Qr code

Description automatically generated with low confidence

Blockchain

research report

Dimitar L. | S-ESE6-CMK | 10.04.2022

Table of Contents

[Introduction 2](#_Toc105866202)

[Research Questions 2](#_Toc105866203)

[What is blockchain technology and why does it matter? 2](#_Toc105866204)

[Research methods 3](#_Toc105866205)

[Report 3](#_Toc105866206)

[What are the different types of blockchain technology? 3](#_Toc105866207)

[Is blockchain secured? 4](#_Toc105866208)

[What are the limitations of blockchain? 5](#_Toc105866209)

[How was It implemented in the beginning? 6](#_Toc105866210)

[What are the challenges of blockchain adoption? 7](#_Toc105866211)

[What is the impact of the blockchain on the society? 8](#_Toc105866212)

[Resources 11](#_Toc105866213)

# Introduction

This research is made as part of my studies for Fontys University of Applied Science and the topic Blockchain was chosen, because my specialization was done for CyberSecurity and I am curious to learn more about it and to provide more information to me and my fellow classmates.

The goals that I want to reach with this research are to learn what is blockchain and to explain that to normal users as well, because it is a relatively new concept. It was published in the early nineties and the first implementation was Bitcoin in 2008. Where cryptocurrencies were the first application, the blockchain is also used in different fields. I will explain the history, challenges with blockchain adoption and when it was implemented and how it continues to improve.

# Research Questions

I am starting with the main research question and then continue with sub-questions after that. Those are the questions that I think are relevant in my point of view and those are the answers that I am curious about and want to answer.

## What is blockchain technology and why does it matter?

**What are the different types of blockchain technology?**

**Is blockchain secured?**

**What are the limitations of blockchain?**

**How was It implemented in the beginning?**

**What are the challenges of blockchain adoption?**

**What is the impact of the blockchain on the society?**

# Research methods

* Library method
  + Best good and bad practices.
  + Community research
  + Literature study
* Field method
  + Document analysis
  + Problem analysis
  + Survey
* Showroom
  + Benchmark test
* Workshop
  + Brainstorm

# Report

Living in the 21st century, we are all well versed with terms like bitcoins and cryptocurrency. Blockchain is the newest and friendliest technology launched in the market so far.

## What are the different types of blockchain technology?

A blockchain network is a technical network that is providing ledger and smart contract (chaincode) services to the applications. Primarily, these smart contracts are used to generate transactions which are subsequently distributed among every peer node in the network where they are unalterably recorded on their copy of the ledger. The users of applications must be end users using client applications. There are four types of blockchain technology.

The first one is the Public Blockchain, which is permissionless in nature and allows anyone to join. It is completely decentralized. Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create or validate blocks of data.  
Nowadays, Public blockchains are mainly used for exchanging and mining cryptocurrency. Some of them are Bitcoin, Etherium, Litecoin.

The second one is Private or Managed Blockchain, which is permissioned blockchain controlled by a single organization. In this type of blockchain, the central authority determines who can be a node. The central authority also does not necessarily grant each node with equal rights to perform functions. Private blockchains are only partially decentralized because public access to these blockchains is restricted. Examples of such blockchains are business-to-business virtual currency exchange network Ripple and Hyperledger.

Both private and public blockchains have drawbacks - public blockchains tend to have longer validation times for new data than private blockchains, and private blockchains are more vulnerable to fraud and bad actors.

Consortium Blockchains are the third type of Blockchain, which is permissioned blockchain governed by a group of organizations, rather than one entity, as in the case of the private blockchain. Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security. However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk.

The next fourth type is hybrid blockchain. This type of blockchain are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations. An example of a hybrid blockchain is IBM Food Trust, which was developed to improve efficiency throughout the whole food supply chain.

## Is blockchain secured?

Blockchain technology produces a structure of data with inherent security qualities. It's based on principles of cryptography, decentralization and consensus, which ensure trust in transactions. In most blockchains, the data is structured into blocks and each block contains a transaction or bundle of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it is nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

This enables decentralization through the participation of members across a distributed network. User cannot change the record of transactions and there is no point of failure.

However, the blockchain networks can differ in who can participate and who has access to the data. Usually, the networks are public or private, which shows who is allowed to join and who has permission, which describes how participants gain access to the network.

When building a blockchain application, it is critical to assess which type of network will best suit the goals. Private and permissioned networks can be tightly controlled and preferable for compliance and regulatory reasons. However, public and permissionless networks can achieve greater decentralization and distribution.

## What are the limitations of blockchain?

As every other technology, Blockchain also has its own limitations. In order to implement something, we always have to know not only the pros, but also the cons and the limitations.

The first limitation is the low scalability and the problem is that transaction speed always depends on network congestion. This means that the more people are involved, the slower the pace is. One example is Bitcoin. Centralized payment systems can process thousands of transactions per second, while Bitcoin can only manage seven.

This happens often because with Blockchain, the controlling unit notify the other members about transactions and lower the speed. Nodes also need to authorize the transaction. Therefore, we should consider the performance factor prior to implementing blockchain-enabled solutions.

The other limitation is the implementation. It’s all about initial financial investments. For some businesses, implementation costs may turn out to be overwhelming. Even though most existing solutions are free of charge, a vast contribution is a must when involving proficient software engineers engrossed in diverse aspects of blockchain development, licensing costs in case of switching to a chargeable software version, overall maintenance and more. If company is not ready to allocate a large amount of budget, maybe it is better to postpone the blockchain introduction.

Shortage of talent pipeline is the third limitation of blockchain. According to estimates, each year, the need for high-skilled blockchain developers skyrockets by 300-500%. It’s a global issue that countries from the USA to Singapore suffer equally. As this technology is still evolving, a development community requires some time to compose the relevant educational programs and alleviate the market demand.

The fourth limitation is the private key issue. Sometimes in the decentralized environment, private keys owned by individuals may become a weak spot. Once generated during a wallet creation, they provide access to all the data stored. If stolen, it puts both sensitive data and finances in jeopardy. If lost, then wallet access is gone forever.

Number 5 on the list is the problematic integration with legacy systems. When integrating blockchain solution with outdated systems already in use, possible data loss or corruption risks arise, especially if organizations have no seasoned specialist in place. To avoid operational disruption, before performing this transition, it is worth asking a question “Will it be a good fit for my infrastructure, or am I just following the hype?”

The last limitation is the High Energy Consumption. Most blockchain-based solutions like Bitcoin use a proof-of-work consensus algorithm for validating the transactions and this utilizes excessive computing power comparable to the yearly electricity consumption of a country like Denmark. And then with the resources needed to cool down the equipment, prices are only rising.

## How was It implemented in the beginning?

Blockchain was first introduced in 2008 as the distributed ledger behind bitcoin transactions. It has potential to grow to be a bedrock of the worldwide record-keeping systems, but was launched just a couple of years ago. It was created by the unknown persons behind the online cash currency bitcoin, under the name of Satoshi Nakamoto.

In 1991 a cryptographically secured chain of blocks is described for the first time by Stuart Haber and W Scott Stornetta.

Then 7 years later, in 1998, the computer scientist Nick Szabo works on ‘bit gold’, a decentralized digital currency.

After 2 years Stefan Konst publishes his theory of cryptographic secured chains, plus ideas for implementation.

In 2008, Satoshi Nakamoto released a white paper establishing the model for a blockchain.

A year after he implements the first blockchain as the public ledger for transactions made using bitcoin.

In 2014, Blockchain technology is separated from the currency and its potential for other financial, interorganizational transactions is explored. Blockchain 2.0 is born, referring to applications beyond currency

The Ethereum blockchain system introduces computer programs into the blocks, representing financial instruments such as bonds. These become known as smart contracts.

Posting their seminal whitepaper in 2008 and launching the initial code in 2009, Nakamoto created bitcoin to be a form of cash that could be sent peer-to-peer without the need for a central bank or other authority to operate and maintain the ledger, much as how physical cash can be.

While it wasn’t the first online currency to be proposed, the bitcoin proposal solved several problems in the field and has been by far the most successful version.

The engine that runs the bitcoin ledger that Nakamoto designed is called the blockchain; the original and largest blockchain is the one that still orchestrates bitcoin transactions today.

Other blockchains include those that run the several hundred “altcoins” – other similar currency projects with different rules – as well as truly different applications, such as:

**Ethereum**: the second largest blockchain implementation after bitcoin. Ethereum distributes a currency called ether, but also allows for the storage and operation of computer code, allowing for smart contracts.

**Ripple**: a real-time gross settlement system, currency exchange and remittance network, based on a public ledger.

## What are the challenges of blockchain adoption?

Blockchain is undoubtedly still the leading buzzword in the tech world. But however every new technology will always go through a hype stage. It takes a lot of time to get rid of all the challenges and use it to power the modern world. The blockchain is not different here.

Inefficient Technological Design is one of the major challenges of blockchain adoption. Although blockchain technology has a lot of perks, it still lacks in many technological ways. A coding flaw or loophole is one of the significant points in this.

The anonymous feature of the blockchain technology attracted not only experts but also criminal personals. Why? Well, the nature of the network is decentralized so that no one can know your true identity. This makes bitcoin the primary target used as a currency in the black market and the dark web.

Another one of the challenges of implementing blockchain is scalability. In reality, blockchains work fine for a small number of users. But what happens when a mass integration will take place? Ethereum and Bitcoin now have the highest number of users on the network, and needless to say, they are having a hard time dealing with the situation.

Energy consumption is another blockchain adoption challenge. Most of the blockchain technology follow bitcoins infrastructure and use Proof of Work as a consensus algorithm. However, Proof of Work is not as great as it looks. To keep the system live, it will need computational power. Mining will require you to solve complex equations using your computer. So, your PC will take more and more electricity to overcome this situation when you start mining.

Blockchain and privacy do not go really well with each other. The public ledger system fuels the system, so full privacy is not the first concern. Organizations for example cannot really work without privacy. Many companies that work with the privacy needs to have defined boundaries. Their consumers trust them with sensitive information. So, if they are all stored in a public ledger, it will not actually be private anymore now. That is why it is necessary to change the registers to limit access to the data. Making it available for only the customers will be a solution here.

No Regulations is one of the main challenges of implementing blockchain in an organization. Many organizations are making blockchain technology a means of transaction. You will see many products depended on this. But even now, there are not any specific regulations about it. So, no one follows any specific rules when it comes to the blockchain. Now, this is where the issue comes in. Although blockchain guarantees visibility as one of its benefits, there is still no security. You will not know for sure if it will be safe for you or not. To get over these challenges, governments and extremely controlled sectors may need to create regulations for blockchain.

Security is another crucial topic. Every blockchain technology boasts about its security, but like every other technology, blockchain also comes with a few security loops. The 51% attack on the network is one of the security flaws of the network. In this attack, hackers can take over the network and exploit it in their way. They can even alter the transaction process and restrict other people from creating a block.

The performance is other challenge. The blockchain is complex. That is why it takes more time to process any transactions. Also, the encryption of the system makes it even slower. Although they claim to be faster than traditional payment methods, still, in some cases, they cannot deliver it. Completing a transaction can take up to several hours. So, if you want to pay for something in the supermarket, it will cause you trouble. It is most suited for making large transactions where time is not a vital element. It is an element of risk.

Another one of the huge challenges to adopting blockchain technology is the lack of knowledgebase. In reality, the majority of the public is still not aware of the existence and potential use of this technology. If we want blockchain to be successful, it has to earn acceptance. Even though the technology is making history, still it is not enough to attract more consumers.

## What is the impact of the blockchain on the society?

Social impact has various definitions but generally deals with how actions and activities affect individuals, families, and communities. Often, social impact is framed within meeting a social challenge or the positive effects something has on people. Blockchain can not only help track social impact but help to shape it. There is much discourse about public and private bodies announcing what they will do, but it is hard to prove if it happens.

The use of blockchain offers far-reaching possibilities for social impact, including:

* Transparency
* Supply chain management
* Digital identity
* Personal data protection
* Legitimacy
* Compliance
* Trust

Big tech companies keep their algorithms secret, because blockchain’s selling point is openness and irrefutable record keeping. Some technologists claim blockchain and cryptocurrencies can realign capitalism thanks to blockchain’s alternative trust-based, peer-to-peer systems.

Many organizations are already using blockchain to effect social impact. IBM has partnered up with several big players in the food industry, using blockchain to provide a transparent supply chain for produce. This builds brand trust, and people can check if labeling and packaging are truthful. People can track every step of the supply chain and check, for instance, what pesticides were used, if it is local food and where it grew.

Proof Points has developed blockchain to translate data from traceability tools across supply chains so shoppers can check product claims of sustainability or origin. Blockchain means brands need to back up their positive impact claims. Customers can choose honest and worthy suppliers with their cash based on real information.

There are many potential uses for blockchain. Government spending could be trackable and transparent, as would financial transactions for everything from paying taxes to taxes on profits. Looking at healthcare, your medical records and treatments could be safely stored and instantly available to doctors in case of emergency.

Accessibility is a critical element of blockchain. On a macro level, more than 1 billion people worldwide do not have access to a bank account because centralized systems at banks exclude them. Cryptocurrencies have allowed the unbanked to pay for items digitally and to become more connected members of society. There are many new potential customers for businesses or people to be paid or taxed digitally.

Healthcare is one of the most important impacts of the blockchain in my opinion. Medical records get lost. One healthcare computer system won't talk to another. And healthcare fraud means patients get billed for items or services they didn't receive or pay for treatments they didn't need.

This could lead to a system that protect each patient's confidentiality and because it's tamper proof ensured no record could possibly disappear. Your whole medical history could be stored securely and easily accessed with your permission wherever it was needed. And medical fraud is a lot harder when there is a traceable paper trail.

# Conclusion

Blockchain technology is only going to grow in the fields of business, finance, law, medicine, and real estate. The reason the blockchain matters is that it is an agent of change.

Blockchain is not just a technology, but a fundamentally new way to think about data that will create a new iteration of the internet. It is as fundamental to data as the internet backbone is to information transmission.

There is a ton of potential for blockchain technologies — and it is constantly expanding. Also, the future of blockchain technology looks bright, and when you consider that it is already showing promise in almost every industry, it seems like the best is yet to come.

It will be interesting to see what the future holds for blockchain technology, especially regarding money transfers, banking services, decentralized marketplaces, and more.

# Resources

(Mathur, 2022)

(IBM, n.d.)

(Knysh, 2021)

(Javatpoint, n.d.)

(Wikipedia, n.d.)

(Iredale, 2020)

(Iredale, Top 10 Blockchain Adoption Challenges, 2021)

(Brown, 2021)

(Mitra, 2019)

(Cointelegraph, n.d.)

(Terrapass, 2021)

(Spatz, 2018)

(Tomaso Aste)

(Newbery, 2021)