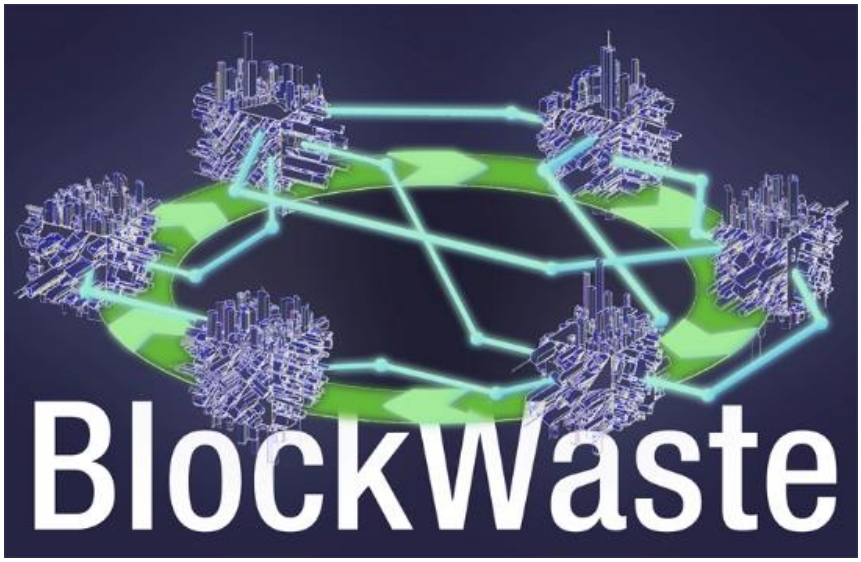
O1.A3. Handbooks of Circular Economy strategies applied to Municipal Waste Management using Blockchain technologies

Handbook 2: Blockchain



This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Consortium members: National Technical University of Athens (NTUA), Stichting Saxion (SAXION), Asociación Empresarial de Investigación Centro Tecnológico del Mármol, Piedra y Materiales (CTM), Tallinna Tehnikaulikool (TalTech), Fachhochschule Bielefeld (Fh-Bielefeld)

Output factsheet:

Funding Programme	Erasmus+ Programme of the European Union
Funding NA	EL01 Greek State Scholarship's Foundation (IKY)
Project full title	Innovative training based on Blockchain technology applied to waste management - BLOCKWASTE
Field	KA2 - Cooperation for innovation and the exchange of good practices KA203 - Strategic Partnerships for higher education
Project Number	2020-1-EL01-KA203-079154
Project Duration	24 months
Project Start Date	01-10-2020
Project End Date:	30-09-2022

Output details:

Output title: O1: Learning materials for interdisciplinary Blockchain-MSW

Task Title: O1/A3. Handbooks of Circular Economy strategies applied to Municipal Waste Management using Blockchain technology

Output leader: NTUA

Task leader: Saxion UAS

Contents

Index of Figures

1 Introduction

1.1 Brief project description

The BlockWASTE project aims to address the interoperability between waste management and blockchain technology and promote its proper treatment through educational training, so that the data collected will be shared within a safe environment, where there is no room for uncertainty and mistrust between all parties involved. For this purpose, the objectives of BlockWASTE project are as follows:

- To conduct research on solid waste generated in cities and how it is managed, so that it can be used to create an information base of good practices, in order to reintroduce waste into the value chain, promoting the idea of Intelligent Circular Cities.
- To identify the benefits of the Blockchain Technology within the municipal waste management (MSW) process.
- To create a study plan that allows the training of teachers and professionals of organizations and companies of the sector, in the overlap of the fields of Waste Management, Circular Economy and Blockchain Technology.
- To develop an interactive tool based on Blockchain Technology, which will make it possible to put into practice the management of data obtained from urban waste, thus visualizing the way in which the data is implemented in the Blockchain and enabling users to evaluate different forms of management

BlockWASTE aims to implement transnationally new educational contents with the goal of training its students in the partner countries and providing them with the necessary basic skills that allow them to act professionally as future workers in the sector, adding digital competences required by companies that are embracing the process of digital transformation. In this sense, the project is addressed to:

- Enterprises and SMEs, IT professionals, urbanisms and waste management professionals.
- Universities (professors, students and researchers).
- Public bodies

The project includes four Intellectual Outputs as follows:

- O1. Learning materials for interdisciplinary Blockchain-MSW
- O2. European common curriculum on MSW applying Blockchain technologies to Circular Economy strategies
- O3. E-Learning tool based-on Blockchain-MSW focused on Circular Economy
- O4. BlockWASTE Open Educational Resource (OER)

1.2 Objectives of the document

This document describes and explains the basic principles of Blockchain. It describes what Blockchain is, when you can use it, what components a Blockchain is made up of, what Blockchain technologies are used and it gives a description of various successful Blockchain applications.

2 Blockchain Fundamentals

Understanding blockchain principles through Bitcoin

"Sorry to be a wet blanket. Writing a description for this thing for general audiences is bloody hard. There's nothing to relate it to."
- Satoshi Nakamoto (2010)

2.1 Introduction and learning objectives

Learning objectives

- Blockchain at the most basic level by looking at Bitcoin.
- Blockchain is essentially a distributed ledger in which you can store data.
- The differences between a blockchain network and a centralized network.

Introduction

On October 31, 2008, an email was sent under the name Satoshi Nakamoto to the Cryptography mailing list.[1] The email included a reference to a **white paper** entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*. The white paper he attached to the announcement is a mere 9 pages long document, outlining the technical workings of Bitcoin. This system makes it possible to send online payments to other parties, without the need of a financial institution.

The main features of this payment system, according to Satoshi:

1. Double-spending is prevented with a peer-to-peer network.
2. No mint or other trusted parties.
3. Participants can be anonymous.
4. New coins are made from Hashcash style proof-of-work.
5. The proof-of-work for new coin generation also powers the network to prevent double-spending.

Technical terms like double-spending, peer-to-peer network, Proof-of-Work, Hashcash, timestamps, hashing, and digital signatures in the email make it difficult for the general public to understand Bitcoin or more generally blockchain. Especially, at the time, when there was nothing to relate it to for most people. In this chapter, we discuss Bitcoin as the means to understand basic blockchain principles.

[1] The original email can be found at: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

2.1.1 Bitcoin vs bitcoin

We generally make a distinction between (lower case) bitcoin, the digital money also called a cryptocurrency, and (upper case) Bitcoin, the underlying financial network that allows bitcoins to be sent and received.

2.1.2 Peer-to-peer network

The computers, also called ***nodes***, that run this financial network hold and have access to a ledger unto which all bitcoin transactions are recorded. This Bitcoin ledger is a record of all valid transactions that have ever been transmitted to the network, which is the underlying infrastructure that consists of the nodes that keep track of, validate, and timestamp all the bitcoin transactions. We call this network a ***peer-2-peer (P2P) network***.

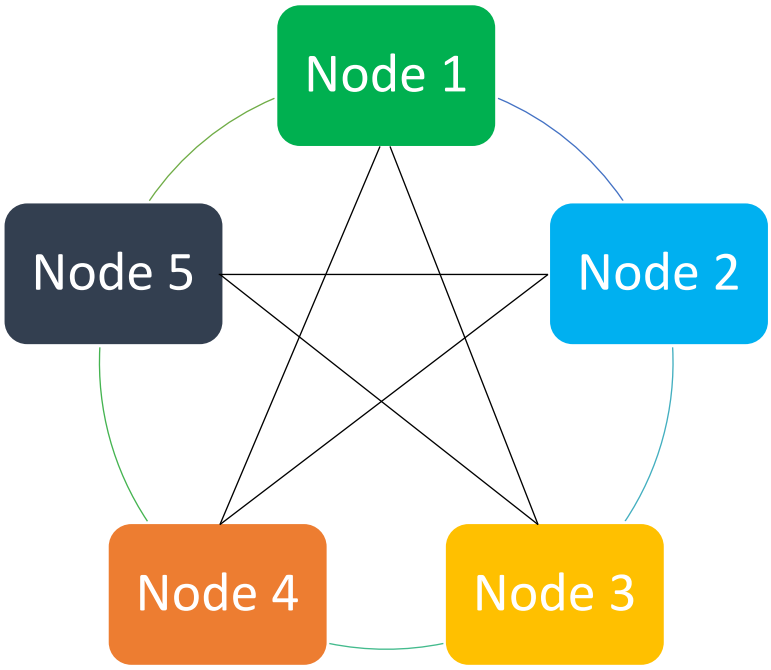


Figure 1: A representation of a distributed network, where the blockchain is distributed over a network of full nodes (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 1, page 14).

A P2P network is a network of nodes, often a computer, that are equally privileged. Each node can be a service provider, as well as a service consumer. Everyone has access to the Bitcoin network and is free to manage a node on the network. Specialized nodes on the network, also called ***full nodes***, keep the entire transaction history. To take down the whole network and its corresponding transaction history, one would have to shut down all the nodes, which is nearly impossible when the network consists of many nodes.

Every participant within the network follows the Bitcoin protocol. The Bitcoin protocol is the procedural rules that govern the Bitcoin network. In addition, there is no intermediary between two different nodes. This also means that there is no central party that can regulate, stop and freeze your transactions. The elimination of such intermediaries allows for more efficient and cheaper transactions.

2.1.3 Client-server network

This P2P network contrasts with the ***client-server network*** (workstation-server network).

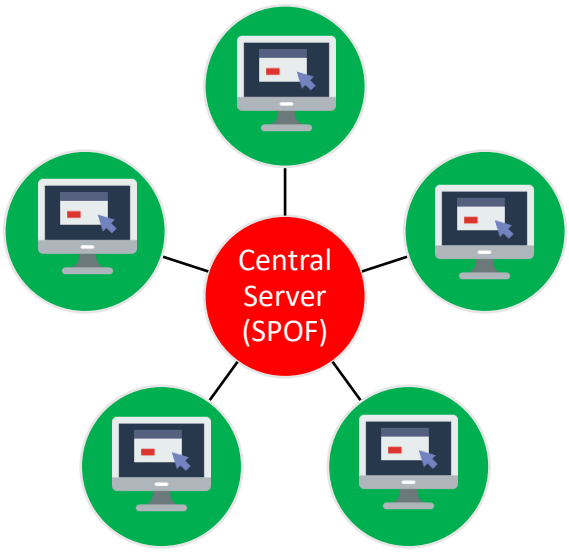


Figure 2: Simplified decision tree whether or not to use blockchain (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 1).

A client-server network uses centralized servers that provide services, such as an e-mail service, to its clients. The server often contains data and applications. When clients need access to these resources, they can submit a request to the server. A weakness of client-server networks is that it contains a ***Single Point Of Failure (SPOF)***. In this case, the SPOF is the central server. Once disabled, the clients will no longer be able to access the server's services.

The need to trust a central party with your data and to trust that the SPOF will not fail makes the model vulnerable. Large reputable companies can also suffer from a SPOF network design. For example, in 2015 there was a power outage at a single PayPal data centre. As a result, many users could no longer access the PayPal website, credit card transactions could no longer be processed, people could no longer access their personal account information, or incorrect balance sheets were displayed.[2]

[2] https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

2.1.4 Hybrid networks: the case of Napster

There are also hybrid networks. One famous example is Napster, a music download service that gained notoriety in the late 1990s and early 2000s.

In 1999, a peer-to-peer file sharing service called Napster was launched by teenagers Shawn Fanning and Sean Parker. Napster made it possible for people to easily share and download digital music files from others. It caused a lot of commotion, because for the first time music was widely shared with each other for free. Napster allowed people to download and listen to individual songs. Before, if you wanted to get a single song, you had to buy a full album. In 2001, Napster was eventually closed after a lawsuit with the Recording Industry Association of America, because the distribution and downloading of digital music files was deemed to be in violation of copyright law. Nevertheless, Napster is still known as a revolutionary service that has disrupted the music industry. In the United States, CD sales peaked in the year 2000, after which there was a sharp decline - partly due to Napster and subsequent services such as BitTorrent and Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

Figure 3: New York time news item; Napster is told to remain shut, July 12, 2001.

Napster is known to use a P2P network. How come authorities have been able to shut down Napster, which is virtually impossible with Bitcoin?

Napster uses a central index that keeps track of which computer has which files to share with other users. If a user (computer A) wants to search for a song such as Michael Jackson - Billie Jean, a connection is made to the index and the index searches which computers have this song. If the index shows that computer B has this song, a direct peer-to-peer connection is made between computers A and B, allowing A to directly download the number from B's computer.

Napster is a mixed model of client-server and peer-to-peer. The central index element is client-server, but the actual files are downloaded peer-to-peer. The central index server has proven to be a serious Achilles heel for Napster because it can be closed easily, causing Napster to stop working. Because Napster only has a central index server, which lists which computers have which shareable music files, Napster itself does not have music files on its server. It has only facilitated users to make peer-to-peer connections and share music with each other.

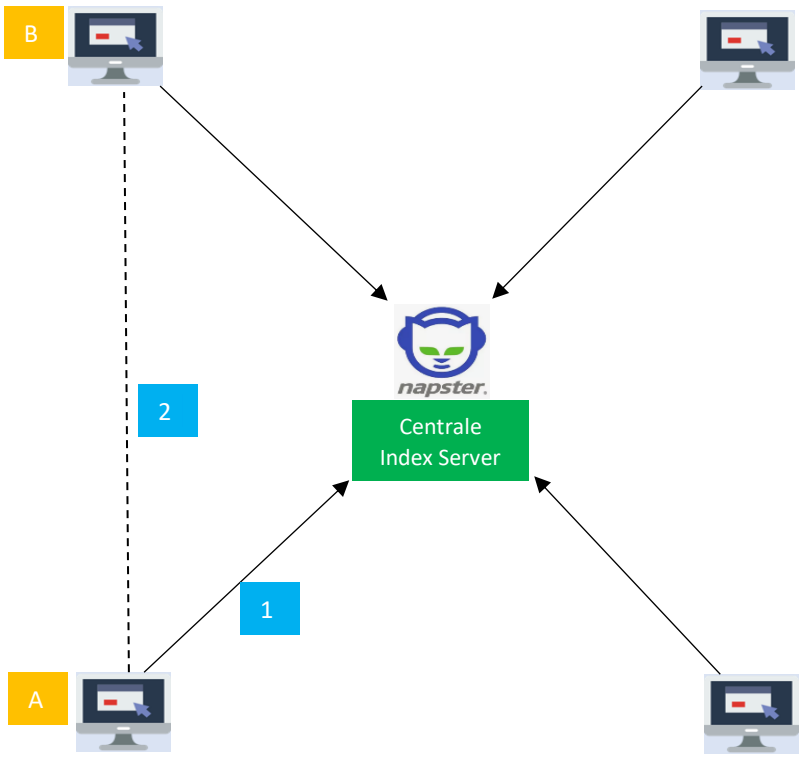


Figure 4: Napster network. (1) Computer A performs a search on Napster's central index server for Michael Jackson - Billy Jean. Napster's central index server looks for computers connected to the network that have the number available on their hard drive. (2) Computer B has the number. Laying computers A and B a direct peer-to-peer connection, after which computer A downloads the music file from computer B.

While music file sharing is peer-to-peer with Napster, it also includes a central server element, which makes it prone to attacks. In this case, it was closed down by law enforcement. With the Bitcoin network, all nodes have an exact copy of the Bitcoin public ledger. The Bitcoin network consists of many nodes, which are spread all over the world, making it difficult to locate and close them all.

2.1.5 Blockchain

The Bitcoin public ledger is considered decentralized as it is distributed across nodes all around the world. The Bitcoin public ledger is also called a chain of blocks or a blockchain

which contains the transaction data. If we view the blockchain as a database that records information, these are the essential inherent properties of a blockchain:

1. The data is arranged in data blocks.
2. The blocks are incrementally ascending in block numbers.
3. The data is reliable because it is cryptographically verifiable.

The chain is the transaction database that is built by nodes participating in the mining process on the Bitcoin network. The chain is maintained by a timestamp server, which generates proof of the chronological order of transactions. Every block contains a hash reference to the block it builds upon, which creates a linear sequence over time. Blocks can be thought of as the individual pages of a record book.

Miners are constantly processing transactions into blocks, which they add to the end of the chain. The process of which miners add new blocks to the chain is also called ***Proof-of-Work***. This process avoids ***double-spending***.

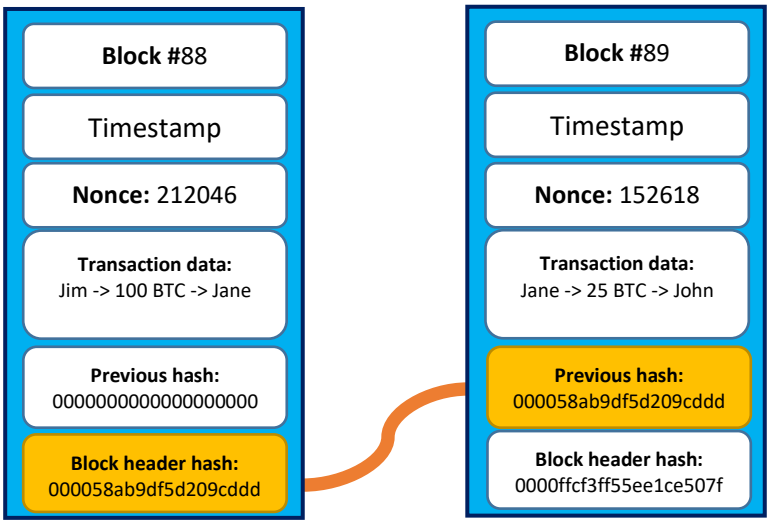


Figure 5: Vereenvoudigde weergave van een geldig genesis blok en blok #2 waarbij beide blokken aan elkaar zijn geketend door middel van de block header hash en de previous hash. (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 3).

2.1.6 Double-spending

An important issue that a peer-to-peer electronic financial system needs to solve is the issue of double-spending. Double-spending is the act of spending a bitcoin more than once. For example, if you have 1 bitcoin and you spend it to person A and person B at the same time. Within a centralized financial network, the double-spending problem can be solved by a ***Trusted Third Party (TTP)*** that maintains the ledger and checks all transactions within the ledger.

Within the Bitcoin network, this problem is solved via its economic incentives and the use of a timestamp server. Miners have a strong incentive not to include these transactions in a block because they are at risk of having their block rejected by other Miners, and in addition, would be complicit in carrying out a crime.

2.1.7 Proof-of-Work

In addition to avoiding double-spending, the purpose of proof-of-work is also to protect the network from attackers and to reach consensus on the state of the public ledger. In short, proof-of-work is a mechanism that requires miners to use computer power to find the correct values for a block they are working on. By finding the correct hash value, they are allowed to add the block to the blockchain and to receive a reward in bitcoins. The process of finding the correct value is called mining.

Transactions broadcast to the network are neither directly added to a block by the miner, nor are they directly stored in the ledger. They first end up in a ***memory pool*** (mempool) with other transactions that have yet to be added to a block by miners and that have yet to be confirmed by the network. You can think of the mempool as a waiting area for all incoming transactions that have yet to be confirmed by the network. Each miner has its own mempool and it is possible that the individual mempools differ per miner. That's because there is always network latency within a computer network: it always takes a bit of time for a transaction sent to the network to reach all miners on the network.

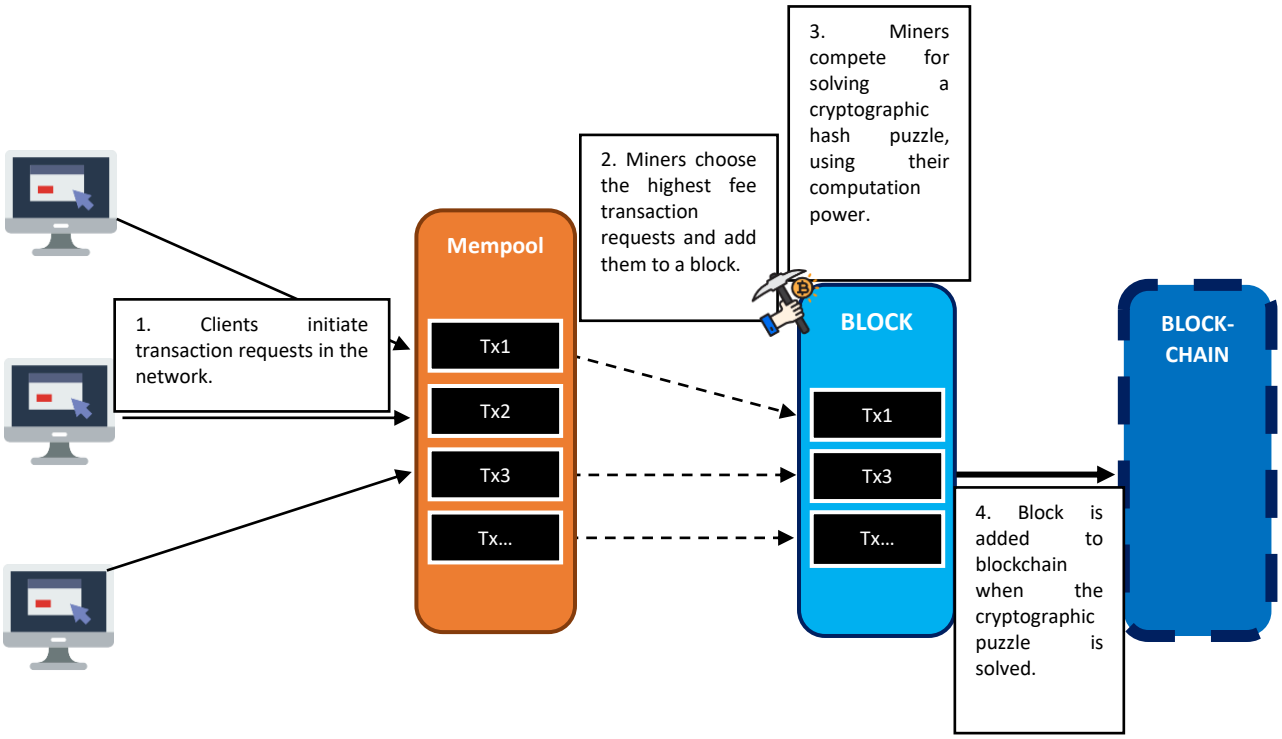


Figure 6: Schematic representation of how a transaction is added to the blockchain. The mempool is where unconfirmed transactions come in and are kept. Miners choose which of the transactions from the mempool they want to add to the block. Subsequently, they try to solve a cryptographic puzzle.

Once solved, they receive a block reward in bitcoins.(Source: Book: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 4).

Every transaction requires transaction fees. Miners are economically encouraged to add the highest fee transactions to their block because they collect these fees when they are first in finding a valid hash for the block. In addition to the transaction fees, miners also receive a block reward, which halves every 210,000 blocks.

The system is secure as long as honest nodes collectively control more computation power than any cooperating group of attacker nodes.

2.1.8 Decentralization

The terms 'decentralized network and 'distributed network' are often used interchangeably.[3] Decentralization provides for another important security feature with respect to the destruction of any single node which is hosting the data as a SPOF. The usual solutions that enterprises have is to keep multiple copies for their whole system/application hosted on data centers at multiple locations. This is a huge cost duplication that is needed for the security of data that Bitcoin achieves just by its native architectural design.

- **A decentralized blockchain requires confirmations of new data from other nodes**

With a centralized server, it is relatively easy to include new data injections in the database. The new data only needs be added by a single party. This is different for a decentralized network. If the new data is added to a blockchain by a miner, this data must still be verified by other full nodes and then also included in the blockchains hosted by other nodes.

- **A decentralized blockchain requires consensus**

What about new updates to the network protocol? A decentralized blockchain requires consensus to updates and agreements on the correct state of the blockchain.

- **A decentralized blockchain is difficult to hack**

As the blockchain is kept on different nodes that may reside on different places in the world, it is difficult to take over control over the network. To control the network, you have to be able to create the longest chain which can only be achieved by having a majority computation power. It allows you to find valid block hashes faster than the rest of the network combined.

[3] Because the blockchain is a database distributed across different servers, this technology is also referred to as a ***Distributed Ledger Technology*** (DLT). Blockchain can be considered a DLT, but a DLT does not always have to be a blockchain.

An attack based on majority computation power Is also called a ***51% attack***.[4] A 51% attack allows you to double-spend.

- **A decentralized blockchain complicates censorship and fraud**

The blockchain, if distributed far and wide enough, is more tamper proof. It is, however, possible to change or delete data if there is consensus within the network to do this. If we assume that the network is well decentralized, we can say that censorship of the blockchain is difficult to accomplish.

2.1.9 Privacy

Satoshi Nakamoto stated at his first announcement of the Bitcoin network that bitcoin is anonymous, but that's actually not true. Bitcoin is pseudonymous. This means that it is private but not anonymous. It publishes all the transactions on a public blockchain in cleartext for anyone to audit and run things like machine learning algorithms to perform tracing analytics on it. It however is private, which means that unless there is a need to know (like a court order) and if the user is using it with the intent to keep their financial transaction private (by not reusing their public addresses multiple times) as privacy is built-in.

Privacy is still maintained by keeping public keys and its corresponding wallet address pseudonymous. The public ledger allows everyone to see which address has done what transaction, but as long as your addresses are unknown and not linked to your personal information, you can transact rather 'anonymously'.

In the Bitcoin whitepaper, Satoshi also mentioned that as an additional firewall to preserve privacy, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

The mainstream view of Bitcoin being a currency that is anonymous is hence factually incorrect. On the contrary, it works as a transparent open ledger and this created a space for a whole new set of cryptocurrencies focusing on being anonymous like monero, zcash, and some others. Many countries are actually already actively working on legislation.

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

[4] While the 51% attack is the best known, many other attacks are also possible. Regular attacks that occur on centralized networks, such as corruption of core developers, bugs in incorrectly written code, or stealing keys that give access to servers also occur with blockchains.

2.1.10 Summary

Although there are many different types of blockchains and with different levels of decentralization, we can conclude that in general a decentralized blockchain network has the following attributes:

1. There is no Single Point of Failure (SPOF).
2. New data must be confirmed by other nodes.
3. Some form of consensus is required to make updates and agree on the correct state of the blockchain.
4. It is difficult to hack.
5. It makes it more difficult to censor or change the data on the blockchain.
6. It is a peer-to-peer network, which does not require trust in a central party.

Comments you can now explain

- Blockchains differ from traditional databases.
- The reason Napster failed is because it had a SPOF. A blockchain, on the other hand, has no SPOF and is therefore more difficult to switch off.
- A blockchain is a peer-to-peer network.

Glossary of Terms

51% Attack: An attack on the blockchain that is accomplished by gaining more than 51% of all the network's computing power.

Client-server model: The model where clients (user) are connected to a server. The server contains data relevant to the clients. The clients connect to the server to access this data. This makes the clients dependent on the server.

Distributed Ledger Technology (DLT): Distributed ledger technology.

Double-spending: Spending a Bitcoin twice. For example, that you have 1 Bitcoin, but with that you send 1 Bitcoin to person A and 1 Bitcoin to person B.

Full node: A node that has a full copy of the blockchain.

Miner: A computer that provides computing power to produce a valid block. A block is only valid if it finds a nonce that leads to a valid hash value.

Node: Device that is connected to a computer network.

P2P: See peer-to-peer.

Peer-to-peer: A computer network where computers are equal to each other and can offer each other services.

Proof-of-Work: A consensus mechanism that requires miners to use computer power to find the correct hash value for a new block. By finding the correct hash value, they are allowed to add the block to the blockchain and receive a reward.

Single Point of Failure (SPOF): The part of a network that stops the operation of the entire network in the event of a failure.

SPOF: See Single Point of Failure.

Trusted Third Party (TTP): Trusted intermediary.

TTP: See trusted third party.

White paper: A document that describes how a specific problem is solved. Satoshi Nakamoto has written in the Bitcoin white paper how Bitcoin solves the problem of double-spending in a distributed network.

Icons used

Computer made by Prettycons from www.flaticon.com

Mine made by Strip from www.flaticon.com

2.2 Blockchain 2.0 and smart contracts

"We want a whole sequence of companies: digital title, digital media assets, digital stocks and bonds, digital crowdfunding, digital insurance. If you have online trust like the Blockchain provides, you can reinvent field after field after field."
- Marc Andreessen (2014)

2.2.1 Introduction and learning objectives

Learning objectives

- What blockchain 1.0 is and why there is a need for blockchain 2.0.
- Ethereum is an example of blockchain 2.0.
- What smart contracts are.
- What decentralized applications (dApps) are.
- What decentralized autonomous organizations (DAOs) are.

Introduction

The previous chapter mainly discussed basic blockchain principles through Bitcoin. In this chapter, we shift our attention to a newer generation of blockchains that are specifically intended to create a plethora of other types of decentralized applications or dApps. One specific blockchain we focus on is Ethereum, which also touts itself as the world's decentralized computer.

2.2.2 Blockchain 1.0 and 2.0

The first generation of blockchains is also known as ***blockchain 1.0***, which mainly focus on digital money. Vitalik Buterin had the idea to develop a new blockchain, Ethereum, on which one could create new coins, contracts with conditions and requirements and even full-fledged ***decentralized applications*** (dApps). Blockchains with such capabilities are also known as 2nd generation blockchains: ***blockchain 2.0***.[5]

2.2.3 Ethereum

Ethereum was first introduced by Vitalik Buterin in "Ethereum White Paper: a next generation Smart Contract & decentralized Application Platform" (2013). In the white paper, Buterin explains that Bitcoin can be described as a "first-to-file system" in which the order of the transactions is crucial. Technically, Bitcoin can be considered a simple state transition system

[5] These are blockchains that have solved a cluster of issues that blockchain 2.0 still deal with. Examples of such issues are scalability, interoperability, privacy, and sustainability and governance (Ackermann & Meier, p. 1). EOS, Cosmos, Cardano, Avalanche, Terra are examples of blockchains that could be considered blockchain 3.0.

where (a) the "state" consists of the ownership status of all existing bitcoins and (b) the "state transition function" that takes a state and a transaction and outputs a new state which is the result. However, it is difficult to execute contracts concerning the transaction, which can capture across multiple states. For example, it is hardly possible to pass on a piece of logic that says that Bob can send his money to Alice, but that Alice can only claim it after she has provided something in return. (Buterin, 2013, p. 12)

Ethereum's goal is to provide developers with the ability to develop applications based on arbitrary terms and conditions. The programming language specifically developed for Ethereum is called ***Solidity***.

2.2.4 Ethereum transactions and gas

The underlying cryptocurrency of the Ethereum blockchain is ether (ETH). Making a transaction on the Ethereum network requires ***gas***. Gas is expressed in the cryptocurrency Ether. Gas on the Ethereum network is basically the same as transaction costs. This is calculated using standard costs per unit of computation power x the number of units. You can specify a specific amount of gas, or transaction costs, for each transaction you perform. The user must pay an appropriate amount of gas for the transaction. If too little gas is paid, miners may not include the transaction in the block and thus this transaction will not be executed. In addition to the block reward, the miner also receives all the gas fees that were included with the transactions in the block.

The crypto economic reason gas has been introduced to the Ethereum network is that it prioritizes important transactions. A block only has room for a limited number of transactions. The gas system ensures that no energy is wasted on spam or low-value transactions.

2.2.5 Smart Contracts

A smart contract is decentralized automation and can be defined as a contract with certain terms and conditions that are laid down in code. The contract is self-executing, as it performs appropriate corresponding actions when the terms and conditions are met.

For example, a smart contract could be an employment contract, where Alice wants to pay Bob €500 to develop a website. The contract could work as follows:

1. Alice puts €500 into the contract and the funds are locked.
2. When Bob has developed the website, Bob sends a message to the contract to release the funds to him.
3. The fund is released when Alice agrees.
4. If Bob decides not to finalize the website, Bob can cancel his job by sending a message to the contract, after which the fund is automatically returned to Alice.
5. If Bob claims that he has completed the website, but Alice disagrees, a judge could be called in after a 7-day waiting period to express an verdict in favour of Alice or Bob. (Buterin, 2014)

Advantages of smart contracts

Smart contracts offer many advantages. Chaintrade (2017) has listed the following eleven:

1. *Accuracy:* All terms and conditions must be recorded in detail in a smart contract. If certain conditions are omitted, this can lead to undesired behaviour of the smart contract.
2. *Transparency:* all terms and conditions are fully visible and accessible to all parties involved. Once the contract has been finalized, you can no longer dispute it.
3. *Clear communication:* the need for meticulously defined smart contracts ensures that the communication in the contract is clearly laid down so there is no room for miscommunication and misinterpretation.
4. *Speed:* smart contracts can automate and significantly accelerate traditional business processes. No applications need to be submitted for approval and no documents need to be processed or approved by individuals.
5. *Security:* smart contracts run on blockchain platforms and use data encryption.
6. *Efficiency:* Due to the accuracy and speed, smart contracts execute business processes more efficiently or even completely eliminate them.
7. *Paper-free:* no paperwork is required for the execution of smart contracts.
8. *Storage and backup:* smart contracts and their details are permanently stored on the blockchain. As a result, they cannot be lost and are easy to find.
9. *Cost savings:* smart contracts can save a lot of costs, because there is less need for intermediaries such as lawyers, witnesses and banks to interpret and enforce the contracts.
10. *Trust:* involved parties can trust that smart contracts - if they are properly set up - will be executed fairly, without the possibility of data manipulation and prejudices.
11. *Guaranteed outcomes:* by using self-executing contracts, parties will comply with the rules of the smart contract and there will be fewer legal disputes.

2.2.6 Decentralized applications

We define a ***decentralized application*** (dApp) as an application that uses the decentralized data storage of a blockchain. The application is not executed via a central server, but via a decentralized network of nodes. Just like a normal application, it often has a front end and a user interface. The interface offers the user an easier interaction with smart contracts and the blockchain. By storing and executing the smart contracts that make up the core code of a dApp in a decentralized manner, there is no Single Point of Failure. The operation of the application and the data of the application cannot be simply censored or removed.

2.2.7 Decentralized autonomous organization (DAO)

Decentralized autonomous organizations (DAOs) can be defined as a non-hierarchical organization that performs and registers routine tasks on a blockchain. The rules that the DAO adheres to are also recorded on the blockchain. In addition, the DAO is dependent on

voluntary contributions from internal stakeholders to guide the organization through a democratic consultation process. (Hsieh et al., 2018, p. 2)

What makes a DAO fundamentally different from a centralized organization is that it does not have a top management team or a CEO. It also has no branches, employees, or subsidiaries. Instead, a DAO exists on a decentralized network of users and nodes that collect, verify and update transactions on a blockchain. Decisions about changes to the code are made by democratic voting processes. It is a radically different way to set up a business organization. Due to its autonomous nature - after all, it is a self-sufficient and self-organizing system - Bitcoin can be characterized as a DAO, because it (a) runs a payment system, (b) employs subcontractors who work as miners and (c) pays these subcontractors with newly distributed bitcoins (Vigna & Casey, 2015, p. 229). In addition, miners can vote for proposals for improvement to the protocol by means of their computation power. DAOs are controlled by a collective decision-making process of stakeholders through a decentralized protocol and are not influenced by a central governing body.

Comments you can now explain

- With Blockchain 2.0, a plethora of new types of applications can be built developed.
- You can develop smart contracts on Ethereum where terms and conditions are so clearly laid out that in the event of a breach of contract, interpretation of third parties is no longer required.
- Bitcoin is a first-to-file system.
- Bitcoin is the first decentralized autonomous organization (DAO).

Glossary of Terms

Blockchain 1.0: The first generation of blockchains that have mainly been used to facilitate the storage and transfer of cryptocurrencies.

Blockchain 2.0: The second generation of blockchains that are more focused on enabling smart contracts, dApps and DAOs.

Blockchain 3.0: The third generation of blockchains that have solved a cluster of issues that blockchain 2.0 still has to deal with. Examples of such issues are scalability, interoperability, privacy, sustainability and governance.

Gas: Transaction costs for performing a transaction on the Ethereum blockchain.

Decentralized Application (dApp): An application that uses the decentralized data storage of a blockchain. The application is not executed via a central server, but via a decentralized network of nodes. Just like a normal application, it often has a front end and a user interface.

Decentralized Autonomous Organization (DAO): An autonomous entity that also relies on hiring individuals. These individuals can perform certain necessary tasks that the entity cannot. The DAO has internal capital at its disposal for this purpose, with which certain

activities of these individuals can be rewarded. What makes a DAO fundamentally different from a centralized organization is that it does not have a top management team or a CEO. It is a non-hierarchical organization.

Smart contract: A contract with certain terms and conditions that are laid down in code. The contract is self-executing, as it performs appropriate corresponding actions itself when the terms and conditions are met. The contract must, however, contain sufficient information from each party involved in the contract to deprive parties of their ability to terminate the contract. There are two types of smart contracts: deterministic and non-deterministic.

Solidity: The programming language specifically developed for Ethereum to write smart contracts.

3 Types of Blockchain

In this chapter we will divide blockchain into its types from three perspectives, consensus protocol, governance and types of cooperation between blockchain systems.

3.1 Types of blockchain according to consensus protocol

Consensus protocols are essential to ensure trust among different participants within a distributed network. There must be confidence that the participants are not corrupt and that the data that is shared among them is not corrupt. To ensure this trust, participating nodes must verify messages or transactions for correctness and neutralize other participants who are corrupt and misleading: the solution to the Byzantine Generals Problem as discussed in the previous chapter.

As a consensus protocol therefore touches the essence of a blockchain system it is used here as one way to discern blockchain types.
In the previous chapter the first consensus protocol, **Proof-of-Work**, was introduced using the Bitcoin as an example. According to this protocol, a data block may only be added to the blockchain when a valid hash of the block has been found. As Bitcoin miners entered into a fierce competition in computing power to receive the rewards of finding a valid hash first, the electricity consumption of the Bitcoin network has led to worries about the negative effects of blockchain to the environment. The resulting search for more sustainable solutions to the Byzantine Generals problem has led to alternative consensus protocols.
One of the main alternatives to Proof-of-Work is Proof-of-Stake which now has been implemented in various blockchain projects with the notable example of Ethereum which is transferring to Proof-of-Stake in 2022.

While miners at Proof-of-Work are allowed to produce new blocks when they can find a valid hash, a block producer at Proof-of-Stake is chosen based on (a) a random selection process and (b) a **'stake'** such as the number of coins he has. As a consequence you do not need computing power to participate. All it takes is a standard computer, an internet connection and having a coin. The block producer at Proof-of-Stake is therefore not called a miner but a ***forger***. Because the forger also receives a reward when producing a new block, you can also **forger** see Proof-of-Stake as a method where you earn a passive income on your coins. The more stake you have, the higher the chance that you may produce the next block. In addition to producing blocks, forgers also validate transactions, helping to secure the network.

Next to energy efficiency, the advantages of Proof-of-Stake of Proof-of-Work are that the ease of staking allows the blockchain to be better distributed and that conducting a 51% attack is less appealing.

There are different variants within Proof-of-Stake that have their own unique properties. First, in the **Delegated Proof-of-Stake** anyone who has a coin can vote for witnesses and delegates. The witnesses validate transactions and produce new blocks for which they receive a reward. Delegates oversee the governance structure of the blockchain protocol. As a result delegated Proof-of-Stake can handle more transactions per second than blockchains that are more decentralized.

Second, in a **leased Proof-of-Stake** everyone can lease their coins at stake nodes thus increasing the chance for stake nodes to produce a block. Stake nodes distribute their reward proportionally between themselves and lessees. As a result this protocol encourages people to participate in the staking process.

Third, with **Proof-of-Stake Velocity** users are rewarded for (a) the number of coins they hold and (b) how actively they use their coins. The community is therefore encouraged to not only keep the coins, but to actually use them for transactions.

Fourth, with **Proof-of-Authority**, block producers (authority nodes) are authenticated and approved based on their identity and reputation. By linking the reputation to identity, authority nodes are extra stimulated to show good behaviour and not to include malicious transactions in the blockchain. If they do, it will cause reputational damage. Proof-of-Authority is an example of creating a Proof-of-Stake variant where the chance of creating a new block is not entirely dependent on the number of coins you stake.
Mind it is doubtful whether Proof-of-Authority falls under Proof-of-Stake. It is sometimes thought of as a form of Delegated Proof-of-Stake and more commonly used in closed, permissioned blockchains.

One advantage of typifying the blockchain using consensus protocols is that it helps to explain the differences in **scalability of blockchains**. This as scalability in general depends on the influence of the consensus protocols on block time, block size, the distribution or decentralization level of the blockchain and the way in which blocks are produced, transactions are sent to the blockchain and transactions are verified. To improve this scaling, different solutions such as taking transactions off-chain are tested. Well known examples of this are the lightning network, plasma (both so called 'Layer 2' solutions) and sharding.

3.2 Blockchain governance and who can participate with which role

A blockchain, like any partnership, needs to be managed and controlled. The resulting blockchain governance structure offers a second way to discern blockchain types that will be discussed here.

Notable governance elements are:

1. **Rights** to submit, execute and monitor **decision** proposals by a group or to all.
2. **Accountability** and the right to monitor decisions and behaviours and to be held accountable for your responsibilities.
3. **Incentives** and encouraging participants to maintain the blockchain.

The way these elements are interpreted depends on the goals that the partnership pursues and therefore the type of governance it needs.

One of governance needs may be that a central group of people exercises control and dictates terms (**central** control mindset**)**, versus the needs of a larger group to work together on an equal basis without a hierarchy or central control (**decentralized** control mindset).

The type of control that is exercised is used to decide on who is granted permission to participate in a blockchain or not. If central authorities grant the access, the blockchain is the

private blockchain type. If access is arranged for everyone, the blockchain is called a **public** blockchain. The public and private blockchain types find themselves combined in the **consortium** blockchain type, an intermediate form that is more centralized than a public blockchain and more decentralized than a private blockchain.

In a consortium, multiple organizations work together to set up a blockchain and the consensus is managed by a selection of nodes. The consortium decides for the entire network who can participate with which role, which transactions can be seen openly or can be shielded from other participants and how the governance should be structured.

You mainly use a **public blockchain**, where everyone is treated equally, if you want a group of like-minded people to work together. Cooperation is guaranteed here by the consensus mechanism that acts as a 'trust machine'. 'Access to all' leads to a larger number of nodes which build confidence in the blockchain system. A public blockchain shows a lesser degree of trust in authorities that govern the blockchain in the name of others. This attitude towards confidence and trust favours the decision for consensus protocols with a more decentralized nature, trust in the open source nature of its blockchain as well as the want for full transparency of decision-making. This attitude therefore leads to a greater confidence in having strangers join and participate in the partnership. After all, trust lies in the system and not in the user.

In general a company that is inclined towards a **private blockchain**, will want to know who is in the blockchain system. Think of an intranet in which you check the nodes, data and source code. You know everyone and all transactions can be viewed if this is necessary, but you also shield people from verifying or seeing certain transactions. This is useful when the data is company sensitive. In a public system it is also possible to build this in technically, but for the time being in practice this proves to be a challenge.

So in a private blockchain its relevant to be aware of all roles you assign to the participants that you granted access to. One important role is the possibility to **maintain the consensus mechanism**. Should this possibility be given to all participants in the blockchain or only to a select group?

The answer to this question leads to the **permissionless** and **permissioned** blockchain types.

If every entrant to the blockchain is allowed to maintain the consensus mechanism, it concerns a **permissionless** blockchain type. If the role to maintain the consensus mechanism is reserved for a select group, we are talking about a **permissioned** blockchain type.

Next to maintaining consensus there are roles that allow you to execute, view and adjust transactions in the blockchain, technically maintain the blockchain, or participate in voting on ideas. These roles are not relevant for the choice between a permissionless or permissioned system. However these roles are relevant for the nature of the partnerships. This is relevant because if authorities do not mind who accesses the system, and puts trust in the system itself, it will more likely be inclined to grant anonymity to the participants. Currently companies using classis management control systems however would choose to know the people they grant access to, as well as would choose to know which roles are there and to which participant they can grant what role.

By segregating the roles, these companies can remain using their underlying organizational structure. Thus they can enforce their company identity within their blockchain as they control the profile of the persons as well as their roles. Additionally next to partly transferring trust to the system, they can continue to manage their organization their your own management control system like specific personnel management.

This helps to explain why within a permissionless system, crypto tokens are made available to encourage collaboration.

The different blockchain types are used in combination in today's blockchains:

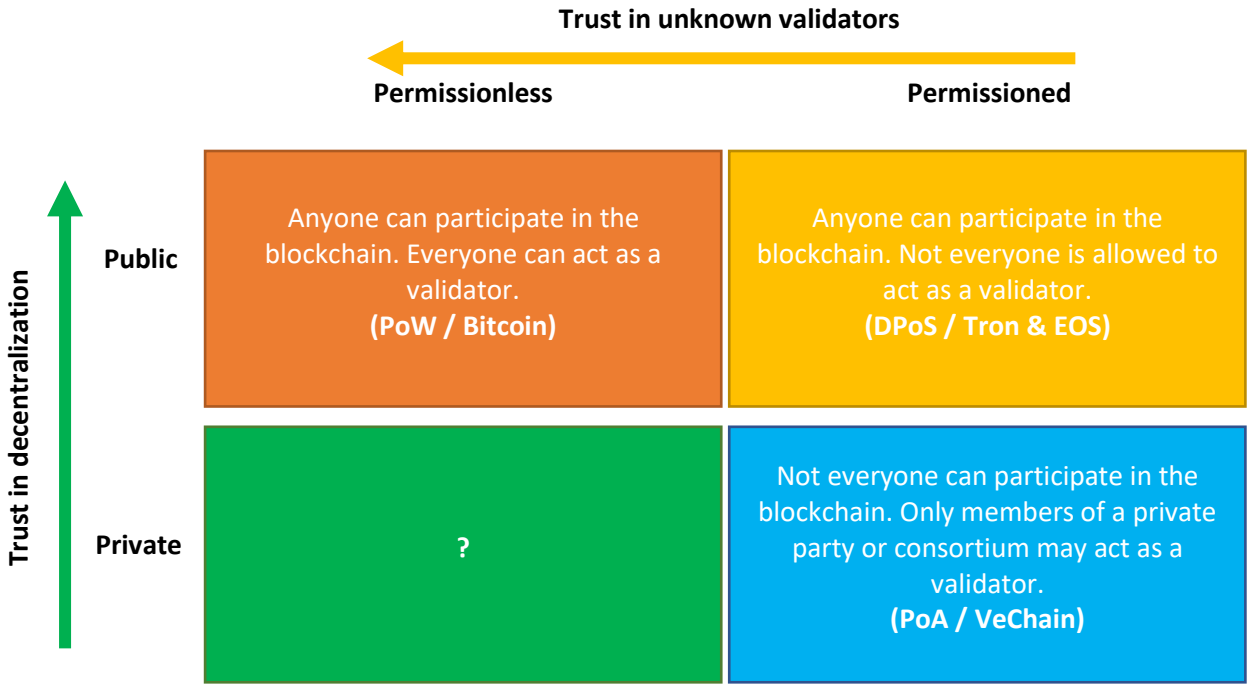


Figure 7: An overview of different blockchain types, expressed in permissionless, permissioned, private and public (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 9).

With trust lying in the system with public blockchains, the 'who writes data to the blockchain', 'who reads data from the blockchain' and 'who is allowed to maintain the blockchain' is considered of lesser importance. This in turn leads to most public blockchains being permissionless. Due to the low barrier to joining the network, such blockchains are the most decentralized.

The participants determine the functioning of the blockchain in line with group motives such as openness, neutrality and freedom. Within the public blockchain, everyone can also participate in decision-making on all governance issues.

A **public** blockchain is not always desirable for companies, especially in a more regulated environment in which it is expected, among other things, that they know the identity of all parties who write data to the blockchain.

This central party has often set up a number of nodes that manages itself and that keep the blockchain running together. In the most extreme case, the party has a single node on which the blockchain runs. However, this does not offer any advantages over a centralized network which is also a SPOF.

Choices between the different types of blockchains affect the control of the organization. The more confidence there is in the decentralized nature of the blockchain, the easier it is to participate. The more confidence there is that validators may participate in consensus building as unknowns, the more transparent the system. After all, everyone can then run a full node and help validate all data. Due to the decentralized nature, such systems often have many validators and, partly because of this, still have scalability problems. Also, such blockchains are relatively more expensive than the less decentralized and permissioned variants.

In the long run, however, a permissionless public blockchain is expected to become increasingly efficient, so that more professional parties will opt for such blockchains. These blockchains must then be arranged in such a way that the roles that participants can take for business applications are well defined and meet business requirements. For example, companies on permissionless public blockchains can anonymize data through Zero-Knowledge Proofs and participants at the application level can be asked to show their identity.

3.3 Platforms and consortia

A blockchain where different companies and third parties cooperate without a central user controlling this blockchain, is called an enterprise blockchain. To build such a Enterprise Blockchain, companies use blockchain platforms. These **platforms** allow you to write applications using certain technologies. Various partnerships have been organized around these platforms. Platforms are the third and last way we look at different types of blockchains here.

Blockchain **platforms** allow your application to collaborate with other applications, for example, in its own or shared programming language, documents are stored or shared and access to a specific network is obtained. The two most prominent platforms are currently Ethereum and Hyperledger, with Corda as the third most prominent.

Each platform has its own unique features. Ethereum is, generally, a public blockchain, Hyperledger offers plug-and-play modules using various technologies, and Corda is Decentralized Ledger Technology that is more specialized in financial services. Members who have joined a partnership around one platform are often also members of partnerships around the other platforms. The platforms themselves are open source. Ethereum and Hyperledger have been striving for more integration between the two of them in recent years in their mutual aim to implement blockchain systems at companies everywhere.

When partnerships concern a form of cooperation of blockchains in which the new entrants are known and assigned specific roles, they work in structures that confusingly are also called consortia (see above paragraph 3.2.) but from another perspective then mixing characteristics

of public and private blockchains only. The cooperating parties can vary from government bodies, interest groups and unknowns, to suppliers, customers and direct competitors.

In addition consortia here help parties to overcome four main challenges that organizations meet in implementing blockchain. First, consortia share knowledge about and maintain active contact with (supra) national supervising bodies. Consortia then help to clarify the laws and regulations, among other things.

Second, consortia help organizations to spread the risks over different parties by sharing resources to develop blockchain systems.

Third, through collaboration, consortia provide critical mass to adopt a stable performing system.

And fourth, consortia give the opportunity to establish new decentralized partnerships with trusted and untrusted parties, without having participating organizations losing too much of their autonomy. This offers competitors for example standard procedures to create and exchange data with each other, or collaborate with each other's customers and suppliers. However as participating parties will have to trust each other in order to work together, they usually enforce their trust with contracts on shared resources, decision-making, sanctions, sensitive information and mutual data sharing. These contracts tend to both raise the barrier to join a consortium, as raises the barrier to leave a consortium. Different consortia are likely to coexist. Interoperability within and between consortia plays an important role in this.

3.4 Further reading;

Lin Lim, C., Janse, A., *Blockchain Handbook*, September 2021, Chapter 6, 9, 18. Publisher: De boekdrukker Amsterdam. NUR: 781 ISBN: 978-90-80866140
https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

4 Cryptocurrencies and tokens

One of the great inventions of Satoshi Nakamoto is the combination of pre-existing technologies with a reward system that keeps a decentralized network up and running. As mentioned earlier, the reward in Bitcoins is paid to the miner who produces a block.

Tokens in our current society are known as vouchers and coins - for example, loyalty points, casino coins and gift cards. We also know tokens in IT that provide access rights to a network to perform a task or as representations of rights to underlying assets. A Bitcoin, which you could also see as a cryptographic token, differs from the aforementioned tokens in the sense that it represents value. Cryptographic tokens can be used for many reasons. In the blockchain landscape, they mainly serve an **Internet of Value** where values can be exchanged over a decentralized internet in a trusted manner.

With cryptographic tokens like Bitcoin, you can pay or save, but you can also take it a step further. Bitcoin, for example, can be earned by supplying computer power to produce new blocks. Thus, it creates an economy where several participants are encouraged to help secure the network in exchange for crypto. The use of cryptographic tokens to stimulate certain behaviour of participants and to punish wrong behaviour through a consensus protocol is part of **crypto economics**.

In this chapter, 4.1 first describes **crypto economics** as the basis concept in which tokens are proving to play a useful role. Subsequently, 4.2. describes **what tokens** are and **classifies** them. This classification includes dApp tokens and cryptocurrency, but also the difference between fungible and non-fungible token and how they support the crypto economy. The chapter is continued in section 4.3 with an overview of how tokens can be used for fundraising by an Initial Coin Offering, Security Token Offering and Initial Exchange Offering.

4.1 Crypto economics

Cryptographic tokens serve different purposes such as accessing a system or representing information from a physical object. This provides the tokens with **value** that can be exchanged between different parties within a blockchain. This new discipline that studies the transfer of wealth through computer networks, cryptography, game theory and software development, together with wealth creation and consumption, is called **crypto economics.**

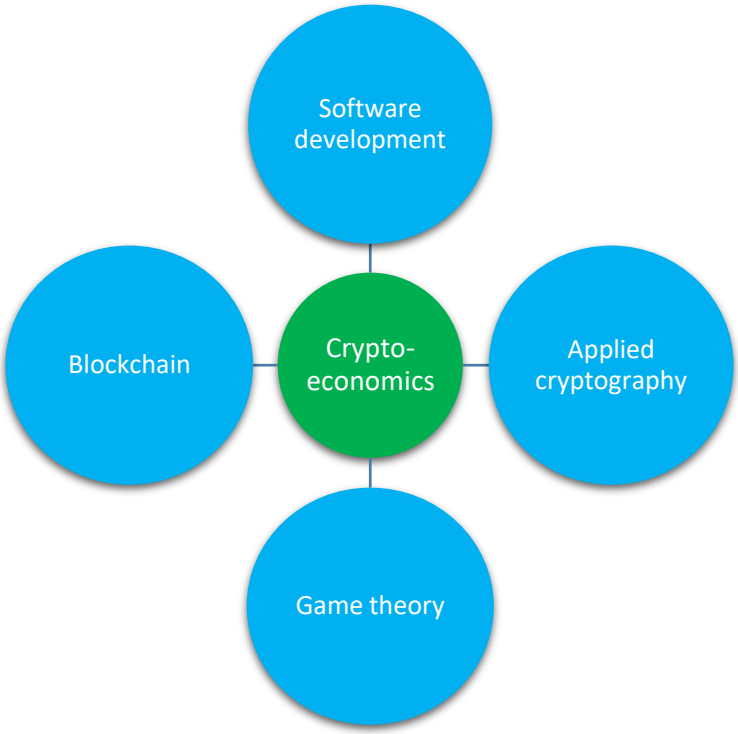


Figure 8: Multidisciplinary aspects of cryptoeconomics. (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 10).

Computer networks are designed with certain rules that act as a kind of law for everyone who participates. These laws however are designed by private parties / communities and in part enforced by software rather than by governments. Within these laws then, assumptions are made about how participants can behave and misbehave within the network.

The central idea behind crypto economics within **blockchain** is that protocols are developed that encourage people to participate in the network in such a way that the **value** of the network **is maximized** for the participants. Network value can only be maximized if the network and the transactions that take place therein are also **secured**. To accomplish this, **cryptography** is used to secure transactions within the network via **software** like e.g. hash functions and digital signatures. Additionally rewards are paid to participants who help secure the network via e.g. mining or staking. The combination of this thinking is exemplified in the role of Bitcoin as a token that stimulates people to collaborate and thus help maintain a self-organizing crypto economic system. Crypto economy is an important premise to support the idea of a sustainable and preferably self-organizing system, without central parties urging people to act in a certain way. Significant for this premise is **Game theory,** a study at how to optimal conditions are created in a competitive environment in order to have participants always choosing to display good behaviour in their choices as this leads to more profit than bad behaviour. One way to encourage participants on good behaviour is through crypto token rewards.

4.2 Classification of blockchain tokens

The internet was initially set up to exchange information with each other. This is also known as an **Internet of Information**. Within this, it is difficult to store and move value without a trusted intermediary (Tapscott, 2016) which mainly checks to see if a value, like euro, is not spent twice (Satoshi, 2008, p. 2). With the advent of blockchain, you can bypass the need for intermediaries and trade peer-to-peer value directly. This is also known as the **Internet of Value**. Crypto tokens play a pivotal role in contributing to this crypto economic system. A crypto token can be created on a blockchain and also represent a tradable asset. Sometimes tokens are created in an ICO or an STO to fund a project. The process of token creation is called **tokenization**. Trading these tokens allows you to transfer ownership to the underlying assets.

There are different perspectives of how to look at crypto tokens. The following format encapsulates all different tokens with the added advantage of addressing the future role of tokens in an Internet of Value:

Application	Token at the benefit of the application	Token as assets
Fungible Tokens	Network: Ether dApp: Augur	Asset: gold Security: part Shell Crypto currency: Bitcoin
Non-fungible tokens		Asset: birth certificate Security: personal loan

Figure 9: Dual format of tokens. On the one hand, to distinguish tokens that are used to blockchain network to maintain vs to demonstrate and transfer ownership. On the other hand, to distinguish tokens that exchangeable vs not being exchangeable. (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021, chapter 10).

Mind that tokens can have a dual token structure in which they serve multiple purposes at the same time. For example, Bitcoin is used as a network or application token and an asset.

Tokens at the benefit of the application are used at the most basic level to encourage people to participate in a blockchain application and keep this network going. This network can serve as a platform on which decentralized applications, dApps, run. Here **network tokens** are used to **reward** participants for the work they do to help maintain the network. These tokens occupy a central place within a blockchain, because as an organizational idea they support a distributed trusted network and thus shape the crypto-economic system of a blockchain. In addition to an application, a network can also be a **platform** on which applications run like on

Ethereum or Cardano with their ETH and ADA tokens to achieve consensus and reward the transaction system. Taking the thinking a step further you can see that within a blockchain there is the choice to use a token, or to ignore using tokens all together.

dApp tokens , or **utility tokens**, are only useful within their own application and are used to access this utility. They are of no use outside of that application. You can still trade them outside the application. However, they are not always programmed as currency or share in a network. For example Siacoin (SC) where people can earn SC when they make their free disk space available to others in the network.

dApp tokens on Ethereum are made according to the **Ethereum Request For Comments 20** (ERC-20) protocol. The protocol defines certain rules and standards related to issuing tokens on the Ethereum network. All dApp tokens made according to ERC-20 are unique to their application and can be traded within the Ethereum network.

Tokens for the benefit of applications differ from tokens that revolve around capturing and exchanging value within the blockchain applications by which they demonstrate possession of this value and enable the transfer of the right to this value, **tokens as assets**. This can be subdivided in Asset tokens, Security tokens and crypto valuta.

Asset Tokens represent records of rights and obligations to the underlying asset like to gold or oil, but also to a house, a paperclip or crypto collectibles like game avatars or digital artwork. These tokens can represent negligible to very vast underlying values. An important condition for asset tokens is that the identity of the owner can be established. Asset crypto tokens potentially bring benefits due to the possibility to program them (**smart tokens**) and trade them with low friction and high security:

1. You can easily divide the asset holdings and make them available in small units. An example of this **fractioning** is representing ownership to the Mona Lisa in 1,000 tokens to sell / lease.
2. You can program rights to the cryptographic token and enforce them via smart contracts. For example set your Mona Lisa token to be sold only to non-profit organizations, or program that a resale automatically includes a 2% commission to the original seller.
3. You reduce the friction of buying and selling, partly due to the fast and cheap microtransactions. For example, a smart refrigerator scans the cheapest electricity for certain time intervals.
4. You can record all relevant information for the underlying assets in the token. For example, check previous owners of your second-hand machine thus improving sharing economy.
5. You can easily create an asset yourself, such as an entrance ticket to a home concert.

In short, smart tokens easily transfer value, information, ideas, rights and obligations through smart contracts.

Security tokens represent bonds, stocks, loans, futures, options and other negotiable financial assets. Although they belong to the asset tokens, they are mentioned separately. All kinds of

rights can be given to security tokens. For example, the right not to resell the security to everyone, or to be able to temporarily lend your voting rights about the direction of the company to someone.

Cryptocurrency tokens also belong to asset tokens and are treated separately given their major expected financial-economic impact. Bitcoin is the best known example of a cryptocurrency. In this case, the token is intended to act as money. Slowly but surely **stable coins** are garnering attention as they demonstrate possible ways to stabilize the value of crypto tokens and therefore amongst others potentially to serve as decentralized alternatives to or representations of fiat currencies. Stable coins can be collateralized with several assets like fiat currency or gold or crypto's, or not be collateralized at all.

A number of central banks are testing stable coins in what is called a **Central Bank Digital Currency** (CBDC). While the CBDC can use elements of blockchain, it is not necessarily a blockchain application. CBDC's are diametrically opposed to Bitcoin's decentralized origins as a CDBC is a centrally regulated currency.

There is the question of how to apply crypto tokens in an economic system where exchange takes place. One way to do this is to look at **token fungibility**. Some tokens can be more easily be exchanged for an another. For example a 1 kg pack of flour can be exchanged for another 1 kg pack of flour. A €10 banknote can also be exchanged for two €5 banknotes. The same goes for **fungible tokens**: the individual units are indistinguishable from each other and can be exchanged with each other. An example is Polkadot: 1 Polkadot token can be exchanged for another and two half Polkadot tokens can be exchanged for 1 whole Polkadot.

Opposite to this are **non-fungible tokens** where tokens are unique in itself and therefore scarce. Think for example of persons, country and birth certificates that cannot be exchanged against other persons, country and birth certificates.

Blockchain in particular is well suited to capture and trade these tokens efficiently, even if the tokens only represent a minuscule value and/or are unique in their kind. This is important as in a digital world, it is easy to create a copy of a digital good. So in having a token as a representation, there is not only an opportunity to easily trading goods from the real world. It also gives you the opportunity to give any physical good an authentic digital representation, however small or silly that good may be, and to trade it. In addition, creating a scarce token is economically interesting if you want to keep the price up given the adagio: 'the lower the supply of a tokens, the greater the scarcity and thus the chance of a higher price'.
A number of the advantages that were earlier mentioned for asset crypto tokens like fractioning and creating smart tokens, support the user case for non-fungible tokens in that they can become highly individual representations of any (to be digitalized) object created and traded via a low barrier (all can enter, all can participate) secure network, the Internet of Value. An internet that can be used to transparently measure your impact on the environment and nudges you into supporting the goals of a larger community. Be your role that of a solar panel owner, electricity user or grid network investor.

In the future, you could theoretically use any asset you own, tokenize and use these tokens fractionally or otherwise as a means of payment or funding.

4.3 Fund acquisition tokens

All these separate tokens then can be used in several ways to acquire funds: from Initial Coin Offerings (ICO), via Security Token Offerings (STO) and Initial Exchange Offerings (IEO) to Initial DEX offerings (IDO).

The **Initial Coin Offering** (ICO) was mainly used in the past to raise funds on the internet for blockchain projects. Ethereum in particular was the primary blockchain to create and sell tokens. A substantial number cases of abuse arose in the beginning of the ICO trend, also as ICO's took place outside protection of national laws and regulations. As a result, the **Security**

Token Offering (STO) was conceived serving the same purpose as an ICO however now with regarding a token as a security with standard protocols, voting rights and more in line, though not fully, to several national securities and exchange laws and regulations. The STO has not proved particularly successful in the public space to date. Also as new more regulated, but still 'open' alternatives, were conceived like the **Initial Exchange Offering** (IEO) and **Initial DEX Offering** (IDO). Here centralized or decentralized exchanges like Binance or Uniswap hand start-ups an opportunity to obtain crowdfunding via their intermediary platform, which usually takes on KYC and AML checks.

The trend of shaping a decentral Internet of Value by the community seems to continue in a whirlwind of colliding ideals, ideas, technical possibilities, mistakes, marvellous accidents and perseverance.

4.4 Further reading

Lin Lim, C., Janse, A., *Blockchain Handbook*, September 2021, Chapter 10. Publisher: De boekdrukker Amsterdam. NUR: 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

5 Uses and applications of blockchain

In this chapter three examples of the use and applications of blockchain are given. Before doing so, an introduction is given on how organizations can strategically think about relevant elements of their business model and the opportunities that blockchain offers. The chapter finishes with specific points a company pays attention to once implementing blockchain.

5.1 Business models

Blockchain typically delivers value within business models and business ecosystems where digital data and technology are/can be created and shared between partners. This as blockchain is a digital technology that fits with these digital data driven business models and enables partners to work together where they could not before. These partners can now put their trust 'in the system' where before blockchain they didn't trust each other to cooperate from the start. In this sense blockchain is especially an opportunity to grow and digitize ecosystems that use **digital data driven business models**.

As to business models, the **decentralized Business Model Canvas**[6][7] is relevant as well as decentralization is central to the public permissionless blockchain adaptations. In this particular canvas token holders have a central position as they have multiple roles such as both user, validator, employee and/or owner. This type of 'new' thinking gives an idea of the potential new opportunities that public permissionless blockchain brings as parties that do not know each other have an alternatively to setup and use a relatively low barrier system to share and verify data together while they not know each other.

The governance then is set up in a decentralized manner by the public, data is stored in a decentralized manner and communication between the various parties takes place peer-to-peer. This is the most open form of a blockchain. A company is free to adjust the building blocks of blockchain itself. With a centralized system, a central organization makes the decisions.

In a decentralized business model, sales are often shared among those who contribute the most to the network and the costs of using the platform are very low - for example, with the social blogging blockchain platform Steemit.

5.2 Enterprise blockchain applications

This paragraph outlines three deployed applications within four different industries, and compares them using a that assesses the comparative advantages that blockchain offered in these applications. The four applications are:

1. Government and Public Goods by Lantmäteriet.
2. Manufacture by BMW.
3. Digital wallet by Singapore Airlines.

[6] https://canvanizer.com/new/decentralized-business-model-canvas
[7] https://medium.com/mvp-workshop/decentralized-business-model-canvas-1-9daf6e4bc9fe

One helpful overview here to help you understand where many blockchain sectors are implementing blockchain is from below research amongst 67 enterprise blockchain networks and the sectors these implementations fall into (Rauchs, Blandin, Bear, McKeon, 2019).

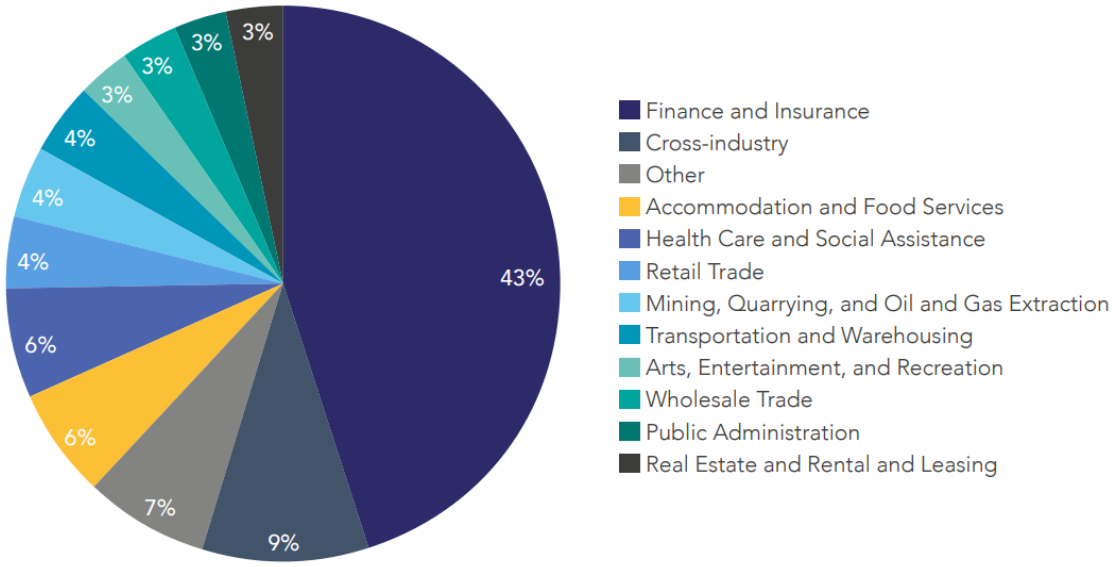


Figure 10: Overview of 67 live enterprise blockchain networks and which sectors they fall into (Source: Rauchs, Blandin, Bear, McKeon, 2019).

The first example is within the **Government and Public Goods sector**. The Swedish **Lantmäteriet** has the task to maintain the cadastral system, provide geodata and perform land registration. There is need for greater transparency and more efficiency of the project as different partners work together while using manual processes which seems inefficient and error prone.

Lantmäteriet therefor tested a solution to see how actors like property buyers, sellers, brokers, financial services, lawyers, pension funds and the Lantmäteriet can work together on an efficient online platform that provides immediate transparency of a request via digital devices. The project was setup as an incremental project (2015-2019) in a controlled boxed situation with trusted partners but without over ambitiously pursuing decentralization on short term. There was a clear focus on picking low-hanging fruit with the registry of land titles while creating a foundation for future services.

During the project legal issues came up that needed to be overcome. For one Lantmäteriet had to consider how to deal with the right of individuals to control their own data (EU General Data Protection Regulation - GDPR) including being able to protect and delete it where desired and possible. As well as on how digital signatures can be used as legally binding signatures within the EU (eIDAS guideline) or the status of digitally signed (e-)contracts based on blockchain.

The sale of land titles was ambitious in that different parties created a new process and game with a new technological solution. The blockchain solutions included both private, closed, permissioned blockchain systems as well as a distributed public network. The private

blockchain is government owned, run by a limited number of nodes from trusted intermediaries and under the supervision of Swedish public government. This system collaborates with ChromaWay and stakeholders' private network. It uses smart contracts, the Practical Byzantine Fault Tolerance and Proof-of-Work consensus mechanisms, off and on chain digital identities via a mobile phone app and no tokens.

The deed remains registered with Lantmäteriet and is not transferred to a public blockchain given the earlier problems with GDPR. Contracts are signed manually and placed on the blockchain via hashes. The original contracts are on the server with other parties, this information has back-ups. Telia offers a mobile app ID solution that allows people to register without publishing their Swedish Civil Service Number. These registrations are stored on the Bitcoin blockchain via a hash and verified. Digital personal information can be removed if an individual so wishes and it is not required by law to be public information.

The main advantages were security of using blockchain technology as well as operational. As to the latter, as the time frame of registering a land title moved from 4-6 months to a few days. Also, €100 million/year savings were envisioned through fewer errors and maintenance (Kairos Future, 2017). This then reduces the risks of contract with ambiguous characteristics, fraudulent data or chances to steal property. The audit trail to both client, auditor as legislator became transparent as well. Also, the ecosystem strengthened its mutual processes and data exchange without too much upheaval of its central service and business model. And, last but not least, the publicly accessibility increased the confidence in the process and the parties. After the test, the system could be expanded to include parties such as insurers, notaries and other local public authorities.

The project was finalized in 2019 showing both the platform architecture worked proved the possible, however according to Mats Snäll, chief innovation officer at Lantmäteriet, "It was never integrated into the production system of the land registry," as a change in legislation would be needed before the system could be scaled up in the future. (Baraniuk, 2020). Likely this points to the challenge of publishing user identity data on the public blockchain.

Other research also points in the direction of a ‘fundamental change in the governance structure, such as the role of the Lantmäteriet’ that might have provided an underlying motive specifically for the real estate ecosystems to freeze further progress on the project (Schnuer, 2020).

Meanwhile though Lantmäteriet uses its lessons to continue experimentation with blockchain. For instance the joint governmental assignment with DIGG where it is to find ‘a model or conceptual solution on how to build trust in automatization with AI and with other new technology such as blockchain technology.’ (AI Sweden, Lantmäteriet, 2020).

The second blockchain application example concerns BMW within the **Manufacturing sector. The automotive business models have to deal with** 4th industrial revolution technologies such as electrification and autonomous systems under ever increasing environmental conscious conditions.

BMW in this example tries to understand how a digital identity for cars can be used so it can enable usage of other 4th Industrial Revolution technologies and concepts. In particular the privacy/security issues of having a constant internet connection of the car and user, as well as

the need to store this data securely. This secure data exchange between devices guaranteeing secure digital identities is what blockchain potentially brings to the table thus offering an entrance to the car sharing economy market for BMW.

BMW has tested a number of car sharing apps like Share Now where the digital identity of both car as user can be involved. These automotive combined digital identities can for example register when petrol is tanked or where the car is parked. This type of information then can be used in business models where the car manufacturers, together with or without intermediaries, offers personalized services like non-life insurance, autonomous car rides or improves its car experience in general.

In this particular example, however, BMW experimented with a simpler project with sole focus on the ID of the car and its stored data, so no focus on the user. The idea is that possible buyers of used BMW's would be interested in trusted data about the mileage, accident history, service history and other info of the car. A prospect seller could share this data with a prospect seller or its insurer, BMW could use the info to improve its business model like using it to better service its customers.

To create this solution, BMW's Startup garage worked with blockchain start-ups, in this case VeChain. Also, BMW uses the results to develop a car's ID, a first step to a Vehicle Identity (VID) that the members of the Mobility Open Blockchain Initiative (MOBI) can use together. MOBI is a blockchain consortium that develops blockchain standards together.

The cooperation with VeChain resulted in the **VerifyCar** app. VeChain is a Decentralized Autonomous Organization with a central governing body that uses the Proof-of-Authority consensus method and different tokens on its public VeChain blockchain.

The VID has a unique ID on this blockchain. Periodically the app captures data (via in-car SIM cards and Machine-to-Machine communication), which is verified on the VeChain blockchain: VeChain only stores the reference to the data, the data remains on the vehicle itself. The captured car data contains both static information such as type and production date for the car as well as dynamic information such as the number of kilometres drive. Whenever a car owner want to share data with another party, he uses the VerifyCar app to show the data including the references on the blockchain to show this is the actual data stored on the vehicle.

Its BMW's intention to have no control over the VeChain governance or the code. Beginning 2022 the app has not seen production.

In piloting this solution BMW is taking a controlled first step towards incrementally integrating decentralized blockchain technology. Also, if VerifyCar can be used for cars, then why not have a VID like digital identity card to ensure car parts are not counterfeited, what location purchased raw materials can be found in the production line or understand the manufacturing or transport conditions of certain production machines you've ordered? In line with that thinking BMW experiments with blockchain to the benefit of a **transparent supply chain** as well.

For example in 2019 the **PartChain** pilot for purchasing front lights using Amazon Web Services, Microsoft Azure and Hyperledger Fabric blockchain (Ledger Insights (2020, 31

March) was expanded to other suppliers. This allowed BWM to be able to trace its components and in the long term critical raw materials 'from mine to smelter'. (BMW Pressclub Global, 2020). And additionally to ensure 'easier certification and shorter customs procedures' (BMW, 2019).

A **last example is the digital wallet by Singapore Airlines, KrisPay**. Singapore Airlines was looking to further increase the loyalty of its customers by the use of blockchain. This resulted in fortifying its frequent flyer program KrisFlyer with the KrisPay digital blockchain wallet in 2018.

With KrisPay customers can exchange their KrisFlyer airmiles for KrisPay miles, cryptocurrency tokens. These KrisPay tokens can be saved at / spend with different merchants like banks, petrol stations and shops. Also the customer can save and exchange other rewards like by using the credit card of DBS (Development Bank of Singapore Limited), or earn, buy or spend Singapore Airlines miles like for flight upgrades. The monetary value of the KrisPay token itself is dictated by Singapore Airlines. So the solution that KrisPay offers here is to give customers an easy way to redeem their rewards to prevent miles from going to waste next to saving these tokens in the merchant network. In a way customers are receiving a digital addition / alternative to fiat backed currencies.

The functionality of KrisPay is simple to use via an app on your mobile device and instant point-of-sale transactions. To enhance further usability, the KrisFlyer miles can be transferred within the family or authorized nominees.

By combining blockchain wallets and cryptocurrencies, KrisPay uses blockchain strengths such as security to all users as the registration of the transactions is tamper proof. Merchants immediately have their transactions approved and made insightful, without the use of a slower more costly middleman. This supports the reconciliation of token payments amongst the merchants (and their financial administrations) and gives them up to date customer information.

KrisPay was developed with KPMG Digital Village and Microsoft. KrisPay is a private company owned by Singapore Airlines working on a combination of Microsoft Azure (originally based on the Ethereum protocol) with Azure app and database functions. Different partners maintain and verify the blockchain database so that each has the customer/transaction information available at the same time.

Microsoft announced to retire its Azure blockchain in 2021 and support customers migration to the Quorum Blockchain Service, another variant of the Ethereum protocol (Microsoft, 2021).

The KrisPay tokens and wallet were combined in a new app in 2020, Kris+. This app further uses customer data in order for Singapore Airlines to better service its customer as well as offer personalized deals, even based on geo location from the mobile phone.

Potentially the KrisPay wallet can be used for ticketing, proofing your digital identity or as a further generic token that can be used to exchange against fiat currencies or other loyalty points.

In conclusion **all of these applications** are manageable well-defined blockchain cases that are carefully implemented as part of a larger vision within an environment the initiators trust and control. The cases show clarity on the elements they see as an opportunity or no opportunity, and use an incremental change process in which they step up the effort from cautious first steps to full implementation.

Their environment consists of a stable processes, a known business model, and trusted partners to experiment with the more tried aspects of the technology and its decentral business implications.

There was no space to show the application of a complete decentralized business model, if you want an example be sure to read the Augur Predication market example in Chapter 16.5. (Lin Lim, Janse, 2021).

5.3 When does what blockchain implementation make sense?

From the previous examples it is clear that certain conditions need to exist to implement blockchain successfully.

There are a number of criteria you can look at to decide if blockchain is a meaningful case for your business. These criteria aim to remove frictions with data or data traffic, or to create opportunities with data and data traffic between parties. As a rule of thumb, the criteria can be summarized as follows:

1. **Digital innovation** is part of the strategy.
2. Different parties **share data**.
3. These data and their transactions concern **monetary value**.
4. The data are **confidential**.
5. Different parties edit data.
6. Data must be verified.
7. There is a **clear and sufficient Return on Investment** to be calculated.
8. Verification is **complex, cost and or time-increasing**.
9. The solution to choose blockchain is the **simplest solution** to overcome the problem.
10. The solution influences the existing organizational structure.
11. The solution affects the existing workflow.
12. The solution affects the existing ecosystem.
13. The technical solution is close to or can be integrated with existing systems.
14. The solution is data intensive but scalable. Think in differences of 1k, 10k, 100k, 1 million or> 10 million transactions per hour.

Once you see the chance to implement blockchain based on these criteria, you can proceed with understanding the underlying user utilities that are needed as well as the building blocks that make up these utilities. For example, the "payment token" building block has an impact on the ease, speed and transparency of payment transactions. Other examples of building blocks are wallets, smart contracts, dApps, tokens types, oracles, and so on.

Currently, the impact of blockchain in companies is mainly focused on efficiency, disintermediation and registration. And the impact is highest there where cooperating parties

unlock and create new data. In the future however complex blockchain implementations that drive decentralization and integration of ecosystems are expected to see the largest benefits of blockchain.

You can use the following simplified decision tree to estimate the use of a blockchain project:

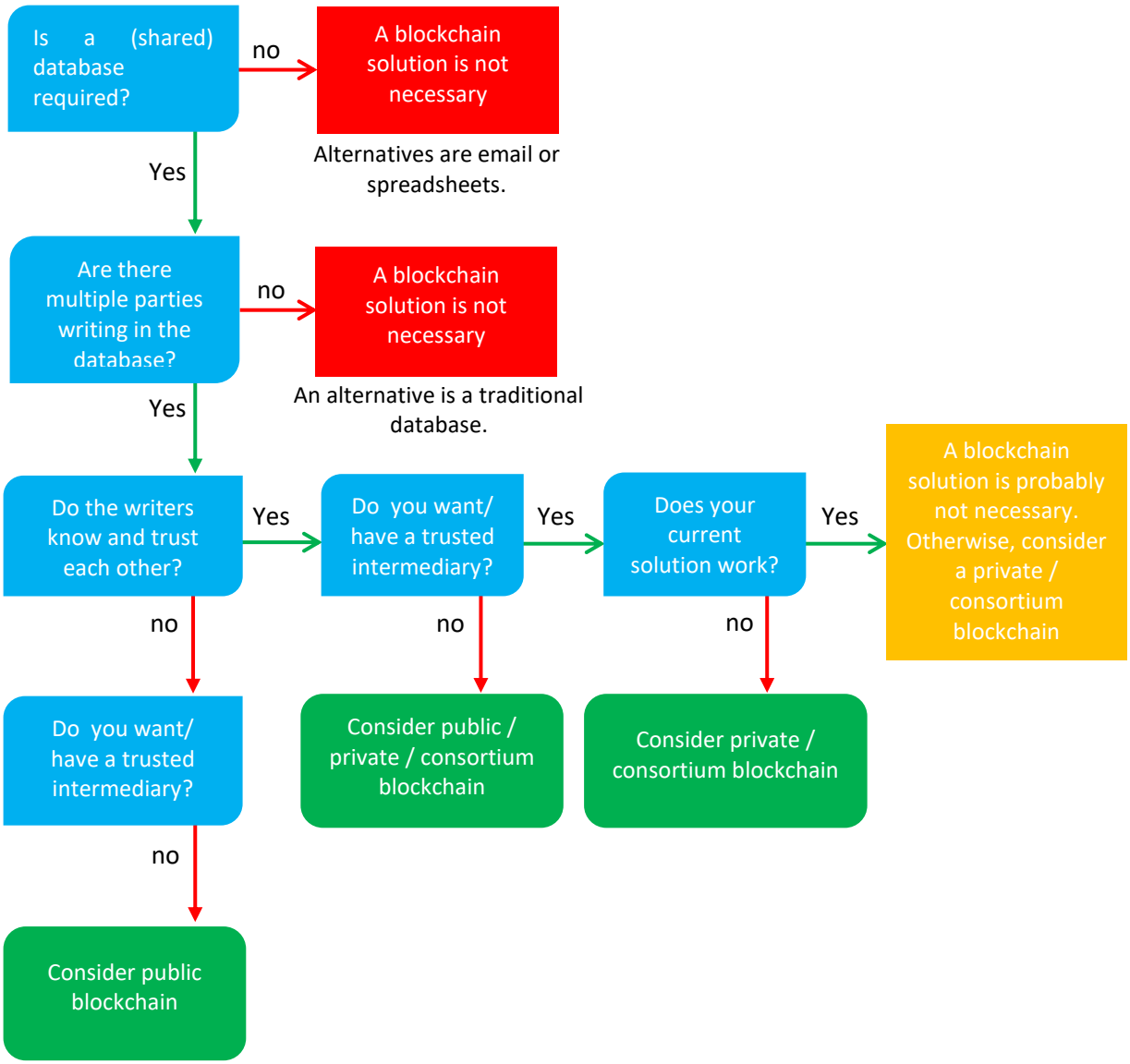


Figure 11: Simplified decision tree whether or not to use blockchain (Source: Lin Lim, C., Janse, A., Blockchain Basics, 2021).

5.4 Sources and Further reading

Ackermann, J. & Meier, M. (2018). *Blockchain 3.0: The next Generation of Blockchain Systems.*

Advanced Seminar Blockchain Technologies, Summer Term 2018, Technical University Munch.

AI Sweden, Lantmäteriet (2020, November). *Building an AI trust model for the public sector,* Consulted from https://www.ai.se/en/node/85154

Antonopoulos, A. M. (2016). *The Internet of money: talks by*. Merkle Bloom Llc.

Augur. (n.d.). *Overview*. Consulted on 23 December 2019, from https://docs.augur.net/#overview

Augur. (2018, July 9). *Forecast Foundation OU Privacy Policy*. Consulted on 23 December 2019, from Augur.net website: https://www.augur.net/privacy-policy/

Baraniuk, C. (2020, February 11). *Blockchain: The revolution that hasn't quite happened*. Consulted from https://www.bbc.com/news/business-51281233

Bitcoin Block Reward Halving Countdown. (2019). Consulted on December 23, 2019, from Bitcoinblockhalf.com website: http://www.bitcoinblockhalf.com

BMW, (2019, October 14). How Blockchain solutions can help driver. Consulted from https://www.bmw.com/en/innovation/blockchain-automotive.html

BMW Pressclub Global (2020, 31 March). *BMW Group uses Blockchain to drive supply chain transparency.* Consulted from https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency.

Buterin, V. (2013). *Ethereum white paper: a next generation smart contract and decentralized application platform* [White paper]. Consulted on 27 December 2019, from Blockchainlab: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, May 6). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide.* Consulted on 27 December 2019, from Ethereum.org website: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

ChainTrade. (2017, December 27*). 10 Advantages of Using Smart Contracts*. Consulted on December 27, 2019, from Medium website: https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. Journal of Organization Design, 7(1). https://doi.org/10.1186/s41469-018-0038-1

Kaoris Future. (2017) *The Land Registry in the blockchain – testbed*. Consulted from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia, ChromaWay & Kairos Future. (2016). *The Land Registry in the blockchain.* Consulted from http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Ledger Insights (2020, 31 March). *BMW expands supply chain blockchain for parts traceability.* Consulted from https://www.ledgerinsights.com/bmw-blockchain-supply-chain-parts-traceability/

Ledger Insights (2020, October 15), *Singapore Airlines extends its blockchain-based reward digital wallet*. Consulted on https://www.ledgerinsights.com/singapore-airlines-extends-its-blockchain-based-reward-digital-wallet/

Lin Lim, C., Janse, A., *Blockchain Handbook*, September 2021, Chapter 10. Publisher: De boekdrukker Amsterdam. NUR: 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

Microsoft, 2021, May 14). *Action Required: Migrate your Azure Blockchain Service data by 10 September 2021*. Consulted on https://azure.microsoft.com/en-us/updates/action-required-migrate-your-azure-blockchain-service-data-by-10-september-2021/

Microsoft (2019, May 2), *Singapore Airlines transforms customer loyalty with blockchain on Azure*. Consulted on 4

MOBI. (2019). *Vehicle Identity Standard*. Consulted from https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Nakamoto, S. (2008). *Bitcoin P2P e-cash paper.* Consulted on December 23, 2019, from Metzdowd.com website: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, September 30). *Re: I broke my wallet, sends never confirm now.* [Online forum comment]. Message posted on https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, November 1). *PayPal's recent power outage drives bitcoin adoption*. Consulted on December 23, 2019, from Bravenewcoin.com website: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Rauchs M., Blandin, A., Bear, K., McKeon, S. (2019). 2nd *Global Enterprise Blockchain benchmarking study*. Consulted from https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf

Schnuer, C. (2020, December 7). *Changing the property market through blockchain*. Consulted from https://delano.lu/article/delano_changing-property-market-through-blockchain

Strategyzer. (n.d.) *Business Model Canvas*. Consulted on December 23, 2019, from https://www.strategyzer.com/canvas/business-model-canvas

Sultan, K., Ruhi, U., & Lakhani, R. (2018). *Conceptualizing Blockchains: Characteristics & Applications.* 11th IADIS International Conference Information Systems 2018, 49–57

Vigna, P., & Casey, M. (2015). *The age of cryptocurrency: how bitcoin and the blockchain are*

challenging the global economic order. New York, N.Y.: Picador/St. Martin's Press.

Young, S. (2018). *Enforcing Constitutional Rights Through Computer Code.* Consulted from CUA Law Scholarship Repository website: https://scholarship.law.edu/jlt/vol26/iss1/5/