receive funds. A public key is also used to ensure the integrity of the transaction. This key can be shared with everyone since it does not control the sending of funds.

RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160): A cryptographic hash function produces a 160-bit output. It is used in the Bitcoin address generation.

Smart contracts: A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of an agreement written in code.

Scaling: Scaling is used in digital assets to describe how many transactions per second the network can handle. Scaling up the network would equate to more transactions per second.

SHA-256: is a cryptographic hash algorithm and one-way compression function, which Bitcoin and other digital assets implement. It generates an almost unique 256-bit (32 bytes) signature of random text.

Spam attack: sending transactions or messages repeatedly with the intent to slow down the network. Therefore, transaction fees are present to mitigate users from spamming the network purposely.

Stablecoin: A stablecoin is a digital asset that is in simple terms stable. Mostly these stablecoins are dominated in a fiat currency like the Dollar, Euro, and so forth in order to mitigate drastic price fluctuations.

Target: This is a 256-bit number that all Bitcoin clients share. The target is in hexadecimal, but it is still a number. The SHA-256 hash of the block's header must be lower than or equal to the current target in order for the block to be accepted by the network. It regulates how fast new blocks gets mined.

Timestamps: Timestamps is a way to track time as running a total of seconds. The counter starts on the 1st January 1970 UTC, so every second passed since that date.

Transaction malleability: the ability of someone to change unconfirmed transactions without making them invalid, which changes the transaction ID making child transactions invalid.

Unique Node List (UNL): These are the list of transaction validators a given participant believes will not conspire to defraud them. These are regarded as trusted validators since they have proven themselves over a more extended time period to be trustworthy

Wallet/Digital wallet/e-wallet: A software, online service, or electronic device that allows electronic transactions with another party to exchange digital assets for other digital assets or goods and services.

Whitepaper: An academic paper that outlines the technology and goals of the project.

Validator(XRP): These are the safe guarders of the XRPL they relay cryptographically signed transaction, and maintain a local copy of the complete shared ledger history. These participate in the consensus process.

Validator(blockchain): Responsible for performing validation, by verifying transactions that are legitimate within a blockchain network.

21 Bibliography

[1] Newman, M. H. A. (1955). Alan Mathison Turing, 1912-1954.Retrieved from https://royalsocietypublishing.org/doi/pdf/10.1098/rsbm.1955.0019

[2] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[3] Lopp, J. (2016). Bitcoin and the Rise of the Cypherpunks. Retrieved from https://www.coindesk.com/the-rise-of-the-cypherpunks

[4] Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences Ii* (pp. 329-334). Springer, New York, NY.

[5] Institute, S. N. (2008). Bitcoin P2P e-cash paper. Retrieved from https://satoshi.nakamotoinstitute.org/emails/cryptography/6/#selection-35.2-37.59

[6] Asolo, B. (2018). Full Node and Lightweight Node. In. *Mycroptopedia*. Retrieved from https://www.mycryptopedia.com/full-node-lightweight-node/

[7] Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: the Works of Leslie Lamport* (pp. 203-226).

[8] Frankenfield, J. (2019). Double-Spending. Retrieved from https://www.investopedia.com/terms/d/doublespending.asp

[9] Hooda, P. Comparison - Centralized, Decentralized and Distributed. Retrieved from https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/

[10] Decentralization: A Sampling of Definitions, 1999, p. 13. Retrieved from http://web.undp.org/evaluation/documents/decentralization_working_report.pdf

[11] distributed systems. (n.d.) *McGraw-Hill Concise Encyclopedia of Engineering*. (2002). Retrieved April 8 2020 from https://encyclopedia2.thefreedictionary.com/distributed+systems

[12] WorldBank. Distributed Ledger Technology (DLT) and Blockchain. 2017. Retrieved from. http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

[13] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

[14] Technical background of version 1 Bitcoin adresses. (2019). In. *Bitcoin Wiki*. Retrieved from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

[15] Paul, E. (2017). What is Digital Signature- How it works, Benefits, Objectives, Concept. Retrieved from https://www.emptrust.com/blog/benefits-of-using-digital-signatures

[16] Bitcoin. (2020) Wallets. Retrieved from https://bitcoin.org/en/wallets-guide#introductions

[17] Ledger (Producer). (2020). Ledger Nano X. Retrieved from https://cdn.shopify.com/s/files/1/2974/4858/products/ledger-nano-x-stand-up_grande_7a016731-824a-4d00-acec-40acfdfed9dc_large.png?v=1573828954

[18] Hackernoon. (2019). Centralized vs Decentralized Cryptocurrency exchanges. Retrieved from. https://hackernoon.com/centralized-vs-decentralized-cryptocurrency-exchanges-explained-simply-639411ecb452

[19] PwC. (2013). [PDF]. Know Your Customer: Quick Reference Guide. Retrieved from https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf

[20] Finra. Anti-Money Laundering (AML). Retrieved from https://www.finra.org/rules-guidance/key-topics/aml

[21] Bitcoinik. (2019). Blockchain Version 1.0, 2.0, 3.0 And Future. Retrieved from https://bitcoinik.com/blockchain-evolution-1-0-to-3-0/

[22] Technopedia. Directed Acyclic Graph (DAG) Retrieved from https://www.techopedia.com/definition/5739/directed-acyclic-graph-dag

[23] Technologies, S. (2018). Blockchain 3.0 & The Future of the Decentralized. Retrieved from https://medium.com/@saratechnologiesinc/blockchain-3-0-the-future-of-the-decentralized-internet-63ba199e2a5

[24] VISA Fact Sheet. (2019). Retrieved from VISA: https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-fact-sheet-july-2019.pdf

[25] Bitcoin. (2020). Blockchain. Retrieved from https://bitcoin.org/en/developer-reference#block-chain

[26] Block. (2019). ln *Bitcoin* Wiki. Retrieved from https://en.bitcoin.it/wiki/Block?fbclid=IwAR3HH6Bd0W-pZz82TSVXwjZE5_PJ-peDGS5JnDJJGy2juVBmQFRAW9q5SjU

[27] Merkle Tree. *Brilliant.org*. Retrieved 16:42, February 14, 2020, from https://brilliant.org/wiki/merkle-tree/

[28] Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018, December). A comparative analysis of DAG-based blockchain architectures. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 27-34). IEEE.

[29] Back, A. (2002). Hashcash-a denial of service counter-measure.

[30] Fortney, L. (2019). Bitcoin Mining, Explained. Retrieved from https://www.investopedia.com/terms/b/bitcoin-mining.asp

[31] Bitcoin. (2020). Target nBits. Retrieved from https://bitcoin.org/en/developer-reference#target-nbits

[32] Blockchain (Producer). (2020). Network Difficulty. Retrieved from https://www.blockchain.com/charts/difficulty?timespan=all

[33] Blockchain (Producer). (2020). Hash Rate. Retrieved from https://www.blockchain.com/charts/hash-rate?timespan=all

[34] FPGA. (2015). ln *BitcoinWiki*. Retrieved from https://en.bitcoin.it/wiki/FPGA

[35] Smith, M. J. S. (1997). *Application-specific integrated circuits* (Vol. 7, pp. 1-1). Reading, MA: Addison-Wesley.

[36] Eyal, I., & Sirer, E. G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436-454). Springer, Berlin, Heidelberg.

[37] Karamat, S. (2018). What is a mining pool? Retrieved from https://coinrivet.com/guides/what-is-cryptocurrency-mining/what-is-a-mining-pool/

[38] Blockchain (Producer). (01/05/2020). Hashrate Distribution. Retrieved from https://www.blockchain.com/pools?timespan=24hours

[39] Buterin, V. (2017). Minimal Slashing Conditions. Retrieved from https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c

[40] Weaknesses. (2018). *Attacker has a lot of computing power*. ln *BitcoinWiki*. Retrieved from https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

[41] Proof of Stake Explained. (n.d). Retrieved from Binance Academy: https://www.binance.vision/blockchain/proof-of-stake-explained

[42] Ray, S. (2017). What is Proof of Stake. Retrieved from https://hackernoon.com/what-is-proof-of-stake-8e0433018256

[43] Martinez, J. (2018). Understanding Proof of Stake: The Nothing at Stake Theory. Retrieved from https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

[44] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297-315). Springer, Cham.

[45] Ray, J. (2018). Problems. *Proof of Stake.* Retrieved from https://github.com/ethereum/wiki/wiki/Problems

[46] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297-315). Springer, Cham.

[47] Cohen, D., Schwartz, D., & Britto, A. (n.d). Consensus. Retrieved from https://xrpl.org/consensus.html

[48] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/anatomy-of-a-ledger-complete.png

[49] Ripple. (2020). XRP. Retrieved from https://ripple.com/xrp

[50] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/xrp-ledger-network.png

[51] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-rounds.png

[52] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-calculate-validation.png

[53] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-declare-validation.png

[54] Hards Forks and Soft Forks. (n.d). Retrieved from Binance Academy: https://www.binance.vision/blockchain/hard-forks-and-soft-forks

[55] Buterin, V. (2013). Ethereum white paper. *GitHub repository*, *1*, 22-23.

[56] What is Ethereum? (2020). Retrieved from Ethereum: https://ethereum.org/what-is-ethereum/

[57] Base, K. (2019). What is gas? Retrieved from https://support.mycrypto.com/general-knowledge/ethereum-blockchain/what-is-gas

[58] district0x. What is Gas. Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-gas/

[59] Szabo, N. (2018). Smart Contracts: Building Blocks for Digital Markets.

[60] Bahga, A., & Madisetti, V.K. (2016). Blockchain Platform for Industrial Internet of Things

[61] Solidity. (n.d). *Documentation*. Retrieved from Solidity: https://solidity.readthedocs.io/en/v0.6.2/

[62] Antonopoulos, A. M., & Nugent, T. (2020). Ethereum Book. Retrieved from https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc#what-is-a-smart-contract

[63] Sillaber, Christian & Waltl, Bernhard. (2017). Life Cycle of Smart Contracts in Blockchain Ecosystems. Datenschutz und Datensicherheit - DuD. 41. 497-500. 10.1007/s11623-017-0819-7.

[64] What is the «Unstoppable World Computer»?. (n.d) Retrieved from Bitrates: https://www.bitrates.com/guides/ethereum/what-is-the-unstoppable-world-computer

[65] district0x. Ethereum vs. Ether. Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-gas/

[66] district0x. The Role of Tokens. Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-gas/

[67] Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business*, *100*, 64-75.

[68] Nonninger, L. (2018). Block.One just raised aq $4 billion ICO Retrieved from https://www.businessinsider.com/blockone-raises-4-billion-ico-2018-6?r=US&IR=T

[69] Vogelsteller, F., & Buterin, V. (2019). EIP20: ERC-20 Token Standars. Retrieved from https://eips.ethereum.org/EIPS/eip-20

[70] district0x. What is an ERC20 Token? Retrieved from https://education.district0x.io/general-topics/understanding-ethereum/what-is-an-erc20-token/

[71] Transaction Cost. (n.d) Retrieved from XRP Ledger: https://xrpl.org/transaction-cost.html

[72] XRP Distribution. (2015). Retrieved from Ripple Labs: https://web.archive.org/web/20150806120942/https:/www.ripplelabs.com/xrp-distribution/

[73] Quora. David Schwartz. Retrieved from. https://www.quora.com/What-is-the-difference-between-XRP-XRP-Ledger-and-Ripple?share=1

[74] Thomas, S., & Schwartz, E. (2015). A protocol for interledger payments. URL https://interledger. org/interledger. pdf.

[75] Wikipedia. (2020). Ledger. Retrieved from https://en.wikipedia.org/wiki/Ledger

[76] Interledger Architecture. (n.d). Retrieved from Interledger: https://interledger.org/rfcs/0001-interledger-architecture/

[77] Interledger Overview. (n.d). Retrieved from Interledger: https://interledger.org/overview.html

[78] Leopold, S. J., & Englesson, N. (2017). How Eco friendly is our money and is there an alternative? Retrieved from http://papers.netrogenic.com/sid/eco-friendly-money.pdf

[79] Validator Registry. Retrieved 17 February 2020 from XRP Charts: https://xrpcharts.ripple.com/#/validators

[80] Market Performance. Retrieved 19 May 2020 from Ripple: https://ripple.com/xrp/market-performance

[81] Leopold, S. J., & Englesson, N. (Producer). (2017). Eco-Friendly Currencies. Retrieved from https://www.stedas.hr/ripple/Eco-friendly-cryptocurrency.pdf

[82] Scalability. (2019). In *BItcoinWiki*. Retrieved from https://en.bitcoin.it/wiki/Scalability

[83] Blockchain (Producer). (2020). Fees Per Transaction (USD). Retrieved from https://www.blockchain.com/charts/cost-per-transaction?timespan=all

[84] Bitinfocharts. (Producer). Ethereum average transaction fee. Retrieved from. https://bitinfocharts.com/comparison/ethereum-transactionfees.html

[85] BitcoinWiki. (2018) Conformation. Retrieved from https://en.bitcoin.it/wiki/Confirmation

[86] Blockchain (Producer). (2020). Median Confirmation Time. Retrieved from https://www.blockchain.com/charts/median-confirmation-time?timespan=2years

[87] Etherscan. (Producer). (2020). Ethereum Average Block Time Chart. Retrieved from https://etherscan.io/chart/blocktime

[88] Market Performance. (n.d). *XRP Market Metrics*. Retrieved from https://ripple.com/xrp/market-performance/

[89] Segregated Witness Proposal. (2018). *GitHub repository, Bitcoin/bips/BIP 141.* Retrieved from https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[90] Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

[91] LND Overview and Developer Guide. (n.d). Retrieved from Lightning Network Developers: https://dev.lightning.community/overview/

[92] Webb, N. (2018). A Fork in the Blockchain: Income Tax and the Bitcoin/Bitcoin Cash Hard Fork. *North Carolina Journal of Law & Technology, 19*(4), 283.

[93] Stark, J. (2018). Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit. Retrieved from https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

[94] What is the Raiden Network. (2018). Retrieved from Raiden Network: https://raiden.network/101.html

[95] Jordan, R. (2018). How to Scale Ethereum: Sharding Explained. Retrieved from https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce

[96] Buterin, V., & Poon, J. (2017). Plasma: Scalable Autonomous Smart Contracts. Retrieved from https://plasma.io/plasma-deprecated.pdf

[97] Andrews, E. (2019). Who Invented the internet? Retrieved from https://www.history.com/news/who-invented-the-internet

[98] FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

[99] Zug. (2019). ln *Bitcoin Wiki.* Retrieved from https://en.bitcoinwiki.org/wiki/Zug

[100] Our Story. (n.d). Retrieved from Crypto Valley: https://cryptovalley.swiss/about-the-association/

[101] FINMA publishes ICO guidelines. (2018). Retrieved from FINMA: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[102] Monetary Authority of Singapore. (2019). A GUIDE TO DIGITAL TOKEN OFFERINGS [PDF FILE]. Retrieved from https://www.mas.gov.sg/-/media/MAS/Sectors/Guidance/Guide-to-Digital-Tokens-Offering---23-Dec-2019.pdf

[103] Allison, I. (2020). Singapore Announces New AML Rules for Crypto Businesses. Retrieved from https://www.coindesk.com/singapore-announces-new-aml-rules-for-crypto-businesses

[104] Zhang, L. (2017). China: Regulators Ban Companies from Raising Money Through Virtual Currencies. Retrieved from https://www.loc.gov/law/foreign-news/article/china-regulators-ban-companies-from-raising-money-through-virtual-currencies/

[105] Press Release, Finanstilsynet, Finanstilsynet advarer forbrukere om kryptovaluta [Financial Supervisory Authority Warns Users on Cryptocurrencies] (Feb. 28, 2018). Retrieved from https://www.finanstilsynet.no/markedsadvarsler/2018/finanstilsynetadvarer-forbrukere-om-kryptovaluta/

[106] Norges Bank [Central bank of Norway]. Utfyllende Etiske Regler for Ansatte i Norges sentralbankvirksomhet [Additional Ethical Rules for Employees of Norway's Central Bank] (28. Nov 2018). Retrieved from https://www.norges-bank.no/tema/Om-Norges-Bank/samfunnsoppdrag/Lover-regelverk/Utfyllende-etiske-regler/

[107] Skatteetaten [The Norwegian Tax Administration] (2020). Kjøp av virtuell valuta. [Purchase of virtual currency] Retrieved from https://www.skatteetaten.no/person/skatt/hjelp-til-riktig-skatt/aksjer-og-verdipapirer/om/virtuell-valuta/kjop/

[108] Skatteetaten. [The Norwegian Tax Administration] (2020). Tax and VAT relating to Bitcoin and other virtual currencies. Retrieved from https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies/

[109] Tiwari, A. (2019). All you Need to Know about the Token Taxonomy Act. Retrieved from https://btcmanager.com/all-you-need-to-know-about-the-token-taxonomy-act/

[110] GPO (Authenticated U.S. Government Information). H.R.2144 - Token Taxonomy Act of 2019. Published April 9, 2019 [PDF FILE]

[111] Brett, J. (2020). Congress Has Now Introduced 32 Crypto And Blockchain Bills. Retrieved from https://www.forbes.com/sites/jasonbrett/2020/04/28/congress-has-introduced-32-crypto-and-blockchain-bills-for-consideration-in-2019-2020/?fbclid=IwAR3dh5z4Q9e8njGWxVeKHrkXphEqNL7bv9wVb-0kg3RFnYgn0haqZ6PwN54

[112] Wikipedia (Producer). (2020) Libra. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/4/4b/Libra_logo.svg/2880px-Libra_logo.svg.png

[113] David, M. (2019). HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS. Retrieved from https://www.banking.senate.gov/imo/media/doc/Marcus%20Testimony%207-16-19.pdf?utm_campaign=BitDigest&utm_medium=email&utm_source=Revue+newsletter

[114] Meyer, B. S. (2019). Facebook's Libra faces eurozone backlash. Retrieved from Politico: https://www.politico.eu/article/facebook-libra-faces-eurozone-backlash/

[115] Feiner, L. (2019). Facebook's libra cryptocurrency coalition is falling apart as eBay, Visa, Mastercard and Stripe jump ship. Retrieved from CNBC: https://www.cnbc.com/2019/10/11/ebay-drops-out-of-facebook-libra-cryptocurrency-one-week-after-paypal.html

[116] An Introduction to Libra. (n.d). Retrieved from The Libra Association: https://libra.org/en-US/white-paper/

[117] The Libra Blockchain. (2019). Retrieved from Libra: https://developers.libra.org/docs/assets/papers/the-libra-blockchain/2019-09-26.pdf

[118] Orlowski, A. (2010). Facebook founder called trusting users dumb f*cks. Retrieved from The Register: https://www.theregister.co.uk/2010/05/14/facebook_trust_dumb/

[119] Wikipedia (Producer). (2020). Coinbase. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/1/1a/Coinbase.svg/2880px-Coinbase.svg.png

[120] About Coinbase. Retrieved from https://www.coinbase.com/about

[121] Chaparro, F. (2018). Bitcoin exchange Coinbase reportedly made more than $1 billion in revenues last year. Retrieved from https://www.businessinsider.com/coinbase-reportedly-made-more-than-1-billion-in-revenues-last-year-2018-1?r=US&IR=T

[122] Kauflin, J. (2020). The 10 Biggest Fintech Companies In America 2020. Retrieved from https://www.forbes.com/sites/jeffkauflin/2020/02/12/the-10-biggest-fintech-companies-in-america-2020/#289949fa1259

[123] Wikipedia (Producer). (2020). Coinbase. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/1/12/Binance_logo.svg/2880px-Binance_logo.svg.png

[124] Binance Overview. (n.d). Retrieved from Crunchbase: https://www.crunchbase.com/organization/binance#section-overview

[125] Bitmain (2020). ln *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Bitmain

[126] Madore, P. H. (Producer). (2019). Bitcoin Mining Giant Bitmain Launches New Chip, Hints at New Miners. Retrieved from https://www.ccn.com/wp-content/uploads/2018/11/bitmain.jpg

[127] Forbes. Bitmain. 2018. Retrieved from. https://www.forbes.com/sites/pamelaambler/2018/08/17/all-you-need-to-know-about-crypto-mining-phemon-bitmain/#4c76f67b580f

[128] Wikipedia (Producer). (2020). Ripple. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/8/88/Ripple_logo.svg/2880px-Ripple_logo.svg.png

[129] RippleLabs. (2019). Ln *BitcoinWiki.* Retrieved from https://en.bitcoinwiki.org/wiki/Ripple_(company)

[130] Our Company. (2020). Retrieved from Ripple: https://ripple.com/company

[131] Gartner (Producer). (2019). Gartner's Hype Cycle for Blockchain Business. Retrieved from https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/Blockchain-HC-2019.png

[132] Hameda, A. (Producer). (2017). OSI Model. Retrieved from https://abdulazizhameda.files.wordpress.com/2017/02/osi-model-table.png?w=1166

[133] Bora, G., Bora, S., Singh, S., & Arsalan, S. M. (2014). OSI reference model: An overview. *International Journal of Computer Trends and Technology (IJCTT)*, *7*(4), 214-218.

[134] Thomas, S., & Scwartz, E. A Protocol for Interledger Payments. Retrieved from https://interledger.org/interledger.pdf

[135] Swift. (2020). ln *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

[136] Messaging and Standars. Retrieved from Swift: https://www.swift.com/about-us/discover-swift/messaging-standards

[137] Maverick, J. B. (2019). Nostro Account vs. Vostro Account: What's the Difference? Retrieved from https://www.investopedia.com/ask/answers/051815/what-difference-between-nostro-and-vostro-account.asp

[138] HSBC. (2020). International Payments. Retrieved from https://www.hsbc.co.uk/international/money-transfer/

[139] Barclays. What are the timescales for sending international payments? Retrieved from https://ask.barclayswealth.com/help/ukprivatebank/wealth-online/payments/payment-timescales

[140] TransferWise. (2018). Western Union money transfer fees: A full overview. Retrieved from https://transferwise.com/us/blog/western-union-fees

[141] WesternUnion. (Producer) Fee Table. Retrieved from https://www.westernunion.com/content/dam/wu/EU/EN/feeTableRetailEN-ES.PDF

[142] Ripple (Producer). (2020). On-demand liquidity. Retrieved from https://ripple.com/wp-content/uploads/2019/09/XRP-Graphic.png

[143] Dallasnews. (2010). MoneyGram chooses downtown Dallas for new headquarters. Retrieved from https://www.dallasnews.com/news/2010/09/24/moneygram-chooses-downtown-dallas-for-new-headquarters/

[144] *MoneyGram and Ripple discuss XRP*. (2019). Paper presented at the Swell Conference. https://www.youtube.com/watch?v=yrezhEfUt4E

[145] TheWorldBank. (2018). Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows [Press release]. Retrieved from https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows

[146] Donovan, F. (2018). 1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018. Retrieved from https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018

[147] IMB. (2019) IBM Food Trust. Retrieved from https://www.ibm.com/blockchain/solutions/food-trust

[148] Sentiman. (2018). E-Voting and Blockchain. Retrieved from https://www.sentiman.io/wp-content/uploads/2018/08/e-voting-and-blockchain-1.png

[149] Barontini, C., & Holden, H. (2019). Proceeding with caution-a survey on central bank digital currency. *Proceeding with Caution-A Survey on Central Bank Digital Currency (January 8, 2019). BIS Paper*, (101).

[150] Griffoli, M. T. M., Peria, M. M. S. M., Agur, M. I., Ari, M. A., Kiff, M. J., Popescu, M. A., & Rochon, M. C. (2018). *Casting Light on Central Bank Digital Currencies*. International Monetary Fund.

[151] Riksbank, S. (2020). The Riksbank to test technical solution for the e-krona. Retrieved from https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2020/the-riksbank-to-test-technical-solution-for-the-e-krona/

[152] Accenture (Producer). (2020). Conceptual architecture for the e-krona pilot. Retrieved from https://www.riksbank.se/imagevault/publishedmedia/327ame3mfehgr0qvkg30/Riksbankens-e-krona_ENG.png

[153] Bech, M. L., & Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review September*.

[154] Bech, M. L., & Garratt, R. (Producer). (2017). Central Bank Cryptocurrencies. Retrieved from https://www.bis.org/publ/arpdf/ar2018e/images/graph-V1.jpg

[155] Adrian, T., & Griffoli, T. M. (2019). Central Bank Digital Currencies Retrieved from https://blogs.imf.org/2019/12/12/central-bank-digital-currencies-4-questions-and-answers/

[156] Zhang, T. (2020). Deputy Managing Director Tao Zhang's Keynote Address on Central Bank Digital Currency. Retrieved from https://www.imf.org/en/News/Articles/2020/03/19/sp031920-deputy-managing-director-tao-zhangs-keynote-address-on-central-bank-digital-currency

[157] Auer, R., Cornelli, G., & Frost, J. (2020). Covid-19, cash, and the future of payments. ISSN:2708-0420. Retrieved from https://www.bis.org/publ/bisbull03.pdf

[158] van Doremalen, N, T Bushmaker, D Morris, M Holbrook, A Gamble, B Williamson, A Tamin, J Harcourt, N Thornburg, S Gerber, J Lloyd-Smith, E de Wit and V Munster (2020): "Aerosol and surface stability of SARSCoV-2 as compared with SARS-CoV-1", NEJM.org, March.

[159] Chen, J. (2020). Inflation. Retrieved from https://www.investopedia.com/terms/i/inflation.asp

[160] U.S. Bureau of Labor Statistics, Consumer Price Index for All Urban Consumers: Purchasing Power of the Consumer Dollar in U.S. City Average [CUUR0000SA0R], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/CUUR0000SA0R, April 7, 2020.

[161] Board of Governors of the Federal Reserve System (US), M2 Money Stock [M2], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/M2, April 7, 2020.

[162] Board of Governors of the Federal Reserve System (US), M1 Money Stock [M1], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/M1, April 7, 2020.

[163] Supply and Demand. (2019). In Encyclopedia Britannica: The Editors of Encyclopedia Britannica.Retrieved from https://www.britannica.com/topic/supply-and-demand

[164] St. Louis federal reserve bank. *Functions of Money* [Retrieved from https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money

[165] Chen, J. (2019). Bretton Woods Agreement and System. Retrieved from https://www.investopedia.com/terms/b/brettonwoodsagreement.asp

[166] Sandra, G. (2013). Nixon ends convertibility of US dollars to gold and announces wage/price controls. Retrieved from. https://www.federalreservehistory.org/essays/gold_convertibility_ends

[167] Farley, A. (2019). Understanding the Correlation of Oil and Currency. Retrieved from https://www.investopedia.com/articles/forex/092415/oil-currencies-understanding-their-correlation.asp

[168] Kenton, W. (2020). Hyperinflation. Retrieved from https://www.investopedia.com/terms/h/hyperinflation.asp

[169] Llewellyn, J., & Thompson, S. (2019). The hyperinflation of 1923. Retrieved from https://alphahistory.com/weimarrepublic/1923-hyperinflation/

[170] Logarithmic chart of German Hyperinflation. Based on the values in Table IV (page 441) of The Economics of Inflation by Costantino Bresciani-Turroni, published 1937. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/4/4f/Germany_Hyperinflation.svg/1920px-Germany_Hyperinflation.svg.png

[171] OPEC Share of World Crude Oil Reserves. (2018). Retrieved from https://www.opec.org/opec_web/en/data_graphs/330.htm

[172] J.Kiger, P. (2019). How Venezuela Fell From the Richest Country in South America into Crisis. Retrieved from https://www.history.com/news/venezuela-chavez-maduro-crisis

[173] IMF. Inflation rate, average consumer prices. Retrieved from https://www.imf.org/external/datamapper/PCPIPCH@WEO/WEOWORLD/VEN

[174] Petro Whitepaper. (2018). [PDF] Retrieved from https://www.petro.gob.ve/files/petro-whitepaper-english.pdf

[175] Bloomberg. (2018). President Trump Bans U.S. Citizens From Buying Venezuelan Cryptocurrency Petro. Retrieved from https://fortune.com/2018/03/19/donald-trump-cryptocurrency-venezuela/

[176] Coindance (2020). Venezuela Local Bitcoins Volume. [April 9th, 2020] Retrieved from https://coin.dance/volume/localbitcoins/VES

[177] World Gold Council. How much gold has been mined?. Retrieved from https://www.gold.org/about-gold/gold-supply/gold-mining/how-much-gold

[178] Goldprice. (14th May 2020) Retrieved from https://goldprice.org

[179] Coinmarketcap. (14th May 2020. Retrieved from https://coinmarketcap.com

22 Bibliography attachments

[Figure 12] Ledger (Producer). (2020). Ledger Nano X. Retrieved from https://cdn.shopify.com/s/files/1/2974/4858/products/ledger-nano-x-stand-up_grande_7a016731-824a-4d00-acec-40acfdfed9dc_large.png?v=1573828954

[Figure 18] Blockchain (Producer). (2020). Difficulty. Retrieved from https://www.blockchain.com/charts/difficulty?timespan=all

[Figure 19] Blockchain (Producer). (2020). Hash Rate. Retrieved from https://www.blockchain.com/charts/hash-rate?timespan=all

[Figure 20] Blockchain (Producer). (2020). Hashrate Distribution. Retrieved from https://www.blockchain.com/pools?timespan=24hours

[Figure 21] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/anatomy-of-a-ledger-complete.png

[Figure 22] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/xrp-ledger-network.png

[Figure 23] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-rounds.png

[Figure 24] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-calculate-validation.png

[Figure 26] Cohen, D., Schwartz, D., & Britto, A. (Producer). (2020). Consensus. Retrieved from https://xrpl.org/img/consensus-declare-validation.png

[Figure 31,32,33] Leopold, S. J., & Englesson, N. (Producer). (2017). Eco-Friendly Currencies. Retrieved from https://www.stedas.hr/ripple/Eco-friendly-cryptocurrency.pdf

[Figure 35] Blockchain (Producer). (2020). Fees Per Transaction (USD). Retrieved from https://www.blockchain.com/charts/cost-per-transaction?timespan=all

[Figure 36] Bitinfocharts. (Producer). Ethereum average transaction fee. Retrieved from. https://bitinfocharts.com/comparison/ethereum-transactionfees.html

[Figure 38] Blockchain (Producer). (2020). Median Confirmation Time. Retrieved from https://www.blockchain.com/charts/median-confirmation-time?timespan=2years

[Figure 39] Etherscan. (Producer). (2020). Ethereum Average Block Time Chart. Retrieved from https://etherscan.io/chart/blocktime

[Figure 44] Brett, J. (2020). Congress Has Now Introduced 32 Crypto And Blockchain Bills. Retrieved from https://www.forbes.com/sites/jasonbrett/2020/04/28/congress-has-introduced-32-crypto-and-blockchain-bills-for-consideration-in-2019-2020/?fbclid=IwAR3dh5z4Q9e8njGWxVeKHrkXphEqNL7bv9wVb-0kg3RFnYgn0haqZ6PwN54

[Figure 45] Wikipedia (Producer). (2020) Libra. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/4/4b/Libra_logo.svg/2880px-Libra_logo.svg.png

[Figure 46] Wikipedia (Producer). (2020). Coinbase. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/1/1a/Coinbase.svg/2880px-Coinbase.svg.png

[Figure 47] Wikipedia (Producer). (2020). Binance. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/1/12/Binance_logo.svg/2880px-Binance_logo.svg.png

[Figure 48] Madore, P. H. (Producer). (2019). Bitcoin Mining Giant Bitmain Launches New Chip, Hints at New Miners. Retrieved from https://www.ccn.com/wp-content/uploads/2018/11/bitmain.jpg

[Figure 49] Wikipedia (Producer). (2020). Ripple. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/8/88/Ripple_logo.svg/2880px-Ripple_logo.svg.png

[Figure 51] Gartner (Producer). (2019). Gartner's Hype Cycle for Blockchain Business. Retrieved from https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/Blockchain-HC-2019.png

[Figure 52] Hameda, A. (Producer). (2017). OSI Model. Retrieved from https://abdulazizhameda.files.wordpress.com/2017/02/osi-model-table.png?w=1166

[Figure 54] Ripple (Producer). (2020). On-demand liquidity. Retrieved from https://ripple.com/wp-content/uploads/2019/09/XRP-Graphic.png

[Figure 55] Sentiman. (2018). E-Voting and Blockchain. Retrieved from https://www.sentiman.io/wp-content/uploads/2018/08/e-voting-and-blockchain-1.png

[Figure 56] Accenture (Producer). (2020). Conceptual architecture for the e-krona pilot. Retrieved from https://www.riksbank.se/imagevault/publishedmedia/327ame3mfehgr0qvkg30/Riksbankens-e-krona_ENG.png

[Figure 57] Bech, M. L., & Garratt, R. (Producer). (2017). Central Bank Cryptocurrencies. Retrieved from https://www.bis.org/publ/arpdf/ar2018e/images/graph-V1.jpg

[Figure 58] U.S. Bureau of Labor Statistics, Consumer Price Index for All Urban Consumers: Purchasing Power of the Consumer Dollar in U.S. City Average [CUUR0000SA0R], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/CUUR0000SA0R, April 7, 2020.

[Figure 59] Board of Governors of the Federal Reserve System (US), M2 Money Stock [M2], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/M2, April 7, 2020.

[Figure 60] Logarithmic chart of German Hyperinflation. Based on the values in Table IV (page 441) of The Economics of Inflation by Costantino Bresciani-Turroni, published in 1937. Retrieved from https://upload.wikimedia.org/wikipedia/commons/thumb/4/4f/Germany_Hyperinflation.svg/1920px-Germany_Hyperinflation.svg.png

[Figure 61] Coindance (2020). Venezuela Local Bitcoins Volume. [April 9th, 2020] Retrieved from https://coin.dance/volume/localbitcoins/VES