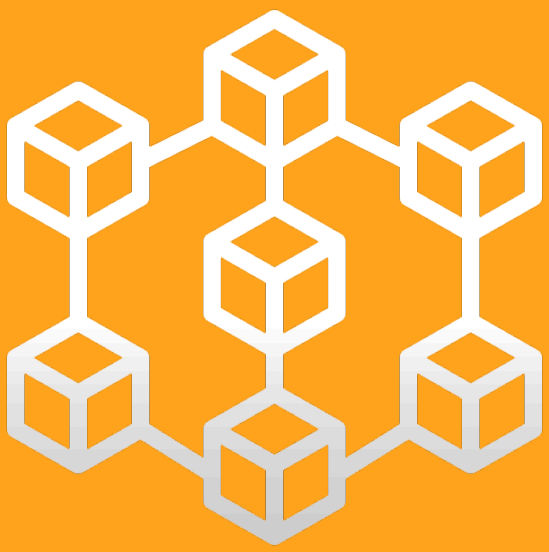
The Effects of Blockchain Technology on E-government Services



MSc International Public Administration

Nina Martin Da Silva
468044

Supervisor: Freek de Haan

Second Reader: Jasper Eshuis

Word Count: 19.984

Erasmus School of Social and Behavioural Sciences

Abstract

The use of blockchain technology is scarce among public services. The existing literature draws on the potential positive effects of blockchain implementation in the public sector. Indeed, various author claim that the technology can increase efficiency, trust and security in public services. Yet, governments remain cautious. The skepticism is mainly linked to a lack of regulations surrounding the topic. Furthermore, there are too little use cases to predict the real positive and negative affects the technology could have on public services, as well as how the public would react or utilise the technology. In this regard, taking into account the theoretical gap, this thesis aims to not only contribute to the existing literature by showing analysing use cases that show how blockchain technology affects e-government services but also identify the factors for successful of non-successful implementations of the technology in order to set the ground for future research but also identify the ideal parameters for blockchain technology to reach its full potential.

The study takes a look at five different cases in order to build upon the existing theories concerning the effects of blockchain technology on e-government services. For each case, a direct active participant in the project is interviewed and provide substantial information on how the technology was implemented and the effects it had on its respective use case. The study uses pattern matching analysis and cross-case analysis to derive the main findings.

Table of Contents

Index of Abbreviation

DEG	Digital Era Governance
DLT	Distributed Ledge Technology
EC	European Commission
GDPR	General Data Protection Regulation
G2B	Government to Business
G2G	Government to Government
G2C	Government to Citizen
G2E	Government to Employee
ICT	Information and Communication Technology
IoT	Internet of Things
ML	Machine Learning
NPM	New Public Management
OECD	Organisation for Economic Co-operation and Development

I - Introduction

1.1 Problem Statement

While still being a relatively new feature within the private sector, Blockchain technology is considered an unknown for the public sector. Berryhill, Bourgery and Hanson (2018) recently shed light on the subject by publishing a paper for the Organisation for Economic Co-operation and Development (OECD) about the use of blockchain technology within the public sector. The former utilise the definition from the World Economic Forum to define blockchain technology: "*currently, most people use a trusted middleman such as a bank to make a transaction. But Blockchain networks allow consumers and suppliers to connect directly, removing the need for a third party*" (Hutt, 2016; Berryhill et al., 2018; 10). Blockchain technologies are presented in such a way that society expects breakthroughs with high potential for the public sector (Cartier & Ubacht, 2018). Indeed, the authors Cartier and Ubacht (2018; 1), state that "*blockchain has the potential to make government operations more efficient by improving the delivery of public services and increasing trust in public sectors*". The idea of blockchain technology implementation within e-government, specifically, is linked to the expectations of government integrity, data quality, transparency, anti-corruption, increase in trust, privacy and security (Cartier & Ubacht, 2018; 2). The question remains, if blockchain technology comes with such promises for the public sector, how can blockchain technology in the field of public e-services reach its full potential? The answer the does not come easy. Indeed, a number of scholars, namely Batubara et al. (2018) and Peck (2017), agree with the fact that the concept is not only unknown but also controversial for the few who dare to adventure within the realm of blockchain technology implementation in the public sector. Reason for the lack of attention on the topic is due to the fact that a big majority of academic research relating to the use of blockchain focuses on its applications in the financial sector; such as cryptocurrencies like Bitcoin or Ethereum (Cartier & Ubacht, 2018). In fact, Ølnes and Jansen (2017) highlight the importance of interdisciplinary research on the topic of blockchain implementation for government bodies. A statement that Batubara et al. (2018) agree with as for their systematic literature review on the challenges of blockchain adoption in e-governments, from a pool of more than 300 articles relating to the subject, only 21 focused on blockchain adoption specifically in relation to e-government and e-government services. That is also a reflection of the general population as media sources tend to also present blockchain technologies in relation to cryptocurrencies (Cartier & Ubacht, 2018).

While the above statements explain why the idea of blockchain use in the public sector remains widely unknown by the general public, it is still relevant to look at the ongoing debate between the knowledgeable few. Indeed the topic of blockchain is considered controversial in both private and public sector (Lindman, et al 2017). This is due to certain blockchain use cases, specially linked to cryptocurrencies, that have shown how blockchain technology can have negative effects on the world (Lindman, et al 2017). As Lineman et al. (2017) state, one effect that is often mentioned by several scholars but also by the mainstream media is the energy consumption that tags along the technology. For context; the mining of Bitcoin, one of the most known cryptocurrencies, consumes an estimated 150 terawatt-hours of electricity on an annual basis (Hinsdale, 2022). That amount is higher than the consumption of an entire country like Argentina that has a population of 45million (Hinsdale, 2022). Nonetheless, the limitations do not stop there. Indeed, other concerns arise, such as questions on security, the regulations and governance, but also awareness and understanding surrounding the technology (Lindman, et al 2017; Boireau, 2018). Indeed, the linked to the question of regulations surrounding the blockchain and acknowledging the typical decentralised nature of the technology, Boireau, 2018 mentions that security concerns are at the heart of arguments against blockchain technology adoption in both the public and private sector. While no one, as of today, has been able to hack the system without getting caught, it does not give an insurance that it will not happen in the future (Boireau, 2018). With lack of regulations concerning the technology, it is normal to take into account this security concern when looking at blockchain adoption, specially within the public sector. Nonetheless, this has not stopped governments from trying. Indeed, the governments of Austria, Slovenia, Sweden and others have introduced pilot projects to test the benefits of the technology in providing safe, efficient and trustworthy e-government services. From online identity to credential checks or property transactions, governments have made a step towards the implementation of blockchain while being mindful of the potential concerns. These specific examples will be expanded upon in the next chapters.

The ongoing debate on the effects of blockchain in combination with the lack of research on the topic of the technology's use in the public sector provides an interesting basis for research.

1.2 Research Focus

Research Question

In light of the lack of research on the topic of blockchain use in the public sector and in particular lack of research on the implementation of blockchain technology within e-government services, the

research at hand focuses on understanding how blockchain works within e-government and more specifically, understanding the effects of blockchain on public services offered through e-governance. This allows for the tackling of the problem statement and the making of a contribution within the debate of how controversial blockchain really is. In this regard, the research aims to answer the following question:

How does blockchain technology affect e-government services?

To facilitate the approach to the research question, it becomes relevant to introduce the following subquestions:

1. *What does blockchain mean in the context of e-government?*
2. *What are the factors contributing to a successful implementation of blockchain technology on e-government services?*

Social Relevance

As priorly mentioned, blockchain technology is a novice and unknown technology. This can cause scepticism to change and adoption not only from a government perspective but also from the public when it comes to citizen adoption and acceptance. Hou (2019) emphasises that technological immaturity is common for all new technologies and that it should not be the base for decision making on adoption or use. Being less fearful to try new technologies, processes or structures drives us forward as a society, but also makes us more prone to positive change and innovation on a governmental but also citizen level. Unfortunately, various research confirms that governments are not prone and programmed to facilitate change and push for the new and unknown (Tiron-Tudor, 2021). A theory that New Public Management also contributes towards by demonstrating traditional governments to be too rigid and less flexible and acceptant to change.

However, it is important to acknowledge that a new technology can also bring more harm that good. Even if the technical aspects of the technology are promising, the impact on society and the world, is not necessarily a positive one. In this regard, it is important to remember that blockchain technology remains a controversial topic in light of security, regulatory, economic, environmental and governance concerns.

In light of these visions, this thesis hopes to contribute to the literature on blockchain technology use in the public sector, but also to contribute to the debate on the technology by providing empirical arguments on blockchain's effects within public e-services. By doing so, it pushes towards questioning the stigma around this new technology by freely empirically analysing real impacts of blockchain technology on our society. Therefore allowing both governmental organisations and citizens to make up their mind based on existing applications rather than theoretical potentials.

Scientific Relevance

Literature has shown that the existing body of research looking into blockchain technology has a tendency to focus on the application of cryptocurrencies rather than its adoption, impacts and benefits in other contexts, such as in the context of e-governance (Yli-Huumo et al., 2016; Ølnes et al., 2017; Batubara et al., 2018). Adding on, various academic authors have stressed the importance of research focusing on blockchain use in e-governance as that could become the step towards improving public services, but also helping solve governmental challenges like corruption, fraud or inefficiency (Ølnes et al., 2017; Batubara et al., 2018). Some literature shows that the characteristics of blockchain technology allow for an increase of trust between stakeholders, but also an increase of efficiency in public processes through the automation of mundane administrative tasks (Batubara et al., 2018, Berryhill et al., 2018). Unfortunately, these statements are hard to prove due clear lack of empirical research, therefore making it hard to map out the direct impacts of blockchain technology use in e-government services. Furthermore, while theoretical impacts have been lightly considered, there is no guide in what designing a successful use of blockchain technology for e-government services. This is due to an absence of research assessing the factors that contribute towards a successful adoption and application of blockchain technology in e-governance. In fact, Batubara et al. (2018) has called for further research on blockchain technology adoption for governance, not only focusing on impacts but also in design variables. Considering the above arguments, this thesis bridges the knowledge and research gap linked to the impacts and design variables of blockchain technology use within e-government services. This claim will be further elaborated and argued upon in the following section.

II - Literature Review

The following chapter therefore aims to establish familiarity and understanding of the current body of research concerning the application of blockchain technology in e-government services. In this regard it will look at the theoretical definition of e-government as well as understand its impact on the public sector. Following, this thesis will uncover the literature on blockchain technology to understand what it entails and the attractiveness it implies for e-government services. Last but not least, we will identify the relevance of blockchain technology in the public sector. Finally, we will put forward the gap in prior research concerning the matter at hand and how this thesis contributes towards bridging the latter.

2.2 Analysing the concept of e-government

2.2.1 Defining e-government

Fang (2002; pp.2) defines an e-government as 'a continuum from information provision when organisations and public agencies publish static information to the Internet to web interactive communication and e-transactions, and to one-stop integrated virtual governmental services''. In this regard, the concept of e-government puts the public sector on a path towards technological innovation but also government transformation (Fang, 2002). Dunleavy et al., (2005; 2013) link this digital era of governance (DEG) to the reformations introduced in new public management (NPM).

As priorly mentioned, Pollitt (2011) believes that the NPM allows public processes to become decentralised and competitive. The former allows the rigid and strict structures present within bureaucracy to become flexible and allow for the public sector to innovate (Pollitt, 2011). Thanks to these changes, concepts like DEG have been introduced (Pollitt, 2011). It seems that NPM has incentivised public officers to shift towards a citizen-focused design for public processes. Therefore consolidating the idea that DEG became the main product of NPM (Pollitt, 2011). More recently, the European Commission (EC) (2019) mentioned the multiple benefits of including e-government services within public administration. E-governance seems to increase efficiency, transparency and accessibility to political involvement (EC, 2019). Authors Fang (2002) and Cartier and Bélanger (2005) have found that e-government has the potential to become the necessary tool for citizens to be more in touch with the public sector. Indeed, even the United Nations defines digital transformation from the public sector as a more effective and efficient manner to deliver public

services through the use of Information and Communication Technology (ICT). For the sake of clarity, the research at hand refers to e-government as the use of ICT by governmental sectors in order to improve the user-experience of citizens in order to increase transparency, efficiency and public accountability. In this regard, e-government becomes the tool and the incentive for the transformation and improvement of public processes, in which the use of e-government ICTs allows the public sector to deliver constantly improved services to citizens.

2.2.2 Types of e-government

As the concept of e-government can remain broad, it becomes relevant to look the different forms it can take (Basel Institute of Governance, 2017). Indeed, different categorised have been defined based on the different types of interactions an e-government can have. The existing established categories are; Government to Business (G2B), Government-to-Government (G2G), Government-to-Citizen (G2C) and Government-to-Employee (G2E) (Basel Institute of Governance, 2017). Government to Business refers to governments buying products from the private sector or utilising private services in order to complete a public mean (Basel Institute of Governance, 2017). For e-government processes, they specifically look into reducing handling time, gathering information as well as storing efficiency between businesses and governments (Basel Institute of Governance, 2017). Evans and Yes (2006) went further into the topic and mention that G2B has a strong focus on cost-reduction and regulatory requirements.Government to Government type looks into the sharing of information among two different governments bodies (Basel Institute of Governance, 2017). For e-government, the focus is on making the process of information sharing more efficient. Government to Citizen refers to the communication between government and its citizens, but also takes a deep dive into the processes and public services towards citizens (Evans and Yen, 2006). In this regard, e-government focused on the communicative abilities, efficiency and transparency of public processes (Evans and Yen, 2006). Finally, Government to Employee looks at the relationship between a government and its internal sector, departments, including public officers, or namely, employees (Aiolfi, Basel Institute of Governance, 2017). This thesis will take a stronger focus on the relationship between G2C, namely, government and citizens.

2.2.3 Impact on the public sector

Until now the body literature focused on the potential of e-government rather than its current impact. Indeed, authors have claimed that e-government is aimed at increasing efficiency in public

processes, this sub-section aims to review the existing research assessing the impacts on e-government on the public sector.

Researchers, Sachan et al., (2018) have examined the impact of e-government process by basing on on user, namely citizen, satisfaction. By analysing the data gathered from 197 respondents, they found that through e-government processes, citizen felt that that the overall public process improved (Sachan et al., 2018). With a focus on the technological capabilities embedded in a government website, the study provides evidence that technological capability became an important factor in determining e-government service quality and e-government user satisfaction (Sachan et al., 2018). It seemed that citizens, in ages to be able to manoeuvre simple modern technology, found it more practical and above all, time efficient, to complete simple administrative task through e-government services included in government websites, rather than through the traditional way of working (Sachan et al., 2018).

A more profound and more recent systematic literature review on the subject, has been made by MacLean and Titah (2022). Their research is centred around the impacts of e-government from a public value perspective. The motive of their research is centred around the idea that there remains an uncertainty concerning the benefits generated by e-government systems. MacLean and Titah (2022) examine 60 empirical studies focusing on the impacts of e-government. The analysed studies have been sourced from leading public administration and information system journals. While the researchers have acknowledged that it is important to denote that there are many areas in which limited research was available. By classifying the impacts of e-government using the public value theory, the results of their empirical literature review showed that e-government impacted productivity, increase citizen satisfaction and service quality for citizens as well as increased trust in the government body and streamlined communication for citizens. Overall the conclusion of their literature review confirms and supports the older body of literature in stating that e-government seems to improve efficiency in public processes but also increased trust and satisfaction towards the government body in question.

While the switch to digital is core when improving government services for the public, e-governments can't stop there. Mazzucato (2011) author of '*The Entrepreneurial State*' makes an important claim that the crucial role of the government lies in creating the right infrastructure with the right tools and the appropriate rules. Governments around the world have been leading agents for innovative breakthroughs in the public sector, the switch to digital being one. However, the only factor that should remain constant is the creation of strategies for high-growth and the consideration on taking chances on new technologies (Mazzucato, 2011). In this regard, the next section will

introduce one specific technology that is presented as having potential for the public sector, by not only scholars but policy makers; blockchain technology.

2.3 Understanding blockchain technology

2.3.1 What is blockchain technology?

For a big number of enthusiasts, the introduction to blockchain technology can be compared to the rise of the Internet (Rosic, 2017; Berryhill et al., 2018). The authors Berryhill et al. (2018; pp.10) mentioned that it was ‘‘*referred to as a new “trust machine” because of its ability to allow people to interact and conduct transactions even though they may not know each other or have a pre-existing trust-based relationship*’’. Hutt (2016) defines blockchain technology as a network that allows two parties to connect directly. Thus removing the need for a trusted middle man such as a bank in order to make a financial transaction (Hutt, 2016). In more technical terms, blockchain technology acts as a ‘‘*form of distributed ledger technology (DLT) that acts as an open and trusted record (i.e., a list) of transactions from one party to another (or multiple parties) that is not stored by a central authority*’’ (Berryhill et al., 2018; pp.11). DLT is defined as a technology in which record of transactions are ‘‘*spread across multiples sites, countries or institutions, and is typically public. [Transaction] records are stored one after the other in a continuous ledger, but they can only be added when participants [confirm the feasibility and validity of the transaction]*’’ (Berryhill et al., 2018; pp.11; Walport, 2016; Rinearson, 2017).

The principle behind blockchain technology was first introduced by Haber and Stornetta in 1991 through the idea of stamping digital documents in order to prevent their tempering with. Nonetheless, the idea took off when Satoshi Nakamoto (2008), presented the concept in the more recent years. In the words of its own creator; blockchain technology represents the idea that networks enable and allow financial transactions to run instantly without using an intermediary party such as a regulated financial institutions (Nakamoto, 2008).

Alternatively, a copy of each blockchain transaction is stored through each user using blockchain software while connected on a blockchain network, or namely, a node (Berryhill et al., 2018). More clearly, a node refers to a user or a computer connected on a blockchain platform while using a blockchain software (Yaga et al., 2018). The aim of full nodes, or a complete blockchain networks, is to store full copies of blockchain ledgers, to receive data from other nodes, and to transmit the information to other nodes as long as the blockchain has not been tampered with (Yaga et al., 2018).

The important attribute to keep in mind, is that instead of using a central authority such as a bank to maintain a database, all nodes have copies of the ledges (Berryhill et al., 2018). Within the blockchain network, nodes usually review and validate a specific transaction before it can go forward (Berryhill et al., 2018). In this regard, the decentralised system allows for everyone to inspect it, and therefore limits the risks of tampering and increases trust in the technology (Berryhill et al., 2018). Nonetheless, transactions are not always made within multiple nodes. Indeed, there is the possibility to complete individual transactions through cryptography. The former is defined as the "*the act of creating codes that allow data to be kept secret*" (Berryhill et al., 2018; pp.11). Cryptography permits authorised user to convert data into a coded information (Berryhill et al., 2018). In this regard, data can be exchanged without the worry then an unauthorised user would access its contents (Berryhill et al., 2018).

The following section with describe and present a visualisation of how blockchain works by explaining the uniqueness of each block within the chain.

2.3.2 How does Blockchain technology work?

Considering that blockchain is a distributed ledge that is open source, how come it is considered such a trusted source for financial transactions?

Laurence (2017), mentions that every single block within the blockchain holds on to the digital fingerprint of the previous block, making it a chain. This digital fingerprint, also referred to as a digital ID number or hash, is unique to every block, much like our human fingerprints are unique to us (Laurence, 2017). If an authority is in possession of your fingerprints, it can trace where you have been, very much like tracing the hash of a block and getting information about its past. In this regard, a hash links the block to each other by providing information its past and future whereabouts, this way creating a block chain (Laurence, 2017). Figure one represents the blockchain with the visualisation of hashes;

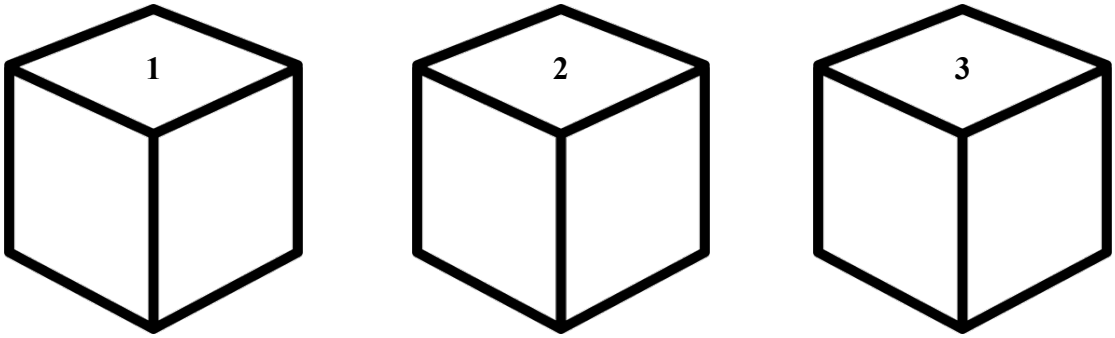


Figure 1: Original blockchain

The best analogy would be that, as a person, if we have your fingerprint, we can link it back to you. By linking it back to you, we will then have information about your genes and we will therefore be able to traces your ancestors and your offsprings even though each of these individuals have unique fingerprints, just like in figure 1. However, if there was a tampering with the genealogical tree, then the biological lineage would be broken and it would be possible to trace the moment in which it happened. Similar within the blockchain as shown in figure 2.

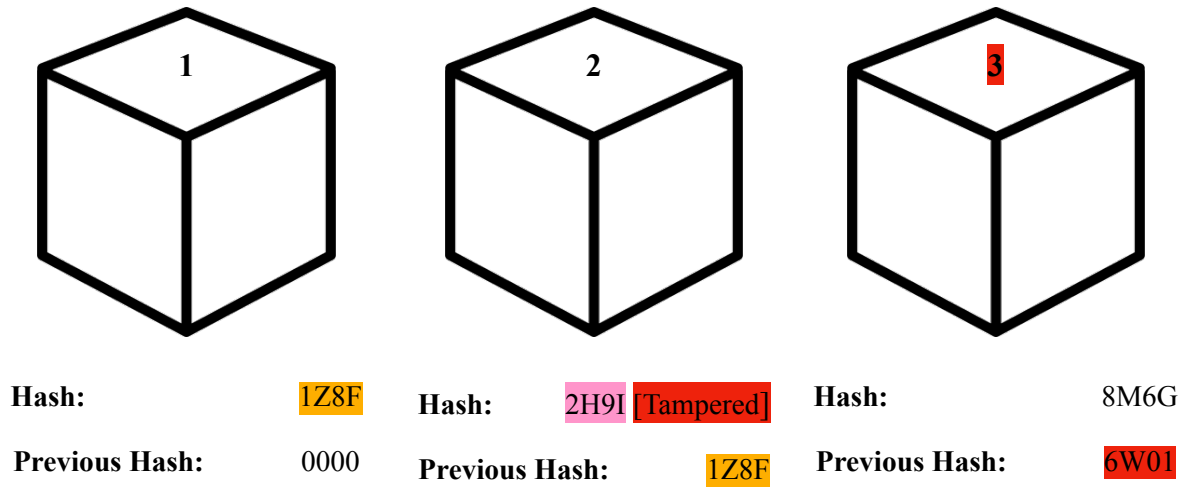


Figure 2: Tampered blockchain

When tampering is present in the blockchain, it is detected and makes all the blocks after the tampering invalid and therefore breaks the blockchain (Laurence, 2017). Tampering within the blockchain is detected due to a consensus mechanisms put in place such as 'Proof of Work' (POW) used in the case of Bitcoin (Nakamoto, 2008). Bitcoin is an example of decentralised digital currency that can be transferred within a blockchain network (Nakamoto, 2008). POW is a consensus mechanism that manages to slow down the creation of blocks within the blockchain, making is an excruciating complex process for tampering (Nakamoto, 2008). POW works the following way; if an individual creates a new block within the blockchain, a notification would be received by all the other nodes participating within that specific blockchain network (Nakamoto, 2008). These nodes then verify that the block contains valid information and that it has therefore not

been tampered with (Nakamoto, 2008). When the verification has been successfully completed, only then all the nodes add the block to their individual blockchain (Nakamoto, 2008). The name of consensus mechanism comes from the fact that multiple nodes have to verify and agree, therefore coming to a consensus, that the block is valid and does not present any tampering.

2.3.2 Types of Blockchains

While the most well known type of blockchain is private, there remains two other types of blockchains (Bashir, 2017). The most relevant for the scope of the research at hand, being the public blockchain, and second, the semi-private blockchain (Bashir, 2017). While these types have some overlapping characteristics, they remain crucially different (Bashir, 2017).

Private blockchains refer to the fact that the blockchain is not open source, and has purposely limited its access to a group of individuals or organisations that have consented in sharing a ledger (Bashir, 2017). Within private blockchains, there is the possibility to have an administrator allocating roles and access-levels among individuals that chose to participate (Bashir, 2017). The fact that this type of blockchain has an extra layer of manual control over the participants prevents even further the possibility of tampering or fraudulent activity within the blockchain (Bashir, 2017). The benefit of a private blockchain lies in the fact that individuals already know and trust each other, which therefore removes the need for consensus mechanisms such as POW, which in return, speeds up the transaction processes within the blockchain (Bashir, 2017).

Public blockchains on the other hand are referred to as permission-less. Therefore meaning that there is no existent hierarchical structure between nodes. This is the case as they are open source and accessible to any node using blockchain software connected to a blockchain network (Bashir, 2017). Their open source characteristic implies that any node can choose to participate in decision making and, for example, consensus mechanisms (Bashir, 2017). One important criteria that the nodes must possess, is all the relevant and required information regarding the status of the ledger in question (Bashir, 2017). Without it, they can’t make an informed decision, and therefore can’t participate in decision making, such as consensus mechanisms (Bashir, 2017). Considering the complexity in attempting to tamper the blockchain without getting caught, as explain in the previous sub-section of this literature review, public blockchain therefore represent a transparent and trust-implying transaction method, specially within the public sector (Bashir, 2017; Berryhill et al., 2018). The main benefit of a public blockchain is that there is no centralised power overseeing the transaction, a very attractive asset for many and what made blockchain so popular among our modern society (Bashir, 2017; Berryhill et al., 2018). On one hand decentralisation attracts curiosity

an interest within the blockchain model that is, 'trustless' (Berryhill et al., 2018). This implies that each node within a decentralised blockchain owns a copy of a distributed ledger, therefore simplifying the verification process, without having to trust a central entity (Bashir, 2017; Berryhill et al., 2018). The fact that nodes do not have to rely on the morale compass of a central authority makes them feel safer against the possibilities of corruption (Berryhill et al., 2018). On the other hand, decentralisation means that there is no reliance in institutional parties, therefore creating concerns from legal and regulatory perspectives. Indeed, nodes do not have the added layer of security when making verifications in the blockchain. If a fraudulent activity were to happen, it would be complex to reach out for help. Nodes therefore have to rely on their own trust in the technology (Berryhill et al., 2018).

Semi-private blockchains are a combination of public and private blockchains (Bashir, 2017). The former include as an open source concept in which any node can enter to ledger, while regulating roles and accessed through a ledger administrator like in private blockchains (Bashir, 2017). This type of blockchain is considered the middle man as it is decentralised like public blockchains but keeps the option to implement permissions like the private type of blockchains (Bashir, 2017). The benefit from these hybrid models is that it can appeal to a wider audience, the blockchain remains to a certain degree 'trustless' but works within a structure with the appearance of having regulations (Bashir, 2017).

This section explained blockchain technology in order to provide an understanding of the characteristics of the technology. The latter are used to explain how blockchain's permissions can be tailored to the networks and potential use cases. The next section will take a deeper dive into the relation of blockchain technology and public services.

2.4 The relevance of blockchain technology for the public sector

2.4.1 An attractive set of features

There are two key features that the blockchain offers, that are yet to be explained, that makes it a specially attractive technology for the public sector: Smart contracts and digital signatures. In a nutshell, these features are faster and more cost effective than traditional contract making as they do not require manual enforcement through third parties (Rosic, 2017). In the previous sections it was possible to see how current literature shows blockchain to be a trust and efficiency driver within a specific community, whether it is public or private. Smart contracts and digital signatures contribute towards this trustworthy environment.

Smart contracts are very similar to traditional hard copy contract as we know them (Rosic, 2017). However, one big factor differentiates them; smart contracts are fully digital (Rosic, 2017). A smart contract is not more than a coded computer program inside a blockchain (Rosie, 2017). They were initially introduced by Nick Szabo (1997), a now famous cryptographer and digital currency enthusiast (Rosic, A (2017). Nonetheless, due to the lack of technology available to support this concept in the late 1990s, smart contracts as we currently know them were implemented by Vitalik Buterin in 2015, the creator of a famous blockchain: Ethereum (Rosie, 2017). Buterin quickly realised and recognised the importance of blockchain as tool for transactions outside of the financial world (Rosie, 2017). This invention revolutionised many industries outside the financial sector, for example, within real estate, government agencies and health care systems. Indeed, smarts contracts have the potential to automate mortgages, to reduce counterfeit identities but also support cross-institutional visibility in clinical trials by automating data sharing and improving privacy (Rosie, 2017). This is the case because smart contract remove a degree of administration that allows for processes such as the ones described above to be implemented faster, but also facilitates trusted data sharing between relevant parties (Rosie, 2017). Of course, for these features to work as they should, all participants from all boundaries of a process in the blockchain have to have the trust and knowledge in the technology. A common example utilised to theoretically illustrate the benefits of smart contract use is crowdfunding platforms (Yadav et al., 2020). Crowdfunding platforms refer to digital communities that have the power to digitally collect funds from unknown individuals who support a certain product, startup, idea, cause or person (Yadav et al., 2020). The crowdfunding platform therefore becomes the middle man handling the financial transactions, make sure that the received resources are correctly allocated to the desired, if successful, funding project (Yadav et al., 2020). Naturally, this type of platform requires trust and efficiency from both sides of the parties. As the funded party expects to accurately receive the funds towards their cause, while the individual giving the funds expects its money to go to the desired location. In this regard, allowing trust to flourish between two or more parties. Following on the example of crowdfunding platforms, smart contracts are programmed in such a way that all the funds would be held onto until the project is deemed to have reached its funding goal, in which case capital resources would be automatically allocated to the correct account. The smart contract would be automated in such a way that it would be able to use the project requirements as a source for automation triggers and correct allocation or relocation of the funds accordingly, therefore leaving little to no space for fraudulent activities such as scammer accounts pretending to work on a project, misplacement of funds in the transaction chain and misuse of funds from project owners (Yadav et al., 2020).

Back in 2016, three researchers compared two use cases for smart contracts in order to look at the potential benefits and challenges the technology would bring up (Ream et al., 2016). The cases compared were one relating to secure trades and settlements while the other one focused on regulatory documents (Ream et al., 2016). Both cases require accurate actions, like the systematic verification on transactions and the documents that come with it (Ream et al., 2016). Furthermore, in order to secure trade, settlements or look into regulatory documents, there is the need for multiple intermediaries from the parties involved to the relevant publics and/or private officials, and all of these come at a cost (Ream et al., 2016). The analysis of the use cases concluded that due to the characteristic of smart contracts, the automations in place as well as the internal layer of security reduces the number of intermediary necessary (Ream et al., 2016). In this regard, the main identified characteristics in both use cases were; automation, efficiency and security (Ream et al., 2016). This was the case because through the automation that smart contract provide, a large level of manual errors usually encountered in these types of use case processes were avoided, but also lowers the risk of fraudulent activity, therefore leading to an added layer of security for parties involved as well as a strong sense of efficiency (Ream, et al., 2016). As an added value, the researches found out that the use of smart contract turned out to be the cheapest option overall (Ream, et al., 2016).

While smart contracts seem to already make the case for blockchain technology implementation, digital signatures can also be considered a feature that adds value for both private and public uses. Digital signatures were introduced to implement another layer of security to transactions taking place inside the blockchain (Monrat et al., 2019). One prominent concern that was raised at the introduction stage of blockchain technology is that there was no marked legal stamp that could assess the legitimacy of a node (Monrat et al., 2019). This is why digital signatures were developed through asymmetric cryptographic technology, which allowed, just as on a traditional hard paper contract, to legitimise, validate and control a transaction (Monrat et al., 2019). Digital signature, work in the following (for the sake of the research, simplified) way: each node owns a private key and has access to a public key, in order to make a transaction, they gain access through the public key, but once the transaction is made, they stamp their private key on the block, or smart contract for example (Nakamoto, 2008). Private keys then allow to identify and verify the validity of a specific node, creating the same effect as a hard copy signature but in the blockchain world. All in all, digital signatures are important because they lower the risks of duplication or changes within the document it self (Monrat et al., 2019). They ensure that the signatures are authentic and legitimate, which prevents fraud, as the added layer of security confirms the identity

of parties involved in signing a certain document (Monrat et al., 2019). For example if an individual were to upload a smart contract in the blockchain, they would have to confirm that the correct authorised and relevant person is doing the uploading, this person can confirm their fit and identity through the filling in of their digital signature. They are fundamental building blocks within blockchain as they are required to authenticate transactions or any other selected action within the blockchain (Monrat et al., 2019).

2.4.2 The question of blockchain technology adoption and success within e-government & use cases

Batubara et al. (2018) recognised that blockchain implementation in the context of e-government was an unexplored a lacking subject within the academic realm. In this regard, they worked towards adding on to this modest set of academic research. Their paper makes up a systematic literature review on the topic of blockchain adoption by e-governments that allows them to understand current topics as well as the future directions for blockchain-based applications within e-government services (Batubara et al., 2018). Out of 354 articles linked to blockchain technology adoption, only 21 linked the technology to e-government and e-government services. This possibly surprising finding supports the allegations of Ølnes (2017) that claims that the use of blockchain technology within the public sphere has not yet been realised and reported on.

Batubara et al. (2018) present e-governments as an entity that provides and maintains a technological environment in which the focus on transforming government business models and organisation processes is key. Furthermore, they emphasise the fact that e-governments have a strong focus on transforming the relationships between governments and citizens, business and non-state actors through the implementation of new innovative technologies (Batubara et al., 2018). In this regard, it confirms the previously mentioned theory that the adoption of new technologies aiming to improving public services and public service delivery has become a priority for governmental entities (Batubara et al., 2018). The authors emphasise the fact that blockchain technologies represent a great potential benefits for the public sectors, through increased efficiency, and increased trusts (Batubara et al., 2018). More specifically, Ølnes et al. (2017; pp. 357) present more specific benefits from blockchain technology adoption from the side of e-governments include ‘‘data integrity, data quality, transparency, avoidance of fraud manipulation, reducing corruption, and enhancing trust, security and privacy’’. These benefits have already convinced countries into the technology adoption, namely; Estonia with the concept of digital identity, Malta with the concept of academic credential verification and Sweden with property transaction processes (Deloitte Insights, 2017). Batubara et al. (2018) talk about the belief that the potential benefits gained from blockchain

technology would be particularly of use in developing countries as they are the most vulnerable to corruption, fraud, lack of efficiency and trust.

A more concrete example would be property transaction in Sweden. In the domain of real estate, due to the high value at stake, security and transparency in property transaction are key features that should theoretically be part of the process (Zevenbergen, 2008; Chromaway, 2017). However, settlements within the domain of real estate are slow, costly and associated with a multitude of risks, such as the invalidation of the transaction, the risk of reclamation or the risk of recognition of the transaction not concluded. (Zevenbergen, 2008). In order to optimise the process, the Swedish Mapping, Cadaster and Land Registration Authority accompanied by the Landshypotek Bank, Telia, Kairos Future, SBAB and Chromaway joined forces in hopes of increasing trust between parties involved as well as make the process more efficient to improve the speed of transactions (Chromaway, 2017). The project aimed to solved the key pain points of the system in place, namely: the lack of transparency, the slow registration system and the lack of trust (Zevenbergen, 2008; Chromaway, 2017). The current system in place experienced a lack of transparency due to the big body of documentations circulating among different parties (Zevenbergen, 2008). The land authority not being involved from the start made it difficult to assess the reliability of certain actions and documentations performed by either party (Zevenbergen, 2008). Because the land authority needs to verify the reliability of the documents and actions performed throughout the transaction process, the approval required to move forward can take as much as 6 months (Zevenbergen, 2008). This process creates frustration and a lack of trust between parties (Zevenbergen, 2008). The reported impact of the blockchain technology adoption in the case of property transaction in Sweden have mainly being regarded as extremely positive. Indeed, the overall effects were: reduced process time, increase trust between parties and a better handling grasp for the public authorities in charge (Constantin, 2019; Chromaway, 2017). Due to the automative feature implemented within the new blockchain workflow, transaction time were drastically reduced which naturally reduced transaction costs. Further, as the process became fully digital, it eliminated a drastic amount of paperwork as well as opportunities for fraudulent activities, which contributed towards the reduced costs benefits. The more efficient and secure workflow in market operations increased the sense of reliability in the offered service which restored trust among the transaction participants. Indeed, the smart contract workflow disables the option to back out from both sides once having entered a negotiating commitment. Considering the reported benefits, it is safe to assess that the implementation of blockchain technology in the case of property

transaction in Sweden did increase efficiency, trust and security in this specific e-government service. Indeed, the process being sped up allowed for an efficient service, and the security in reducing fraudulent actions as as well as backing out from either involved party increase the trust between stakeholders but also towards the e-service.

While the example of property transaction in Sweden shows a use case in which blockchain can be implemented, it does not mean that the technology has a use for every kind of public service. Indeed, a question is posed in the current literature, it is not whether blockchain technology is useful or not useful but whether it is needed in the first place (Andolfatto, 2018). While there is the ongoing trend to state that blockchain technology makes public and private processes more efficient, trustworthy and secure, it is not necessarily a necessity for every case (Andolfatto, 2018; Golosova, et al. 2018). For example, when certain actions take place within one organisation and does not involved external stakeholders, the implementation of blockchain technology would have little to no positive effect (Golosova, et al. 2018). Golosova, et al. (2018) mention that within one entity it would not make sense to have a decentralised network as a 'petit committee' organisation can achieve trust through other means. For these kinds of organisation, the only 'use' of blockchain would be to drive up costs and lead to complexity (Golosova, et al. 2018).

Even with all the academic stances, or use cases like Sweden that present the potential benefits for e-government with the adoption of blockchain technology, Batubara et al. (2018) point out that academics much like Golosova, et al. (2018) & Andolfatto (2018) remain skeptical and refer to more than one challenge to be empirically addressed. As Lindman et al. (2017) state, the topic of blockchain remains controversial, specially in link to data security concerns. Peck (2017) contributes towards the research findings by being one of the authors that identifies security, scalability and flexibility as the main challenges for blockchain technology implementation within the public sector. While security seemed to be the main strength of blockchain technology with the priorly mentioned scholars, studies conducted with a direct link to e-governance shows deeper concerns with security issues and threats (Moura et al., 2017). The public sectors does not feel safe if the technology and its features are not identified, controlled and overlooked carefully and that the cost of doing that is higher that the traditional government methods (Moura et al., 2017). In addition, Ølnes et al. (2017) puts forward the fact that for blockchain technology to work in an e-government setting, its crucial for design variables to be well thought of by fulfilling all the requirements and needs of the government organisations. One point in which many academics surrounding the subject agree, is that blockchain implementation within government organisation is

challenging mainly due to the change needed on an administrative public level (Hou, 2017; Konashevych, 2017; Ølnes, 2016; Ølnes et al., 2017). Indeed, such technology would require some further thought on new governance models in order to successfully introduce cooperations within multiple public dimensions (Hou, 2017; Konashevych, 2017; Ølnes, 2016; Ølnes et al., 2017). Furthermore, only with a remodelling of the governmental organisation it is possible to get the substantial benefits from blockchain technology use in e-government services (Ølnes, 2016). While some might see a remodelling as a positive requirement to bring forward, due to the existing rigid structures within a government, it actually has the habit to lead to unfavourable reactions coming from the inside of the organisation (Ølnes, 2016). Therefore making the adoption and the success of a new technology challenging. Authors also argue that there is a fear among public workers that acceptability and adoption range on side of the citizen will be a challenge (Hou, 2017; Konashevych, 2017; Ølnes, 2016; Ølnes et al., 2017). This theory relates to the assumptions by Moura et al. (2017) and is backed by the idea that there is a lack of trust in the technology itself, not only from the government side but also from the citizen side. That is the case because blockchain technology remains new and its reliability has not yet been proven in the long term for the private sector, let alone for the public sector (Ølnes, 2016; Ølnes et al., 2017; Sharples et al., 2016; Sullivan et al., 2017). In this regard, other challenges that must be considered are; organisational readiness, implications, trust but also the auditing of the blockchain (Ølnes, 2016; Ølnes et al., 2017; Sharples et al., 2016; Sullivan et al., 2017). Supporting the argument of public readiness as a challenge comes with regulatory concerns. Research shows that laws and regulations were found to be the most important factors in new technology adoptions (Yeoh, 2017). Logically, potential future users of blockchain technology in an e-government setting want to be ensured that the technology is backed by all the laws and regulations required, so that there is a legal certainty supporting them if something were to happen (Yeoh, 2017). Finally, remaining factors bound to challenge user adoption are; the internet infrastructure of the government, levels of citizen education, the technological skills and language barriers (UN, 2014). Indeed, this also links to the challenge of organisational readiness, while implementing new tools regarded as a positive action, new fancy tools can become counter productive if users don't know how to use it (UN, 2014).

2.4.3. Bridging a theoretical gap

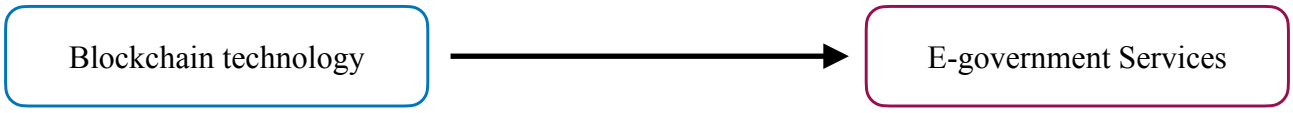
As shown by the above section, while literature on blockchain technology is vast, there is a clear lack of research focus on on applying this new technology to the public sector (Berryhill et al., 2018). Indeed, Yli-Huumo et al. (2016) talks about the fact that most of the current body of literature is focused on analysing and researching the application of cryptocurrencies, such as

Bitcoin and Ethereum, and only a very small amount is dedicated to exploring the use and adoption of blockchain technology in other contexts. This is also shown by Batubara et al. (2018)' systematic literature review on the subject as the authors were limited to a total of 21 articles for their analysis. One of the mentioned articles in the academic review, Ølnes et al. (2017), mentions the importance of interdisciplinary research for the adoption and success of blockchain technology in a public administration and policy context (Batubara et al. 2018). The authors stress out that this type of research would help improve public services as well as tackle some governments challenges, such as fraud, corruption but also inefficiency (Batubara et al. 2018).

The focus of this thesis is on researching the effects of blockchain technology on e-government services, by understanding what blockchain means in an e-government context, but also by identifying the factors that contribute towards a successful implementation of blockchain technology in e-government services. This thesis's literature review, on one hand shows the lack and need for research focused on blockchain technology in the public sector, but one the other hand, proves that even the small amount of current literature, fails to investigate the factors contributing towards a successful implementation. Indeed, authors have focused on the theoretical implications, whether they are positive or negative, rather than the practical applications and their outcomes. Articles that did in fact use case studies, did it on a theoretical level rather than on an empirical level. In fact Ølnes et al. (2017) mention the complete lack of empirical evidence for research of blockchain in the context of e-government services. In light of that claim, Batubara et al. (2018) call for further interdisciplinary research within the broader context of blockchain technology adoption for governments, such as governance models, design variable, impact and risk. This thesis will focus on providing an empirical analysis assessing the impact of blockchain technology on e-government services, but also looking at the factors contributing to a successful technological implementation, therefore providing the base for design variable. Finally, one of the thesis 's subquestion: *What does blockchain mean in the context of e-government?* was answered through this literature review who succeeded in providing the broader context and scope of the research and hence stating what blockchain meant in an e-government the context.

III - Conceptual framework

Through the literature review we are able to identify key theoretical concepts that link to the research question at hand: *How does blockchain technology affect e-government services?* Indeed, the existing body of literature pointed towards the potential impacts of blockchain technology in an e-governance context. In fact, a big majority agreed that the adoption and application of blockchain technology would increase efficiency, trust and security in e-government services. However for those effects to be felt as a benefit from blockchain technology application in e-government services, it is important to not disregard the potential challenges rising in before and during adoption phase of blockchain technology. In this regard, this chapter will take into account the theory and application on research design frameworks redacted by Latham (2005) in order to construct a conceptual framework drafted upon the previous theory. As a first step, Latham states the importance of finding the independent variable as well as the dependent variable (Latham, 2005). The independent variable is defined as the variable which is manipulated or observed in an experimental study in order to explore its effects, it is not influenced by any other variable, hence the name (Latham, 2005). On the other hand, the dependent variable is the variable that changes as a result of the manipulation of the independent variable (Latham, 2005). In the case of this research, we are looking at blockchain technology as the independent variable as it is the trigger variable that will cause an effect. In this regard, the dependent variable represents the effects on e-government services, whether these are positive or negative effects, namely; efficiency, trust and security.



However there is more to take into account in order to have a proper depiction of the theory relating to the research focus. Latham introduces the concepts of control, mediating and moderating variables (Latham, 2005). Control variables are any variable that is held constant in a research study (Latham 2005). It isn't necessary of interest in the study but it is controlled as it could influence the outcomes (Latham, 2005). A mediating variable shows the way in which an independent variable impacts the dependent variable, it therefore explains why or how an effect occurs (Latham, 2005). Finally, a moderating variable refers to a variable or multiple variables that have the power to

strengthen, diminish or change the relationship between independent and dependent variables (Latham, 2005).

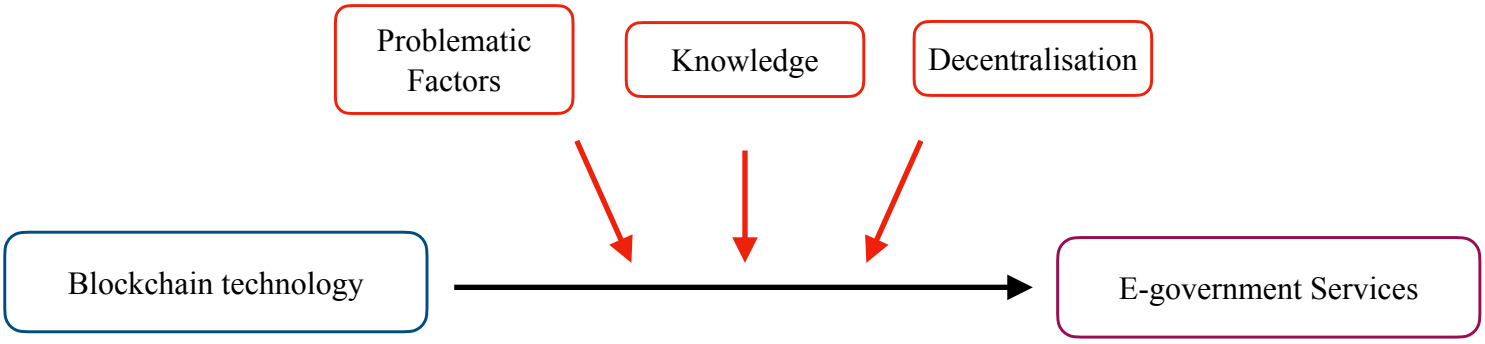
If we take a look at the existing body of literature, it becomes clear the challenges brought up by Batubara et al., (2018), Moura et al. (2017), Ølnes (2016;2017) and others would be the moderating variables. Indeed, challenges in blockchain technology adoption and application would have the power to negatively impact the positive relationship between the independent variable (blockchain technology adoption by e-government) and the dependent variable (efficiency, trust and security in e-government services). However, if these challenges were to not exist, then the relationship between the independent variable and the dependent variable would be reinforced. In order to have a clear set of moderating variables, this thesis has categorised the challenges into three different concepts.

1. Problematic factors - This moderating variable links back to the concerns behind, on one hand governmental acceptance and adoption, but also citizen acceptance and adoption. Indeed, the existing research has shown that there is a widespread concern that there is the possibility of lacking technological acceptance from all sides but also, organisational readiness and rigidness to push forward the acceptance, adoption and application of blockchain technology (Batubara et al., 2018; Yeoh, 2017; UN, 2014). In this regard, user adoption becomes a variable that theoretically has a negative impact on the independent variable (blockchain technology adoption by e-government).

2. Knowledge - While this variable links back to user adoption, it takes a deeper step forward. Considering that blockchain technology is relatively new, there is a lack of common knowledge on the subject, specially relating to blockchains technology use within the public sector. Indeed, while the subject is hyped, it is often in the context of cryptocurrency rather than the public sector (Cartier & Ubacht, 2018). The wider public is then not aware of the potential benefits for the public sector and therefore reinforces skepticism for adoption and application in e-government services.

3. Decentralisation - Term used to refer to the fact that blockchain technology does not rely on institutionalised third parties, which creates concerns from a legal and regulatory perspective of potential users and therefore has the power to affect negatively the relationship between the independent variable and the dependent one.

Including the moderating variables, represented here in the boxes colour red, the conceptual model is illustrated as such:

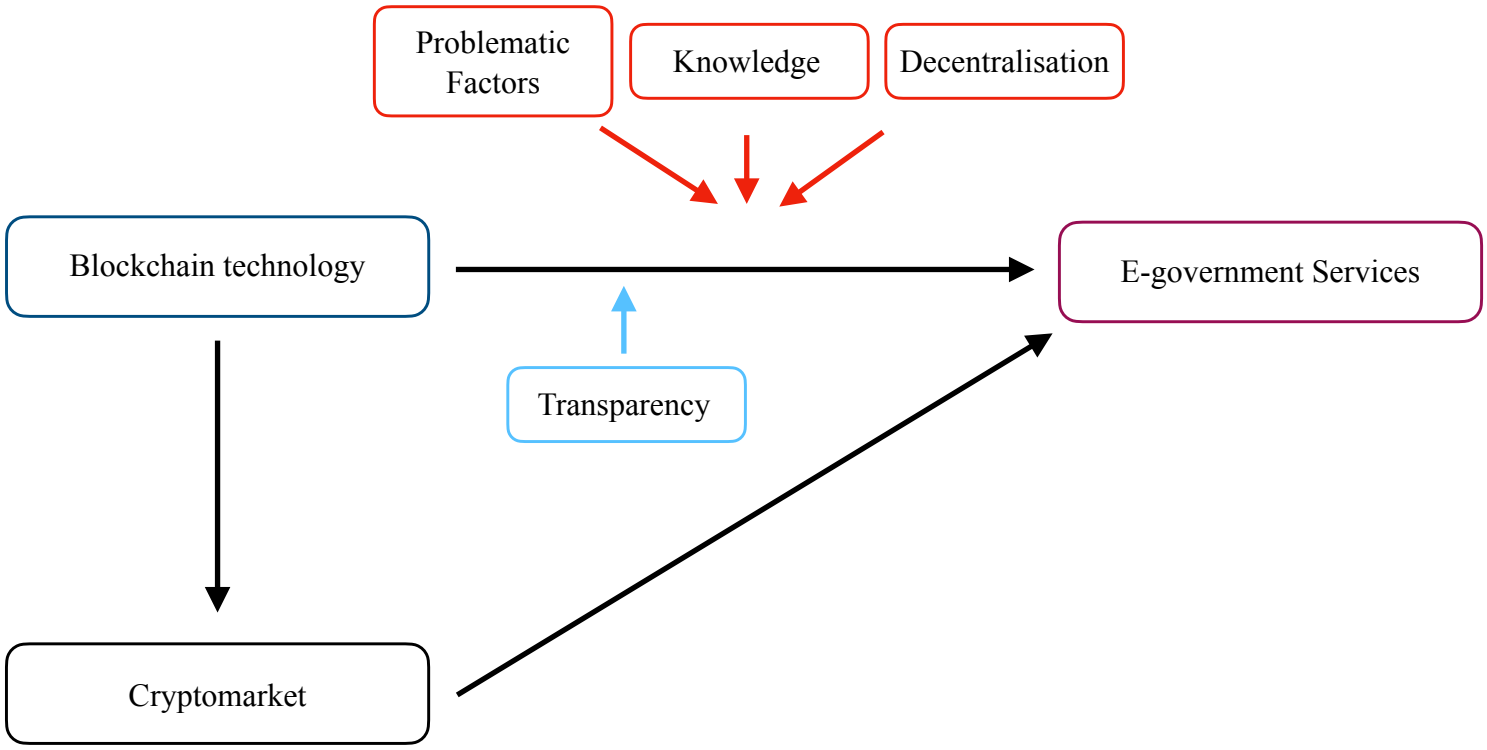


While this model is starting to feel complete, there remains to add the mediating variables as well as the control variables. In order to identify the mediating variables, it is important to look at the existing literature and identify which factors contribute towards an increase in efficiency, trust and security within e-government services. These success factors can be linked to the offered features by blockchain technology which make it an attractive technology. The mediating variables therefore are:

1. Transparency - Ironically, the same feature that can cause the doom of the technology, also causes its attractiveness. The decentralised power of blockchain technology allows nodes that are connected to a blockchain network to keep each accountable, by various circles of verification, it is little to impossible to commit fraudulent activities, therefore increasing trust and security within the blockchain applications.

Finally, the control variables should impact blockchain technology while not being necessary relevant for the focus of the study. Considering the literature review that linked a negative image of cryptocurrencies to blockchain technology, this thesis choose the crypto market economy as the control variable. When cryptocurrencies drop value in the market, society tend the reevaluate the benefits of blockchain technology, therefore potentially having a negative impact on the independent variable (Dumas et al., 2021). Furthermore, this is backed by the research from Cartier & Ubacht (2018) that depict a causal relation between the portrayed reputation in the media of cryptocurrency and the reputation of blockchain technology for any kind of use case.

Considering all the following variables, the final look of the conceptual framework for which this thesis basis itself upon is the following:


Problematic Factors
Knowledge
Decentralisation
Blockchain technology
E-government Services
Transparency
Cryptomarket

IV - Research Design and Methods

The following chapter explains the setup for this thesis, which sources are used as well as defines the specific content of the research. Furthermore, the different sections will go into the specifics on the tools and methods applied as well as elaborate on the limitations and challenges of the research and how those are mitigated.

4.1 Research Design

In terms of research design, multiple case study is selected. This research design seems to be the most appropriate since the goal of the paper is to identify the effects of blockchain implementation in e-government services. Multiple case design is the best fit as the cases explored explore difference adoptions of blockchain by different government entities. Langley and Abdallah (2011) present the two most appropriate methods to conduct a qualitative study; the Eisenhardt method and the Gioia method. On one hand, the Gioia method takes on an inductive approach that through first order and second order codes, allows for the formation of aggregation dimensions that make up the basis of a theory (Langley and Abdallah, 2011). On the other hand, the Eisenhardt method is based on the process of comparison of data a theory (Langley and Abdallah, 2011). The method focuses on theory building from multiple cases (Langley and Abdallah, 2011). In this regard, the Eisenhardt method is the most appropriate as it relies on multiple cases studies to build a theory (Langley and Abdallah, 2011;109).

Yin (2014; 9) presents three criterion of selection to decide whether multiple case study is the fitting research design for a study. The criterion includes; the form of the research question, the control of behavioural events as well as a focus on modern events (Yin, 2014; 9). According to Yin (2014), research questions that start with ‘why’ or ‘how’ are the most appropriate for multiple case study designs. Considering that the aim of this thesis is to find out how blockchain technology implementation impacts e-services, the method chosen is a confirmed fit. Furthermore, the research is focused on modern events as it is looking at recent applications of blockchain technology on e-services to observe the potential negative or positive effects deriving form the technology’s use. This is achieved by conducting interviews with policy makers involved in the steering of the projects. In this regard, each project that is ‘interviewed’ constitutes one case study. Findings derived from a comparison between the answers of the interview participants and the project documentation provided. The results of the interviews are compared to the hypothesis drawn from the literature review and represented in the conceptual framework. Considering that there is no

research requirement to control the behaviour of the interview participants, the potential method of experimentation is not appropriate. Multiple case studies, on the other hand, allow for the researcher to look into aspects within single cases and compare and contrast the former, in this regard allowing cross-case analysis (Yin, 2014).

Considering that the main data source for this thesis is interviews, the research is therefore of primary nature. The units of analysis are the governmental projects in which blockchain technology was used on e-services, the strategies for blockchain implementations and the effects of the technology's use on e-government services. The units of data collection are the interviews of individuals involved in the case studies, internal documents, public documents, articles and websites. Articles and websites are utilised in order to include and assess public reviews or opinion on the different cases. These different units of data allow for a holistic overview of the effects of blockchain technology on e-government services. The comparison of the different cases allows for the finding, not only what kind of impact blockchain technology has had on the public sector, but also to find common factors leading to the success or failure of a certain blockchain application on an e-government service.

4.2 Data Collection

The data collection method is twofold. On one hand, it aims to gather the relevant data able to answer both the main research question, namely: "*How does blockchain technology affect e-government services?*" as well as the subquestion: "*What are the factors contributing to a successful implementation of blockchain technology on e-government services?*". In this regard, it is important to gather enough information on the effects and impacts of blockchain technology on e-government services, therefore focusing on the 'after' of an the specific event: blockchain technology adoption on behalf of an e-government. But also, on the during, in order to assess the design variable within the adoption phase that lead to a successful implementation of blockchain technology within e-government services. The research requires then a number of different sources of information. Consequently, websites, articles, project documentation and interviews are used. Nonetheless, the last two data sources are the most relevant to this study. Indeed, documentation from a certain project is an important information source as it is not produced by the research, in this regard is not influenced by it. Moreover, it provides detailed information and the content can be reviewed on a regular basis. Project documentation is the ideal data source to combine with interviews. Interviews allow to gather valuable insights on information that would otherwise not be available (Yin, 2014). Further, the exchanges with the participants can lead to reaching further

dimensions of depth on the topic that can result valuable to the analysis (Yin, 2014). The combination of project documentation and interviews makes up the ideal setup to gather as much detailed information on the topic of analysis. In this regard, this approach provides a holistic pictures of the effects of blockchain technology on e-government services as well as the factors that allow for a successful or non successful implementation.

The type of interviews conducted were semi-structured with decision makers in their respective projects relating to blockchain implementation on e-government services. Semi-structured interviews are a mixture between structured and unstructured interviews (Smith, 1995). The interviewer has an idea of the questions and topics they want to address but will adapt the flow of the conversation. This allows for the discovery and discussion of elements that would otherwise not be brought up in a structure interview. The interviewees were either project managers, policy makers or deeply involved consultants for the projects. Their roles allowed all access to information on the projects. Four of the projects are located on the European Continent, with a majority located around eastern Europe, and one is located in Kenya. Based on (Smith, 1995), interviews are necessary in order to conduct an explorative qualitative research. It allows a to gather explanations and insights on topics that are not easily accessible.

According to Yin (2014), when the interview is performed correctly, the findings of the interview contain the unbiased perspectives of the respective participants. Ensuring that the gathered information is not influenced by the study is important to assure the reliability of the data. In this regard, the interview questions are based on the content and main findings of the relevant items contained in the literature review. Furthermore, the latter are phrased in a way that does not guide the interview to certain conclusions.

The interviewees were selected through convenience sampling. The former represents a method that researchers use in which they collect data from a conveniently available pool of participants (Smith, 1995). The participants were found through their involvement in relevant projects and contacted through the professional social platform; LinkedIn.

All interviewee participants were informed about the purpose of the research, its content and the interview process. All participants have given their consent for both the conduction of the interview as well as the recording of the latter, for transcription purposes. While none of the interviews needed a non-disclosure agreement, as one participant required anonymisation, participant data is anonymised to keep a constant on the type of information provided per case study.

The semistructured interviews were drawing upon a drafted protocol (Appendix A). This protocol allowed to keep in mind the research objectives and steering of the conversations, as well

as providing consistency between the contents of the distinct interviews. Yin (2014), suggests the conduction of a pilot interview in order to refine the interview protocol. A test run was done with a personal acquaintance well informed in topics relating to blockchain technology and the public sector. The pilot interviewee was selected through convenience sampling and relevance to the topic at hand. After the pilot test, the interview protocol was adjusted.

4.3 Data Analysis

As Eriksson et al. (2008) mention, making the correct choice in research methodology sets the tone for the quality of the study. In this regard, this thesis will use distinct tools and methods to analyse the data. Based on Welch et al. (2011) a relevant method to combine with the case study approach would be pattern uncovering as an inductive method of theory building. Pattern uncovering refers to finding patterns within case studies that can make up for the generalisation of theories on multiple cases studies (Welch et al. 2011). It creates a great addition to the multiple case study, as pattern matching identifies the relevant variables that seem to come up often while the multiple case approach looks at comparing the variation between this variables / patterns. In this regard laying the groundwork for future research. Yin (2014, p.142) also mentions analytic techniques that should be considered when analysing data. In regard to this study, pattern matching is the technique that will be the most useful for analysing the data. Further, Yin (2014) reminds that analytic technics should be kept in mind when analysing data. Linking to the concepts of Welch et al. 2011, as well as the multiple case study method, pattern matching seems to be the most suitable approaches at hand.

The use of the pattern matching technique permits the comparison between the theoretical findings of the literature review and the results drafted from the interviews. As presented, the reviewing of the previous literature has allowed to make certain predictions on which kind of effects blockchain technology has on e-government services as well as identified some core characteristics that make or break the implementation of blockchain technology in public services.

These findings are then compared with the conclusions drawn from the interviews. Once the comparison is made, the thesis looks into other potential explanations that could have affected the outcome of the predictions.

A cross- case synthesis is then performed in which the individual case studies are compares and the findings, based on the common trends identifies, are presented. Through the application of these methods, this thesis does not only utilise the literature and connects it to the results of the interviews, but makes use of the common denominators to identify trends among the effects of

blockchain technology on e-services. The trends identified through the interview data was using the manual coding method. Manual coding is suitable as the sample is a small N.

4.5 Study Sample

As previously mentioned, the data sample consists of public projects relating to blockchain implementation on e-government services. The interviewees hold relevant positions, in regards to blockchain implementation, within the public e-service. Positions include, the blockchain technologies coordinator at the Ministry of Economic Development and technology, founders in the realm of blockchain actively participating and assisting public projects, project leader within the ministry of innovation and blockchain experts acting as consultants for public projects. As shown by the literature review, the implementations of blockchain technology in the public sector are rather scarce. In this regard, the study does not focus on blockchain implementation on one type e-service but rather looks at different use cases of the technology in e-services. In total five interviews were conducted on each specific case study.

4.6 Validity and Reliability

The validity and reliability of the research are relevant in order to support the purpose and outcome of the research at hand. This paper implements several approaches to ensure the validity and reliability of its study. As a matter of fact, Yin (2014) proposes a number of tactics to guarantee the quality of a research. Currently, this study is based on multiple sources which establishes evidence that constructs validity. This is initiated through the extensive literature review which provides a holistic overview of the topic at hand and with an explanation of the steps taken towards data analysis. In fact, Yin (2014) considers the used data analytical techniques of pattern matching and cross case synthesis as two pertinent techniques ensuring internal validity. Further, in order to achieve external validity with studies that follow the methodology of multiple case analysis, Yin (2014) mentions that it is important for the research to follow a design that is easily transferable and replicable. In order to allow for the replicability of the study, this thesis follows an analytical structure that could be transferable to other case studies of the same nature.

4.6 Limitations & Challenges

This study faces a number of limitations. First, due to the novelty of the subject at hand, there is little literature on the existing subject, let alone profound documentation on cases that have

implemented blockchain technology. One challenge faced was to get enough and relevant participants for the interviews. The most prominent aspect of this was the fact that there are not many publicly available information on public projects on blockchain technology on e-government services. While the challenge was overcome using convenience sampling, the limitation remains that the number of case studies and interviews is limited to 5. However, it is important to keep in mind that considering the little information on the topic, 5 case studies and interviews are already a relevant number for inductive research on the topic.

In addition to the above, one important factor to acknowledge is participation bias. Indeed, the participants are asked to talk about their projects. While the questions are phrased objectively in order to gather unbiased information, that fact remains that the participants could have a more positive view on the outcomes of their projects, as they themselves believe in it more than external person would.

Another limitation that the study faces is the diversification in case studies. Indeed, which each case study refer to the use of blockchain on an e-government services, each application is on a different type of services. In this regard, it would be beneficial for future research, once blockchain technology is more widespread within the public sector, to look into the effects of blockchain technology on one specific e-government services domain, rather than a multitude. Furthermore, the cases do not come from the same socio-economic background as four of the cases are located on the European continent and the last one is located in Kenya, while this give a broader view of blockchain implementation in different environments, it is an aspect to keep in mind when making generalisations about the effects of blockchain and the factors that contribute towards those effects.

V - Analysis of the cases

This section includes the analysis of the selected research cases. Each sub-section presents and individual case, including a short description of the e-government service and its adoption and application of blockchain technology, as well as a short description of the interviewee, showing both the relevance of the specific case choice as well as the interview participant. Furthermore, the most relevant quotes are included in these sections. For each case, the data is analysed through the concept of pattern matching. As previously mentioned, the research relies on five interviews with relevant participants, each representing one case of blockchain application on an e-government service. Each case is then analysed in comparison to the theoretical findings drawn form the literature review. On one hand these findings include the hypothesis that the adoption and application of blockchain technology would increase efficiency, trust and security in e-government services through the defined success factor of transparency in processes. On the other hand, they include the theoretical negative factors that would negatively influence the implementation of blockchain technology on e-services, namely; decentralisation, knowledge and problematic factors in general. Furthermore, the implementation strategies for each of the use cases will be presented and discussed in this section. As previously mentioned, the identity of the participant is anonymised for data protection purposes, there will be no gendered pronouns. In addition, in all but two cases, participants preferred the names of specific organisations or institutions that they are not directly working for, involved in the use cases to not be disclosed.

5.1 Digital Identity in Austria

5.1.1 Participant description

With over 7 years of experience in the blockchain realm, in 2019, participant A founded its own company relating to digital identity on the blockchain after being crowned the best digital identity project in Austria. While the project launched with a focus on the corporate sector, the startup launched their first partnership with a public entity in 2020. Participant A was at the core of the blockchain implementation and adoption as well as performed an analysis on the outcomes and effects of the partnership for its own private database.[1] One of the goals of participant A is to implement a standard process of digital identity both the private and the public sector, on the blockchain in Austria.

[1] Sources in this section include the documentation provided by Participant A and the recorded interview of Participant A.

5.1.2 Background and case description

This specific case presents a partnership between a private company providing the blockchain technology and a public organisation looking to implement digital IDs within their organisation and their external partners. In 2020, a public business agency (referred to as Use case 1, from now on) partnered with participants' A company in order to implement digital IDs for their employees as well as the startups they onboarded. Use case 1 is a publicly funded and organised institution that provides funds to innovative startups that are registered in Austria.

'*Use case 1 wanted to implement blockchain technology to facilitate due diligence, preserve and exchange startup data and in the future, secure transactions. The first step was to establish a digital identity for their employees as well as for the corporate entity they were onboarding*' (Participant A)

Participant A stated that the aim of the project was to facilitate stakeholder communication and sharing of high level documents linked to the due diligence of startups. Through the adoption of digital identities for employees and onboarded startups, Use case 1 wanted to facilitate the enabling of authentication, registration and the digital signing of digital documents. For the case of digital identity in Austria, the public service is the facilitation of public funding to promising entrepreneurial projects that benefit the Austrian ecosystem.

''*First, it was important to identify if blockchain technology would be a fit and which specific features were relevant to implement. We decided to establish a private blockchain in which we* (refers to Participant A's company) *and Use Case 1 had administration rights and therefore the power to choose who can participate and with which levels of access.'*

For use case 1, the startups were instructed to upload their due diligence documents on the blockchain, using their digital ID and relevant external startup stakeholder would have to confirm that the information within the documents were correct and had to digitally sign the document using their own digital ID.

5.1.3 Outcome, effects & contributing factors

Due to the preparations requires and the participation of external parties that were not directly taking part in the experiment of use case 1, participant A describe the experiment as a '*Flop*' (Participant A). In fact, the participant referred to use case 1 as an unsuccessful launch but not a discouragement for future testing.

'It is important to talk about the use cases that did not have a successful implementation or adoption, it can make us better in the future. And make us reflect on which organisations or institutions can really benefit from blockchain' (Participant A).

Participant A explicitly stated that the implementation of the technology was costly from a time perspective and a financial perspective to use case 1. Indeed, the technology required training not only from inside of use case one but also for the external stakeholders. Furthermore, certain documents were problematic as they required more than a signature from an external stakeholder to be able to be accredited as valid.

'*If we're talking about specific effects that the use of blockchain had on use case 1, then we can talk about an added layer of complexity in the coordination and delivery of public funds to the onboarded startups - it seemed that they found their previous methods to be more or just as efficient and that they didn't require the technology to work efficiently and in a trusted and secure environment*' (Participant A).

Indeed, initially use case 1 thought that the implementation of blockchain would significantly increase efficiency in the delivery of certain tasks related to the public service of funding that they offer. Instead, while they still believed in the potential for blockchain technology said participant A, they did not think that they personally had a real use for it and that the cost did not justify the means. In this regard this specific use case seems to contribute towards the theoretical debate that blockchain technology does not necessarily increase efficiency, trust and security within an public service but rather add 'layer of complexity'.

'*If I think about the factors that lead to this outcome, I think the preparation and education on the technology required is crucial - people have to know how to use the technology but also have to be open to change their current way of working. That is not an easy fit*.' (Participant A)

In this regard, participant A found the willingness for adoption and change to be the biggest factor in steering a use case to be deemed successful or unsuccessful. He also mentioned that the subconscious link that individuals make between crypto-currencies and blockchain technology hurts the potential implementations in the public sector. Previous literature agrees that user adoption and education, in this regard problematic factors surrounding blockchain and knowledge on the

technology can make or break the implementation of blockchain technology on a public service *(Batubara et al., 2018)*. Furthermore, participant A also mentioned that it is important make a realistic assessment of the impacts that the technology could have taking the above factors into account. The implementation of blockchain technology on a service can be costly, and if the impacts do not live up to the expectations of the institution or organisation looking to implement the technology, then it is simply not worth it according to participant A.

5.1.4 Additional expert perceptions of the use of blockchain technology in the public sector

When asked on which use cases participant A can see blockchain technology being more relevant and leading to positive effects on an e-services. Participant A responded that he believed that the added value of blockchain would really lie facilitated small actions.

'*For example if you need to clarify something with the tax authorities, through the digital identity and the blockchain you can securely send information that is confidential.*' (Participant A)

Participant A refers to 'click and submit' type of solutions and takes the example of 'KYC' know your customer or know your user - in which with the use of digital identity in the blockchain, participant A sees the most potential.

5.2 Smart Contracts for Notarial Acts in Slovenia

5.2.1 Participant description

Participant B works for the Slovenian Ministry of Economic Development and technology and is in charge of coordinating strategy for digital transformation by being the head of the project for new economy and blockchain technology in Slovenia. The participant is also a member of the European blockchain partnership as well as a member of the government advisory and the national coordinator for European projects for common European interests in the steer of digital technologies.

"*Initially the ministry was reluctant to look into blockchain technology because its link to crypto currencies, something that the government explicitly did not approve of at the time. But with time and education on the technicalities of the topic, the potential of blockchain technology*

implementation for the public sector could not be ignored, that's why the strategic plan was drafted" (Participant B)

Participant B was the coordinator in the pilot projects concerning the use of smart contracts to replace public notarial acts. She explained that she saw incredible potential in the implementation of blockchain technology for document/contract reliability due to decrease in administration time.

5.2.2 Background & case description

In 2019, Slovenia was among the first member states of the EU to establish a blockchain test infrastructure. The former established the 'SI-Chain' in cooperation with private operation Hashnet. SI-chain core services include Smart Contracts, eDelivery, Notarisation and Data Storage[2]. The initial idea was for the technology to facilitate transactions as well as the creation of smart contracts (GOV.SI, 2019). At the time, the ambition for Hashnet technology was to integrate blockchain technology, not only in the business models of companies but also into public services (GOV.SI, 2019).

The findings from the projects and the testing were aimed to help the Slovenian Government to create regulations around blockchain technology (GOV.SI, 2019). The was achieved with the introduction of smart contracts definition into Slovenian law, as well as the regulation across different fields of industry as well as the public sector. Which allowed further testing of blockchain technology in public services. One specific use case was the use of smart contracts for public notarial services.

Public notary services refer to the act of being considered an official state witness, preventing fraud. Certain activities or transactions have to be notarised, for example, the writing of a will, the naming of power of attorney or the signing of bank documents. The notarisation process can be quite lengthy and complex. Indeed, common processes points include; the participant's requirement to be physically present, the documents having to be reviewed, the correct notarisation process being identified and the identities of the participants involved have to be verified.

In order to mitigate the lengthy and costly processes of notarial acts, the Ministry of Economic and Development and Technology decided to test the effects of blockchain technology on the latter. In 2020, with the arrival of the global pandemic, the ministry decided is was the right time to proceed with the implementation of blockchain technology's feature; smart contracts on a

[2] Sources in this section include the Slovenian government website, the documentation provided by Participant B and the recorded interview of Participant B.

number of non-disclosed test cases. The aim was to reduce the administrative burden and transfer the notarial act into the digital realm. The pilot project was tested on a use case (now referred to as use case 2) relating to , all relating to the notarial act among multiple stakeholders of witnessing the signing of a contract to prevent fraud and confirm the identifications of the involved parties. While the application does not get rid of notaries, it enables document owners to prove their ownership and reliability and well as protect rights, contract creation between an unlimited amount of stakeholder and have the latest signed document stored on the blockchain. While the project is officially still in its testing phase, the conduction of use case 2 allowed for the ministry of economy of economy development and technology to already draw some conclusions about the effects of the technology on the services and the factors to take into account prior to implementation.

Before the implementation of blockchain the notarisation process of use case 2 looked like this: first the relevant parties had to visit a notary, second, they had to prove their identity, third, the notary would oversee the signatures, authenticate the document and verbally confirm that each involved party understand an agreement. Finally the notary provides a stamp or seal that proves that the document has gone through the notarisation process and the relevant party pays the fees.

With the implementation of blockchain the step is simplified, specially as smart contracts are legally valid in Slovenian Law. First, the relevant parties verify their identity through blockchain. Second, they sign the document in question. Third, a public verifier such as a notary provides a certificate by giving a validation signature. The document is then available and non-changeable.

5.2.3 Outcome, effects & contributing factors

According to Rosie (2017), smart contracts remove a certain degree of administration work and therefore allows processes to be implemented faster but also facilitates the data sharing between all the stakeholder. Participant B reports similar observations linked to use case 2:

‘‘*I think that the example of how notary acts can be implemented in the blockchain just shows the benefits of blockchain technology. I think that it really simplifies the work of the public sector in four different ways. First the decrease of an administrative burden, second, it enables the reuse of data in a very efficient and traceable way as blockchain gives you a timestamp - it is easier to follow the documents and trace its origins and the different versions - therefore enables multiple use without putting additional administrative work. Third, blockchain enables peer to peer communication because we don’t need any third party intermediaries to access the data. Therefore,*

it acts as a trusted base for the public sector. It provides reliable data that is easily auditable which improves trust into public institutions'' (Participant B).

The positive effects observed by participant B include the reduction of administrative tasks through the efficiency of public processes, the enablement of peer to peer communication that leads to trust between institutions and the public, and an important added outcome and effect is that is lacking in theory, is the facilitation of auditing. This can link to the transparency provided by blockchain technology that is often mentioned by 'blockchain believers'. Participant B mentioned that when it came to use case 2, these effects were concretely present. The use of blockchain reduced the handling time by five. This means the traditional method could take up to five times more than the process through blockchain. Participant B mentions that it includes the time in which participants look and ask for the latest versions of documents. The interviewee stated that having one source of truth stored in the blockchain in which all versions of the document are also kept in the same place, really reduced administration work and therefore made the whole notarisation process more efficient and trustworthy.

When asked on what factors contributed towards this successful implementation, participant B mentioned that all stakeholders involved in use case 2 were knowledgeable in blockchain, its use, potential positive and negative effects. Therefore the technology adoption went very smoothly. She attributes the successful implementation of blockchain technology on notary public acts mainly on stakeholder's knowledge of the technology.

5.2.4 Additional expert perceptions of the use of blockchain technology in the public sector

Linking back to the concept of knowledge and education on the topic of blockchain technology, participant B stated the following:

''*In order to use the technology properly you need to properly understand how it works - it is important to be aware of its advantages but also its complexity and the environments surrounding it - Further, it is important to denote that it is not only about blockchain but also about the combination of multiple emerging technologies like AI or ML*'' (Participant B).

When asked about the potential negative effects of blockchain technology, participant B mentioned that the only thing participant B could think of was General Data Protection Regulation (GDPR) concerns surrounding blockchain technology.

5.3 Transaction Monitoring in Ukraine

5.3.2 Participant description

Participant C is a tech entrepreneur and has founded several companies related to blockchain. Participant C is now also a professor on the topic of blockchain implementation in both the private and public sector and one of the most renown universities in Europe. Through participant C's expertise, participant C acted numerous times as an expert consultant in the topic of blockchain implementation on different kinds of use cases. One of them, related to a public financial institution in Ukraine. Participant C was leading the technical implementation and process definition within the use case (from now on referred to as use case 3)[3].

5.3.2 Case description

Use case 3 related to highly technical concepts within the financial sector. Participant C explained that In the banking sector, there is a concept called transaction monitoring. This concept related to the monitoring of transactions made by the user, whether it is deposits, a withdrawal or a transfer. A number of factors, including nationality, country of residency, amount deposited, amount withdrawn or amount transferred, can trigger certain transaction monitoring rules. When a rule is triggered, employees of a financial institution must check that the transaction is not suspicious. The information is then shared to different departments within a financial institution, usually relating to compliance. These will have the regulatory knowledge to determine whether the case is suspicious or not. In some cases, the financial institutions will require proof of funds for example. On a yearly basis, financial authorities must confirm that the financial institution does a good job at the monitoring of transactions. In this regard, the institution must assure a proper documentation process with clear audit trail. Use case 3 decided to implement blockchain technology as as distributed permissions database.

"*Use case 3 is a public financial entity that attempted to use blockchain technology as a way to store data relating to transaction monitoring. It was appealing to the financial regulation authorities as there is an audit trail of the transactions and the actions that the financial institution*

[3] Sources in this section include the the recorded interview of Participant C.

has taken - In this regard it is possible to adequately verify whether a suspicious transaction has adequately been dealt with- blockchain also facilitates the sharing of these documents''. (Participant C).

In addition, whenever the public needed to provide documentation, the documentation would automatically be added to the case report in the blockchain mentioned participant C.

5.3.3 Outcome, effects & contributing factors

Participant C mentioned that in theory, the project was promising as he believes that the real benefit from using blockchain technology is through the default synchronisation of documents in the blockchain. All relevant stakeholders within the financial realm have a copy updated copies the databases. However, in practice, the implementation of blockchain technology was left aside. Participant C commented:

"There was an added layer of complexity to the topic. Use case 3 had the transaction monitoring process incredibly engrained in their traditional methods of data storage. They saw the appeal in making the process more efficient by having a shared data storage, but they debate whether blockchain technology was the way to go. After two months of application, the project leaders and myself decided that it was too complex and the structure was too rigid to implement that kind of technology in the backend. We therefore decided to improve the process with the current methodology rather than through a shiny new toy. (Participant C).

As participant C mentions, similarly to use case 1, the stakeholders of use case 3 believed that the implementation of blockchain technology would just add another layer of complexity to the process. In the specific case of use case 3, participant C adds that it was a risky process to make the transition from old to new. Decision makers of the project, including participant C, believed it would be safer to keep the sensitive customer data within their own storage softwares rather than adding it on a distributive ledger even with the restrictions that can be put in place. This links back to the comments by Andolfatto (2018) and Golosova et al. (2018) in which it is mentioned that not all services benefit from the use of blockchain. Furthermore, use case 3 still managed to improve their process situation.

‘‘*In order to benefit from the efficiency improvement that blockchain technology would have given them, we decided to apply automatisation systems that would mimic certain features of the blockchain. They now have a data sharing possibility of the latest updated documentation including an audit trail.”* (Participant C).

Participant C adds to that:

‘‘*You need to really evaluate what the point is of introducing blockchain, sometimes the traditional digital way of doing things can work quite well. In fact, the thing about public sector is that they don’t necessarily need decentralisation. The government or whatever institution that is in charge of storing the information, and regulate it in a certain way that only the relevant individuals have access. And current systems work quite well. - The best use cases then for the implementation of blockchain technologies are when different parties need access to a certain data, then it makes the most sense because the characteristics of blockchain are useful in increasing efficiency and trust*’’

Taking into account what participant C says, it is crucial to keep in mind what Batubara et al. (2018) and Carter & Bélanger (2005) said about the importance of technological acceptance. Indeed, the case of transaction monitoring fits the criteria for blockchain technology usefulness in the eyes of participant C, however the decision makers in use case 3 still decided that their traditional current systems were sufficient and could mimic the efficient processes without having to implement blockchain technology in their service.

5.3.4 Additional expert perceptions of the use of blockchain technology in the public sector

Following the outcome of use case 3, participant was then asked to restate the benefits of blockchain technology. Indeed, if stakeholders in use case 3 could mimic the benefits of blockchain technology without risking security, regulatory or complexity issues - why would anyone use blockchain?

‘’*In the end, it does have a unique added value, it gives a lot of confidence and trust between stakeholders and allows for automations between shared processes, and of course, value stands in distributed databases for the processes to store information in which the database is immutable and different participants can take part. Even if some areas of the characteristics are mimic-able the combination of all the experience is not”* (Participant C).

5.4 Diploma verification in Hungary

5.4.1 Participant description

Participant D is a former employee of the Hungarian Minister of Innovation through external contraction. Participant D was involved in the pilot project at the Milton Friedman University for the implementation of e-diplomas on the blockchain in 2021. Participant D's role was to implement new technologies in the Hungarian public sector, it was not limited to blockchain technology but just as participant B, it includes the inclusion of AI or ML.[4]

5.4.2 Case description

E-diploma is a digital platform in which electronic diplomas are issued by Hungarian higher education institutions. Diplomas can be shared by the document owners and authenticated very easily for whom it is relevant. The platform makes use of the ILGON blockchain, developed in Hungary and ensuring the compatibility with GDPR regulations as well as ensuring the fact that it is tamper-proof. In 2021 some students from the Milton Friedman University were able to test the platform and comment on its use. The CEO of ILGON technology mentioned in 2021 already that the project was a success and that it confirmed his pre established idea that blockchain technology can be implemented even in the oldest institutions (BBJ, 2021). Participant D commented:

"*E-diploma set the tone for the future of digital documents authentication. Much like Matla in 2017, Hungary would like to make it the norm. Of course paper diplomas would not be replaced but blockchain based e-diplomas will become the standard requirement for entering the labor market*." (Participant D).

5.4.3 Outcome, effects & contributing factors

Participant D mentions that the e-diploma project was a good stepping stone for the implementation of other areas of document authentication within the blockchain realm in relation to public e-services.

---

4 Sources in this section include the Hungarian government website, the documentation provided by Participant D and the recorded interview of Participant D as well as press releases.

‘’E-diploma turned out to be really efficient, convenient, secure but also environmentally friendly.’’ (Participant D).

E-diploma seems to have improved the verification of diplomas coming from recent graduates. For the employers of Milton Friedman University students, they did not have to hire external parties and contact the university directly. They were provided an authenticated e-diploma issued by the university, which was enough to prove the credentials of the students.

‘’*The process of implementation was very smooth, I really think this was due to our target audience. Students are more likely to be ok with using new technologies, the reputation of cryptocurrencies does not scare them away from mingling with blockchain technology. […] The technology was also welcomed by employers due lower costs linked to ILGON rather than the traditional verification methods*’’. (Participant D).

Cases like e-diplomas are the perfect type of example that proves Ølnes et al. (2017) & Batubara et al. (2018), in saying that blockchain technology can fight against corruption, fraud and inefficiency in digitally available public services.

5.4.4 Additional expert perceptions of the use of blockchain technology in the public sector

Participant D wanted to emphasise the fact that in his experience states that act with an entrepreneurial drive are more likely to succeed and engrain in their culture the idea of being an open minded risk taker. This goes in line with Mazzucato (2011) who emphasises the importance of having an entrepreneurial state than created the appropriate infrastructure with the right set of tools and rules. Furthermore, as a last point participant D compared the use of blockchain technology to the use of the interview a bit more than a decade ago.

‘‘ *Currently I think there is a media hype surrounding the subject which usually focuses on the unsuccessful applications of blockchain technology. I really think that blockchain can be compared to the start of the internet. No one know how to use it so it was considered dangerous. Its the same for blockchain technology now.*’’ (Participant D).

5.5 Property transaction in Kenya

5.5.1 Participant description

Participant E is currently a full time researcher at the blockchain and climate institute in Kenya. Participant E is the pioneer of blockchain expert in Africa and has worked in numerous projects relating to the public sector in Africa but also in the UK.

In 2019 participant E was onboarded at an expert consultant in the implementation of blockchain technology for property transaction in Kenya. Participant E was an active decision maker within the project and had an overview of the justifications behind certain choices as well as a clear picture of the outcomes that blockchain technology produced. [5]

5.5.2 Case description

The initial idea through the interview of participant E was to present blockchain implementation in a public service in relation to climate change in the UK, one of the interviewee's latest projects. However, participant E could contribute on a deeper level with the case of property transaction in Kenya, project implemented in late 2019.

"*Like a lot of other developing countries, Kenya is a country that is victim of many fraudulent deals in relation to property transactions. Before the introduction of digitalisation or blockchain technology, property transactions were were manually recorded since the late 19th century.*" (Participant E).

The goal behind the implementation of blockchain technology on this public service is to legitimise property ownership with blockchain and avoid tampering of property deals. In this regard, the government fostered the use of blockchain technology to act as a public database heavily reliant on networks as it is completely decentralised. Participant E however explains the benefit of a decentralised system over a traditional centralised benefits in the case of Kenya.

"*In our country, the issue with a centralised system is the fact that we live in an endemic corruption. Bureaucrats often have the ability to infiltrate and tamper the system and traditional digital databases would suffer the same fat*e" (Participant E).

[5] Sources in this section include the Kenyan government website, the documentation provided by Participant E and the recorded interview of Participant E as well as press releases.

Furthermore, participant E mentions that there were concerns over the implementation of blockchain technology, specially relating to regulations and governance as well as data security and privacy. However, the Kenyan government had introduced a Computer Misuse and Cybercrimes Act, referred to as 'The Act' . This act gave peace of mind for the implementation of blockchain technology in property transaction as it would assure that a recognised government authority would take care of a case if an issue arises relating to governance or data security.

''*Another issue we had to overcome were the high costs linked to the implementation of blockchain technology. The traditional digital system was extremely week so we had to start from scratch".* (Participant E).

Regardless of the challenges that the project faced, a decentralised system for property transaction regulation and storage was put in place through blockchain the use of blockchain technology.

5.5.3 Outcome, effects & contributing factors

The main outcome and positive effect that was clear since its first implementation was the reduced number of reports linked to property transaction. That was the case because multiple copies of a certain document were held and multiple interested parties like owners, agents of potential buyers had the keys to access to view the documents. These copies were then automatically updated once a selling took place - while keeping the information of the previous owner. This data storage allowed to provide clarity on who is the owner of a certain property.

''*While the use of blockchain was a transition from all, specially for individuals who can't even wrap their head around the idea of digital, it was not as complex as our current system, therefore it was given as chance and people really appreciated the fact that once the document was signed, there was no tampering possible*'' (Participant E).

It seems to be clear that at the core of the project, is the idea to increase transparency and utilise a network to legitimise property transactions instead of relying on a central entity. Participant E already touched upon the fact that public adoption was a success factor of the successful implementation towards blockchain implementation in the public sector. Nonetheless participant reinforced multiple times through the interview the need for education on the subject matter.

‘‘*Public awareness is absolutely key. Even some government officials had no idea what blockchain was or could do. There are a lot of good people in my country that would fight for blockchain if they knew it could prevent corruption*’’ (Participant E).

5.4.4 Additional expert perceptions of the use of blockchain technology in the public sector

Further comments were made on the challenges that participant E and the project team faced. Indeed it was mentioned developing countries might have a harder time expanding on blockchain uses in the public sector as it lacks the right skillset both in management as well as the technical side. Furthermore, participant E wanted to highlight the fact that developing countries are a special case where blockchain can fight corruption because the technology is much better than the legacy systems. However, participant E warns against too much hype around blockchain.

‘*The complexity lies in assessing which areas can benefit from blockchain over centralised solutions*’ (Participant E).

This has a direct link to Andolfatto (2018) and Golosova et al. (2018), as well as use case 3 that mention the idea that blockchain is not supposed to be fitted everywhere but it is important to think about the real impacts it can bring before jumping right into it.

VI - Findings

The previous sections analysed all the case on an individual basis. These included a presentation that justified the choice for case and participant selection. Furthermore, the individual cases have already been analysed in accordance with the hypothesis made in the conceptual framework. That first level of analysis constitutes the base of this chapter.

First, the results from the pattern matching analysis are introduced. This shows how the outcomes of the case analysis results are compared to the theoretical basis presented in chapter two of this thesis.

Second, a cross-case analysis is performed. These include the trends identified above as well as singular results coming from the research on the effects and factors influencing the outcomes of the case studies.

6.1 Pattern Matching Analysis

This section provides an overview of the outcomes of the pattern matching analysis. As said above, pattern matching relates to the comparing of the case results to the findings from the literature review and the conceptual framework. Pattern matching serves as an analytical tool that ensures the internal validity of the thesis.

6.1.1 Effects of the blockchain technology on the e-government services

According to the literature findings, there are three possible effects of blockchain technology use on e-government services; positive, negative and none.

Ølnes et al. (2017), Batubara et al. (2018) and Berryhill et al. (2018) are the main drivers of the theoretical assumption that the use of blockchain technology on e-government services would lead to a positive outcome. Indeed, they repeatedly argue that blockchain technology in the public sector helps to solve governmental challenges such as corruption, fraud or inefficiency through technological characteristics that increase trust, security and efficiency. When comparing those assumptions with outcomes of blockchain implementation on the specific case studies, we can see that three out of five, therefore 60% of the use cases have experience a positive effect and outcome from the implementation of blockchain technology. Indeed, Use case 2, relating to the notary act in Slovenia, has seen this public e-service become 5 times more efficient. This was the case du to the automation of mundane tasks that decrease administrative work. Furthermore, as denoted by

participant B, the data storage within the blockchain allows for peer to peer communication which increases trust among parties. For use case 4, namely e-diplomas implementation in Hungary, all stakeholders, including students, universities and employers were satisfied with the outcome. The use of blockchain technology reduced costs for employers, saved time to all relevant stakeholders and overall solidified trust among the different parties. In this regard, it brought, trust through transparency, and efficiency through saved time and costs. Finally, for the case of property transaction in Kenya, the effect was clear. Blockchain technology significantly reduce corruption in this e-government service. There is a focus on trust and security rather than efficiency in this use case. While the process deemed more efficient from a time saved standpoint, the implementation of blockchain technology was unfortunately very costly. However, the benefits in terms of decreased fraud and corruption was significant which in that case organically increased trust in the service as well as the parties involved and the data storage feature with the combination of the Act from a regulatory perspective increase the perception of security on a public level.

Peck (2017), Moura et al. (2017), Andolfatto (2018) and Golosova et al. (2018) are behind the skepticism of blockchain adoption in e-government services. They argue on one hand that blockchain brings security concerns from a regulatory point of you, as well as increases complexity when applied on a not appropriate case. These types of effects were perceived in two of the five case studies, therefore in 40% of the use cases. Indeed, in use case 1, participant A clearly mentioned the unfitness of digital identity through blockchain in the case of a public business agency that publicly funded Austrian startups. Participant A could find two reasons why that was the case. First, the lack of use case fitness - the central system that the public agency was using was not dysfunctional and therefore the adoption of blockchain technology just added a layer of complexity. Furthermore, participant A talked about how there was a lack of knowledge and willingness to adopt the technology from required stakeholders, which led to even more confusion and complexity. Similarly, use case 3, relating to transaction monitoring for a public financial institution in Ukraine. The former had a mixture of negative effect and none due to the shortcoming of the project. Indeed, while in theory the blockchain implementation had a lot of promise, the application resulted in the mimic of certain blockchain characteristics related to automation instead of the technological adoption. The combination of sensitive data, regulation concerns and most of all the complexity of switching to blockchain, made the decision makers stop the implementation.

6.1.2 Factors contributing towards a negative or positive effect

The main theme that is gathered through the empirical analysis, whether the outcome was positive or negative, is the concept of technology adoption and acceptance as well as organisational readiness. From a theoretical standpoint, it was Ølnes (2016), Ølnes et al. (2017), Sharples et al. (2016), Sullivan et al. (2017) and Yeoh, (2017) that brought forward the factors of organisational readiness, public readiness and general stakeholder stance on adoption and acceptance. These concerns from different stakeholders in the adoption of blockchain technology on e-government services, is said to be due the potential negative effects arising from the technological implementation related to a lack of regulations.

In the case studies, on one hand, it was possible to see how organisational readiness, or stakeholder acceptance contributed towards the make or break of an implementation. Indeed, in the cases of Slovenia, Hungary and Kenya, the organisation readiness to either prior knowledge on the topic, general acceptance to new technologies, or public acceptance through desperation, these were big factors that contributed towards the positive effects and the successful implementation of blockchain technology on their respective use cases. On the other hand, the cases of Austria and Ukraine reported a lack of either organisational readiness of willingness of adoption from relevant stakeholders.

In addition the to the overarching topic of technology readiness, there were the mentions of decentralisation and transparency. Indeed, while decentralisation for the case of Kenya was a positive attribute, for all the other four cases, this drew upon regulatory concerns. All other four cases either had semi-private types of blockchain or fully private.

Finally, the topic of transparency was a positive factor that led to the choice of implementation in 100% of the cases. Indeed, transparency being the main attribute to blockchain technology, as there is a tendency to want to increase trust among stakeholders. Therefore, it remains a driver for the choice of implementation, however, it being an attribute for choice of implementation, it does not have a causal effect on the outcome of a use case.

6.3 Cross-case synthesis

This section includes the literature assumptions present in chapters two and three of this paper, the observed theoretical and empirical patterns linking to not only the effects of blockchain technology on an e.government services but also the factors that influence the outcome.

Table two depicts an overview of the data collected empirically with the theoretical assumption derived from the findings of the literature review and the conceptual framework. These have been confirmed during the pattern matching analysis as either effects of blockchain technology

implementation on a specific e-government service, or as an influential factor that lead to an outcome, regardless if it is positive or not. For that reason, the transparency variable is left out. Transparency is not included because it has been judged to be a factor in the choice of blockchain adoption rather than an influential factor.

Most emphasised effects & outcomes	Austria	Slovenia	Ukraine	Hungary	Kenya
Increase in Trust		X		X	X
Increase of Security					
Increase in Efficiency		X		X	X
Complexity	X		X		
Security Concerns			-		
Factors influencing the outcome					
Problematic factors	X	X	X	X	X
Knowledge	X	X	X	X	X
Decentralisation					X

Table 1 - Data Metrics

From the pattern matching analysis and the overview on Table 1, it is possible to see how 60% of the empirical case studies experienced an increase in trust. Indeed participant B, D and E all reported a higher trust among stakeholders and in the e-government services due to one of blockchain's characteristics, which is data sharing available among stakeholders with the latest version of the documents, including the possibility to audit.

"Blockchain enables peer to peer communication because we don't need any third party intermediaries to access the data. Therefore, it acts as a trusted base for the public sector. It provides reliable data that is easily auditable which improves trust into public institutions" (Participant B).

&

"*While the use of blockchain was a transition from all, specially for individuals who can't even wrap their head around the idea of digital, it was not as complex as our current system, therefore it was given as chance and people really appreciated the fact that once the document was signed, there was no tampering possible*" (Participant E).

Furthermore, these participants also reported an increase in efficiency, much like participant D mentions:

"*E-diploma turned out to be really efficient, convenient, secure but also environmentally friendly."* (Participant D).

These reports on efficiency relate to the fact that the original process was improved through the automations and time saving characteristic of blockchain implementation. Indeed, originally, a notarisation process in Slovenia would many more steps, including a physical appearance in front of the notary. It is therefore understandable that through the implementation of blockchain, the process of notarisation takes 5 times less time that it usually would. Similarly for the use cases of e-diplomas in Hungary. Employers and universities would have to communicate through third party providers, which would cost money and time. Therefore the fact that the student can provide and link and a key to see an authenticated version of the digital diploma, reduced time and costs. Furthermore, in the case of Kenya and property transactions, it is easy to understand how blockchain contributed to an increase in efficiency considering that the norm was manual storage of physical documents as the digitalisation was not fully operational at the time.

The remaining 40% of the cases observed an increase in complexity and a partial security concern in the case of the Ukrainian application. Participants A and C, confirmed that blockchain technology is just not fit for all:

"*If we're talking about specific effects that the use of blockchain had on use case 1, then we can talk about an added layer of complexity in the coordination and delivery of public funds to the onboarded startups*" (Participant A).

&

"*You need to really evaluate what the point is of introducing blockchain, sometimes the traditional digital way of doing things can work quite well. In fact, the thing about public sector is that they don't necessarily need decentralisation. The government or whatever institution that is in charge of*

storing the information, and regulate it in a certain way that only the relevant individuals have access. And current systems work quite well." (Participant C).

Furthermore, participant C also mentioned the concern of security due to the sensitive nature of the data use case 3 was handling. That was not the case for participant A although you could consider corporate information to be sensitive as well.

When it comes to the factors that influenced the outcomes, it was a revealing finding that 100% of the cases studies mentioned, by themselves, the influence of problematic factors, namely; organisational readiness, public acceptance public adoption or just general stakeholder acceptance of the technology. For example, participant A explicitly mentions that one of the factors for the failure of the blockchain implementation on digital identity for the use case of a public business agency;

"*If I think about the factors that lead to this outcome, I think the preparation and education on the technology required is crucial - people have to know how to use the technology but also have to be open to change their current way of working. That is not an easy fit*." (Participant A).

Similarly, how one factor can cause the doom of an implementation, it can also allow for a use case to flourish. Participant E makes sure to mention the important factor than public acceptance of the technology had on the positive outcome of the use case.

"*While the use of blockchain was a transition from all, specially for individuals who can't even wrap their head around the idea of digital, it was not as complex as our current system, therefore it was given as chance and people really appreciated the fact that once the document was signed, there was no tampering possible*"

There is an additional factor that seems to have only affected one use case. The case of property transaction in Kenya. Indeed, for the participant E, the decentralised nature of blockchain was actually an added benefit. This is due to the fact that centralised systems in this specific country are the reason for corruption and fraud within public services and specially in the domain of property transaction. Participant E confirms it by making this statement:

"*In our country, the issue with a centralised system is the fact that we live in an endemic corruption. Bureaucrats often have the ability to infiltrate and tamper the system and traditional digital databases would suffer the same fat*e" (Participant E).

There is a number of additional findings that are not included in the table. Those relate to; first the fact that participant A, participant D and participant E agree that blockchain reputation is linked to cryptocurrency reputation. They mentioned that it impacted the public opinion on the technology and therefore has an indirect influence on the outcome of blockchain implementation. Furthermore, an area that has not been heavily discussed is the combination of blockchain technology with other converging technologies such as AI and ML. Both participants B and D expressed its relevance.

"*Further, it is important to denote that it is not only about blockchain but also about the combination of multiple emerging technologies like AI or ML"* (Participant B).

VII - Discussion & Conclusion

7.1 Discussion of Findings & Conclusion

This research's purpose was to contribute to the existing academic debate on the effects of blockchain technology on e-government services and in this regard to answer questions about how blockchain technology affects e-government services, what are the factors that contribute towards a specific effect, whether positive or negative, and what is the current landscape of blockchain technology in the field of e-governance. Through pattern matching analysis and a cross-case synthesis the study was able to determine that the assumptions derived from the theoretical analysis were correct expect for the factor of transparency that was discussed in the previous chapters.

Concrete findings included the facts that 60% of the use cases had the predicted effects and outcomes, while the other 40% observed an increase in complexity when it came to the public e-service in itself. Furthermore, from the factors that influenced the outcome, problematic factors, namely organisational readiness, public adoption and acceptance as well as stakeholder acceptance in general and the concept on knowledge, namely the background knowledge on the subject matter, influenced the outcome of the respective use case. Decentralisation seemed to only be a factor for the use case of Kenya as it was important for the blockchain to not be linked to government authorities. Further, there were two additional minor findings; the fact that three of the participants mentioned that the reputation of cryptocurrencies has a direct impact on the public perception of blockchain technology and the reflections that participants B and D provided when mentioning that blockchain technology should be linked with implementations of AI or ML.

7.2 Limitations

In spite of the number of findings and the confirmation of the majority of the theoretical assumptions made in chapter 2, there are limitations to this thesis. The first limitation being the sample size for this thesis. Even though for the type of study and the topic of interest, N=5 is enough, Yin (2014) would argue that a bigger N would allow for more generalisable conclusions and the identifications of patterns and trends in the realm of blockchain technology use in the public sector.

Another limitation is the diversification of the case studies. Indeed, each case study tackled one use case that was not related to the others. Furthermore, the environment in which the case studies took place are not equal are one case study in particular comes from a developing country.

In this regard, the study is not able to create clear guidelines for one specific use case with pre-disposed factors but rather provides an overview of a multitude of use cases and look at the general trends within them.

Lastly, the link to convenience sampling is important to mention in the light of this kind of research. Indeed, as the participants were directly related to the fruition of the case studies, they all have a predisposition to be bias towards a positive view on blockchain technology. This was mitigated as much as possible by a neutral and complete interview protocol as well as the inclusion of non bias internal and external documentation on the projects. Furthermore, the case of Kenya linked to the remarks from Batubara et al. (2018) which related to the importance of including developing countries in the research for blockchain adoption, as the authors deemed that these areas would benefit the most due to high corruption, fraud, lack of efficiency and trust.

7.3 Recommendations for Future Research

As priorly mentioned, this paper contributes towards the identification of the effects of blockchain technology on e-government services as well as factors that contribute towards a positive or negative effect, however the range of application remains broad simply because blockchain application in the public sector is not a common topic for empirical research. By bringing more awareness to the effects of blockchain technology use on e-government services and the influential success or failure factors, it opens opportunities to further research. As briefly touched upon in the limitations sections of this chapter, there is relevance in looking further into the differences between blockchain implementation on a same type of e-government services with similar cultural, political and economical backgrounds.

References

Aiolfi, G. (2017). Working Paper 23: New perspectives in e-government and the prevention of corruption. This paper is part of the Basel Institute on Governance Working Paper Series, ISSN: 2624-9650.

Allessie, D. Sobolewski, M. Vaccari, L. & Pignatelli, F. (2019). Blockchain for digital government: Ans assessment of pioneering implementations in public services. *European Commission, JRC Science for policy report.* 1-79

Andolfatto, D. (2018). Blockchain: What it is, what it does, and why you probably don't need one. *Federal Reserve Bank of St. Louis Review*, *100*(2), 87-95.

Batubara, R. F. Ubacht, J. Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. *Proceedings of the 19th Annual Internatinal Conference on Digital Government Research: Governance in the Data Age.* No. 76, Pages 1–9, https://doi.org/10.1145/3209281.3209317

Barr, Dan; Fedesova, Kate; Filipova, Mariya; Housman, Dan; Israel, Adam; Killmeyer, Jason, Krawiec, RJ, Nesbitt, Allen; Quarre, Florian; Tsai, Lindsay; White, Mark, 2016, "Blockchain: Opportunities for Healthcare", Deloitte

Bashir, I. (2017). Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Packt Publishing Ltd.+

BBJ. (2021). *Milton Friedman Uni presents 1st certified e-diplomas in Hungary.* BBJ.Hu. https://bbj.hu/business/tech/innovation/milton-friedman-uni-presents-1st-certified-e-diplomas-in-hungary

Berryhill, J., T. Bourgery and A. Hanson (2018), "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", *OECD Working Papers on Public Governance*, No. 28, OECD Publishing, Paris, https://doi.org/10.1787/3c32c429-en.

Boireau, O. (2018). Securing the blockchain against hackers. *Network Security*, *2018*(1), 8-11.

Carter, L. and Bélanger, F. (2005) The Utilization of E-Government Services: Citizen Trust, Innovation and Acceptance Factors. Information Systems Journal, 15, 5-25. http://dx.doi.org/10.1111/j.1365-2575.2005.00183.x

Cartier, L. & Ubacht, J. (2018). Challenges of Blockchain Technology Adoption for e-Government: A systematic Literature review. *Blockchain applications in government, Conference Paper*. DOI: 10.1145/3209281.3209329

Constantin (2019). Sweden uses Blockchain for real estate purchases. Retrieved in 2022, from: http://revolutionofthings.com/sweden-uses-blockchain-for-real-estate-purchases/

Chromaway. (2017). Blockchain and Future House Purchases Third phase to be completed in April 2018. Retrieved May 30th, 2022, from https://chromaway.com/landregistry/#oc-slider

Chromaway. (2017). Blockchain Land Registry Report 2017. Retrieved May 30th, 2022, from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Dumas, J. G., Jimenez-Garcès, S., & Șoiman, F. (2021, January). Blockchain technology and crypto-assets market analysis: vulnerabilities and risk assessment. In *IMCIC 2021-The 12th International Multi-Conference on Complexity, Informatics and Cybernetics* (Vol. 1, pp. 30-37).

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—long live digital-era governance. *Journal of public administration research and theory*, *16*(3), 467-494.

Ejersbo, N., & Greve, C. (2016). Digital era governance reform and accountability: The case of Denmark. In *The Routledge handbook to accountability and welfare state reforms in Europe* (pp. 281-293). Routledge.

Eriksson, P., & Kovalainen, A. (2008). Qualitative Methods in Business Research (Introducing Qualitative Methods series) (1st ed.). SAGE Publications Ltd. https://methodssagepub-com.eur.idm.oclc.org/book/qualitative-methods-in-business-research/d3.xml

European Commission. (2019). EU Blockchain Observatory and Forum.

Evans, D., & Yen, D. C. (2006). E-Government: Evolving relationship of citizens and government, domestic, and international development. *Government information quarterly*, *23*(2), 207-235.

Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International journal of the Computer, the Internet and management*, *10*(2), 1-22.

Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

GOV.SI. (2019). *Slovenia launches national test blockchain infrastructure and Slovenian Blockchain partnership*. Portal GOV.SI. https://www.gov.si/en/news/slovenia-launches-national-test-blockchain-infrastructure-and-slovenian-blockchain-partnership/

Haber, S., & Stornetta, W.S. (1991). How to time-stamp a digital document. *J. Cryptology 3*, 99–111. https://doi.org/10.1007BF00196791

Hinsdale, J. (2022, July 28). *Cryptocurrency's Dirty Secret: Energy Consumption*. State of the Planet. https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/#:%7E:text=But%20crypto%20has%20a%20dirty,of%20Argentina%2C%20population%2045%20million.

Hofmann, S., & Ogonek, N. (2018). Different but still the same? How public and private sector organisations deal with new digital competences. *Electronic Journal of e-Government*, *16*(2), pp127-135.

Hou, H. 2017. The application of blockchain technology in E-government in China. 2017 26th International Conference on Computer Communications and Networks, ICCCN 2017 (Jul. 2017), 1–4.

Hutt, Rosamond, 2016, "All you need to know about blockchain, explained simply", World Economic Forum, Online, last accessed 11 April 2018, https://www.weforum.org/agenda/2016/06/blockchain-explained-simply

Kim, C. (2018) Swedish Land Registry and Blockchain project have concluded their third phase of testing with a full demonstration. Retrieved in 2022, from: https://www.coindesk.com/markets/2018/06/15/swedens-land-registry-demos-live-transaction-on-a-blockchain/

Konashevych, O. 2017. The concept of the blockchain-based governing: Current issues and general vision. Proceedings of the European Conference on eGovernment, ECEG (2017), 79–85.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy.

Kumar, R., Sachan, A., Mukherjee, A., & Kumar, R. (2018). Factors influencing e-government adoption in India: a qualitative approach. *Digital Policy, Regulation and Governance*.

Latham, J. (2005). The research prospectus. *Retrieved September*, *9*, 2005.

Laurence, T. (2017). Blockchain for dummies, IBM limited edition. *For dummies*.

Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and risks of Blockchain Technologies–a research agenda.

MacLean, D., & Titah, R. (2022). A systematic literature review of empirical research on the impacts of e-government: a public value perspective. *Public Administration Review*, *82*(1), 23-38.

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: a quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987), 20120382.

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134-117151.

Mazzucato, M. (2011). The entrepreneurial state.

Moura, T. and Gomes, A. 2017. Blockchain Voting and its effects on Election Transparency and Voter Confidence. Proceedings of the 18th Annual International Conference on Digital Government Research - dg.o '17 (New York, New York, USA, 2017), 574–575.

Nakamoto, S. (2008). A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Oks, S. J., Fritzsche, A., & Lehmann, C. (2016, July). The digitalisation of industry from a strategic perspective. In Proceedings of Research and Development Management Conference 2016, From Science to Society: Innovation and Value Creation (pp. 3-6).

Ølnes, S. 2016. Beyond Bitcoin enabling smart government using blockchain technology. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer, Cham. 253–264.

Ølnes, S. and Jansen, A. 2017. Blockchain Technology as s Support Infrastructure in e-Government. Springer, Cham.

Ølnes, S. et al. 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly. 34, 3 (Oct. 2017), 355–364.

Peck, M.E. 2017. Blockchains: How They Work and Why They'll Change the World - IEEE Spectrum. IEEE Spectrum.

Pollitt, C. (2011). Innovation in the public sector: An introductory overview. *Innovation in the public sector*, 35-43

Ream, J., Chu, Y., & Schatsky, D. (2016). Upgrading blockchains: Smart contract use cases in industry. *Retrieved December*, *12*, 2017.

Rijswijk, K., Bulten, W., Klerkx, L., den Dulk, L., Dessein, J., & Debruyne, L. (2020). Digital Transformation: Ongoing digitisation and digitalisation processes.

Rinearson, Tess, 2017a, "Making Money: Bitcoin Explained (with Emoji), Part 1". https://medium.com/@tessr/makingmoney-530d2bb2b8f7

Rosic, A. (2017). *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*. Blockgeeks. Retrieved from https://www.coindesk.com/information/ethereum-smart-contracts-work/

Sachan, A., Kumar, R. and Kumar, R. (2018), "Examining the impact of e-government service process on user satisfaction", *Journal of Global Operations and Strategic Sourcing*, Vol. 11 No. 3, pp. 321-336. https://doi.org/10.1108/JGOSS-11-2017-0048

Sharples, M. and Domingue, J. 2016. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. Springer, Cham. 490– 496.

Smith, Jonathan A. (1995) Semi structured interviewing and qualitative analysis. In: Smith, Jonathan A. and Harre, R. and Van Langenhove, L. (eds.) Rethinking Methods in Psychology. Sage Publications, pp. 9-26. ISBN 9780803977334.

Smith, R. (2022, January 17). *The private sector is taking the lead on digital inclusion*. World Economic Forum. https://www.weforum.org/agenda/2021/06/the-private-sector-is-taking-the-lead-on-enabling-digital-inclusion-here-s-how/

Sullivan, C. and Burger, E. 2017. E-residency and blockchain. Computer Law and Security Review. 33, 4 (Aug. 2017), 470–481.

Tiron-Tudor, A., Deliu, D., Farcane, N., & Dontu, A. (2021). Managing change with and through blockchain in accountancy organizations: A systematic literature review. *Journal of Organizational Change Management*.

United Nations 2014. UN E-Government Survey 2014.

Understanding the basics of blockchain in government | Deloitte Insights: 2017. https://www2.deloitte.com/insights/us/en/industry/public-sector/understandingbasics-of-blockchain-in-government.html.

Walport, Mark, 2016, "Distributed Ledger Technology: Beyond Block chain. A Report by the UK Government Chief Scientific Advisor", UK Government

Welch, C., Piekkari, R., Plakoyiannaki, E., & Pavilaainen-Mäntimäki, E. 2011. Theorising from case studies: Towards a pluralist future for international business research. Journal of International Business Studies, 42(5): 740-762

Yadav, N., & Sarasvathi, V. (2020, August). Venturing crowdfunding using smart contracts in blockchain. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 192-197). IEEE.

Yaga, Dylan; Mell, Peter; Roby, Nik; and Scarfone, Karen, 2018, "Blockchain Technology Overview", United States National Institute of Standards and Technology (NIST), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202- draft.pdf

Yeoh, P. 2017. Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance. 25, 2 (May 2017), 196–208.

Yin, R. K. (2014). Case Study Research and Applications: Design and Methods (5th ed.). SAGE Publications, Inc.

Yli-Huumo, J. et al. 2016. Where is current research on Blockchain technology? - A systematic review. PLoS ONE. 11, 10 (Oct. 2016), e0163477.

Zevenbergen, J. (2008). Real property transactions. Procedures, transaction costs and models. Ios Press.

Appendix A - Interview Protocol

1. Overview of the Interview Protocol

This interview protocol is part of the research design included in this master thesis whose end is the completion of the master's programmes Governance & Management in the Public Sector (GMPS), Erasmus University. The audience of this study includes scholars in the fields public administration, public policy, blockchain technology & e-governance, but also public public decision makers and the thesis committee. The thesis committee is formed by supervisor Prof. Freek de Haan and Jasper Eshuis. The aim of the multiple case study is to provide an answer to the following research questions:

(1) How does blockchain technology affect e-government services?

(2) What does blockchain mean in the context of e-government?

(3) What are the factors contributing to a successful implementation of blockchain technology on e-government services?

2. Data Collection Procedures

The data collection relies on two main sources. First, interviews conducted through the video software Zoom and recorded with consent. Second, specific case study documentation, both available online as well as documents shared by the interviewees. The combination of these two source types allows the portraying of a holistic picture for each case study, which improves the accuracy and quality this thesis's findings. Considering the importance of data security for this research, all interviewees are be anonymised.

3. Data Collection Questions

Concepts	Questions
Introduction	1. What is your name and the name of the place you work for? 2. What is your position?

Blockchain & E-governance Check	1. Confirm that they consent to the interview, the recording and the use of the data for academic means & remind them that they are free to stop at any time. 2. Could please expand on your area of expertise 3. Please provide a specific example of projects that you have worked on that includes the use of blockchain technology
Expanding on the use case & strategies for blockchain implementation	1. Could you please provide a background on the use case 2. What was the reasoning behind the choice for the use case? 3. Could you expand on how the technology was used 4. How did you introduce the technology? If mentioned, could you elaborate on the strategies for blockchain implementation, who were the stakeholders, what there the challenges. 5. What was the outcome of that project? If mentioned, could please expand on any positive or negative effects that the technology had on that specific e-government service. 6. Would you have done anything differently? Why?
General questions (Expert opinion)	1. You talked about a use case, do you have any examples from your professional or personal experience where you wouldn't implement blockchain technology within a public service? 2. How do you personally feel about blockchain technology? What do you think are the advantages or disadvantages for blockchain technology 3. What do you think is the future for blockchain technology in the public sector
Wrap up	1. Would you like to add anything? 2. Do you know if any of your relevant acquaintances or other would be open to an interview for this research? 3. Do you have any project documentation that could be helpful for my research and that you would feel comfortable sharing? 4. Is is possible to disclose the names of the organisations or institutions mentioned during your interview?