PYRY PAJUNEN

Blockchain For Business

How can Blockchain ecosystems serve small and medium-sized enterprises?

THE DEGREE PROGRAMME IN ARTIFICIAL INTELLIGENCE
2022

Author(s) Pyry Pajunen	Type of Publication Bachelor's thesis	Date January 2022
	Number of pages 57	Language of publication: English

Title of publication
Blockchain for Business – How can Blockchain ecosystems serve small and medium-sized enterprises?

Degree Programme
Artificial Intelligence – Bachelor of Business Administration

Abstract

Small and medium-sized enterprises currently face many challenges, such as financial-, technology- and supply chain challenges. The aim of this thesis is to determine how SMEs can benefit from blockchain as part of their business operations and tackle the challenges that come along with it without taking unnecessary risks. The systematic examination of existing literature allowed a set of topics and research questions to be formed, which ultimately guide the structure of the entire thesis. An understanding of the most relevant properties of blockchain technology is pivotal for the addressing of the main chapters of this thesis which seek to form an appropriate understanding of what blockchain opportunities and challenges there are for SMEs, what an application framework could look like and how it may be restricted by policy and regulatory trends as well as limitations of the technology itself. The chapters enable one to conclude that SMEs may be faced with a multitude of resource-intensive challenges, especially in terms of adoption, implementation and management of the technology. Yet, the promised opportunities of the technology may be the opposite of a highly demanding planning and implementation process as they hold a high level of automation, low resource intensity and even the freeing up of resources in the long run, alongside improved efficiency of cumbersome and complex practical processes.

Keywords
Blockchain, Distributed Ledgers, Consensus, Cryptography, Small and Medium-Sized Enterprises, Cryptocurrency, Business Management, Business Data Processing, Risk management.

	Sivumäärä: 57	Kieli: Englanti
Otsikko: Lohkoketjut yrityksille – Kuinka PK-yritykset voisivat hyödyntää lohkoketjuteknologiaa?		
Koulutusohjelma: Artificial Intelligence – Bachelor of Business Administration		
Abstrakti: Pienet ja keskikokoiset yrityksen kohtaavat monia ongelmia liittyen finanssiin, teknologiaan ja toimintaketjuun. Tämän opinnäytetyön tarkoituksena on määrittää kuinka pk-yrityksen voisivat hyödyntää ja implementoida lohkoketjuteknologiaa ottamatta turhan suuria riskejä siirtyessä tähän uuteen innovatiiviseen teknologiaan. Systemaattinen tarkastelu olemassa olevasta tutkimuksista on mahdollistanut tutkimuskysymysten muotoilun, jotka ovat toimineet punaisena lankana koko kirjoitusprosessin aikana. Opinnäytetyö opettaa sen lukijalle, mitä lohkoketjut ovat, millaisista elementeistä lohkoketjut rakentuvat millaisia mahdollisuuksia lohkoketjut tuovat sen käyttäjälle ja myös millainen mahdollinen lohkoketjun käyttöönoton suunnittelutyökalu voisi näyttää. Kirjallisuuskatsauksessa syvennytään myös lohkoketjujen regulaation haasteisiin ja millaisella lähestymistavalla on mahdollista ylläpitää datankäsittelyyn liittyviä lainsäädäntöjä teknologiaa käyttäessä. Lohkoketjujen käyttöönoton hyödyt kuulostavat usein ylimitoitetuilta, joten tarkastelen kriittisesti myös lohkoketjujen haasteita ja puutteita. Pk-yrityksen saattavat kohdata resurssi-intensiivisiä haasteita, kuten liittyen lohkoketjujen käyttöönottoon, käyttöön ja ylläpitoon. Lohkoketjujen mahdollisuudet voivat olla tarkkaan suunnittelun ja käyttöönottosuunnitelman vastakohtia automatisoimalla prosesseja, säästämällä resursseja ja tehostamalla monimutkaisia prosesseja yliajan.		
Avainsanat Lohkoketjut, Hajautettu tietokanta, Konsensusprotokolla, Kryptografia, PK-yritykset, Kryptovaluutta, Datankäsittely, Riskienhallinta.		

CONTENTS

1 INTRODUCTION

Blockchain Technology. What is this mysterious technology that everybody in the technology field is talking about? What are basic blockchain principles, and what kind of problems can blockchain solve in this time of data-overload? Data volume grows exponentially every year, which makes it increasingly difficult to utilize information both efficiently and safely. Almost all data are mutable, and that causes significant security issues when users want to keep their sensitive data safe from manipulation and misuse.

Besides data incorrectness and storage there is a multitude of problems that different industries face with the handling of data such as the legality of the document, transparency problems during processes, trust issues, transactions, supply chain, voting systems and government operations (Felin & Lakhani, n.d.). One technology that can provide organizations with appropriate safety and efficiency for using and storing data is Blockchain. The adoption of blockchain technology can not only offer businesses enhanced security, but also provide other advantages such as greater transparency, increased trust by using smart contracts, instant traceability of data shared across a business network, and increased efficiency and reduced costs through automation (Golosova & Romanovs, 2018).

With the growing interest in the adoption of blockchain technology, the lack of a clear roadmap in the implementation of this technology creates considerable confusion as to whether blockchain is the appropriate technology for the business that intends to use it.

> Many individuals and organizations thwart positive changes in business due to their inability to see how innovative technologies can revolutionize the future. Emerging technologies bring new opportunities and change our lives by changing the way that we think and operate (Jai Singh Arun, Jerry Cuomo, Nitin Gaur, 2019 s. 25).

Although interest towards blockchain seems to be on the rise, it is clear that it is currently mostly applied in larger organizations as the benefits and resources for its adoption are more scarce in small and medium-sized businesses. Large organizations have strong knowledge management capabilities and can rely more on their financial and human resources; for small and medium-sized companies that often suffer from resource constraints, the compatibility of this technology is important in the assessment of blockchains impact (Jai Singh Arun & Jerry Cuomo & Nitin Gaur, 2019).

The purpose of this thesis is to share basic knowledge of blockchain technology and discuss the ways in which SMEs can use blockchain in their daily business. The thesis will set out with the basics of blockchain, such as transaction data, hashes, how blocks are created, consensus and immutability. Based on this information the thesis aims to develop a roadmap for SMEs assessment on whether blockchain is an appropriate technology to respond to their needs.

As blockchain is not always a suitable technology for SMEs to improve their business processes, organizations should critically analyze whether the innovative features of blockchain are compatible with their business and operating model. A failure to do this can be a disappointment for the smaller firms both by wasting financial capital and human resources for a futile initiative (Arun et al., 2019a).

This thesis will focus only on blockchain technology, not on cryptocurrency such as Bitcoin, even though blockchain is the underneath technology behind Bitcoin and many other cryptocurrencies.

2 BACKGROUND

2.1 Basic terms

Anonymous: Blockchain ensures that the participants' identity is never revealed, but either fully anonymous or nicknamed.

Baas: Blockchain-as-a-service. The term refers to a cloud-based blockchain development platform that businesses use to develop their own blockchain solutions, the same as the software-as-a-service concept.

Cryptocurrency: Cryptocurrency is a digital currency protected by cryptography that is almost impossible to hack or duplicate. Many cryptocurrencies are specialized networks based on blockchain technology - a distribution code implemented on a computer network.

Hash: The hash function is a function that can meet the encrypted demands of blockchain computation (digital fingerprint).

HyperLedger: An open-source project created to support blockchain-based distributed ledger development.

Peer-to-Peer Network (P2P): A peer-to-peer network is formed when two or more PCs share files and access devices such as printers without needing a unique server computer or server software.

Programmable: Blockchain is customized by programming.

Ripple: Ripple: is a real-time gross settlement system, currency exchange and remittance network created by Ripple Labs Inc.

Salting technique: A concept that typically pertains to password hashing. Usually, the length of the string is 32 characters or more.

Token: An asset or utility that resides within a blockchain and allows the holder to use it for investment or financial purposes.

Zero-knowledge proofs: An encryption scheme in which one party verifies the accuracy of specific information to another party without disclosing any additional information.

3 RESEARCH QUESTIONS AND METHODS

The research for this study was conducted in the manner of a literature review. A total of 75 articles and studies were included in the review and their content was carefully studied in order to acquire a broad enough base of sources for an appropriate understanding of existing literature on the topic. The included sources were selected based on accuracy for the topic as well as variety; it was crucial to include sources that had studied the different features and landscapes of blockchain and its application to ensure that a broad enough understanding could be established.

In order to arrive at the most optimal outcome, the thesis was guided by the following research questions:

1. What is blockchain technology?

2. What should SMEs know when starting a blockchain-based project?

3. How do SMEs use blockchain-based technology in their business?

4. What are the benefits that SMEs can have by using blockchain?

5. What are the blockchain-related risks?

6. What are the limitations of using blockchain?

In order to establish an appropriate understanding of the ways in which SMEs can utilize blockchain, it is necessary to be aware of potential risks that may come along with it – in order to prevent them from realizing. In addition, for an SME to make the assessment of blockchains utility it is necessary to account for both the benefits and the limitations of the technology through. Each of the research questions are reflected in dedicated chapters, with the aim of the systematically addressing the most relevant question about blockchain technology for SMEs.

4 BLOCKCHAIN FUNDAMENTALS

This section sums the main components of blockchain technology with the aim to provide a simple yet uncompromised understanding of what exactly it entails and how it functions.

4.1 The properties of blockchain

A blockchain is a distributed ledger shared amongst various computer networks. It is a shared, immutable ledger that enables recording transactions in a computer network, making it challenging or nearly impossible to hack. The blockchain stores information in a block that holds sets of information. It is like a primary database, but the information is in order.

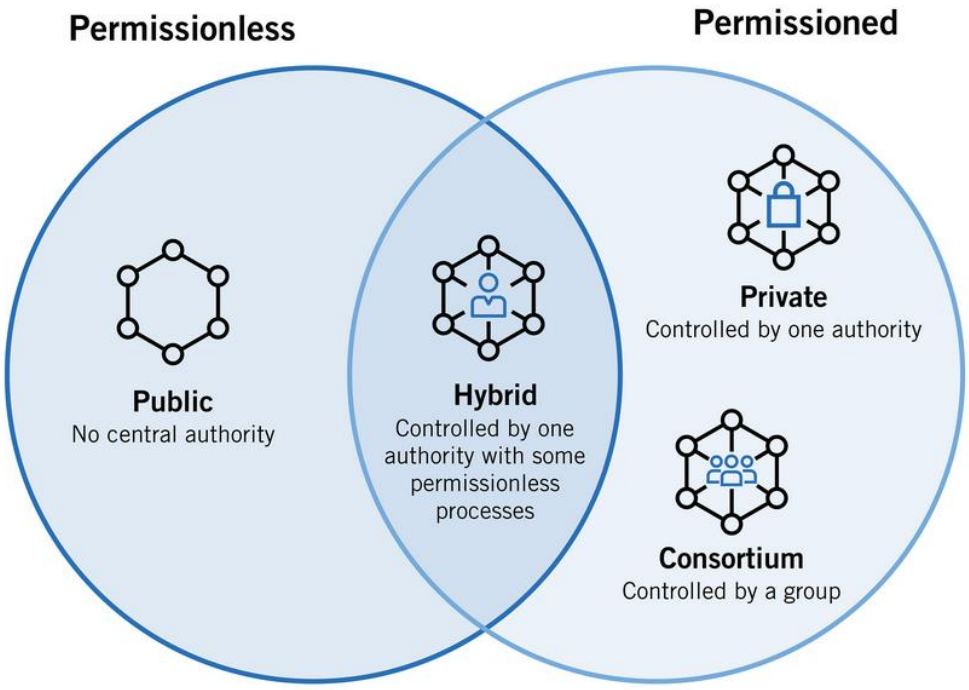
Ultimately blockchain is a dynamic digital transaction log. The contents of this log are distributed across a network of nodes on the blockchain. Each block contains data that is connected to another block. More simply, whenever a new activity occurs in a blockchain, it will timestamp the data and store it into a new block, which is connected to its predecessor. Many participants a.k.a nodes, host a distributed ledger, also known as Distributed Ledger Technology (DLT).

DLT uses a cryptographic signature in the identification process, preventing block replacing. This means that if one block is replaced, it will come instantly out of use. The cryptographic signature is similar to a digital version of a fingerprint, also known as a hash. If cybercriminals seek to damage a blockchain or its functionality, they would need to alter each block that is part of the chain, which becomes nearly impossible due to the highly advanced identification process.

Blockchain shows potential in altering digital interaction and manage complex things across industries, government agencies and social institutions. Thanks to its solid security properties and high level of enabled automation, blockchain technology may be able to also increase trust between parties and reduce costs. Thus, it is believed that blockchain will fundamentally change how businesses across the world operate (Gupta, 2020).

4.2 Types of blockchain

Add brief overview here: i.e. For developing a proper understanding of blockchain technology, it is important to learn what types of blockchain there are. Below is an introduction to the four different types of blockchain, which will each be covered individually in sections 4.2.1, 4.2.2, 4.2.3 and 4.2.4.



(*Types of Blockchain*, n.d.).

4.2.1 Public blockchain

Public blockchains allow anyone to join and are entirely decentralized. The public blockchain allows a user to access, create new data blocks and verify all blockchain nodes with equal rights. Public blockchains are mainly used for the exchange and mining of cryptocurrencies (S. G. Aruna Sri & Lalitha Bhaskari, 2018).

4.2.2 Private blockchain

A private blockchain is one that maintains a shared record of transactions. The network is accessible only by permission and administrators can edit transactions. This is an obvious choice if SMEs use or store sensitive data in a blockchain such as medical records (Sheth & Dattani, 2019).

4.2.3 Consortium blockchain

Consortium blockchains allow blockchains to be managed by a group of companies rather than a single entity. Therefore, consortium blockchains are more decentralized than private blockchains, resulting in a higher level of security. (Panda et al., 2019)

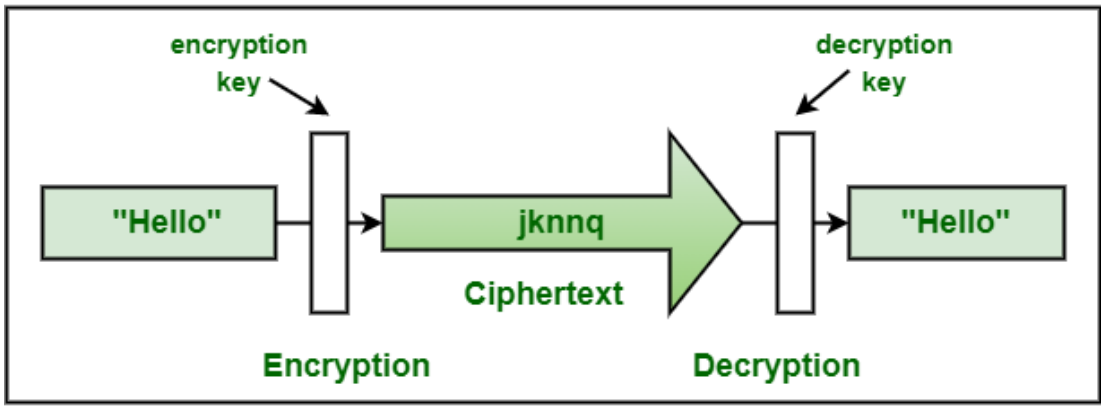
4.2.4 Hybrid blockchain

Hybrid blockchain takes the best out of public and private blockchain features and allows participants to take advantage of decentralization while at the same time maintaining sensitive personal data and enabling improved efficiency. With hybrid blockchains the benefits include the market access of public blockchains and the privacy and security benefits of private blockchains (S. G. Aruna Sri & Lalitha Bhaskari, 2018).

4.3 Cryptography

Cryptography explores secure communication methods that only allow the intended sender and recipient of the message to view its content. The word Crypto comes from ancient Greek and means "hidden". First, the message will be encrypted, which means that the original characters will be replaced with other characters. Second, the message must be decrypted before anyone can see the content of the message. It can be decrypted with a secret key. Otherwise, it is only random characters in a row. In addition, cryptography also incorporates image encryption using techniques such as microdots or combinations. The people of ancient Egypt used these methods in complex hieroglyphs, and the Roman Consul Julius Caesar reportedly used one of the first modern alphabets. The Enigma is the most known cryptography machine that Nazi's used during World War II to send messages (Diffie & Hellman, 1976).

When a message is captured, the receiver needs to be able to remove the encryption in order to read the message. Cryptologists developed a system called public key that makes decryption much tricky. To decrypt the message, a user should have one public and one private (sometimes referred to as secret) key (Diffie & Hellman, 1976). Senders request a public key to enter a message and send it along with it. Only the recipient's private key will be decrypted when the message arrives, meaning theft is useless because the message will stay encrypted.

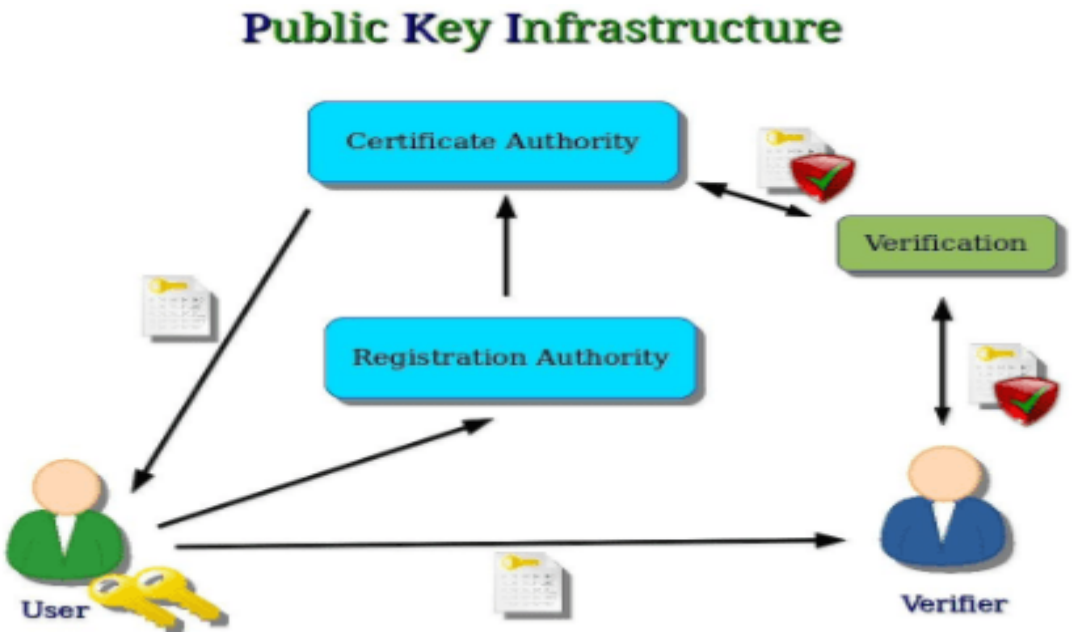


Cryptography

(*Fig. Encryption and Cryptography.*, 2021).

4.4 Public key infrastructure

Public key encryption is also known as public key infrastructure (PKI). It is a collection of different methods which are used for data encryption. PKI is based on generating digital certificates, managing operations, and storing and encrypting a public key. While in the physical world we use ID cards to prove our identities, a digital certificate accomplishes the same thing in the digital world, yet it is not limited to a person (Axon, 2021). The goal of PKI is to securely transfer electronic information to several network functions, such as e-commerce, online banking and email. Proof of the common password requires the necessary evidence to verify the identities of the parties involved in communicating and verifying the information to be transmitted (Jiang & Chen, 2021).



(Network Encyclopedia, 2019).

4.5 Consensus protocol in blockchain

The consensus algorithm is the process by which all blockchain network peers reach an equal agreement regarding the status of the distributed ledger. The goal is to gain

credibility in the blockchain network and build trust and mutual agreement between anonymous peers in a distributed environment (Xiao et al., n.d.). In particular, the consensus algorithm ensures that each new block is added to the chain only if the block is valid.

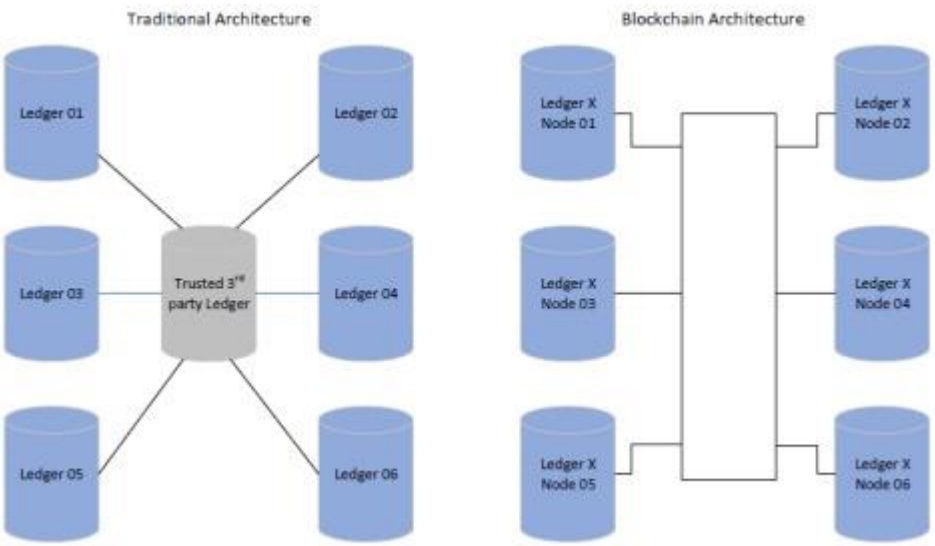
Blockchain consensus protocols have specific objectives such as reaching an agreement, enforcing cooperation and equal rights across all nodes, and each node's mandatory participation in the contracting process. Therefore, the goal of the consensus algorithm is to find the same deal that won in the network (Dash et al., 2021).

4.6 Proof of work

Proof of work is an algorithm that protects many cryptocurrencies, such as Bitcoin. Many digital currencies have a medium-sized business or leader that keeps track of every user and how much currency they have. Nevertheless, no such leader is in control of cryptocurrencies like Bitcoin. Proof of work is required for the online currency to operate without the company or government in charge of the exhibition (Karakostas & Kiayias, 2021).

4.7 Shared ledger

At the core of the blockchain is a ledger, a calendar of events in which all transactions performed in the chain are stored and can be checked in real-time by the actions of network parties. The information stored in the ledger is also unchangeable. Shared ledger is like a shared database maintained by independent participants (Salah et al., 2019). The shared ledger is not shared by a central authority, such as a central bank server, but each participant manages its copy of the registry separately from the others and updates it independently.



(Hughes et al., 2019).

Transactions and updates that take place online will be shared with all participants. After depending on the structure and operation of the network, a consensus is formed on how the ledger should be updated (Treleaven et al., 2017). Once the consensus is reached the shared ledger is updated for new transactions, and each participant keeps their identical copy of the ledger. Transactions are stored in a cryptographically signed and encrypted chain that can no longer be modified afterwards. This makes it unintentional or impossible to change the paths in the ledger (Mainelli & Smith, n.d.).

A shared ledger has the following characteristics:

- Records all activities in the business network; a shared book is a recorded program, the only source of truth.
- Shared between all participants in the network; repeatedly, each participant has a duplicate copy of the ledger.
- Participants only see the purchase they are authorized to watch.

(Crosby, 2016a).

4.8 Permission

Blockchain can require permission or not. Permissioned blockchain (a.k.a private blockchain) is primarily used in industrial use because it offers better security and identity and is easier to manage. For example, many SMEs could use a permissioned blockchain to produce a product and manage the supply chain. Permissioned blockchains also work best to control the stability of the data embedded in the blockchain to restrict access to transaction information (Wong et al., 2020). Transaction information can be stored on the blockchain and specify transaction details.

Some participants may only have the authority to care for one thing, while others, such as auditors, may be granted access to a broader range of functions. Public blockchains, in contrast, limit the level of transaction details to protect the privacy and provide anonymity (Panda et al., 2019).

For example, if Group A's assets are transferred to Group B, both Group A's assets and Group B's transaction details can be viewed. Group C assumes that these events linked to Group A and B have occurred but have not seen the transfer details. When the auditor or administrator is connected to the network, privacy services ensure that only the auditor sees a complete description of all the activities on the network (Shi et al., 2020).

4.9 Smart contracts

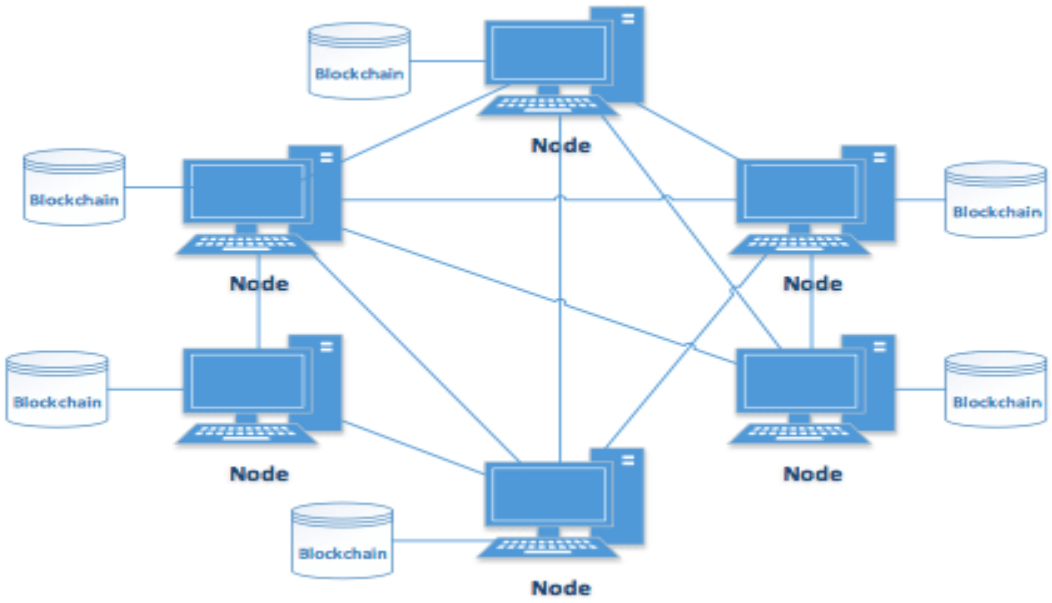
Smart contracts are blockchain-based applications that are theoretically the same as physical contracts but written in a programming language. Smart contracts are executed automatically when all predetermined conditions are confirmed. This saves time and builds trust between agents or organizations involved in the contract (Cong & He, 2019).

In other words, smart contracts are transaction protocols for enforcing and underlying legal agreements. The purpose is to implement the contract terms themselves: such as payments and legal obligations without the assistance of an established trusted third party. Thus, smart contracts aim to reduce transaction and enforcement costs as well as enable tamper-resistant transactions. The potential for smart contracts is much more than just cost savings. They can change entire business operations such as supply chain management through the application of smart contracts with the internet of things. The adoption of smart contract into processes as such would allow many industries to address critical issues in manufacturing and process coordination (Younus & Younus, n.d.).

4.10 Peer-to-peer network

A peer-to-peer network is a model divided by a group of devices (nodes) sharing files where each node acts as a peer. In a P2P network connections are made without central administration, which means that simply the nodes keep the network up and running and manage it (Li & Chen, 2007).

P2P structures are suitable for a wide range of applications and can be broken down into structured, unstructured, and hybrid networks for peers. The unstructured peer-to-peer networks are made up of random nodes, but do not work better than structured ones. In structured peer-to-peer programs, organized nodes can effectively search the network for desired data. Hybrid models are a combination of P2P and client-server models, when compared to structured and unstructured P2P systems. Hybrid networks often perform better than structured- or unstructured networks (Crosby, 2016b).

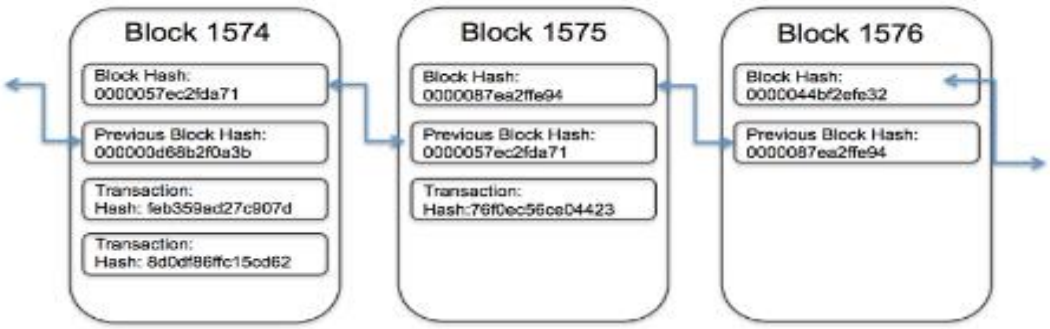


(*Fig. 1. Blockchain P2P Network.*, n.d.).

4.11 The block

A block is a key concept in systems of blockchain, as the name indicates. Blocks can be thought of as files that store data. The block stores some or all of the most recent data sent to the blockchain network that has not yet been included in the blocks that arrived earlier. Thus, the block is like a single page in the ledger. When a block is complete, it makes room for a new block in the chain. The information contained in the blocks is encrypted and organized in a specific format. Each block includes a reference to the preceding block (Yaga et al., 2018). When new blocks are subsequently created, they together form an unbroken chain, with each block constantly referring to the block preceding itself. This self-repeating process ensures the continuity of the chain and the integrity of the previous blocks up to the first block of the entire blockchain. The first block is called the Genesis block (Bowden et al., 2018).

Every time a block is completed, it becomes part of the past and gives space to a new block in the chain. The completed block is a permanent record of past data, and current data are instead stored in the current block until they become part of the past. The system operates in cycles and the data contained in the blocks is stored permanently. Blocks consist of encrypted paths and reference the previous block, forming an unbroken chain. Because the chains operate primarily in a distributed peer-to-peer network, it is almost impossible to hack previously stored data (Johar et al., 2021).



(Gupta, 2020)

4.12 Nodes

A node is usually a crossroads in a communication network. A node can also refer to any system or portable device connected to a network and may perform certain functions such as creating, receiving or sending information through a network channel. The node definition varies depending on the protocol layer to which it refers.

For example, a basic residential network may have a file server, two laptops and a printer. In this case, the network has four nodes, each with a MAC address to identify them separately (Florian et al., 2019).

5 BLOCKCHAIN OPPORTUNITIES AND CHALLENGES

The main objective of this thesis is to answer the following question: what is blockchain technology, and how can SMEs use and implement it in their business. One thesis is not enough to discuss all blockchain-based applications, so going through the fundamental opportunities and challenges is more sensible. This thesis also presents ideas for ways of adopting blockchain technology and what to keep in mind while doing so. The primary challenges to the success of the blockchain projects are scope, motivation and governance rather than technology itself.

5.1 The promise of blockchain technology

Digitization is impacting all sectors of the developed economy. The new and potentially disruptive digital blockchain technology and the decentralized ledger, offer great promise for many financial and business applications.

In recent decades, businesses have transcended local boundaries and become globalized in many ways. However, the most critical challenge is trust. In many cases potential partners have little or no trust, which is why an intermediary is needed between two or more parties to verify their business activities. Blockchain is a new way to generate trust between parties while altering how to do business because intermediaries can be removed.

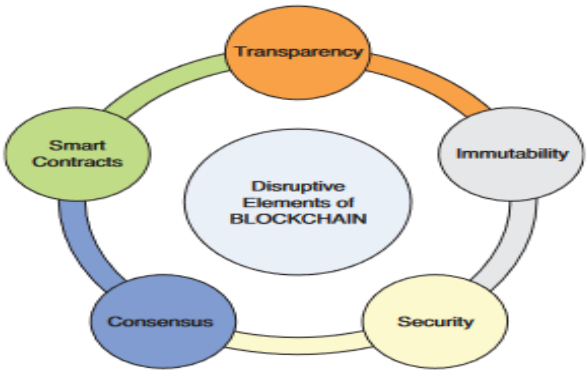
The promises of blockchain also entail increased connectivity and this way, more opportunities on a global scale. The spreading use of blockchain also forces organizations and even industries to rethink their business processes and models. Implementing blockchain technology is challenging because the governance structure is complex and slow to develop (Avgouleas & Kiayias, 2019). In addition, blockchain is not the development of traditional payment methods but rather a completely different recording and ownership-exchange system. While in traditional

accounts money is linked by financial intermediaries to a major network, blockchain is a public but encrypted transaction registration for all participants. Transactions are recorded in so-called blocks, encoded, and stored permanently. That way, the old blocks record past activity, while the newest block records the most recent transactions of all participants. These features of blockchain transactions enable a transparent way to track, analyze and record historical transactions (Wu & Duan, 2019).

Expectedly, blockchain technology will reduce the costs by dropping the need for intermediaries to maintain payment system. Thus, many banks and financial institutions are researching the potential use cases of this technology. Besides financial actors, governments can also benefit from the cost-reducing and security-increasing technology. For example, the UK government is debating how to adopt blockchain technology into its public service and regulation processes (Holotescu, 2018).

5.2 Disruptive elements of the blockchain

Blockchain has the potential to close the trust gap in business networks and communities through its five disruptive elements: immutability, smart contracts, security, consensus, and transparency. These five-elements make blockchain technology a powerful challenger for contemporary alternatives.



(Arun et al., 2019b).

5.2.1 Transparency of the blockchain

Blockchain provides complete visibility of transactions with a single replica shared in a ledger distributed across a network, depending on the permissions granted in the private or public blockchain-based network, who can view the complete path of the transaction. Previously, transparency was lacking in multi-participant business networks. Blockchain transactions are not hidden or altered in any way. Everything recorded in the ledger must have the consensus of the network to be approved and recorded in the same way in each ledger. Therefore, deleting or editing an item creates a record of when and by whom it was deleted on the network (Avgouleas & Kiayias, 2019).

Imagine a supply chain network with full transparency. Achieving real-time visibility in supply-chain management is tricky because many participants (consumers, retailers, distributors, manufacturers, suppliers, and sellers) operate their own platforms, which do not sync neatly. A blockchain-based supply-chain network could enable more transparency as every participant has the right to view transactions data and see the status and changes in real-time (Yiannas, 2018).

5.2.2 Immutability of the blockchain

Once the transaction has been recorded on the blockchain, nobody can modify it. If someone tries to modify the transaction, the blockchain will pop the update visible to the whole network. Every action in the blockchain is encrypted, timestamped and hashed which allows the connecting of blocks in order. If one block is removed from the chain, the previous blocks will be invalid. The hashes of the blocks have synced up all the time. The unchanging features eliminate counterfeiting and fraud challenges that many businesses face (Hofmann et al., 2017).

The biggest challenge is the duplication of legal and financial documents and valuables such as drugs, food products, luxury clothing and jewelry. Falsified legal documents lead to costs of up to $ 4 trillion worldwide, amounting to more than 7% of annual organizational expenses on a global scale. Simply put, fraudulent documents cause major expenses that could be at least to some extent avoided with smarter systems, such as smart contracts. Unchanged digital records and property or goods transfer history are recognizable and visible to participants in the blockchain, which prevents fraud and spoilage attempts on the system or process (Arun et al., 2019).

5.2.3 Security of the blockchain

Blockchain provides a secure transaction system that is very difficult to hack. Every data in the block is cryptographically secured with a hash and a trial of transaction updates. Participants in the network have their private keys assigned to the transaction or update anything to an existing transaction. Hence, security vulnerabilities in the blockchain are detected and prevented naturally. Every transaction is copied or shared in a distributed ledger, so hackers have to solve all blocks' hashes and have the right keys to see the block's content (Karame & Capkun, 2018).

Data and transaction security are fundamental concerns in all industries. Security is the main driving force in today's economy. According to analysts at Gartner, the cost of global cyber security is projected to exceed $ 114 billion in 2018, and by 2022 it will exceed $ 234 billion in total. These significant and growing investments into means of cyber security emphasize the increasing importance of security in technology. Due to its fundamental features being built on the notion of security blockchain has the potential to become ever more relevant as it may help businesses prevent fraud and mismanagement of funds in the future (Krikken et al., 2020).

Usually, companies store all their data in a centralized database which often are vulnerable to attacks and security breaches. In such cases a decentralized ledger can offer improved security because even if one ledger is inactive, other ledgers will copy the transaction and confirm the availability. Moreover, blockchain's immutability and transparent transaction history provide instant accessibility for compliance and regulations (Zhang et al., 2019).

5.3 Blockchain opportunities

An industry of information and cyber security has emerged, yet blockchain technology is by many experts believed to be the next significant transformational technology of the 21st century (Rot & Blaicke, 2019). Gartner estimates that blockchain-based business value will reach $ 3.1 trillion by 2030. Actual business value is driven by new opportunities for customers to change their businesses. From cryptocurrencies to border payments, from food security to source, from supply chain to commercial finance, clinical trials for health care conversion, digital identification for the management of rights for royalty settlement, land registry and more. Blockchain offers endless possibilities (Pal et al., 2021).

Blockchain opportunities can sound too fancy to be accurate, but Renault has been using a blockchain-based supply chain since April 2021 (Ballatore et al., n.d.). Odile Pancientici, the vice president of the blockchain project, Renault group, said: "Instead of spending time in linear exchanges — trading files, emails, calls — we have a direct common tool that everybody shares," says Panciatici. "We have real-time exchanges, we have transparency, and we have increased reactivity, all of which benefit our customers." (IBM, 2021). To summarize, blockchain technology entails many promises and many challenges, yet the single biggest impact of its implementation may exactly be what the underlying technology is capable of – scaling and streamlining a variety of operations regardless of its context or operators.

6 BLOCKCHAIN APPLICATION FRAMEWORK

The primary challenges with blockchain application are not just sophisticated technology: the development of blockchain technology will undoubtedly continue, just as many other old and new technologies continue to be developed. For many years blockchain technology has been mostly linked to cryptocurrencies amongst the wider public, for which blockchain does construct the technical foundation. In more recent years more and more companies seem to have adopted blockchain as well, to ensure readiness for i.e., entry or expansion to other industries. Significant challenges include finding a suitable workplace, having commitment and motivation on all levels, ensuring suitable governance processes and structures, as well as having the needed human and technological resources. These are significant challenges, yet they can be overcome with dedicated effort to manage the blockchain network effectively and focus on the ultimate transformation envisioned (Bianchini, 2020).

6.1 Scope

Current business policies and requirements may not support blockchains rapid development nor adoption in many cases. The build of companies does influence the ease or complexity of blockchain integration with importance on i.e., business and legal agreements and organization and decision-making structure. In addition, blockchain may not be a viable solution for possible hindering external reasons such as current government and legislation or bureaucracy or even the possible impact of disclosure on international reputation or partners. Therefore, it is crucial to choose the scope carefully to prevent failure and negative impact on other operations. If blockchain affects core aspects of a business model, it is essential to evaluate the scope of each of these following factors in the context of the short- and long-term goals (Kent Baker et al.,v 2021).

According to IBM, the right choice of scope determines blockchain project success. First, it is necessary to determine the minimum viable product (MVP) and minimum viable ecosystem (MVE) with a clear starting point for the blockchain project (Arun et al., 2019b). This means setting the specific, measurable, achievable goals, result-focused and time-limited (SMART) goals; and identifying the main actions that need to be undertaken by pointing out the following:

- Weaknesses and inability to identify cases of disruptive business use
- Business network participant readiness and ecosystem
- Business model and differentiation required for competition
- Governance planning and approach for cooperation and trust
- Action plan including costs and responsibilities
- Technology and vendor choice

(Arun et al., 2019b)

6.2 Technology

Perhaps surprisingly, technical concerns are not the biggest barrier to the adoption of blockchain. In fact, multiple organizations, including IBM and Amazon, have made calculated efforts to prepare blockchains for enterprise use by seeking to address concerns regarding the crucial processes involved in the adoption of the technology, such as implementation, expansion, integration, and operational concerns (Arun et al., 2019b). Often the technological challenges concerning matters such as confidentiality may seem too overwhelming for companies to see the benefit of adopting blockchain. In complex processes that include multiple alterations throughout the process – such as transactions, interaction and contracting, these challenges can be viewed as significant barriers to the benefits of blockchain. However, the adoption of blockchain technologies by many other agents has in fact addressed these concerns directly and provides futures adopters with case-examples.

Authorized and private blockchains can resolve privacy issues by ensuring the authenticity of transactions from authorized participants or by maintaining participant anonymity by deploying complex technology to control the display of private information. In public blockchain enforcement, organizations may opt for off-chain execution — meaning only transaction information needs to be recorded in the public ledger, whilst other information is kept private (White, 2017).

The scalability of a blockchain network depends most on the levels of security, cryptography and the capabilities of the consensus algorithm. The flow capacity will increase if the defensive force is highly automated. The proof-of-work component is the basic calculation and time-intensive task that guides many public blockchain implementation. For example, in such processes for cryptocurrencies these often consist of single-digit transactions that are verified and recorded every second. In comparison, a more powerful blockchain that is ripe for enterprise-level use and licensed for it, i.e., Hyperledger, is suited to deliver over a thousand transactions every second while upholding uncompromised security (Szalachowski et al., n.d.). Choosing the most appropriate technology for a blockchain project can be tricky. Below are some features which should be considered for a planned blockchain project:

- Public, private or hybrid blockchain network?
- What are the standard technological requirements?
- What are the privacy requirements?
- Can it be scaled? / Are there resources for scaling?
- Is it possible to integrate it with existing systems and applications?
- Can end-to-end support for implementation, deployment, and operation be provided for?

(Arun et al., 2019b).

6.3 Governance

A businesses ability to create and exist in an ecosystem that is suitably maintained and promoted, dictates much of the businesses success. Solid governance is the most vital requirement for the success of blockchain-implementation project as it manages the decentralized property with self-executable business and command over contracts. As this approach drives high efficiency via automation it is crucial to understand how smart contracts are built and maintained, especially as a fundamental part of the governance structure. Building consensus is another crucial elements, which however becomes easier in networks with trusted and motivated partners. Thus, a businesses success does in blockchain implementation also come much down to network and shareholder management (Werbach, 2018).

In a blockchain project, the risk is directly proportional to the systems of governance and what their implications are on the complexity of increasing uncertainty, delays and costs (Arun et al., 2019b). Public blockchain networks carry more risk than their private, licensed, or hybrid counterparts because of the much more challenging systems of governance. Thus, the system of blockchain network and its governance must be carefully planned and justified, in order for it to succeed. Poor planning may lead to compliance issues privacy and regulatory requirements, and thus make an open and decentralized governance structure the least suitable choice. As a relatively new technology, blockchain and the implications of its utilization are closely monitored and inspected in multiple industries by respective regulatory organs. Therefore, the risk of unintended compliance breaches may come in costly if the operational environment and its compatibility are not carefully studied and assessed (Sulkowski, 2018).

Blockchain network governance is multilayered, each of them in need of special attention to address the following specific concerns:

- The disruptive nature of the expected business model and its impact on participants
- Role and accountability of participants
- Decision making
- Encouragement and encouragement of partnership
- Intellectual Property Rights and Responsibilities
- Awareness of current regulatory and compliance policies and future changes
- Technical design and architecture

(Arun et al., 2019b)

6.4 Motivation

A blockchain network consists of the network founder and the participant. Establishing motivation and incentives are central in such distributed and decentralized ecosystems. Building focus on shared profit and pain comes through developing a system that is incentivizing enough. Actors with poor motivation or incompatible objectives can undermine the blockchains or its other participants success and goal achievement.

Such incentives are commonly not monetary but may instead entail access and exchange rights. For example, a founding member may seek access and transparency of transactions for regulatory consent purposes. A founding may have interest in specific authority or transactions while maintaining credibility and transparency (Wang et al., 2019).

Across the network equity can be shared in the form of a token to drive incentive for trading and exchanging assets and thus, impact the value of the traded assets. Such tokens can also function as rewards in the system and the value of these rewards increases if more participants work at or above the expected level. “These tokens are used in managing the loyalty points in retail or consumer businesses, carbon credits in energy trading, credit scores in a financial system, course or

merit certification in an educational system, or even a brand or a social image in a reputation system." (Arun et al., 2019b s.43).

In order to motivate participants of the blockchain network on a continuous rate, the following topics should be taken into account:

- What data, knowledge, or assets does it bring to the network?
- What is the value of their contribution to the network?
- What do they expect in return?
- What motivates them to be trusted partners?
- What incentives can you offer for short-term and long-term engagement?
- Which policies can enable automatic incentive allocation?

(Arun et al., 2019b)

7 BLOCKCHAIN APPLICATION IDEAS FOR SMES

Blockchain technology for industrial use offers exceptional opportunities for SMEs. This chapter determines the potential application of blockchain to accelerate SMEs and the challenges preventing small businesses from reaping blockchain adoption benefits. In addition to possible blockchain application this chapter also seeks to provide an overview of relevant policy and regulatory trends.

7.1 Transactions

One of the most typical applications of blockchain is for the purpose of money transfer. Accepting and completing payments in digital currencies is an example of this. Different sizes of businesses have come to implement blockchain in their financial services, offering more variety in payment methods for customers as well as an additional means of paying their employees and stakeholders directly in a digital currency. The most significant advantage is that the payment is faster, safer, and cheaper than through intermediates such as banks (Hashemi Joo et al., 2020).

Most often these transactions are done through public blockchains such as Bitcoin. However, public blockchains face issues with scalability and confirmation time. Bitcoin has long taken about ten minutes to confirm a payment which may be considered as way too long. Yet, there are constant improvements made in order to advance the technology and overcome issues in this area. Besides improvements in public blockchains, there are alternative digital currencies which utilize private blockchains instead, such as XRP (Ripple). It takes about three to five seconds to confirm a transaction with Ripple, and it is also much cheaper to acquire than Bitcoin. Using digital currencies to complete cross-border or even cross-continent payments swiftly is one significant incentive for an SME, as more traditional means of money transfer can take a long time on a scale as such (Jiang & Chen, 2021).

In the PayPal network users are now able to complete payments to merchants by utilizing cryptocurrencies. The way it works in practice, is that owners of PayPal wallets are no per se able to *pay* with a cryptocurrency, but instead they are able to convert currencies like Bitcoin, Bitcoin Cash, Ether and Litecoin into more commonly known fiat currencies such as dollars and euros. Although merchants do not technically accept the payments in crypto, this measure does enable more people to buy products and services using digital currencies. When receiving cryptocurrencies via PayPal it may include some additional fees, however small. When using crypto-wallets, transactions typically cost between zero to one percent. This is due to currencies such as Bitcoin not requiring the bank to guarantee each transaction (the Proof-of-work concept does that), so paying fees to financial

institutions is not necessary as it is with credit card purchases. However, along with the low costs come some risks. Typically cryptocurrencies are highly volatile, making it harder for merchants to accept crypto payments without taking on price risks (Chepurnoy et al., 2019). Thus, it is important for SMEs to carefully assess and evaluate the risks and benefits as well as the compatibility of a said currency and the organizations processes prior to accepting cryptocurrencies as a payment.

7.1.1 Blockchain-based funding

For the topic of SME funding, blockchain technology has the potential to change the current approaches completely by directly addressing some common issues in crowdfunding processes. The most commonly encountered barriers in crowdfunding are trust, choosing the right platform, setting realistic goals and deadlines, project implementation and copyright or intellectual property issues (Rosa Righi et al., 2020).

The utilization of blockchain technology enables many of these to be addressed in a fully altered system. As for trust, blockchain helps digitize P2P lending practices to increase transparency and this way build and facilitate more reliability between lenders and borrowers.

The disintermediation element of blockchain makes it easy and fast for SMEs to raise funds as well as reduces complexity of the entire process. Removing the traditional barriers of fundraising, such as intermediary involvement and incomplete transparency, reduces the need for complicated paperwork whilst the automated nature of the process can eliminate commissions, high brokerage fees and all other overheads related to the sale of shares (Hassija et al., 2020).

Fundraising for SMEs can be made easier, safer and faster via the utilization of blockchain-based smart contracts. For example, on crowdfunding platforms the utilization of smart contracts can alter the most basic terms of the whole investment

process. First, investors place their money into projects during the fundraising phase, which is then secured through smart contracts. Second, the creators are funded to realize the project only after the campaign is successful in the terms set in the smart contract, meaning the actions satisfy the pre-determined conditions of the contract. If the project fails to reach its goal, the funds will automatically be returned to the investors (Ganne, n.d.).

7.1.2 We.trade

We.trade is a blockchain application that allows SMEs to receive foreign trade payments. It was founded by nine European banks (Rabobank, Deutsche Bank, HSBC, KBC, Natixis, Nordea, Santander, Societé Generale and UniCredit) with the aim of helping SMEs manage transactions on the same platform with another. Foreign trade payments can be complex for SMEs as the supply chain may pose risks and challenges such as complex paperwork, susceptibility to errors, high costs and and room for fraud. For solving or addressing these challenges, SMEs usually lack the resources and expertise. We.trade is designed to address such challenges by simplifying and allowing country crossing transactions via a safe and legitimate blockchain platform.

We.trade connects all participants such as the buyer, seller, bank and transportation providers with the same right to access order details and view potential changes in almost real-time. Furthermore, We.trade is fully automated and every transaction is recorded using blockchain, a secure, shared database. Each entry in the blockchain is timed and stamped with a unique cryptographic signature and all allowed parties can access the information simultaneously. Smart contracts guarantee that if one party of the transaction completes their part as agreed it becomes recorded in the blockchain and the contract will automatically initiate the process of sending the payment or cancel the order if not all conditions are met (Civelek & Özalp, 2018).

7.2 Using smart contracts

The use of smart contracts in SMEs can involve many benefits not only for the business, but also employees and customers. With often limited resources SMEs need to be efficient in their operations and spend resources wisely and productively. Smart contracts can potentially automate the invoicing process allowing employees to focus on other tasks (Chang et al., 2019). Automating the invoicing process also reduces the risk of manual errors.

In terms of customer-company relationships, smart contracts can benefit from an unprecedented new automation layer. Upon completion of this automation layer, the design ensures payment for SMEs and benefits the client by ensuring that SMEs are encouraged to complete the work within the agreed time frame; Otherwise, there may be aftereffects such as penalties for the defector. In addition, smart contracts can be used as a mechanism for conflict resolution as it stores a permanent record of past transactions used as evidence in cases of arbitration (Youngson & Dounas, 2021).

The smart contract can introduce many other benefits for SMEs as well, such as autonomy, decentralization, security and speed. However, the smart contract technology is not perfect and it has several disadvantages such as an uncertain legal status as well as a challenging process of making changes to the contract or its programming. Changing the smart contract information is very difficult and risky as any error in the contract can be expensive to correct. The critical thing to remember is the transaction costs. In some cases, smart contracts may be more expensive than traditional contracts, which is one of the problems with blockchain. The transaction costs consist of development and gas fee (the fee of validation transaction) (Alharby & Moorsel, 2017).

Initially, smart contracts were designed to save third party involvement. However, a lack of external familiarity can reduce the effectiveness of smart contracts. Sometimes, a person who enforces an external enforcer shows better flexibility and solves the problem very well (Sklaroff, n.d.).

7.3 Blockchain-as-a-service

Blockchain-as-a-service (BaaS) is a model for businesses and organizations which has been built and developed in a cloud. Blockchain is developed, hosted, and implemented in the cloud as a service application. This application is similar to any other blockchain application hosted locally with smart contracts and other related blockchain functions. The advantage of the BaaS model application is that the business does not have to worry about managing and setting up any infrastructure such as servers and can instead rely on the cloud to manage all these IT-related tasks (Singh & Michels, 2018).

Like Software-as-a-service (SaaS), BaaS encourages more and more industries to adopt blockchain technology into their businesses, although they are heavily reliant on IT-capabilities to adopt it. The technical implications of blockchain and the development and maintenance of its affiliate infrastructure have prevented many industries from adopting mainstream blockchain technology in their areas. (Yang et al., 2019).

The following are examples of BaaS services:

- Data security
- Supply chain management
- Resource allocation
- Smart contracts
- We.trade
- App-building and monitoring tools
- Preconfigured networks and infrastructures

BaaS is a suitable solution for non-developers as it is enough to understand where to use blockchain without needing to know how to code it or maintain servers.

7.4 Blockchain supply chain management

Modern supply chains are inherently complex, with multi-segment competing to serve geographically. Globalization, different regulatory guidelines, and supply chain procedures make it difficult to evaluate information and manage risk in this complex network (Esmaeilian et al., 2020). A supply chain can benefit from using blockchain to trace chain activities, but chain activities are usually extremely complicated and delicately curated. For example, shipments, payments, orders, and transportation are usually split into several parts, and different parties manage order data in their own databases which directly leads to poor over-all traceability. Lack of traceability can enable inefficiency, mismanagement and even fraud.

As customers increasingly want to trace their orders and show more interest in respobsibility, it is evident that traceability is becoming a more valuable feature of the supply chain. People have become more aware of supply chain loopholes and concern for environmental impact of production processes forces businesses to transform into more sustainable practices. For these reasons, businesses have to facilitate more transparent ways to manage their supply chains and for SMEs it may be a prerequisite for further growth. Through the Hyperledger supply chain group, SMEs can implement blockchain technology in their business and strengthen trust and traceability with the customer and other parties (Wong et al., 2020).

7.4.1 Blockchain technology in supply chain

The usual supply chain includes manufacturers, suppliers, distribution centers, coordinators, transporters, and services involved in informatics, building materials, and cash flow. The activities that occur within the supply chain are commonly complex and often challenging as orders, shipments and payments may not sync up neatly. For SMEs this may be more often a challenge than to larger companies due to the scarcity of resources to manage the supply chain. The use of blockchain technology may introduce improved recording, tracking and information sharing to

the supply chain, thus boosting the functionality of the chain overall. Such improvements can be made possible with a real-time digital transaction log for all participants in the supply chain network (Cocco et al., 2021).

The features of blockchain technology help track the raw material production journey from supplier to consumer in the supply chain. It assists in eliminating counterfeit goods by using the ability to identify the source of the asset. However, data errors are common in the supply chain and are often created in the input phase. As fewer people on the blockchain do the data entry task, errors in data entry can be minimized. In addition, using blockchain allows for ending eventually unnecessary activities around the tracking, recording and sharing information of the supply chain processes, as all stakeholders in the supply chain can access the same information.

It is also possible to manage inventory estimation with blockchain technology, which ultimately lowers inventory costs. The timestamped feature in a blockchain enables higher security, as after a purchase, it is not allowed to change or manipulate the order data, making the supply chain more transparent and reliable (Younus & Younus, n.d.). Typically, data is stored and integrated on a service provider's central server within a simple traditional supply chain. These servers are often vulnerable to outside attacks. However, due to distributed consensus and highly secure cryptography methods, blockchain technology may provide an environment safe from cyber-attacks (Cole et al., 2019).

There is plenty of room for improvement in the common supply chain regarding end-to-end traceability, product delivery speed, coordination and financing. Blockchain is a powerful tool to address deficiencies as such as well as common loopholes. For those supply chain managers who are looking to make assessments about blockchain potential for their businesses, the shift may seem mainly resource-intensive. They need to develop new regulations, experiment with different technologies, operate pilots with different blockchain platforms and participate in efforts to build ecosystems with other organizations. Yes, it does require a commitment of scale, but post-implementation the investment promises to produce good returns in a less resource-intensive manner than the current methods. The investment however is

worthy for long-term productivity increase rather than the short term. For less resource-intensive solution seekers, companies that offer Baas may be a more viable option. Baas is also the way to go for non-developers (Esmaeilian et al., 2020).

8 POLICY AND REGULATORY TRENDS IN BLOCKCHAIN

One of the critical challenges in utilizing blockchain technology is the law and regulation framework. Where technology is evolving rapidly, legislation often comes much after. New technology phenomena are difficult to regulate, especially if the subject of regulation is not adequately understood or its effects are difficult to predict. Blockchain technology has so far evolved without significant regulatory constraints, but with the increased media visibility and increased practical applications in recent years, states have woken up to the fact that blockchains have come to stay.

There is a lot of uncertainty in the market about legislation and the risk that regulations will be formulated and implemented with a lack of knowledge and innovation development may thus be hampered. However, regulation can create clear rules between actors in different sectors, which could allow for development and deployment, both in a safer and more reliable environment. Moreover, the European Union is very receptive to blockchain technology, which speeds up innovation.

8.1 Ensure GDPR compliance

In a nutshell, GDPR sets the rules for how companies, governments and other agencies can process data from residents of the European Union (Radley-Gardner et

al., 2016). GDPR's primary goal is to improve and unify data protection laws for individuals in the European Union. If using blockchain technology in SMEs it is crucial to keep the following three examples of managing GDPR in mind, depending on the blockchain- or application type.

Example 1: Public blockchain. Buying and selling cryptocurrencies, for example, can be done without the involvement of a third party. In terms of GDPR compliance, it is impossible to hold anyone accountable for it because there are no data controllers. Consumers are responsible for compliance under the terms of service, limiting the uploading and processing of specific categories of personal data. In public blockchains, a developer can use zero-knowledge proofs to guarantee users. However, it should be emphasized that more minor compliance updates to may be introduced based on the specific governance scheme utilized by blockchains (*Blockchain and GDPR*, n.d.).

Example 2: An application that uses a public blockchain as a backend. The owners of applications can decide from whom personal data is collected. They are also responsible for informing the user that a portion of their data is stored on the blockchain (Wright, n.d.). According to the European Union,

> "Currently, the only way to guarantee GDPR compliance in this scenario is to hash out any personal data to a server controlled by someone that will be identified as a data controller. To decrease the possibility of pre-image attacks, state of the art salting techniques can be used. A salt is a random string that is concatenated to data to be encrypted, kept under the control of the data processor. Also, any table that matches pseudonyms (public keys) generated on behalf of data subjects required by the smart contract, to their identities needs also to be stored off-blockchain. In use cases where actual processing (instead of only storage) of personal data is encoded in a smart contract and a hash cannot be used, a possibility is the use of multi-party private computation schemes, however, although the encryption provided by the scheme might be considered enough for GDPR purposes, further research is needed to verify that the level of

decentralisation offered by the additional network correspond to expectations".

(European Parliament. Directorate General for Parliamentary Research Services., 2019).

Example 3: Private Blockchain. A person who voluntarily joins a private blockchain should agree with the terms, including how personal data are processed, stored, and that others might process any data inputs with corresponding responsibility in the event of data breaches or misuse (Wright, n.d.). In a private blockchain the members can be appointed into roles of data controllers, in which they jointly enforce GDPR. Those data controllers need to agree on a set of terms for data processing and storing and make sure that GDPR rules are complied with within this process (European Parliament. Directorate General for Parliamentary Research Services., 2019). In both, centralized and decentralized data control mechanisms, the data processing another person's data should entail consideration of the following:

1. Is personal data collected? Where is it stored?
2. How is personal data is processed? What is the purpose of decentralizing that process?
3. Which blockchain is in use (public, private or hybrid)? Can the blockchain validators agree with GDPR rules?
4. If the data will be encrypted or hash entered into the blockchain, who will have the keys (or links to the original data)?

(European Parliament. Directorate General for Parliamentary Research Services., 2019).

9 PROJECT RISK MANAGEMENT

Proper risk management helps succeed in the implementation of a blockchain project. This chapter emphasizes the importance of a risk management plan and the

fact that risks need to be considered carefully during the shaping of a blockchain strategy.

9.1 Blockchain-related risks

Blockchain adoption is a good proposition for all SMEs at present. However, failure to recognize the risks of blockchain adoption is dangerous to blockchain implementation. A proper understanding of the risks associated with blockchain adoption can help SMEs formulate an optimal blockchain implementation strategy.

1. The first risk of blockchain adoption is strategic. SMEs should evaluate whether they want to adopt or wait for blockchain technology to mature. SMEs should consider both of these options to assess each ones level of introduced risk on their business strategy (Drljevic et al., 2020). In addition, the P2P environment of the technology can influence the choice of networks to participate. Most importantly, understanding technology limits on services and products.

2. Business continuity is crucial in blockchain adoption. Blockchain management (BCM) consists of these elements: analysis, solution design, implementation, testing & acceptance, and maintenance. So, BCM goes in a cycle and it is necessary to keep this in mind all the time as business processes in the blockchain can lead to technical and operational failures (Kwak & Stoddard, 2004). Therefore, the business continuity plan can decrease unnecessary risks.

3. The risk of blockchain-related information (in)security is also one of the most important aspects to consider. Blockchain technology provides better transaction security, however, it does not provide the desired security of the wallet (Zhang et al., 2019). Distributed ledger and cryptographic precedents can confirm the limitations of data corruption. On the other hand, the amount

kept in a particular account will always be at risk of being taken over (Vishwakarma et al., 2018). When choosing a crypto wallet, the wallet's security solutions need to be considered at first.

4. One of the most widely known risks related to blockchain adoption is regulatory risks. The blockchain-related application does not have specific regulatory requirements. In addition, different operating conditions, different role-players and cross-border activity permissions can also create regulatory barriers to blockchain adoption. (Woodside et al., 2017).

Clarifying the benefits and risks of blockchain adoption helps choose the right technology and strategy to support the SMEs own business goals. Keeping the risk management process dynamic and systematic is critical to success in blockchain adoption as well as following the relevant industry's regulations helps find immaculate approaches for adaptation challenges (Kwak & Stoddard, 2004).

10 BLOCKCHAIN LIMITATIONS

Blockchain technology sounds revolutionary as it can solve many contemporary challenges, but every revolutionary technology has limitations, and blockchain has them too. This chapter discusses the most common blockchain limitations and gives example cases where blockchain is an unsuitable technology. Blockchain technology has several limitations: lack of privacy, security model, scalability, latency, and governance (Hughes et al., 2019).

10.1 Limitations

- Lack of privacy. The data is stored permanently in a block, and every node has whole transcription history. This argument is for a specific security

application but not for privacy (Axon, 2021). The permanently stored data is an attribute in a security context, but it is a limitation when privacy is a necessity. Blockchain technology is not suitable for a process where data deletion or modification is essential. The data deletion is possible, but it is challenging.

- Security model. Blockchain security models are based on public-key infrastructure technology which authenticates users and devices in the digital world. PKI generates one public and one secret key for a document. The public key and secret key construct a pair linked to specific documents or data. The document will stay " locked " without a public and secret key (Singla & Bertino, 2018). PKI indeed is a secure system, but there is no protocol to return the keys if the user loses the keys. Thus, the model in fact creates complexity.

- Scalability. The scalability issues are related to block size, numbers of transactions and latency. The block size depends on the type of blockchain that is in use, but approx; one block can store 1 Mb of information. The increasing usage of blockchain leads to more transactions. If the system overloads, gas fees (transaction fees on blockchain) and the whole system's processing time increase (latency). However, most of the scalability problems are related to hardware problems (Zhou et al., 2020).

- Governance. The governance structure is complicated and develops slowly. The distributed nature of blockchain provides many advantages, but who is chargeable in situations of dispute and problem situations (Wright, n.d.). In a private blockchain, the answer is obvious as it is the responsibility of the service provider, but what about this in public blockchains?

The list above shows non-technical and technical limitations on blockchains that may limit the adoption and utility of blockchain. Blockchains are relatively innovative, yet organisations nor regulators have not mastered them yet. When blockchain

reaches a level of maturity that increases its significance in terms of regulation, policy and regulatory improvement can also be expected.

11 CONCLUSION

The future of SME financing requires a combination of innovations in fintech, financing models and emerging blockchain technology. Blockchain-based applications allow capital providers to access more data, advanced algorithms, and application-programming interfaces — tracking payments, contract fulfilment, and many other aspects of business operations — by allowing you to define how you leverage various software and tools to interact.

Standard financial instruments developed in a digital environment enhanced by blockchain allow all parties to represent the duplicate accounts and certified and audited cash flows. Such standards lead to near-real-time reporting and securitization of loan portfolios, which was previously considered impossible.

The adoption of blockchain technology facilitated by the asset digitization process revolutionizes the way we view risk and provides innovative solutions to manage value, hedging and loss in financial markets and the real economy. Its adoption will eventually give lenders better capabilities and give new confidence to not currently considered creditworthy lenders.

However, in order to succeed with revolutionary technologies as such, the adopting party must have an appropriate understanding of what exactly the technology is and this way what it may introduce to the adopter. This thesis has outlined a number of properties, challenges, opportunities, limitations, ideas as well as regulatory facts that are central in the formulation of this understanding. The most valuable input derived here is as follows. The adopting enterprise must formulate their blockchain implementation on a careful assessment of business and strategic needs, resources

and objectives in order to be guided to select the appropriate properties of blockchain technology. Due to various options, it is crucial, that an enterprise is aware of their implications on their own operations and this way is able to make an appropriate risk-analysis. The compatibility of the selected type of blockchain application with the business model is necessary, as one of the central benefits of the technology is the ability to scale its use. However, ranging from the subject of its use to the types of management (i.e. public, private, hybrid) blockchain can be realized in a variety of ways. Poor planning and a lack of understanding may lead to the adoption of an expensive, yet incompatible technology that ultimately cannot redeem its promises.

REFERENCES

Alharby, M., & Moorsel, A. van. (2017). Blockchain Based Smart Contracts: A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*, 125–140. https://doi.org/10.5121/csit.2017.71011

Arun, J. S., Cuomo, J., & Gaur, N. (2019a). *Blockchain for Business*. Addison-Wesley Professional.

Arun, J. S., Cuomo, J., & Gaur, N. (2019b). *Blockchain for Business*. Addison-Wesley Professional.

Avgouleas, E., & Kiayias, A. (2019). The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment. *European Business Organization Law Review*, *20*(1), 81–110. https://doi.org/10.1007/s40804-019-00133-3

Axon, L. (2021). *Privacy-awareness in Blockchain-based PKI*. 18.

Ballatore, M., Arena, L., & Attour, A. (n.d.). *When an Institutional IT Renews a Connected Vehicle Ecosystem: Evidence from the trust-mediator Role of Blockchain Technology* *. 18.

Bianchini, M. (2020). *Blockchain for SMEs and entrepreneurs in Italy*. 78.

Blockchain and GDPR. (n.d.). 8.

Bowden, R., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2018). Block arrivals in the Bitcoin blockchain. *ArXiv:1801.07447 [Cs]*. http://arxiv.org/abs/1801.07447

Chang, S. E., Chen, Y.-C., & Lu, M.-F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process.

Technological Forecasting and Social Change, *144*, 1–11. https://doi.org/10.1016/j.techfore.2019.03.015

Chepurnoy, A., Kharin, V., & Meshkov, D. (2019). A Systematic Approach to Cryptocurrency Fees. In A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, & M. Sala (Eds.), *Financial Cryptography and Data Security* (Vol. 10958, pp. 19–30). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-58820-8_2

Civelek, M. E., & Özalp, A. (2018). *BLOCKCHAIN TECHNOLOGY AND FINAL CHALLENGE FOR PAPERLESS FOREIGN TRADE*. *15*, 8.

Cocco, L., Mannaro, K., Tonelli, R., Mariani, L., Lodi, M. B., Melis, A., Simone, M., & Fanti, A. (2021). A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery. *IEEE Access*, *9*, 62899–62915. https://doi.org/10.1109/ACCESS.2021.3074874

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management: An International Journal*, *24*(4), 469–483. https://doi.org/10.1108/SCM-09-2018-0309

Cong, L. W., & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, *32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007

Crosby, M. (2016a). *BlockChain Technology: Beyond Bitcoin* (No. 2). *2*, 16.

Dash, S. S., Das, S., & Panigrahi, B. K. (Eds.). (2021). *Intelligent Computing and Applications: Proceedings of ICICA 2019* (Vol. 1172). Springer Singapore. https://doi.org/10.1007/978-981-15-5566-4

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Drljevic, N., Aranda, D. A., & Stantchev, V. (2020). Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Computer Standards & Interfaces*, *69*, 103409. https://doi.org/10.1016/j.csi.2019.103409

Esmaeilian, B., Sarkis, J., Lewis, K., & Behdad, S. (2020). Blockchain for the future of sustainable supply chain management in Industry 4.0. *Resources, Conservation and Recycling*, *163*, 105064. https://doi.org/10.1016/j.resconrec.2020.105064

European Parliament. Directorate General for Parliamentary Research Services. (2019). *Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law?* Publications Office. https://data.europa.eu/doi/10.2861/535

Felin, T., & Lakhani, K. (n.d.). *Before jumping on the bandwagon, companies need to carefully consider how ledger technologies fit into their overall strategy.* 7.

Fig. 1. Blockchain P2P Network. (n.d.). ResearchGate. Retrieved 2 December 2021, from https://www.researchgate.net/figure/Blockchain-P2P-Network_fig1_320127088

Fig. Encryption and Cryptography. (2021, February 5). GeeksforGeeks. https://www.geeksforgeeks.org/difference-between-encryption-and-cryptography/

Fig. Types of Blockchain: Public, Private, or Something in Between | Foley & Lardner LLP. (n.d.). Retrieved 29 December 2021, from

https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

Florian, M., Beaucamp, S., Henningsen, S., & Scheuermann, B. (2019). Erasing Data from Blockchain Nodes. *ArXiv:1904.08901 [Cs]*. http://arxiv.org/abs/1904.08901

Ganne, E. (n.d.). *BLOCKCHAIN AND SME FINANCING*. 18.

Golosova, J., & Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, 1–6. https://doi.org/10.1109/AIEEE.2018.8592253

Gupta, M. (2020). *Blockchain For Dummies* (3rd IBM Limited Edition). John Wiley & Sons, Inc.

Hashemi Joo, M., Nishikawa, Y., & Dandapani, K. (2020). Cryptocurrency, a successful application of blockchain technology. *Managerial Finance*, *46*(6), 715–733. https://doi.org/10.1108/MF-09-2018-0451

Hassija, V., Chamola, V., & Zeadally, S. (2020). BitFund: A blockchain-based crowd funding platform for future smart and connected nation. *Sustainable Cities and Society*, *60*, 102145. https://doi.org/10.1016/j.scs.2020.102145

Hofmann, F., Wurster, S., Ron, E., & Bohmecke-Schwafert, M. (2017). The immutability concept of blockchains and benefits of early standardization. *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, 1–8. https://doi.org/10.23919/ITU-WT.2017.8247004

Holotescu, C. (2018). *Understanding-blockchain-opportunities-and-challenges_Content File-PDF.pdf*. https://www.ceeol.com/search/viewpdf?id=682300

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

IBM. (2021, May 10). *Driving auto supply chains forward with blockchain*. IBM. https://www.ibm.com/case-studies/renault

Jiang, J., & Chen, J. (2021). Framework of Blockchain-Supported E-Commerce Platform for Small and Medium Enterprises. *Sustainability*, *13*(15), 8158. https://doi.org/10.3390/su13158158

Johar, S., Ahmad, N., Asher, W., Cruickshank, H., & Durrani, A. (2021). Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey. *Applied Sciences*, *11*(14), 6252. https://doi.org/10.3390/app11146252

Karakostas, D., & Kiayias, A. (2021). Securing Proof-of-Work Ledgers via Checkpointing. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–5. https://doi.org/10.1109/ICBC51069.2021.9461066

Karame, G., & Capkun, S. (2018). Blockchain Security and Privacy. *IEEE Security & Privacy*, *16*(4), 11–12. https://doi.org/10.1109/MSP.2018.3111241

Kent Baker, H., Nikbakht, E., & Stein Smith, S. (Eds.). (2021). Prelims. In *The Emerald Handbook of Blockchain for Business* (pp. i–xxviii). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-198-120211001

Krikken, R., Belak, A., & Hevesi, P. (2020). *2021 Plannig Guide for Security and Risk Management*.

https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/729015-2021-planning-guide-for-security-and-risk-management.pdf

Kwak, Y. H., & Stoddard, J. (2004). Project risk management: Lessons learned from software development environment. *Technovation*, *24*(11), 915–920. https://doi.org/10.1016/S0166-4972(03)00033-6

Li, H., & Chen, G. (2007). Data Persistence in Structured P2P Networks with Redundancy Schemes. *Sixth International Conference on Grid and Cooperative Computing (GCC 2007)*, 542–549. https://doi.org/10.1109/GCC.2007.59

Mainelli, M., & Smith, M. (n.d.). *Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology)*. 47.

Network Encyclopedia. (2019, October 16). *Fig. 1. Public Key Infrastructure (PKI)*. Network Encyclopedia. https://networkencyclopedia.com/public-key-infrastructure-pki/

Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key management for blockchain technology. *ICT Express*, *7*(1), 76–80. https://doi.org/10.1016/j.icte.2019.08.002

Panda, S. S., Mohanta, B. K., Satapathy, U., Jena, D., Gountia, D., & Patra, T. K. (2019). Study of Blockchain Based Decentralized Consensus Algorithms. *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, 908–913. https://doi.org/10.1109/TENCON.2019.8929439

Radley-Gardner, O., Beale, H., & Zimmermann, R. (Eds.). (2016). *Fundamental Texts On European Private Law*. Hart Publishing. https://doi.org/10.5040/9781782258674

Rosa Righi, R. da, Alberti, A. M., & Singh, M. (Eds.). (2020). *Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment*. Springer Singapore. https://doi.org/10.1007/978-981-15-1137-0

Rot, A., & Blaicke, B. (2019). Blockchain's Future Role in Cybersecurity. Analysis of Defensive and Offensive Potential Leveraging Blockchain-Based Platforms. *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 447–451. https://doi.org/10.1109/ACITT.2019.8779855

S. G. Aruna Sri, P., & Lalitha Bhaskari, D. (2018). A study on blockchain technology. *International Journal of Engineering & Technology*, *7*(2.7), 418. https://doi.org/10.14419/ijet.v7i2.7.10757

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and Open Research Challenges. *IEEE Access*, *7*, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507

Sheth, H., & Dattani, J. (2019). Overview of Blockchain Technology. *Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146*. https://asianssr.org/index.php/ajct/article/view/728

Shi, J., Li, R., & Hou, W. (2020). A Mechanism to Resolve the Unauthorized Access Vulnerability Caused by Permission Delegation in Blockchain-Based Access Control. *IEEE Access*, *8*, 156027–156042. https://doi.org/10.1109/ACCESS.2020.3018783

Singh, J., & Michels, J. D. (2018). Blockchain as a Service (BaaS): Providers and Trust. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 67–74. https://doi.org/10.1109/EuroSPW.2018.00015

Singla, A., & Bertino, E. (2018). *Blockchain-based PKI solutions for IoT*. Google Docs. https://drive.google.com/file/d/1X3G3KH3-y6jyp1zC1tPr9T7My7Ucu0OC/view?usp=embed_facebook

Sklaroff, J. M. (n.d.). Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, *166*, 43.

Sulkowski, A. J. (2018). *Blockchain, Law, and Business Supply Chains: The Need for Governance and Legal Frameworks to Achieve Sustainability* (SSRN Scholarly Paper ID 3205452). Social Science Research Network. https://doi.org/10.2139/ssrn.3205452

Szalachowski, P., Reijsbergen, D., Homoliak, I., & Sun, S. (n.d.). *StrongChain: Transparent and Collaborative Proof-of-Work Consensus*. 19.

Treleaven, P., Gendal Brown, R., & Yang, D. (2017). Blockchain Technology in Finance. *Computer*, *50*(9), 14–17. https://doi.org/10.1109/MC.2017.3571047

Vishwakarma, P., Khan, M. Z., & Jain, D. T. (2018). *Cryptocurrency, Security Issues and Upcoming Challenges to Legal Framework in India*. *05*(01), 5.

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, *7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

Werbach, K. (2018). *Trust, but Verify: Why the Blockchain Needs the Law*. https://doi.org/10.15779/Z38H41JM9N

White, G. R. T. (2017). Future applications of blockchain in business and management: A Delphi study. *Strategic Change*, *26*(5), 439–451. https://doi.org/10.1002/jsc.2144

Wong, L.-W., Leong, L.-Y., Hew, J.-J., Tan, G. W.-H., & Ooi, K.-B. (2020). Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs. *International Journal of Information Management*, *52*, 101997. https://doi.org/10.1016/j.ijinfomgt.2019.08.005

Woodside, J. M., Jr, F. K. A., & Giberson, W. (2017). *Blockchain Technology Adoption Status and Strategies*. *26*(2), 30.

Wright, A. (n.d.). *Blockchain and the Law.pdf*. Google Docs. Retrieved 27 December 2021, from https://drive.google.com/file/d/1jfMcmh3zMMlHFLJ5iJqOtLiqPnrk1II6/view?usp=embed_facebook

Wu, B., & Duan, T. (2019). The Application of Blockchain Technology in Financial markets. *Journal of Physics: Conference Series*, *1176*, 042094. https://doi.org/10.1088/1742-6596/1176/4/042094

Xiao, Y., Zhang, N., Li, J., Lou, W., & Hou, Y. T. (n.d.). *Distributed Consensus Protocols and Algorithms*. 31.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NIST IR 8202; p. NIST IR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., & Kang, B. (2019). A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future. *IEEE Access*, *7*, 75845–75872. https://doi.org/10.1109/ACCESS.2019.2917562

Yiannas, F. (2018). A New Era of Food Transparency Powered by Blockchain. *Innovations: Technology, Governance, Globalization*, *12*(1–2), 46–56. https://doi.org/10.1162/inov_a_00266

Youngson, L. M., & Dounas, T. (2021). *Invoice Smart Contracts for Design SMEs*. 2–10. https://doi.org/10.35490/EC3.2021.173

Younus, A. M., & Younus, K. M. (n.d.). *SUPPLY CHAIN USING SMART CONTRACT BLOCKCHAIN TECHNOLOGY IN ORGANIZATIONAL BUSINESS*. 7.

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, *52*(3), 51:1-51:34. https://doi.org/10.1145/3316481

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access*, *8*, 16440–16455. https://doi.org/10.1109/ACCESS.2020.2967218