



## Assignment of master's thesis

<b>Title:</b>	Blockchain Smart Contracts in Public Sector
<b>Student:</b>	Bc. Katarína Krbilová
<b>Supervisor:</b>	Ing. Marek Skotnica
<b>Study program:</b>	Informatics
<b>Branch / specialization:</b>	Managerial Informatics
<b>Department:</b>	Department of Software Engineering
<b>Validity:</b>	until the end of summer semester 2022/2023

### Instructions

Blockchain smart contracts (SC) are an emerging technology that aspires to change the way people interact with the public administration. However, real-world case studies are still missing as the technology remains in a cloud of novelty. This thesis's primary goal is to provide a practical case study of smart contracts applied in the public administration and evaluate its benefits.

- Review blockchain smart contracts and decentralized identity (DiD) in the context of public administration processes.
- Pick a suitable process for digitalization.
- Create an as-is and to-be process and technological architecture.
- Evaluate the benefits and impacts of the to-be state.





**FACULTY  
OF INFORMATION  
TECHNOLOGY  
CTU IN PRAGUE**

Master's thesis

# **Blockchain Smart Contracts in Public Sector**

*Bc. Katarína Krbilová*

Department of Software Engineering  
Supervisor: Ing. Marek Skotnica

May 4, 2022



---

## **Acknowledgements**

Firstly, I want to thank my supervisor for his guidance, patience, constructive feedback and for giving me the opportunity to work on such an intriguing topic. Secondly, I would like to express my gratitude to my family for their love and support throughout my studies. Last but not least, I would like to thank my friends and schoolmates who accompanied me on this journey and always provided high-quality mental support.



---

# Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No.121/2000 Coll., the Copyright Act, as amended, in particular that the Czech Technical University in Prague has the right to conclude a license agreement on the utilization of this thesis as a school work under the provisions of Article 60 (1) of the Act.

In Prague on May 4, 2022

.....

Czech Technical University in Prague

Faculty of Information Technology

© 2022 Katarína Krbilová. All rights reserved.

*This thesis is school work as defined by Copyright Act of the Czech Republic. It has been submitted at Czech Technical University in Prague, Faculty of Information Technology. The thesis is protected by the Copyright Act and its usage without author's permission is prohibited (with exceptions defined by the Copyright Act).*

### **Citation of this thesis**

Krbilová, Katarína. *Blockchain Smart Contracts in Public Sector*. Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2022.



---

# Abstract

Despite living in a digital age with intelligent gadgets simplifying most mundane tasks, some processes remain complicated and burdened with unnecessary administration. It is most visible in the public sector, and the number of existing offices also indicates it. Blockchain is becoming an established technology. Its use cases have extended far beyond financial transactions in recent years, but practical examples of using blockchain in public administrations are still missing. Blockchain smart contracts have the potential to revolutionize how citizens communicate with public offices. The primary purpose of this thesis is to explore the use of smart contracts and decentralized identity in public administration. The theoretical part summarizes the essential concepts of blockchain technology with an emphasis on smart contracts and decentralized identity. Existing uses of blockchain in the public sector are explored. The practical case study analyses the process of registration of a company in Czechia with all administrative steps and proposes its simplification through a smart contract. The impacts of the proposed solution are evaluated.

**Keywords** process digitalization, public sector, blockchain, smart contract, decentralized identity, DasContract

---

# Abstrakt

Napriek životu v digitálnej dobe, keď je väčšina denných povinností zjednodušená inteligentnými zariadeniami, zostávajú niektoré procesy formálne zložité a zaťažené zbytočnou administratívou. Najviditeľnejšie je to v štátnej správe, kde túto skutočnosť indikuje aj vysoký počet existujúcich úradov. Blockchain sa stáva zaužívanou technológiou, ktorej použiteľnosť prekročila hranice finančných transakcií, no praktické príklady jeho využitia v štátnej správe stále chýbajú. Blockchain smart kontrakty majú potenciál zmeniť spôsob komunikácie občanov s úradmi. Hlavným cieľom tejto práce je preskúmať možnosti využitia smart kontraktov a decentralizovanej identity v kontexte štátnej správy. Teoretická časť sa zaoberá najdôležitejšími konceptami blockchainu s dôrazom na smart kontrakty a decentralizovanú identitu. Taktiež skúma existujúce spôsoby využitia blockchainu vo verejnej správe. Praktická časť analyzuje proces registrácie firmy v Českej republike a všetky jeho administratívne kroky. Štúdia prezentuje návrh modelu, ktorý zjednodušuje proces za využitia smart kontraktu a vyhodnocuje dopady a prínosy upraveného modelu.

**Kľúčová slova** digitalizácia procesov, štátna správa, blockchain, smart kontrakt, decentralizovaná identita, DasContract

---

# Contents

<b>Introduction</b>	<b>1</b>
Motivation	1
Objectives	2
Structure	2
<b>1 Review of the Blockchain</b>	<b>3</b>
1.1 Introduction to Blockchain	3
1.1.1 Trust Without Intermediaries	4
1.1.2 Chains, Blocks and Transactions	4
1.1.3 Consensus Mechanisms	5
1.1.4 Main Types of Blockchain	8
1.1.5 Characteristics of Public Blockchain Networks	9
1.1.6 Evolution of the Blockchain	10
1.1.7 Conclusion	11
1.2 Smart Contracts	12
1.2.1 Current Research	12
1.2.2 Introduction to Smart Contracts	12
1.2.3 Smart Contract Platforms	14
1.2.4 Ethereum Smart Contracts	15
1.2.4.1 Programming Languages	15
1.2.4.2 Smart Contract Design	16
1.2.4.3 Oracles	16
1.2.4.4 Accounts and Transaction Execution	17
1.2.5 Limitations of Smart Contracts	19
1.2.5.1 Security	20
1.2.5.2 Expressive Limitations	20
1.2.5.3 Enforceability	20
1.2.6 Conclusion	21
1.3 Blockchain 3.0	21

1.3.1	Decentralized Identity	21
1.3.1.1	Evolution of Identity	22
1.3.1.2	Verifiable Credentials and Zero Knowledge Proofs	22
1.3.2	Decentralized Applications (DApps)	23
1.3.3	Decentralized Autonomous Organizations (DAO)	24
1.3.4	Decentralized Law	26
1.4	Domains That Could Benefit from Blockchain	26
1.5	Conclusion	28
<b>2</b>	<b>Blockchain in Public Sector</b>	<b>29</b>
2.1	State of the Research	29
2.2	Blockchain Use Cases for Public Sector	30
2.3	Countries Adopting the Blockchain	31
2.4	EBSI	33
2.5	Conclusion	33
<b>3</b>	<b>Case Study</b>	<b>35</b>
3.1	Establishment of a Company	35
3.1.1	Choice of the Process for the Case Study	35
3.1.2	Incorporation of a Company in the World	36
3.1.3	State of Digitalization of the Process	38
3.2	Establishment of a Company in Czechia As-is	38
3.2.1	As-is Process Model	39
3.2.2	Signing Memorandum of Association	39
3.2.3	Registration for Trade License	40
3.2.4	Declaration of Integrity	41
3.2.5	Creation of a Bank Account	41
3.2.6	Registration of the Company in the Company Register	41
3.3	To-be Establishment of a Company Using Smart Contract	42
3.3.1	DasContract	43
3.3.2	To-be Model in DasContract	44
3.3.3	Generating the Smart Contract	47
3.3.4	Prerequisites for Adoption of the Model	48
3.4	Conclusion	49
<b>4</b>	<b>Evaluation</b>	<b>51</b>
4.1	Quality Evaluation Framework	51
4.2	Process Evaluation	52
4.2.1	Performance Evaluation	52
4.2.2	Efficiency Evaluation	55
4.2.3	Permissibility Evaluation	56
4.2.4	User Experience	57
4.3	Conclusion	58

<b>Conclusion</b>	<b>59</b>
<b>Bibliography</b>	<b>61</b>
<b>A Acronyms</b>	<b>69</b>
<b>B Figures and Tables</b>	<b>71</b>
<b>C Contents of Enclosed SD Card</b>	<b>75</b>



---

## List of Figures

1.1 Network with an intermediary vs. peer-to-peer network	4
1.2 Simplified bitcoin blockchain	5
1.3 Proof-of-Work vs Proof-of-Stake	7
1.4 Main types of blockchain	9
1.5 Three blockchain generations	11
1.6 Smart contracts created on Ethereum	13
1.7 Smart contract example	13
1.8 Centralized oracle	17
1.9 Structure of Externally Owned Account and of Contract Account	18
1.10 Decentralized application example	24
2.1 Blockchain research disciplines	30
3.1 Countries with the slowest process of registering a company	37
3.2 Countries with the fastest process of registering a company	37
3.3 Simplified model of the current state of registering a company in Czech Republic	39
3.4 Concept architecture of DasContract	43
3.5 To-be model of company registration process in DasContract	46
3.6 Proposal of communication flow between entities	47
B.1 Most cited articles on smart contracts	71
B.2 As-is model of company registration part 1	72
B.3 As-is model of company registration part 2	73
B.4 Data model of the smart contract	74





---

## List of Tables

1.1 Strengths and weaknesses of smart contracts . . . . .	19
3.1 New businesses registered per 1000 people . . . . .	37
4.1 Documents required throughout the company registration process .	53
4.2 Duration of tasks during the company registration . . . . .	54
4.3 Total current costs for company registration . . . . .	56
4.4 Individuals accessing the data throughout the company registra- tion process . . . . .	57
4.5 Key observed parameters . . . . .	58



---

# Introduction

## Motivation

Official websites of the public administration of the Czech Republic list almost 200 types of different public offices. The Czech Republic counts 201 offices of the financial authority and 227 trade licensing offices.<sup>[1]</sup> There are probably hundreds if not thousands of offices of other types. These numbers indicate the incredible complexity of the processes in public administration. The majority of the processes used by citizens require special documents and validations from multiple of these institutions.

An ongoing effort to digitalize communication between citizens and public offices is present, but no significant improvement is visible. Employees in the offices are still performing the same repetitive tasks each time a citizen comes with the most basic request like registering a car, confirming the ownership of a real estate, or registering a company. Prospects for digitalization are not bright as most of the ministry offices do not have a plan to digitalize anything in the upcoming four years.<sup>[2]</sup> Websites for digitalization of the state just underline this as the latest <sup>[1]</sup> announcements published on them are dating to 29th of November 2021 or even to 2019. <sup>[3][4]</sup> Is it possible to find a sustainable way towards digitalization of the public administration with the use of intriguing technology like blockchain?

Blockchain is a widely spread buzzword that everyone came across, most probably in the context of cryptocurrencies as it is their underlying technology. Blockchain technology remains surrounded by critique for its power consumption and lack of scalability but also by optimistic predictions of being omnipresent in the future. Literature mainly offers two viewpoints on this technology. It either focuses on the technical details and challenges or vaguely presents numerous domains where blockchain could bring a great value, public administration being one of them. Unfortunately, practical demonstrations of

---

<sup>1</sup>at the time of writing this thesis

using the blockchain are still lacking, and the scientific literature does not offer enough real-life process case studies.

## Objectives

This thesis aims to research how blockchain is being used to support processes in different domains but mostly in the public administration and to evaluate the possible benefits that smart contracts and decentralized identity could bring. This investigation is supported by a practical case study where the as-is state of a suitable administration process is analyzed. To-be model of the process with the use of smart contracts is proposed. The final evaluation and comparison of the models summarize the impacts and benefits of using a blockchain-based solution in the public domain.

## Structure

This thesis is comprised of two main parts that are structured as follows:

- Theoretical Background
  - Chapter [1](#) presents the fundamental concepts of the blockchain, explains the working of smart contracts and decentralized identity, and stresses the limitations that should be taken into account when using them.
  - Chapter [2](#) summarizes suggestions from literature for the usage of blockchain for public sector and observes state of blockchain projects in the world.
- Practical Case Study
  - Chapter [3](#) compares the process of creating a company in Czechia to the countries with the most successful digitalization of this process. The current state of the company registration process is modeled. To-be model of the company creation process through blockchain smart contract is proposed.
  - Chapter [4](#) evaluates the economic and practical benefits of the proposed solution and lists its impacts on public administration offices.

---

# Review of the Blockchain


Claiming that blockchain is a new technology nearly 15 years after its appearance is incorrect. Blockchain is still mostly known to the public in relation to cryptocurrencies, and the crypto craze continues to grow despite governments trying to regulate its usage and mining. However, blockchain is much more than just cryptocurrencies. Nonetheless, stories of successful implementations in different domains are still lacking, and ambitious, publicly presented projects are not reaching the promised goals.

This chapter introduces blockchain technology and serves as a base for understanding how necessary it is to grasp the limitations of the blockchain and its related concepts. To profit the most from this technology in any project, it is needed to work with these limitations actively.

The first section concentrates on the blockchain architecture. It explains the most popular consensus mechanisms, differences in the recognized types of the blockchain, and their strengths and weaknesses. At the end of the first section, recognized generations of the blockchain are presented. The second part is focused on the concept of smart contracts and summarizes the most interesting platforms and languages. It also describes the working of Ethereum smart contracts that are a foundation for the practical case study. The third chapter explores the most complex of all generations of the blockchain that brought decentralized applications and organizations and the question of decentralized identity.

## 1.1 Introduction to Blockchain

Founder of Institute for Blockchain Studies Melanie Swan anticipates that blockchain is *the seamless embedded economic layer the Web has never had, serving as the technological underlay for payments, decentralized exchange, ...*

 The following sections will cover how the transactions work and how it is possible to ensure trust in a decentralized environment.

### 1.1.1 Trust Without Intermediaries

Most used payment technologies require an intermediary for a transaction to happen. One needs a bank account to pay using a card on the internet, but the bank is often not the only intermediary. Buyers are usually redirected to a payment gate that has either interest rates on payments or demands a regular fee from the vendor so they can embed it to their online store. The same happens in the more offline world when paying through a terminal. There is an acquirer that processes the payment with a set commission.

How does blockchain allow transactions without any intermediaries? Blockchain is a decentralized database that is replicated over all nodes of a peer-to-peer network. [6] As depicted on Figure 1.1, in a peer-to-peer network, all nodes are equal. The trust is given by the fact that every node stores the chain of blocks that contain information about the transactions that have happened. It is easy to verify whether all other nodes are aware of some transaction or not.

Nodes on the network are, in fact, "users". Each node has an address and a public and a private key which is used to sign transactions. Everyone on the network can track down the origin of the money sent in a transaction which creates great transparency. [6] For the bitcoin network, the content of the blocks and how they are chained can be inspected through blockchain explorer, e.g. [www.blockchain.com/explorer](http://www.blockchain.com/explorer).

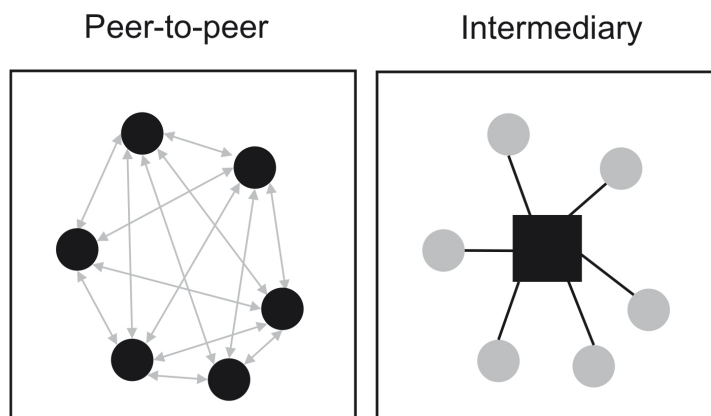


Figure 1.1: Network with an intermediary vs. peer-to-peer network [7]

### 1.1.2 Chains, Blocks and Transactions

As its name suggests, blockchain is a chain of blocks that are tied together. The first block of the chain is often referred to as the *genesis block*. Blocks consist of a header and a body that contains a list of transactions. Once

the block is added to the chain, transactions are validated. Before the block is added, they have a pending status. Blocks are tied together using cryptographic functions. Each header contains a hash that is calculated based on the previous block. [8] This structure is illustrated by Figure 1.2. It is impossible to modify a block in the middle of the chain since that would mean changing all of its successors. Information about a validated transaction cannot be manipulated. Merchants accepting blockchain tokens as a form of payment consider the transaction as validated once their block has six or more blocks on the top of it. The amount of computing power needed to change six blocks makes the reversion unfeasible. [6]

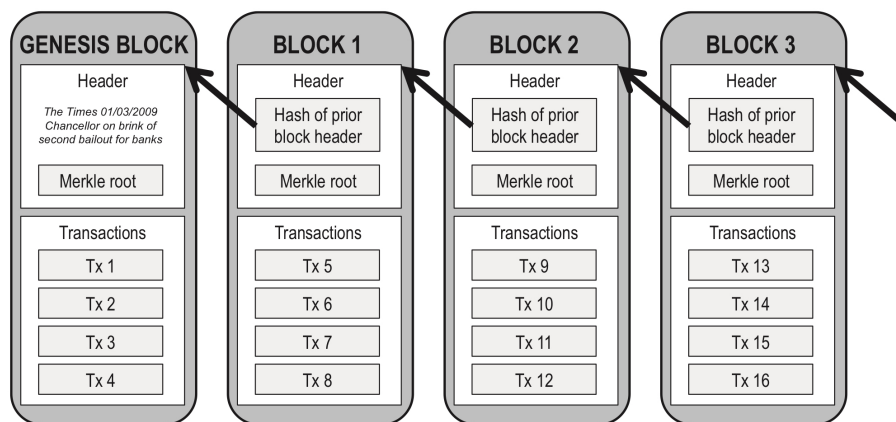


Figure 1.2: Simplified bitcoin blockchain [7]

Adding a new block to the blockchain must be validated by the majority of the network. That prevents the double-spending problem, which occurs when a node attempts to spend the same token twice for two transactions. The record of transactions will always prove that the node only had one token to spend, and the block with the second transaction will be rejected by the network. One entity would need to own more than 50% of the network to manipulate validating the transactions. [6] How the nodes reach the agreement to add a block is called the consensus mechanism. A brief overview of the different consensus mechanisms will follow in the next section.

### 1.1.3 Consensus Mechanisms

In a distributed system, the whole network needs to acknowledge its state. It is a consensus of at least 51% of the users that approve of the global state of the network. Consensus mechanisms are not a novelty emerging with the blockchain. They are commonly used to establish a state between application servers or parts of enterprise infrastructures. [9] Consensus algorithms are used

in all kinds of scenarios where multiple entities need to maintain a common state of information or a data item.

Multiple nodes can attempt to add their block to the chain at once. That means the local state of the blockchain that nodes hold can differ from the global state of the chain. This is why the network needs to take a union of all the local states and decide what the global state will be. The existence of multiple possible branches of the chain is called a fork. [10]

Consensus mechanisms are also prevention to the 51% attack when the malicious entity becomes the owner of more than 51% of nodes and can compromise the data on the network. Mechanisms solve this problem in different ways, and with the blockchain, new types are being developed and tested. Besides being a security element, the logic of the consensus mechanism determines the conditions under which a new block is added. Creating a new block is expensive, which prevents nodes from creating a whole chain of blocks and presenting them as the "right chain".

**Proof-of-Work** is currently being used by both biggest cryptocurrencies - Ethereum and Bitcoin. In a network using Proof-of-Work exist miner nodes that collect transactions and then form a block from them. Each new block is a problem to be solved. This problem is very difficult, but the verification of the solution is not. Whoever is first to find a solution to the problem gets rewarded with a part of the token hence the activity of solving the puzzle is called "mining". The downsides of this mechanism are very high energy costs and long transaction processing. [9] In case branching of the chain happens, the Bitcoin network chooses the deepest branch as the main branch. Ethereum network selects the heaviest subtree as the main branch. [10]

**Proof-of-Stake** Main idea of the Proof-of-Stake mechanism is that to become a validator who can add new blocks to the chain, one must send a transaction with a deposit (*stake*) of a certain value. Validators get randomly chosen to create a new block. They get rewarded after confirming transactions, and their reward corresponds to the stake they initially entered with. If a validator attempts to validate a fraudulent transaction, he will lose his stake. This system tends to get centralized as the more you own, the more often you are chosen to validate transactions and the more you get. To prevent the centralization, different modifications to this mechanism were proposed, e.g. Casper mechanism of "decided punishment", where users can vote to erase the deposit of a person who attempted a faulty transaction. Ethereum is planning a transition from Proof-of-Work to Proof-of-Stake in June 2022. [11]

**Delegated Proof-of-Stake** In this mechanism, users choose *witnesses* and *delegates* in elections. Users' vote is relative to how much they stake.



Witnesses are able to collect transactions and form new blocks. Delegates are registered in the genesis block, and they are allowed to vote on changes on the chain. In case a node acts suspiciously, users are allowed to remove their vote. This mechanism can lead toward centralization over time as the votes are dependent on the assets nodes own. [12]

**Ripple** is using subnetworks that are trusted by other participants of the network. The consensus algorithm works in rounds. At the beginning of each round, all nodes announce lists of transactions they have collected and consider valid. Each node votes on the validity of these lists of transactions. In the last round of voting, a new block is added if an accordance of 80% is reached. [10]

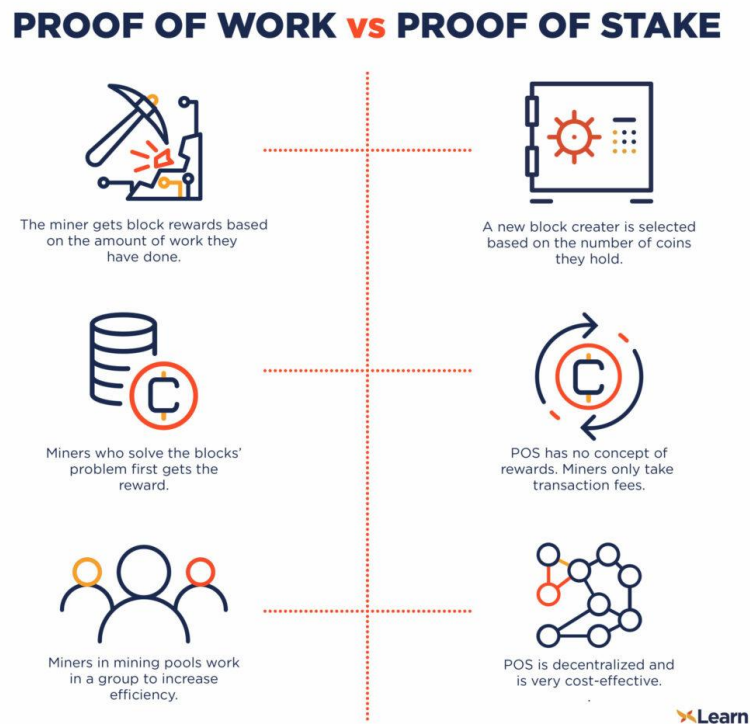


Figure 1.3: Proof-of-Work vs Proof-of-Stake [13]

With ongoing research, many new consensus algorithms emerge. Their authors attempt to improve the most pressing problems, such as scalability and power consumption. This section listed some of the most known mechanisms. A brief comparison of the Proof-of-Work and the Proof-of-Stake is depicted by Figure 1.3. [10] offers an interesting comparison and evaluation of some of the newest consensus algorithms and stresses the importance of choosing the right mechanism for projects.

### 1.1.4 Main Types of Blockchain

Literature differs in the classification of types of the blockchain. Some uses the terms permissioned and private as synonyms. Other goes into more detail and distinguishes subtleties such as what kinds of rights users have or how many nodes own the majority of the network. Based on sources [14], [15], [12] two main classifications of the blockchain can be recognized. Categorization based on the permissions that users have, and categorization based on the level of centralization of the network.

Two types of blockchain in regards to permissions:

- *permissionless* - all users are equal, and there are no conditions upon entering or leaving the network. All nodes have the same rights and opportunities to participate in the voting. Code of permissionless blockchains is often open-source, and besides being a user, one can contribute as a community member.
- *permissioned* - nodes in the network can have different roles and rights. Entering the network may be conditioned and can require proving identity.

Three types of blockchain, based on the level of centralization:

- *public* - large distributed network with a native cryptocurrency or a token that is available to anyone who wants to join, it is non-restrictive. It is fully decentralized, and no trust between the nodes is required, which means that little information about the users or owners of the nodes is needed. An example of a public blockchain is Bitcoin.
- *private* - also known as distributed ledger technology (DLT) is usually a smaller closed network without tokens and has a strict entering policy for new users. The network is monitored by a central authority, and write and read permissions may be restricted. Private blockchain solutions are mostly used within the scope of a single organization.
- *hybrid* - also known as a partially centralized or consortium network, has a set of pre-elected voting nodes that the participants choose upfront. Hybrid blockchain networks are often used for inter-enterprise solutions.

Each type of blockchain targets different needs, so the one suitable for a global service will not be ideal for a cross-enterprise supply chain planning solution. [16] sums up the most important advantages and disadvantages of the different types in Figure 1.4. It is clear that private and hybrid blockchains offer good performance, but transparency is the cost. For document validation, public blockchains are the most suitable.

	<b>Public</b> (permissionless)	<b>Private</b> (permissioned)	<b>Hybrid</b>
ADVANTAGES	+ Independence + Transparency + Trust	+ Access control + Performance	+ Access control + Performance + Scalability
DISADVANTAGES	- Performance - Scalability - Security	- Trust - Auditability	- Transparency - Upgrading
USE CASES	■ Cryptocurrency ■ Document validation	■ Supply chain ■ Asset ownership	■ Medical records ■ Real estate ■ Supply chain

Figure 1.4: Main types of blockchain [16]

### 1.1.5 Characteristics of Public Blockchain Networks

As described in the previous section, existing types of blockchain have different properties and specific scope of use. Public blockchain networks share some key characteristics that ensure the good usability of the technology. Most of these characteristics can be considered advantageous. Following list is a compilation of key attributes by [6] and [8]:

- *integrity of the network* - transactions are protected by hashing the key content of the previous blocks
- *privacy* - only the recipient himself can read the message of the transaction
- *distribution of computing power* - the network is resilient and can handle when one or multiple nodes are temporarily unavailable because all nodes of the network store the same data. 50% of the nodes would need to drop out at once, so the network or the transactions could be compromised. Users of the network are so diversified that they have no motivation to allow such a situation.
- *decentralization* - there is no central authority, no intermediaries and no entity that could manipulate the network
- *democracy* - no entity or node is more powerful than the other, all nodes can participate equally, and the consensus mechanism ensures a consistent state of the ledger
- *immutability* - transaction that is once recorded cannot be modified and can be verified easily by any user of the network

- *auditability and transparency* - is directly related to the immutability and the distribution of the computing power. The network stores an immutable history of all transactions that happened. The origin of any assets sent in a transaction is always traceable, and ownership cannot be questioned.
- *forgery resistance and reputation* - any attempt of forgery is visible. Since transactions are public, it can be seen which addresses/users interacted in them. Thanks to this transparency, it is easy to uncover who can be trusted and who not. The activity of the nodes on the network determines their reputation over time. If someone has many unfulfilled smart contracts, it will be visible, and it is the user's own consideration if they want to start a business with such a counterpart.
- *increased transaction speed* - removing intermediaries and international settlements enables much faster transaction processing

Based on the attributes mentioned above, it is unnegotiable that blockchain is an intriguing technology with a lot of potential and a wide range of use. Characteristics that could be considered disadvantageous are mainly the transparency and the democracy, but these are addressed by private or hybrid blockchains. What can be built on top of these characteristics is discussed in the following sections.

### 1.1.6 Evolution of the Blockchain

Blockchain is still an evolving technology that has many challenges to overcome. However, just like there was the TCP/IP protocol at the beginning of the internet, we can already see that blockchain technology is just a foundation for more. The literature is already distinguishing three generations of the blockchain. [5]

**Blockchain 1.0** - Bitcoin is the widely known representative of the first generation of the blockchain. Its primary purpose was to process transactions in a decentralized manner and store the information about them in a public ledger. It quickly became a new form of digital payment system that complemented the existing monetary system. Most of the first generation blockchains were written in C++ and use Proof-of-Work as the consensus mechanism which results in a enormous energy consumption. [17]

**Blockchain 2.0** - The second generation evolved to improve energy consumption and open the doors to new usages of the public ledger. Developers understood that it was not just transactions that could be recorded on the blockchain. That is how smart contracts were born. They provided a plethora of new usages as it suddenly became possible to capture logic

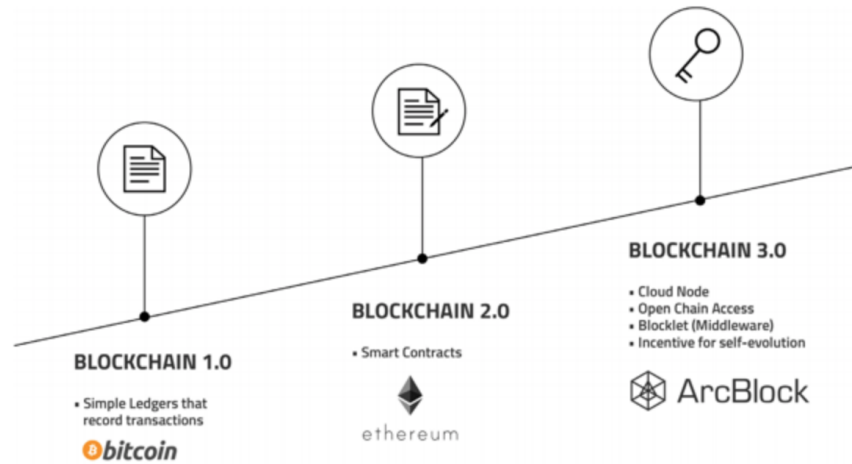


Figure 1.5: Three blockchain generations [17]

and processes on the blockchain. The first representative of the second generation was Ethereum. The second generation did not reach its potential in reducing energy consumption.

**Blockchain 3.0** - Blockchains of the third generation are trying to reach better scalability and they usually use different consensus mechanisms from Proof-of-Work. Additionally, they build on the smart contracts, and add concepts of decentralized applications (dApps) or decentralized organizations (DAO) that are universal enough to be applied in the public sector, healthcare, law or other domains. An interesting representative of this generation is Cardano. ArcBlock depicted in Figure 1.5 is also worth mentioning as a prospective decentralized developer platform that facilitates the development of dApps.

Blockchain 3.0 might not be the last generation yet. The blockchain community argues that new generations may arise from combining blockchain with artificial intelligence or the internet of things. [17] Just as it was impossible to predict what variety of layers and applications would once be built on top of the TCP/IP protocol, we can only guess what the blockchain still has to offer.

### 1.1.7 Conclusion

This chapter introduced the underlying concepts of blockchain technology and explained its relation to cryptography. The most known consensus mechanisms were presented, and a classification of the blockchain types was proposed. Essential characteristics of the blockchain networks were described, and a distinction between blockchain generations was made. Upcoming chap-

ters will address concepts added in the second and third generations of the blockchain.

### 1.2 Smart Contracts

Besides recording transactions on the network, blocks on the chain can contain executable code, also called *smart contracts*. The use of these contracts is very flexible as they are the main component for dApps and DAOs, but this will be addressed in later chapters. This chapter aims to explain how smart contracts work, what are the most popular smart contract platforms with a close up on the Ethereum smart contracts and highlight the main limitations of using smart contracts for real-world processes.

#### 1.2.1 Current Research

An extensive literature review for the topic of smart contracts by [18] uncovered six main strands of research that were peaking at the beginning of 2021. Aligned with the objectives of this thesis 3 strands are interesting:

- blockchain smart contracts for the disruption of existing processes and industries
- potentials and challenges of smart contracts
- smart contracts and the law

#### 1.2.2 Introduction to Smart Contracts

The idea of contracts between two parties without an intermediary was first described a long time before the first usage of the term blockchain by Nick Szabo when he proposed a computerized transaction protocol. He eliminated the need for trust between two exchanging parties. [6] First blockchain network that allowed the creation of smart contracts was Ethereum in late 2013. Stable growth of created smart contracts on the Ethereum platform can be observed from Figure 1.6 which underlines prospects of this technology.

Smart contracts enhance transactions with logic that can represent a set of commitments, a flow of a process or a formulation of rules. Smart contracts are incredibly powerful because they can use the computing power of the whole network. They have their own storage that can store variables used during computation, but otherwise, they do not store any off-chain information. However, they can access data stored elsewhere on the network. The execution of smart contracts is always triggered by a transaction, and the result of such execution is immutable. Once a smart contract becomes a part of a validated block, the logic can not be changed, but it is possible to build

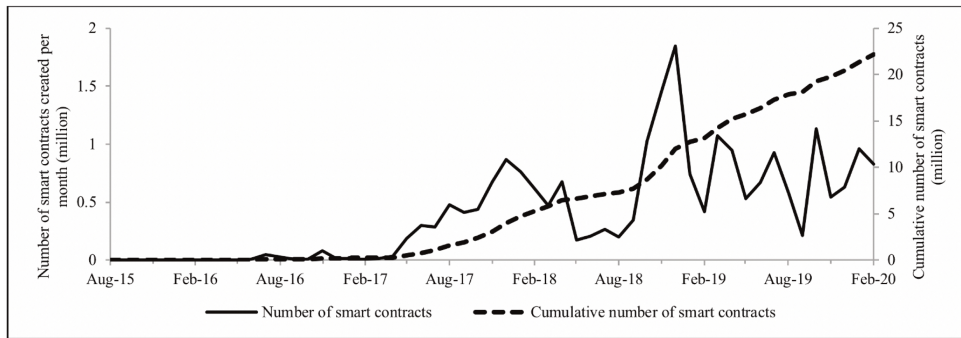


Figure 1.6: Smart contracts created on Ethereum (2015-2020) [18]

on the top of this logic in the next block. The auditability of the chain ensures that the evolution of the contract logic is transparent to all users of the network.

A simple example of using a smart contract for a transaction between buyer and seller can be seen from Figure 1.7. The final state of the transaction is decided based on checking the conditions predefined in the smart contract. In practice, once a confirmation of the payment is received by the smart contract, or the smart contract is able to retrieve this confirmation from some external source, the transaction is completed with status sold. Smart contract can have an included condition to cancel the transaction in case the payment is not received within a certain time frame.

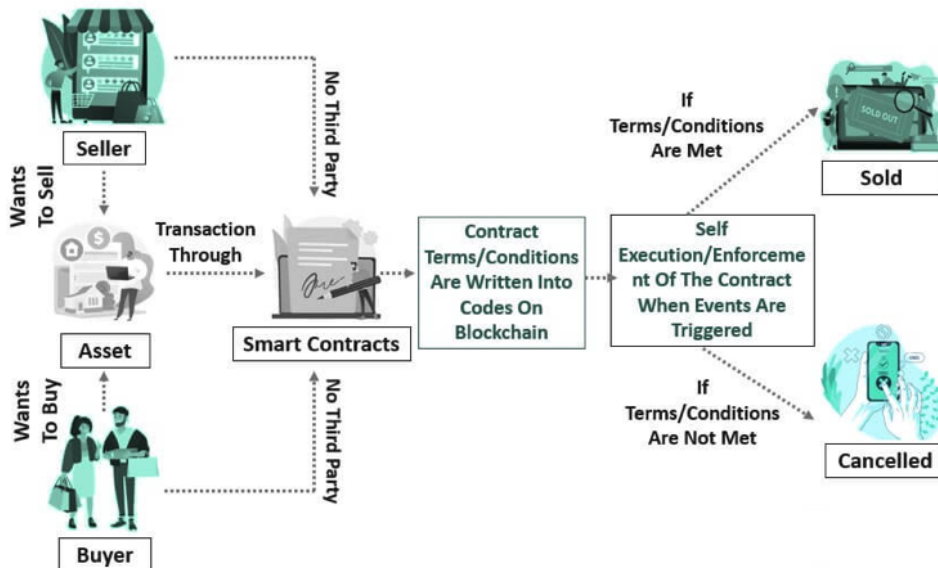


Figure 1.7: Smart contract example [19]

Multiple parties can participate in the fulfilment of a smart contract. Payments, values or assets are only exchanged when all conditions coded in the smart contract are met. This is very practical as a form of withholding assets instead of having to store them at an intermediary such as a court or notary.

[5] recognizes three crucial aspects of smart contracts:

- *autonomy* - once a transaction initiates the execution of a smart contract, there is no more need for communication between the initiating agent and the smart contract
- *self-sufficiency* - smart contracts are self-sufficient in terms of handling assets and resources
- *decentralization* - a smart contract is distributed over the nodes of the network that removes the risk emerging from having a single centralized server

These three attributes ensure that the smart contract's code is executed without any delay once the required conditions are met. Smart contracts help avoid non-compliant behaviour and mitigate risks related to frauds, server failures or unauthorized changes.

### 1.2.3 Smart Contract Platforms

The nature of the blockchain comes with support for smart contracts. However, blockchains of the first generation were primarily designed to support only financial transactions and did not offer enough tools and concepts to build smart contracts. The notion of accounts and distributed contracts with more complex operations was first fully supported by Ethereum. [7] Since then, a multitude of other smart contract platforms have been introduced. Some of the most interesting ones are:

**Polkadot** is specific for its ability to run multiple chains inside the blockchain and, therefore, process transactions much faster. [20]

**Solana** attempted to bring scalability to smart contracts, and with its Proof-of-History consensus mechanism, can reach an incredible transaction processing speed of 65 thousand transactions per second. Smart contracts for Solana can be written in C or in rust, making it easily accessible to developers without the need to learn a new language. [20]

**Cardano** - introduced the support for smart contracts in September 2021 with their development platform called Plutus. Cardano is considered a very promising platform that could challenge Ethereum's first place, but the quantity of deployed smart contracts remains low. [21]



**Hyperledger** - offers smart contracts for private blockchains. They are run in a Docker container and can be written in Java or Go. [22]

When choosing a smart contract platform, multiple attributes should be considered:

- *execution environment* - some of the platforms use the Ethereum Virtual Machine (EVM) as the execution environment, others like Solana built their own environment, which gives them the independence from the roadmap of Ethereum
- *application of smart contracts* - not all platforms offer the same complexity for smart contracts application
- *supported languages* - smart contracts can be written in a multitude of languages. While Solana supports C or rust, Ethereum supports Ethereum-specific languages like Solidity or Serpent. The working of Ethereum smart contracts will be covered by the following section.
- *permission(less)* - Ethereum, Solana or Polkadot are public smart contract platforms while Hyperledger offers smart contracts for smaller permissioned networks [22]

### 1.2.4 Ethereum Smart Contracts

Unlike Bitcoin, which was primarily designed for financial transactions, Ethereum was intended as a distributed platform for running applications from the beginning. The developers pay for using this distributed computing power to run their applications on Ethereum, which is advantageous as they do not need to design their own blockchain. [7] This section will concentrate on smart contract design and how they can be run through transactions.

#### 1.2.4.1 Programming Languages

Multiple languages for creating Ethereum smart contracts are available. It is mostly high-level languages that are primarily designed for Ethereum, but tools to compile them for other networks also exist already. Some of the most used languages are:

**Solidity** is a procedural language with Java-like or C++ like syntax. It is currently the most heavily used language for smart contracts.

**Vyper** is a Python-like language. It does not offer the same flexibility as Solidity, but it represents a form of bugs prevention for developers as a limited range of functions is available to them.

**Serpent** is a procedural Python-like language. [23]

### 1.2.4.2 Smart Contract Design

Ethereum smart contracts can contain custom operations and validations of any complexity. They can store variables and detect changes in the stored data. The execution of a smart contract can only be triggered by a transaction, so the originator is always known. Such a transaction can be sent by a user as well as by another smart contract. The result of running a smart contract must always be deterministic. It can not happen that nodes over the network would have different results of running a smart contract. [23]

The smart contract code is compiled to bytecode that runs on an EVM. Running a smart contract on the distributed computing network has its cost. In Ethereum, the cost is paid in ether, also called gas. The purpose is to prevent malicious contracts containing infinite loops or introducing bugs into the network and use all its computing capacity. Since the smart contracts are executed on all nodes in parallel, the costs for execution can be high. The cost itself is determined by the compiler, and each instruction used in the contract has a price. [7]

When composing a smart contract, the resources need to be used wisely due to the cost of all operations. Storing data costs gas as well. Storage "on the chain" is mainly used to communicate the state of the contract or the results of a computation. Variables used locally within functions do not cost gas. When it comes to functions available in Solidity, multiple types exist. Internal functions can only be called by the smart contract itself, while external ones form the contract's interface that others can use to communicate with the contract. Other commonly used functions are view functions and events. View functions do not modify the contract, they only serve to retrieve data. Events work on the standard publisher-subscriber principle, and usually, it is external applications that retrieve them. Solidity also provides means for error handling as asserts and reverting functions. [23]

### 1.2.4.3 Oracles

As was previously mentioned, smart contract can also communicate with other sources within the network to retrieve external data. These sources are called oracles and ideally, they should also operate in a decentralized manner to be trustless. Unfortunately, it is not always easy to assure that. Oracles bring a hint of centralization to Ethereum and can represent the single point of failure if they are not properly secured. Decentralized oracles can be built with Chainlink and are independently retrieving data from an off-chain source and aggregating it to reach a consensus on the value that will be made available to the users of the network. [24]

Oracles collect data from off-chain sources and transfer it onto the chain with a signed message. Oracles make the data available to other smart contracts by putting them in the smart contract storage of their own. Other

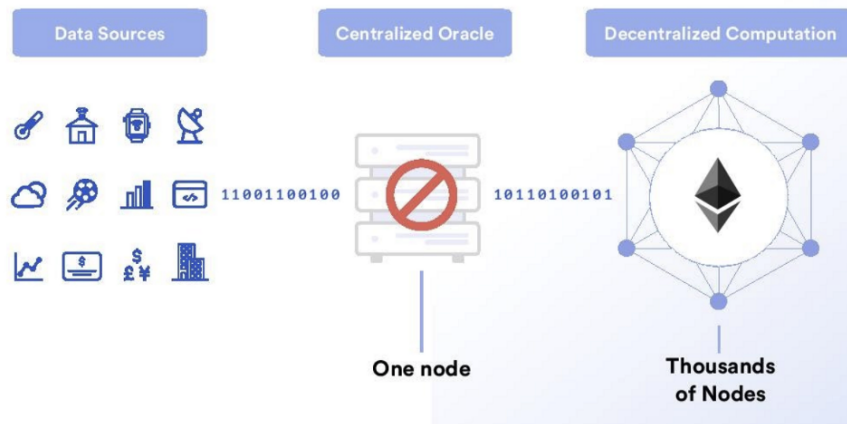


Figure 1.8: Centralized oracle can be a weak point of the whole network [24]

contracts can retrieve the data by viewing the content of this storage or simply by sending a transaction. Oracles ensure that all nodes of the network retrieve the same data. This would not be the case if nodes themselves were calling some external API since the information could change over time. Oracles record the information on the blockchain, and all users receive the same value. They are considered to be the "middleware" of the blockchain. [25]

Oracles can be set up in three different ways:

- *immediate read* - this type is used when other users query information on a just-in-time basis, mostly for verifications of e.g. age, reached degree, etc. This means that details do not have to be stored and a simple answer yes/no or a hash of a certificate is enough.
- *publish-subscribe* - oracle provides a broadcast service with a defined frequency of updates, it works similarly to RSS feeds. On-chain smart contracts are able to poll the changes of the data.
- *request-response* - is probably the most challenging as it is used when large amounts of data need to be stored somewhere, but users retrieve only small parts of them at a time. This type requires multiple on-chain smart contracts and an off-chain infrastructure that is able to retrieve incoming requests. [23]

#### 1.2.4.4 Accounts and Transaction Execution

At this point, it is clear what smart contracts do, what they are composed of, and how they can access off-chain data, but how exactly do the transactions initiate the execution of the smart contract? As previously mentioned, smart contracts are executed on a globally accessible virtual machine EVM. Transactions are signed data packages that can contain a message with instructions

## 1. REVIEW OF THE BLOCKCHAIN

---

for the smart contract. Transactions are always sent by an account and the network distinguishes two types of accounts:

**EOA** - externally owned accounts - are accounts controlled by a private key, and only they can create contract accounts. They have a public address and can hold ethers.

**CA** - contract accounts - hold the smart contract's code, they have their own ether balance and can have their own storage that is pointing to the EVM storage. They can read and write on the blockchain and communicate with other contracts using messages. Their address is derived from the public address of the creating EOA. [26]

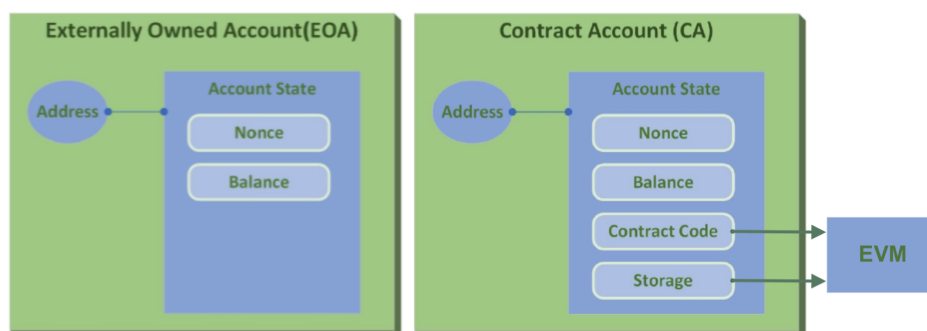


Figure 1.9: Structure of Externally Owned Account and of Contract Account [26]

Just like accounts have their structure that can be seen from Figure 1.9, transactions also have a structure and attributes that need to be predefined:

- *nonce* - is a number issued by sender EOA that is used to prevent executing the content of the message twice
- *gas limit* - as running a smart contract consumes gas. This is the maximal gas that can be spent when executing the transaction. Unspent gas is sent back to the sender. However, if the limit is not large enough, execution might consume all the gas without finishing, and there is no way of a rollback, so the gas is lost.
- *gas price* - the price of one unit of gas that the sender is willing to pay, it usually depends on the previous block
- *recipient* - destination address
- *sender* - originator address
- *value* - amount of ether to be sent to the destination

- *data* - data payload usually of a size to store variables that are being sent to the smart contract [23]

### 1.2.5 Limitations of Smart Contracts

Smart contracts are a promising technology, but their potential can only be used when their limitations are fully understood. It was also probably due to misconceptions about smart contracts and false expectations that many blockchain projects announced for 2021 stopped. Tech leaders did not dare to introduce solutions on public blockchains for enterprise landscapes, and ambitious projects like EBSI<sup>2</sup> were not progressing fast. [27]

A deeper understanding of where the capabilities of the blockchain technology end is lacking. Misconceptions about smart contracts probably appeared due to oversimplified explanations of their working. The following table summarizes the advantageous and disadvantageous attributes of smart contracts. Some are classified as ambivalent because it strongly depends on the point of view and the way of using the smart contract, whether the attribute is positive or negative. Some of these attributes are addressed more in detail in the following subsections.

Advantages	Disadvantages	Ambivalent
Reduction of risk of human error	Smart contracts do not copy real-world human language contracts 1:1	Once in a block on the chain, smart contract can not be changed
Reduction of delays and expenses for normal contracts or transactions	Decentralization is endangered by oracles on the network	Smart contracts always behave the same way
Smart contracts can serve as templates and be reused based on the use case	Smart contracts need to be integrated with other components like interfaces	Security of the contract is in the hands of the developer
Evolution of the smart contract can be tracked thanks to the blockchain	Handling confidential information within a public blockchain is a challenge	
Smart contracts remove the need for intermediaries	When a bug is found in a smart contract, it is a vulnerability for the whole network	

Table 1.1: Strengths and weaknesses of smart contracts

<sup>2</sup>European Blockchain Services Infrastructure

### 1.2.5.1 Security

Security of the smart contracts lies fully within the hands of their creator. This can represent a risk because if a bug is found in a contract that is already deployed on a chain, it can not be fixed. The developer can release a corrected version of the smart contract. However, firstly, he will need to pay again, and secondly, no one will prevent participants of the network from using the previous incorrect version. Fortunately multiple automated tools like *Securify* [28] or *Oyente* [29] that are specifically designed to mark possible bugs in smart contracts are already available.

Besides bugs that smart contracts can contain, the confidentiality of the data and the security of individuals may also be at risk. [30] Transparency is a very questionable attribute of the blockchain as it is both the biggest strength and weakness of public blockchains. Handling confidential data within a public blockchain remains a difficulty. One solution would be, to always use data encryption, but also the concept of decentralized identity and verifiable credentials could help solve this problem. It will be covered in the following sections.

Contacting external services from a smart contract also represents a security risk. As depicted already in the chapter about oracles, retrieving external information is a challenge. This can be solved by decentralized oracles that put the data on the chain themselves instead of the smart contracts needing to retrieve them. Nonetheless, the issue with the centralization remains because even if the oracle itself is decentralized, the source where it retrieves the information is not, and we must trust it. [30]

### 1.2.5.2 Expressive Limitations

An essential challenge of smart contracts is how to relate them to real-world contracts. Smart contracts have limited expressive capabilities, and they can not fully replace human language contracts. This problem can be addressed by using the DEMO methodology that proves to be suitable to capture nuances of human language thanks to ontologies, as was demonstrated by [31] in the process of applying for a mortgage. Ontologies and BPMN are combined in the DasContract modeling language that will be used in the case study and explained into more detail there.

### 1.2.5.3 Enforceability

Many use cases for smart contracts are trying to profit from the logic encoded in them and only exchange assets when predefined conditions are met. The catch of these use cases is that they all suppose that these assets are on the chain. Financial assets can be on the chain but only in the form of a cryptocurrency, and the participating parties need to agree with that. A legal infrastructure needs to be provided for other assets to be recorded on the

blockchain. Until assets or smart contracts on the network are recognized as full equivalents of old offline documents like birth certificates, licenses, and diplomas, the applicability of the smart contracts will remain limited. [32]

### 1.2.6 Conclusion

This chapter explained the potential of the smart contracts together with how they work and what are the different platforms that support them. It further concentrated on the design and working of Ethereum smart contracts with detail on how the transactions are executed and how smart contracts retrieve external data. All of this will be applied in the solution proposed by the case study. Last but not least, the limitations of the smart contracts were discussed.

## 1.3 Blockchain 3.0

Smart contracts explained in the previous chapter are just building blocks that can be put together to create something bigger and more complex, thanks to their ability to communicate with each other. When adding other layers to the smart contract, a decentralized application can be created. Combining multiple smart contracts can lead to a definition of processes in a company, and this is referred to as Decentralized Autonomous Organization (DAO). Besides dApps and DAOs, attempts to structure even more complex constructs using the blockchain exist. These initiatives are trying to construct whole decentralized nations and jurisdictions. All of these applications are very promising, but the privacy of personal data needs to be handled. This could be solved through decentralized identity. The aim of this chapter is to explain the above-mentioned concepts in further detail.

### 1.3.1 Decentralized Identity

The internet allowed connecting people, businesses, and entities on a global scale. Access to information or data of any kind is almost unlimited. Nevertheless, any life-changing technology has its dark sides. First adopters of the internet did not realize their information would become a tradable asset of the network. Nowadays, users are warier of the tech giants trying to accumulate data about them for their own profit, but the data remains a hostage of these companies. [5] We create accounts with fake names and random credentials, but in the end, it all comes down to whether some algorithm is smart enough to identify us anyway. This could change thanks to the decentralized identity. Future generations could become rightful owners of all their data.

### 1.3.1.1 Evolution of Identity

The motivation for an identity where only the owner truly decides about the data related to his identity is clear. Such identity is also called self-sovereign. When interacting in the digital space, we always have an identity. Multiple types of digital identities exist based on who is the owner of the data:

- *centralized identity* - administrative control by a single authority, this authority can be a provider of a web page as well as a government that issues ID cards
- *federated identity* - multiple authorities form a federation that accepts the same universal identity
- *user-centric identity* - multiple authorities accepting and integrating the same identity without being a federation. Examples of such are OpenID or OAuth. Unfortunately, these are providers that can be regarded as centralized authorities.
- *self-sovereign identity* - users have full control over their identity and over the information that gets published or shared. The advantage is that it is a lifetime portable identity, so even with a change of name, gender, or any other key data, the entity is able to retain the same digital identity [33]

A decentralized identifier (DID) is a key step towards an independent self-sovereign identity. DID enables individuals to interact with services provided by other entities. An individual can have multiple DIDs, and he can choose which specific identifier will be visible to the other entity when using their service. *A DID itself says nothing about its owner since it is just an identifier, it is not an identity* [34]. The next section will explain the technological foundation for decentralized identity.

### 1.3.1.2 Verifiable Credentials and Zero Knowledge Proofs

Verifiable credentials are the underlying technology for the decentralized identity. They are based on zero-knowledge proofs that are a cryptographic method to prove the ownership of information without revealing its content. Zero knowledge proofs can work in two ways:

- *interactive* - prover exchanges messages with the verifier
- *non-interactive* - prover issues a proof that can be verified, so called verifiable credentials [35]

When a prover issues credentials for an individual, they can then selectively give access to this data to other entities. The information does not need to



be disclosed. An individual can only share a claim that he matches a certain rule or a requirement. A simple example is getting asked for age in a bar. The bartender does not need to know your birth date or your address. He only needs to know whether you are older than 18 years, so why should you give him your ID card with all the information? [36]

This opens the possibility of implementing whole business flows without sharing or copying sensitive information. [35] Self-sovereign identity would be managed by its owner, and they could identify themselves to different entities with the chosen identity. They would no longer need any third party to validate an aspect of their identity, be it a driver's license or a reached degree. [34]

A practical example of using the notion of decentralized identity and verifiable credentials for the use case of European elections was presented in [37]. Voters would register for voting and gain access to the elections. After the elections, the smart contract would automatically assign verifiable credentials to the winners of the elections based on the number of votes. These credentials would prove their role as newly elected officers.

### 1.3.2 Decentralized Applications (DApps)

Sometimes literature does not distinguish between a deployed smart contract and a decentralized application, but in this chapter, dApp will always represent something more complex than just one singular smart contract. DApps are applications that work over the whole blockchain network and are based on smart contracts where the logic of their working can be defined. They can have almost the form of a regular three-tier application, blockchain being its database, the smart contract being the application layer, and account being the user interface, or there can be a real mobile or web user interface connected to it as well. [38]

Decentralized applications are open-source, and since they run in a distributed manner, no central server or authority is controlling them. The risks of downtime of such applications are close to zero since they run on all nodes, and it does not matter if one node is temporarily unavailable. Decentralized applications remove the single point of failure which is usually the server that can be targeted by hackers. A library of dApps works just like any other application store, and the user can install any application. So far, it sounds very positive, but dApps come with disadvantages as well. Most of them root in the blockchain technology itself, so similarly to smart contracts, dApps can be difficult to scale and their modification, once deployed, is impossible. Creating an interface easily comprehensible for everyone can also be a challenge since a regular user will not know how to navigate in the code of a smart contract to understand what it does. [39]

A great use case for a dApp is a supply chain where multiple vendors and partners are involved. A blockchain node could be set up at each of these

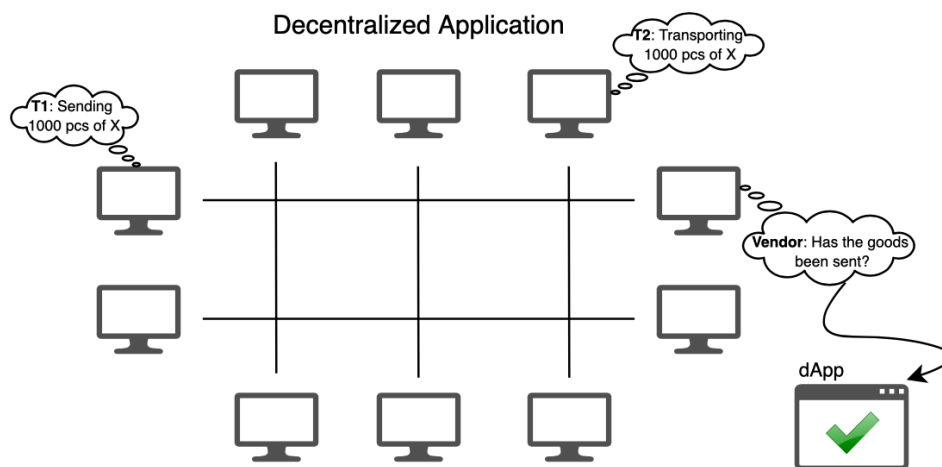


Figure 1.10: Decentralized application example

partners so they could share data about their stocks or the logistics. Each participant would be able to access an interface that would allow him to store, retrieve or verify data on the blockchain. Information about the manufactured goods could be easily uploaded onto the blockchain and later enriched with the data about the transport. Vendors would be able to track ordered or sent goods in the application, and no one could tamper with the data and later claim that they have received fewer goods than the other partner sent. [8]

### 1.3.3 Decentralized Autonomous Organizations (DAO)

Decentralized autonomous organizations are a form of autonomous organizations deployed as smart contracts. The rules describing the organization's coordination and governance are encoded in the smart contract. This makes them incorruptible and publicly auditable. Other key characteristics are that DAOs enable the stakeholders to coordinate online, and the rules for communication can also be defined. There is complete independence of any central authority, and the execution of the rules is without anyone's interference. These attributes are a great base for democratic control of the organization. [40]

The first implementational proposal of DAO was presented in [41]. The author built a smart contract in Solidity deployable on Ethereum, which allowed participants to retain direct real-time control over their funds in the DAO. In the creation phase, voting and ownership rights are assigned to a person who sends funds in ether to the DAO's smart contract. These rights have a form of a freely transferable token after the creation phase ends. The contract can require a certain amount to be raised, and if the amount is not reached within

a given time frame, submitted funds are returned to their owners. DAO itself can not build or develop a product. This is done by a *contractor* that is chosen by DAO. Any DAO token holder can submit their proposal to become a contractor, and other members vote on this proposal. The vote of each member corresponds to the amount of tokens they hold.

More DAO platforms have been developed since the first introduction of DAO's practical implementation. There are platforms like Aragon or DAOstack that enable the creation of a network of stakeholders without centralized governance. Other suggestions for the use of DAO were proposed by the literature, for example:

- decentralized exchange platforms
- entities operating as crowd-funding platform
- ride-sharing platform
- fully automated company
- social media-based content platforms
- collectibles
- automated decision-making tools [\[40\]](#)

A promising application of DAO could as well be in the public administration, but examples of it are lacking. That is comprehensible as it would require significant investment, and in case of negative consequences, no one would want to take responsibility. Unfortunately, DAOs are also still tied to multiple governance issues:

- *procedural tedium* - participants can quickly get tired of constantly having to vote on every minor change. This can further lead to non-sensical votes on modifications which could bring damage to the whole DAO.
- *legal indeterminacy* - economic and legal theory is not yet well built around the concept of DAO. It is true that Wyoming became the first state to recognize DAO as a legal entity in 2021, but many of the legal questions remain unsolved. What is the liability of the participants of the DAO? Who is responsible for the self-executed acts of DAO? This is probably the largest legal burden that keeps hindering the wider adoption of DAOs.
- *structural rigidity* - just like any other concept built on blockchain, DAO's code is transparent and well auditable but not easily fixed once deployed. Modifications need to be allowed by the voters.

- *voter manipulation* - since the voting power corresponds to the amount of tokens owned, the voting power is centralized. It is also impossible to prevent the participants from grouping and voting for their own profit even if it means damaging the DAO. [42]

### 1.3.4 Decentralized Law

Usage of smart contracts can go beyond decentralized organizations. Since smart contracts can represent flows of rules and even act as a state machine, parts of laws could be encoded in them as well. Suggestions for using smart contracts to build decentralized jurisdictions appear, and practical implementation examples exist.

Jurisdiction is usually bound to a certain physical area but also to a particular set of scenarios about which this authority can rule. Rulings of courts in one country may not be enforceable in another and vice versa. This is an interesting problem for law enforcement in the digital space. What are the rules, and where can you appeal in case of fraud? National jurisdictions can never cover ruling about transactions that happened in the digital space. [43]

That is where the idea of having a decentralized jurisdiction originates from. Individual jurisdictions are not prepared for this, but experimental projects are trying to introduce decentralized law and free "virtual nations" like Bitnation Pangea or Aragon. Bitnation Pangea is trying to move all administrative duties to the cyberspace where one has a blockchain ID, and can ask for a birth certificate, marriage certificate, citizenship and any other documents that issuing in real world usually entails running around various offices. Decentralized jurisdiction removes the incompatibility between laws in different countries. Their core idea is that governments should compete for citizens, which will create competition like in a real market and hence augment the quality of services offered by different nations. [44]

The idea of decentralized law is exciting, but Thyse formulates a clear warning: *Without a guiding set of principles or governing laws, the outcomes of these systems will be even more random than the current legal systems they intend to replace.* [43]

## 1.4 Domains That Could Benefit from Blockchain

Being almost 15 years in the digital space, blockchain is still considered a hammer that has yet to find its nail. [34] Authors of [18], [34], [5], [6] mention many domains that could benefit from applying blockchain. They range from the public domain through healthcare, research, and commerce up to marketing. The following list is a compilation of the most frequently mentioned fields and specific use cases for blockchain, excluding the most common finance use cases.

- *Law*
  - transfer of property, e.g. car or real-estate after paying for leasing or mortgage
  - digital asset protection
  - proof of ownership
  - self-executing audit, copyrights, wills, contracts
- *Governments*
  - universal identities
  - public registers - real-estate register, company register, trade license register, ...
  - electronic voting
  - smart municipalities
- *Healthcare*
  - verification of vaccination certificates
  - medical data sharing for research purposes
  - electronic health records
- *Education*
  - obtaining diplomas in a form of verifiable credentials
  - crowdfunding for research
- *Commerce*
  - decentralized markets
  - digital asset handling - contract and document versioning
  - accommodation services - smart contract counting the exact consumption of water and electricity and creating the bill
  - loyalty programs - automatic application of a discount after a number of purchases is made
  - shared economy models like car-sharing
- *Internet of Things*
  - scalable access management
  - smart electronic devices
- *Others*
  - automotive
  - smart cities
  - environmental topics

## 1.5 Conclusion

This chapter covered the foundations of blockchain technology. After the introduction to the characteristics of the blockchain and the different types, more complex concepts were explained. The working of smart contracts was clarified, namely, the working of Ethereum smart contracts. Limitations of smart contracts were summarized, and the most challenging ones were addressed separately. Concepts of blockchain 3.0 like decentralized identity, decentralized autonomous organizations to decentralized jurisdictions, were explored. The last part summarized areas that could or already are benefiting from the blockchain.

The theory of smart contracts and decentralized identity will be crucial for understanding the practical case study.

---

# Blockchain in Public Sector

Many announcements of pilot projects using blockchain in the public sector can be found, but very few of them inform on how the implementation proceeded. Is the number of successful projects really that low? This chapter introduces the current state of the research on smart contracts, lists use cases for governments suggested by the literature and explores real-world projects related to the public domain that try to apply this technology. The last section of this chapter is dedicated to the European Blockchain Services Infrastructure (EBSI).

## 2.1 State of the Research

Topics related to the blockchain and smart contracts have been heavily researched in the latest years. One can sum up hundreds of examples where blockchain could prove useful from the accessible literature, but just a very few examples of practical application. [45] reveals the most researched disciplines in blockchain, and it is visible from Figure 2.1 that disciplines related to government and law are neglected. That is in contrast with most of the academic papers, as they mention public administration processes among the first examples where blockchain could prove its strengths. The lack of practical case studies is just supported by the summary of the most cited articles about smart contracts. [18] Major subjects of the articles in the top 20 list [3] are:

- connecting the smart contracts to the internet of things
- using smart contracts for supply chain management
- using blockchain to share medical data

---

<sup>3</sup>to be found in Appendix B

## 2. BLOCKCHAIN IN PUBLIC SECTOR

---

The use of blockchain for public administration processes is rarely discussed, and proofs of concept are missing.

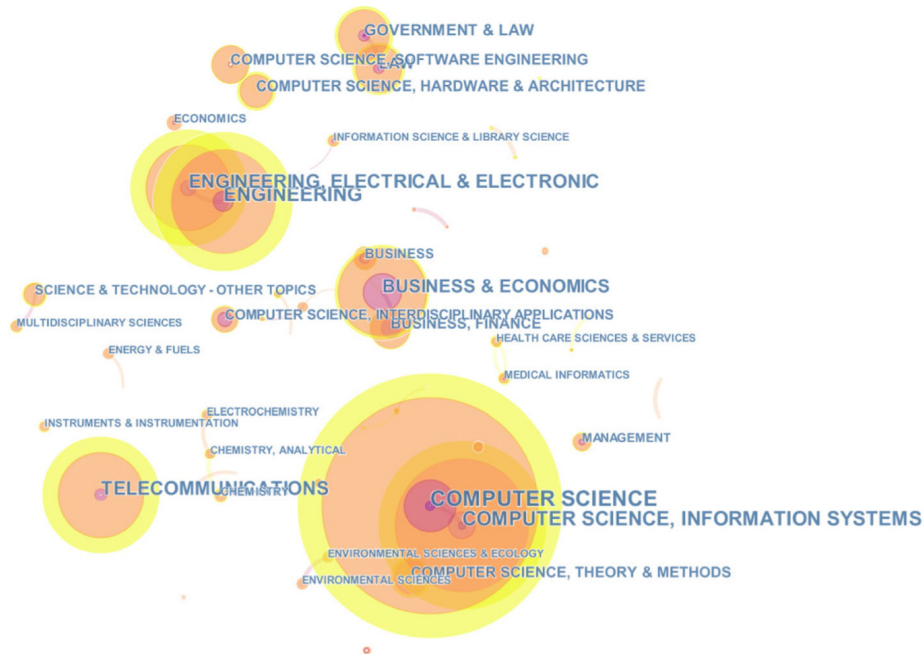


Figure 2.1: Blockchain research disciplines [45]

## 2.2 Blockchain Use Cases for Public Sector

Possible uses of blockchain for governments were lightly addressed in the last section of Chapter 1, but many more use cases exist. They can be divided into two groups - use cases for smart cities and use cases for smart administrative or governments.

**Smart Cities** - blockchain has a great potential for smart cities if combined with data science or the internet of things. Some of the listed uses seem trivial and not in need of a blockchain solution, but for urban planning, for example, proof that the data is not fabricated is very important.

- customs, border protection
- city parking meters
- urban planning with traffic data validated on blockchain
- traffic control in cities [14]



**Smart Administratives** - smart contracts and the decentralized identity are ideal for use cases in the public administration processes. Especially for:

- universal identity - will provide access to public services and also self-service for simple operations like updating data about their identity or issuing verifiable credentials regarding their education. Universal identity will become biographical over time as more and more information will be added to it, and all updates will be stored.
- integrated government - integration of the public services with banks, insurance companies, and other institutions through blockchain would mean that citizens could access both private and public entities with a single identity.
- elections - online voting through blockchain will support better citizen engagement as the elections can take place more often also regarding less important topics. The logic of assigning the seats to the elected representatives can be defined in a smart contract. [46]

## 2.3 Countries Adopting the Blockchain

When searching for projects that successfully implemented blockchain solutions in the public sector, very little information is found. This is probably due to most of the solutions resulting from cooperation between governments and blockchain companies that do not wish to disclose their know-how. Unfortunately, that means that only a few countries are pioneers of the technology, and as the knowledge does not spread, the worldwide adoption of the solutions is slowed down. The following countries are the leaders in the adoption of blockchain projects:

**UK** - issued a report in 2016 approving the use of blockchain across government applications and is actively supporting experimental projects. Some of the blockchain projects are:

- blockchain-based welfare distribution through a mobile app to send and track payments
- government DLT framework allowing companies to experiment with blockchain in the public domain
- blockchain-based international payments

**Singapore** - Singapore is still in a state of analyzing how to apply blockchain in the public sector but already has a well-developed digital identity for their citizens, so it should be easily connectible to the blockchain. Bank in Singapore uses blockchain for cross-border transactions with a branch in Malaysia. [14]

## 2. BLOCKCHAIN IN PUBLIC SECTOR

---

**Dubai** - wants to become host number one for blockchain companies, so it is heavily supporting blockchain projects. Dubai started a Global Blockchain Council (GBC) initiative that intended to move all government documents onto the blockchain by 2020. They announced seven collaborations that should explore the use of blockchain for healthcare, business registrations, tourism, and logistics. More promises are stated on official websites about moving 50% of the government processes on the blockchain by 2021, but no report on the results of the implementation is available. [47]

**Malta** - has an interesting legal environment for businesses as it is governed by a mixture of continental and common law. Besides that, Malta passed multiple acts directly supporting blockchain companies that define regulatory procedures for them.

**Estonia** - is actively applying the *single-window principle* thanks to which citizens can access most of the public services through one point of access. This helped reduce the number of public office visits by 60%. 95% of estonian tax reports are being submitted electronically. Estonia is funding the development of blockchain services enabling business registration. The project, in collaboration with Bitnation, wants to offer also notary services to Estonian e-residents since blockchain notarized documents are not legally binding in the current Estonian law. [46]

**China** - is the first country with a successful project offering electronic data notarization services with 100 participating traditional notarial offices. The project is called Ancun, and it publishes thousands of validated records in a publicly accessible blockchain. [14]

**Illinois** - the state government supported six pilot block-chain programs, blockchain-based ID registry being one of them. The aim is to create a self-sovereign identity for all citizens during the birth registration process. Public offices will verify the registration information and sign the attributes cryptographically. Validated information will become verifiable claims. [48]

Above mentioned countries are the most prominent players in adopting the blockchain, but other countries also have positive standing towards it. Team GovChain maps an overview of blockchain projects in different countries, and interesting information can be found on their websites <https://govchain.world>. [49] The blockchain initiative run by European Union will be addressed in the next section.

## 2.4 EBSI

European Blockchain Services Infrastructure (EBSI) is an initiative started in 2018 signed by 27 EU member states, including Norway and Liechtenstein. The main goals of this initiative are:

- facilitation of cross-border services, e.g., applying for a university
- establishing cooperation between public authorities in different countries to easily exchange data about legal persons
- providing an infrastructure for third-party applications

EBSI is a distributed network of nodes having different levels of permissions. Only validator nodes are able to validate transactions. These nodes will mostly be at the hands of public offices.

Many EU countries already support digital identity usage for their citizens to some extent, but they are not usable cross-border. EBSI aims to integrate the existing identity systems of the member states, but legal modifications may be required from the governments. [\[50\]](#)

## 2.5 Conclusion

This chapter reviewed use cases for smart contracts and decentralized identities in the public sector. Countries supporting the adoption of the blockchain were listed together with projects they are trying to implement. Lastly, the EBSI initiative was presented.



---

## Case Study

The previous chapter illustrated the lack of practical step-by-step examples of using smart contracts in the public domain. This chapter aims to pick a process closely related to the public sector and suggest how it could benefit from smart contracts and decentralized identity. Chapter maps how the process is chosen, its state in general, and its state in the Czech Republic. The As-is model of the process is presented, and improvements are suggested in the to-be model. Suggestion for the architecture of the solution is proposed. The process is modeled in DasContract language, which allows an easy transformation of a diagram into a smart contract code.

### 3.1 Establishment of a Company

This section explains the motivations behind choosing the process of establishment of a company for this case study. A global view of the process of creating a company is presented, and the current state of digitalization of this process in the world is explored.

#### 3.1.1 Choice of the Process for the Case Study

Each country's public sector counts a multitude of processes between the offices and the public. Most of the processes are related to simple document and certificate issuing or validation, but some of the processes are more complex and require the participation of multiple institutions. The future European blockchain (EBSI) is intended to be just infrastructure but does not provide specific use cases. Some of the use cases that are suggested cover mostly applying to universities or for funds, but they assume that the user doing so already has their private or company account on the blockchain. EBSI infrastructure does not solve the creation of a company through blockchain.

Creating a company is a country-specific process as the local laws may differ, but it often requires visiting a trade licensing office, a finance office, and

dealing with many documents. These steps cause delays based on how busy the particular office is, even if all that is needed is just a confirmation, stamp, or signature. This process could be transferred onto the blockchain, the waiting time could be eliminated, and a simplification of the process could encourage more entrepreneurs to start a company. The process is an ideal candidate for the case study as, besides its complexity, there are more subprocesses in a lifecycle of a company that can benefit from the blockchain. The case study is limited to the process of establishing a private limited company.

#### 3.1.2 Incorporation of a Company in the World

The set of requirements to be able to start a company is similar in most countries. According to [43] the most common duties are:

- registration in the local register of companies
- signed memorandum of association
- certificate of incorporation
- registered office
- names of the proposed officers

When considering starting a company, two factors are interesting for entrepreneurs - how long it takes to start a company and what is the cost of the process. A research branch of the World Bank called Doingbusiness concentrates on collecting data related to entrepreneurship from all of the countries in the world. [51] used this data to provide an overview of the countries where most businesses are registered per 1000 people: higher the number, the more favorable conditions for starting a company. Table 3.1 contains a selection of all European countries that got into the top 20 list of countries with most businesses started per capita. It is also clear from the study that countries with less stable political situations tend to have a very long company registration process.

In 2011 European Union called member states to limit the time needed to register a company to three days and the costs to 100 euros. [52] From data collected by Statista in 2019, it is visible that countries did not succeed in simplifying the process. Figure 3.1 shows six countries with the slowest process, Czechia and Slovakia making it to the top of the list, and Figure 3.2 shows the leaders in handling company registration.

According to [54] the average duration to start a company in the EU is 12.17 days. The average time within the Euro area is 9.82 days. It takes 24.5 days to register a company in the Czech Republic, which is double the EU average.

### 3.1. Establishment of a Company

Country	Businesses started per 1000 people
Estonia	23.59
Cyprus	17.58
Malta	17.48
Luxembourg	17.20
United Kingdom	15.65
Bulgaria	10.10
Denmark	10.01
Iceland	9.88
Norway	8.62
Latvia	8.01
Romania	7.32

Table 3.1: New businesses registered per 1000 people [51]

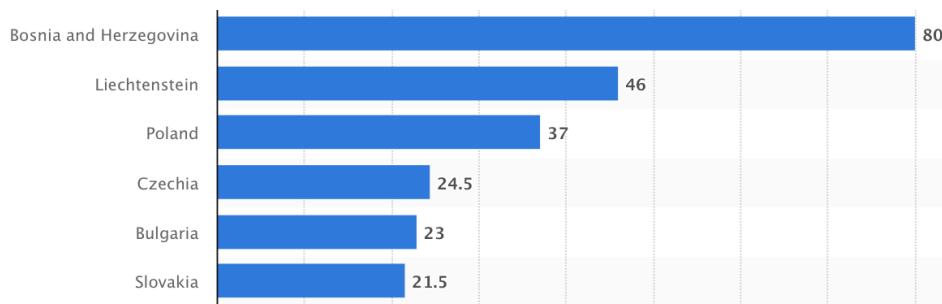


Figure 3.1: Countries with the slowest process of registering a company (in days) [53]

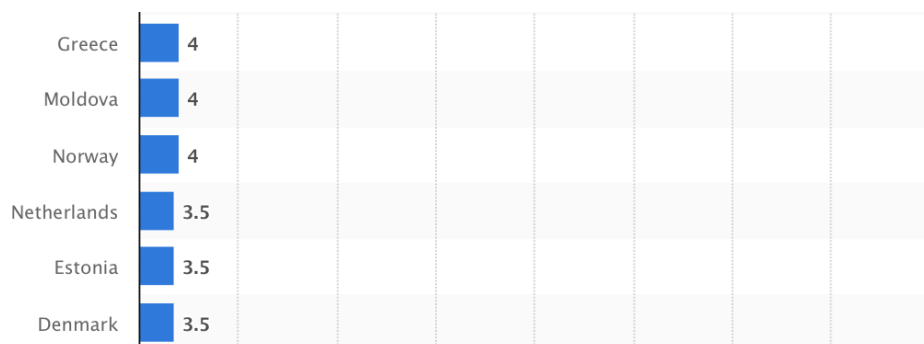


Figure 3.2: Countries with the fastest process of registering a company (in days) [53]

#### 3.1.3 State of Digitalization of the Process

The leaders in the digitalization of the registration process are Estonia, Denmark, and the Netherlands. These countries share very good accessibility of guides on how to start a company. All information for starting a company in Denmark is accessible on web pages provided by the Ministry of Foreign Affairs. Particularly interesting is the omission of signatures with a notarial certificate and also the option to submit all documents in English. [55] What can be a downside of registering a private limited company in Denmark is a relatively high required minimum share capital of approximately 5400 euros.

Estonia claims it takes only three hours to set up a company using their e-Residency. It is an easy three-step process. First, one needs to become an e-Resident, then choose a contact person for their company in Estonia and finally register their company in the e-Business registry and open a bank account. E-residency and the registration cost 365 euros, and the required share capital is 2500 euros. The intermediary step with a contact person makes sure that the company meets the legal obligation of having a physically registered office which is the main obstacle to full digitalization of the process in most countries. [56]

In Section [1.3] the topic of DAOs was addressed, and it could seem that DAO has the potential to replace the company as an entity. The main issue with DAO is its recognition as a legal entity. More progressive governments like the one in Wyoming will allow recognition of DAO as a legal corporation over time, but this recognition needs to be well prepared. [42] Until the question of liability is properly solved, DAO can not represent a real company, and also, from its nature, it can not take over all tasks that the governance and lifecycle of a company currently require. The concept of DAO is not an ideal representation of a company on the blockchain. However, the company's lifecycle can be transferred on the blockchain in a more granular way, which will be proposed in the following sections.

## 3.2 Establishment of a Company in Czechia As-is

The establishment of a company in Czechia has many similar compulsory steps to other countries. This section models the current flow of the process, explains its steps in detail with all necessities that one must provide and submit when registering a company, and suggests modifications to the process by applying some of the concepts based on the smart contracts. The process description is based on sources [57], [52] and [58]. The process is modeled using the BPM notation and its standard set of symbols. Clarity was one of the main objectives when modeling. Hence, the models should be comprehensible also for readers non-proficient in BPMN. All translations of legal terms were taken from the official translation of the Business Corporation Act passed by the parliament of the Czech Republic. [57]



Some of the first most noticeable differences when starting a company in Czechia compared to Estonia or Denmark are the minimum required capital and the accessibility of information. The minimal required capital counts only 1Kč, which makes starting a company easily accessible to anyone. When searching for a comprehensible explanation of the process, no official pages of the ministry show up. It is mostly articles from private companies or advocates that explain the full process of starting a company. Companies like Ofigo or Založ Firmu offer to register a company on behalf of the members and herewith avoiding visits to multiple public offices and certifications of signatures at the notary. Prices of the service range from 5 000 Kč to approximately 10 000 Kč, varying based on the need for virtual headquarters. [59] [60] Some renowned banks even offer the service free of charge under the condition of opening a business account at them. The customer only pays the obligatory registration fees in such a case. [61] Creating a company through an intermediary requires authorizing them to act on your behalf, which can come with a risk of possible misuse. The customer also needs to rely on the intermediary to input the correct data everywhere.

### 3.2.1 As-is Process Model

To begin, a simplified model of the process is captured on Figure 3.3. The process can be broken down into five steps that have dependencies on each other. Each of these steps will be addressed separately. The complete flow of the process can be seen on Figure B.2 and Figure B.3. The whole process begins with an idea for a business plan. The creation of the business plan is out of the scope of this thesis.

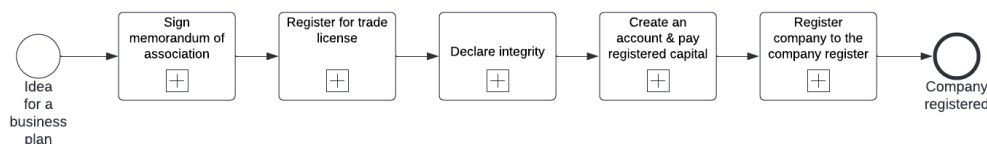


Figure 3.3: Simplified model of the current state of registering a company in Czech Republic

### 3.2.2 Signing Memorandum of Association

If one person is creating a company, signing a deed of foundation is required. A memorandum of association in the form of an authentic instrument is needed for multiple members. Prior to visiting the notary, all information needs to be provided to him so he can prepare the document. Set of the data required for the document consists of:

### 3. CASE STUDY

---

- *name of the company*
- *headquarters of the company* - it is enough to fill in the city, that way in case the company moves within the city, the memorandum of association will not need to be modified and more notary fees can be avoided
- *objects of the company* - one of the objects that are listed in the trade licensing act
- *executives and members*
  - name and surname
  - identification number
  - place of birth
  - permanent residence
  - in case of multiple executives also a specification of the way in which they will act in the name of the company
- *registered capital*
  - value of the contribution
  - type - cash contribution, contribution in kind
  - contribution administrator
  - to what extent it needs to be paid at the beginning and when the rest needs to be paid

Notary prepares the documents, and executives and members need to sign them. He then certifies all the signatures, and the memorandum of association is complete.

#### 3.2.3 Registration for Trade License

The second step of the process is the registration for a trade license. Before applying for a trade license, a company needs to have the address of its headquarters. The trade licensing office requires documents based on two situations that can happen:

- *founding member is the owner of the building where HQ will be situated* - approval of the owner with a certified signature must be presented, the trade licensing office will confirm the ownership of the location with the land register
- *company will be renting a property* - rental agreement with approval to locate HQ at that place with certified signatures of the owner must be presented

Registration for a trade license can be delivered personally or electronically with a digital signature, but that requires having an activated ID card allowing electronic signatures. Information necessary for the registration is the same as the data needed for the memorandum of association, but a complete address of the HQ must be specified. Registration is submitted together with attachments such as the rental agreement with certified signatures or proof of eligibility in case a craft trade license is being registered. The trade licensing office accepts the registration and processes it within 3-5 business days. Confirmation about registration of the trade license is issued, but the applicant is not notified and needs to pick up the confirmation himself at the office. [\[62\]](#)

### 3.2.4 Declaration of Integrity

Executives need to declare integrity by signing a declaration of honor and by providing an extract from the judicial record. The extract from the judicial record can be obtained for free in an electronic form from [www.gov.cz](http://www.gov.cz) or in physical form at any Czech POINT for a fee of 100 Kč.

### 3.2.5 Creation of a Bank Account

Before submitting the final application for registration of the company, an official bank account needs to be created, and the registered capital needs to be paid. Banks offer a designated type of account for this purpose. Most banks do not charge for creating such an account, and it is often possible to do it online. Bank creates the account, and members can pay their part of the registered capital. The amount of the registered capital does not need to be paid at once, it depends on the conditions written in the memorandum of association, but each member needs to pay at least 30% of the determined amount. The latest date to pay the rest of the registered capital is five years after signing the memorandum of association.

The bank withholds paid funds until the registration of the company is completed, and then it is the assigned contribution administrator who is responsible for them. Bank issues a confirmation about the downpayment of the capital that is later needed at the company register. Once the company is registered and has confirmation about it, any member can bring this confirmation to the bank, and the bank unfreezes the funds.

### 3.2.6 Registration of the Company in the Company Register

Application for the registration of the company can be filled out online and then printed and signed at the notary. Information required is:

- number of trade license
- name of the company

### 3. CASE STUDY

---

- precise address of the HQ
- objects of the company
- statutory body, its members and their roles, executives and how they act
- members
- value of the registered capital

The application needs to be submitted with all corresponding attachments:

- memorandum of association
- rental agreement with allowance to locate HQ
- declaration of the integrity of the executive and extract from his judicial record
- confirmation of paying the registered capital at a bank
- specimen signatures of the executives

The application can be submitted via notary or via regional court. When delivering the application to the regional court, the mailroom confirms the delivery of the documents with a stamp and marks the number of received attachments. Then the documents are passed to the clerk. Based on the completeness of the documents, the clerk accepts the registration application or denies it requesting missing documents. If all documents were correctly submitted, the clerk adds the company to the company register.

### 3.3 To-be Establishment of a Company Using Smart Contract

Many proposals on how to simplify registering a company were presented over the years, but most of them have the change of legislation as a preliminary step. Any changes in the law need to be discussed in the parliament, which makes the adoption of new ideas a lengthy process, and only little steps forward are achieved. As an example, in 2019, members of a political party Piráti proposed a new way of creating a company fully online, which would only take one day. Unfortunately, their proposal fully relied on changing the legislation. It presented how a company could be registered through a simple website. That would eliminate the need to visit different offices, but the security aspects of the transmission of the data were not addressed in this proposal. [\[63\]](#)

The solution that is proposed in this section tries to profit from the security aspects of the blockchain and also respect as many steps of the current

process as possible. The changes to the legislation would not need to be so dramatic. The to-be model is designed in DasContract language that allows easy transformation of the process into a smart contract. The next section is a brief introduction to the DasContract followed by the proposal for the to-be process model of the company registration process.

#### 3.3.1 DasContract

DasContract is a domain-specific language that allows using a higher level of abstraction as it implements principles from enterprise engineering. It combines DEMO modeling language with BPMN and UML to facilitate viewing smart contracts as business processes. It is designed to be platform-independent to work with any platform that will support it. DasContract language focuses on human understanding because both legal texts and code can be challenging to comprehend. Visualization of the process and automatic generation of the smart contract allows the user to fully focus on the process rather than on the technicalities of creating a smart contract. Usage of a domain-specific language helps to mitigate risks emerging from a different understanding of the semantics. [64]

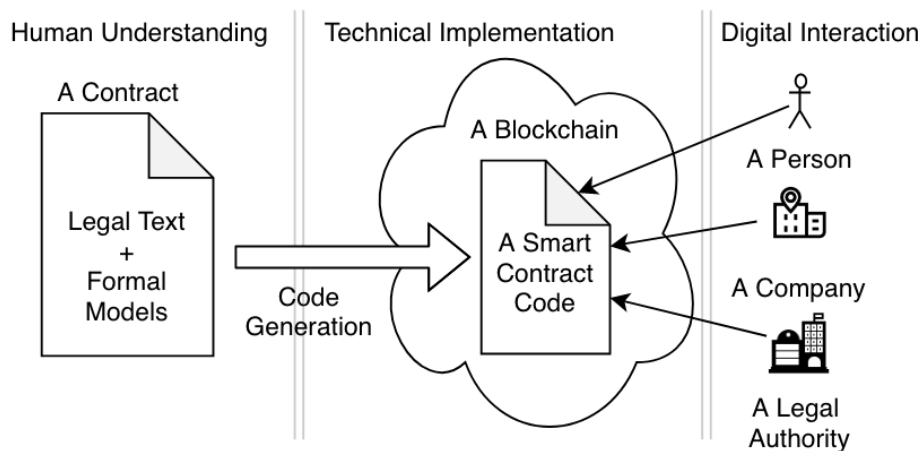


Figure 3.4: Concept architecture of DasContract [65]

DasContract is a language that is still under development, and support for oracles, and decentralized identities are promised to be added in future versions. There are three key components to the DasContract architecture that are also shown in Figure 3.4:

- *Human understanding* - since it is often a challenge to contain the gist of a real contract in a process model, legal text and ontological models are combined

### 3. CASE STUDY

---

- *Technical implementation* - a transformation of formal models into an executable code in the form of a smart contract
- *Digital interaction* - fully digital interaction of users with the smart contract that is recorded on the blockchain and can also serve as an audit trail [65]

An experimental DasContract modeler<sup>4</sup> supports generating a skeleton of the smart contract in Solidity or Plutus from the process model. This modeler was used to design the to-be model of the company registration process. DasContract language supports the most important BPMN elements such as:

- user tasks, business tasks, script tasks
- call activities
- exclusive and parallel gateways
- start, end and timer boundary events [66]

#### 3.3.2 To-be Model in DasContract

The proposed model eliminates a large portion of the administrative tasks thanks to the decentralized identities that allow their holders to sign documents electronically and herewith create a permanent record of their signature on the blockchain. There is no more need to certify signatures at the notary. The to-be model suggests the use of a blockchain oracle to retrieve data from registers of the public offices in order to validate all conditions for issuing a trade license or adding the company to the register. Script tasks represent operations automatically executed by the smart contract. The registered capital is paid in cryptocurrency, and each member receives a token representing their share that is easily exchangeable or can be broken into smaller parts.

The following list describes modifications to the different steps of the process that are visualised in Figure 3.5:

**Signing Memorandum of Association** - In the proposed solution, it is possible to fill the memorandum of association as a form in an application. All individuals listed in the document as executives or members must sign it with their digital signatures. Since the signatures will be stored on the blockchain, the foundation of the company is immutable, and it is possible to verify whether all required individuals signed it. Unless special conditions regarding the shares or the capital are concerned, the presence of the notary is not needed anymore.

---

<sup>4</sup>available at <https://black-plant-0fb6dc03.azurestaticapps.net/>

**Registration for Trade License** - Registration for trade license requires a confirmation of the location of the headquarters. This confirmation can now be easily requested from the property owner. He will either confirm the location with his signature or deny the request. The form for the trade license is similar to the memorandum of association. After submitting the form, the smart contract verifies that all necessary conditions are fulfilled. It retrieves data from an oracle of the public administration that merges data from all public registers so ownership of the property of HQ can be verified as well as proof of eligibility to get a craft license. Smart contract issues verifiable credentials proving the issuance of the trade license.

**Declaration of Integrity** - Executives can declare integrity by their signature and the smart contract verifies their judicial record communicating with the oracle.

**Creation of a Bank Account** - Bank account is no longer needed as the capital can be paid in cryptocurrency and recorded as a blockchain transaction. The smart contract will issue a share token in exchange and block the funds until the registration process is complete.

**Registration to the Company Register** - The registration application needs to be signed by executives and members. Smart contract easily audits the completeness of all previous steps and documents. In case all conditions are fulfilled, the company is registered and the funds are freed, else the applying individuals get a notification listing the missing documents.

The communication between users, smart contract, and the oracle is visualized in Figure 3.6. It is expected that the founders of the company communicate together to provide all necessary signatures for the applications.

The impact of the changes proposed to the model will be discussed later in Chapter 4. The most significant changes to the model were:

- no more need of the notary
- digitalization of all of the applications
- automatic verification of the data from the public registers
- payment of the registered capital in cryptocurrency

3. CASE STUDY

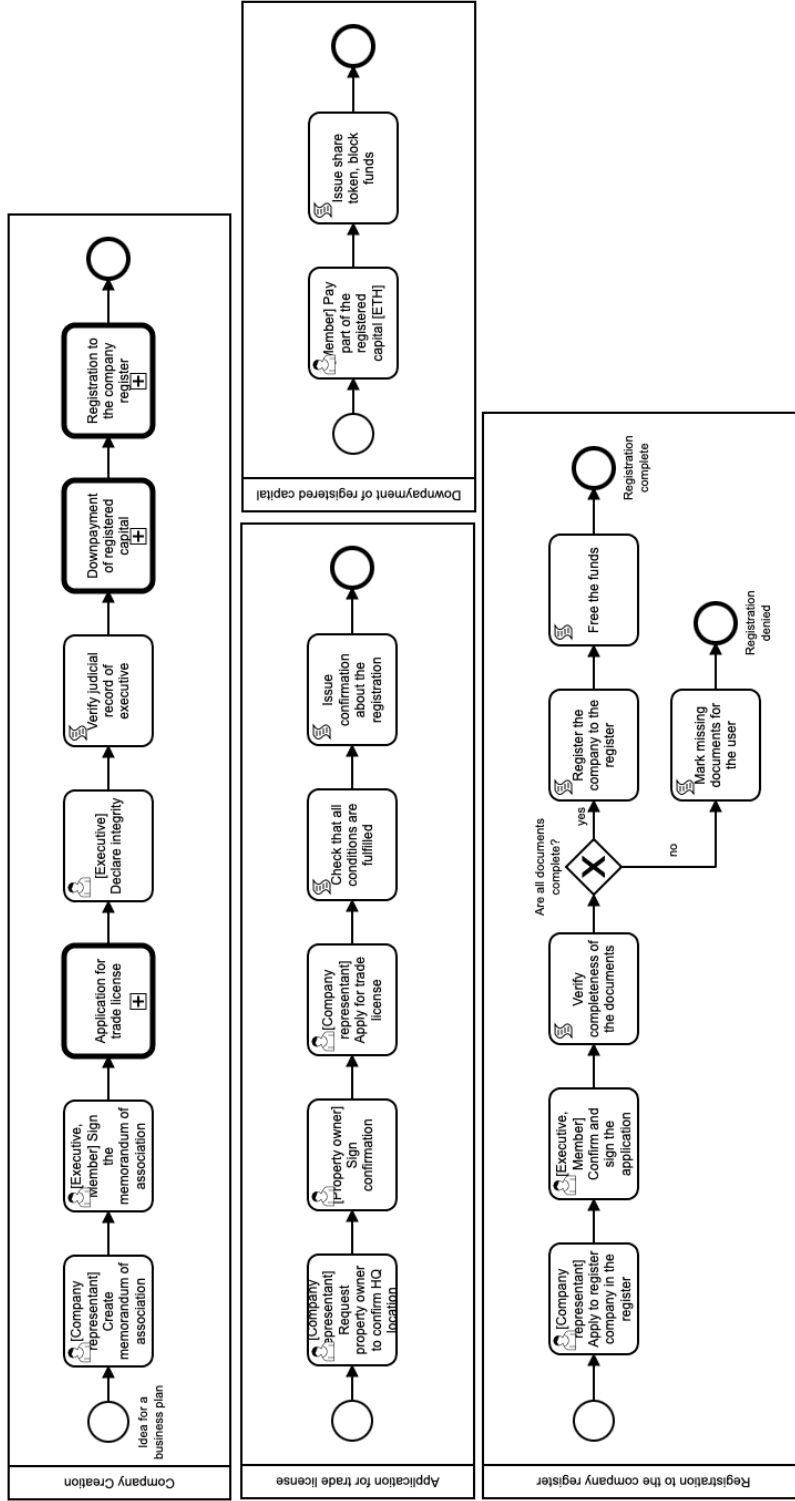


Figure 3.5: To-be model of company registration process in DasContract



### 3.3. To-be Establishment of a Company Using Smart Contract

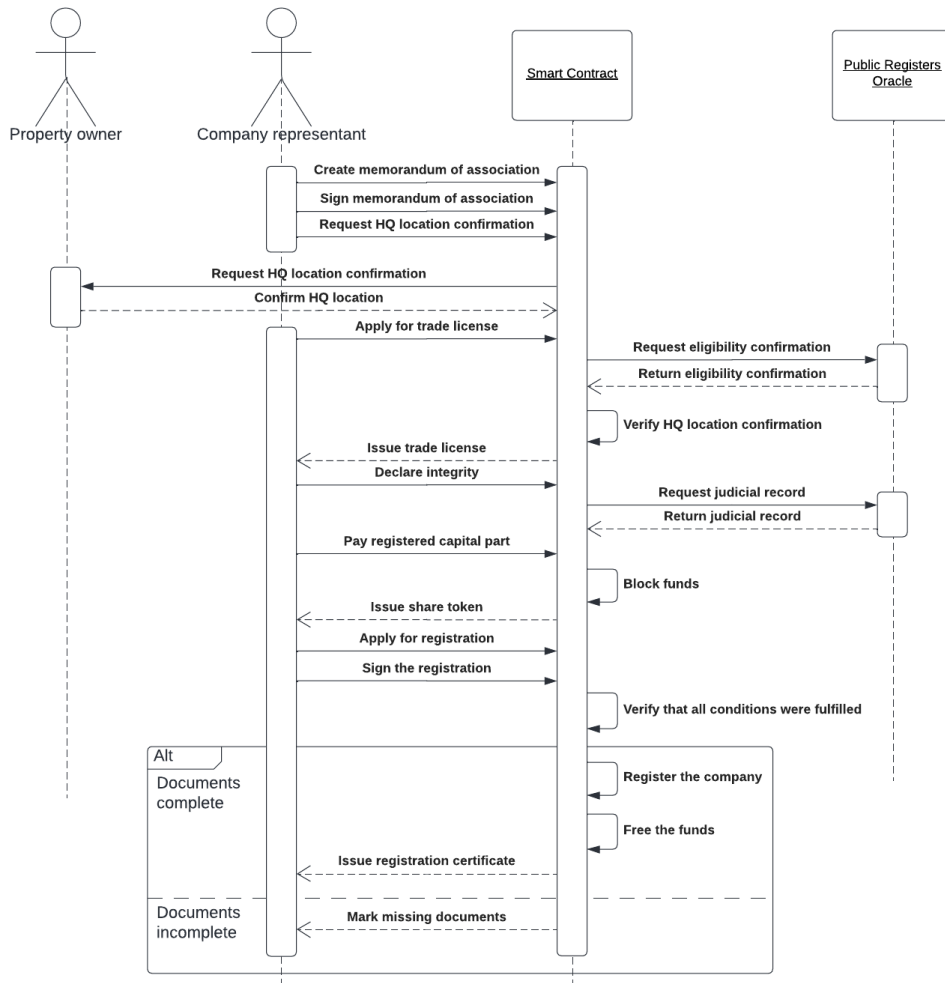


Figure 3.6: Proposal of communication flow between entities

#### 3.3.3 Generating the Smart Contract

As mentioned earlier, DasContract allows generating the smart contract in Solidity directly from the process model. The designer supports easy configuration of forms and additional definitions of validations.

Before generating the smart contract, first of all, a data model needed to be specified. The data model can be found in Appendix B as Figure B.4. The main entity serves to store all necessary data about the registration, including data about members and executives of the company. It also stores variables showing the status of the registration process such as `HQconfirmed` or `TradeLicenseIssued`. Besides storing data about executives and members, it stores the key timing data of the memorandum of association since the capital has to be fully paid within five years from the issuance of the memorandum.

### 3. CASE STUDY

---

The `ShareToken` represents shares of the company in exchange for the paid capital.

Secondly, user roles had to be defined. The to-be model operates with four roles only and removes practically all administrative roles since the smart contract automatically does the validations, and all submissions and signatures are digital. The four used roles are:

- *company representant* - any person representing the company, be it a lawyer or a future member, who is submitting all necessary documents in the name of the future company
- *member* - person partaking in the registered capital having their share in the company
- *executive* - a person acting in the name of the company
- *property owner* - a person giving allowance to situate HQ of the company in their property

The generated code is a great basis for the smart contract but to completely implement the proposed model, communication with the oracles would need to be manually added as it is currently not supported by `DasContract`. The code can be found on the enclosed SD card.

#### 3.3.4 Prerequisites for Adoption of the Model

To adopt the modified process of registering a company, multiple prerequisites would need to be fulfilled. They can be grouped into two categories - technological prerequisites and legal prerequisites:

- *technological prerequisites*
  - creation of a centralized public register grouping all publicly accessible data
  - detailed analysis of using the blockchain in the public administration landscape
  - implementation of the blockchain
  - development of the interface for communication between users and the public administration through blockchain
- *legal prerequisites*
  - equivalence of decentralized identity and signatures on the blockchain to the currently used electronic signatures
  - recognition of documents on the blockchain with specified structure as binding legal documents

- legalization of paying the registered capital in cryptocurrencies

The legal prerequisites must be fulfilled. Otherwise, the accountability of a company registered through this process would be in question, as well as the enforceability of contracts signed on the blockchain. The last point regarding the payment of the registered capital in cryptocurrency could be implemented later during the adoption process. The model can be easily modified to still include payment of the capital at a bank.

### 3.4 Conclusion

The beginning of this chapter introduced the process of creating the company in general and explored the state of the digitalization of this process in the world. The case study concentrated on the formalization of the company registration process in Czechia, and an as-is model of the process was presented. The steps of the process were detailed, and all data requirements were addressed. The second part of the case study proposed the modification of the process and how it could be transformed into a smart contract. To-be model of the process was designed using the DasContract language. A communication model of the process flow was created, and a data model for the smart contract was defined. Prerequisites for the adoption of the suggested solution in the public administration were discussed. Evaluation of the impact of the proposed modifications follows in the next chapter.



---

# Evaluation

The main goal of this section is to compare the as-is to the proposed to-be model and evaluate the impacts of the proposed changes. For this purpose, a Quality Evaluation Framework (QEF) for the evaluation of processes is used. The evaluation considers multiple quality factors, which allows a complex overview of the introduced modifications.

## 4.1 Quality Evaluation Framework

A language-independent framework for evaluation of business processes QEF introduced in [67] was chosen to evaluate the proposed to-be process model. This framework identifies key attributes of the processes that are worth measuring when trying to optimize them. It introduces five different quality dimensions that concentrate on four key business process concepts - event, output, input, and activity.

- performance
- efficiency
- reliability and recoverability
- permissability
- availability

Since the as-is process is not being monitored at present besides approximate estimations, precise data about its runs are not available. Nonetheless, it is still beneficial to use quality dimensions from the framework as they provide a good selection of aspects to take into account. Information used for evaluating the process about its duration, costs, and involved officers is available or deductible.

As the to-be model is only a proposal and was not deployed, quality dimensions like reliability, recoverability, and availability are not addressed in the evaluation. Also, from the nature of the used technology, some of the factors can be omitted. Since blockchain works in a decentralized manner, most factors related to the above-mentioned quality dimensions will not represent a great concern.

The dimensions have associated quality factors that can be measured by different units based on the context. Quality dimensions and their recognized factors that are used for the evaluation are:

- *performance*
  - throughput - amount of work, users or things that are processed in a given period of time
  - cycle time - total time needed by the process to transform a set of inputs into defined outputs
  - timeliness - response time of the process
  - cost - amount of money needed to complete the process
- *efficiency*
  - resource efficiency - how successful the process is in avoiding wasted resources
  - cost efficiency - total processing cost, how well any wasted budget is avoided
  - time efficiency - real time spent on the process versus planned duration of the process
- *permissability*
  - authority - design of the process ensures that inputs are consumed by authorized activities only [\[67\]](#)

## 4.2 Process Evaluation

Selected quality dimensions are considered one by one and evaluated on both the as-is model and to-be model. User experience is evaluated separately as it is not a quality dimension of QEF.

### 4.2.1 Performance Evaluation

The quantity of needed documents is considered the unit of measurement of the *throughput* in this case. The following table lists all documents required by the current process and what is their equivalent in the to-be model.

Document in the current process	Form of submission (as-is)	Form in the to-be process
Memorandum of association	physical	electronic
Rental agreement	physical	electronic signature
Trade license application	physical/electronic	electronic
Declaration of integrity	physical	electronic signature
Extract from judicial record	physical	retrieved automatically by SC from register
Confirmation about payment of the registered capital by the bank	physical	retrieved automatically by SC from transactions
Application to the company register	filled online, delivered physically	electronic
Specimen signatures of the executives	physical	no longer needed

Table 4.1: Documents required throughout the company registration process

Even though some documents can be submitted through Datová schránka provided by Czech Post, their processing is far from digital. Employees of the public offices usually print all of the online submitted forms, fill the rest of them manually, scan them and insert them back into the system. The digitalization of the process completely removes the need for physical documents. Furthermore, some of the data no longer need to have a form of a document. It is either a simple signature, a blockchain transaction, or a piece of information retrievable through a blockchain oracle. The trade license and the registration in the company register have a form of verifiable credentials once issued. Counting the documents that are replaced by signature or by automatic retrieval of the data, the number of required documents dropped from 8 to 3.

*Cycle time* represents the total time of the process. *Timeliness* is the response time, but in the case of the company registration process, the response time to secure each needed document will be addressed, and the sum of these response times will be considered the cycle time. Table 4.2 is a compilation of durations of different tasks listed in [59] and official time limits to complete the tasks given by the regulations. The durations are just approximate as it is not possible to predict how long one waits at the public office or post office. Each task also has an estimated duration in the newly proposed process.

Task	Duration as-is	Processing time limit	Duration to-be
Signing memorandum of association and certification of the signatures	1 hour	not given	filling in the form $\approx 1$ hour
Securing the agreement with location of the HQ	30 minutes	depends on property owner	depends on property owner
Applying for trade license	2 hours	3-5 days	filling in the form $\approx 1$ hour, automatic validation $\approx 0$
Extract from the judicial record	15 minutes	not given	automatic retrieval $\approx 0$
Certification of the signatures	30 minutes	not given	automatic validation $\approx 0$
Creation of a bank account	1 hour	not given	no longer needed $\approx 0$
Applying for registration in the company register	2 hours	5 days (up to 17 days)	filling in the form $\approx 1$ hour, automatic validation $\approx 0$
<b>Total</b>	<b>9 days</b>		<b><math>\approx 3</math> hours</b>

Table 4.2: Duration of tasks during the company registration



Some steps in both of the compared process models depend on human factors. We suppose that individuals founding a company will secure all necessary signatures and payments of the registered capital as fast as possible in their own interest. The only human factor that can not be rushed too much is the owner of the property providing his agreement with the location of the HQ. It was mentioned in Chapter 3 that the process of registering a company currently takes 24.5 days on average. Table 4.2 presents a more optimistic duration of 9 days for the current process if everything goes fast. With the proposed modifications, the whole process (excluding the reactivity of humans) could take only 3 hours.

*Cost* as the total amount of money needed to complete the process will be addressed in the efficiency evaluation.

### 4.2.2 Efficiency Evaluation

*Resources* are usually any assets needed for execution of the process such as people, time or money. Time and cost efficiency will be covered separately and this section will consider the human resources needed in the process. Two categories of participants can be recognized:

- *individuals paid by state*
  - notary
  - trade license office clerk
  - post office clerk
  - regional court mail room
  - regional court officer
- *independent actors*
  - founders of the company
  - property owner
  - banker

The modified process automatizes verification of the documents as well as issuing of trade license and registration into the register. This can free the officers from the burden of administration and mundane tasks and provide them with time for more important things. Also, many responsibilities given to notaries, such as certification of signatures, are a relic from the past that can be fully digital.

*Cost efficiency* is problematic to measure since also the costs for the adoption of the modified process would need to be included, and that is not possible without more specific planning of the implementation. Also, the cost can be looked at in two different ways - the total cost that the state pays to provide

## 4. EVALUATION

---

the registration process versus the cost that the applicant has to pay when starting a business. These two costs should be similar, but if the state wants to support the creation of the new businesses, they will try to keep the fees low. By removing various officers from the process as described above, also the total cost of the process will drop. Table 4.3 lists all fees that need to be currently paid when registering a company. [68]

Activity	Fee
Signing memorandum of association at the notary	2000 - 4000Kč
Certification of signature on the rental agreement	30Kč
Application for trade license	1000Kč
Extract from the judicial record (per executive)	100Kč
Bank confirmation about payment of the registered capital	0 - 500Kč
Certification of signatures on application to the company register	1000Kč
Fee for company registration (at notary/at court)	300/2700Kč
<b>Total</b>	<b>4430 - 9330Kč</b>

Table 4.3: Total current costs for company registration

In case the structure of the company is more complicated, the company is registered at a court for a higher fee. Also the fee at the notary for composing the memorandum of association is higher in such case. The total company registration fee ranges from 4430 to 9330Kč, which is approximately 177 to 373 euros. EU wanted the registration costs to drop to 100 euros. In case of the digitalization of the process, most of the activities in the table would not be needed anymore, and the registration could be free apart from paying the registered capital and possible fees for legal guidance in case of a complex company structure. The final fee for the registration would depend on the price of implementing the new process.

The official average time of the company registration is 24.5 days. In optimistic cases, it can be registered in 9 days. As mentioned in chapter 3, the EU wants member states to provide similar company registration services in terms of cost and duration. The desired duration of the company registration is 3 days. Proposed digitalization of the process cuts this time by 95% to 3 hours, achieving great *time efficiency*.

### 4.2.3 Permissability Evaluation

When evaluating whether the inputs are only consumed by authorized activities, it is also useful to observe whether only authorized individuals can access the inputs. In the as-is model, all documents that are being submitted are considered inputs. A table of all individuals who possibly interact with

some of the documents follows, together with a specification of the subprocess where the interaction happens. The different subprocesses were described in Section 3.2.1. Some individuals act in multiple subprocesses. Individuals founding the company, such as members or executives, are omitted. The table shows which individuals access the data in the current process and which in the proposed model. Their participation is marked with *X*.

Individual	Subprocess	As-is	To-be
Notary	Memorandum of Association	X	
Property owner	Registration for Trade License	X	X
Notary	Registration for Trade License	X	
Trade license office clerk	Registration for Trade License	X	
Post office clerk	Declaration of Integrity	X	
Banker	Creation of Bank Account	X	
Notary	Registration in Company Register	X	
Regional court mail room	Registration in Company Register	X	
Regional court officer	Registration in Company Register	X	

Table 4.4: Individuals accessing the data throughout the company registration process

Table 4.4 shows nine individuals accessing the data throughout the original process compared to one single individual that accesses the data in the proposed to-be model. Limitation of access to the data comes with multiple advantages, especially since sensitive data is concerned in this process. It is not just about the security of the data but also about preserving a competitive advantage. The fewer people know what the new name and occupation of the company will be before its registration, the smaller the chance that someone will misuse this information.

#### 4.2.4 User Experience

Apart from the quality factors selected from the QEF, also user experience is worth evaluating. Countries with the best handling of company registration share the accessibility of information about the registration process. When searching for a step-by-step guide on registering the company in Czechia, no official websites appear. When going through the process of the registration, the applicant will visit these pages minimally:

- Trade license register - <https://www.rzp.cz>

## 4. EVALUATION

---

- Application for online submission of the registration - JRF - <https://www.rzp.cz/epo/cs/napoveda>
- Information about extract from judicial records - <https://www.mvcr.cz/clanek/vypis-z-rejstriku-trestu-lze-nove-ziskat-kdykoliv-kdekoliv-a-zdarma.aspx>
- Information about registration to the company register - <https://epodatelna.justice.cz/ePodatelna/homepage>
- Form for registration to the company register - <https://or.justice.cz/ias/ui/podani>

Most public office websites contain old data or redirect users to non-existing websites. Needless to say, the information is shattered across websites of multiple offices. For online submission of the trade license application, proprietary software must be downloaded. The company registration form is accessible online, but all information is filled manually as strings anyway, and it must be printed and delivered in person. In conclusion, the overall user experience when registering a company is very poor.

### 4.3 Conclusion

The following table summarizes the impacts of the proposed model that were previously evaluated in detail. Apart from all the quantifiable advantages

Observed parameter	As-is process	To-be process
Number of documents in the process	8	3
Total duration of the process	9 days (up to 24.5 days)	≈ 3 hours
Price of the registration	4330 - 9330 Kč	free
External individuals accessing the documents	9	1
Number of visited websites and needed applications	minimally 5	1
Number of activities in the process model	32	17

Table 4.5: Key observed parameters

that the proposed solution brings, it has a more complex implication. Lowering the cost and the duration of the process and making it clear and easily understandable will attract more people to start a business. That implies the creation of new workplaces and a boost for the whole economy.

---

# Conclusion

The main goal of this thesis was to review blockchain smart contracts and decentralized identity in the context of public administration and propose a way to digitalize one of the administrative processes with the use of blockchain. Theoretical research introduced blockchain technology and concentrated on smart contracts and decentralized identity. Limitations of using smart contracts were addressed with particular care to avoid common mistakes when designing the solution. Furthermore, research on the possible use of blockchain in the public sector was conducted and review of blockchain projects run by governments was presented.

In the practical case study, we have chosen the company registration process for digitalization. The process was first reviewed in general, together with the state of its digitalization in the world. We created a BPMN model capturing the as-is state of the process in Czechia. To-be model of the process was designed in DasContract language. We designed a proposal for the communication model of the process and the data model for the smart contract. The skeleton of the smart contract was generated using the DasContract editor. We also summarized essential prerequisites for adopting the proposed model.

The second chapter of the practical part evaluated the proposed solution compared to the current state of the process. Quality Evaluation Framework was chosen to evaluate different quality dimensions of the process. We considered the performance, efficiency, permissibility and user-friendliness of the process. The evaluation showed considerable improvement in the process. We managed to shorten the process by 95% and cut the paperwork by five no longer needed documents. Administrative costs of the process were lowered by removing the participation of multiple officers.

Digitalization of the company registration through blockchain will significantly simplify the process and boost the number of created companies. Since this thesis presented mainly the concept of digitalizing the process, ways of its implementation should still be explored. Creating an oracle centralizing data from public registers will also be an important challenge for further research.



---

## Bibliography

- [1] Státní správa a European Business Enterprise a.s. Druhy Úřadů. [Online], 2000/2022, accessed 2022-03-23. Available from: [https://www.statnisprava.cz/rstsp/ciselniky.nsf/druhy\\_uradu](https://www.statnisprava.cz/rstsp/ciselniky.nsf/druhy_uradu)
- [2] Redakce ISVS.CZ. Jaký Je Stav Digitalizace Veřejné Správy v České Republice? [Online], 2021, accessed 2022-03-23. Available from: <https://www.isvs.cz/jaky-je-stav-digitalizace-verejne-spravy-v-ceske-republice/>
- [3] Digitální Česko. Digitální Česko. [Online], 2019, accessed 2022-03-23. Available from: <https://www.digitalnicesko.cz>
- [4] Rekonstrukce státu. Digitalizace Státu. [Online], 2021, accessed 2022-03-23. Available from: <https://www.rekonstrukcestatu.cz/temata/prosazujeme-protikorupcni-zakony/digitalizace>
- [5] Swan, M. *Blockchain: Blueprint for a New Economy*. O'Reilly, first edition edition, 2015, ISBN 978-1-4919-2049-7.
- [6] Gates, M. *Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money*. Wise Fox Publishing, 2017, ISBN 978-1-5470-9068-6.
- [7] Werbach, K. *The Blockchain and the New Architecture of Trust*. Information Policy Series, MIT Press, 2018, ISBN 978-0-262-03893-5.
- [8] Singhal, B.; Dhameja, G.; et al. *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Apress, 2018, ISBN 978-1-4842-3443-3.
- [9] Fowler, H. Consensus Mechanisms. [Online], 2022, accessed 2022-03-13. Available from: <https://ethereum.org/en/developers/docs/consensus-mechanisms/>

- [10] Chaudhry, N.; Yousaf, M. M. Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, IEEE, 2018, ISBN 978-1-5386-9564-7, pp. 54–63, doi:10.1109/ICOSST.2018.8632190. Available from: <https://ieeexplore.ieee.org/document/8632190/>
- [11] Millman, R.; Kelly, L. J. What Is Ethereum 2.0 and Why Does It Matter? [Online], 2021, accessed 2022-03-14. Available from: <https://decrypt.co/resources/what-is-ethereum-2-0>
- [12] Mingxiao, D.; Xiaofeng, M.; et al. A Review on Consensus Algorithm of Blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, 2017, ISBN 978-1-5386-1645-1, pp. 2567–2572, doi:10.1109/SMC.2017.8123011. Available from: <http://ieeexplore.ieee.org/document/8123011/>
- [13] DCX Learn. Proof of Work vs Proof of Stake - All Differences You Need to Know. [Online], 2020, accessed 2022-03-31. Available from: <https://dcxlearn.com/blockchain/proof-of-work-vs-proof-of-stake-vs-delegated-proof-of-stake-the-3-most-important-consensus-protocols-compared/>
- [14] Laurence, T. *Blockchain for Dummies*. For Dummies, John Wiley & Sons, Inc, second edition, 2019, ISBN 978-1-119-55501-8.
- [15] Pilkington, M. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*, Edward Elgar Publishing, 2016, pp. 225–251.
- [16] Parizo, C. What Are the 4 Different Types of Blockchain Technology? [Online], 2021, accessed 2022-03-24. Available from: <https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology>
- [17] Cummings, S. The Four Blockchain Generations. [Online], 2019, accessed 2022-03-06. Available from: <https://medium.com/the-capital/the-four-blockchain-generations-5627ef666f3b>
- [18] Ante, L. Smart Contracts on the Blockchain – A Bibliometric Analysis and Review. *Telematics and Informatics*, volume 57, 2021: p. 101519, ISSN 07365853, doi:10.1016/j.tele.2020.101519. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0736585320301787>
- [19] Dheeraj Vaidya; Wallstreetmojo Editorial Team. Smart Contracts. [Online], 2021, accessed 2022-04-05. Available from: <https://www.wallstreetmojo.com/smart-contracts/>



- 
- [20] The Shrimpy Team. The Best Smart Contract Platforms. [Online], 2021, accessed 2022-02-24. Available from: <https://academy.shrimpy.io/post/the-best-smart-contract-platforms>
- [21] Dickens, S. Will Cardano's Smart Contracts Ever Become as Popular as Ethereum? [Online], 2021, accessed 2022-02-24. Available from: <https://finance.yahoo.com/news/cardano-smart-contracts-ever-become-111046481.html>
- [22] Cointelegraph. A Deep Dive into the 5 Popular Smart Contract Development Platforms and Their Comparison. [Online], 2018, accessed 2022-04-05. Available from: <https://cointelegraph.com/blockchain-for-beginners/a-deep-dive-into-the-5-popular-smart-contract-development-platforms-and-their-comparison>
- [23] Antonopoulos, A. M.; Wood, G. *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly, first edition, 2019, ISBN 978-1-4919-7194-9.
- [24] Chainlink. Chainlink Documentation. [Online], 2017, accessed 2022-04-08. Available from: <https://docs.chain.link/docs/>
- [25] Collins, P. What Is a Blockchain Oracle? [Online], 2020, accessed 2022-04-08. Available from: <https://betterprogramming.pub/what-is-a-blockchain-oracle-f5ccab8dbd72>
- [26] Wu, B.; Zou, Z.; et al. *Learn Ethereum: Build Your Own Decentralized Applications with Ethereum and Smart Contracts*. Packt, 2019, ISBN 978-1-78995-411-1.
- [27] Bennett, M. Predictions 2021: Blockchain Is A Tale Of Two Speeds. [Online], 2020, accessed 2022-02-06. Available from: <https://www.forrester.com/blogs/predictions-2021-blockchain-is-a-tale-of-two-speeds/>
- [28] Tsankov, P.; Dan, A.; et al. Securify: Practical Security Analysis of Smart Contracts. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2018, ISBN 978-1-4503-5693-0, pp. 67–82, doi:10.1145/3243734.3243780. Available from: <https://dl.acm.org/doi/10.1145/3243734.3243780>
- [29] Luu, L.; Chu, D.-H.; et al. Making Smart Contracts Smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2016, ISBN 978-1-4503-4139-4, pp. 254–269, doi:10.1145/2976749.2978309. Available from: <https://dl.acm.org/doi/10.1145/2976749.2978309>

## BIBLIOGRAPHY

---

- [30] Greenspan, G. Why Many Smart Contract Use Cases Are Simply Impossible. [Online], 2016, accessed 2022-02-22. Available from: <https://www.coindesk.com/markets/2016/04/17/why-many-smart-contract-use-cases-are-simply-impossible/>
- [31] Hornáčková, B. Použití Blockchain Smart Contracts v Metodice DEMO. Available from: <https://dspace.cvut.cz/bitstream/handle/10467/74045/F8-DP-2018-Hornackova-Barbora-thesis.pdf>
- [32] Jenks, T. Top 4 Misconceptions about Ethereum Smart Contracts. [Online], 2018, accessed 2022-02-22. Available from: <https://www.blockchainbeach.com/top-4-misconceptions-about-ethereum-smart-contracts/>
- [33] Allen, C. The Path to Self-Sovereign Identity. [Online], 2016, accessed 2022-04-01. Available from: <https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/>
- [34] Grech, A.; Sood, I.; et al. Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. *Frontiers in Blockchain*, volume 4, 2021: p. 616779, ISSN 2624-7852, doi:10.3389/fbloc.2021.616779. Available from: <https://www.frontiersin.org/articles/10.3389/fbloc.2021.616779/full>
- [35] damienbod. Verify Vaccination Data Using Zero Knowledge Proofs with ASP.NET Core and MATTR. [Online], 2021, accessed 2022-01-20. Available from: <https://damienbod.com/2021/05/31/verify-vaccination-data-using-zero-knowledge-proofs-with-asp-net-core-and-mattr/>
- [36] Mazúchová, S. Blockchain Umí Víc Než Jen Kryptoměny, Leč Evropa Zaspala, Míni Šéf Startupu. [Online], 2021, accessed 2021-11-01. Available from: [https://www.idnes.cz/ekonomika/podniky/tatum-startup-blockchain-technologie-kryptomeny.A211029\\_135450\\_ekoakcie\\_maz](https://www.idnes.cz/ekonomika/podniky/tatum-startup-blockchain-technologie-kryptomeny.A211029_135450_ekoakcie_maz)
- [37] Tomáš, B. Decentralizovaná Identita v Decentralizovaných Aplikacích Jazyka DasContract. 2021, accessed 2022-01-31. Available from: [https://dspace.cvut.cz/bitstream/handle/10467/94500/F8-DP-2021-Bydzovsky-Tomas-DP\\_Bydzovsky\\_Tomas\\_2021.pdf](https://dspace.cvut.cz/bitstream/handle/10467/94500/F8-DP-2021-Bydzovsky-Tomas-DP_Bydzovsky_Tomas_2021.pdf)
- [38] Ly, T. A Complete Mental Model for Ethereum dApp Development. [Online], 2018, accessed 2022-03-22. Available from: <https://medium.com/heartbanklab/a-complete-mental-model-for-ethereum-dapp-development-5ce08598ed0a>

- 
- [39] Frankenfield, J. Decentralized Applications (dApps). [Online], 2021, accessed 2022-03-22. Available from: <https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp>
- [40] Hassan, S.; De Filippi, P. Decentralized Autonomous Organization. *Internet Policy Review*, volume 10, no. 2, 2021, ISSN 2197-6775, doi:10.14763/2021.2.1556. Available from: <https://policyreview.info/glossary/DAO>
- [41] Jentzsch, C. Decentralized Autonomous Organization to Automate Governance. 2016.
- [42] Chohan, U. W. The Decentralized Autonomous Organization and Governance Issues. *SSRN Electronic Journal*, 2017-2021, ISSN 1556-5068, doi:10.2139/ssrn.3082055. Available from: <https://www.ssrn.com/abstract=3082055>
- [43] Thyse, W., MSc. The Decentralized Legal System - The First Framework for Decentralized Law. 2018. Available from: <https://decentralizedlegalsystem.com/whitepaper/>
- [44] Bitnation Pangea. Bitnation Pangea Whitepaper. [Online], 2018, accessed 2022-01-02. Available from: <https://tse.bitnation.co/documents/>
- [45] Xu, M.; Chen, X.; et al. A Systematic Review of Blockchain. *Financ Innov*, volume 5, no. 1, 2019: p. 27, ISSN 2199-4730, doi:10.1186/s40854-019-0147-z. Available from: <https://jfin-swufe.springeropen.com/articles/10.1186/s40854-019-0147-z>
- [46] Tapscott, D.; Tapscott, A. *Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World*. Portfolio / Penguin, 2016, ISBN 978-1-101-98013-2 978-1-101-98015-6 978-0-399-56406-2.
- [47] Government of United Arab Emirates. Blockchain in the UAE Government. [Online], 2021, accessed 2022-04-05. Available from: <https://u.ae/en/about-the-uae/digital-uae/blockchain-in-the-uae-government>
- [48] Treiblmaier, H.; Beck, R. (editors). *Business Transformation through Blockchain: Volume II*. Springer International Publishing, 2019, ISBN 978-3-319-99057-6 978-3-319-99058-3, doi:10.1007/978-3-319-99058-3. Available from: <http://link.springer.com/10.1007/978-3-319-99058-3>
- [49] GovChain. GovChain Project. [Online], 2022, accessed 2022-04-05. Available from: <https://govchain.world>

- [50] European Commission. Experience Cross-Borders Services with EBSI. 2022, accessed 2022-04-05. Available from: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>
- [51] Victoria University Online. Easiest Countries to Start a Business. [Online], 2021, accessed 2022-01-15. Available from: <https://online.vu.edu.au/blog/easiest-countries-start-business>
- [52] Herz, V. Založení s.r.o. Je v Česku Stále Relativně Obtížné, Na Vině Je Byrokracie. [Online], 2021, accessed 2022-04-19. Available from: <https://www.euro.cz/byznys/zalozeni-sro-cena-postup-podminky-1417153>
- [53] Statista. Median Number of Days It Takes to Complete the Registration of a Firm in European Countries in 2019. [Online], 2019, accessed 2022-04-20. Available from: <https://www.statista.com/statistics/879739/average-time-to-start-a-company-in-eu-countries/>
- [54] World Bank. Time Required to Start a Business (Days). [Online], 2019, accessed 2022-04-20. Available from: [https://data.worldbank.org/indicator/IC.REG.DURS?name\\_desc=false](https://data.worldbank.org/indicator/IC.REG.DURS?name_desc=false)
- [55] Ministry of Foreign Affairs of Denmark. How to Set Up Business in Denmark. [Online], 2021, accessed 2022-04-20. Available from: <https://investindk.com/our-services/how-to-set-up-a-business-in-denmark>
- [56] Republic of Estonia e-Residency. Start a Company. [Online], 2021, accessed 2022-04-20. Available from: <https://www.e-resident.gov.ee/start-a-company/>
- [57] Act Passed by the Parliament of Czechia. On Commercial Companies and Cooperatives (Business Corporations Act). [Online], 2012, accessed 2022-04-12. Available from: <http://obcanskyzakonik.justice.cz/images/pdf/Business-Corporations-Act.pdf>
- [58] Janoušek, M. Založení s.r.o. v Roce 2014 – Postup pro Založení Společnosti s Ručením Omezeným. [Online], 2014. Available from: <http://www.ceve.cz/cs/blog/jak-zalozit-sro-v-roce-2014/>
- [59] Ofigo. Kompletní Založení s.r.o. Online Za 15 Minut. [Online], 2021, accessed 2022-03-23. Available from: <https://www.ofigo.cz/zakladani-firem/>
- [60] Založ Firmu. Zakládání Nových Firem Online. [Online], 2021, accessed 2022-03-23. Available from: [https://www.zalozfirmu.cz/?aid=0135913289&gclid=CjwKCAjwx46TBhBhEiwArA\\_](https://www.zalozfirmu.cz/?aid=0135913289&gclid=CjwKCAjwx46TBhBhEiwArA_)

- DjJ7A0b3E5ibufrJD7PQUwSFMHIRQGSh1ErNSgiIAKwg\_\_Bq\_  
dE3KZR0CGsoQAvD\_BwE
- [61] Komerční Banka. Firma pro Vás. [Online], 2021, accessed 2022-03-23. Available from: <https://www.kb.cz/cs/podnikatele-a-male-firmy/ostatni-sluzby/firma-pro-vas>
- [62] Registr Živnostenského Podnikání. Náповěda pro Elektronické Podání Prostřednictvím Jednotného Registračního Formuláře (JRF). [Online], 2021, accessed 2022-03-20. Available from: <https://www.rzp.cz/epo/cs/napoveda>
- [63] Profant, O. Firma Za 1 Den - Pirátský Návrh Zjednodušení Podnikání. [Online], 2019, accessed 2022-04-19. Available from: <https://www.profant.eu/2019/firma-za-1-den.html>
- [64] Skotnica, M.; Pergl, R. Das Contract - A Visual Domain Specific Language for Modeling Blockchain Smart Contracts. In *Advances in Enterprise Engineering XIII, Lecture Notes in Business Information Processing*, volume 374, edited by D. Aveiro; G. Guizzardi; J. Borbinha, Springer International Publishing, 2020, ISBN 978-3-030-37932-2 978-3-030-37933-9, pp. 149–166, doi:10.1007/978-3-030-37933-9\_10. Available from: [http://link.springer.com/10.1007/978-3-030-37933-9\\_10](http://link.springer.com/10.1007/978-3-030-37933-9_10)
- [65] Skotnica, M.; Aparício, M.; et al. Process Digitalization Using Blockchain: EU Parliament Elections Case Study:. In *Proceedings of the 9th International Conference on Model-Driven Engineering and Software Development*, SCITEPRESS - Science and Technology Publications, 2021, ISBN 978-989-758-487-9, pp. 65–75, doi:10.5220/0010229000650075. Available from: <https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0010229000650075>
- [66] CCMiResearch. DasContract. [Online], 2021, accessed 2022-03-28. Available from: <https://github.com/CCMiResearch/DasContract>
- [67] Heidari, F.; Loucopoulos, P. Quality Evaluation Framework (QEF): Modeling and Evaluating Quality of Business Processes. *International Journal of Accounting Information Systems*, volume 15, no. 3, 2014: pp. 193–223, ISSN 14670895, doi:10.1016/j.accinf.2013.09.002. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1467089513000389>
- [68] Hejná, V. Jak Založit Společnost s Ručením Omezeným a Kolik to Stojí? [Online], 2020, accessed 2022-03-05. Available from: <https://www.e15.cz/finexpert/vydelavame/jak-zalozit-spolocnost-s-rucenim-omezenym-a-kolik-to-stoji-1367417>



## Acronyms

**BPMN** Business Process Modeling Notation

**CA** Contract Account

**dApp** Decentralized Application

**DAO** Decentralized Autonomous Organization

**DID** Decentralized Identifier

**DLT** Distributed Ledger Technology

**EBSI** European Blockchain Services Infrastructure

**EOA** Externally Owned Account

**EVM** Ethereum Virtual Machine

**HQ** Headquarters

**QEF** Quality Evaluation Framework

**SC** Smart Contract





# Figures and Tables

Most-cited articles on smart contracts.

Article	Citations	Title	Journal
<a href="#">Christidis and Devetsikiotis (2016)</a>	517	Blockchains and Smart Contracts for the Internet of Things	IEEE Access
<a href="#">Xia et al. (2017)</a>	99	MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain	IEEE Access
<a href="#">Novo (2018)</a>	92	Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT	IEEE Internet of Things Journal
<a href="#">Dorri et al. (2017)</a>	83	BlockChain: A Distributed Solution to Automotive Security and Privacy	IEEE Communications Magazine
<a href="#">Reyna et al. (2018)</a>	81	On blockchain and its integration with IoT. Challenges and opportunities	Future Generation Computer Systems
<a href="#">Wang et al. (2018)</a>	81	Blockchain challenges and opportunities: a survey	International Journal of Web and Grid Services
<a href="#">Peters and Panayi (2016)</a>	68	Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money	Banking Beyond Banks and Money (book chapter)
<a href="#">Zhang and Wen (2017)</a>	63	The IoT electric business model: Using blockchain technology for the internet of things	Peer-to-Peer Networking and Applications
<a href="#">Pop et al. (2018)</a>	63	Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids	Sensors
<a href="#">Dinh et al. (2018)</a>	59	Untangling Blockchain: A Data Processing View of Blockchain Systems	IEEE Transactions on Knowledge and Data Engineering
<a href="#">Sun et al. (2016)</a>	54	Blockchain-based sharing services: What blockchain technology can contribute to smart cities	Financial Innovation
<a href="#">Kshetri (2017)</a>	51	Blockchain's roles in strengthening cybersecurity and protecting privacy	Telecommunications Policy
<a href="#">Risius and Spohrer (2017)</a>	45	A Blockchain Research Framework - What We (don't) Know, Where We Go from Here, and How We Will Get There	Business & Information Systems Engineering
<a href="#">Dai and Vasarhelyi (2017)</a>	44	Toward Blockchain-Based Accounting and Assurance	Journal of Information Systems
<a href="#">Saberi et al. (2019)</a>	43	Blockchain technology and its relationships to sustainable supply chain management	International Journal of Production Research
<a href="#">Dagher et al. (2018)</a>	42	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	Sustainable Cities and Society
<a href="#">Werbach and Cornell (2017)</a>	36	Contracts Ex Machina	Duke Law Journal
<a href="#">Kim and Laskowski (2018)</a>	36	Toward an ontology-driven blockchain design for supply-chain provenance	Intelligent Systems in Accounting Finance & Management
<a href="#">Zhang et al. (2018)</a>	35	FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data	Computational and Structural Biotechnology Journal
<a href="#">Brandstätt et al. (2011)</a>	32	Locational signals to reduce network investments in smart distribution grids: What works and what not?	Utilities Policy

Citation data refers to Web of Science (January 2020).

Figure B.1: Most cited articles on smart contracts [18]

B. FIGURES AND TABLES

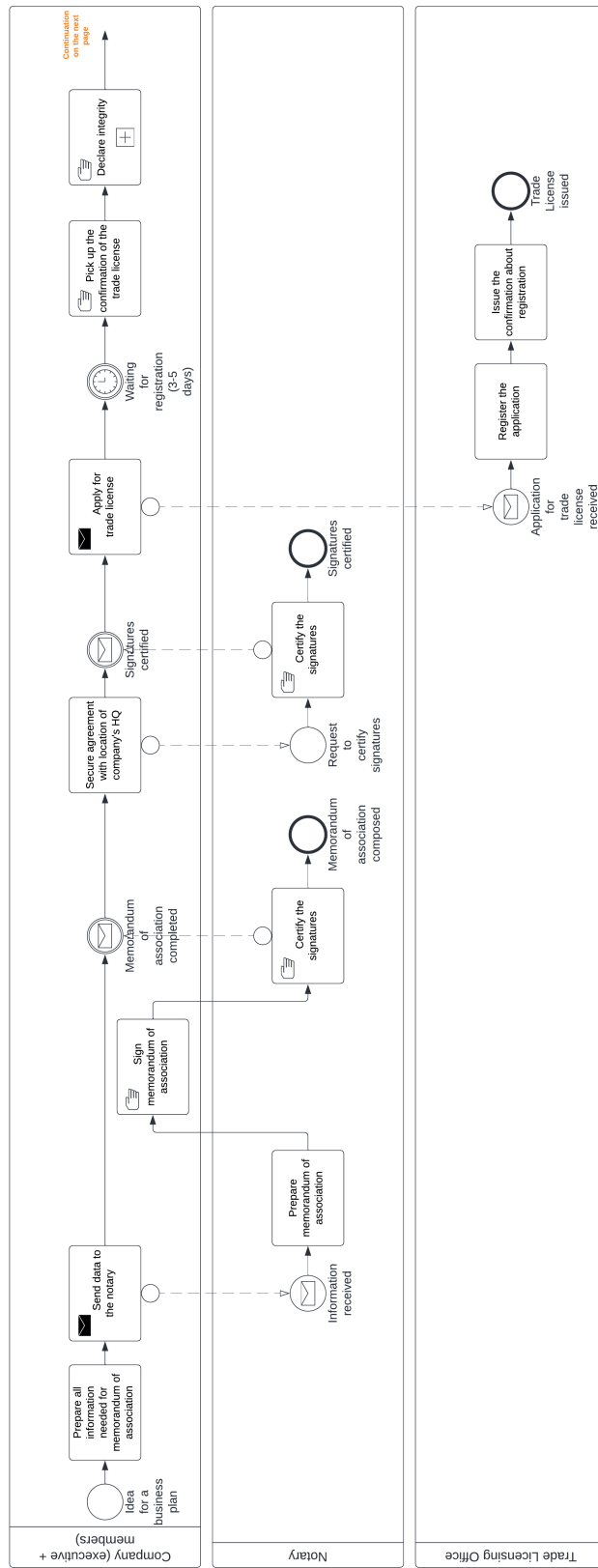


Figure B.2: As-is model of company registration part I

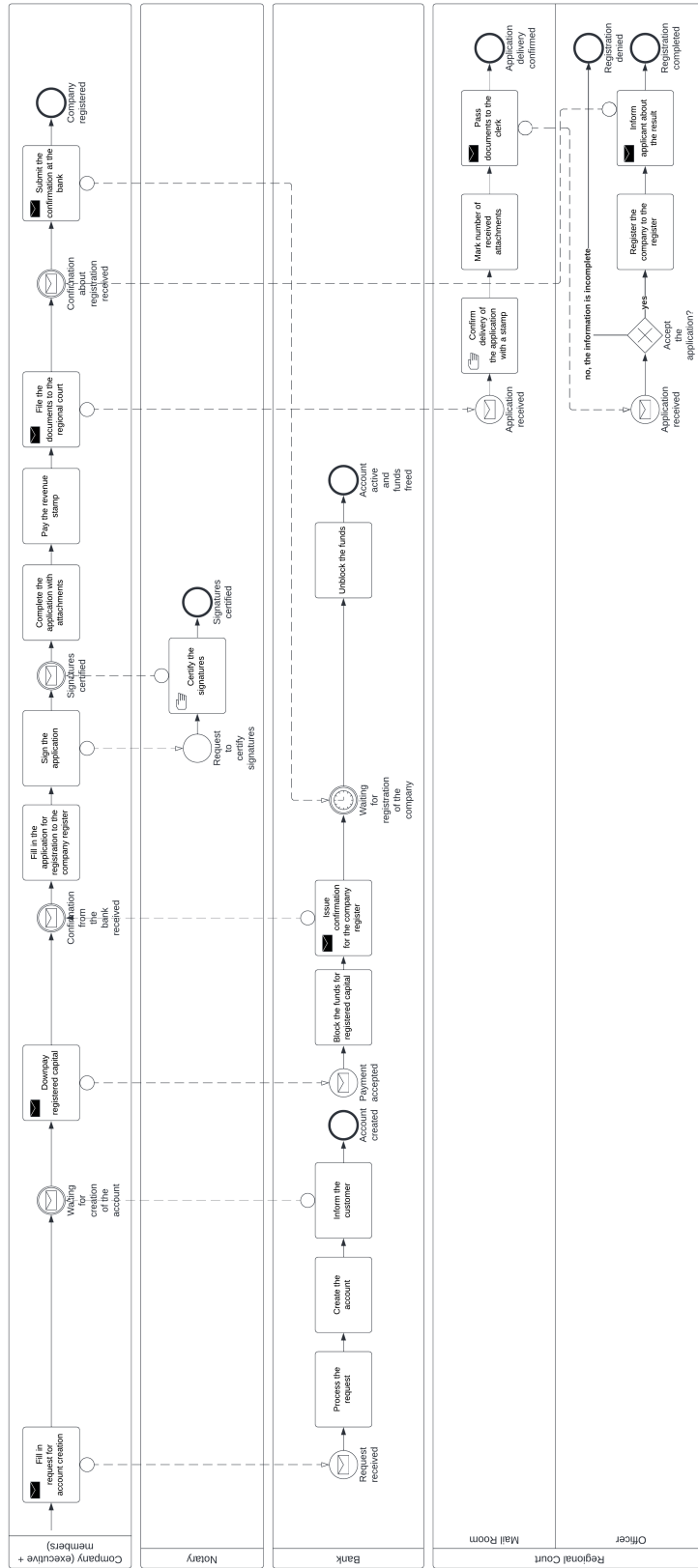


Figure B.3: As-is model of company registration part 2

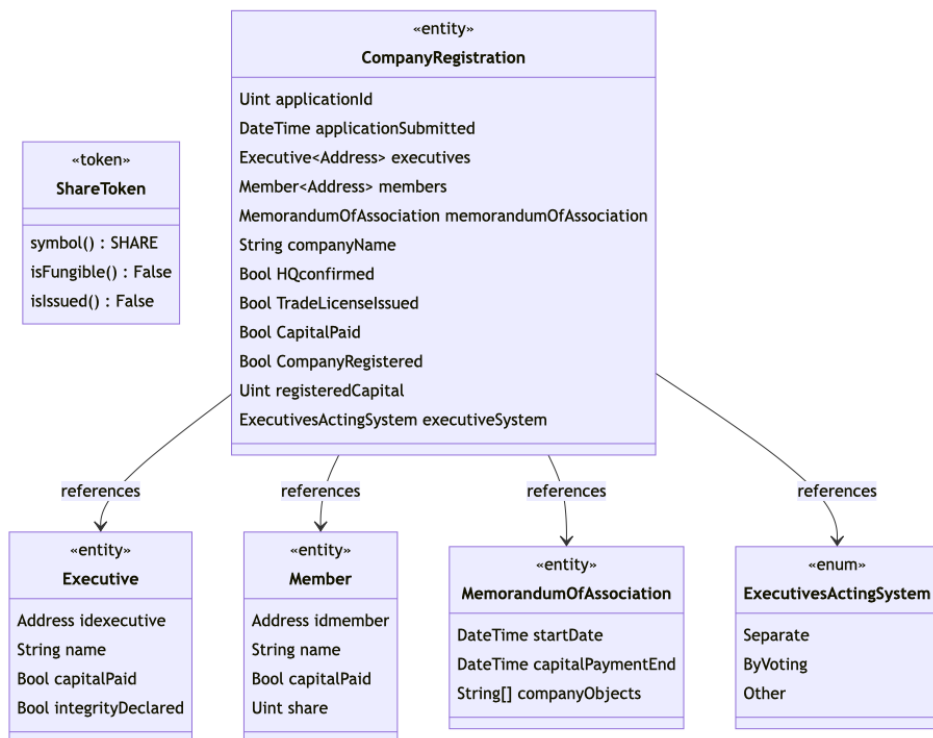


Figure B.4: Data model of the smart contract

---

## Contents of Enclosed SD Card

readme.txt	.....	the file with SD contents description
src	.....	the directory of source codes
├ thesis	.....	the directory of L <sup>A</sup> T <sub>E</sub> X source codes of the thesis
├ models	.....	the directory of models from the case study
└ smart-contract	.....	the code of the smart contract skeleton
text	.....	the thesis text directory
└ DP_Krbilova_Katarina.2022.pdf	.....	the thesis text in PDF format