

## MASTER

### The Not-So Disruptive Nature of Blockchain Technology A systematic review

Kwant, Stefan

*Award date:*  
2023

[Link to publication](#)

#### **Disclaimer**

This document contains a student thesis (bachelor's or master's), as authored by a student at Eindhoven University of Technology. Student theses are made available in the TU/e repository upon obtaining the required degree. The grade received is not published on the document as presented in the repository. The required complexity or quality of research of student theses may vary by program, and the required minimum study period may vary in duration.

#### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain



# The Not-So Disruptive Nature of Blockchain Technology: A systematic review

Master Thesis Innovation Sciences

**Stefan Kwant 0965651**

---

Stefan Kwant, faculty IE&IS

1<sup>st</sup> Supervisor: Bert Sadowski, faculty IE&IS

2<sup>nd</sup> Supervisor: Kevin Gallagher, NOVA School of Science and Technology, Department of Computer Science

3<sup>rd</sup> Supervisor: Georgios Papachristos, faculty IE&IS

An aerial photograph of a modern, multi-story glass building at sunset. The building is illuminated from within, and the sky is a deep orange-red. The surrounding area includes trees and other city buildings in the background.

Eindhoven, April 10, 2023

# Contents

<b>1</b>	<b>Introduction</b>	<b>7</b>
<b>2</b>	<b>Theoretical Background</b>	<b>9</b>
2.1	Blockchain Technology . . . . .	9
2.2	Disruptive Innovation . . . . .	18
<b>3</b>	<b>Methodology</b>	<b>23</b>
3.1	Bibliometric Network Analysis . . . . .	23
3.2	Thematic analysis . . . . .	24
<b>4</b>	<b>Results</b>	<b>26</b>
4.1	Bibliometric network analysis . . . . .	26
4.2	Thematic Analysis . . . . .	27
<b>5</b>	<b>Discussion</b>	<b>34</b>
5.1	Overview of Results . . . . .	34
5.2	Research questions . . . . .	34
5.3	Implications . . . . .	35
5.4	Limitations . . . . .	36
5.5	Future research . . . . .	37
5.6	Conclusions . . . . .	37
5.7	Recommendations . . . . .	38
<b>6</b>	<b>Acknowledgements</b>	<b>39</b>
<b>7</b>	<b>References</b>	<b>40</b>
<b>8</b>	<b>Appendix A: Articles used in Thematic Analysis</b>	<b>46</b>
<b>9</b>	<b>Appendix B: Description of all themes</b>	<b>48</b>
9.1	Problem Statement . . . . .	48
9.2	Advantages . . . . .	50
9.3	Limitations . . . . .	53

## Abstract

Blockchain is often heralded as a disruptive technology that will shape the world of the future. An abundance of literature on blockchain claims that it will disrupt supply chain management, contribute to sustainability goals, give citizens control over their personal data and facilitate financial inclusion in Africa. However, there are also researchers that claim the very opposite. In a letter to the US congress, a collective of scientists claimed that “blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit”. The aim of this study is to address this dichotomy between these two views and to determine if blockchain can be considered a disruptive technology. We perform a bibliometric network analysis to identify different application domains of blockchain technology. Next, we use thematic analysis to study influential publications on blockchain, focusing on how they presented the problem(s) that blockchain solves and what advantages and limitations they associate with blockchain technology. Our results show that blockchain research often attributes advantages to blockchain that are not exclusive to blockchain technology. In addition, the limitations of blockchain technology have received relatively little attention, resulting in an overly optimistic view of the technology. This leads us to conclude that blockchain lacks the key attributes of a disruptive technology, as it is shown to be very expensive, hard to scale and the advantages of decentralisation and immutability do not outweigh these expected costs. We urge the academic community to be more transparent in blockchain research by adequately addressing its limitations and evaluating alternative technologies that may offer viable solutions to the suggested problems.

**Keywords:** Blockchain Technology, Limitations, Disruptive technology, Thematic analysis, Concerns, Critical analysis

## Summary

### Introduction

In the academic literature, blockchain is often heralded as a disruptive technology that will shape the world of the future (Tapscott and Tapscott, 2018). A common definition of blockchain is a decentralised, digital ledger that allows for peer-to-peer transactions to be conducted without the need of a central authority on a trustless network (Rauchs et al., 2018). Since the concept of blockchain emerged in 2008, scholars have explored the potential of blockchain in a wide variety of fields. Some authors claim that blockchain will make supply chains more efficient (Kshetri, 2018; Hald and Kinra, 2019; Köhler and Pizzol, 2020; Mukherjee et al., 2021), allow citizens to control their own personal data (Mainelli, 2017), contribute to the solution of a wide variety of sustainable development goals established by the United Nations (Aysan et al., 2021a,b; De Villiers et al., 2021) and blockchain will contribute to solving climate change (Dorfleitner et al., 2021).

However, there are also researchers who claim the very opposite. In a letter to the US Congress, a group of scientists claimed that “blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit”(concerned.tech, 2022). Moreover, research on the limits of blockchain has found that cryptocurrencies and the blockchains on which they operate are extremely unsustainable, requiring an ever increasing amount of electricity (De Vries, 2018; De Vries et al., 2022), while producing enormous amounts of electronic waste (De Vries and Stoll, 2021). It has also been found that blockchain facilitates certain practises related to shadow banking, is one of the causes of the financial crisis in 2008 (Allen, 2022; Steele, 2021), is related to an abundance of pump-and-dump schemes aimed at making a small group rich, at the expense of the majority who miss out (Dhawan and Putniņš, 2021; Hamrick et al., 2021; Peterson, 2021) and that cryptocurrencies are used to finance large amounts of illegal activity, according to research by Foley et al. (2019) half of all bitcoin transactions are associated with illegal activity. Finally, researchers are also questioning the decentralised aspect of blockchains (Walch, 2019; Ekblaw et al., 2016; Sai et al., 2021). A variety of mechanisms can cause centralisation to emerge in a decentralised network. One major issue is “the Oracle Problem”. The problem lies in the fact that even though the data stored on the blockchain is considered reliable, the information initially entered onto the blockchain may be inaccurate(Caldarelli, 2020). This currently reintroduces the need for a central authority to monitor if the data that is put on the blockchain is reliable.

This thesis investigates this dichotomy within blockchain research. On the one hand, there are researchers that claim that blockchain can disrupt a wide variety of markets, and on the other hand there are those that claim it will not achieve anything. This thesis answers the following research question: *“How applicable is the theoretical concept of disruptive innovation to blockchain technologies?”*

### Theoretical Background

To discuss blockchain technology, a basic understanding of blockchain and a clear definition are needed. A blockchain is essentially a ledger on which transactions can be recorded. In essence, a blockchain functions as a register for recording transactions, which may encompass monetary exchanges involving cryptocurrencies, as well as transactions of data. A blockchain always has the following general features:

- An append-only distributed ledger that stores data in time-stamped blocks, which are linked together via cryptographic hashes.
- A consensus mechanism which are the rules that regulate which and how new transactions can be added to the blockchain.
- A peer-to-peer network made of nodes that can only read and cooperatively write transactions on the blockchain (Ghiro et al., 2021).

Any decentralised transaction network is complicated by the double spending problem, which means that a user is able to spend the same money twice. In our current system, banks monitor transactions and make sure that someone cannot spend more money than they are allowed to. However, in a decentralised transaction network, such as a blockchain, there is no central authority that monitors transactions and for a long time this was the main hurdle to introduce decentralised transaction networks. However, Bitcoin was the first cryptocurrency that solved the double spending problem by applying blockchain technology (Nakamoto, 2008).

To fend off double spending attempts, a blockchain needs the following characteristics:

- **Tamper-proof:** It must be easy to verify that a registered transaction has not been altered after its recording, and it should be easy to determine if a transaction is altered at a later point in time.
- **Immutable:** A distributed payment system should make it very hard to tamper the data on the ledger. (Ghiro et al., 2021)

Blockchains achieve the tamperproof property by embedding Cryptographic Hash Functions (CHFs) into the blockchain data structure. In cryptography, hashing is a method that is used to convert data into a string of a fixed length, and the output will always be the same given the same input. Once the data is transformed, it is impossible to revert the hash of the data back to the original data. However, if the hash of a data set is known, it is possible to check if another data set is identical, by applying the same hash function to the second data set.

Transactions on the blockchain are stored in blocks. A block can contain a fixed number of transactions and contains the hash of all previous transactions. When a small change is made in a previous transaction, this will result in a completely different hash, and this invalidates the block. When a block is full, it is transmitted to all nodes in the network for validation. Nodes are the participants in a blockchain network that ensure that the blocks are valid and do not contain malicious transactions. The nodes essentially take the role of a bank in a centralised system in monitoring all transactions. A block can only be validated when a node solves a very difficult cryptographic puzzle in order to proof that they put in the resources to validate a block, this is called Proof of Work (PoW). In a PoW blockchain, a block is valid if the hash of the block contains a predefined number of leading zeros. However, as stated before, the hash of a block of data would always yield the same hash, as long as the data stays the same. Therefore, a random value is added to the data, called the nonce, and the nodes have to guess the nonce, which yields a hash that has the predefined number of leading zeros. In order to guess the nonce, a lot of computational power, and as a result energy, is expended. Once a node has guessed the nonce, it transmits its block to all other nodes, and they can easily check if the block is valid.

However, a malicious user that happens to be the first to find the nonce could still make a malicious transaction by selectively broadcasting its block, so different nodes believe different transactions are made. In order to prevent such an attack, a block is not immediately validated when the nonce is correct. After the first block is broadcast, all nodes will continue to validate the blocks and listen to other validated blocks. If a different block is received, two separate chains are created, one with the malicious block and one with the correct block. This is an example of a fork. When this kind of fork occurs, it means that different nodes believe that a different block order is the truth. Since the malicious node did not broadcast its block to all other nodes, all other nodes will continue to add blocks to the chain with the correct block. As soon as one branch is a predefined number of blocks longer than the other, the shorter chain is rejected. This mechanism is known as the “Longest Chain Rule” (Shi, 2019). Once a block is validated, the node that validated this block will receive a payment in the form of cryptocurrency.

The system ensures that the nodes act in a manner that maintains the integrity of the blockchain. It can be seen as a lottery system. In this analogy, the amount of computational power a node puts in is correlated to the number of tickets the node has. The more computational power is expended, the bigger the chance to win the price. If a node wants to make a malicious transaction, it is extremely unlikely that it will win the lottery as a result of the Longest Chain Rule. A malicious node needs to control 50% + 1 of all nodes to successfully make a malicious transaction, and this is extremely expensive. Nodes are incentivised to only validate correct blocks, since that is the only way to receive cryptocurrency from the validation process. Due to these mechanisms, the blockchain becomes practically immutable, since nodes would have to expend extreme amounts of resources in order to change data on the blockchain.

## A Blockchain Definition

We define a blockchain as:

An append-only chain of cryptographically-linked ‘blocks’ of data, maintained and updated by a decentralised network, with network nodes encouraged by economic incentives to engage non-strategically to maintain and secure the system so that the data - organised in a specific structure often referred to as ‘global ledger’ - is robust to adversarial interference, double-spend, censorship, counterfeit, collusion, tampering, or other types of malicious actions Rauchs et al., 2018, p. 21.

This definition complies with the three fundamental characteristics of a blockchain proposed by Ghiro et al. (2021):

1. Openness to anonymous users



2. Full & public history of transactions
3. A strong distributed consensus protocol.

These characteristics ensure the immutability of the blockchain. Private blockchains are proposed as more efficient alternatives to public blockchains, which were described above. In a private blockchain some decentralisation is sacrificed in exchange for better scalability. However, a more centralised blockchain cannot ensure the immutability of the data in the same way as a public blockchain. Moreover, various authors argue that a private blockchain is more akin to a traditional distributed ledger, rather than to a blockchain, that requires a strong decentralised consensus mechanism that incentivises people to act honestly (Ghiro et al., 2021; Catalini and Tucker, 2018; Gramoli, 2016; Narayanan and Clark, 2017; Ammous, 2016).

Blockchain is well-known for its implementation as a digital payment system. However, blockchain has been proposed as a potential solution for various industries that require data transfer and record management. In particular, industries that rely heavily on intermediaries could benefit from the implementation of blockchain, as it has the potential to eliminate the need for intermediaries, resulting in reduced transaction costs.

### Limitations of blockchain

Blockchain technology faces a variety of challenges that need to be mentioned when addressing the question whether blockchain can be considered a disruptive technology.

- Blockchain consumes a lot of energy, because PoW requires a lot of computers to spend a lot of computational power.
- Scalability is a big issue for blockchains. Due to the decentralised nature, growing the blockchain is very costly. Moreover, blockchain is very slow compared to traditional ledgers.
- Data privacy laws aim to give people control over their own data. However, on a blockchain, data cannot be modified or deleted.
- Since blockchain is decentralised and the addresses of users are pseudonymous, it facilitates illegal activity.
- Blockchain transactions cannot be reversed, even if the transaction was faulty.
- Data that enters the blockchain still needs to be valid. This currently still requires a central authority that could potentially be compromised.
- There are a variety of different mechanisms that centralise blockchains. This undermines the purpose of the blockchain in the first place.

### Disruptive innovation

Disruptive innovation replaces current products on the market over time by offering new, simpler, and more affordable alternatives that better meet the needs of a previously underserved or ignored customer base. The current study uses the disruptive innovation framework developed by Van Orden et al. (2011). Innovation can disrupt the market through low-end encroachment, when the new innovation is either significantly cheaper than existing products or it offers a new set of characteristics that creates a new market for the innovation. While this cheaper innovation may fall short on existing characteristics that customers value, it improves over time and takes over the market. Another way to disrupt the market is through high-end encroachment. This innovation is more expensive than existing technologies, but it provides significantly better characteristics or fulfils needs that were currently not attended to by existing products.

In order to identify a disruptive innovation, the following steps need to be taken (Nagy et al., 2016): 1) Identify the innovation and its characteristics, 2) Identify where in an organisation's value chain the innovation is used, and 3) Compare the potentially disruptive innovation with technologies currently used.

## Method

A bibliometric network analysis on 9476 articles on blockchain was conducted in order to identify the main application domains of blockchain technology, which were: Internet of Things, Supply Chain Management, Smart Grids, Healthcare, and Smart Cities.

The five most cited articles of each application domain were further analysed in a thematic analysis. Three primary thematic domains were established: problem statement, advantages, and limitations, and codes were created accordingly.

## Results

In accordance with prior work ([Chen et al., 2021](#)), we observed that blockchain characteristics are often double-edged swords. For example, while the transparency of data on the ledger facilitates accountability, it also causes data privacy problems.

Moreover, one key observation is that blockchain solutions are often suggested for issues that could be resolved using centralised digital technologies. It is essential for authors to clearly articulate why blockchain is superior to alternatives. However, academic research on blockchain rarely considers alternative solutions to these problems. Second, researchers need to support their problem statements with academic literature. Research is needed on what problems occur in different blockchain application domains and why blockchain could be a superior solution over other digital technologies.

Similarly, the analysis showed that a variety of advantages are attributed to blockchain technology, which are not necessarily exclusive to blockchain. It is imperative that when discussing blockchain technology, researchers critically look at what benefits are a result of using blockchain and which benefits could be achieved using different technologies. In doing so, blockchain research can provide a more nuanced understanding of the potential applications of the technology and help avoid overhyping its capabilities.

Finally, blockchain limitations receive very limited attention in academic research. It is imperative for scientific research on an innovation to consider both the potential and the limitations of an innovation. In particular, little attention is paid to the blockchain trilemma, which holds that blockchains cannot maximise decentralisation, scalability, and security at the same time. Other important limitations that receive little attention are the Oracle Problem and centralisation within blockchains.

## Discussion

The literature showed that the main characteristics that blockchain offers are immutability and decentralisation. These characteristics are achieved by having a blockchain that is completely open to anonymous users, having a complete and fully public history of transactions, and using a strong consensus protocol. This ensures that it is extremely expensive to collude and endanger the integrity of the blockchain network.

The main question is to what extent the different market segments are interested in these unique characteristics of blockchain technology. Our thematic analysis showed that these characteristics also come with significant disadvantages. This makes it questionable whether the market is interested in innovation. Although the current study was not a market analysis, we did observe that after a decade of blockchain research, no blockchain application has become mainstream or is widely applied in an industry. This leads us to believe that the inherent limitations of blockchain technology outweigh the advantages of decentralisation and immutability.

Blockchain technology is unlikely to disrupt markets through low-end encroachment, since it is significantly more expensive than traditional ledger technologies. Furthermore, blockchain does not perform better on currently valued characteristics of ledgers, such as scalability and speed, and therefore it will not disrupt the market by being a better, but more expensive, version of current products. An argument could be made that blockchain will disrupt the market through new-market disruption. The characteristics of blockchain may satisfy needs in the market that are currently not addressed, such as the need for decentralisation and immutability. However, blockchains can still be centralised in a variety of ways ([Sai et al., 2021](#)). Additionally, immutability does not guarantee data accuracy, so a central authority is still required to verify the trustworthiness of individuals or machines entering the data. This leads us to conclude that blockchain cannot be considered a disruptive technology.

These findings have various theoretical implications. First, academic articles must clearly define the type of blockchain they are discussing, as different characteristics are attributed to private blockchains compared to public blockchains. Second, research on blockchain should provide a clear rationale for why blockchain is the solution and should provide sufficient academic literature on which to base its rationale.



Third, researchers should pay more attention to addressing the limitations of blockchain technology. Specifically, how to work around centralisation tendencies of blockchain, for example caused by oracles.

Our study suggests several venues for future research. To determine the value blockchain technology can bring to an industry, it is necessary to conduct research that compares blockchain applications with the performance of technologies currently in use. Moreover, research is needed to establish the cost of scaling up a blockchain. Many proposed applications of blockchain require significantly more transactions and larger storage than current blockchain applications. Our study showed that scalability is a significant problem for blockchains, so further research can address the size of this problem.

This study provides compelling evidence why blockchain technology should not be considered a disruptive technology. Therefore, it is recommended that policy makers and managers take caution when considering an investment in blockchain technology. Since blockchain is unlikely to disrupt any industry soon, it is recommended that businesses exercise patience and wait to invest in blockchain until the technology has had time to mature.

## 1 | Introduction

In the academic literature, blockchain is often heralded as a disruptive technology that will shape the world of the future (Tapscott and Tapscott, 2018). A common definition of a blockchain is a decentralised, digital ledger that allows for peer-to-peer transactions to be conducted without the need for a central authority on a trustless network Rauchs et al. (2018). The first and most famous application of blockchain is Bitcoin. The goal of Bitcoin is to create a completely decentralised digital currency, removing control from banks, government, and other financial institutions (Nakamoto, 2008).

Since the concept of blockchain emerged in 2008, scholars have explored the potential of blockchain in a wide variety of fields. Some authors claim that blockchain will make supply chains more efficient (Kshetri, 2018; Hald and Kinra, 2019; Köhler and Pizzol, 2020; Mukherjee et al., 2021), allow citizens to control their own personal data (Mainelli, 2017), contribute to the solution of a wide variety of sustainable development goals set by the UN (Aysan et al., 2021a,b; De Villiers et al., 2021), enable an efficient smart grid electricity network (Mollah et al., 2020), facilitate financial inclusion in Africa (Agbo and Nwadiakor, 2020; Mavilia and Pisani, 2020), providing an ID to refugees (Franke, 2022) and blockchain will contribute to solving climate change (Dorfleitner et al., 2021).

In recent years, researchers have argued that there has been an overwhelming amount of hype surrounding blockchain (Nordgren et al., 2019; Ammous, 2016; Kazmi et al., 2021). It is rather difficult to find a current problem for which blockchain has not been proposed as a solution. This is prevalent in the academic literature as the opportunities of blockchain technology seem endless. However, there are also researchers that oppose the promises of blockchain technology and calls attention to the risks involved. In June 2022, 1500 scientists wrote a letter to the US Congress raising their concerns regarding the developments in the blockchain technology field (concerned.tech, 2022). These scientists stated that: “By its very design, blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit”.

There is also an emerging literature field that questions the potential of blockchain. In this tradition, it has been found that blockchain facilitates practices related to shadow banking, is one of the causes of the financial crisis in 2008 (Allen, 2022; Steele, 2021), is related to an abundance of pump-and-dump schemes aimed at making a small group rich, at the expense of the majority who miss out (Dhawan and Putniņš, 2021; Hamrick et al., 2021; Peterson, 2021) and that cryptocurrencies are used to finance large amounts of illegal activity, according to research by Foley et al. (2019) half of all bitcoin transactions are associated with illegal activity. Furthermore, research indicates that cryptocurrencies are extremely unsustainable, requiring an ever increasing amount of electricity (De Vries, 2018; De Vries et al., 2022), while producing enormous amounts of e-waste (De Vries and Stoll, 2021). Moreover, some academics argue that blockchains are not decentralised at all and that this undermines their entire purpose (Walch, 2019; Ekblaw et al., 2016; Sai et al., 2021). Finally, many blockchain applications face “the Oracle Problem”. While data on the blockchain might be immutable and trustless, the data that is entered on the blockchain may still be false to begin with. This is already a great obstacle for blockchain-based solutions that facilitate traceability in supply chains, as the information placed on the blockchain may be false to begin with (Caldarelli, 2020).

While research on the possibilities of blockchain is abundant and research on the limits of blockchain is also emerging, it is difficult to find studies that have systematically reviewed these two opposing positions in the literature. Research should always be objective and it is important that not only the opportunities of a technology are discussed, but also its limitations and how these can be overcome. Through a systematic review of the literature on blockchain technology, this study investigates the extent to which it can be categorised as disruptive, considering both its advantages and disadvantages. More specifically, the following questions will be addressed, based on Nagy et al. (2016) framework for defining disruptive innovation:

1. How applicable is the theoretical concept of disruptive innovation to blockchain technologies? (See Chapter 5: Discussion)
  - [a] What are the key features of blockchain technology that contribute to its disruptive potential? (See Chapter 2: Theoretical Background)
  - [b] What does the existing scientific literature suggest about the potential application domains of blockchain technology in relation to these features? (See Chapter 4: Results)
  - [c] To what degree do these application domains demonstrate the disruptive potential of blockchain technology? (See Chapter 5: Discussion)

The first sub-question is addressed in the theoretical background section, where a definition of blockchain is constructed, and the main characteristics of the technology are outlined. The second sub-question is tackled through a bibliometric network analysis, which clusters blockchain research into various application segments. This approach helps identify the most prominent areas of research and application of blockchain technology. Lastly, the discussion section answers the third sub-question by presenting the results of a thematic analysis, which examines the disruptive potential of blockchain. While blockchain technology has been hailed as a potential disruptive force in numerous industries, this study offers a critical assessment of its disruptive potential.

## 2 | Theoretical Background

In the scientific literature, the term blockchain is used to describe a variety of applications in the computer science domain. In section 2.1, a clear definition of blockchain is constructed. The first section provides a review of the fundamental principles of blockchain. Next, we will detail the distinction between a public and a private blockchain. Furthermore, an overview of the consensus mechanisms currently available is given. Finally, the specific features of blockchains are condensed into a connotative definition of blockchain, based on which the question of when you need a blockchain is addressed. In the second part of the theoretical background, the literature on disruptive innovation is discussed.

### 2.1 | Blockchain Technology

In the aftermath of the global financial crisis of 2008, Bitcoin's mysterious founder, or group of founders, developed Bitcoin as an "electronic payment system based on cryptographic proof instead of trust" (Nakamoto, 2008, p. 1). Bitcoin made the transaction of currencies possible, without a central authority validating your transactions. It achieved this in a rather remarkable way. Every transaction that was made on the Bitcoin network had to be validated by a group of participants, called miners. Every miner stores a copy of every transaction that has ever been completed on the Bitcoin network. To add a new transaction to this ledger, every miner has to solve a complex cryptographic puzzle. After solving this puzzle, the miner adds the transaction to their list of transactions and shares this with all other miners. Solving this cryptographic puzzle is hard and costs a lot of computing power, however, it is very easy to verify whether it is correct. This is very similar to how it is hard to solve a Sudoku but easy to check whether a solved Sudoku is correct. Once 50% + 1 of all miners agree on the same transaction list, the transaction is notified to the users and the miner who first solved the puzzle is rewarded with a payment in Bitcoin. Since it is very expensive to solve the cryptographic puzzle, in terms of electricity costs, this system incentivises miners not to add false transactions, since a single bad actor will only waste resources by trying to solve the cryptographic puzzle, but will never be rewarded, as there will not be 50% + 1 miners that agree on their transaction list (Ammous, 2016).

Bitcoin thus provided a transaction system without interference of a central authority like a bank, the underlying technology that was used to achieve this is known as blockchain technology. The blockchain features that were observed in Bitcoin, like decentralisation, resistance to cyberattacks, and the preservation of the user's privacy raised a lot of enthusiasm in the research community. As was mentioned in the introduction, an extremely large number of different applications were suggested, ranging from supply chain management (Kshetri, 2018) to financial inclusion in Africa (Agbo and Nwadiakor, 2020). This apparent universality of the blockchain suggests that the term might be used under different definitions (Ghiro et al., 2021). In this section, a definition of blockchain technology will be constructed by building on academic literature.

#### 2.1.1 | Blockchain Fundamentals

This section describes the fundamental principles of blockchain. In describing how blockchain works, everything starts when a transaction is issued. A transaction does not have to be a monetary transaction; it can also be the exchange of data. The introduction of this chapter described how the Bitcoin blockchain handles transactions. From a broader perspective, a blockchain can be considered a decentralised system that included the following general features:

- An append-only distributed ledger that stores data in time-stamped blocks, which are linked together via cryptographic hashes.
- A consensus mechanism, which are the rules that regulate which and how new transactions can be added to the blockchain.
- A peer-to-peer network made of nodes that can only read and write transactions cooperatively on the blockchain (Ghiro et al., 2021).

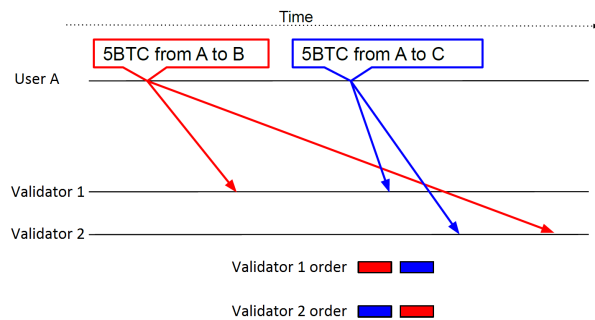
The group of entities in this peer-to-peer network that is allowed to write new transactions on the ledger are called the nodes<sup>1</sup>. Nodes also validate transactions on the blockchain and in order to do this, nodes need to know how many resources each user owns. This is determined by knowing the entire history

<sup>1</sup>In Bitcoin, nodes are referred to as miner or in Ethereum as validators

of transactions. However, any distributed transaction system is complicated by the double spending problem, briefly detailed below.

### Double Spending Problem

A user might try to make two transactions in quick succession. This transaction can be the transfer of a cryptocurrency, but could also be the exchange of data between two entities. Imagine that user A has 5 Bitcoin (BTC). They first transact 5 BTC to user B immediately followed by a transaction of 5 BTC to user C. Due to different propagation delays in the network, validator 1 receives the first transaction first, but validator 2 receives the second transaction first, see Figure 2.1.



**Figure 2.1:** Example of how propagation delays can result in different orders of transactions (Ghiro et al., 2021).

At this point, the nodes have to find an agreement on the correct order of transactions to determine which came first, and should be validated, and which came second, and should be rejected. This is a fundamental in distributed systems known as the Distributed Consensus Problem. A straightforward solution to this problem would be to add a timestamp to the transaction of user A.

However, a malicious user might alter the timestamps on their transaction in order to reject a transaction, thus falsifying the validation procedure. Therefore, a history of transactions may not be enough for correct validation. Traditional online payment services would solve the double spending problem by clearing every transaction through a central database. To fend off falsification attacks

in a decentralised payment system, the system needs the following characteristics:

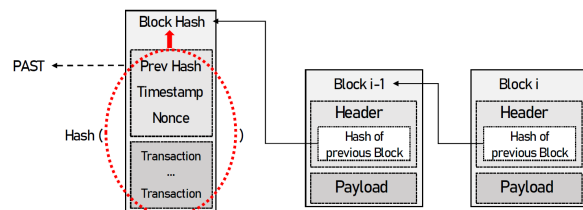
- **Tamper-proof:** It must be easy to verify that a registered transaction has not been altered after its recording, and it should be easy to determine whether a transaction is altered at a later point in time.
- **Immutable:** A distributed payment system should make it very hard to tamper with the data on the ledger.

These characteristics are essential in a blockchain ledger. The tamperproof property is achieved by embedding Cryptographic Hash Functions (CHFs) into the blockchain data structure, which is explained in Section 2.1.2. The immutability property comes from the consensus mechanism, which is described in Section 2.1.3.

### 2.1.2 | Blockchain Data Structure

Cryptographic hashing is an integral part of the blockchain data structure. In cryptography, hashing is a method that is used to convert data into a string of a fixed length, and the output will always be the same given the same input. Once the data is transformed, it is impossible to revert the hash of the data back to the original data. However, if the hash of a data set is known, it is possible to check if another data set is identical, by applying the same hash function to the second data set.

CHFs are crucial to make blockchains tamper-proof. This is achieved by storing every transaction on the ledger, along with the hash of all previous transactions, as is shown in Figure 2.2. Each block of data contains a list of transactions and once a block is full, the block needs to be validated, and this is where the nodes have to solve a cryptographic puzzle in order to proof that they put in the resources to validate the block, this is called the Proof of Work (PoW). In Bitcoin, this is done by applying the SHA-256 hashing function on the block. The hash of this block then consists of 256 0's and 1's.



**Figure 2.2:** The Blockchain Data Structure (Ghiro et al., 2021).

In Bitcoin, a block is valid if the hash of the block contains a predefined number of leading zeros. The number of leading zeros is changed to adjust the difficulty of finding a valid block. However, as stated before, the hash of a block of data would always yield the same hash, as long as the data stays the same. Therefore, a random value is added to the data, called the nonce, and the nodes have to guess the nonce, which yields a hash that has the predefined number of leading zeros. The block is then added to the blockchain and it is very easy for other nodes to validate this block, by checking whether it starts with the predefined number of zeros.

Although CHFs make the blockchain tamper-proof, as a small change anywhere in data on the blockchain will completely change the hash of the data on the blockchain, one malicious node could still be the first to find the correct nonce for their malicious transaction and get this validated by all other nodes in the above described system. It is important to note that any chain with a transaction that is not valid according to the agreed rules of the blockchain, for example, a chain that creates currency out of nowhere or double spends currency, is rejected by testing the chain against those rules. Furthermore, all transactions need to be signed using the private key of the sender, and thus the transaction can be easily verified using the public key of the sender.

An example of how a malicious node could make a malicious transaction is by trying to double spend their own currency. The following example describes how a double spending attack can occur. Node 1 wants to double spend its Bitcoin. It could do so by broadcasting to node 2 that 100 Bitcoin are transferred to Alice. However, this block is not broadcast to the rest of the validators. Node 1 then makes a transaction of 100 Bitcoin to Bob, and this transaction is added to the transaction pool and then validated by all other nodes in the network. If by pure chance, node 1 finds the correct nonce before the rest of the network, Bob will believe that they received their payment and conduct the transaction, for example, a payment in euro. As the other nodes are not aware of node 1 broadcasting to Alice, they will believe that the transaction by node 1 is valid, so node 1 has double spent its Bitcoin.

To ward off tampering attacks as described above, the network does not immediately verify all the transactions in a block after validation. After the first block is broadcast, all nodes will continue to listen to other validated blocks. If a conflicting block is received, two separate chains are created, one with the malicious block and one with the correct block. This is an example of a fork. When this kind of fork occurs, it means that different nodes believe that a different block order is the truth. Since the malicious node did not broadcast its block to all other nodes, all other nodes will continue to add blocks to the chain with the correct block. As soon as one branch is a predefined number of blocks longer than the other, the shorter chain is rejected. This mechanism is known as the “Longest Chain Rule” (Shi, 2019) and together with guessing the nonce, this is needed to validate a block and this is what makes the blockchain immutable. A malicious validator will have to out-compete all other nodes for an extended period of time in order to make a false transaction. In practise, the only way a malicious validator could out-compete all other nodes is by having 51% of all computing power.

### 2.1.3 | Consensus Mechanisms

In the aforementioned example of a blockchain, consensus is reached through Proof of Work. Proof of Work is an example of a consensus mechanism that a blockchain uses to decide which block is valid. Consensus mechanisms are a decision-making process for a network where participants in the network construct and support a decision that works best for the network. In this section, the three most common consensus mechanisms will be discussed. Furthermore, the blockchain trilemma, which formulates how blockchains are limited in the extent to which they can be decentralised, scalable, and secure, is discussed.

The most common way to reach consensus is through voting, in which each individual has one vote. This works in traditional centralised networks, where there is an authority that keeps track of identification of the voters, as you do not want a single individual to cast multiple votes. However, there is no authority that checks your identity on a blockchain. This would undermine the goal of decentralisation and introduce a single point of failure. Therefore, most blockchains work with so-called “proofs”. Instead of proving your identity, a node proves its commitment to the blockchain in different ways. All nodes participate in a lottery in which the participant that shows the most commitment has the highest chance of winning the lottery.

#### Proof of Work(PoW)

In Section 2.1.2 Proof of Work was introduced. In Proof of Work, nodes are tasked with guessing the nonce, a process that involves attempting many different values and using brute force to arrive at the solution. Other nodes can easily check if the solution is correct, but finding the solution in the first place is extremely difficult. This consensus mechanism forces nodes to commit a lot of computing power, and this



in turn results in electricity costs. However, the node whose block is validated is commonly rewarded in the form of the cryptocurrency whose ledger is on the blockchain, to incentivise the behaviour of the node. One common objection to PoW cryptocurrencies is that they consume a huge amount of energy (De Vries, 2018). Furthermore, the transaction speeds are fairly slow. Firstly, it needs to be significantly hard to find the correct nonce to ensure security and secondly, after a block has been validated, a transaction will only occur after the predefined number of blocks have been validated after this block.

### **Proof of Stake(PoS)**

PoS is designed as a more energy-conscious alternative to PoW that relies on economic rationality to achieve consensus. In PoS, all nodes stake a certain amount of their resources, commonly cryptocurrency, to participate in a lottery. The lottery is biased so that nodes that staked more resources have a higher chance to win. The reasoning behind this consensus mechanism is that owners of cryptocurrency have an interest in keeping the network trustworthy and running. If these owners would not do this, this would quickly devalue the worth of their cryptocurrency and they would lose money.

### **Delegated Proof of Stake (DPoS)**

DPoS is a variant of PoS and is dependent on stakeholders to vote on delegates. The votes by the stakeholders are weighted according to the amount of resources, commonly cryptocurrency, is staked. These delegates are responsible for validating the blocks. In some applications, the delegates need to make a deposit, known as the escrow, that can be confiscated if they do not run the internal consensus mechanisms honestly. This method is significantly faster than PoW and PoS, since a small group of elected delegates gets to decide which blocks are valid, rather than a decentralised network of nodes. These delegates are presumed to be trustworthy since they are committed and accountable since they have made the deposit.

The above examples of consensus mechanisms each have their advantages and disadvantages. However, it is impossible to resolve all the disadvantages of a blockchain system due to a phenomenon known in blockchain research as the scalability trilemma.

### **Scalability Trilemma**

The scalability trilemma, also called the blockchain trilemma, is a major challenge for blockchain developers. The scalability trilemma illustrates the conjecture that a decentralised database cannot be fully decentralised, fully secure, and fully scalable at the same time. The above examples of consensus mechanisms show this as well. PoW is fully decentralised and secure; however, it is very hard to scale, given the low transaction rate and the high energy cost (Chauhan et al., 2018). PoS is more scalable, since it does not have a high energy cost. However, this comes at a cost in the loss of decentralisation, since only people who own a lot of cryptocurrency get to govern the blockchain. DPoS is even more centralised, as stakeholders now vote on delegates, instead of directly on transactions on the blockchain.

## **2.1.4 | Public and Private Blockchain**

Up to this section, only public or permissionless blockchains have been discussed. A public blockchain is a blockchain network where everyone can participate. In Bitcoin, for example, everyone can be a node and set up their own mining equipment. In addition, the data on the ledger is visible to anyone and any node can make transactions on the blockchain. Another feature of public blockchains is that they offer high security. It is extremely hard to tamper data on a PoW blockchain as described in Section 2.1.2. Another feature is that the users are pseudonymous. This means that although it is visible to everyone that a certain transaction was made to a wallet, the system does not show who owns the wallet.

Public blockchains allow users to interact free from a trusted centralised authority, such as banks, with the addition that transactions are transparent, without uncovering the identity of the user. Consensus mechanisms and cryptography ensure that the data on the blockchain is tamper-proof and immutable and can thus be trusted, as detailed in Section 2.1.2. A public blockchain can be considered as a trust builder in a trustless environment and as an enabler of an open, privacy-preserving, and disintermediated marketplace (Berg et al., 2017; Ghiro et al., 2021)

Private or permissioned blockchains arose as an attempt to improve the scalability of blockchains and to make the blockchain data structure more suitable for enterprises, who do not want all their data publicly available. Private blockchains are governed by an organisation or group of organisations, and they decide who can participate in the network and who has rights to view the data on the blockchain. In a public blockchain, trust in the network is ensured through the PoW consensus mechanism and through hashing. However, in a private blockchain, the organisation appoints the validating nodes, and hence a

certain degree of trust in these organisations is necessary. The security of private blockchain depends more on traditional authentication mechanisms than on the strength of PoW. This allows blockchain managers to replace the resource-hungry consensus mechanisms of permissionless blockchain, with more efficient and faster ones (Ghiro et al., 2021). Businesses typically cannot tolerate the low transaction rates and high resource cost of public blockchains, and private blockchains provide a more efficient alternative.

While private blockchains are much more scalable, they are much less decentralised (Chu and Wang, 2018). This leads some academics to raise the question if private blockchains should be considered blockchains (Gerard, 2017; Ghiro et al., 2021; Catalini and Tucker, 2018). Private blockchains do not adequately protect against double-spend attacks, since they are not immutable (Catalini and Tucker, 2018), since a certain degree of trust in the nodes is necessary (Gramoli, 2016). In Section 2.1.5 a definition of blockchain will be constructed by looking at various existing definition.

### 2.1.5 | A Blockchain Definition

In the previous sections, the structure of blockchain and its characteristics have been discussed. Furthermore, the trade-offs and limits of different consensus models have been discussed. In this section, a precise definition of blockchain is proposed. The simplest definition of blockchain that can be found in the literature comes from the 1970s (Halatsis and Philokyprou, 1978). From a computer science perspective, a blockchain can be defined as a data-structure made of blocks of information chained by hash-pointers. However, since the advent of Bitcoin and cryptocurrencies, the meaning of blockchain has become more restrictive. This first definition does not include characteristics that are now commonly attached to blockchain, such as immutability and transparency. In their discussion on different blockchain definition, Rauchs et al. (2018) provide the following narrow definition of blockchain:

An append-only chain of cryptographically-linked ‘blocks’ of data, maintained and updated by a decentralised network, with network nodes encouraged by economic incentives to engage non-strategically to maintain and secure the system so that the data - organised in a specific structure often referred to as ‘global ledger’ - is robust to adversarial interference, double-spend, censorship, counterfeit, collusion, tampering, or other types of malicious actions (p. 21).

This narrow definition highlights the key characteristics commonly attributed to blockchains. Ghiro et al. (2021) define blockchain by its most important characteristics. The characteristics of a blockchain are the following.

1. Openness to anonymous users
2. Full & public history of transactions
3. A strong distributed consensus protocol.

These characteristics match very well with the definition given by Rauchs et al. (2018). First, openness to anonymous users is fundamental for decentralisation. If identification of users was required, a central authority would be needed, compromising the decentralisation of the blockchain. Furthermore, it enables the blockchain to preserve the privacy of its users better than what banks or centralised shared ledgers do. Openness to anonymous users does pose a new problem regarding the dispute of transaction, as it is not possible to prosecute an anonymous user in case of fraud. Therefore, users must accept that any transaction is indisputable.

Second, the ledger should be fully public, to enable the validation of the correctness of the ledger by anyone. If only a small group of users control the ledger, these users could collude and double spend resources. A fully public and transparent ledger enables people to verify that no resources have been double-spend.

Third, a strong distributed consensus mechanism is needed to avoid tampering with the chain. As described in Section 2.1.2, the immutability characteristic of blockchains is derived from its consensus mechanisms. There must be sufficient incentive for users to act honestly, making it more expensive for malicious users to make a fraudulent transaction.

However, some academics argue that this definition is too narrow as it excludes existing and potential future applications of distributed ledger technologies (DLT), such as private blockchains. Rauchs et al. (2018) opt for the term DLT system, rather than blockchain and they describe DLT systems in terms of both characteristics and provide a formal definition. The main characteristics of a blockchain should be:

1. **Shared record-keeping:** enable multiple parties to collectively create, maintain and update a shared set of authoritative records (the ‘ledger’).

**2. Multi-party consensus:** enable all parties to come to agreement on a shared set of records

- [a] If permissionless, without relying on a single party or side-agreements, and in the absence of ex ante trusted relationships between parties; and
- [b] If permissioned, through multiple record producers who have been approved and bound by some form of contract or other agreement.

**3. Independent validation:** enable each participant to independently verify the state of their transactions and the integrity of the system.

**4. Tamper evidence:** allow each participant to detect non-consensual changes applied to records trivially.

**5. Tamper resistance:** make it hard for a single party to unilaterally change past records (i.e. transaction history).

Therefore, Rauchs et al. (2018) propose the less restrictive definition:

A DLT system is a system of electronic records that i) enables a network of independent participants to establish a consensus around ii) the authoritative ordering of cryptographically-validated ('signed') transactions. These records are made iii) persistent by replicating the data across multiple nodes, and iv) tamper-evident by linking them by cryptographic hashes. v) The shared result of the reconciliation/consensus process - the 'ledger' - serves as the authoritative version for these records. (p. 24)

The main difference from the first definition is that this definition includes private blockchains. Rauchs et al. (2018) hold that the objective of a DLT system is to create a collection of verified and executed official records using a consensus process that involves multiple independent entities, without the involvement of a central authority.

In summary, two definitions of blockchain can be discerned. One definition includes both public and private blockchains, such as Rauchs et al. (2018) and one definition that only includes public blockchains in its definition. In this article, we follow the definition of Ghire et al. (2021), which limits the definition of a blockchain to public blockchains. Ghire et al. (2021) hold that by reintroducing centralised trust and not being completely open to the public, private blockchains are more akin to traditional distributed ledgers, rather than to blockchains, which require a strong decentralised consensus mechanism that incentivises people to act honestly. This view is broadly supported by the literature (Catalini and Tucker, 2018; Gramoli, 2016; Narayanan and Clark, 2017; Ammous, 2016).

### 2.1.6 | Applications of blockchain

With a clear definition of blockchain in mind, the next step is to describe why people believe that blockchain will be so impactful. In the previous chapter, the essence of blockchain was discussed. Blockchain allows network members to transact with each other, without having a trusted intermediary, in a trustless peer-to-peer setting. Blockchain has seen many proposed applications, which can be divided into three main fields: (Ammous, 2016)

#### Digital Payment

The most well-known application of blockchain is that of decentralised digital payments. Current digital payments rely on centralised authorities to maintain account balances and record transactions. In a blockchain, every transaction is transmitted to all nodes that maintain the ledger in a decentralised manner. Since no intermediary is needed, value and digital assets can reliably be transferred between distant parties without any external organisation.

#### Database & Record Management

A blockchain can essentially be used as database that is used to store immutable information. Once information has been put on the blockchain, it cannot be tampered with and therefore data on a blockchain is more reliable. Moreover, data stored on the blockchain is publicly available, thus increasing the transparency of the data. If organisations put their data on the blockchain, they can be held accountable if malicious activities are registered on the blockchain.

#### Self-executing Contracts

The third proposed application of blockchain is that of self-executing contracts that are automatically triggered by changes on the ledger. These so-called smart contracts use data on the blockchain to trigger

transactions. Once a smart contract is deployed on the blockchain, it cannot be interfered with. The core idea here is that if two parties make an agreement, the smart contract can enforce this agreement by digitising this agreement and by automatically making a transaction once certain conditions are met.

### 2.1.7 | Limitations of Blockchain

Much of the academic literature focusses on the potential of blockchain to have an impact in a variety of sectors. However, in order to get a holistic view of blockchain technology, it is important to also consider those who raise concerns about blockchain technology. In this section, the academic literature on the limitations of blockchain is discussed.

#### Energy consumption

In a blockchain, every transaction must be validated and recorded by every node. Moreover, in Proof-of-Work blockchains, all nodes have to perform computations, which requires a lot of energy. Recent research estimates that electricity consumption is 14.63 GW or 0.57% of the total electricity consumption of the world (CCAF, 2023). There are concerns about the environmental impact of blockchain technology if large-scale adoption is achieved (De Vries et al., 2022)

#### Scalability issues

Blockchain requires all nodes to validate all transactions and store the entire ledger. First, the validation process is hard to scale because the larger it is, the more energy needs to be consumed, which is costly. Second, the transaction ledger grows exponentially faster than the number of nodes, since each transaction needs to be stored by all nodes. Thus, the storage and computational burden on the nodes will eventually become too large to be sustainable and profitable (Ammous, 2016).

Furthermore, Proof-of-Work blockchains can only support a limited amount of transactions. Bitcoin can currently handle less than seven transactions per second (tps). In comparison, Visa has achieved 47,000 tps and averages around hundreds of millions transactions per day. If a blockchain with a block size of 1 MB was to support that many transactions, the ledger would grow by over 400 TB per year. Storing that much data would require a large amount of storage and infrastructure, making it unfeasible for all but the largest enterprises, reintroducing centralisation, which is the very opposite of what blockchain is intended for (Vujičić et al., 2018).

#### Regulatory issues

In the European Union, data privacy laws aim to give people control over their own data. Specifically, someone needs to be able to delete their own data. However, a blockchain is an append-only ledger on which all data should be public, and to ensure the immutability characteristic of blockchain, data cannot be modified or deleted. Moreover, the General Data Protection Regulation (GDPR) holds that there should be a data controller that governs the data. A blockchain should be completely decentralised in order to ensure immutability, and therefore there cannot be a singly authority governing the data. This is a problem for organisations that want to use blockchain, as they also have to comply with the GDPR (Haque et al., 2021).

#### Illegal activities

Due to the decentralised and pseudonymous nature of cryptocurrency transactions, it is attractive to use cryptocurrency for illegal transactions. Banks have the obligation to control transactions that are made within their system, to prevent illegal transactions, such as money laundering or funding terrorism (Akartuna et al., 2022). The bank can check who has made an illegal transaction and can identify the culprits. However, since blockchain is not governed by a central authority, illegal transactions can be made without regulation. Moreover, due to the immutable nature of blockchains, the transaction is also irreversible, even when it is discovered that the transaction was illegal (Foley et al., 2019).

#### Irreversibility

With transactions on centralised ledgers, human or software errors can easily be reversed by the governing organisation. However, once a block has been confirmed and new blocks are attached to it, it is only possible to reverse the transaction by means of a fork. A blockchain that would be alterable by a central authority does not make sense, as this is in conflict with the core characteristics of blockchain, namely immutability and decentralisation (Ammous, 2016).

## Security

The security of a blockchain is entirely dependent on the expenditure of resources for the validation of transactions. The system remains secure because the nodes that expend these resources are compensated in the currency of the payment system itself to align their incentive with the goals of the network. If a node or group of nodes manage to control 51% of the resource that needs to be expended, then the network is no longer protected against a double spending attack (Lin and Liao, 2017). Therefore, it is important to expend a significant amount of resources to make a 51% attack as expensive as possible.

## The Oracle Problem

Any blockchain application that involves transactions of off-chain data faces “the Oracle Problem” (Egberts, 2017). Oracles are the gateways between the blockchain and the physical world. Oracles are fundamental for most applications of blockchain, as they allow smart contracts to access data from sources other than the blockchain. As mentioned above, smart contracts allow for the automatic execution of a transaction under certain conditions. For example, a smart contract might state the following: When the delivery package arrives at the customer, a transaction of five tokens of cryptocurrency is made to the user that sends the package. However, someone or something needs to tell the blockchain that the package arrived at its destination, and this is the oracle. In the previous example, the oracle could be the delivery person, who confirms that the delivery reached its destination. However, this reintroduces a single point of failure, thus jeopardising the acquired benefits of decentralisation. The delivery person could collude with the sender of the product and confirm delivery, even if the package was never delivered.

One often mentioned solution is automated oracles. An automated oracle uses digital information for confirmation. In the previous example, a GPS tracker in the package needs to confirm that the package reached its destination, along with the confirmation of the delivery person. This two-step verification does reduce the trust we need to have in the first oracle. However, GPS signals can still be spoofed, so it is still possible to collude in this example (Egberts, 2017).

Oracles reintroduce a single point of failure, and thus negate the advantages of decentralisation that blockchains offer. In many solutions to the Oracle Problem, a centralised authority that monitors the oracles is needed to ensure that dishonest oracles can be punished (Caldarelli and Rossignoli, 2022).

## Unintended Centralisation

Even though blockchain was initially implemented to enable circumventing centralisation in a network, new avenues of centralisation in blockchains are emerging (Sultanik et al., 2022; Walch, 2019). For a more comprehensive and detailed discussion on this the topic, we recommend the work of Sai et al. (2021). Their work provides a thorough exploration of the topic and offers valuable insights that complement the discussion presented in this paper. In this section, we only touch upon a few of the centralising factors in blockchains.

Although public blockchains often have an open platform for proposing improvements, such as BIP for Bitcoin and EIP for Ethereum, centralisation still occurs at the governance layer of a blockchain. It is often a small subset of all participants on the blockchain that are active in the voting process for improvements or modifications to the network. The group that controls the improvement protocol has a large impact on the future of the network. If a select few developers primarily drive the development of the network, it contributes to centralisation (Azouvi et al., 2019; Sai et al., 2021).

Another centralising factor in blockchains is that of consensus power centralisation. In Bitcoin, consensus power depends on the amount of computational power the node can expend for the Proof-of-Work. Nodes that cannot expend large amount of computational power have a lower probability to guess the nonce, and this leads to a lack of stable income. This has prompted users to mine as a group and share the profit. These groups are known as mining pools. In a mining pool, a pool manager decides which transaction to include in a block and distributes the workload among participants of the pool. However, this type of structure reintroduces a trusted authority, thus limiting the decentralisation of the blockchain (Chesterman, 2018). On average, the four largest Bitcoin mining pools controlled more than 50% of the computational power. If these four mining pools would collude, this can result in a 51% attack (Sai et al., 2021).

The exchange of cryptocurrency to fiat currency happens on application layer entities known as exchanges. They serve as a mechanism for establishing consensus on the exchange value. Vulnerabilities present in exchanges have been targeted by attackers to carry out successful attacks on Bitcoin and Ethereum on numerous occasions (Chia et al., 2018). Centralised systems that serve as a central key repository represent a single point of failure. This was illustrated by the closure of the centralised exchange called Mt. Gox following the exploitation of multiple security flaws that resulted in the loss of Bitcoins

from its users (Abrams et al., 2014). The attacks on centralised exchanges have instilled doubts in the community over the security of the network. In Bitcoin, seven centralised exchanges serve more than 95% of all trades (Sai et al., 2021).



## 2.2 | Disruptive Innovation

To better understand the topic of disruptive innovations and how they impact established businesses, a review of the existing literature is conducted. The review first provides an overview of what disruptive innovations are, how they arise, and their effects on the market. The literature is then presented that describes a way to identify disruptive innovation in the market.

### 2.2.1 | Definition of Disruptive innovation

Christensen's theory of disruptive innovation (Christensen, 1997) is based on the idea that when a company tries to make a product that meets the needs of high-end customers, they often create a product that is too advanced for mid- to low-end customers along a key performance dimension. This creates an opportunity for a new product to enter the market. This new product is not as good as the first product along the key performance dimension, but is lower cost or performs better along a second dimension. While existing high-end customers dislike the new product because it does not meet their needs along the first dimension, a new market segment or the existing low-end segment is happy to accept the lower performance along the first dimension in exchange for lower cost or better performance along the second dimension.

However, over time, the new product is continually improved, particularly with regard to the first performance dimension, where it was initially inferior to the old product. Through this continuous upgrading, the new product becomes acceptable to customers of the old product, who then switch from buying the old product to the new product. With further upgrading, the new product eventually becomes acceptable to high-end customers as well, who also switch from the old product to the new product. This process is called low-end encroachment, because the new product starts at the low end of the market and gradually moves upward toward the high end, potentially after first selling only to a new market segment (Christensen, 1997).

One example of a disruptive innovation in history is the steam engine. Before the steam engine, most industrial processes were powered by water wheels or windmills. The steam engine, developed in the 18<sup>th</sup> century, was initially less efficient and more expensive than these traditional sources of power. However, it offered the advantage of being able to operate in any location, rather than being limited to sites with fast-flowing rivers or steady winds.

As technology improved and costs decreased, steam engines began to replace water wheels and windmills in many industries, including mining, manufacturing and transportation. The steam engine was a disruptive innovation because it introduced a new set of performance attributes, such as location flexibility and scalability, that fundamentally changed the way many industries operated. Over time, the steam engine became the dominant source of power for industrial processes and paved the way for many other technological innovations.

The theory of disruptive innovation has faced criticism for its lack of a widely accepted definition. This has led to the term being loaded with various meanings and connotations (Schmidt and Druehl, 2008). Christensen himself provided only a loose definition of disruptive innovation (Klenner et al., 2013), and did not establish clear criteria to determine whether a particular innovation is considered disruptive (Danneels, 2004). Despite this lack of consensus on a precise definition, there is some agreement in the literature on the general concept of disruptive innovation. Most definitions emphasise that disruptive innovation involves the introduction of a new set of performance attributes along which firms can compete (Govindarajan and Kopalle, 2006; Danneels, 2004; Kostoff et al., 2004).

In his original work, Christensen (1997) described disruptive innovations as having initially lower performance, highlighting different product attributes, or being first launched in emerging or insignificant markets.

#### Lower Performance

In the context of disruptive technology, a "lower attack" refers to the way in which these technologies often enter the market at a lower price point with lower performance than existing technologies (Christensen, 1997). Disruptive innovations are often less expensive and have lower profit margins than the existing solution. Christensen (1997) calls the process of technology diffusion in low-end markets low-end encroachment. The term encroachment denotes that the new product takes sales away from the old product. Low-end encroachment describes the scenario where the new product first displaces the old product in the low end of the old product market and then diffuses upward. The low end of a product market is defined to consist of those customers with the lowest willingness to pay for the product (Schmidt and Druehl, 2008; Christensen, 1997). According to Adner (2002), while a certain level of performance is necessary for a disruptive technology to gain traction, it is ultimately the price of the technology that

determines its success. When the existing solution exceeds the minimum functional threshold, customers are less willing to pay for additional performance improvements. At this point, technologies that offer lower performance at a lower price become more attractive to consumers. This is because consumers' performance requirements are already being met, so they are willing to trade some performance for a lower price.

Firms that are already well established in the market may not perceive disruptive technology as a threat because it is initially inferior to existing technologies. The new technology may not be as advanced or offer the same level of performance, so incumbent firms may not see it as a serious threat to their market share (Schmidt and Druehl, 2008). As a result, they may not invest as much in the new technology or take steps to defend against it. This can allow disruptive technology to gain foothold in the market and eventually disrupt the existing market. Additionally, incumbent firms may be hesitant to invest in a new technology that has not yet proven itself in the market, and may prefer to wait and see how it performs before making any major investments.

An example of a technology that disrupted the market through low-end encroachment is the personal computer. In the early days of computing, computers were large, expensive machines that were mainly used by businesses and government organisations. However, as personal computers became more affordable and powerful, they began to compete with the larger and more expensive computers that were already on the market. This led to a decline in the market for larger and more expensive computers, as personal computers were able to offer many of the same capabilities at a lower price point. This is an example of low-end encroachment, as the personal computer was a cheaper and lower-end alternative to the existing solution. As suggested by the personal computer example, disruptive innovation maps to low-end encroachment. High-end encroachment progresses in reverse fashion, starting at the high end of the old-product market (Schmidt and Druehl, 2008; Schmidt and Porteus, 2000). The DVD is an example of high-end encroachment because it was a more advanced technology that could compete with existing solutions in the high-end market. The DVD was a much smaller and more versatile format compared to VHS tapes, which was able to store more data and offer higher-quality audio and video. This made it an attractive alternative to VHS tapes for consumers willing to pay a premium for the improved technology.

Sood and Tellis (2011) conducted research on 36 technologies in seven markets and found that although entrants with lower attacks can cause disruption, this phenomenon has been exaggerated. In fact, disruptions caused by entrants using a lower attack account for only a small percentage of cases. For example, only 8% of all technological disruptions and 25% of all firm disruptions were caused by entrants using a lower attack. Danneels (2004) cites the DVD as an example of a technology that did not use a lower attack to disrupt the market. This is because the DVD had higher performance than the existing technology, VHS tapes, when it was first introduced. The DVD offered higher resolution, clearer picture, and other benefits that made it more attractive to consumers. As a result, it was able to quickly gain market share and disrupt the VHS market without using a lower attack.

### Different Attributes

While disruptive technologies may initially start with lower performance on dimensions valued by mainstream markets, they have higher performance on alternative dimensions valued by emerging market segments. These technologies change the way competition is conducted by altering the performance metrics on which firms compete. The needs and desires of customers drive them to seek specific benefits from the products they use, which forms the basis for their choices between competing products. The benefits that customers seek determine the attributes of the product they value, and different segments of the market may value different attributes. Competing products offer varying levels of performance on various dimensions (Danneels, 2004).

One example of disruptive technology that changed the market by offering different attributes is the smartphone. Before the advent of smartphones, mobile phones were mainly used to make calls and send text messages. Smartphones, on the other hand, offered a range of additional features such as internet access, GPS navigation, and app-based services. These features were not as important to mainstream consumers, who were primarily interested in making calls and sending texts, but were highly valued by emerging market segments such as young professionals and tech-savvy individuals. As a result, smartphones were initially seen to have lower performance on dimensions valued by mainstream markets, since they were not optimised only for calling and texting, but they ultimately disrupted the market by offering higher performance on alternative dimensions.

This smartphone example also shows how disruptive technologies do not necessarily disrupt the market through low-end encroachment. The smartphone was more expensive than the existing cellphones. The new market segment values the unique attributes of disruptive innovation so highly that they are willing

to pay a high price for it, even though the new product may not perform as well as the existing solution on the parameter that mainstream customers prioritise. This is because the alternative attributes of the disruptive innovation are more important to the new market segment than the performance on the mainstream parameter (Schmidt and Druehl, 2008). In addition, Sood and Tellis (2011) also found contradictory results in Christensen's statement that disruptive innovations are generally cheaper. While they acknowledge that a lower price can increase the likelihood of disruption, they found that most potentially disruptive innovations do not enter the market at a lower price than existing technologies. In other words, although a lower price may be an effective strategy to disrupt the market, it is not the only factor at play.

### Emerging Markets

Christensen (1997) made a distinction between low-end disruptions and new-market disruptions. New market disruption refers to the process by which a new market entrant, offering a novel product or service, shakes up the existing market, and disrupts the status quo. This can lead to significant changes in the way the market functions and can potentially lead to the decline of established market leaders who are unable to adapt to the changing market conditions. A fringe market is a small and specialised market that is often outside of the mainstream market. A new-market disruption often starts by attracting customers in a fringe market segment before eventually moving up to compete with established market players. This can result in low-end encroachment, where the new market entrant begins to steal customers from established players at the lower end of the market before moving upward.

### A Framework for Disruptive Innovation

Van Orden et al. (2011) have created a framework for different encroachment patterns in different markets, as shown in Table 2.1. This framework is a way of understanding the ways in which new technologies enter the market and disrupt existing products and services. According to this framework, there are six different paths a new technology can take to gain foothold in the market.

Sustaining innovation is a type of innovation that seeks to improve existing products or services, rather than creating entirely new ones. This type of innovation is often incremental, meaning that it involves small incremental improvements to existing products or services. This type of innovation typically targets the high-end market, as the new improved products are more expensive than the existing alternatives.

New-market high-end disruption describes the case where the new product initially sells only to customers in the new market. This type of innovation is typically more expensive than existing options, but creates a new need in customers that was not previously addressed by existing technology. Although this technology is not necessarily better in terms of traditional preferences, it creates new desires in consumers who are willing to pay a premium for the new product (van der Rhee et al., 2012).

High-end disruption is a type of innovation that occurs when a new technology enters the market at the high end of the existing market. The new technology is more expensive than the current technology, but it offers significantly better performance or features (van der Rhee et al., 2012).

Another path innovation can take is through low-end encroachment, which is what (Christensen, 1997) traditionally classified as disruptive innovation, where technology is cheaper than existing options, but also has poorer performance. This type of innovation diffuses through the market by offering a more affordable alternative to existing solutions. However, it may not necessarily create a new market, as it does not necessarily create a new need or desire among consumers.

Low-end new-market disruption is a type of innovation that occurs when a new technology enters the market and creates a new market space for itself at the low end of the existing market. This type of innovation may score worse in terms of performance compared to existing technology, but it creates new needs in customers that were not addressed by existing technology.

Finally, there is disruptive innovation that diffuses through low-end disruption, where the innovation offers a lower price, while offering mostly the same benefits as the incumbents. This type of innovation can be disruptive, as it threatens the viability of existing products and services.

In conclusion, disruptive innovations can occur both through high-end encroachment of the market and through low-end encroachment of the market. Different patterns of encroachment have resulted in disruptive innovation in the past, contradicting Christensen's (1997) initial idea that disruptive innovation occurs only through low-end encroachment. Sood and Tellis (2011) showed that most disruptive innovations do not initially target the low-end market. Furthermore, while some disruptive innovations will target the same market as the existing product, it is also possible that the new technology has ancillary characteristics that allow it to address different needs in consumers. This innovation initially targets a detached or fringe market, but over time, as the technology is improved, it will also encroach on the existing product.

Type of Innovation	Type of Diffusion to Which It Maps	Description	Examples
Sustaining innovation	High-end encroachment	The new product first encroaches on the high end of the existing market, and then diffuses downward	
New market disruption	New-market high-end encroachment	These products create new market space, and encroach after a monopoly period.	Smartphone
	New attribute high-end disruption	These products open up additional high-end market space in addition to encroaching on current products.	
High-end disruption	Immediate high-end encroachment	High-end encroachment begins immediately upon introduction of the new product.	DVD
Disruptive innovation	Low-end encroachment	The new product first encroaches on the low end of the existing market, and then diffuses upward.	Personal Computer
New-market disruption	Detached-market low-end encroachment	Before encroachment begins, the new product opens up a detached market.	5.25-inch disk drive (relative to 8-inch)
	Fringe-market low-end encroachment	Before encroachment begins, the new product opens up a fringe market.	
Low-end disruption	Immediate low-end encroachment	Low-end encroachment begins immediately upon introduction of the new product.	Discount retailer

**Table 2.1:** Mapping of the Type of Innovation to the Type of Diffusion

### 2.2.2 | Identifying Disruptive Innovation

This section offers insight in how new innovations might impact the market. Nagy et al. (2016) developed a framework for incumbent firms that sell an existing, well-established product to identify disruptive innovations. Their identification framework consists of three steps.

**Step 1: Identify the innovation and its characteristics.** The first step of this process involves identifying the various market segments that currently use the product and arranging them from high end to low end. This analysis should consider not only current users but also potential new market segments that could arise if the product's price were reduced or if alternate features were improved.

**Step 2: Identify where in an organisation's value chain the innovation is used.** The next step is to assess the willingness of each market segment to pay for the various attributes of the product, both the key attributes of the current product and the alternative attributes that are preferred by the fringe markets.

**Step 3: Compare the potentially disruptive innovation with the technologies currently used in the organisation for that value chain segment.** This process should assess which market segments will be interested in purchasing a new product over time. Depending on the primary attributes on which the new innovation is based, different market segments will be interested. For instance, a product that is less expensive but of lower quality will appeal to different users than a product that is small in size. This analysis can help understand which market segments are likely to be interested in the new product.

In this study, the framework developed by Nagy et al. (2016) is used to assess whether blockchain technology can be classified as disruptive innovation. Using this framework, the study provides a systematic approach to evaluating whether blockchain technology has the potential to disrupt existing markets.

### 3 | Methodology

The aim of the present study is to investigate whether blockchain technology should be considered a disruptive innovation. To determine whether an innovation is disruptive, the defining characteristics of the technology must be known and the market segments that are targeted. Once the market segments have been determined, their interest in the new innovation needs to be analysed. The methodology of this study is three-fold. First, a bibliometric network analysis is conducted to identify which applications of blockchain appear in literature. These results are used to identify the market segments and applications where academics believe that blockchain has potential. Second, a literature review of the literature on different applications of blockchain is conducted using a thematic analysis. This analysis gives insight in how academics believe blockchain can be applied in different contexts. Finally, these insights are analysed using literature on the limitations of blockchain, to determine if these limitations are adequately addressed in the literature on applications of blockchain.

#### 3.1 | Bibliometric Network Analysis

A bibliometric network analysis can be used to summarise large amounts of bibliometric data to present the state of the academic field and emerging trends of a research topic or field (Donthu et al., 2021). The research method was divided into four steps:

1. Database and search term selection
2. Screening
3. Network analysis

##### 3.1.1 | Database and search terms selection

The first step of the protocol is to define how to identify which articles are included in the analysis. The literature is sourced the articles from Web of Science, because this database provides a comprehensive amount of scientific journals and it is widely used in academic research. To retrieve an overview of the foundational themes within blockchain research, the search was limited to the title and keywords, using the term *blockchain* as the search term. The goal of this study is to gain insight in the current developments in the field of blockchain research; therefore, only publications from 2021-01-01 onwards are considered. The bibliometric network analysis will use no more than 10,000 publications that are most cited, as networks with too many nodes are difficult to handle in VOSviewer, the software used, due to computational limitations and memory constraints (Eck and Waltman, 2014). This search resulted in 9476 articles (retrieved on December 20, 2022).

##### 3.1.2 | Screening

The second step involves defining the raw criteria to screen the collected sample of articles. This screening is done by reading the title and keywords of each article. The exclusion criteria are:

1. Articles not related to blockchain,
2. Articles not in English,
3. Duplicate articles.
4. Articles with no author

After eliminating publications according to the exclusion criteria, a population of 9342 publication remained.

##### 3.1.3 | Network Analysis

To explore whether there are specific clusters within the academic literature on blockchain, a bibliometric network analysis was performed. This study used the VOSviewer software version 1.6.18 (Eck and Waltman, 2014). VOSviewer is a software tool for visualising bibliometric networks. A bibliometric network can take different units of analysis. A co-citation network shows which articles are often cited together, creating clusters of commonly co-cited articles. Co-citation analysis is commonly used to



understand the development of foundational themes within a research field. Bibliographic coupling is a technique for literature mapping that clusters articles if they share common references. The advantage over a co-citation network is that recent publications that have not been cited much will also emerge in the network. Therefore, bibliographic coupling is suitable for uncovering the current developments within a research field. A co-word analysis looks at the co-occurrence of words within different publications. The most common unit of analysis are keywords, and this allows researchers to explore the existing relationships between topics in a research field. The usage of words as a unit of analysis has its downsides, as certain words can have different meanings depending on the context (Donthu et al., 2021).

The present study aims to investigate the relationships between current themes in blockchain research. Since this study uses recent literature, it is probable that a significant number of the articles have received limited citations. Therefore, bibliographic coupling is used to cluster documents based on their shared references. The next step is to identify the themes among the different clusters. This is done by reading the title of each publication in a cluster to establish what common theme is portrayed by this cluster.

### 3.2 | Thematic analysis

Thematic analysis is a way of analysing data to identify common themes or patterns within the data. It involves systematically organising the data into categories or themes and then interpreting and analysing the data to identify trends, patterns, or insights. Thematic analysis is often used in qualitative research to help researchers understand the experiences, perspectives, or meanings that participants have attached to a particular phenomenon or event. It allows researchers to identify common themes or patterns within the data and provide insight into the underlying meaning or significance of the data (Clarke et al., 2015). The purpose of thematic analysis is to decompose the text into smaller units of content and handle these units through descriptive analysis (Boyatzis, 1998).

In this part of the study, thematic analysis is used to analyse the literature on the market segments where blockchain has potential that were identified in the bibliometric network analysis. This analysis consists of the following steps:

1. Database and search term selection
2. Sample selection
3. Coding and Analysis

#### 3.2.1 | Database and search terms selection

The first step is to identify which articles are included in the literature review. The literature is sourced from Web of Science. Next, a set of keywords was identified that was used to search the keywords, titles, or abstracts of papers. The search strings consist of two parts, the first word limits the results to blockchain technology, and the second expression limits the result to specific application domain.

- TITLE-KEY (Blockchain) AND TITLE-KEY (Internet of Things) OR TITLE-KEY(IoT)
- TITLE-KEY (Blockchain) AND TITLE-KEY (Supply Chain Management)
- TITLE-KEY (Blockchain) AND TITLE-KEY (Smart Grids) OR TITLE-KEY (Energy Trading)
- TITLE-KEY (Blockchain) AND TITLE-KEY (Healthcare)
- TITLE-KEY (Blockchain) AND TITLE-KEY (Smart City) OR TITLE-KEY (Digital Twin)

#### 3.2.2 | Sample selection and screening

The next step involves selecting articles for thematic analysis. The five most cited articles of each search query are selected for the thematic analysis. In addition, these articles were screened by reading the title, keywords, and abstract of each article. The exclusion criteria are:

1. Articles not related to blockchain,
2. Articles not related to the application of blockchain
3. Articles not in English,
4. Duplicate articles.
5. Articles with no author

### 3.2.3 | Coding and analysis

This research uses thematic analysis to identify how blockchain is applied in different domains and to identify the characteristics of blockchain that add value compared to traditional ledgers in different application domains. In other words, this thematic analysis combines fragments of the data, which often are meaningless when viewed alone (Clarke et al., 2015). A coding reliability approach was adopted, where themes are conceptualised prior to the coding process (Braun and Clarke, 2006). In this thematic analysis, the following three themes guided the coding process:

1. **Problem statement:** What problem is Blockchain solving according to this paper.
2. **Advantages:** What are the advantages of using blockchain in this context.
3. **Limitations:** What are the limitations of using blockchain in this context.

In this study, the six phases for performing a thematic analysis by Braun and Clarke (2006) are followed. The first phase consists of transcribing and reading the data, while noting down initial ideas. In this study, the articles were organised according to their application domain and read to gain a good understanding of the data before continuing with the coding phase. The next step is to generate initial codes. This study planned to use software for qualitative data management called "NVivo" to automatically identify reoccurring topics in the selected articles. However, when testing the auto-coding functionality of NVivo, it was deemed too inaccurate for the purpose of this study. For example, the software could not differentiate between statements that said security is an advantage of blockchain and statements that said that security is a big liability in blockchain. The third step is to find significant themes. However, since a coding reliability approach was used, the main thematic areas were already determined. However, first- and second-order themes were defined. Phase 4 begins when a set of candidate themes has been devised, and it involves refining these themes. Some themes might not be supported by enough data, while others can be merged with a different theme, or a theme has to be broken up into two distinct themes. In phase 5, the themes are defined and named accordingly. For each individual theme, a detailed analysis is written, and the theme is related to the research question. The final step is to write the results and tell the story of your data in relation to your research goal. Evidence for the themes should be provided through citations that capture the essence of that theme.

This data analysis was performed by one coder, a master student. To improve the accuracy of the thematic analysis, a relatively small sample was collected, which allowed an in-depth analysis within limited time.

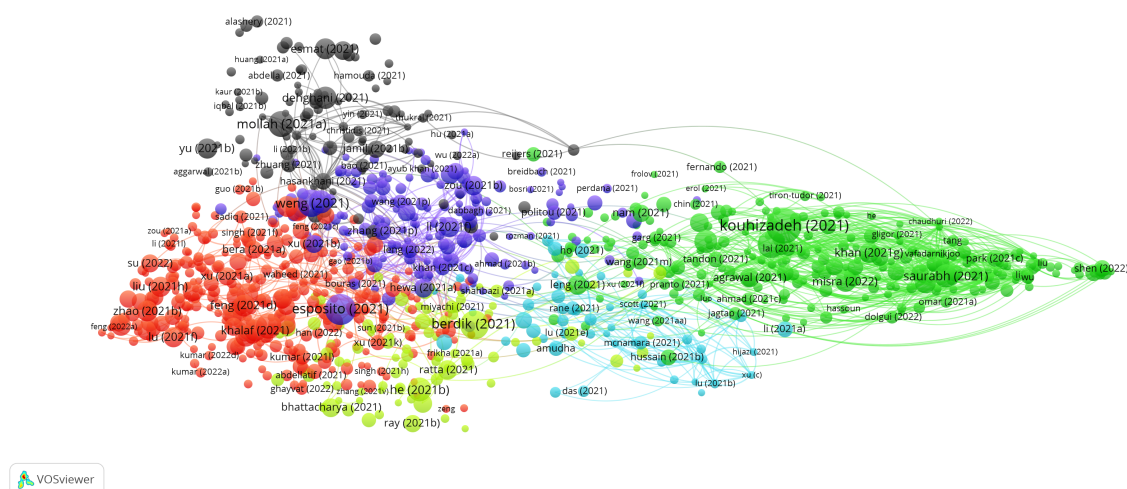
## 4 | Results

The first part of the results focusses on the quantitative review of publications on blockchain technology. In this study, a bibliometric network of literature on blockchain from 01-01-2021 to 20-12-2022 is constructed using bibliographic coupling. The bibliometric network is used to deduce what current themes are in blockchain research.







#### 4.1 | Bibliometric network analysis

Following the methodology presented earlier, the blockchain literature since 2021 is visualised in a bibliometric network. This network clusters the literature based on how many references they share, known as bibliographic coupling; the more references are shared between two publications, the more likely they are to be clustered. In the case of the clustering technique, different values were tried for the parameter *Resolution*. The resolution determines the level of detail in the bibliometric network. A high resolution leads to more small clusters, whereas a low resolution creates large clusters. After some experimentation, this parameter was set to 1.00. This yielded a clustering with a satisfactory level of detail. To determine this value, the clustering results were evaluated using multiple metrics, including cluster size, coherence, and interpretability. A resolution value of 1.00 produced a clustering that balanced these metrics. The resulting clusters were small enough to reveal meaningful relationships between papers, but not so small as to obscure the big picture. Additionally, the clusters exhibited high coherence, meaning that the papers within each cluster shared similar characteristics and themes. Finally, the resulting clusters were interpretable, meaning that they could be easily understood and labelled.

A visualisation of the bibliometric network is shown in [Figure 4.1](#), showing how the thousand most strongly connected publications since 2021 are clustered. As can be seen in [Figure 4.1](#), the blockchain literature can be clustered into six distinct clusters. [Table 4.1](#) summarises the main themes of each cluster. Six distinct themes arose from the data. The largest cluster is related to blockchain in combination with Internet of Things and smart appliances. The second cluster concerns the application of blockchain technology in supply chain management. One cluster is not related to the application of blockchain technology but is concerned with more in-depth technical research on the blockchain data structure. The three smallest clusters in the blockchain literature data are “Smart Grids and Energy Trading”, “Healthcare”, and “Building environment: Smart Cities and Digital Twins”.



**Figure 4.1:** Network visualisation map of publications using bibliographic coupling.

Colour		Main Theme	No. of pub.
Red		Internet of Things and Smart Appliances	349
Green		Supply Chain Management	247
Blue		Technical Aspects of Blockchain	161
Black		Smart Grids and Energy Trading	98
Yellow		Healthcare	95
Cyan		Smart Cities, Digital Twins and Contracting	50

**Table 4.1:** Summary of the content of the six blockchain clusters. The colour used to indicate a cluster in Figure 4.1 is shown in the second column.

Interestingly, these findings differ from the findings of a previous bibliometric analysis by Yang et al. (2022). Their study used publications on blockchain in business and economics journals from 2015 to 2021. In their study, the largest cluster was cryptocurrency governance and initial coin offerings, while smart grids, healthcare and building environment were not identified. A possible explanation is that these topics are unlikely to be covered in business and economics journals. However, it is interesting that cryptocurrencies as a topic did not emerge from our data set, as this is the largest cluster in their data. Since the current study only used publications from 2021 and 2022, this result may indicate that less academic literature is being produced on cryptocurrencies in recent years.

## 4.2 | Thematic Analysis

Data obtained in previous studies has shown that much less attention is paid to the limitations of blockchain technology compared to the benefits (Chen et al., 2021). According to the study by Chen et al. (2021), only 25.2% of all blockchain research articles are concentrated on challenges, while 78.3% focus on benefits. Furthermore, the authors were able to identify various benefits of blockchain technology using a thematic analysis, including 1) enhanced efficiency, 2) accurate traceability, 3) reliable transparency, and 4) elimination of intermediaries. In addition, they identified several challenges related to 1) complexity of integration, 2) immature application of blockchain technology, 3) protection of privacy, 4) error intolerance, 5) transaction capability of blockchain, 6) proving a guarantee that the data initially entered is actually reliable, 7) high initial investment, and 8) absence of regulations, legislation, and standards (Chen et al., 2021). Their analysis led to the conclusion that various characteristics of blockchain technology can be viewed as a double-edged sword, providing both benefits and implementation challenges. This finding is supported by the work of Treiblmaier (2020). For example, while the transparency of data on the ledger facilitates accountability, it also causes data privacy problems.

However, their study did not identify the extent to which the limitations of blockchain are adequately addressed in the literature and also did not look at interaction between different codes and different application domains of blockchain. In our study, we explore the different themes that emerged from the literature and relate them to the different application domains. First, interesting findings are discussed regarding the themes discovered in each thematic area. The interaction between these thematic areas is then examined to gain a deeper understanding of the complex relationships between them. By exploring these themes and their interactions, we aim to provide a comprehensive understanding of the data used in the thematic analysis.

In the discussion, this study will relate the results of the analysis to the theory of disruptive innovation developed by Christensen (1997) in order to determine to what extent the market is interested in blockchain technology. Table 4.2 shows the results of the thematic analysis. Appendix B contains the description of each theme individually.

### 4.2.1 | Problem statement

The thematic area *Problem statement* is concerned with the way different publications address the actual problem that blockchain solves in their respective application domain. In 15 (60.0%) of the articles, the theme *Centralisation* was mentioned as a problem that can be addressed with blockchain. This is in line with the main purpose of blockchain, which is to facilitate decentralised control by eliminating central authorities.

### Problems pertaining to digitisation

However, many articles described problems that were not necessarily related to blockchain, but rather to digitisation in general. For example, one article discussed a problem within smart grid networks:

*“Current procedures involve manual post-processing and increased communications to consolidate information held separately by each part of the transaction. As a result, current procedures are slow and time-consuming”* (Andoni et al., 2019, p. 152).

Another article on application of blockchain technology also referred to issues arising from a lack of digitisation:

*“For Maersk, the key problem was the “mountains of paperwork” required with each container. For instance, Maersk’s storage room at Mombasa office, on the coast of Kenya was reported to have shelves and shelves of paper records that date back to 2014”* (Kshetri, 2018, p. 83).

These examples show a lack of understanding on what technological opportunities blockchain offers compared to centralised solutions, since digitisation can be achieved without using blockchain. Upon examining the codes from different themes, the analysis showed that problem statements regarding *financial costs*, *inefficiencies* and *lack of control over data* actually refer to a lack of digitisation. Arguably, a *lack of traceability* could potentially be addressed through a centralised ledger system, but the features of the blockchain provide added layers of trust to traceable data. Therefore, we did not categorise this theme under the overall theme *digitisation*.

### Unsupported problem statements

Another noteworthy observation from our analysis of the problem statements is that many of the issues purportedly associated with blockchain technology lack references or evidence to support these claims. One article discusses why blockchain should be used in supply chains:

*“Whenever goods and related documentation (e.g., bills of lading or ship notifications) pass from one actor in the supply chain to another, items are subject to counterfeiting or theft.”* (Francisco and Swanson, 2018, p. 4)

Another article on blockchain integration with the internet of things describes another problem, without providing supporting evidence:

*“Nowadays, we trust in the information of financial entities and the government among others, but can we be sure that the information provided by them and by other external entities, such as IoT companies, has not been tampered/alterd/falsified in any way?”* (Reyna et al., 2018, p. 174)

This article on blockchain in sustainable supply chain makes another unsupported claim:

*“The cost involved in handling intermediaries, their reliability, and transparency further complicate managing this traceability in the supply chain.”* (Saber et al., 2019, p. 2117)

While this statement specifically mentions the cost, no references detailing cost implications are provided. The above three citations are typical of the kinds of problems blockchain is said to solve. However, research on how severe these problems are or their cost implications is rather scarce.

Based on these findings, new fruitful research can be expected on the potential problems that can be addressed by blockchain technology. One key observation is that blockchain solutions are often suggested for issues that could be resolved using centralised digital technologies. It is essential for authors to clearly articulate why blockchain is superior to alternatives. However, academic research on blockchain rarely considers alternative solutions to these problems. Second, researchers need to support their problem statements with academic literature. Research is needed on what problems occur in different blockchain application domains and why blockchain could be a superior solution over other digital technologies.

### 4.2.2 | Advantages

All the publications in the sample highlighted the advantages of using blockchain technology. The most commonly identified benefit was its *Distributed characteristics* in 84% of all publications, which aligns with the fundamental promise of the technology of eliminating the need for trusted intermediaries. Furthermore, we found that the themes *Immutable* (68%), *Trustless* (52%) and *Publicly available* (64%) are often mentioned as advantages. This is in line with the characteristics described in our definition of a blockchain. A blockchain needs to be open to users and provide a full and public history of all transactions.

Thematic Area	First-order theme	Second-order theme	F	R
<b>1. Problem Statement</b>	1.1 Centralisation	1.1.1 Centralised Management	12	18
		1.1.2 Single point of failure	8	9
	1.2 Digitisation	1.2.1 Financial cost	3	3
		1.2.2 Inefficiencies	8	8
		1.2.3 Lack of control over data	3	3
		1.2.4 Lack of digitalisation	4	5
	1.3 Network shortcomings	1.3.1 Data synchronisation	2	3
		1.3.2 Heterogeneity of devices	2	3
		1.3.3 Rigidity of the network	3	3
		1.3.4 Scalability of the network	2	3
	1.4 Lack of privacy		9	18
	1.5 Lack of traceability		4	14
	1.6 Lack of trust		6	9
	1.7 Security		8	17
<b>2. Advantages</b>	2.1 Authentication		12	26
	2.2 Digitisation	2.2.1 Automation	8	26
		2.2.2 Digital replaces manual	5	12
	2.3 Decentralisation	2.3.1 Decentralised	15	32
		2.3.2 Democratic	1	1
		2.3.3 Disintermediation	13	27
		2.3.4 Market of services	2	2
	2.4 Performance	2.4.1 160 bit address space	1	1
		2.4.2 Efficiency	6	13
		2.4.3 Low cost	2	12
		2.4.4 Mobility	4	6
		2.4.5 Scalability	7	13
		2.4.6 Speed	5	10
	2.5 Immutable		17	34
	2.6 Privacy		11	19
	2.7 Publicly available	2.7.1 Traceability	11	42
		2.7.2 Transparency	13	57
	2.8 Security		20	59
	2.9 Trustless		13	29
<b>3. Limitations</b>	3.1 Centralisation	3.1.1 Large mining pools	2	3
		3.1.2 Limited technical knowledge	4	4
		3.1.3 Miner selection	3	4
	3.2 Crypto Issues	3.2.1 Coin loss	1	2
		3.2.2 Illegal activity	3	4
		3.2.3 Volatility of cryptocurrency	1	2
	3.3 Inefficiencies	3.3.1 Energy consumption	7	13
		3.3.2 Inefficient	3	3
		3.3.3 Resource cost	8	14
		3.3.4 Scalability	8	17
		3.3.5 Storage issues	13	29
	3.4 Irreversible		8	10
	3.5 Legal issues		3	3
	3.6 Problems of public data	3.6.1 Privacy	8	12
		3.6.2 Unwilling to share all data	7	19
	3.7 Regulatory barriers		2	3
			5	8
	3.8 Security concerns		12	29
	3.9 The Oracle Problem	3.9.1 Data entered not reliable	4	6
		3.9.2 Off-chain oracles	1	1

**Table 4.2:** Themes Table. (F: Number of files, R: Amount of references)



Furthermore, a strong distributed consensus protocol is needed to ensure the immutability of data on the blockchain.

### Advantages pertaining to digitisation rather than blockchain

However, certain themes indicate benefits that are not directly related to our definition of blockchain. Firstly, the themes *Digitisation* and *Performance* actually mention the advantages of digitisation, rather than the use of blockchain. For example, a publication on the application of blockchain in the energy sector states:

*“The trial showed there can be significant gains in costs and efficiency by the automation of trade processes such as confirmations, actualisations, invoice generation, settlement, audit, reporting and regulatory compliance.”* (Andoni et al., 2019, p. 160)

This citation from a paper on blockchain in supply chain management also mentions the advantage of *Digitisation* as an advantage of blockchain:

*“Several mechanisms are available to ensure cost reduction. In the supply chain, manual paper-based processes and humans carrying documents such as air courier expenses are eliminated.”* (Kshetri, 2018, p. 86)

Again, a lack of differentiation between blockchain technologies and other digital technologies can be observed in the discussion related to the advantages blockchain provides. Although within the themes *Digitisation* and *Performance*, some advantages were related to blockchain, the analysis still showed that many researchers do not clearly address the benefits of blockchain in contrast to the benefits provided by other digital technologies.

### Security in blockchains

Another interesting finding is that 20 (80%) articles mentioned *Security* as an advantage. Security is not directly included in our definition, as it is a direct consequence of the immutable and decentralised nature of a blockchain. The following citations demonstrate how these characteristics improve security:

*“The decentralised storage of data reduces the risk of single point of access failure associated with centralised databases.”* (Wang et al., 2019, p. 63)

*“Data unforgeability: The decentralized nature of consortium blockchain combined with digitally signed transactions ensure that an adversary cannot pose as the user or corrupt the network, as that would imply the adversary forged a digital signature, or gained control over the majority of system resources.”* (Kang et al., 2017, p. 3161)

Although some articles cite encryption as an advantage of blockchain technology, it should be noted that encryption can also be employed to secure centralised databases and is not unique to blockchains. As with digitisation, researchers do not clearly distinguish between security benefits that are derived from using blockchain and security benefits that are the consequence of a different technology. The following citation demonstrates this:

*“We employ the blockchain techniques to enable secure and reliable IoT [Internet of Things] data sharing. Each IoT data provider can encrypt the data instances locally by its own private key, and then record the encrypted data on blockchain via specially formatted transactions.”* (Shen et al., 2019, p. 7702)

Drawing on these results, more research is expected on what makes blockchain unique compared to traditional ledgers that use a similar data structure but are not decentralised. The analysis showed that a variety of advantages are attributed to blockchain technology that are not necessarily exclusive to blockchain. It is imperative that when discussing blockchain technology, the researcher critically looks at what benefits are a result of using blockchain and which benefits could be achieved using different technologies. By doing so, blockchain research can provide a more nuanced understanding of the potential applications of the technology and help to avoid overhyping its capabilities.

### 4.2.3 | Limitations

Although every publication covered the benefits of blockchain, only 20 (80.0%) publications discussed limitations. Furthermore, of all (605) coded references regarding *Advantages* and *Limitations* 30.4% pertained to *Limitations*. In the literature, greater emphasis was placed on the potential benefits of blockchain technology compared to its limitations, according to our findings.

### Inefficiencies make blockchain hard to scale

In 18 (72%) of the publications *Inefficiencies* were mentioned as a limitation. Interestingly, all subthemes of *Inefficiencies* relate to scalability issues of blockchain technology. First, with the growth of a blockchain, *Energy consumption* typically increases exponentially, as every node in the network has to commit more resources to validate a block. Second, with high *Resource cost*, it becomes more expensive to expand a blockchain. One article on blockchain in the energy market noted:

*“Another important challenge is that blockchain systems have currently high development costs. Blockchains may realise significant cost savings by circumventing intermediaries, however for several use cases, they might not have the competitive advantage against already existing solutions in well-established markets.”* (Andoni et al., 2019, p. 166)

Another inefficiency is related to the fact that blockchain is *Slow* compared to centralised ledgers. This makes it difficult to scale blockchain, as for large-scale applications, either a lot of computational power is needed or the network becomes significantly slower. As one author noted:

*“Latency is another barrier, as time passes for each verified block of transactions to be added to the ledger. For Ethereum, one of the most popular blockchains for smart contracts, this occurs approximately every 17 seconds – a far cry from the milliseconds to which we are accustomed while using non-blockchain databases.”* (Wang et al., 2019, p. 74)

Finally, *Storage issues* occur since every node in a blockchain network has to store a continuously expanding ledger. An article on blockchain applications in smart cities details how this leads to scalability issues:

*“If the transaction volume of VISA system is processed by the Bitcoin blockchain, the blockchain size will grow rapidly at a speed of 3.9 GB per day. When applying blockchain technology in smart cities, a huge quantity of data will be generated by various devices and be processed by blockchain technology.”* (Xie et al., 2019, p. 2821)

### Centralisation is often the solution

Interestingly, when discussing solutions to these limitations, researchers often conclude that centralisation is needed to make the blockchain system more scalable. The following citations reflect this pattern:

*“For instance, when high performance is required, blockchain alone may not be the right solution, but a hybrid approach could be applied to optimize it”* (Reyna et al., 2018, p. 180)

*“Thus, it is not possible to directly apply the blockchain technology to smart city scenarios where devices have limited storage resources. Therefore, it is necessary to study what information is stored on or off the blockchain”* (Xie et al., 2019, p. 2821)

*“For fast-paced scenarios, private customised blockchains work best.”* (Wang et al., 2019, p. 74)

However, only a few authors acknowledged how reintroducing centralised governance compromises the characteristics of immutability and transparency of the blockchain. This article discusses this in relation to the *Storage issues* of blockchain:

*“For example, energy transactions can be recorded in conventional databases, such as relational databases that are designed to recognise relations between stored items of information. These solutions are already largely available and currently faster and less costly to operate, albeit they cannot offer immutability of records or transparency.”* (Andoni et al., 2019, p. 166)

This shows that researchers have a rather different understanding of how blockchain achieves its unique properties like immutability or decentralisation. Researchers discuss the advantages of public blockchains, but propose solutions that reintroduce centralisation, directly impeding these advantages of a blockchain.

### Large problems receive little attention

This finding is further supported by the observation that *The Oracle Problem* is only mentioned in 4 (16%) of the articles, while all applications discussed require off-chain data. While some articles do address the Oracle Problem, it is often briefly mentioned and the ramifications of having off-chain oracles are not discussed in great detail. The use of off-chain oracles reintroduces the need for a central authority (Caldarelli and Rossignoli, 2022) for monitoring the oracles, but the following excerpt contains the discussion of off-chain data, but does not consider that testing of the sensors actually requires a trusted authority:

*“One of the main challenges in the integration of the IoT with blockchain is the reliability of the data generated by the IoT. Blockchain can ensure that data in the chain are immutable and can identify their transformations, nevertheless when data arrives already corrupted in the blockchain they stay corrupt ... Sometimes the devices themselves and their sensors and actuators fail to work properly from the start. This situation cannot be detected until the device in question has been tested, or sometimes it works properly for a while and changes its behavior for some reason (short circuit, disconnection, programmed obsolescence, and so on).”* (Reyna et al., 2018, p. 166)

Although we found that researchers often advocate solutions that reintroduce centralisation, the first-order theme *Centralisation* is only mentioned in 9 (36%) of all publications as a limitation. Moreover, the only aspects of centralisation mentioned are *Large mining pools*, *Limited technical knowledge*, which centralises the power to those with expertise in blockchain technology, and *Miner selection*, which describes the process of choosing participants in a private blockchain. The results show that little attention has been paid to the consequences of centralisation within a blockchain network.

Another noteworthy finding is that *Problems with public data* is mentioned only in 7 (28%) of the publications. Many organisations might not want their ledger to be publicly available, as one article puts it:

*“Although information transparency and verifiability is a need for evaluating sustainability performance of a supply chain, some organisations may assume information as a competitive advantage which makes them unwilling to share valuable and critical information.”* (Saber et al., 2019, p. 2125)

Many applications of blockchain involve publicly sharing the data of an organisation on an immutable ledger. However, this total transparency can also be a liability for businesses and organisations. Moreover, immutability is accompanied by a variety of *Privacy* concerns that are related to the first-order theme *Legal issues*. As the following article on healthcare applications of blockchain notes:

*“In the case of personal data management, it is important to consider the General Data Protection Regulation (GDPR) that is passed by the European Union (EU) in 2016 and becomes enforceable from 25 May 2018. The goal of GDPR is to give EU citizens more rights and control over their personal data. According to GDPR, EU citizens have the right to erase their personal data, which is in conflict with the immutability feature of the blockchain systems.”* (Xie et al., 2019, p. 2125)

This problem is common in public blockchains, as data on the blockchain is publicly available. However, the second-order theme *Privacy* is only mentioned in 7 (28%) of all publications as a limitation and the first-order theme *Legal issues* is mentioned in 8 (32%) of all publications. This shows that the literature does not pay sufficient attention to problems related to privacy and legal issues.

Surprisingly, our thematic analysis revealed a lack of attention to the blockchain trilemma. As a distributed network cannot maximise security, scalability, and decentralisation at the same time, it poses a significant challenge for the implementation of blockchain. For example, in our analysis of blockchain applications in the supply chain, we found that centralisation was often suggested as a solution to scalability issues. However, this solution is not without its drawbacks, as it can lead to decreased trust and transparency in the data on the blockchain. In the energy sector, our analysis of blockchain applications found that, while the technology has the potential to enable peer-to-peer energy trading, scalability remains a major obstacle. Again, the trilemma was not discussed in any of the articles analysed, despite its relevance to this challenge. Academic literature needs to acknowledge this inherent limitation of blockchain technology to provide a more nuanced understanding of the potential of blockchain technology. On the basis of these findings, valuable research can be conducted on how the blockchain trilemma affects different application domains in blockchain. Depending on the specific context, some applications may be able to prioritise decentralisation and scalability over security, while for others, a different balance may be more appropriate. Such research could shed light on how to optimise blockchain solutions for different use cases and identify the trade-offs that must be made to achieve the desired outcomes.

In accordance with past research by Chen et al. (2021), the current results show that the characteristics of blockchain provide both advantages and implementation challenges. In this study, a thematic analysis has been used to identify the advantages and limitations of blockchain research to determine if blockchain can be considered a disruptive technology. The results suggests that while advantages of blockchain are abundant in the academic literature, these advantages are not always linked to blockchain, but rather to digitisation. Furthermore, the results suggest a general lack of attention to certain limitations of blockchain. The research community seems to be emphasising the benefits of blockchain technology, with little regard for its drawbacks. Even when negative aspects are acknowledged, the implications are seldom

discussed in detail. These results were consistent along every application domain.

## 5 | Discussion

Several authors have postulated in the past that blockchain technology can be considered a disruptive innovation (Nordgren et al., 2019; Mufti et al., 2020). However, in a study that included expert interviews, Della Valle and Oliver (2020) assert that blockchain technology should be viewed as a sustaining innovation. According to the authors, the experts interviewed proposed that there is currently no market demand for blockchain and that citizens have a need to adopt it. They noted that the real challenge is to find a working use case, where blockchain is successfully applied in an industry, since that would facilitate adoption in a broader industrial setting. The experts questioned also agreed that the added value that blockchain brings to the market is a distributed consensus mechanism that removes single points of failure and creates an immutable ledger. However, they also proposed that current industrial tests that apply blockchain are centralised, which violates the immutable characteristic and reintroduces a single point of failure.

There exists a significant gap in the current literature concerning the potential disruptive nature of blockchain technology. While some authors argue that blockchain is a disruptive innovation, others suggest that it is a sustaining innovation. However, there is a lack of empirical evidence to support these claims and a limited understanding of the factors that contribute to the disruptive potential of blockchain.

In this study, a novel approach was taken to determine whether blockchain should be considered a disruptive technology. We used the framework developed by Nagy et al. (2016) for identifying disruptive technologies. This process consists of three steps: First, we describe the blockchain and its characteristics. Second, we identify in which market segments blockchain could be applied. Third, we assess the degree of interest among market segments in blockchain technology by comparing it with alternative technologies. The present study differs from the study by Della Valle and Oliver (2020), which used expert interviews, in that it conducts a systematic review of the literature to address the research question. This systematic review consists of a bibliographic network analysis to determine what market segments blockchain can be applied in and a thematic analysis, which is used to identify the characteristics of blockchain and to determine to what extent market segments are interested in blockchain technology.

### 5.1 | Overview of Results

Our results showed that there appears to be a lack of understanding on what the unique value proposition of blockchain is. Many problem statements and advantages that are mentioned do not pertain to blockchain but to different processes, most commonly digitisation. Similarly, our findings indicate that when addressing blockchain limitations, reintroducing centralisation in the network is often suggested, thereby compromising its decentralisation and immutability aspects. Moreover, references to what problem blockchain is solving are often lacking, supporting the claim of Della Valle and Oliver (2020) that there is currently no market demand for blockchain. The analysis also shows that there is a significant lack of attention to the limitations of blockchain. In line with prior research by Chen et al. (2021), limitations of blockchain are generally discussed much less frequently than the advantages. In contrast to previous studies, this research delves deeper into often unacknowledged limitations, such as the Oracle Problem and the effect of centralisation in a blockchain network. Despite numerous limitations related to the inefficiencies of blockchain that have been discussed in the literature, only a handful of publications have pointed out how centralisation and oracles contradict the fundamental principles of blockchain.

### 5.2 | Research questions

The research questions that were presented at the beginning of this document have been extensively examined. This section will provide answers to the research questions based on the results of the bibliographic network analysis and the thematic analysis. The first sub-question aimed to ascertain the key attributes of blockchain technology that distinguish it from the technologies already in use. A literature study found that the main attributes are 1) openness to anonymous user, 2) a full and public history of transaction, and 3) a strong distributed consensus protocol. These three attributes ensure immutability and result in a network in which trust is moved from a central authority to a decentralised network of nodes, where it is extremely expensive to collude against the network.

The second sub-question involved identifying the market segments that might be interested in blockchain technology. By conducting a bibliographic network analysis, we were able to identify five primary areas where the literature suggests that blockchain technology can be implemented. These areas are internet of things, supply chain management, smart grids, healthcare and smart cities and digital twins.



The final step was to study to what extent these market segments are interested in blockchain technology. This was done through a thematic analysis in which the literature on blockchain applications was analysed in different market segments and the benefits and limitations of blockchain technology were compared. This thematic analysis showed that the academic literature is not clear about the problem that blockchain needs to solve and that the advantages of blockchain technology come with considerable limitations. Therefore, it is questionable whether the market has interest in the technology. This is further backed by the lack of successful use cases in the industry setting. Furthermore, it was observed that the results of the thematic analysis were largely consistent between the diverse market segments. Consequently, rather than pinpointing the disruptive impact of blockchain on each market segment, we will address the core question more broadly.

With answers to each sub-question, the main research question remains to be answered: To what extent is blockchain a disruptive technology? A literature study on disruptive innovation showed that a technology can be disruptive if it is either significantly cheaper than a current product or if it provides a competitive advantage over the current technology. We observe that while blockchain is in some studies heralded as a more cost-effective alternative, this is often compared to a nondigital solution or nonautomated solutions. These benefits can also be achieved by centralised ledgers. However, blockchain is very expensive, with high initial costs and high costs to maintain the network, in terms of energy costs, maintenance, and transaction fees. This cost is not expected to go down since blockchains need to provide an incentive in order to ensure that nodes will not collude. Therefore, blockchain will not disrupt the market through low-end encroachment, since it is more expensive than the existing solutions.

When considering disruption through high-end encroachment, blockchain should either provide better quality on existing highly valued features or provide additional benefits that allow blockchain to create a new market. Compared to traditional ledgers, blockchain technology performs significantly worse when it comes to current valued features such as speed, energy consumption, privacy, scalability, and storage space requirements. Therefore, high-end disruption is unlikely as blockchain does not perform better on the currently valued attributes. The last way to disrupt the market is through high-end new-market disruption, where a technology encroaches on current products by creating a new market space. In order to create a new market place, a technology needs to address a need that is not addressed by existing technology. In the case of blockchain technology, this could be the need for a decentralised and immutable ledger that replaces intermediaries. The thematic analysis has confirmed that the literature also views these as benefits associated with blockchain technology. However, there are also drawbacks associated with these benefits. Looking beyond the aforementioned limitations regarding currently valued features, blockchain also struggles to fully eliminate centralisation. Sai et al. (2021) showed that there are many different modes of centralisation in blockchains, which diminishes their decentralised nature to some degree. Second, while data on a public is immutable and can be trusted, trust is needed in off-chain oracles. Data still needs to be entered on the blockchain, and this is a security liability, since it introduces a single point of failure. Finally, it is observed that blockchain has very limited mainstream application with wide-spread adoption, while the technology has been around for over a decade. Therefore, blockchain is not expected to disrupt the market through the creation of a new market.

Although blockchain cannot be considered a disruptive innovation, it also does not classify as a sustaining innovation. As Christensen (1997) noted, a sustaining innovation is, by definition, targeted at a known market in which the customer needs are well understood. However, the market where blockchain will establish its presence and the specific customer demands within that market are still unclear. Although blockchain does offer some unique features, there seems to be little interest on industry- and market-level to implement public blockchains. However, over time, new applications might be discovered and blockchain might become more relevant in some industries. Businesses do not have to expect a sudden disruption of their industry by blockchain technology, as blockchain is expected to incrementally evolve and eventually settle within its market segment.

### 5.3 | Implications

This study has some theoretical implications. First, academic articles should clearly define what type of blockchain they are discussing. Private and public blockchains are technologically very distinct and need to be treated as two different innovations. In much of the literature, it is observed that when public blockchain limitations are discussed, the solution proposed in the literature is often to move toward a private blockchain. However, public and private blockchains are inherently different from a technological perspective and should be regarded as two separate innovations.

Second, this study highlights that many of the problem statements in the blockchain literature are



not supported or can be addressed by using more centralised technologies. Researchers need to clearly describe the characteristics of blockchain that are relevant to their study and to clearly distinguish between problems that are solved by implementing blockchain technology and problems that could be solved without decentralisation. Blockchain's advantage is that it is a censorship-resistant immutable ledger, and researchers need to describe why these characteristics are relevant in for their application.

Third, significantly more attention should be paid to addressing the limitations of blockchain technology. Although blockchain technology has distinctive features that traditional ledgers lack, these features often come with certain drawbacks. The limitations concerning centralisation and the Oracle Problem warrant specific attention, as they pose a considerable obstacle to the fundamental purpose of blockchain technology, which are decentralisation and immutability. In addition, blockchain researchers should clearly describe the characteristics of blockchain that are relevant to their study.

Finally, scalability presents a significant challenge for blockchain applications. Despite its acknowledged inefficiencies, our study found that decentralised solutions to the scalability problem are rare in academic research. It is crucial for researchers to recognise that blockchain's inefficiencies make scalability difficult to achieve, and thus, any proposed large-scale applications should be approached with caution.

## 5.4 | Limitations

Some limitations are worth noting when considering the implications of this study. First, the systematic review methodology is associated with several limitations, including publication bias, sample selection bias, and inconsistent coding or data interpretation. Publication bias refers to the fact that positive results are published more often in academic journals than negative results (Rothstein et al., 2005). In order to address this, grey literature was initially consulted to identify potential limitations of blockchain technology, which were subsequently validated through a review of peer-reviewed publications that specifically address these limitations.

Sample selection bias occurs when data points in a study are not random and do not represent the larger population. This is a considerable limitation of this study, since only the most cited publications of each application domain were included. It is possible that there is an interaction effect between citation frequency and the portrayal of blockchain technology, which could introduce bias into the study. This bias could have been mitigated by increasing the sample size and randomly selecting the literature, rather than relying solely on the most cited publications. This would have ensured a more representative sample and minimised the risk of sample selection bias. It is worth noting that within the limited sample, few additional codes were generated at the end of the coding process, indicating that a sufficient level of saturation had been achieved by the end of the coding process.

Inconsistent coding and data interpretation is also a noteworthy limitation of the current study. Inconsistent coding and data interpretation occur among researchers who interpret and extract data in different ways. The thematic analysis was performed by a single researcher and has not been checked by different researchers. Although the results of the thematic analysis were extensively discussed, the coding process itself was not. Therefore, the data is subject to inconsistent coding and data interpretation.

Another limitation involves how the application domains were determined. After the bibliographic network analysis had yielded various different clusters, the titles of these publications were manually analysed in order to determine the names for each cluster. The clusters' names are the application domains that were later studied in the thematic analysis. The use of a text mining approach would have been preferred, as it would have eliminated the potential biases introduced by the researcher.

In addition, the current study approaches disruptive innovation mainly from the technology side rather than actually looking at the industry- and firm-level. When evaluating disruptive technology, it is important to consider not only the features of the technology, but also the characteristics of the market (Rothaermel and Hill, 2005). Although this study clearly identified which features of blockchain support disruptiveness and which features do not, it remains unclear how these features of blockchain would affect industries. However, 15 years since the introduction of Bitcoin, industry use cases are still very limited and have not yet been able to disrupt the market (Della Valle and Oliver, 2020). Therefore, we believe that this study can offer an explanation for the lack of industry disruption despite the unique characteristics of blockchain technology.

Finally, this study clearly differentiates between public and private blockchains as distinct technologies. However, the literature from the thematic analysis did not clearly distinguish between these two, resulting in the inclusion of research on private blockchains, while this study focusses on applications of public blockchains. Upon further inspection of the literature, it was found that many authors do not clearly specify which type of blockchain they employed, and this complicates studying private or public blockchain

separately.

## 5.5 | Future research

The findings of this study provide a foundation on which future research can be based, and there are still many unanswered questions that need to be addressed. First, the blockchain research field is in desperate need of a clear problem description that blockchain can solve. One common criticism of blockchain is that it is a solution in search of a problem (Chowdhury et al., 2019). This calls for research on what industry needs are currently not satisfied and how blockchain can be leveraged to address these needs. In this study, we found that the current state of research does not provide a clear distinction between the benefits generated by digitisation and automation and those resulting from having a decentralised ledger. More research is needed to determine the cost effectiveness of a blockchain solution compared to a traditional ledger solution.

Likewise, more research is needed to establish the cost of scaling up a blockchain. Many proposed applications of blockchain require significantly more transactions and larger storage than current blockchain applications. Our study has confirmed that scalability is one of the biggest challenges facing blockchain. However, research on how expensive it is to scale a blockchain is sparse. Researchers need to address this issue when proposing a large-scale blockchain solution.

An additional avenue for further research is on the Oracle Problem that occurs in any blockchain application that deals with off-chain data. Although blockchain ensures trust in the data recorded on the ledger, it does not eliminate the need for trust in oracles, which initially supply the data. Despite its importance, the issue of trust in oracles within blockchain technology is relatively understudied, highlighting the need for further research to explore the nuances of how a blockchain system, despite its touted trustlessness, still relies on trusted sources of data such as oracles.

Similarly, there is a need for research on identifying how centralisation affects the trustlessness of a blockchain. The findings indicate that researchers tend to recommend centralised solutions for addressing blockchain limitations, and this impedes the main advantages of blockchain like decentralisation and immutability. Furthermore, unintended centralisation has diverse impacts on blockchains, and this topic has received little attention in the literature. Sai et al. (2021) provided a comprehensive taxonomy of centralisation in the context of blockchain. Future research should include their findings and acknowledge how centralisation occurs in their context.

Furthermore, future research is needed on how private blockchains compare to traditional ledgers in terms of trust and cost-effectiveness. Current research often compares private blockchains to scenarios in which no or an inferior digital technology is employed. While such comparisons are valuable in understanding the advantages of private blockchains over inferior ledgers, they fail to provide a comprehensive understanding of how private blockchains compare to other digital technologies that function similarly. This study observed that many advantages are attributed to blockchains that can be achieved through digitisation. To address this gap, it is necessary to compare private blockchains with other digital technologies that share similarities but are not private blockchains. This approach would enable us to conduct comparative analyses and obtain a definitive answer on the costs and merits of private blockchains.

## 5.6 | Conclusions

In conclusion, the present study provides evidence that blockchain should not be considered a disruptive technology. Blockchain is inefficient, expensive, and hard to scale and therefore it cannot disrupt the market through low-end disruption. Although blockchain does offer additional characteristics, namely decentralisation and immutability, these characteristics come with great costs. The issue of centralisation and the oracle problem are prevalent in many blockchains, which hinders the potential for new-market disruption. Moreover, use-cases implementing blockchain technology are sparse, whereas the technology has been around for more than a decade. Blockchain is not a panacea, and it is unlikely to disrupt existing markets the way that some proponents have claimed.

This study has laid the foundation for more nuanced blockchain research in which the limitations of blockchain research are adequately addressed. By highlighting the main limitations of blockchain implementation and suggesting areas for further research, we have advanced the understanding of the theoretical underpinnings of blockchain technology.

## 5.7 | Recommendations

Given that blockchain cannot be classified under any disruptive type of innovation, it is recommended that policy makers and managers take caution when considering investing in blockchain. According to Christensen's theory of disruptive innovation (Christensen, 1997), managers must act quickly to capture the strong first-mover advantages associated with disruptive technologies. However, since blockchain technology is not classified as a disruptive innovation, it is recommended that companies exercise patience and wait to invest in blockchain until the technology has had time to mature.

## 6 | Acknowledgements

I want to thank my first and second supervisors, Bert Sadowski and Kevin Gallagher, for their continued support during my master thesis. Bert consistently provided valuable feedback in our weekly meetings, drawing from his extensive knowledge in both technical and innovative areas. Bert would always stress how he knew that what he asked from me was not easy, but he also trusted me to be able to deliver and this greatly motivated me. Kevin was always available to support me in my research and his help was very useful whenever I was stuck. He initially sparked the interest in me that resulted this specific thesis. Kevin not only knew a lot about the technical side, but also greatly contributed with his knowledge on science in general. His constructive feedback and willingness to engage in meaningful discussions were instrumental in the success of this project. I also want to thank Georgios Papachristos, who provided feedback on my section on disruptive innovation. I am deeply grateful for the time and effort that my supervisors invested in this project and for their ongoing support of my academic endeavours.

I would also like to extend my gratitude to the faculty members of the Innovation Science department for their support and encouragement throughout my academic journey. Their valuable input and feedback have been instrumental in shaping my research and enriching my learning experience.

Furthermore, I would like to thank my family and friends for their unwavering support and understanding during this sometimes challenging period. Their encouragement and motivation have kept me motivated throughout the writing process.

Finally, this master thesis has been an incredible learning experience, and I am thankful for the opportunity to have worked with such knowledgeable and supportive individuals.

## 7 | References

- Abrams, R., Goldstein, M., and Tabuchi, H. (2014). Erosion of faith was death knell for mt. gox. *New York Times*.
- Adner, R. (2002). When are technologies disruptive? a demand-based view of the emergence of competition. *Strategic management journal*, 23(8):667–688.
- Agbo, E. I. and Nwadior, E. O. (2020). Cryptocurrency and the african economy. *Economics And Social Sciences Academic Journal*, 2(6):84–100.
- Aitzhan, N. Z. and Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852.
- Akartuna, E. A., Johnson, S. D., and Thornton, A. E. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*, pages 1–36.
- Allen, H. J. (2022). Defi: Shadow banking 2.0? *William & Mary Law Review*, *Forthcoming*.
- Ammous, S. (2016). Blockchain technology: What is it good for? *Available at SSRN 2832751*.
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., and Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, 100:143–174.
- Aysan, A. F., Bergigui, F., and Disli, M. (2021a). Blockchain-based solutions in achieving SDGs after COVID-19. *Journal of Open Innovation: Technology, Market, and Complexity*, 7(2):151.
- Aysan, A. F., Bergigui, F., and Disli, M. (2021b). Using blockchain-enabled solutions as SDG accelerators in the international development space. *Sustainability*, 13(7):4025.
- Azouvi, S., Maller, M., and Meiklejohn, S. (2019). Egalitarian society or benevolent dictatorship: The state of cryptocurrency governance. In *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22*, pages 127–143. Springer.
- Berg, C., Davidson, S., and Potts, J. (2017). Blockchains industrialise trust. *Available at SSRN 3074070*.
- Biswas, K. and Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*, pages 1392–1393. IEEE.
- Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. sage.
- Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101.
- Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information*, 11(11):509.
- Caldarelli, G. and Rossignoli, C. (2022). Beyond oracles—a critical look at real-world blockchains.
- Catalini, C. and Tucker, C. (2018). Antitrust and costless verification: an optimistic and a pessimistic view of the implications of blockchain technology. *SSRN Electronic Journal*.
- CCAF (2023). Bitcoin network power demand. <https://ccaf.io/cbeci/index>. Accessed: 2023-03-06.
- Chauhan, A., Malviya, O. P., Verma, M., and Mor, T. S. (2018). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 122–128. IEEE.

- Chen, S., Liu, X., Yan, J., Hu, G., and Shi, Y. (2021). Processes, benefits, and challenges for adoption of blockchain technologies in food supply chains: a thematic analysis. *Information Systems and e-Business Management*, 19:909–935.
- Chesterman, X. (2018). *The P2POOL mining pool*. PhD thesis, PhD thesis, Ghent University.
- Chia, V., Hartel, P., Hum, Q., Ma, S., Piliouras, G., Reijnders, D., Van Staaldouin, M., and Szalachowski, P. (2018). Rethinking blockchain security: Position paper. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (Green-Com) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1273–1280. IEEE.
- Chowdhury, S., Rodriguez-Espindola, O., Beltagui, A., and Mackenzie, L. (2019). If blockchain is the answer what is the question?
- Christensen, C. (1997). *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Harvard Business Essentials. Harvard Business School Press.
- Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303.
- Chu, S. and Wang, S. (2018). The curses of blockchain decentralization. *arXiv preprint arXiv:1810.02937*.
- Clarke, V., Braun, V., and Hayfield, N. (2015). Thematic analysis. *Qualitative psychology: A practical guide to research methods*, 222(2015):248.
- concerned.tech (2022). Letter in support of responsible fintech policy. <https://concerned.tech/>. Accessed: 2022-11-08.
- Danneels, E. (2004). Disruptive technology reconsidered: A critique and research agenda. *Journal of product innovation management*, 21(4):246–258.
- De Villiers, C., Kuruppu, S., and Dissanayake, D. (2021). A (new) role for business—promoting the united nations' sustainable development goals through the internet-of-things and blockchain technology. *Journal of business research*, 131:598–609.
- De Vries, A. (2018). Bitcoin's growing energy problem. *Joule*, 2(5):801–805.
- De Vries, A., Gellersdorfer, U., Klaßen, L., and Stoll, C. (2022). Revisiting bitcoin's carbon footprint. *Joule*, 6(3):498–502.
- De Vries, A. and Stoll, C. (2021). Bitcoin's growing e-waste problem. *Resources, Conservation and Recycling*, 175:105901.
- Della Valle, F. and Oliver, M. (2020). Blockchain enablers for supply chains: How to boost implementation in industry. *IEEE access*, 8:209699–209716.
- Dhawan, A. and Putniņš, T. J. (2021). A new wolf in town? pump-and-dump manipulation in cryptocurrency markets. *Review of Finance, forthcoming*.
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., and Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133:285–296.
- Dorfleitner, G., Muck, F., and Scheckenbach, I. (2021). Blockchain applications for climate protection: A global empirical investigation. *Renewable and Sustainable Energy Reviews*, 149:111378.
- Dwivedi, A. D., Srivastava, G., Dhar, S., and Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):326.
- Eck, N. J. V. and Waltman, L. (2014). Visualizing bibliometric networks. In *Measuring scholarly impact*, pages 285–320. Springer.
- Egberts, A. (2017). The oracle problem-an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems. *Available at SSRN 3382343*.



- Ekblaw, A., Barabas, C., Harvey-Buschel, J., and Lippman, A. (2016). Bitcoin and the myth of decentralization: Socio-technical proposals for restoring network integrity. In *2016 IEEE 1st international workshops on foundations and applications of self\* systems (FAS\* W)*, pages 18–23. IEEE.
- Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37.
- Esposito, C., Ficco, M., and Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, 58(2):102468.
- Foley, S., Karlsen, J. R., and Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5):1798–1853.
- Francisco, K. and Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2(1):2.
- Franke, M. F. (2022). Refugees’ loss of self-determination in unhcr operations through the gaining of identity in blockchain technology. *Politics, Groups, and Identities*, 10(1):21–40.
- Gerard, D. (2017). *Attack of the 50 foot blockchain: Bitcoin, blockchain, Ethereum & smart contracts*. David Gerard.
- Ghiro, L., Restuccia, F., D’Oro, S., Basagni, S., Melodia, T., Maccari, L., and Cigno, R. L. (2021). What is a blockchain? a definition to clarify the role of the blockchain in the internet of things. *arXiv preprint arXiv:2102.03750*.
- Govindarajan, V. and Kopalle, P. K. (2006). Disruptiveness of innovations: measurement and an assessment of reliability and validity. *Strategic management journal*, 27(2):189–199.
- Gramoli, V. (2016). On the danger of private blockchains. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL’16)*, pages 1–4.
- Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42:1–7.
- Halatsis, C. and Philokyprou, G. (1978). Pseudochaining in hash tables. *Communications of the ACM*, 21(7):554–557.
- Hald, K. S. and Kinra, A. (2019). How the blockchain enables and constrains supply chain performance. *International Journal of Physical Distribution & Logistics Management*.
- Hamrick, J., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., and Vasek, M. (2021). An examination of the cryptocurrency pump-and-dump ecosystem. *Information Processing & Management*, 58(4):102506.
- Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., and Smolander, K. (2021). Gdpr compliant blockchains—a systematic literature review. *IEEE Access*, 9:50593–50606.
- Huh, S., Cho, S., and Kim, S. (2017). Managing iot devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)*, pages 464–467. IEEE.
- Kamble, S., Gunasekaran, A., and Arha, H. (2019). Understanding the blockchain technology adoption in supply chains-indian context. *International Journal of Production Research*, 57(7):2009–2033.
- Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., and Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, 13(6):3154–3164.
- Kazmi, A. R., Afzal, M., Abbas, H., Tahir, S., and Rauf, A. (2021). Is blockchain overrated? In *2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC)*, pages 187–192. IEEE.
- Khan, M. A. and Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82:395–411.

- Klenner, P., Hüsigg, S., and Dowling, M. (2013). Ex-ante evaluation of disruptive susceptibility in established value networks—when are markets ready for disruptive innovations? *Research Policy*, 42(4):914–927.
- Köhler, S. and Pizzol, M. (2020). Technology assessment of blockchain-based technologies in the food supply chain. *Journal of cleaner production*, 269:122193.
- Kostoff, R. N., Boylan, R., and Simons, G. R. (2004). Disruptive technology roadmaps. *Technological Forecasting and Social Change*, 71(1-2):141–159.
- Kshetri, N. (2018). Blockchain’s roles in meeting key supply chain management objectives. *International Journal of information management*, 39:80–89.
- Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., and Zhang, Y. (2017). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*, 14(8):3690–3700.
- Lin, I.-C. and Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, 19(5):653–659.
- Mainelli, M. (2017). Blockchain could help us reclaim control of our personal data. *Harvard Business Review Digital Articles*, pages 2–5.
- Mavilia, R. and Pisani, R. (2020). Blockchain and catching-up in developing countries: The case of financial inclusion in africa. *African Journal of Science, Technology, Innovation and Development*, 12(2):151–163.
- Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., and Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The brooklyn microgrid. *Applied energy*, 210:870–880.
- Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, pages 1–3. IEEE.
- Mollah, M. B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A. M., Koh, L. H., and Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, 8(1):18–43.
- Mufti, T., Saleem, N., and Sohail, S. (2020). Blockchain: A detailed survey to explore innovative implementation of disruptive technology. *EAI Endorsed Transactions on Smart Cities*, 4(10).
- Mukherjee, A. A., Singh, R. K., Mishra, R., and Bag, S. (2021). Application of blockchain technology for sustainability development in agricultural supply chain: justification framework. *Operations Management Research*, pages 1–16.
- Nagy, D., Schuessler, J., and Dubinsky, A. (2016). Defining and identifying disruptive innovations. *Industrial Marketing Management*, 57:119–126.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260.
- Narayanan, A. and Clark, J. (2017). Bitcoin’s academic pedigree. *Communications of the ACM*, 60(12):36–45.
- Nordgren, A., Weckström, E., Martikainen, M., and Lehner, O. M. (2019). Blockchain in the fields of finance and accounting: a disruptive technology or an overhyped phenomenon. *ACRN Journal of Finance and Risk Perspectives*, 8:47–58.
- Novo, O. (2018). Blockchain meets iot: An architecture for scalable access management in iot. *IEEE internet of things journal*, 5(2):1184–1195.
- Peterson, T. (2021). To the moon: a history of bitcoin price manipulation. *Journal of Forensic and Investigative Accounting*, 13(2).
- Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., and Zhang, B. Z. (2018). Distributed ledger technology systems: A conceptual framework. *Available at SSRN 3230013*.

- Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with iot. challenges and opportunities. *Future generation computer systems*, 88:173–190.
- Rothaermel, F. T. and Hill, C. W. (2005). Technological discontinuities and complementary assets: A longitudinal study of industry and firm performance. *Organization Science*, 16(1):52–70.
- Rothstein, H. R., Sutton, A. J., and Borenstein, M. (2005). Publication bias in meta-analysis. *Publication bias in meta-analysis: Prevention, assessment and adjustments*, pages 1–7.
- Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7):2117–2135.
- Sai, A. R., Buckley, J., Fitzgerald, B., and Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*, 58(4):102584.
- Schmidt, G. M. and Druehl, C. T. (2008). When is a disruptive innovation disruptive? *Journal of product innovation management*, 25(4):347–369.
- Schmidt, G. M. and Porteus, E. L. (2000). The impact of an integrated marketing and manufacturing innovation. *Manufacturing & Service Operations Management*, 2(4):317–336.
- Sharma, P. K. and Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, 86:650–655.
- Shen, M., Tang, X., Zhu, L., Du, X., and Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. *IEEE Internet of Things Journal*, 6(5):7702–7712.
- Shi, E. (2019). Analysis of deterministic longest-chain protocols. In *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*, pages 122–12213. IEEE.
- Sood, A. and Tellis, G. J. (2011). Demystifying disruption: A new model for understanding and predicting disruptive technologies. *Marketing Science*, 30(2):339–354.
- Steele, G. (2021). The miner of last resort: Digital currency, shadow money and the role of the central bank. *Technology and Government, Emerald Studies in Media and Communications, Forthcoming*.
- Sultanik, E., Brunson, T., Myers, M., Remie, A., Moelius, S., Amir, T., Manzano, F., Kilmer, E., and Schriener, S. (2022). Are blockchains decentralized? unintended centralities in distributed ledgers. Technical report, Trail of Bits.
- Tapscott, D. and Tapscott, A. (2018). *Blockchain revolution*. Senai-SP Editora.
- Treiblmaier, H. (2020). Toward more rigorous blockchain research: Recommendations for writing blockchain case studies. *Blockchain and distributed ledger technology use cases: Applications and lessons learned*, pages 1–31.
- van der Rhee, B., Schmidt, G. M., and Van Orden, J. (2012). High-end encroachment patterns of new products. *Journal of Product Innovation Management*, 29(5):715–733.
- Van Orden, J., van der Rhee, B., and Schmidt, G. M. (2011). Encroachment patterns of the “best products” from the last decade. *Journal of Product Innovation Management*, 28(5):726–743.
- Vujičić, D., Jagodić, D., and Ranić, S. (2018). Blockchain technology, bitcoin, and ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)*, pages 1–6. IEEE.
- Walch, A. (2019). Deconstructing ‘decentralization’: Exploring the core claim of crypto systems.
- Wang, Y., Han, J. H., and Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1):62–84.
- Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., and Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE communications surveys & tutorials*, 21(3):2794–2830.

- Yang, J., Ma, C., Li, D., and Liu, J. (2022). Mapping the knowledge on blockchain technology in the field of business and management: A bibliometric analysis. *IEEE Access*, 10:60585–60596.
- Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40:1–8.

## 8 | Appendix A: Articles used in Thematic Analysis

### Internet of Things

- Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303
- Huh, S., Cho, S., and Kim, S. (2017). Managing iot devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)*, pages 464–467. IEEE
- Khan, M. A. and Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82:395–411
- Novo, O. (2018). Blockchain meets iot: An architecture for scalable access management in iot. *IEEE internet of things journal*, 5(2):1184–1195
- Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with iot. challenges and opportunities. *Future generation computer systems*, 88:173–190

### Supply Chain Management

- Francisco, K. and Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2(1):2
- Kamble, S., Gunasekaran, A., and Arha, H. (2019). Understanding the blockchain technology adoption in supply chains-indian context. *International Journal of Production Research*, 57(7):2009–2033
- Kshetri, N. (2018). Blockchain’s roles in meeting key supply chain management objectives. *International Journal of information management*, 39:80–89
- Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7):2117–2135
- Wang, Y., Han, J. H., and Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1):62–84

### Smart Grids

- Aitzhan, N. Z. and Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., and Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, 100:143–174
- Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., and Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, 13(6):3154–3164
- Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., and Zhang, Y. (2017). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*, 14(8):3690–3700
- Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., and Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The brooklyn microgrid. *Applied energy*, 210:870–880

### Healthcare

- Dwivedi, A. D., Srivastava, G., Dhar, S., and Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):326
- Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37
- Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42:1–7
- Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, pages 1–3. IEEE
- Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40:1–8

### Smart Cities and Digital Twins

Biswas, K. and Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*, pages 1392–1393. IEEE

Esposito, C., Ficco, M., and Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, 58(2):102468

Sharma, P. K. and Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, 86:650–655

Shen, M., Tang, X., Zhu, L., Du, X., and Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. *IEEE Internet of Things Journal*, 6(5):7702–7712

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., and Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE communications surveys & tutorials*, 21(3):2794–2830



## 9 | Appendix B: Description of all themes

The following appendix gives a brief account of all the themes generated through the thematic analysis. We have focused on the lowest order themes in our discussion, as these were the themes that the codes were assigned to.

### 9.1 | Problem Statement

#### 9.1.1 | Centralised management

Centralised management is a problem in cases where intermediaries increase the transaction costs or when a central authority cannot be trusted with data. This is illustrated by the following citations:

*“Rather than relying on centralized intermediaries (e.g., banks) this technology allows two parties to transact directly using duplicate, linked ledgers called blockchains.”* (Francisco and Swanson, 2018, p. 1)

*“The cost involved in handling intermediaries, their reliability, and transparency further complicate managing this traceability in the supply chain.”* (Saber et al., 2019, p. 2117)

#### 9.1.2 | Single point of Failure

Another problem that blockchain is said to solve is that of a single point of failure. When one central organisation governs transactions, this introduces a single point of failure and this creates a security liability. As one author illustrated:

*“Centralised systems also have significant disadvantages due to a single point of failure, which renders them more vulnerable to both technical failures and malicious attacks.”* (Andoni et al., 2019, p. 145)

#### 9.1.3 | Financial cost

Another problem that was mentioned is that of costs. As one author noted:

*“From the manufacturer’s side, the current centralized model has a high maintenance cost – consider the distribution of software updates to millions of devices for years after they have been long discontinued.”* (Christidis and Devetsikiotis, 2016, p. 2298)

#### 9.1.4 | Inefficiencies

This theme bundled codes related to problem statements about inefficiencies in the current system. For example, one author mentioned the inefficient distribution of personal data:

*“Currently, personal information is distributed among different entities: government, universities, companies and so on. The information is spread across many entities and accessing it is time consuming, even when said entities answer to the same authority, e.g., the government.”* (Reyna et al., 2018, p. 177)

#### 9.1.5 | Lack of control over data

Lack of control over data was mentioned by a few authors as a problem in their introduction. In some systems, users have limited control over what an organisation does with their data. A common example is how your data is used for targeted online advertisement. This is illustrated by the following example:

*“It is natural to enable patients to own and control their data without compromising security or limiting the sharing of healthcare service.”* (Yue et al., 2016, p. 7)

#### 9.1.6 | Lack of digitisation

Some author would mention problems related to a lack of digitisation. Digitisation is the process of moving from manual processes to more automated and digital processes. As one author stated:

*“Current procedures involve manual post-processing and increased communications to consolidate information held separately by each part of the transaction. As a result, current procedures are*

*slow and time-consuming, as transactions need to be verified and reconciled multiple times from initialisation to final settlement.” (Andoni et al., 2019, p. 152)*

#### 9.1.7 | Data synchronisation

Data synchronisation refers to the necessity for multiple parties to have access to the same data. One author noted how blockchain technology can facilitate this:

*“However using blockchain on IoT, IoT devices can synchronize easily with other devices because of its distributed ledger.” (Huh et al., 2017, p. 464)*

#### 9.1.8 | Heterogeneity of devices

Heterogeneity of devices refers to the problem that in a network, different protocols and mechanisms are used. This can create security issues and hampers communication between different devices. This is best illustrated by the following citation:

*“The huge expansion of the IoT has to be supported by standard mechanisms and protocols in order to reduce the existing heterogeneity in the field. This heterogeneity leads to vertical silos and reduces the adoption of the IoT.” (Reyna et al., 2018, p. 174)*

#### 9.1.9 | Rigidity of the network

Some authors note how centralised networks are more rigid compared to decentralised networks. In some scenarios, flexibility and mobility are required, as one author stated:

*“RES [Renewable energy sources] are variable, difficult to predict and depend on weather conditions, hence raise new challenges in management and operation of electricity systems, as more flexibility measures are required to ensure safe operation and stability. Flexibility measures include the integration of fast-acting supply, demand response and energy storage services.” (Andoni et al., 2019, p. 174)*

#### 9.1.10 | Scalability of the network

One problem that was mentioned a few times, was that of scalability of a network. For example:

*“Due to the continued growth of data volume and number of connected IoT devices, however, issues such as high latency, bandwidth bottlenecks, security and privacy, and scalability arise in the current smart city network architecture.” (Sharma and Park, 2018, p. 650)*

#### 9.1.11 | Lack of privacy

A variety of privacy issues were reported in centralised networks. As this author noted:

*“Lack of privacy and anonymity: Following Wood’s behavioral modeling of electricity consumption profiling approach, a centralized middleman may reveal patterns of an agent’s energy generation and predict the agent’s daily activities.” (Aitzhan and Svetinovic, 2016, p. 840)*

#### 9.1.12 | Lack of traceability

In supply chains particularly, there is a need to establish the provenance of a product. A lack of traceability is observed in these areas, as it is difficult to track a product to its origin.

*“Traceability is becoming an increasingly urgent requirement and a fundamental differentiator in many supply chain industries including the agri-food sector, pharmaceutical and medical products, and high value goods.” (Saberi et al., 2019, p. 2117)*

#### 9.1.13 | Lack of trust

One common problem that blockchain is said to solve is a lack of trust. Blockchain decentralises trust and rather than putting trust in a central authority, trust is created through decentralised consensus mechanisms. The following citation describes this problem:

*“Nowadays, we trust in the information of financial entities and the government among others, but can we be sure that the information provided by them and by other external entities, such as IoT companies, has not been tampered/alterd/falsified in any way.” (Reyna et al., 2018, p. 174)*

#### 9.1.14 | Security

A variety of security problems were assigned to this theme. Authors mentioned multiple problems that exist in centralised digital networks. For example:

*“However, these technologies [remote patient monitoring] also pose grave privacy risks and security concerns about the data transfer and the logging of data transactions. These security and privacy problems of medical data could result from a delay in treatment progress, even endangering the patient’s life.” (Dwivedi et al., 2019, p. 1)*

### 9.2 | Advantages

#### 9.2.1 | Authentication

Blockchain is often said to facilitate the authentication of an identity or ownership. As the following author stated:

*“Blockchain has been used widely for providing trustworthy and authorized identity registration, ownership tracking and monitoring of products, goods, and assets ... lockchain can be used to register and give identity to connected IoT devices, with a set of attributes and complex relationships that can be uploaded and stored on the blockchain distributed ledger. ” (Khan and Salah, 2018, p. 406)*

#### 9.2.2 | Automation

Another often mentioned advantage of blockchain is automation. Specifically smart contract are said to automate processes that current involve a lot a steps. For example:

*“Automation: Blockchains could improve control of decentralised energy systems and microgrids [18]. Adoption of local energy marketplaces enabled by localised P2P energy trading or distributed platforms can significantly increase energy self-production and selfconsumption, also known as behind the meter activities [83], which can potentially affect revenues and tariffs.” (Andoni et al., 2019, p. 151)*

#### 9.2.3 | Digital replaces manual

Blockchain-based ledgers are said to replace costly manual processes. As one author noted:

*“Several mechanisms are available to ensure cost reduction. In the supply chain, manual paper-based processes and humans carrying documents such as air courier expenses are eliminated.” (Kshetri, 2018, p. 86)*

#### 9.2.4 | Decentralised

Blockchains facilitate decentralisation, by removing a centralised authority and instead reaching consensus using proofs in a decentralised public network. Many authors mentioned decentralisation as an advantage. For example:

*“Decentralized Consensus: The transactions are validated by all the nodes of a network instead of a central entity. This breaks with the paradigm of centralized consensus.” (Novo, 2018, p. 1185)*

#### 9.2.5 | Democratic

In a blockchain, power is removed from a central authority to all participating nodes. This can be perceived as a more democratic system. This theme was only coded once, which is interesting, given the democratic nature of blockchain.

*“Democracy: Consensus algorithms are executed by all decentralized nodes to reach an agreement before a block is included into the blockchain. Thus, in the blockchain system, decisions are made by all nodes in a peer-to-peer manner, which makes it democratized.” (Xie et al., 2019, p. 2801)*

### 9.2.6 | Disintermediation

Similarly to decentralisation, blockchain also facilitate disintermediation. Intermediaries, such as banks, are often needed to monitor the transactions in a network. A blockchain is monitored by a predefined set of rules and its nodes and therefore an intermediary is no longer needed. This is illustrated by the following citation:

*“A key potential blockchain supply chain advantage is the disintermediation of financial intermediaries, including payment networks, stock exchanges, and money transfer services.” (Sabeti et al., 2019, p. 2121)*

### 9.2.7 | Market of services

A few authors noted the potential of blockchain to become a decentralised marketplace. This is best described in the following citation:

*“Market of services: blockchain can accelerate the creation of an IoT ecosystem of services and data marketplaces, where transactions between peers are possible without authorities. Micro-services can be easily deployed and micro-payments can be safely made in a trustless environment. It would improve IoT interconnection and the access of IoT data in blockchain.” (Reyna et al., 2018, p. 179)*

### 9.2.8 | 160 bit address space

One author specifically mentioned the advantage that blockchain networks have a larger network space than current networks:

*“Address Space. Blockchain has a 160-bit address space, as opposed to IPv6 address space which has 128-bit address space.” (Khan and Salah, 2018, p. 405)*

### 9.2.9 | Efficiency

Blockchain is said to increase efficiency through a variety of mechanisms. One example is:

*“By eliminating middleman auditors, efficiency can be increased and costs can be lowered.” (Kshetri, 2018, p. 80)*

### 9.2.10 | Low cost

Blockchain is said to reduce the marginal costs of network in a variety of ways. For example:

*“A commercial report by Deloitte states that blockchain-enabled transactional digital platforms could offer operational cost reductions, increased efficiency, fast and automated processes, transparency and the possibility of reducing capital requirements for energy firms.” (Andoni et al., 2019, p. 144)*

### 9.2.11 | Mobility

Mobility refers to how quickly the network can respond. As one author explains:

*“Mobility: The architecture can be used in isolated administrative systems or domains. Thus, every administrative domain has its own freedom to manage the IoT devices while the access control policies are still enforced by the rules in the blockchain.” (Novo, 2018, p. 1184)*

### 9.2.12 | Scalability

Blockchain as a technology to handle data is said to improve the scalability of a network. Authors mention a variety of ways in which blockchain improves scalability, although it is not exactly clear how blockchain achieves this. For example:

*“Other benefits that come with the decentralization of the architecture are an improvement of the fault tolerance and system scalability. It would reduce the IoT silos, and additionally contribute to improving the IoT scalability.” (Reyna et al., 2018, p. 179)*

### 9.2.13 | Speed

Various authors note how blockchain is capable of speeding up certain processes. Specifically in the supply chain domain:

*“Specifically, the tests performed on Chinese pork, and U.S. mangoes revealed that tracing food origins could be handled in 2.2 s, which used to take many weeks with non-blockchain technologies.”* (Kshetri, 2018, p. 84)

### 9.2.14 | Immutable

One of the core characteristics of blockchain is that the data on the blockchain cannot be tampered with and is thus immutable. Many authors mentioned immutability as an advantage. For example:

*“Immutability of information is another important feature of blockchain technology. It means that information cannot be changed and removed in blockchain without consensus. That prevents falsifying and adulteration of data.”* (Saberi et al., 2019, p. 2126)

### 9.2.15 | Privacy

Addresses on a blockchain are pseudonymous, meaning that although it is possible to know which address made a transaction, it is supposedly hard to figure out which person is behind the address. Furthermore, data on the blockchain is encrypted, which is said to increase privacy. This author mentions a variety of privacy related characteristics:

*“Electricity trading information and digital asset records are stored in a consortium blockchain. The trading information includes PHEVs’ [Plug-in Hybrid Electric Vehicle] pseudonyms used for privacy protection, data type, metadata tags for raw transactional data, complete index history of metadata, an encrypted linked to transaction records, and a timestamp of transaction generation.”* (Kang et al., 2017, p. 3156)

### 9.2.16 | Traceability

Some authors argue that traceability in blockchain technology can simplify the tracking of asset movements and ownership verification. While other digital technologies may also offer this functionality, blockchain’s immutable ledger ensures that all transactions are recorded securely and cannot be altered once entered into the blockchain. Therefore, blockchain provides an added layer of trust and integrity to the recorded transactions. As one author explains:

*“The characteristics of blockchains make them especially suited for traceability applications. Whenever goods and related documentation (e.g., bills of lading or ship notifications) pass from one actor in the supply chain to another, items are subject to counterfeiting or theft. To protect from this, blockchain technology involves the creation of a digital “token” which is associated with physical items when they are created. The final recipient of the item can then authenticate the token which can follow the history of the item to its point of origin. End users have more confidence in the information they receive since the no one entity or group of entities can arbitrarily change the information contained within the blockchain.”* (Francisco and Swanson, 2018, p. 1)

### 9.2.17 | Transparency

Data on a blockchain is transparent and open to the public in the sense that all transactions are recorded on a public ledger that anyone can access. This allows for a high degree of transparency and accountability. The next citation explain how accountability is achieved:

*“Blockchain improves supply chain dependability by exerting pressure on supply chain partners to be more responsible and accountable for their actions. Gemalto’s case indicates that individual responsibility and accountability can be stipulated and warranted. Note that in a conventional or “centralized” ledger, a single authority acts as the “trusted third party.”* (Kshetri, 2018, p. 86)

### 9.2.18 | Security

A wide variety of security benefits of blockchain are mentioned in the academic literature. Most notable are the immutability of data on the blockchain and the absence of a single point of failure due to decentralisation. One author describes blockchain as:

*“A robust, truly distributed peer-to-peer system that is tolerant of node failures.”* (Christidis and Devetsikiotis, 2016, p. 2298)

### 9.2.19 | Trustless

Blockchain allows two parties to transact without having to trust each other. In centralised systems, trust is typically established through the use of intermediaries such as a bank. In contrast, blockchain technology uses consensus mechanisms to create a decentralised and trustless network that eliminates the need for intermediaries. The following author highlights the trustless nature of blockchain technology:

*“A system that allows non-trusting participants to interact with each other in a predictable, certain manner.”* (Christidis and Devetsikiotis, 2016, p. 2298)

## 9.3 | Limitations

### 9.3.1 | Large mining pools

In Proof of Work blockchains, it has become too costly for an individual to mine Bitcoin themselves. Therefore, people work together in mining pools and distribute the profit over all participants. However, this concentration of mining power into the hands of a few mining pool managers poses a significant security risk. As is illustrated by this citation:

*“Additionally, the incentives in PoW are unexpectedly promoting centralization as the proliferation of mining pools confirm. This together with the mint reduction, reward diminution and fee increase could compromise the system.”* (Reyna et al., 2018, p. 178)

### 9.3.2 | Limited technical knowledge

The application of blockchain technology requires very specific technical knowledge. This hinders blockchain adoption, but it also centralises power to those who have the ability to maintain the blockchain. As one author noted:

*“The technical complexity of the blockchain makes it a challenge for individual users to understand, accept and have confidence in participation.”* (Wang et al., 2019, p. 74)

### 9.3.3 | Miner selection

In private blockchain, nodes are selected by an authority. As this reintroduces the needs to trust an authority and the need to trust individual miners. This is best illustrated by the next citation:

*“Another issue to consider when deploying (or participating) in a blockchain network is deciding on (or examining) the miner set. Recall that while a miner cannot fake a transaction or rewrite history, it can prevent a new, valid transaction from being added to the blockchain, effectively censoring it. The tolerance of a consensus mechanism against Byzantine nodes is limited; if the number of miners that conspire violates that threshold, the risk of transaction censorship is severe.”* (Christidis and Devetsikiotis, 2016, p. 2300)

### 9.3.4 | Coin loss

A large problem in cryptocurrencies is that of coin loss. If someone loses the key to their wallet, there is no way to retrieve these coins. As one author explains:

*“A common problem of virtual currencies, beyond the controversy surrounding their real value, is the problem of coin loss. If the wallet key is forgotten, there is no mechanism to operate with these coins. It has been estimated that 30% of bitcoins are lost.”* (Reyna et al., 2018, p. 176)



### 9.3.5 | Illegal activity

Cryptocurrencies are widely used to facilitate illegal activity. There is no authority that monitors the transactions and transactions are made pseudonymous. This allows criminals to use cryptocurrencies to transact, without federal regulation.

*“The criminal use of cryptocurrency is equally alarming when the automatic and autonomous properties of a blockchain are exploited: money laundering, illicit marketplaces and ransomware. Increasing cybercrimes lead to data breaches, financial crimes, market manipulation, IP theft and public safety and security risks.”* (Wang et al., 2019, p. 176)

### 9.3.6 | Volatility of cryptocurrency

Another issue when dealing with cryptocurrency is its volatility. Extreme fluctuations in price over a short period of time are common in most cryptocurrencies. This makes it difficult to use cryptocurrencies as a means of exchange of value.

*“The European Central Bank, has warned of its volatility risk but have also admitted its potential as a financial innovation.”* (Reyna et al., 2018, p. 177)

### 9.3.7 | Energy consumption

Blockchains, specifically Proof of Work blockchain, require an enormous amount of energy to keep running. This energy is needed to ensure the immutability aspect of the blockchain. This is not only an environmental hazard, but it also makes blockchains very expensive to maintain. As reflected in this citation:

*“A main criticism point is that PoW is responsible for wasting large amounts of real resources such as electricity. For example, Ethereum’s Wiki pages claim that Bitcoin and Ethereum burn over \$1 million worth of electricity and hardware costs per day for running their consensus mechanism.”* (Andoni et al., 2019, p. 166)

### 9.3.8 | Inefficient

A variety of characteristics make blockchain technology inefficient compared to alternatives. As one author noted:

*“One view is that there is not much value in setting up proprietary centralized blockchains for financial purposes, which do the same thing less efficiently than existing databases.”* (Kshetri, 2018, p. 87)

### 9.3.9 | Resource cost

Many authors acknowledge the high resource costs that come with blockchain. Blockchain requires expensive and specialised equipment required for running the network. This creates a barrier to entry and centralises power in the hands of those who can afford the necessary hardware. Moreover, this makes blockchain hard to scale, since growing the network becomes increasingly expensive.

*“At present, information in blockchain systems can be transferred for very low costs, but validation and verification of data comes with high hardware and energy costs.”* (Andoni et al., 2019, p. 166)

### 9.3.10 | Scalability

A number of characteristics make it hard to scale blockchain have already been discussed and the scalability issue of blockchain is recognised by many authors.

*“Storage capacity and scalability have been deeply questioned in blockchain. In this technology, the chain is always growing, at a rate of 1MB per block every 10 min in Bitcoin, and there are copies stored among nodes in the network. Although only full nodes (a node that can fully validate transactions and blocks) store the full chain, storage requirements are significant. As the size grows, nodes require more and more resources, thus reducing the system’s capacity scale.”* (Reyna et al., 2018, p. 175)

### 9.3.11 | Slow

Blockchain is also extremely slow compared to traditional ledgers. In a blockchain, every transaction needs to be verified and this takes time. Therefore, blockchain may not be the right solution when high performance is required.

*“For Ethereum, one of the most popular blockchains for smart contracts, this occurs “approximately every 17 seconds – a far cry from the milliseconds to which we are accustomed while using non-blockchain databases.” (Wang et al., 2019, p. 74)*

### 9.3.12 | Storage issues

A blockchain network requires all nodes to store the entire ever-growing ledger locally. The following citation describes how this limits blockchain deployment:

*“Full nodes must store the entire blockchain (currently more than 150 and 46 GB in Bitcoin and Ethereum, respectively) for a full validation of transactions and blocks, thus their deployment can be very limited in IoT devices.” (Reyna et al., 2018, p. 180)*

### 9.3.13 | Irreversible

Once a transaction enters the blockchain, it becomes immutable, meaning that it cannot be reversed. While it is possible to correct mistakes through a compensating transaction, this requires the cooperation of all parties involved. However, this issue becomes more complex when dealing with smart contracts, as faulty code can result in security vulnerabilities and bugs that can compromise the integrity of the blockchain.

*“Bugs in contract coding are especially critical because of the irreversibly and immutable nature of the system.” (Reyna et al., 2018, p. 177)*

### 9.3.14 | Legal issues

Blockchain faces a variety of legal issues. Blockchain facilitates illegal conduct, it is often used as a means of tax evasion and it is hard to adhere to privacy regulations.

*“A number of unique legal matters emerge from a blockchain’s distributed nature, as blockchains are decentralised and, in many cases, global. They cannot be shut down by any one legal system, and they exist outside the boundaries of conventional laws defined by jurisdiction. Local and international laws, industry-specific regulations, data sharing regulations, intellectual property, liability and general commercial agreements, such as the service level and performance assurances, should all be carefully examined.” (Wang et al., 2019, p. 79)*

### 9.3.15 | Privacy

Blockchain faces a variety of privacy concerns. All transactions in a blockchain are publicly available and transactions have been traced to specific individuals, even though participants are pseudonymous.

*“The blockchain affords pseudonymity, meaning that all transactions are transparent, yet are not explicitly connected to real-world individuals or organisations. However, this anonymity could be broken, connecting individual transactions to parties. This may not be of concern for upstream suppliers. For instance, for individual farmers in the food sector, this transparency brings marketing and branding benefits. However, for downstream consumers, their privacy may be compromised and sensitive detailed personal information revealed.” (Wang et al., 2019, p. 74)*

### 9.3.16 | Unwilling to share all data

Blockchain proponents often assume that businesses want to implement blockchain. However, sharing all your transaction data on a public ledger is a significant barrier to entry.

*“Some organisations may assume information as a competitive advantage which makes them unwilling to share valuable and critical information.” (Saber et al., 2019, p. 2125)*

### 9.3.17 | Regulatory barriers

Blockchain network have to comply to the same legislation as every other ledger system. Due to the unique properties of blockchain networks, this has proven to be difficult in many cases.

*“First, the global supply chain operates in a complex environment that requires various parties to comply with diverse laws, regulations and institutions. They include maritime laws and regulations, commercial codes, laws pertaining to ownership and possession of multiple jurisdictions in the shipping routes. Since international businesses operate against the backdrop of these established old laws, customs and institutions that are managed by human beings, implementing blockchain-based solutions can be an extremely complex task .” (Kshetri, 2018, p. 88)*

### 9.3.18 | Security concerns

One of the most often cited limitation of blockchain is its security. A variety of characteristics of blockchain contribute to these security concerns. As is highlighted by the next citations:

*“Security: weaknesses and threats The Bitcoin protocol has been thoroughly analyzed, and various vulnerabilities and security threats have been discovered. The most common attack is the 51% attack or majority attack.” (Reyna et al., 2018, p. 175)*

### 9.3.19 | Data entered not reliable

Blockchain is able to ensure that data that has entered the blockchain is immutable. However, the data is that initially entered may not be reliable in the first place. As one author explained:

*“But if you then drill a hole in the container, take out all the teddy bears, and replace them with cocaine, the blockchain won’t catch that. The blockchain is about taming all of the virtual attributes of the container, all of the paperwork that accompanies it. But the boundary between the physical and virtual worlds will always be a bit more lawless.” (Kshetri, 2018, p. 88)*

### 9.3.20 | Off-chain oracles

The previous example actually describes an instantiation of the oracle problem. Only one article specifically used the word oracle to describe the connection between the real world and the blockchain.

*“... working with smart contracts requires the use of oracles which are special entities that provide real-world data in a trusted manner.” (Reyna et al., 2018, p. 182)*