UNIVERSITY OF GOTHENBURG

DEPARTMENT OF APPLIED IT

THE DEMOCRATIC CHAIN

Blockchain in the Context of Swedish Electoral Processes: Applying a Need-Solution Pairing approach with a lens of Legitimacy.

Juan Gonzalez

Mikael Tuncay

Thesis:	30 hp
Program:	Digital Leadership
Level:	Second Cycle
Year:	2023
Supervisor:	Juho Lindman
Examiner:	Johan Magnusson
Report nr:	2023:040

Abstract

Blockchain has been studied extensively in the literature regarding its plausible application on a series of fields. In the same line, the application of Blockchain for public electoral processes has begun to be a matter of study in recent years. However, to our knowledge, most of the existing literature is dominated by what we have decided to call "ad-hoc" proposed solutions with the focus on a specific country, geography, or jurisdiction; so far without any successful cases being documented until the time this thesis was submitted (August 2023).

This thesis reviews the mentioned literature and claims possible requirements and motivations that electoral authorities might have, to get Blockchain implemented into their electoral processes, have not been correctly nor fully addressed. On the other hand, we propose a more comprehensive view in the attempt implementing Blockchain for electoral processes, starting with a less rigid initial problem setting. Instead, the problem setting can be defined parallelly while searching for plausible solutions. Therefore, the so-called "Need-Solution Pairing" approach from Von Hippel & Von Krogh (2016) was chosen as a basis for this means. Furthermore, we conducted this thesis selecting the research from Suddaby et al. (2017) about "Legitimacy" as lens; with the aim to find out how the different functional, social, and cultural relationships could influence the adoption of a new technology -in this case Blockchain- in a process subject of public scrutiny and with a high demand of transparency, such as elections.

Besides the mentioned approach and lens, in Section 2 an extensive overview of the relevant literature regarding the evolution of the Blockchain technology and its adoption studies across as series of fields, with a stress on e-voting, is provided. Additionally, in section 4 the Data Collection was performed by carrying out interviews among three different profiles of interviewees classified as: Electoral Officials (Organizers of the elections), Researchers (Academicians who have conducted studies about Blockchain regarding e-voting) and Practitioners (Industry Professionals in the Development of Digital Solutions). This triangle of perspectives was chosen with the intention to show that the adoption of a new technology, or the digitalization of a traditional paper-based process (such as elections in Sweden), implies much more than technical feasibility evaluations, rather; such implementation should be prestudied and navigated through a wider range of views, going from legal, organizational, and technical aspects and challenges.

Keywords

Blockchain, elections, digitalization, need-solution pairing, legitimacy, e-voting, fraud, agile.

Foreword

The authors of this thesis would like to thank our lecturers and tutors who have accompanied us along the master's program in Digital Leadership, as well as to the staff of the University of Gothenburg for providing and facilitating an amazing educational and life-time experience. We also want to express our gratitude to our Master thesis Supervisor, Professor Dr. Juho Lindman, without his guidance we couldn't have materialized and grounded our idea. Special also thanks to Jörgen Dehlin from The County Administrative Board of Skåne (Sweden), for allowing us to add our small contribution to the Blockchain in Government (BLING) Project. Finally, thank you to Adri Wischmann from the Blockchain Labs in the EU North Sea Region for helping us gaining the insights towards E-voting, as well as to Professor Dr. Jon Crowcroft from the University of Cambridge, United Kingdom (UK), for his support with his expertise, advice, and contributions to materialize this work.

Table of contents

1 Introduction

This Master thesis looks implementation of Blockchain for public electoral processes in Sweden under the framework of the European Blockchain in Government (BLING) project (further information about BLING project in Section 4). This work will contextualize the reader- especially the one with no previous Blockchain knowledge- by exploring a series of study and proposed implementation cases in the literature around the world and the lessons learned from them. While the application of Blockchain for elections remains ambiguous from the problem definition i.e., a proper definition of the adopter's (either a physical person or an organization) need itself is missing across the analyzed literature. Instead, as mentioned in the Abstract, most of the analyzed literature is dominated by proposed solutions for specific geographical boundaries (countries or jurisdictions). Additionally, none of the analyzed research papers has included guidelines that could be used by Blockchain adopters in other regions of the world.

Due to the decentralized nature of Blockchain (Full explanation in Section 2), as well as to the own characteristics of any given electoral process; we aim to provide a more holistic view to this matter based on two constructs: 1) The so-called "Need-Solution Pairing" proposed by Von Hippel & Von Krogh (2016) as approach for problem definition, as well as through 2) the lens of "Legitimacy" proposed by Suddaby et al. (2017).

Since its introduction in 2008, Blockchain technology and its applications have been a matter of study in a series of fields, not only limited to financial transactions or the cryptocurrencies, such as Bitcoin, but in logistics, healthcare, supply chain and property rights among others (Sanka et al., 2021), counting with success cases in most of these fields in a dozen of countries. Though, for E-voting purposes and to our knowledge, there are no concrete documented success cases so far.

Different locations and jurisdictions as well as sizes and scopes of election follow different requirements, the main required characteristics on every election are universal i.e., secret voting, transparent processing, as well as prompt-accurate auditable reporting results (Langwagen, 2018). In the literature about legitimacy (DiMaggio & Powell, 1983) when considering political matters, the concept relates to the per-

-ception of what is perceived as appropriate and the need for public opinion to see this need satisfied. This is where the proposed need-solution pairing approach comes into scene, since again, in the mentioned ad-hoc Blockchain solutions proposed in the literature for specific geographies a proper general problem (need) definition as well as a list of universal considerations and implementation guidelines, are still missing by the time this thesis was written.

Therefore, our claim is that in order to match the dynamics of multiple and diverse electoral processes with the basic characteristics of the Blockchain technology, it is necessary to go two-steps back in the literature in order to generate a more generalized set of guidelines that contains the minimal characteristics a Blockchain application must include in order to be implemented for such purposes. Therefore, our aim is that any implementation attempt or eventually success case would not only benefit one but multiple possible adopters.

Along with the selected need-solution pairing approach (Von Hippel & Von Krogh 2016), the lens of legitimacy is the other side of the cornerstone of this thesis. The lens of legitimacy evaluates the behavioral aspects of decision-making processes as well as having the ability to apply its 3 dimensions proposed by Suddaby et al. (2017) for the means of our thesis: 1) Legitimacy as property (as something that can be possessed and owned), 2) Legitimacy as process (as an ongoing, dynamic negotiation condition), and 3) Legitimacy as perception (which includes peoples evaluation reinforcing the process dimension) that focuses on making judgements based on the socio-cognitive level. Legitimacy was also chosen due to its relevance as concept in the literature (DiMaggio & Powell, 1983) when studying organizational evolution and its richness in dimensions, matching the purpose of this thesis while providing a extensive solution-case for the reader. The theoretical construct of legitimacy (Suddaby et al., 2017), together with the framework of need-solution pairing (Von Hippel & Von Krogh 2016), led us to the formulation of additional research questions stated as follows:

RQ1: What role can Blockchain play in improving legitimacy on a public election process?

RQ2: Which are the matching pairs between the need landscape (legitimacy) and solution landscape (blockchain) in the implementation of Blockchain for elections, if any?

While this thesis intends to contribute to the Swedish case as part of the Blockchain in Government (BLING) project in collaboration with The County Administrative Board of Skåne, it could be the base to extrapolate the findings and learned lessons to broader spheres, allowing us to properly define and limit the general problem as stated on the presented research questions. In addition to our research questions, we considered it important to define and provide main aspects to consider prior to an implementation of Blockchain in electoral processes, as research goal.

Finally, the combination of legitimacy as lens and the need-solution paring as framework in this thesis will introduce the reader to a commonly used technique nowadays in modern product management for technology applications also referred by Von Hippel & Von Krogh (2016): Agile Software Development.

2 Related Research

In the scientific literature a few examples of Blockchain technology applications can be found in different fields, not only to cryptocurrencies or electoral processes. In this section we will cover some of the relevant previous papers to use Blockchain for elections in different geographies. The vast majority of the consulted and found literature presents, as mentioned in the introduction, ad-hoc solution attempts that have not materialized to practical implementation.

On an influential paper called "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research" (Sanka et al., 2021) a group of based Hong Kong researchers explained how Blockchain technology has gotten more attention and adoptions in various countries and companies throughout the globe. Fields of applications include finance, healthcare, supply chain, insurance, registry, the internet of things and elections. Despite counting with a set of advantageous features in terms of transparency and immutability, joined to its decentralized nature, Blockchain still presents the symptoms of an infant technology materialized in challenges in security, privacy, and scalability among others. Rather than focusing on a specific application of the technology, Sanka et al. (2021) stressed on the overall state of the art of Blockchain, its developments and adoption non-related to cryptocurrencies or financial transactions.

Aside the fame gained on cryptocurrencies, Blockchain has as well followed the purpose to mitigate inefficiencies, speed up transactions, optimize costs, while contributing to transparency, auditability, efficiency, and security in several application fields. While its potential benefits have been addressed in the literature (Huang et al., 2021), challenges of different nature such as scalability and legal regulations are still inherent to this technology according to Sanka et al. (2021). The authors also emphasized the big concentration of Blockchain published papers mostly around Bitcoin, security, and Internet of Things (IoT) (More information about Bitcoin history in Appendix 2).

In a known paper from researchers of the California Institute of Technology as well as from the Lausanne University in Switzerland, Alvarez et al. (2009) were precursors on analysing the possibilities that Blockchain could bring up when combining it with another governmental digital initiative, the digital e-Identity. As if the combination of both topics was not already interesting enough, what was more surprising

for us was the battlefield of the study: Estonia. The influential paper is called "Internet voting in comparative perspective: the case of Estonia" and starts describing the small Baltic country as one of the most advanced in the world in terms of implementing e-Identity systems across its citizens for a variety of purposes. The paper narrates how Estonians started using remote E-voting already back in 2005 during the country`s general elections, making the experience of Estonia "…*very revealing, in which voting in local and national elections through the use of the Estonian identity card via the Internet is the right of any voter" (*Alvarez et al., 2009) Even if the experiment already comprehended 2% of the voters, this online voting experience opened a precedent using such a technology for legally binding digital general elections. Alvarez et al. (2009) concluded that the insertion of Blockchain, if conducted properly, could boost the use of E-voting in previously studied jurisdictions´ cases.

Another paper called "Trustworthy electronic voting using adjusted blockchain technology" (Shahzad & Crowcroft, 2019) explored the potential of Blockchain in the context of a highly populated emerging country: Pakistan. The authors emphasized the Distributed Ledger characteristics of Blockchain as technology and its possibilities on adding additional layers i.e., PoP (Proof of person, see Appendix 3 - Glossary) The combination of layers allows for different levels of assurance while obliges that any corruption attempt would need to cover all existing possibilities of hacking within the technological spectrum, a nearly impossible task. The paper by Shahzad & Crowcroft (2019) also addressed some of the main differences between private and public versions of the Blockchain technology, while additionally highlighted not a technical but rather a crucial behavioral factor: Trust.

" *All is about who you trust"* (Shahzad & Crowcroft, 2019) this quote from the authors stated that if a public election would be run on a Public permissionless (Definition in Section 2.1.2) version of Blockchain (as in Bitcoin), that would make all the issued votes fully visible rather than anonymous, leaving the use of a Private Blockchain version as the only plausible option for these purposes. While deanonymization for the means of coercion and fraud reduction can be considered as the main goal of the paper for the Pakistani context, one of the authors, Crowcroft; also commented about the different reality of his home country, the United Kingdom. The main difference between the UK and the Pakistan cases is that, in the European nation, due to the high levels of Trust that the population has in their electoral authorities, there would be no reason for a system as Blockchain to be considered for electoral processes.

2.1 What is Blockchain?

2.1.1 Definition and Characteristics of Blockchain

Blockchain became a widespread term in the literature, it has been often defined in different ways highlighting the characteristics that the authors of the respective articles are interested in about this technology. For the means of this master thesis, the distributed ledger character and the absence of a central authority are 2 main aspects to deal with (since an election is traditionally organized by a centralized authority and transactions are not public), therefore we picked the following definition offered by Sanka et al. (2021):

"Blockchain is a distributed database (ledger) consisting of inter-connected blocks of data protected by cryptographic concepts against tampering. Blockchain works without a central authority and is managed using the consensus of its network participants" (Sanka et al., 2021)

Blockchain as technology is characterized by multiple features, however, for the purposes of analyzing its plausible impact on conducting a public election we considered 2 main characteristics as primordial. The first one relates to preserving the integrity of the data, which is allowed by its so-called "node-base" feature:

"…. Each node in a blockchain network has a copy of the Blockchain (full node) or depends on full nodes for the Blockchain data (lightweight node). Blockchain data continuously grows as new blocks are added. Once added…. Each block in blockchain contains the hash of the previous block for tamper-proof protection and data integrity (immutability). The hash of the block changes when any data in the block is modified" (Sanka et al., 2021)

The second characteristic relates to allowance for verification while preserving the cumulated data i.e., it is a cumulative information block system:

"The transaction data contains all the transactions in the block. Genesis block is the first block in a blockchain and has no previous block hash. All blocks can be traced to the genesis block for verification" (Sanka et al., 2021)

Under which scenario does Blockchain come to the scene?

Blockchain is mostly meant to be used where data is to be shared and there are multiple writers to the ledger, having little or no trust (Cserny & Nemeslaki, 2018) among them. The signed transaction is then broadcasted to the Blockchain peer-to-peer network for verification and addition into the Blockchain. A miner or a validator node, the new block is broadcasted to the network for further verification and acceptance.

The decentralized nature of Blockchain (lacking a central controlling authority**)** therefore acquires relevance in terms of this thesis since, while it provides visibility and transparency to multi-participants processes (Shahzad & Crowcroft, 2019) while at the same time goes in contradiction to the traditional set up of organizing public elections i.e., are centrally controlled and results are kept secret until the polls close at a predefined hour and results began being reported.

2.1.2 How many Blockchains are out there?

Due to the diversification of fields of Blockchain applications, Blockchain is classified into public, private, and consortium blockchains (Sanka et al., 2021)

Table 1
Comparing the three types of Blockchain provided by Sanka et al. (2021)

Blockchain classifications	
Public Blockchain	*"A Public Blockchain is permissionless, hence anyone can join the network, read, or write and participate in its consensus with full right without prior permission. Public Blockchains are fully decentralized, however, they are vulnerable to privacy issues, selfish mining, and 51% of the cyber-attacks. Bitcoin and Ethereum are the most prominent Public Blockchains".*
Private Blockchain	*"A private Blockchain is permissioned, that is, users are required to be authorized to join the network. The authorized users are known and can read or write*

	as well as validate transactions. Normally, a Private Blockchain is used for business process automation in a single organization with sub-divided departments that can act as Blockchain nodes."
Consortium Blockchain	*"A Consortium Blockchain is also permissioned and stands between the Public and the Private Blockchains. Consortium Blockchains are used by independent organizations sharing information with little or no trust. Only preselected nodes (validators)"*

What kind of consensus does Blockchain use to comply with different actors' interests?

A consensus protocol in Blockchain is a general agreement (rules) followed by the Blockchain nodes to synchronize the network, maintain, and update the Blockchain ledger, while the consensus protocol describes how new blocks are created (Sanka et al., 2021).

Blockchain has distinctive features that have made it recognizable, a main one is its distributed ledger (Piazza et al., 2017) i.e., a combination of enabling users of a network to "consume" peer-to-peer digital transactions and at the same time monitoring changes in the ledger in real time.

Blockchain-based systems have developed throughout the years, and this has permeated the development of new E-voting systems. One of the ad-hoc solutions in literature was proposed by Abuirdris et al. (2021), where the authors addressed the so-called "classical consensus" method of Blockchain. The main message of the article was that a Blockchain system should always include the Proof-of-Work (see Appendix 3 - Glossary) feature while the authors solutions include the addition of a PSC-Chain i.e., composed of Proof -of-Concept (see Appendix 3 - Glossary) and Proof-of-Stake (see Appendix 3 - Glossary). This "hybrid" approach, as the authors name it, intends to reinforce security while claims to enhancing a desirable generative characteristic of digital based systems: *Scalability*.

2.1.3 What are the claimed benefits of Blockchain present in the literature?

Blockchain has had ups and downs in its journey to popularization. While it has had its times of hype and great curiosity around it, skepticism towards the plausibility of its application in different fields and discredit towards its reliability and security features have also appeared on the path of Blockchain (Sanka et al., 2021).

On the positive side, Blockchain has also gained backing from a few governments due to its unique characteristics. For example, the UK government office of science endorsed Blockchain´s capabilities to secure data records, reduce operational costs, and provide transparency in transactions (Sanka et al., 2021).

Claimed benefits of Blockchain provided by Sanka et al. (2021)

***Decentralized nature*:** Blockchain dispenses with central authorities and intermediaries, thus becoming more suitable for trustless systems. Blockchain allows systems to be autonomous and free from the risks of intermediaries and central authorities. However, private Blockchains may be partially or fully centralized but still benefit from the other features of Blockchain.

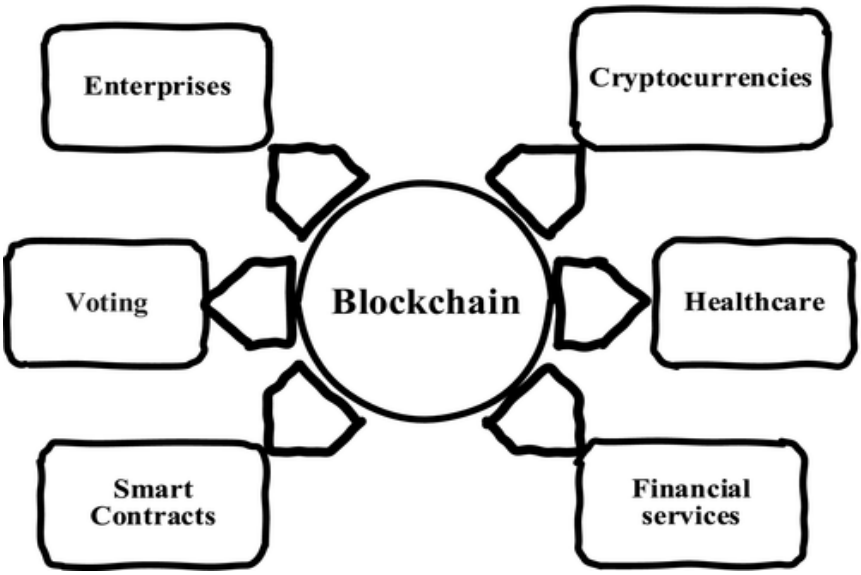
***Cost saving*:** Using Blockchain comes with huge cost savings as costs associated with intermediary systems are saved. This is one of the reasons why some, for example the banking industry started to show interest in Blockchain in the first place.

***Transparency*:** Blockchain allows us to visualize the full history of transactions incurred to all the participants in the process and not only to the controllers` of it.

***Immutability*:** Blockchain is built upon stored blocks of information containing all the preview transactions visible to all the participants in the process, making the creation of a new block dependent on previous registered information, therefore inhibiting manipulation, and alternations.

The main fields of application where Blockchain has been studied for in the literature are cryptocurrencies, supply chain management, healthcare, smart contracts, and financial services as shown in the Figure as provided by Abuirdris et al. (2021).

Figure 1. Blockchain-Based Applications



2.2 Main Applications of Blockchain for Electoral Purposes

After conscious review of the available literature referring to Blockchain in the context of electoral processes, we have located three areas (Digital Identity Management, Voting, and Legal) as the most applied.

Digital Identity Legitimation: Traditional identity Legitimation (passports, ID cards, etc.) is subject to vulnerability due to the possibility of physical loss and identity theft. Blockchain would enable to manage identities autonomously and securely, even in the absence of a central authority. Blockchain in combination with *zero-knowledge proof* (see Appendix 3 - Glossary) would also reinforce identity verification.

Voting: Traditional paper-based voting is not perceived as homogeneously transparent across different geographies and jurisdictions, being the developing countries the most pointed out to experience difficulties, either due to logistical, systematical or

corruption issues. Blockchain could add the transparency element craved by its electoral authorities and probably moreover, by its citizens. There are records indicating that Blockchain based E-voting has been, until today, tested in a series of countries (16 to be precise) around the globe (Sanka et al., 2021).

Legal: Blockchain automatically executes the contract agreements when input information requirements are met while enabling smart contracts´ security and convenience. Smart contracts are used on Blockchain and can be intended to be used by businesses, governments, organizations, and even the public (Piazza et al., 2017).

Sanka et al. (2021) provided a list of countries that have implemented Blockchain to several other areas including land registration, secure trading, healthcare, trade invoice fraud protection, cryptocurrency, public contract, and bidding. Furthermore, Sanka et al. (2021) mentioned the cases of Japan and South Korea as precursors in the use of Blockchain for electoral processes. But more importantly, they highlighted (non-considering or designing for) the scalability, usability as well as the lack of understanding of Blockchain by interested potential adopters as the main threats to be considered as causing adoption failures.

2.3 Blockchain Literature on E-voting: Ad-hoc Solution Cases

This last sub-section describes various solution-implementation cases around the world. The following cases are included in order to provide case-context in the previous research section, while clarifying for the reader what previous efforts have taken place. As stated in the abstract, as to our knowledge, we have not found any successful cases of Blockchain implementation regarding national elections.

Different experiences about electronic voting have been accumulated in a few countries of the world. Particularly, voting using the Internet was applied in some cantons in Switzerland as well as in many other countries like the United States (USA), Japan, India, and Finland (Sanka et al., 2021). However, some cases have gone beyond in their efforts, like in Denmark and Norway (Gebhardt & Bull, 2012) where full digital ID systems have been successfully developed and in the case of Norway experiments linked to voting have been already conducted. In principle, it would be

quite tempting to make a comparison with Sweden, a country that has established a universal digital ID system for several matters via the so-called "Bank ID" but that has not managed to implement it for electoral purposes. Furthermore, countries like Russia have studied the implementation of Blockchain for consulting people regarding referendums or government initiatives (Amelin et al., 2019). For example, in December 2017 the Russian government integrated Blockchain in its "Active Citizen" E-voting platform to allow citizens to take part in taking decisions on the city management and urban transformation. Additionally, the government of the city of Moscow disclosed in August 2018 its plan to use a Blockchain-based system, with the goal to upload applications for trading plots allocations by thousands of farmers for the Moscow market (Amelin et al., 2019).

The list of applications for Blockchain in different fields is extensive within the public sector. Among those, one that stands out is the usage for the means of land title registration and one of the most interesting cases can be found on an unconventional European location: Georgia (Sanka et al., 2021). Georgia was the first government to register land titles on Blockchain. Besides the Georgian example, the UK Government disclosed in recent years that testing around Blockchain for its land registry has been conducted on at regional level. Parallelly and interesting for our case, the Swedish Government reported in 2019 being in the second phase trial of using Blockchain for land registry and in 2020 that its responsible entity [Lantmäteriet] has started Blockchain transactions for land trades after successful testing for two years (Sanka et al., 2021).

Rather than simply affirming that E-voting fraud is a reality and remote absentee ballots are not exempt of manipulation, some authors stress it is more common these days as we think. For example, Abuidris et al. (2021) claim that some studies probed the "*vulnerabilities of centralized ballot storage in e-voting systems are exploited to influence elections*". While we have repeatedly mentioned that the hype Blockchain has enjoyed in recent years can be attributed to its features as decentralized ledger, another important question if the technology failures or fraud attempts are exclusive to non-advanced countries or not. In fact, the same authors stated that some previous examples include a vote fraud controversy in the 2019 elections in North Carolina, USA and a server wipe in the 2017 elections in Georgia, USA (Abuidris et al., 2021)

A common denominator found in the revised literature, is the claim by most of the authors that Blockchain´s adoption in E-voting systems would allow every single vote to be audited/tracked in real time i.e., increase the level of transparency. This argument seeks to provide certainty to Blockchain opponents in their question if Blockchain can improve E-Voting per se.

But if e-voting Blockchain-based systems show technical superiority, what is stopping it from becoming the dominant option for e-voting?

Abuidris et al. (2021), argue that *"a lack of current system structures hinders the diagnosis if such systems in fact comply with the required characteristics"*. Abuidris et al. (2021) also claim that E-voting Blockchain based systems, End-to-End (E2E) voting system (like in the Bitcoin blockchain protocol) as well as other protocols have limitations concerning scalability.

Another important line of research that has developed focuses on enhancing two crucial factors for the adoption of Blockchain in E-voting: 1) Scalability and 2) Performance. Finally, Piazza et al. (2017) claim that they were motivated to reinvestigate the E-voting system and propose a hybrid consensus model for Blockchain. Piazza et al. (2017) claimed that through the usage of Blockchain in the form of a Bulletin Board *"would leave no doubt with regards to the validity and legitimacy of the outcome because of the immutable feature of the blockchain".* This statement refers to one of the pivotal constructs on our thesis that will be used as lens: Legitimacy.

Other Blockchain Ad-hoc Solutions in the literature

A few authors had added to the literature of Blockchain for E-Voting purpose, again proposing their own solutions to specific aspects of the problematic of adding legitimacy to electoral process by the means of using Blockchain. For example, Vijayakumar et al. (2022) published a paper on the security of E-voting system using Blockchain. They stress that distrust on election systems is a more common phenomena than can be thought, even in nations such as Japan, the United States of America and India (Vijayakumar et al., 2022). The authors claim that the argument for distrust comes since there is no guarantee that the votes cast by the voters are being registered. Power-hungry entities can always be tempted to incur non-legitimate practices to keep their status.

On another effort, Amelin et al. (2019) researched on the legal aspects to consider the Blockchain Technology for Electronic Voting. For that purpose, their research studied the possibilities of using electronic voting in the Russian elections as well as in other states. The results of the research looked to establish the requirements that digital technologies need to ensure for the sake of achieving objectivity in a voting process as well as stressing the necessary combination of functionalities between personal electoral rights; digital technologies; electronic voting; law transformation; blockchain and electoral disputes among others.

Amelin et al. (2019) emphasized that goals from electoral authorities aiming to digitalize their processes such as the universality in the transition to electronic voting; multilevel control over the results of voting; the variety of forms of access to the information system of remote voting; as well as the personalized registration of votes must be considered before going into any effort. Likewise, and equally important would be to audit the correctness of the counting, proving mistakes as well as contesting the results of voting. Amelin et al. (2019) not only concluded that these requirements are plausible of technical implementation within information systems, but furthermore it is plausible using the basis of Blockchain technology. Finally, the study goes into a deep literature research on the ideal format to achieve the previously mentioned aims. The main insight of the research paper suggests that information systems for electoral voting purposes must be organized within a single information and communication environment i.e., where information exchange and communication happen simultaneously.

Since process changes, especially the digital ones, do not happen overnight. Cserny et al. (2018) stressed this and added to the literature of Blockchain the concept of *End-to-end verifiability* i.e., where every voter can check by themselves independently if their vote has been counted correctly. Cserny et al. (2018) mentioned that in the paper-based voting systems in most countries, the voter must blindly trust the process of counting. This could be a favorable argument in the acceptance and adoption of a digitalized solution if done correctly, and that would imply to enhance end-to-end verification. The study highlighted the role of transparency as a key factor in achieving trust while stating the question on how long a transition period must last for voters to trust a new E-voting system.

Additionally, Cserny et al. (2018) pointed out the limits of a new implementation of E-voting system. Their paper concentrates on *single vote systems* i.e., one voter has one vote. This condition is not only applicable to the original purposes of the BLING

Project and Skåne, but also reminds us of the complex transactional nature that voting can have when multiple votes can be issued by single voters. Finally, Cserny et al. (2018) presented a couple of *paradoxes* that could be present when aiming to implement an E-voting system based on Blockchain: *Paradox 1*) Securing decentralized E-voting elections is highly improbable since there is a paradox between *accessibility* and *security* that is hard solve when a high security level is demanded, compromising transparency and trustworthiness. *Paradox 2*) The declares the existence of a paradox between *anonymity* and *security* and emphasizes the main aspect future Blockchain e-voting protocols must focus on in order to save the big gap between secured online banking and online voting: *Cryptography* i.e., Banks know who the customer is and voters should be anonymous. The study concluded by saying that while Blockchain might represent an ultimate solution to shape E-voting, it is still on the infant stage of research and testing.

A United States Voting Foundation-sponsored study referred to the E2E verifiable internet voting in 2015 called "The Future of Voting" (U.S. Vote Foundation, 2015) introduced the role of *homomorphic encryption* (see Appendix 3 – Glossary). The study is a comprehensive review of different aspects both from the technical, social, and legal perspectives. The authors start describing the motivation and requirements a remote voting system must comply with to achieve the public trust.

Additionally, "The Future of Voting" (U.S. Vote Foundation, 2015) described the necessary cryptographic, architectural, and engineering foundations, tools, and techniques; according to their understanding, to design and build a system that fulfills the E-voting demands. Despite this, the authors claimed that plausibility i.e., the fact that a system seems to be possible to design and develop it doesn't necessarily imply it to hold another fundamental condition: *Feasibility*. The study of feasibility on an implementation includes all types of non-technical considerations: politics, fiscal, research, development, operational, business, etc. The discussion derivates into the research to consider one last fundamental aspect of any implementation: *Timing.* "The Future of Voting" (U.S. Vote Foundation, 2015) encourage any interested adopters to ask themselves the question: "*Is it practical to tackle the problem of E2E-VIV at this time?"* The set of E2E-VIV can therefore be divided in two groups: Technical requirements and non-functional requirements.

Finally, "The Future of Voting" (U.S. Vote Foundation, 2015) stressed the existence of *"some set unrealistic limits on the accuracy of computer hardware; and some prohibit developers from programming in ways that are widely used when imple*

menting highly reliable software systems." In their proposed solution, the authors go one step further than Amelin et al. (2019) and claimed that in elections where *"voters are allowed to cast multiple ballots with only the last cast ballot counting toward the final election tally as well as in the ones where only one time voting is allowed".* Their proposed system (based on homomorphic encryption) has the flexibility to serve both election formats.

The authors complemented their critics towards the mind set of other ad-hoc solutions using Blockchain for E-voting proposals *"to use blockchains for elections are plentiful but have been shown to be naïve in most instances and inappropriate as a foundation for a public election E2E-V protocol"* (U.S. Vote Foundation, 2015). Finally, they introduced a revised version of their solution: *Fully Homomorphic Encryption (FHE*) i.e., a more powerful type of homomorphic encryption which allows arbitrary computation on encrypted data i.e., desired functionalities can used encrypted data to produce encrypted results.

The last ad-hoc solution revised in this section comes from Park et al. (2021) and its focus lies on cyber security aspects. Therefore, while we are mentioning its main findings, we don't take their research into consideration as adding up on generating legitimacy and trust, but as offering the reader a complementary view of the existing literature. Park et al. (2021) published the article "Going from bad to worse: from Internet voting to blockchain voting" where they mostly highlight the vulnerabilities of electronic voting systems and propose using Blockchains as a ballot box. They claim having showed that Blockchains do not address the vulnerabilities of electronic voting per se while at the same time might introduce new problems. Their main critic comes from the security corner, which according to their perspective is only guaranteed under certain assumptions, and if such are violated, the Blockchain *"might lose its availability, linear ordering, and common prefix guarantees*" (Park et al., 2021).

This research's most revealing insight distinguishes between Blockchain protocols, namely between Bitcoin and Blockchain. *"Unlike Bitcoin, E2E voting protocols generally require an authenticated bulletin board or one where some voting authority signs the contents to indicate that this is the agreed-upon board for the election"* (Park et al., 2021). If this condition doesn't hold, Blockchains lose their validity as a ballot box. Finally, the authors make the distinction between *"voting within blockchains"* which refers to voting used within Blockchain technology, being different from voting in political elections.

3 Conceptual Framework

3.1 Need-solution Pairing

The first proposed construct of this Master thesis work consists of the so called "Need–Solution Pairing" from Von Hippel & Von Krogh (2016). This framework works without an initial defined problem formulation i.e., it works under the assumption that the problem will be discovered, defined, and delimited in a parallel process along with finding the possible solution(s).

3.1.1 Traditional Problem Formulation vs. Need–Solution Pairing

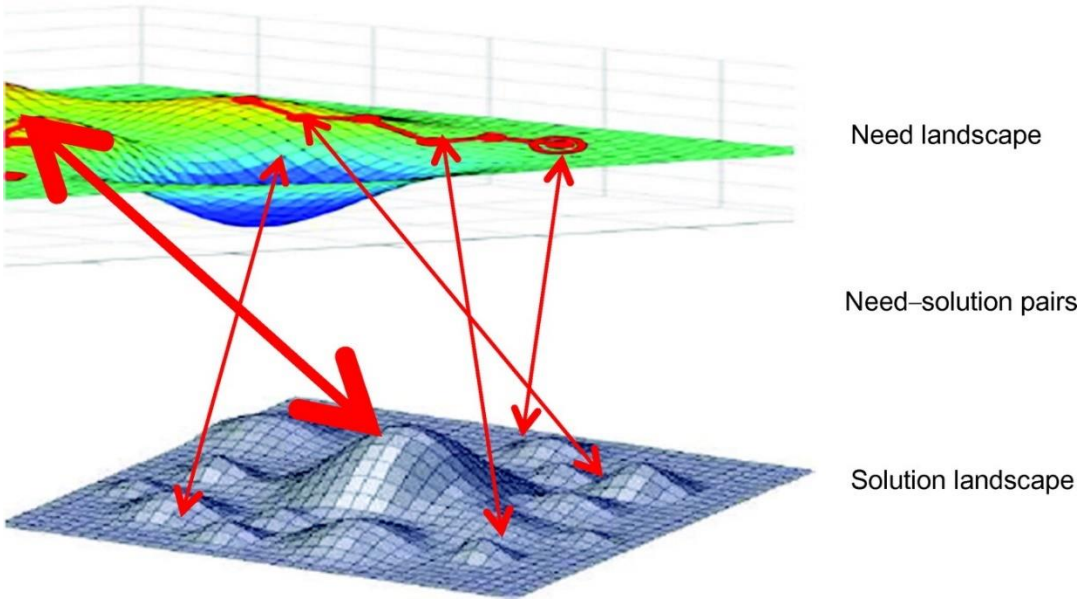
The problem-solving process in traditional research starts with the searching of possible sets of solutions and then carves to find the optimal one. However, traditional research works under a predefined problem setting perspective. An important consideration is how the assumption that prior problem formulation remains as necessary condition for solving, holds only if it is fixed at the beginning and remains unchanged, thus some authors point out the benefit of this approach in situations where the initial statements are progressively re-formulated while the problem-solving process moves forward (Schon, 1983).

Predefined problem statements could lead to restricted problem-solving approaches, as previously mentioned, and hinder the exploration of potential solutions. Von Hippel & Von Krogh (2016) highlighted that the process of problem formulation itself could be influenced by existing models and therefore not fully capture the complexity of factual problems. Need–solution pair identification, in contrast, offers a more dynamic and adaptive method. Unlike traditional problem formulation which relies on predetermined problem statements, *need–solution pair identification* begins with a broader exploration of both need and solution landscapes. The problem solver does not start with a fixed conception of the problematic, but instead looks to understand the broader context of *needs* and challenges faced by individuals or organizations (represented in the need landscapes) and the existing *solutions* that exists or are available to address needs (represented in the solution landscapes). For example, let us

consider the design of an innovative product. In a traditional problem-solving approach, one would start with a specific problem statement like *"design a digitalized version of X process."* Then, one would search for solutions to meet this exact problematic. On the other hand, under the need-solution perspective, one would question the reasons behind the initial formulation of the traditional approach by asking "why, what for and how?" in an on-going manner.

The argument then is extended to the point *"that discovery of viable need–solution pairs without problem formulation may have advantages "*. Additionally, the value of need–solution pair identification compared to traditional problem-solving methods is that when problems are formulated in advance, it could hinder the discovery of groundbreaking solutions and limit creativity. Need–solution pair identification on the other hand enables problem solvers to explore a wide range of potential solutions leading to more valuable outcomes.

Figure 2. Need and Solution Landscapes Connected by Need–Solution Pairs (Von Hippel & Von Krogg, 2016)



The figure above shows how each level of the problem statement points to a different location on the need landscape. If the adopters find themselves only on the first-level problem statement, i.e., it reflects a need to start the process and the solution should clearly point to the plausible options. For cases in need of further research, iterations

should include more specific goal-oriented formulations and questions. The proposed framework goes into the different landscapes as can be observed, addressing the complexity of the richness of landscape search. In the field of management, Sakichi Toyoda who was a founder member of Toyota Motor Corporation, also referred to this process on what he called the "5 Whys" (Von Hippel & Von Krogg, 2016) which 'he methodically applied at the Toyota Motor Corporation. Toyoda proposed that there are 5 stages in which the adopters must ask "why" to get to the root cause of a problem.

Elaboration of a final formulation of the problem would need to consider not only both the short term and long term, but also the scalability of the adoption and its potential use by other adopters (Von Hippel & Von Krogg, 2016).

3.1.2 Need-Solution Approach

Iterative problem reformulation is the first step of the way to Need–Solution Pair discovery and systematic problem formulation-solution. The existing literature (Trieflinger et al., 2021) suggests that the process must be divided into cycles. On any given cycle, a point(s) on the solution landscape -*i.e., a possible solution*-, must be tested against the respective point(s) on the needs landscape to assess for viability: That is the pairing process component in the name of need-solution pairing. The problem formulation keeps being remodified, as well as addressing solving-possibilities if no good fit is found. The repetition of pairing points from the need landscape to the solution landscape will result on *trial-and-error cycles* that should keep going until an acceptable *need–solution pair* emerges (Von Hippel & Tyre, 1995).

Besides the pairing of points in the need-solution landscapes, authors like Walpole (1960) stated that *"You must observe that no discovery of a thing that you are looking for comes under this description".* This statement brings us to the concept of serendipity, which as it is used today, is often considered as a very valuable mode of scientific discovery. On a later research, Merton (2004) redefined serendipity as a concept to be included in the domain of the sociology *"as a scientific method alongside purposeful discovery by experimentation" (*Merton, 2004). In the field of social science, the so-called *grounded- theory development* emphasizes the value of serendipity in the discovery of findings for constructing novel theory (Glaser & Strauss, 1968).

3.1.3 Prototyping - The Final Destination of Iteration

Now that we have introduced the theory and the practical implications of the need-solution pairing approach, the last step towards presenting it as a plausible method to find a solution for an undefined problem is to introduce the concept of prototyping. Von Hippel & Von Krogh (2016) introduced prototyping and its usage by possible adopters *"…. The users then apply the prototype in their own environment using their own data. Based upon what they learn in the trial, users then modify their need specification…. A revised prototype incorporating the modified problem formulation is then quickly developed and sent to the user. The trial-and-error learning and iterative problem-and-solution reformulations by developer and user are repeated until a successful need–solution pairing is found".*

3.2 Need-Solution Pairing in the Context of this Thesis

The implementation of Blockchain into governmental systems has its own technical challenges and difficulties, besides the legal and organizational ones. Rather than having a rigid problem definition and seeking for a specific solution, the approach of "need-solution pairing" offers a more adaptive problem-solving process. It also consists of more extensive and incisive exploration efforts towards the *need* landscape of a specific context that could arise during the solution-finding process. In our case, we are using legitimacy as a lens to look at the aspects on how the Swedish elections could gain legitimacy by implementing Blockchain in its electoral voting processes, i.e., making electoral voting an online validated activity.

Need-Solution pairing was therefore used as a framework to help us navigate through the different landscapes, and locate needs and solutions stated by the participants, with the lens of legitimacy temporarily locking in their position and pairing their respective landscape match.

The iterative nature of the need-solution pairing approach allowed us, therefore, to continuously evaluate the Blockchain solutions presented by the participants in the *solution landscape* though legitimacy goes beyond the technical aspects of Blockchain implementations in electoral process and adds a behavioral dimension to the view of the subject. The *need* landscape should therefore be fed by the collected information derived from the search of achieving legitimacy in each process.

As a result, instead of starting with rigid pre-defined problem formulation (RQ), we kept a flexible and wide search in both landscapes to find viable need-solution pairs with rationalized reasoning behind them. Therefore, from that iterative process, not only a need-solution pair regarding the plausible implementation of Blockchain to electoral processes was derived; but simultaneously the research question *"RQ2: Which are the matching pairs between the need landscape (legitimacy) and solution landscape (blockchain) in the implementation of Blockchain for elections, if any?* was conceived. In conclusion, by following the precepts of the need-solution pairing approach from Von Hippel & Von Krogh (2016) we were able find both the appropriate problem formulation and the matching solution pair to the need parallelly.

3.3 Theory - Legitimacy

The second proposed construct of this Master thesis work consists of the so-called "Legitimacy" lens from Suddaby et al. (2017). However, since the concept has been extensively studied and developed throughout the years, in this section we present a selection of the relevant literature concerning legitimacy towards organizational development. This goes in line with the goal of this master thesis and with the collaboration with the BLING project and the County Administrative Board of Skåne, as well as to contextualize the reader with a more complete view.

On achieving legitimacy by organizations, DiMaggio & Powell (1983) are authorized voices the scientific literature. The authors pointed out how "early adopters" withing organizations looking for innovations in the way they operate, can fall into a desire to improve performance. However, "new practices or techniques" will imply value and organizational considerations beyond the technical requirements of the tasks and activities to be performed. Furthermore, the authors stress that *"As an innovation spread, a threshold is reached beyond which adoption provides legitimacy rather than improves performance"* (DiMaggio & Powell, 1983). For the means of this thesis, we can consider the County Administrative Board of Skåne as the possible adopter and Blockchain as the innovation. Additionally, DiMaggio & Powell (1983) pointed out that organizations have the tendency of trying to model themselves after similar ones, especially if they operate in the same field, that they perceive to have a higher degree of success and innovation. While Public Election Organizational Bodies do not face any kind of competition in their core activity, they

can be tempted look at innovations adopted by other actors in the public sector, both in their home country as well as internationally.

Finally, DiMaggio & Powell (1983) stated in one of their Hypotheses that "*The more ambiguous the goals of an organization, the greater the extent to which the organization will model itself after organizations that it perceives to be successful"*. While the referred organizations with ambiguous goals are likely to be *"highly dependent upon appearances for legitimacy", they might find an advantages* on meeting the expectations (from stakeholders, clients, public opinion or any group they are advocated to impact) about how the way they should be designed and how they should operate. This includes modernizing themselves according to the latest technological trends. DiMaggio & Powell (1983) stressed that they main motivation for such organizations to "legitimize" themselves is not related to achieve competitive advantage, rather to achieve and boost credibility by establishing "legitimated procedures" leading to "organizational legitimacy".

Legitimatized organizations benefit from widespread belief in their good doing and proceeding, improving governance and effectiveness (Tyler, 2006). On his side, Suchman (1995) referred to legitimacy as described as a generalized perception or assumption that an entity's actions are desirable, proper, or appropriate within a socially constructed system of norms, values, and beliefs. Additionally, Suchman (1995) emphasized that legitimacy reflects congruence between an entity's behavior and shared beliefs of a social group, adding up to its to stability and the meaning of its organizational and institutional activities.

In line with the previous argumentation, Adams (2022) defined legitimacy as *"The significance of normative boundaries in guiding behavior"* and explained that in the political realm, legitimacy norms are not only limited to address political disputes; these norms also play a crucial role in establishing and maintaining political institutions by acting as gatekeepers and ensuring that the institutions fulfill their intended purposes effectively (Adams, 2022).

In the context of this Master thesis, we chose to explore the concept of legitimacy theory as defined by Suddaby et al. (2017), expressed in three dimensions:

- Legitimacy-as-property
- Legitimacy-as-process
- Legitimacy-as-perception

Each dimension offers a unique viewpoint on the subject.

Firstly, *legitimacy-as-property* conceptualizes legitimacy as something that can be owned or possessed, such as a tangible object or a valuable resource (Suddaby et al. (2017). Secondly, *legitimacy-as-process* views legitimacy as a participatory process. In this dimension, actors work as agents of change using influence to shape the evaluation of legitimacy (Suddaby et al., 2017). Lastly, *legitimacy-as-perception* focuses on legitimacy as a socio-cognitive perception or judgment made by evaluators. This dimension emphasizes how legitimacy is subjectively perceived and evaluated (Suddaby et al. 2017). By exploring the three dimensions of legitimacy, we aim to provide a comprehensive understanding of the theory.

3.3.1 Legitimacy-as-property

Legitimacy-as-property is a key part of organizations. Think of it as something that can be "owned", like a resource (Suchman, 1995) or an organization (Suddaby et al., 2017). It is something that can grow, could be lost, or even pass it to other groups (Suddaby et al., 2017). Legitimacy-as-property changes and develops based on how well an organization “fits” into different environments and is therefore mostly found at organizational levels between the legitimacy object (e.g., an organization) and its external environment.

One example on how an organization becomes legitimate through the dimension of legitimacy-as-property is through *performing* and demonstrating *pragmatic legitimacy* i.e., Organizations can achieve legitimacy by showcasing the technical superiority or the innovative nature of their products to have advantages over competitors, which helps to gain recognition and acceptance from target audiences.

One way to evaluate legitimacy-as-property is through *regulators' authorizations* that provides permits, licenses, or licenses to organizations (Suddaby et al., 2017). These regulatory bodies are in charge of ensuring that laws, rules, and standards are followed within a specific industry or area. When a regulator grants authorization to an organization, it means that the organization has complied with the norms or requirements established by the regulating body and that the organization adheres to the respective laws and regulations. Authorization through a regulatory body is important in proving an organization's legitimacy since they let stakeholders know that the organization follows quality or safety requirements.

3.3.2 Legitimacy-as-process

Legitimacy-as-process is looked at as an ongoing and dynamic negotiation rather than a stable condition. It analyses a process *"in terms of movement, activity, events, change, and temporal evolution"* (Suddaby et al., 2017) and tends to be found in ongoing social interactions involving multiple actors, particularly those opposing or seeking change. Legitimacy-as-process is therefore seen as following a single-one way trajectory, beginning at the "ground" i.e., when interactions start and is progressively constructed through time. This process eventually reaches a threshold or tipping point where legitimacy is established, this viewpoint emphasizes how legitimacy develops gradually and the accumulation of interactions and activities that lead to its formation.

3.3.3 Legitimacy-as-perception

Legitimacy-as-perception describes how people evaluate the suitability or appropriateness of an organization. Legitimacy-as-perception highlights that legitimacy is not just a characteristic of an institution but also a personal evaluation. So, both the individual (micro) and the communal (macro) levels of legitimacy exist within legitimacy-as-perception (Suddaby et al., 2017). Individuals create their own beliefs on a group's validity by considering both their own perceptions and those of others, contributing legitimacy to a collective phenomenon. Legitimacy-as-perception is therefore found between individual and collective evaluators (society, organizations, groups) and views legitimacy as a social construction that results from the interactions and evaluations of individuals. It acknowledges that people have a significant impact on how organizations are perceived, how legitimacy they are, and how they act in response.

Researchers apply theories from fields like cognitive psychology and microsociology to analyze legitimacy-as-perception. They look at how individuals classify and judge social issues, and how subjective meanings and outside influences affect how people form their opinions. Human beings tend to follow judgments they believe to be true, and these beliefs could be influenced by manipulation of perception or social pressure.

3.4 Legitimacy in the context of Blockchain in Elections

This thesis pursuits to study the application of Blockchain in public elections by collecting primary data from electoral officials, researchers as well as from practitioners of the topic. While voters, parties, observers, and others are primordial actors in elections themselves, their input towards the convenience of E-voting (via Blockchain) is important in an experimental and actual implementation phase, not in conceptual ones like the one we are discussing during this work. Therefore, collecting data as well as points of view from the mentioned actors is discarded for now, but would make full sense for future research following up ours.

3.4.1 Legitimacy-as-property

By looking at legitimacy as a piece of property, researchers could comprehend the institutional dynamics that exist within the electoral processes. It could show how Blockchain technology and the relevant institutions, like electoral authorities and regulatory bodies, interact. By treating legitimacy as a piece of property, the practical effects of Blockchain technology could be evaluated. Researchers could examine how the efficiency, transparency, and security of election processes could be improved by Blockchain. With the use of this dimension, researchers could evaluate whether blockchain technology can achieve their goals, adding to the voting systems legitimacy.

1. *Electoral Authorities:* Looking at applying Blockchain technology, institutions in charge of executing and supervising electoral processes, since they can (and will) be evaluated in terms of their legitimacy. Their acceptance of blockchain technology as a tool to conduct elections can increase the trustworthiness of the electoral process, in line with accepted norms, making them crucial to examine.

2. *Regulatory Bodies (for future research):* Regulatory bodies uphold electoral norms and standards, including governments, data protection authorities or cyber security organizations, are involved in determining whether blockchain technology is legitimate to use in elections. Understanding the legality of the technology under regulatory frameworks is an area that could be part of future research following up this thesis.

Significance: Examining the above-mentioned organizations enables us to evaluate how Blockchain complies with legal and regulatory standards and how they fit inside

existing institutional structures. It offers information on how Blockchain could be incorporated into the current electoral ecosystem and how it could be accepted.

3.4.2 Legitimacy-as-process

Legitimacy-as-process could be useful for understanding how Blockchain technology's legitimacy in election processes evolves over time. It allows researchers to investigate the ways that organizations adapt to changing societal expectations and increase their legitimacy. This dimension focuses on the ongoing negotiation and change that is required to keep legitimacy for the electoral sector. Legitimacy-as-process might also enable the identification of road-blockers that an adopter might meet when looking into Blockchain as an option to conduct an electoral process. Likewise, it can enable researchers to explore the variables hindering or creating acceptance of Blockchain technology.

1. *Practitioners*: Practitioners could examine the legitimacy building used by suppliers creating blockchain solutions for electoral processes while handling legitimacy issues, adapting themselves to shifting society expectations by examining their tactics during the process. Their activities affect the credibility and long-term viability of blockchain technology.

2. *Researchers*: Researchers play a vital part in interpreting the processes and the dynamics that shape it. They understand stakeholders' perceptions by analyzing governance and regulatory considerations, investigate which challenges or trade-offs that could occur and explore how these could be mitigated, making the researchers being part of the and establishment and maintenance of legitimacy. As an example, they might explore how characteristics of Blockchain, such as decentralization, could contribute to enhancing the legitimacy of electoral processes.

3. *Stakeholders (for future research)*: Stakeholders could shape the legitimacy of blockchain technology and negotiate through networks of electoral stakeholders, including political parties, civil society organizations, and voter groups. The dynamics of legitimacy may be influenced by their contacts and alliances. Stakeholder networks influencing the validity of blockchain in election processes is an area that could be part of future research following up this thesis.

Significance: Understanding Blockchain technology, practitioners and stakeholder networks could help to better understand the negotiation and adaptation processes involved in creating legitimacy and upholding it. Legitimacy-as-process helps in evaluating how well Blockchain technology aligns with shifting societal norms and impact of its adoption.

3.4.3 Legitimacy-as-perception

Legitimacy-as-perception could examine how voters view the legitimacy of Blockchain technology in political processes and show the voters' view and evaluation that affect their willingness to accept Blockchain in the voting processes. Legitimacy-as-perception could also include the opinions and evaluation of other parties and individuals involved in the election, such as candidates, political parties, and election observers. Researchers could therefore use this dimension of legitimacy to investigate how various stakeholders view the validity of Blockchain technology and how it affects the overall credibility and integrity of electoral outcomes.

1. *Voters* (*for future research):* The legitimacy-as-perception dimension could be understood in the context of individual voters. The acceptability and trust in the use of Blockchain technology in electoral processes are shaped by their views, beliefs, and judgments about its suitability and appropriateness. It is important to comprehend how voters feel, think, and judge in order to evaluate their acceptance of the use of Blockchain technology in electoral processes and is therefore an area that could be part of future research following up this thesis.

2. *Political Parties and Candidates (for future research):* Political parties and candidates are among the stakeholders in the political sphere who have their own opinions about the legitimacy of Blockchain technology. Their support or opposition to its implementation could have an impact on voters' perceptions and acceptance. Understanding the political dynamics around the legitimacy of Blockchain in electoral processes is an area that could be part of future research following up this thesis.

3. *Electoral Observers (for future research):* As indirect participants, electoral observers can offer insight into the legitimacy of Blockchain technology to

ensure fair and transparent elections. These people or organizations are involved in observing and evaluating electoral processes and is an area that could be part of future research following up this thesis.

Significance: Examining voters, political parties and candidates, and electoral observers allows us to better understand how legitimacy is socially constructed. Their viewpoints could influence how people accept, believe, and view Blockchain technology in relation to election processes.

3.4.4 Thematic Interpretation

Based on the three dimensions of legitimacy; legitimacy-as-property, legitimacy-as-process, and legitimacy-as-perception, a thematic categorization of organizations or individuals involved in the research of Blockchain in electoral processes is provided. The table emphasizes the individual or organizational functions and their inclusion in each respective category. The actors are primarily categorized using one dimension of legitimacy, but there is a dynamic interaction between the dimensions, and certain organizations may fit into more than just one category. This illustrates the complexity of legitimacy, and the variety of roles that different actors play in influencing it.

The following thematic summary table (Table 2) offers a visualization of the various actors participating. It acknowledges that organizations can influence legitimacy from a variety of angles and showcases the complexity of legitimacy as influenced by different variables.

Table 2
The table gives examples of relationships between actors and dimensions.

Organizations/ Individuals	**Legitimacy-as-property**	**Legitimacy-as-process**	**Legitimacy-as-perception**
Electoral Authorities	Evaluating conformity to norms & standard	Examining evolution and adaptability	Identifying public opinion

Practitioners	Displaying compliance to norms & standard	Navigating the dynamics of legitimacy	Improving perception among stakeholders
Researchers		Contribute to the understanding of legitimacy dynamics	
Regulatory Bodies	Future research	Future research	Future research
Stakeholders	Future research	Future research	Future research
Voters	Future research	Future research	Future research
Political Parties and Candidates	Future research	Future research	Future research
Election Observers	Future research	Future research	Future research

4 Method

4.1 Empirical Research Setting

This thesis was initially motivated from a proposal coming from the project called BLING (Blockchain in Government). The Bling project is an EU driven initiative that started in 2019 with the goal of studying how blockchain could be implemented into diverse governance aspects of public matters and processes across the different member states. To achieve their goals, the Bling project management established the so-called 'BlingLabs' across different regions in Europe. One of these regions is the North Sea region, which was founded by The EU program 'Interreg North Sea Region'. These BlingLabs brought together experts and electoral authorities to work together on achieving the project's objectives of digitizing electoral processes via the promotion of E-voting with Blockchain as the main protagonist. The cooperation started with 13 organizations from different countries, including the County Administrative Board of Skåne in Sweden, as well as various universities such as Edinburgh, Aalborg, Gothenburg, and Oldenburg among others, having its leading location in the Dutch city of Groningen.

The proposal caught our attention since we found a match between the Bling project and our own research interests towards what could be another application of Blockchain, such as E-voting, as shown in the literature review. This is the reason why we decided to focus on Blockchain implementation for Swedish elections as a case study and having it as a topic for this thesis.

Sweden consists of 21 regions, each with its own County Administrative Board, i.e., Länsstyrelsen, that delimits election districts and carries out the final counting of electoral votes. Each County Administrative Board in Sweden is therefore the regional electoral authority called 'Valmyndigheten' (Valmyndigheten, 2023). The County Administrative Board of Skåne is the only regional electoral authority acting as a cooperating member of the Bling project in Sweden, which made them the natural partner to focus our efforts. (For more information check Appendix 4).

4.2 Research Approach

To address the research questions, we chose an exploratory research design, semi-structured interviews, and a flexible interview guide. *Exploratory research* design could be used as qualitative research design when pursuing an interesting idea that can later serve as a starting point for a broader exploration (Swedberg, 2020) and when that idea has a flexible and open characteristic (Stebbins, 2001). Semi-structured interviews are suitable to investigate legitimacy, as Suddaby et al. 2015 has conducted. A *flexible interview guide* (Larsen, 2018) allows informants to expand on their responses with supplemental information relevant to the specified problem area.

As a case study, we chose the Swedish elections in order to explore the plausible implementation of Blockchain technology through the lens of legitimacy. This lens, according to our criteria, should be meaningful to study the impact as well as the dynamics and forces driving E-voting implementation. Specifically, the impact the insertion of Blockchain would have in the organization of public elections in Sweden, with the Skåne west region as first experimentation room. By applying the lens of legitimacy, we believed our aim will be easier to grasp due that it allows a holistic (social, organizational, technical) approximation to study the phenomena of public elections and its digitalization process by the means of E-voting and Blockchain. Other possible candidates such as cyber security will be referred too during this thesis though not offer multidimensional analysis possibilities as legitimacy does.

Literature reviews of more than 20 publications have been examined. The literature review was conducted to understand the benefits and challenges of implementing Blockchain in electoral processes. Although showcasing ad hoc solutions for specific contexts, the articles provided valuable insights into the understanding on what to regard when implementing Blockchain technology in electoral processes.

4.3 Data Collection

The data collection for this thesis was performed by conducting interviews using video conference platforms (Zoom and MS Teams). 9 semi-structured interviews were conducted and used as primary data. Interviewing strategy included targeting sampling and snowball method across partners. *Target sampling* is commonly used

when identifying informants who are related to one's research issue and being "snowballed" is an additional strategy used to refer to possible candidates for interviews, resulting in more relevant participants for interviews (Larsen, 2018).

Firstly, we reached out to the interviewees via email inviting them to take part in a 30–45-minute conversation. Surprisingly and luckily, in 7 out of the 9 interviews, the discussions exceeded 45 minutes, since the interviewees showed a high degree of interest and commitment towards the study of the topic, providing multiple insights from their different areas of expertise.

Initially, an interview questionnaire (as shown in Appendix 1) was created and based on prior literature (Lindman et al. 2020; Bhadoria et al. 2022; Amelin et al., 2019; Virayakumar et al., 2022; Anitha et al., 2022) and case studies that explored the implementation of Blockchain in electoral processes in other countries (Sanka et al., 2021), literature regarding E-voting (Cserny & Nemeslaki, 2018), and literature regarding legitimacy (Suddaby et al., 2017). This approach was used to create interview questions that were connected to existing knowledge and provided a foundation for exploring relevant aspects of the topic of Blockchain implementation in electoral processes.

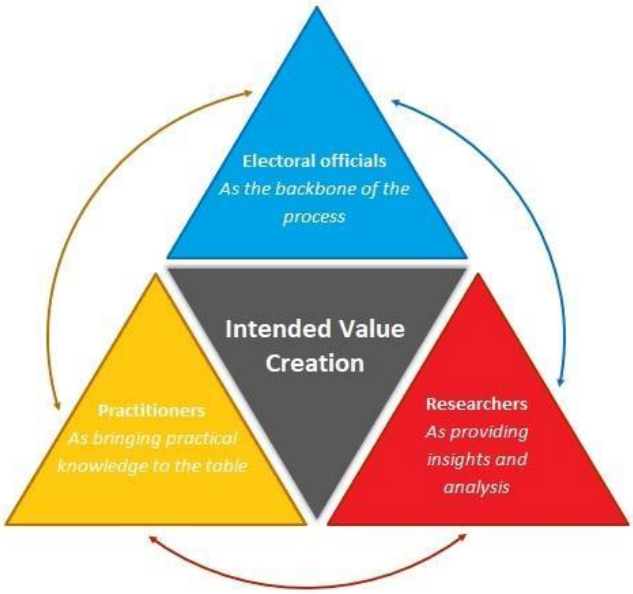
After the first interview, it became clear that the interview questions needed to be more open-ended and flexible in order to allow for further investigation and produce more grounded responses. This change was done to address the diverse profiles of the interviewees while enabling them to fully develop and tailor their responses from their individual scopes i.e., adapted to their respective fields, professions, levels of expertise and experiences with Blockchain and E-voting in order to maximize the quality of the input.

4.3.1 Execution of Interviews

Each of the 9 participants were categorized within one of *three areas of focus* based on their expertise to get an interdisciplinary understanding crossing law, research, and practice. The informants included key stakeholders such as representatives from electoral authorities (*Electoral officials*), a list of academic research contacts in and outside of Sweden (*Researchers*), as well as with digital assets experienced B2B product managers (*Practitioners*) from consulting industries with a high level of expertise on conducting end-to-end prototyping processes to the delivery of *Minimal Viable Product* (MVP) to industry early takers. The MVP is a tool used to validate

the usability hypotheses about a product or service. In order to do that, the company has to come up with a version of its product that is complete enough to demonstrate the value it brings to the users: a minimum viable product (MVP). It then needs to design experiments that will use the MVP to confirm (or refute) its value and growth hypotheses (Moogk, 2012). The intended insights from these interviews should contribute to a comprehensive analysis of the opportunities, limitations, and outcomes enhancing the legitimacy of Blockchain adoption to electoral processes.

Figure 3. Three areas of focus



To preserve the identity of our interviewees we chose to anonymize the data so that participants could not be recognized by either name or specific organization they work for.

Table 3
Informants code name within each respective area of focus

Area of focus	**Code name**	**Location**
Researcher	Professor of Communications Systems	Cambridge, UK
Researcher	Blockchain Expert	Gothenburg, SE
Researcher	Legal Expert	Gothenburg, SE
Electoral official	Operational Architect	Gothenburg, SE

Electoral official	County Council Project Developer	Malmö, SE
Practitioner	Blockchain Lab & IoT Expert	Emmen, NL
Practitioner	Product manager 1	Gothenburg, SE
Practitioner	Product manager 2	Lisbon, PT
Practitioner	Cyber Security Expert	Frankfurt, DE

4.4 Data Analysis

First step: Since our research uses an exploratory approach when investigating the implementation of Blockchain in electoral processes, it is important to note that there is no existing framework specifically addressing nor summarizing the lens of legitimacy of Blockchain technology in electoral processes. Due to the gap in the literature, we took the initiative to develop our own table for thematization, analysis and visualization (as seen in Table 2) of the main ideas represented on the analyzed data i.e., the findings and insights from the interviews combined with the referred lens.

Second step: Transcribing the interviews was the second step in learning about the data. By focusing on the connections to legitimacy, this technique helped us in developing a greater knowledge of the context of the interviews. The interviews were transcribed using Word, as well as manual transcription, and they were coded according to a series of categories or variables that we identified as most discussed. This served as the initial basis to start the data analysis process.

Third step: After transcribing, we coded portions of the material related to legitimacy as we read through the transcriptions several times and produced summaries that showcased important ideas that are relevant to legitimacy. The analyzed information, themes, and patterns, representing how different aspects of legitimacy could be interpreted is presented in Section 5, Results.

Final step: As the final step of the thematic analysis, we synthesized the themes and performed an iterative revision of the findings, comparing notes, and focusing on the themes connected to legitimacy in order to provide a coherent examination with the chosen conceptual framework and strengthen the thesis trustworthiness.

4.5 Ethics

Four research ethical principles were applied and achieved as follows:

- To fulfill *the information requirement*, the interviewees were firstly introduced and educated about this thesis.
- To fulfill *the consent requirement*, the informants provided permission to record the interview.
- To meet *the confidentiality requirement*, all recordings and transcriptions were stored on an external hard drive that was kept locked indoors until the thesis was completed and then permanently deleted.
- To fulfill the *utilization requirement*, we established that all information acquired from this thesis will only be utilized for research purposes.

The *four research ethics principles* (i.e., information requirement, consent requirement, confidentiality requirements and the utilization requirement) are generally used for basic individual protection when conducting research (Bryman, 2011).

5 Results & Findings

This section presents the findings of the series of conducted interviews described in Section 4. Common topics and areas of interest were identified among the first 2 groups of interviewees: Electoral Authorities and Researchers. The process derived into 3 main concepts (Technical, Organizational and Legal) that can englobe the requirements of identification of the need space i.e., Legitimacy. The chosen concepts among the identified themes and patterns show the required degree of interconnectedness, detail on the information and managerial complexity this thesis intended to detect.

The last part of this section describes the solution space that the third group of interviewees (Practitioners) enlightened, by sharing their experience as leaders in the development of Digital Assets Solutions. The interviewees added value to this research by providing a practical perspective on the precepts formulated by Von Hippel & Von Krogh (2016) in their Need-Solution pairing approach.

5.1 Technical Aspects

One of the main concerns towards Blockchain is its security features. This perception is eventually fed and increased with the lack of knowledge from possible adopters on how the system would respond to a possible attack or if it is hackable. The County Council Project Developer acknowledged a lack of expertise in Blockchain, despite of that addressing its potential as a technology that could be utilized to achieve a secure and transparent voting process. While this could be linked to legitimacy-as-property i.e., evaluating if the implementation of the technology represents an upgrade (Pragmatic legitimacy) in the operability of the process, the interviewee also expressed about the negativity when referring to Blockchain among Electoral Authorities i.e., Legitimacy-as-perception from a given group.

"First of all, I'm not a blockchain expert in any ways yeah, I'm not a computer man. For me it's a tool that can be used in different ways to develop things. It's a secure way of, in our case, running polls and elections and the problem that we have when we talk about blockchain is that it's very strongly connected with the Bitcoin and the crypto things and there is rather quite a lot of negativity when it comes to talking about blockchain, but for me it's a tool that can be used. - County Council Project Developer

For adopters with specific requirements towards compliance and control, it is important to find the balance in the searched solution, in order to meet their local jurisdictions' regulations. The County Council Project Developer emphasized the authority´s need for security and compliance aligned with regulations, such as the European GDPR. Studying how Blockchain could address concerns about secure data handling and adherence to standards links to legitimacy-as-property, as the developer considers Blockchain as a plausible tool to ensure control, compliance, and security.

"The other examples we've looked at, the main problem was that it wasn't secure, it wasn't servers in the US, in the Asia using. That's our main concern that we have to make it secure, we have to have control of all the procedures concerning the process. We can't rely on the servers that's out well controlled and so on. That that's the main concern, that has to be secure, and it has to follow the European GDPR on personal security and so on, so that's our main concern when it comes to criticism of the techniques that's been used in other areas in around the world." - County Council Project Developer

It is important to clarify that verifiability, for the means of Blockchain technology, often takes the shape of what some specialists refer to as End-to-End verification (see Appendix 3 - Glossary)**.** The Blockchain Lab & IoT expert talked about the importance for the citizens to be able to have proof of their votes in the end results, and suggested Zero-knowledge-proof, as an approach, making anonymity possible for the users within the Blockchain technology.

"That's the problem because I want to have a proof that my vote was in the end result, but I should not be able to see what I voted. Now and there you go into technologies like Zero knowledge proof, homomorphic encryption, and that kind of stuff, which is a little bit hard to understand, but if you see what the mathematics can do there and how your anonymity is guaranteed, and we are still able to count these votes, that's magic. Right, and that will help the process." - Blockchain Lab & IoT Expert

The results derived from the interviews highlighted the concept of Zero-Knowledge Proof that has been previously highlighted in the reviewed literature (U.S. Vote Foundation, 2015) during this Master thesis. The Zero-Knowledge-Proof is, according to the U.S. Vote Foundation (2015) a way that one can prove something to someone else that one knows, without showing how. It represented an advancement in the Blockchain Technology in recent years compared to previous features such as Proof-of-Work (PoW) and Proof-of-Concept (PoC) (Abuirdris et al., 2021).

Another recent interesting feature from Blockchain that came out during the interviews is the so-called Proof-of-Person (PoP) which in essence is a "proof of humanity" and avoids attacks from chat bots, which is also referenced in the literature by Crowcroft (Shahzad & Crowcroft, 2019).

Both Zero-Knowledge-Proof and Proof-of-Person are clear representations on how Blockchain keeps its innovative character as technology, while at the same time reinforces, in the point of view of the authors of this thesis, the need of continuous exploration towards its potential respectively non-discovered benefits. Looking at different ways of doing things and conducting processes enables generativity, while at the same time going in line with the proposed lens of legitimacy for this thesis.

Another important topic that was addressed by the Blockchain Expert was Security/hacking and the Expert did that by highlighting how the de-centralized nature of Blockchain helps for the means of security as well as the tool having a record of being immutable towards hacking attacks:

"It's pretty obvious it is transparent, it's all there and you know it's immutable as well. So once a vote is recorded on the blockchain it cannot be changed, deleted "- Blockchain Expert

Re-addressing the common association of Blockchain with Bitcoin and the world of cryptocurrencies in relation with the security features of Blockchain**,** the Cyber Security Expert provided a further explanation of two crucial concepts commonly heard and used but often poorly understood: Cryptography and Encryption. The explanation was about how the security aspects are mostly built on cryptography and there are different versions of it:

"There are different methods of cryptography, and everyone has its own algorithm which is being used. One is more secure than the other one. And yeah, encrypting is the process of making a cipher out of specific information and decrypting is the other way around, having the cipher and trying to reconstruct the information out of it by reversing the algorithm." - Cyber Security Expert

Furthermore, while cyber security is also a widespread term among average technology users and pointed out as a primordial feature in the wishing list of adopters, the broadness of the approach is not fully understood and often ignored:

"So, the goal shouldn't be cyber security, it should be information security" - Cyber Security Expert

The Cyber Security Expert also mentioned other aspects to take in consideration when it comes to information security:

"I think you would have to distinguish between two types of attacks that are common when it comes to blockchain, and I think every other kind of service there are the attacks that try to attack the system itself, and they are the ones that try to attack the users." - Cyber Security Expert

While the innovation character of some nations, like Sweden, might be an initial motivator for pursuing digitalization on traditional paper-based processes such as elections, on the researcher side a call was made for adopters in the public sector to consider the need and costs factors up-front by assessing their local realities (ad hoc solutions).

"The motivation was to reduce the level of voter fraud and corruption coercion. Individuals or organizations, there are those sorts of social argument. Interestingly, in the UK, we have almost zero voter fraud. There's that one case a year, out of 35 million voters. So, it's very, very rare. And so, one would not consider such an expensive technology really necessary. In fact, the cost of a paper voting system is fine." - Professor of Communications Systems

However, the consensus among the interviewed practitioners is quite revealing (while also might reflect a different level of understanding compared to authorities and researchers) i.e., E-Voting and Blockchain can address on how to mitigate levels of voter fraud and coercion.

"That's a great question. I think that I already mentioned, but my favorite one is Brannfords work on proof-of-person. And I for a voting system, I think this could be very appropriate for anything that requires verification of identity of the voter. It could be a very powerful approach and it has this property that it doesn't have very high-cost computational cost that way Proof-of-work has. So, the only working proof of work system we have today is Bitcoin, the Bitcoin platform, and it is pretty robust. I mean, many other cryptocurrencies have proved problematic, but Bitcoin is, you know, surviving and it fluctuates value, but so do real current Fiat currencies. But it is too expensive for a system that might have a high throughput every now and then. Having said that, we use Bitcoin in a trusted ID system called trust chain that we have some papers on and software, but we only use it for a node identity, not for user identity. So, it's a very occasional thing when you're on-board new nodes in our network and then we literally use the Bitcoin proof-of-work system, but that's specifically to prevent Sybil attacks, which is a very particular

threat, and we built the network of nodes which is de-centralized. We can then run that with regular ledger systems. If you want, actually, we don't even need a ledger. Just de-centralized replicated service, but we can use the ledger properties for other things, but yeah, so I think that's sort of two things. One is more specialized use of blockchains, where even with proof-of-work, if you know you're only using the proof-of-work, occasionally the rate of increase in cost does not have to be too expensive and the other is systems like proof-of-personhood, which are relatively new, and there are other criticisms of those. Maybe, but I think they're very interesting socially." - Professor of Communications Systems

There is a dichotomy when implementing a new digital technology: If firsts attempts should go digital from the very beginning or to a hybrid model. Some interviewees stated that one of the problems is that experts will understand the repercussions immediately but that is not necessarily the case with the public, and in the end, they would need to trust the experts. On that note, the Professor of Communications Systems showed himself critical about the trustworthiness of such implementations.

"There's a dependency in trusting the government and trusting the service that functions of government, and if you don't trust the government, then you have an inherent distrust of the service too. So, there's a kind of barrier there to using a solution which doesn't solve the distrust in government problem anyhow. So, if you have a perfect voting system that's electronic, it produces a result that the government can just modify the result, ignoring it. Ignore it as it transfers, so then you have a problem, so it didn't help having a blockchain in that." - Professor of Communications Systems

However, the primary goals of implementing a de-centralized ledger technology (DLT) are not strictly related to build up trust, rather identifying what are the best areas (fields) of this technology to be implemented. This constitutes a paradox for our case of study.

"Whereas there are other systems, for example where you want trustworthiness where the government might provide ID for some service, for example, you want to prove your university credentials. You want to show that you've got a master's degree from Gothenburg University, and you want to prove that. But that's issued by the university. But why do you trust the university? Well, maybe the university is given a certificate by the government, and so we have a chain of trust..." - Professor of Communications Systems

Besides the already several times mentioned decentralized technology features, interviewees were questioned on what extra benefits could Blockchain contribute within its application to E-voting. The Blockchain Expert provided a glimpse on this matter and talked about the potential benefits of using Blockchain in voting including efficiency and getting rid of human errors. This aligns with legitimacy-as-property as the Blockchain Expert recognizes Blockchain as a valuable resource for improving voting systems.

"The thing is here they need time right to count to vote, and that makes sense. But humans are error prone, like we make errors all the time. It's like 9:30[am] *and I've probably made a couple of errors today already. You know they are constant, like you know, you have these people there. I mean, are they even getting paid? These people, these volunteers, counting votes? Like they have no incentive to do that job and great, and you see videos... I saw videos from the US where people like hiding boxes of votes and this and that, they all have, you know, their own kind of agenda here, I mean, talk about efficiency. You don't need that; you can just remove that human dependency altogether. And you know, it's like you're saying... I mean, you have swish, or bank ID, whatever… It would be the same thing… You would have a wallet, so it's one vote, one address. So, you would have an app, you would just vote and then you can't vote anymore and it's there, it's immutable. It's done."* - Blockchain Expert

But what are the added dimensions that the Blockchain technology would add in the case of E-voting? Common denominators mentioned by the Blockchain Expert were votes being traceable and verifiable by the voters at the micro-level, however repercussions at the macro-level can be accounted on the technical side:

"First of all, you need to be able to scale it, right? I don't think it's the biggest issue anymore. To be fair in blockchains, I think in terms of just voting, they're scalable I think usually when you talk about scalability in blockchain right now is that exercising direct democracy in communities can it's a challenge, right? Even if you have the system to do so, it still needs to scale, right? We are still talking bigger than currently, you know". - Blockchain Expert

But also, on the cognitive level of the public. Important to highlight here, is how the Blockchain Expert discussed scalability, security, and accessibility in Blockchain-based systems, attributes of legitimacy-as-property.

"We're talking millions of people using it, so it needs to scale right? You know, like I said, transparency is kind of a strength, but it also needs to be to be private and find that balance to protect anonymity. Like I said, you know it needs to be secure. You kind of mentioned hacking. I mean it is a real threat, right? I think there are too regularly, I think I would say certain networks or… It's usually not the networks themselves, but usually bridges, what what's called a bridge. So, when you try to, when you are kind of building bridges to send tokens across networks, when two systems that aren't kind of fully compatible, they kind of those are usually that gets exploited. But yeah, I mean security would be massive, right? And also, taking access as well, right? I mean, not everybody's technical. I think that's a big hurdle right now. If you go in the crypto space, you know it's kind of, it's fairly technical and you need to have that knowledge usually to participate" - Blockchain Expert

As well as in the ease-of-use of the electoral system itself, what to some degree would enhance the democratic character of the system:

"I mean it's improving all the time, but accessibility would be a big one as well. Regulation I would think I'm not, I mean, and I'm biased here of course. But when I'm thinking about it, seems like it's pretty straight forward there. I mean, you know, I, but I would assume there are legal challenges and ethical kind of challenges involved. Not that I would be able to speak on them on any kind of length, but yeah, there is always regulation and stuff, right. But personally, I think you know the benefits outweighs the challenges you know at least, I mean, at this early stage, you know the potential seems to be pretty extraordinary. So, it's kind of worth giving it a go if that makes sense." - Blockchain Expert

However, the Operational Architect went beyond how secrecy of voting and personal ID is preserved on E-voting systems and discussed the encryption within electronic voting systems. This aligns with legitimacy-as-property as the architect acknowledges the technical aspects of E-voting systems and their security features.

"that's sort of how I have understood that the electronic voting schemes work, that you have your vote that is enclosed in an encrypted envelope. And then you have your personal information alongside it. And then everything has encrypted around, so that package could get sent around and then you sort of decrypt it as in layers." - Operational Architect

5.2 Organizational Aspects

The introduction of a new technology, especially when it is about the digitalization of a traditional paper-based process, is not a high-speed highway. Interested organizations or adopters should communicate effectively with their target groups in order to achieve levels of acceptance and shorten times of adoption. However, such processes must be understood as gradual and having phases of implementation. E-voting would not be the exception towards achieving massive levels of adoption. Aligning the former with legitimacy-as-process, organizations should additionally look to overcome roadblocks while reducing adoption time.

"Look at online banking. It's the same right. So, you now have a hybrid system where people use online banking and pay with their phone and their watch, etcetera. But you can also go to the bank and get money. Granted, I don't know how it's in Sweden. And this 90-year-old lady comes to the bank to retrieve some money. They don't give it to her. They go to the machines, like I'm going to come with you.

I'm going to show you how you can do it yourself the next time. Right, and the next time she goes inside again, they will help her again and show her at the ATM machine. They're a little bit stubborn like that. But that's, I think, the transition phase. Also, so people can vote on their phone, they can also go to the polling station and vote there, and their last vote, their most recent vote, will be the actual vote that's put in. We need that because the acceptance of voting on your phone will be, I think, less than 50% in the first year, right and it has its merits voting in the way in the conventional way, we do several tricks that we don't realize, right? One of the tricks is you must go into the voting booth on your own. You're not allowed to take anyone with you. Right. We think that's normal. Right. But there is a reason for that. There is a reason so I cannot coerce you in voting for me, right? OK, so that's normal and everybody accepts that. But now I'm sitting on my couch at home, right? There's nobody watching me. There could be somebody sitting next to me and saying now you're voting for me. Right. So, coercion is something we have to have a solution for in the conventional way we thought that out we've been voting in that way the last 150 years right. Voting is also relatively new" - Professor of Communications Systems

Adopters often might have different motivations towards experimenting with the implementation of a new technology or solution.

"Digitalization is running everywhere, so it has to be, sooner or later, also in the electoral process." - County Council Project Developer

Though, there is often a lack of consensus among adopters, while curiosity and trendiness can be an impulse for some decision makers to inform themselves and even piloting some projects to check on the viability of the "new solution" other seem to be more skeptical and prefer and are more in favor of a preassessment.

"I don't see the need for it. I don't see the problem that needs to be adjusted and then as we move on, we go to voting stations, setting up voting stations where they are again. Not really a problem." ….. "a problem to get hold of enough locations and enough people working. But that's more of a resource problem." - Operational Architect

During our research of elections around the world, we didn't find any major cases of cheating or doubt in Sweden's elections. While we looked at important elections in different countries, Sweden's elections seemed to be perceived as fair and trustworthy. This discovery made us wonder to ask the County Council Project if they viewed the Swedish elections in the same way.

"Yes yes, that's yeah without doubt without any doubts this yes." - County Council Project Developer

Misconceptions and misunderstanding are typical sources of skepticism and in the case of Blockchain and Bitcoin this is not the exception. Some topics are perceived by the regular citizen as to be understood only by experts but at the same time are a popular topic of conversation, that is the case in the confusion of using terms as Blockchain and Bitcoin interchangeably. Since the goal of this work is not to deeply explain technical aspects, the only clarification needed is that Bitcoin is in essence only a byproduct of Blockchain among many others. Those byproducts (often referred to as protocols) are not only related to financial transactions (cryptocurrencies) but to a series of application fields. While addressing this topic, both the Professor of Communications Systems and the Blockchain Expert point out the system failures experimented by Blockchain products such as Cryptocurrencies. Parallelly, both highlighted that the skepticism about Blockchain has a weak reasoning since a perfect system, not to mention the ones governments might be working with now, is not to be found yet for any application or purpose.

"Many cryptocurrencies have seen complete failures. Put in back doors and then steal all the money and you know it's been unfortunately common. And so, governments, when we talk to governments about using ledgers or just decentralized systems, the governments have very reasonable rejections." - Professor of Communications Systems

"You know what happens in crypto doesn't always favor blockchain development. I mean because crypto is a little bit of a Wild West. There's a lot of things going on there, so especially when you have situations like FTX. So, if you have situations like that, people take that as blockchain is bad, but actually the situation only speaks even stronger to why blockchain is needed"
- Blockchain Expert

Additionally, the Professor of Communication systems and the Blockchain Expert point out the arguments in favor of Blockchain related to those same "failure cases", which are not widespread in the popular perception, due to misconception and lack of technical understanding. This is immediately palpable by observing the following quote from County Council Project Developer:

"The problem that we have when we talk about blockchain is that it's very strongly connected with the Bitcoin and the crypto things and there is rather quite a lot of negativity when it comes to talking about blockchain" - County Council Project Developer

Despite the hype of Blockchain through different application fields, levels of information still seem to be uneven among possible adopters (Electoral Authorities in this case). The County Council Project Developer referred to Blockchain as the most "secure" way found so far for the means of digitalizing an election. The County Council Project Developer once again talked about the negativity when referring to Blockchain among a specific group i.e., Electoral Authorities and Government Officials. While this statement links to Legitimacy-as-perception of the mentioned group, a much broader study among voters and other important actors, when validating Blockchain for electoral purposes, would be necessary prior to implementation.

"The Swedish system that we use for election is very secure and we have to stress that, that's a very important thing to mention. We go in the way of developing things digitally and this is just one piece in that process, and as a technique, blockchain is the most secure way that we have found so far that might to be used when it comes to elections and so on. But the securities, the system we use in Sweden today, with paper voting, is very secure, and it has to stay secure, even with the new technique." - County Council Project Developer

Another interviewee, the Blockchain Expert, mentioned a big factor for the successful implementation within a new technology implementation project such as Blockchain in public elections: Education.

"I think education is probably a big component and making people understand, you know, making it accessible. I think currently you know, it's yeah, it's too complex." - Blockchain Expert

Transparency is definitively another major aspect, requisite and a goal when talking about elections (and in the search of Legitimacy), but despite that the concept seems to have different levels of understanding among the interviewees. We asked the question on how Blockchain having implemented, as voting processing and counting system, would make the results of any given electoral process available and visible in real time. This feature was evaluated differently among the interviewees. For example, the Blockchain Expert pointed out not seeing a problem having real time data the day of the election visible during the day of the election.

"You get these benefits; you know you could do so much more with a dashboard and user experience and know it's updated instantaneously. You can track the, you know, imagine if you did this in an election in Sweden where you could have real time data updates for every municipality, every region." - Blockchain Expert.

However, other interviewees pointed out that this could affect the judgement of the voters on election day, producing biases. The Operational Architect highlighted that if results were reported live, while the election is being conducted, could create anxiety while having side effects:

"D*uring counting we publicize each precinct counting, each district. We are people counting constantly from election night, 2 weeks on. And so, the votes shift constantly. Now it's in this party has 30.2%... now it only has 31%.... and now it has 22… What happened? And some people get very anxious, anxious about this, and start Twitter storms, about cheating and whatever when it's just normal counting. So, one application could be to log each change. Now we have counted this precinct, bam… So, in retrospect, one can follow each change, immutably. As opposed to now, when we must be… we have log files, we have log stamps, but those are provided by us."* - Operational Architect

But is there an alternative for reluctant authorities to give away control on the process of the election to implement Blockchain? According to the Professor of Communications Systems there is a scheme available that would make this possible as long as the government in question counts with the needed resources:

"You can run a blockchain on a semi-centralized service. So, for example, there are several blockchain services or ledger services on cloud platforms which are inherently centralized…" - Professor of Communications Systems

The creation of a digital national ID as pre-requirement for implementing Blockchain for elections since the current digital infrastructure of Sweden is not suitable for that particular purpose. The County Council Project Developer stressed the importance of a national digital ID under government control as an important requirement for Blockchain implementation. This emphasizes the property aspect of legitimacy, where a secure and controlled foundation is required for the technology to be considered legitimate in an election context.

"First thing we require is the National Digital ID that is controlled by the government, by the state. In this case in Sweden, Bank ID it's owned by the banks, it's owned by private company that the banks are running together. In principle, they can sell it tomorrow to China or to company in US and then then we lose the control the national control of the system. So, what we have to do in Sweden, first of all, is to establish National Identities, that is controlled by a state authority. That's the main concern, you have that you have it in Denmark, but you don't have it in Sweden for example. That's the main problem here, using the technique that we have today." - County Council Project Developer

5.3 Legal and Political Aspects

The Legal Expert highlighted the framework that digital initiatives have in Sweden as well as in the European Union, and responded to our inquiry if resistance exists towards them from the authorities. The legislative reluctance exists towards implementing new technologies in general, not exclusively about Blockchain. The reason

is that creating specific legislation increases the risk of unintended loopholes or creating unintended blockages. The gradual process, through which the legitimacy of a new adopted technology could be threatened, is a matter of Legitimacy-as-Process and of recommended future research.

"Yeah, I would say there is sort of a… maybe not resistant, but reluctance rather. It's kind of the same with AI technology. The EU has done, I mean the steps they have taken so far, there are more legislative texts coming relating to like, liability and stuff like that. But that's more on a product perspective. But looking at AI as a technology area, well the most legislative… it's like ethical frameworks to sort of help the Creators guide themselves towards following the rules that are already there, I would say. So, it's not blockchain in specific, I would say that's sort of the general approach to technology. And then with technology has specific areas of technology has a few years behind them. And there have been like evident problems... And looking at for example, looking at sort of the platform technologies and the platform business models we started seeing legislative changes there just in the past few years, but they have been around since like early 2000s or 2010. No process." - Legal Expert

Authorities in Sweden in charge of the BLING project emphasized control, traceability, transparency, and costs criteria in their consideration for Blockchain for election. However, the technical implementation challenges were joined by legal implied ones that they were initially not aware of. Despite of having previously endorsed its features and capabilities, the County Council Project Developer expressed concerns regarding security, control, and compliance with GDPR when implementing Blockchain for electoral processes. This includes both Legitimacy-as-Process, where the adoption process must ensure security and transparency, and Legitimacy-as-Property, as adherence to legal and data protection regulations is paramount for establishing Blockchain in electoral processes.

"The other examples we've looked at, the main problem was that it wasn't secure, it wasn't servers in the US in the Asia using... uh... that's our main concern that we have to make it secure, we have to have the control of all the procedures concerning that the process. We can't get relied, we can't rely on the servers that's out well controlled and so on. That's the main concern, that has to be secure, and it has to follow the European GDPR on personal security and so on, so that's our main concern when it comes to criticism of the techniques that's been used in other areas around the world. "- County Council Project Developer

One of the first challenges we found when getting in touch with the electoral authorities for this project was the series of assumptions that were made in legal terms. The digitization of a paper-based process is not only technically challenging but an extremely complex challenge from the legislative perspective. In the eyes of the Legal Expert, those legal questions -connected to legal principles- are to a large extent also technological questions. Therefore, the gradual process of legitimizing a new technology involves aligning it with legal frameworks, while considering fundamental democratic principles, like valid identification, secrecy, and freedom of voting. Ensuring these principles through technological adaptation links to legitimacy-as-property ("How do we do this?") as well as to legitimacy-as-process (since doesn't consider legitimacy as given-stable condition), whilst also touching upon legitimacy-as-perception when highlighting the individuals (micro-level) right to secrecy toward society (macro-level) as a whole. Both the legitimacy-as-process and legitimacy-as-perception concerning legal aspects of a new technology adoption represent good future research opportunities.

"it's very interesting from a legal perspective because those are usually and at least in Sweden. Those legal principles are based on our constitutional *law. So, it's like the strongest legal framework we have can't just be changed. However, it must be like two electoral processes in between and people have to agree. There's a really long process to change it, which sort of makes it and just signifies the fundamental importance of those kinds of laws for our societies. In Sweden, we have the principles that our electoral processes should be secret, which I think is a very interesting in relation to sort of blockchain creation, because how do you ensure? While at the same time tracking things. And while at the same time, like sharing that tracking, probably if you're going with the entire transparency and decentralization principle. And then, so the trip I suppose it's like and the elections should be secret, and they should be free. So, you should be able to vote for whatever you want. And the secrecy is sort of a fundamental requirement for that freedom, in my opinion, and I think in the legislature's opinion as well, is by knowing that no one else can see what I vote for, they can track what I vote for. They're no consequences for me personally. Apart from the sort of the political level that affects society as a whole. I can vote. Vote for whatever I like without the fear repercussions. And I think. Like with a good… I think those are probably the things that people stumble upon when they don't take that into consideration in their initial creation of the blockchain solutions."* - Legal Expert

However, Blockchain for elections doesn't seem to be in the political nor in the legislative agenda in Sweden.

"We have to be very precise in what we want changed. Meaning that we have sort of narrow minded ourselves. We can't look at everything at once. So, for instance, the most popular thing that people talk about is Internet voting or digital voting. That is not on the agenda because it's in the law, you can't vote on the Internet, so we don't think about that. But if we were given the assignment, we will have to solve it and we will solve it if given the assignment. There was a public inquiry, SOU, in 2013, which suggested that there should be a "försöksverksamhet" [experimental operation], *a sandbox experimentation with Internet voting in 10 years ago. That was a suggestion, and it was discussed, and it was not launched, it was not in law, so there was a discussion some years ago and then I think, and we sort of informally think that the changed security worldwide factors have about troll-factories, and this is not on the agenda, there's no one pushing for that. But if since you frame the question in a more intelligent way than I suspected, how can it be used given all? One discussion that we have is during counting, we publicize each precincts counting each district."* - Operational Architect

"No discussion and one need to understand that the election legislation is highly detailed. We are not free to pick and choose what to digitize or what not digitize." - Operational Architect

One of the main challenges of every new system prior to the bare consideration of implementation, digital or not, is to be able to preserve the fundamental principles inherent to the process in question, such as conducting elections. As already mentioned, from the voter`s perspective anonymity, freedom and no repercussions are the pillar ones:

"And the secrecy is sort of a fundamental requirement for that freedom, in my opinion, and I think in the legislatures opinion as well is by knowing that no one else can see what I vote for, they can track what I vote for, they're no consequences for me personally apart from sort of the political level that affects society as a whole." - Legal Expert

"Because once you have something that is tracked and is stored. I think you will stumble upon sort of the 'how' do I ensure people's identity that they are citizens, they have the right to vote while at the same time not compromising their secrecy." - Legal Expert

5.4 Solution Space

For possible adopters to be able to implement new technologies or techniques into their processes, it is necessary for them not only to have a minimal understanding on how the developers of the solution work but also to provide them with the necessary input to find the best possible, ideally, addressing the adopters "needs" and "wants" as Product Manager 1 explained:

"Actually, what product manager does is that connecting people and teams together and also with the with the markets, with senior level managers. So basically, what I do as a product manager is that I work with almost every team in the company from customer success to support the developers design, then I connect to customers. Then I connect to senior managers, and I try to bring everything together so that we can understand what are the problems in the market, what are the problems for the users, how we can solve it? So how I do it is usually I have to be in very close contact with customers." - Product Manager 1

Adopters, ideally, have to have and be clear on their requirements and needs in order solutions providers can fulfill them and formulate the right proposal.

"'Head of product' is also involved. But then when it comes to the actual MVP and really getting things done, you know to that level, then it's the 'product manager'. Usually, we call it like 'product trio' is also like in in theory that is the product manager is a designer and it's a developer 'head of development'. So, these three, we will sit together, and we discuss." - Product Manager 1

Active participation from possible adopters is in fact very important in order to define the need as well as for achieving the goals of implementation while having a real impact in the redevelopment of the process in question, in this case elections. New concepts can refer both to an invention or a new application of an existing technology.

"If you're bringing some concept to the market that hasn't been existing, try to do some user tests, try to show it to people to see what they think about it and sometimes it's also impressive. For example, it has happened to me that sometimes me and the designer, I mean he has designed something that he's also not very happy with it." - Product Manager 1

This is crucial to define the needs correctly, delimiting them and achieving a scope and plan of work with the adopters for them to be able to experiment correctly with the technology or innovation.

"... I was working in this company that we had a pool of users who had signed up with us that we would like to be like testers. And then sometimes we were sending them, for example 2 versions…. we were monitoring how they were working with both of them and then we would see, OK, which one is better? We were asking for the feedback. Which one did you feel was better? …." - Product Manager 1

Besides having their needs clear, which cannot be taken for granted, adopter should be as precise as possible on explaining the generalities of the problematic as well as important details to the solutions providers, while granting them access to the relevant data they request, all under the respective data conventions.

"What is the problem of the customer if you are designing this? What is the thing? So, let's just make it very simple. The customer inputs something into this process does something on it gets the output, so should see what's the effect of this output on the previous like. What is the situation? What is the future situation in this process? So, I would say it's more like, Who is?... If I want to say it in a process, do I understand who is the user? What personas are we talking about? What do they want to do and what do they want? What do they want to get from it? Then when I have this whole picture… That is the base for my MVP." - Product Manager 1

While considering a possible set of solutions once the problem has been properly defined - and the balance needs and wants is clear- thanks to the fruitful interaction between the adopter(s) and the developers of the solution, the process of conceptualizing and developing a base in which the adopter can test the needed/ desired features starts. This is where the solution space in the so-called *Dual Track Agile* (Trieflinger et al., 2021) method starts. Moreover, it marks the moment where two key concepts in the results part of this thesis appear: Prototype and Minimal Viable Product (MVP).

Prototype and Minimal Viable Product (MVP) are often confused with each other, paradoxically to Blockchain and Bitcoin, but it is while it is important for adopters to understand the differences among them, their experimentations and testing will take place using only one of them, the MVP:

"It was not in the MVP, but it was more like in the prototype level that we were sending them like these two versions and then we were monitoring how they were working with both and then we would see, OK, which one is better? We were asking for feedback. Which one did you feel was better? So, in that sense, when it comes to prototype there is a very thin line between MVP and prototype, maybe in some companies they call the MVP as prototype" - Product Manager 1

A prototype is less relevant from the adopter´s point of view due that it is a pre-version not suitable for testing, however the adopter`s input is crucial for the development, Product Manager 1 and 2 helped to understand the chronology while clearly stated the difference between Prototype and MVP.

"Yeah, I would say that 'prototype' is very just simple design. So how for example we have worked with it is that the designer just design something. Is even in a PowerPoint page, so they just design something and but then you can do an interaction with this design, that is what we call prototype in my context" - Product Manager 1

"Yeah, so a prototype is an earlier version of the product that. Its only function is to basically demonstrate to your users what it does… It might not do the work. But it would convey very easily. It would make the users understand very, very easily what the product should do. Or, but it might or might not do the work right…. it does still work, it does it super clumsily, but it does the work, but at the same time it's not scalable. You cannot really build something on top of it and release to users. But you can build it super fast and cost is right, but this is what a prototype does essentially" - Product Manager 2

Paradoxically, while few adopters are conscious that they have a problem to solve, it cannot be assumed that they fully understand it nor have the willingness to do it.

"I usually ask these kind of like techniques of for example, why this like 5 Why techniques, that you ask 5 several guys in the process so you can get deeper and deeper and deeper into something. And because we already have existing customers, so it's not that we want to bring a totally new product to the market. Then I would ask them questions about our existing product, things that what they use, what they don't use, why don't they use it, what we can do so that they use it? You know this kind of question. And then I work directly with two teams all the time, which is design and developers." - Product Manager 1

When it comes to the solution dimensions that Blockchain can contribute with, one of the interviewees, the cyber security expert explained how achieving a full solution in terms of the 3 main aspects 1) decentralization 2) scalability and 3) security is still not technical feasible nor fully available. He referred to this as the *Blockchain Trilemma*:

"Especially when it comes to AI and other topics. But that's another thing. I think I'm not sure how you or I'm not sure if it's possible to use the same system and update it the whole time as the future comes or if it would be easier to implement. Updated systems and replace the old ones because, especially with blockchain, there's a thing that's called, 'blockchain trilemma', and it describes that you're trying to achieve with the blockchain decentralization. You want it to be scalable and you try to achieve security, but the blockchain trilemma describes that it's only possible to achieve two of those three goals, though if you try to have your system scalable for the future and secure, then, it's almost impossible to have a decentralized and would be centralized, and that inherits other risks. And if you want it to be decentralized and secure, then for example, the verification process of users would be too slow and could slow down the whole system." - Cyber Security Expert

Product management plays an important role in successful implementation of prototypes, to navigate the journey from conception to innovation by orchestrating insights and dynamics between different actors.

"What product manager does is connect people and teams together and also with the with the markets, with senior level managers. So basically, what I do as a product manager is that I work with almost every team in the company from customer success to support the developer's design. Then I connect to customers, then I connect to senior managers, and I try to bring everything together so that we can understand what the problems in the market are, what are the problems for the users, how we can solve it?" - Product Manager 1

"I go into a company, and I see that there is always this pressure from salespeople, from customer success, that they want to build things for one individual customer and as a product manager, it's my job to say that, No, this cannot… We cannot do it, because we are focusing on this other thing now which has more strategic value. So, I also try to dig deep that for example, I ask questions that OK, how is the customer doing right now? Is there any other way that they can solve this problem? Is there a possibility that they may turn with us if we don't solve this? And all these things to really understand what the importance is of that one for example feature that the customer is requesting because what happens in." - Product Manager 1

But does the need-solution pairing approach work in reality for technological implementation processes? Product Manager 1 stated that in the digital asset development practice is known with another name: *Dual Agile Development*. Project manager 1 highlights the concept of "dual agile", this could be further explained as having two sides. One side where you have the problem, and on the other side where you have the solution. Then, through iteration, dual agile revolves around the relationships between identifying a problem and finding a solution.

"And this thing that you mentioned about like this parallel thing, problem, and solution, that's exactly how I work. So, it's like we call it this dual agile. So, we have base, and we have solution space and that's exactly what we do like……so when you redefine this problem then you know that OK now you start to go into the solution space and then you start to do the prototype you start to iterate and iterate and iterate show it to the users." - Product Manager 1

When questioning Product Manager 1 about the division line between human and technology, we found ourselves with a rhetorical answer.

"I would say that product manager to a very high level, it comes about like sort of peoples." - Product Manager 1

During the interviews we came to realization that obligations do not purely lie on the adopters´ side, rather the solution providers need to play an active role from the behavioral aspect i.e., managing expectations. Product Manager 2 also highlighted how managing expectations, especially regarding the time of iterations on developing a solution takes, and how to explain it to the possible adopters.

"And at some point, the product was the MVP was maturing more and more. So, I would say sometime after one year after the initial start, we had the official launch. And then we were basically managed, we managed to have some of our clients now the right value. It was still not paid, but we wanted to develop it a bit further before judging it. We also wanted to build their interest a bit more. And then yeah, we continue with that. Meanwhile, the largest opportunity from the public sector that was introduced to us by the investors. Started an RFP and research for proposals for this type of system and that kind of means that we are forking holistic."

- Product Manager 2

While creating consciousness and managing adopters' expectations, solution providers require to think further than the design of a specific solution for a given customer i.e., how the development can benefit other adopters? Product Manager 2, in accordance with Product Manager 1, thereafter emphasizes that in order to achieve flexibility and scalability, you must take your own solutions and make them broader in order to appeal to a wider spectrum of potential adopters.

"We have like the standard product that we're still trying to put in the market at the same time we're building something a bit more custom on top of it for this particular client or the client. The RFP, however, went on for quite a bit of time. Then the pandemic came and then they basically pulled the RFB. They didn't want to buy anything they were too afraid to. I had gotten some traction in the private sector. We were testing this product with more and more users… They were giving us feedback now. I was in discussions with a few organizations and each of them had their own ideas. It was very important that I actually would gather all of these ideas and try to find the common patterns and develop those and not promise to these companies that I would develop everything that they would ask for. We'll say, look, let's see, depending on the direction that we want to take on this product, we want to make this concept strong, that we're in discussions with a few other organizations. We want to make sure that this actually can be used by the other organizations we're going to build a custom product for you, and thankfully they were understanding some of them." - Product Manager 2

The final question for us was, in fact, if there is a matching pair in the need- solution landscapes that can satisfy the control requirements expressed by the adopter while enjoying the potential listed benefits of Blockchain for E-voting. In this sense, the Professor of Communications Systems opened a new window when questioned about this: One could use a semi-centralized server service system for that.

"And then it's kind of semi-centralized. And the relationship now is that you have the public transparency of the process, but you have the government control of the service and perhaps if it's outsourced and it is on a public cloud. They may think that's not enough, but in UK for example, we have government cloud service, so they could use that." - Professor of Communications Systems

While we were not lucky on finding matching literature on how Semi-centralized server systems work, the Professor of Communications Systems provided an extensive technical explanation that we considered to be interest as a matter of future research, beyond the scope of this master thesis.

"You can run a blockchain on a semi centralized service. So, for example, there are several blockchain services or Ledger services on cloud platforms which are inherently centralized. If you look at Azure or AWS, you know the Microsoft Azure on Google Cloud or Amazon's AWS, there are Hyperledger and Ethereum services which run on those and so an electoral body could just use that as a blockchain. It still has the tamper evidence so they can show the public that the votes have not been altered by an agency including themselves. But it is centrally managed, so if you want that's kind of my simple answer that that would be you know it would, it would be completely reasonable for example in multiple countries. Now, perhaps not in the country we were working with in Pakistan, but certainly most of Europe governments have cloud services as part of government services and so running a blockchain on a cloud service is perfectly feasible. And then it's kind of semi centralized. And the relationship now is that you have the public transparency of the process, but you have the government control of the service and perhaps if it's outsourced and it is on a public cloud. They may think that's not enough, but in UK for example, we have government cloud service, so they could use that." - Professor of Communications Systems

6 Discussion

6.1 Technical Challenges: Security and Control

Control & Compliance:

The County Council Project Developer emphasized the need of control, secure procedures, and to comply to regulations as well as stated the government´s concerns on relying on external servers. In the same line, the need for securing processes guaranteed by internal control from Authorities is a necessary condition to meet Swedish jurisdictional regulations. Parallelly, the Professor of Communications Systems also raised concerns about how trust issues in governmental and service functions the implementation of Blockchain might not necessarily solve. If the perception that the government can still manipulate results would remain in a specific country, the implementing authorities would be in the need of showing a high level of compliance and transparency with legal regulations and data protection standards like the GDPR in order for the technology to gain legitimacy, by the means of aligning with established safeguarding regulations of data privacy. The former aligns with legitimacy-as-perception from the public (macro level) and represents the main element of validity electoral authorities should aim for.

Verifiability:

The Blockchain Lab & IoT Expert discussed the concept of End-to-End verification and highlighted the importance of allowing citizens to have proof of their votes in the end results. Zero-knowledge proof was suggested as an approach to ensure anonymity while verifying the vote. However, Blockchain offers additional security features. The Blockchain Expert added that cryptographic methods such as Proof-of-Person (PoP) enhance security by ensuring ID verifiability while preserving anonymity.

The discussion about the importance of End-to-End verification and the role of Zero-knowledge proofs can be linked to legitimacy-as-property. Verifiability mechanisms add up to the transparency and accountability needed for a legitimate election process.

Transparency & Immutability:

The Blockchain Expert highlighted how the immutability of data stored and recorded on a Blockchain reinforces its security against hacking attempts. The interviewee mentioned as well that Blockchain is both transparent and immutable, ensuring that once a vote is recorded on the Blockchain and the polls officially close, it cannot be changed. Furthermore, the Operational Architect explained how the encryption process used in electronic voting schemes would ensure that votes and personal information would be securely enclosed in encrypted envelopes.

When highlighting the immutability of Blockchain and its contribution to security, this finds a link to legitimacy-as-property in our opinion. Since immutability ensures that the integrity of election data is protected, it complies with the critical requirement on maintaining legitimacy and trustworthiness throughout the entire electoral process. Demonstrating such benefits would be the first step by election organizing authorities on the "socio-cognitive perception or evaluation" to achieve legitimacy-as-perception from voters and election participants.

The idea of using Blockchain to combat major concerns such as voter fraud and coercion is also mentioned by the Professor of Communications Systems. The combination of E-voting and Blockchain, however, requires trust in both the technology and the government. Blockchain transparency and immutability could enhance trust if applied where the government provides verifiable ID services, but the technology alone will not help if there is an inherent distrust in government. However, in order to enjoy the benefits of a E-voting and Blockchain integration i.e enhance security while diminishing human errors as stated by the Blockchain Expert, it has to be combined with a reliable identity verification system that Sweden still lacks off. As stated by the County Council Project Developer, the commonly Bank ID legitimation system belongs to the private Banks; making it an unviable candidate for electoral purposes since it can have a direct repercussion not on individuals' private data but in the conformation of the local and national governments.

A recurrent feature mentioned as an inherent characteristic of Blockchain is its decentralized character, while the topic has come commonly across not only in the literature but also in most of the interviews conducted, its full digestion as concept requires time and has a low degree of ease-of-use. As explained in section 2, the decentralized nature of Blockchain contrast with the typical centralized nature of electoral processes where the element of control represents a non-negotiable priority in the case of the Swedish authorities, and most probably for other jurisdictions. However, here it is important to remember and clearly differentiate and clarify how

the different actors look at both centralization and decentralization. As mentioned in Valmyndigheten webpage (Valmyndigheten, 2023) “decentralization” is mentioned as one of the characteristics for the elections in Sweden. However, that conceptualization refers purely to the fact that votes are counted in their respective locations and then results are reported to a central authority. In that case, the counting and reporting procedures make the elections a centralized process controlled by a central authority. In the nature of a public/permissionless Blockchain (Amelin et al, 2019) there is no central authority in charge of the process, rather the information is visible and shared. The insertion of Blockchain would remove, in principle, not only central authority but also the element of control.

“When you talk about centralization and decentralization, you can talk about different degrees and levels, right? I mean. I don't see the benefit of if you can have a network that provides infrastructure to do elections on it, but no one can control it in the sense that they can go in and just change things by themselves.” - Blockchain Expert

Security:

The County Council Project Developer stressed the concerns about security and compliance, particularly related to secure procedures and compliance to GDPR. The Blockchain Expert highlighted the security benefits of Blockchains de-centralized nature and immutability in preventing hacking. The Cyber Security Expert explained in likeness about the role of cryptography and encryption to ensure security. Different cryptographic methods were discussed and the distinction between cyber security and information security was highlighted and that two types of cyber-attacks could be identified: attacks targeting the system itself and attacks that are targeting the users. A secure system (legitimacy-as-property) is a foundational requirement for establishing the legitimacy of the technology in the context of electoral processes (legitimacy-as-property). Ensuring the security of data and processes is essential to maintain the credibility and integrity of elections (legitimacy-as-process), hence the need for control as stated by the County Council Project Developer.

6.2 Organizational Dynamics: Navigating Change

Need & Motivation:

The County Council Project Developer highlighted the "need" to address digitalization in various fields sooner or later, including electoral processes and that digitalization is seen as motivation to step forward. On the other hand, the Operational Architect presented different motivations among potential adopters explaining that, some might see digitalization as unnecessary in some cases, where no palpable benefit in the process in question is perceived.

The combination of technology, public perception, and regulatory frameworks shapes the conversations surrounding innovations like Blockchain, especially when addressing misconceptions around it. Skepticism often arises from misunderstanding, exemplified by the recurrent confusion between Blockchain and Bitcoin, where in reality one (Bitcoin) is a byproduct from the other (Blockchain), as stated by both the Blockchain Expert and the County Council Project Developer. However, it is important to explain these misconceptions to enable informed discussions.

During the interviews, the Trust factor was mentioned continuously as a crucial element on driving a governmental initiative. Sweden has high levels of Trust in the public institutions as shown in the trust index (Organization for Economic Co-operation and Development [OECD], 2023) that places Sweden as in position nr. 4. This set the question of where the need is to add such a feature like Blockchain to its electoral processes.

For the sake of understanding, the appropriate comparison to clarify the expressed need towards having Blockchain in electoral processes in Sweden is the one concerning with the only public area where the country has successfully implemented Blockchain: Property rights (Sanka et al., 2021). The initial motivation for the Swedish authorities was more related to appropriate property classification and fair tax collection rather than combating issues of Trust. While Blockchain and in general Distributed Ledger technologies were designed to restore trust in public systems (Natarén & Herran, 2019), the evidence collected during the results of this thesis does not point out to an existing need on the electoral side.

Natarén & Herran (2019) provided decision criteria a government can follow when deciding whether to implement Blockchain or not, and more importantly in which areas. They studied the case of an emergent country like Mexico, but the lessons general enough to extrapolate them to another country`s case. These include the review of the legal and technical landscapes of the country, as well as considering the main contextual barriers for the implementation *"This consideration arises from the Mexican context and should not be considered from the point of view of the used authors evaluations. So, the best two applications of DLTs in Mexican Government to combat corruption seem to be the Strengthening of the Public Property Registry and the Tracking of Public Funds……. The most obvious barrier for a successful implementation of DLTs in Public Funds Tracking in Mexico is the political legacy system."* (Natarén & Herran, 2019)

Finally, Natarén & Herran (2019) mentioned that the digital infrastructure level of the country can facilitate or slow down the implementation of a government initiative. Digitalization rankings of the countries can be found on the *Digital Evolution Index (DEI)* (Retrieved August 14, 2023, http://www.thenextsiliconvalley.com/2017/07/21/4784-digital-evolution-index-maps-competitiveness-of-60-countries/#.ZHCb2XZBy5c) with a corresponding score. Sweden was classified as number 2 in the world after Norway, setting a good precedent.

When considering the high levels of trust the Swedish citizens have towards their public institutions, the debate about the need of Blockchain from Swedish Electoral Authorities to legitimize themselves appears in first sight at least questionable. The degree of trust (legitimacy-as-perception) in governmental institutions can, paradoxically, influence the perceived legitimacy of technological implementations (legitimacy-as-property) like Blockchain in elections.

During the introduction of this thesis, the term Agile Software Development was brought to the table after the introduction of the respective constructs of Legitimacy and Need-Solution Pairing. But how does this practice relate exactly to literature? The interviewee Product Manager 1 brough the concept of Dual-track Agile as a synonym -in the development of Digital Assets- to the practices of what Von Hippel & Von Krogh (2016) called *Agile Software Development* in their Need-Solution pairing paper. Trieflinger et al. (2021) wrote an interesting paper about the topic of *Dual Agile Development* where they intended to *"Gain a better understanding of how product discovery and product delivery can interact with each other and how this interaction can be implemented in practice, this paper aims to identify suitable approaches to dual-track agile"* (Trieflinger et al., 2021).

Dual-track agile is a type of agile development which combines product discovery (i.e., the ability of the adopter to validate products, services or features before implementation) and product delivery (i.e., the technical implementation and deployment of the identified outputs of product discovery) in parallel (Trieflinger et al., 2021). One of the approaches Trieflinger et al. (2021) presents a paper called "Essential Approaches to Dual-Track Agile: Results from a Grey Literature Review" relates specifically with the conception and creation of *Product Roadmaps* for the means of Digital Assets Development. The reader that has made it until this point of the thesis might relate the former with the concept of Minimal Viable Product (MVP), and with reason.

Communication:

The Professor of Communications Systems discussed how the transitioning process of introducing a new technology like e-voting would look like. He compared it to the adoption of online banking and emphasizes that the acceptance (Legitimacy-as-process) and adoption would take time. A hybrid system could be necessary to accommodate different levels of comfort with the new technology.

Control & Transparency:

Within the solutions landscape, failures of Blockchain products such as cryptocurrencies have promoted resistance and resistance towards the actual Blockchain technology itself would be built upon weak reasoning. The Blockchain Expert emphasized that failures in the crypto space do not equal Blockchain technologies potential, rather highlighted the need for having a more transparent election. This disconnect, between negative perceptions and broader capabilities of Blockchain, is also expressed by the County Council Project Developer, but in similar fashion as the Blockchain expert highlights that Blockchain would be the most secure way to digitalize an election promising transparency and control.

The Blockchain Expert acknowledged regulatory and ethical challenges in implementing Blockchain for electoral processes, but also brought up that the potential benefits would overcome them, making explorations worth it. The Blockchain Expert also brought up the potential benefits of real-time data visibility during an election through a Blockchain-based system. However, the Operational Architect pointed out potential negative effects of reporting live results could include anxiety and misinformation. This balance between security and transparency was a recurrent topic during the interviews when questioning the interviewees about election results reporting and visibility.

The concept of decentralization is central to Blockchain technology. This term is often understood differently depending on the context. For instance, in electoral processes, decentralization means distributing vote counting across different locations (poll stations), whilst in a public Blockchain, it means the absence of central authority. The County Council Project Developer highlighted the importance of balancing control, with the benefits of decentralization. Coincidentally, the notion of a semi-centralized Blockchain, as explained by the Professor of Communications Systems, could be run on government-controlled cloud platforms, and thereby, could be presented as a viable compromise, allowing for transparency whilst retaining control i.e., what can be considered as a sign of pragmatic-legitimacy (legitimacy-as-property) from the proposed solution. This insight also suggests that a semi-centralized Blockchain system could align with governance priorities stated by the County Counsil Project Developer, if properly executed.

6.3 Legal Horizons: Exploring Regulatory Frameworks and Data Privacy

Assumptions:

During the discussions a couple assumptions made by the Swedish Electoral authorities in their initial due diligence about implementing Blockchain, from the legal and political perspectives, popped up. The discussion around the adoption of Blockchain technology in elections could be found between technological processes, legal frameworks, and practical considerations. The unwillingness towards embracing new technologies like Blockchain didn’t have to be based on resistance but instead could be reflected on protecting established legal principles and societal values which identifies the assumption that digitizing a paper-based process would not only be technically challenging but also legally complex, as stated by the Legal Expert. Control, transparency, and cost-effectiveness were the driving forces behind Sweden's investigation of Blockchain for elections, according to the County Council Project Developer. However, these plans were halted by unforeseen legal obstacles such as storage, highlighting how difficult it would be to switch from the secure paper-based systems that Swedish elections has today, to a digitalized one.

Trying to preserve the fundamental characteristics of democracy, which are built on secrecy and freedom, has made Blockchain adoption a difficult challenge. The adoption of Blockchain could hold potential benefits, but how it can develop would depend on how these technologies align with existing legal and ethical norms, ensuring the fundamental principles of democratic processes remain intact. Therefore, one of the main challenges that was identified was the assumption that digitizing a paper-based process would not only be technically challenging but also imply fulfilling a series of legally complex and time-consuming requirements. Considering existing legal principles and societal values, when adopting new technologies such as Blockchain, should look for not only that a process remains legitimate according to established norms but to increase its degree of validity.

Roadblocks:

The County Council Project Developer, responsible for the BLING project, emphasized the control need of the organization considering Blockchain for elections. However, combining technical implementation with to the European GDPR and other regulations was an unforeseen issue. Digital implementation initiatives legislation is a complex process involving multiple processes, including the ones concerning the own elections organizational issues as well as public agreement, b according to both the Legal Expert and Operational Architect. This complexity highlighted one of the multiple implementationroad-blocks new technologies, such as Blockchain, can face. Furthermore, Sweden has another unique trait that adds to the complexity. The nation's high levels of trust in its public institutions, at the top of the global trust index (Organization for Economic Co-operation and Development [OECD], 2023), could question the need of introducing Blockchain into its electoral processes. The Professor of Communication Systems stood in alignment with such question based on the case of UK, where just one fraudulent vote -out of millions of votes- have been occasionally detected, disregarding the Blockchain adoption as necessary, and that the existing operational cost for traditional voting is reasonable. On the other hand, the Legal Expert, both Electoral Officials, as well as the Blockchain Lab and IoT Expert replicated that this reality is also present in the Swedish case. But there are also technical challenges as roadblocks revolving around ensuring security and compliance, and the County Council Project Developer highlighted the need for such secure procedures.

Technical challenges:

Blockchain as solution is aimed to guarantee data security, complying with privacy standards while maintaining voters' identity as well as ensuring their anonymity. The combination represents challenge from the technical perspective. Therefore, the Legal Expert raised the question on how to verify citizens' identities without compromising the secrecy of their votes. While not explicitly mentioned in the legal section, the Blockchain trilemma, discussed by the Cyber Security Expert introduced possibility of achieving decentralization, scalability, and security in Blockchain solutions; though and as explained by the expert only 2 out of 3 of these features can be achieved at the same time.

The technical challenges associated with the Blockchain trilemma can be connected to pragmatic legitimacy (technical superiority) as well as to legitimacy-as-process for future research purposes. Selecting a plausible technical balance should add up on achieving the credibility and trustworthiness aimed by the implementation of the technology.

6.4 Prototyping and MVP: Iterative Development

6.4.1 For Adopters

Problematic:

Both Product Managers provided valuable insights into the roles of product managers in different contexts. They highlighted the importance of understanding users, collaborating with diverse teams, and ensuring that products remained relevant and effective in their evolving part of the landscape. Product Manager 1 discussed the importance of that adopters must clearly understanding their requirements and problems before engaging with solution providers. Product Manager 1 also emphasized the need for adopters to engage in discussions about their problems and challenges with the solution providers to bridge the gap between different teams. Product Manager 1 also brought up techniques like the "5 Whys" to deepen into the understanding of what adopters needs and what their challenges are.

This made us connect the dots that Blockchain must go through a development process like any other Digital Asset. Therefore, are there main considerations a possible adopter (in this case an electoral authority) should make before even considering the implementation of a new technique or technology such as blockchain? Is there as similar process in the practice of Agile Software Development to the need-solution pairing approach? Those 2 questions constitute the pillars of the other half in the results part of this thesis, and like in the legitimacy lens, the answer to both is: Yes.

Needs:

Both Product Managers emphasized the significance of understanding user needs and behaviors (need-solution pairing). By focusing on users and conducting iterative feedback loops, election authorities could ensure that the Blockchain solutions aligns with their own requirements, the voters, and other stakeholders. This approach enhances the transparency of elections and addresses potential concerns that related to voter privacy, trust, and user experience. Product Manager 1 emphasized the importance of adopters being clear on their requirements and needs to allow solution providers to be more flexible to create effective solutions.

Regarding Solution Providers:

The Product Manager 1 explained the role of a product manager in connecting different teams including developers, customers, and senior managers. Product Manager 1 also highlighted the importance of active communication from adopters to drive successful solutions. Product Manager 2 also brought up the challenge of managing adopters' expectations, especially regarding development timelines.

The Product Manager 2's experience of adapting solutions to individual client needs i.e., recognize common patterns and developing those, and ensuring that it could be utilized in other organizations whilst still being able to design a custom product, could be relevant to electoral processes. It could be important in the sense that different regions and countries have different electoral systems and requirements. Applying a similar approach, election authorities could customize Blockchain solutions to suit their specific needs whilst maintaining a standardized core that ensures consistency and security. This balance between customization and scalability would be important for diverse electoral cases.

6.4.2 For Solution Providers

Expectations:

The Product Manager 2 emphasized the importance of managing adopters' expectations, especially in terms of development timelines and iterations. Product Manager 2 also stressed the important of individual client needs i.e., recognize common patterns and developing those, and ensuring that it could be utilized in other organizations whilst still being able to design a custom product, could be relevant to electoral processes. It could be important in the sense that different regions and countries have different electoral systems and requirements. Applying a similar approach, election authorities could customize Blockchain solutions to suit their specific needs whilst maintaining a standardized core that ensures consistency and security. This balance between customization and scalability would be important for diverse electoral cases.

Scalability:

The Product Manager 2 emphasized the importance of making solutions broader and scalable to appeal to a wider range of potential adopters whilst the Cyber Security Expert introduced the concept of the "Blockchain Trilemma," discussing the challenges of achieving decentralization, scalability, and security simultaneously in Blockchain solutions. The Professor of Communications Systems finally suggested the possibility of using a semi-centralized server services for Blockchain implementations for allowing a balance between public transparency and government control.

Both Product Managers stressed the importance of prototypes and MVPs. In the context of elections, these concepts can be used to legitimize Blockchain implementations on a smaller scale before full-scale adoption. Developing prototypes could allow election authorities to showcase the potential benefits of Blockchain technology to stakeholders, and the MVPs enable iterative testing and refinement based on user feedback. This approach could therefore mitigate risks and allow for safer and gradual implementation. Election authorities could thereby exploit the benefits of Blockchain whilst still preserving the integrity, security, and transparency of voting systems by focusing on user demands, collaboration, customization, and iterative testing.

7 Conclusion

The objective of this thesis was to study the plausible application of Blockchain for public electoral processes in Sweden under the framework of the European Blockchain in Government (BLING) project.

First, this thesis established the requirements and combination of factors to be met by a technology, such as Blockchain, to fulfill the need of Legitimacy for a public interest process such as an election (Need space): Control and Immutability for the Central Authority, as well as Transparency, Visibility, as well as Secrecy of voting for the voters and other process participants. This provides, according to the authors of this thesis, an answer to research question 1, however just partially.

In the conceptual framework section of this work, 3 different dimensions of legitimacy were defined: 1) Legitimacy as property 2) legitimacy as process and 3) legitimacy as perception.

As a first layer of legitimacy as property Suddaby et al. (2017) mentions the so-called pragmatic legitimacy i.e., the assessment if the proposed implementation (solution) is in fact technically superior to the current system. Therefore, the first consideration applying the legitimacy lens before going into a new implementation appears to be straightforward: Is it needed? Is there a real reason for it?

"The system we use in Sweden today, with paper voting, is very secure, and it has to stay secure, even with the new technique." - County Council Project Developer

While Blockchain technology could add new dimensions respecting legitimacy as process and perception, there doesn't seem to be currently a need for its application in the Swedish context. If Blockchain can in fact offer pragmatic legitimacy (legitimacy-as-property) that is also a matter of the future research, we are proposing in this work.

Second, this thesis selected the need-solution pairing approach proposed by Von Hippel & Von Krogg (2016) in order to explore among the plausible sets of solutions (Solution space) that could contribute to the implementation of Blockchain for electoral processes in Sweden.

Third, this study claims to have found a matching pair, and therefore have successfully answered research question 2. The proposed answer takes the form of the *use of semi-centralized server systems in order to implement Blockchain for electoral processes* that we propose to be subject of further study by engineering or computer science faculty students or researchers. This would help the County Board of Skåne to fulfill their control requirements over the electoral process (Matching pair).

Implementing a semi-centralized Blockchain would enhance the legitimacy of property as the cloud services would be state-owned, the process of legitimacy would be part of their influence, and the perception of trustworthiness towards authorities by the public is already high in Sweden, making this proposal, in essence, legitimacy within all three dimensions.

However, it is worth noting that in the context of finding a viable pair, we did not conduct any exploration on the potential fulfillment of need at equal or lower cost. This lack of analysis, however, opens the opportunity for future research within this field.

Finally, a series of managerial implications and considerations were proposed for possible adopters, interested in studying the implementation of Blockchain to an electoral process. With this we went two steps back in the literature of existing ad-hoc solutions for Blockchain with E-voting purposes.

While most of the decision makers on the adopter's side (companies, institutions, public sector) would typically rely on their IT or technical departments to advise them of implementation considerations towards a new technology in their search of optimizing their processes and boost their results, in this case Blockchain. We would strongly encourage them to achieve a minimal required understanding of the input requirements, the solution providers need to better address the needs and eventually wants from adopters. This point will appear again in the discussion section as well as be part of the final list of recommendations.

Therefore, our claim is that in order to match the dynamics of any given electoral process with the basic characteristics of the Blockchain technology, it is necessary to go two-steps back in the literature in order to generate a more generalized set of guidelines that contains the minimal characteristics a Blockchain application must include in order to be implemented on any given electoral process. That constitutes the result of this thesis. The aim is that any implementation attempt or eventually success case would not only benefit one but multiple possible adopters.

Proposal: Two-steps back

As brought to the table by the Practitioners during Section 5.4, an MVP is the base for experimentation for early adopters regarding their desired features in the intended implemented system. The MVP englobes the basic needs while allowing the implementation of the wants, but before creating an MVP a series of managerial implications need to be considered. As a result, the final proposition of this thesis consists of a series of recommendations- for the "adopter"- to be consider before pursuing the implementation of a digitalized process, such as Blockchain, into a traditional one, such as the Swedish elections.

Table 3
Our Proposal: Prior Considerations for Blockchain implementation (E-voting): Answer to practical

Managerial Implications prior the Adoption of Blockchain for Electoral Purposes (Inspired by Avital, 2007)	**General system feature**	**Description**
Technical	Control & Compliance Security	Identify the jurisdictional location of needed technological resources and the compatibility with your local GDPR regulations
	Verifiability	Identify the different technological verification mechanisms currently present in the market (i.e., Zero-Knowledge proof, etc.)
	Transparency	Ask your solution provided about transparency features of the technology of your interest (in this case DLT and Blockchain)

	Immutability	Ask your solution provided about the immutability features of the technology of your interest (in this case DLT and Blockchain)
	Security	Investigate the different technological security mechanism currently present in the market (i.e., Encryption, Cryptography, etc.)
Organizational	Need & Motivation	Define your business and organization REAL need as accurate as possible and differentiate it from other motivations
	Communication	Differentiate between needs and wants, try to pre-evaluate the feasibility of your wishes.
	Control	Understand & promote technical understanding within your organization. Increase levels of information about the topics in question within your organization Educate people about the use, possibilities, and limitations of technological resources.
	Transparency	Promote transparency of information and fight biases
Legal & Political	Assumptions	Avoid making assumptions, rather find out the

		how the legal and political landscapes look like regarding you're your digitalization initiative.
	Roadblocks	Pre-identify possible roadblocks and state the question "What have we not considered?"
	Technical-Challenges	Anticipate that you will face technical challenges no matter the endowment of resources you have.
Proposal	*For Adopters:* 1. Problematic	Define and explain clearly the problematic properly so that they are explainable to third parties and solution providers.
	2. Needs	Define and understand your own needs properly so that they are explainable to third parties and solution providers.
	3. Regarding Solution Providers	Understand Solution providers´ perspective & provide requested input.
	For Solution Providers: 1. Expectations	Manage Expectations of your Adopter
	2. Scalability	Design for Scalability, not for individual client purposes

7.1.1 Limitations

One limitation restricting our study was the time limitation. Finding suitable participants for interview took longer than expected since the research area on applying a plausible Blockchain in electoral systems is limited, it made the scope of finding relevant participants for interviews narrow.

Another major aspect worth mentioning is that other candidates for lens, such as cybersecurity, could have been chosen. However, it was discarded due to its high technical level, not matching both the interest and background of the group of researchers responsible for this study, nor from the interested partners from the BLING project. Nevertheless, cyber security could be an excellent candidate for other research efforts to go deep into as well as complementary to this work**.** Furthermore, the so-called *Blockchain Trilemma* (where achieving Decentralization, scalability and security is not achievable at the same time, but only combining 2 out of these 3 elements) that we became aware of by interviewing the Cybersecurity Expert could be a good candidate as an approach for such proposed research.

7.1.2 Future Research

As stated in the conclusion, while Blockchain technology could add new dimensions respecting legitimacy as process and perception, there doesn't seem to be currently a need for its application in the Swedish context. If Blockchain can in fact offer pragmatic legitimacy (legitimacy-as-property) that is a matter of the future research we are proposing in this work.

As stated in Section 4, legitimacy as process analyses the term related to movement, activity, and temporal evolution (Suddaby et al., 2017). Studies about legitimacy as process are intended to produce stage models able to demonstrate how organizations, their practices and outcomes move from one state to another. For Electoral Authorities and Bodies this can be a matter of interesting future research, evaluating the impact of the insertion of an innovative technology such as Blockchain.

An important clarification is that, since most of our results point out in the direction of legitimacy as property rather than as a process, it is important to mention a distinction that Suddaby et al. (2017) made between them. In legitimacy as process focused studies, authors tend to use the term "legitimation" or "legitimizing" rather than "legitimacy." This is the reason we sticked to the term legitimacy across the text of this master thesis. As Suddaby et al. (2017) state in their article, process-oriented research on legitimacy states the three key processes by which legitimation occur: (1) persuasion/translation/narration, (2) theorization, and (3) identification/categorization. Future research could include pilot projects of insertion of Blockchain which include creating a citizen dialogue, storytelling from authorities about other successful experiences with the tool as well as defining the appropriate categories (areas or fields) as subject of implementation.

In Section 4 we stated how the study of legitimacy-as-perception concerning Voters, Political Parties and Candidates as well as Electoral Observers as matter of future research. Typically, researchers going into legitimacy-as-perception should focus on two main constructs: 1) Judgment formation from individuals and 2) the relationship of the aggregation of such judgements forming a "macrolevel legitimacy opinion" i.e. achieving validity from the public as stated by Suddaby et al.(2017) Particularly, that second aspect represents the micro-to-macro translation within social theory as Suddaby et al.(2017) referred to be still underexplored, at least until the time of publication of their famous Legitimacy paper. Furthermore, the authors stated that there is a skewness to the analysis of legitimacy and institutional change in the form of legitimacy-as-process in the literature. The study of implementation of Blockchain in a process of public scrutiny, such as elections, represents an excellent motive to go deeper into the study of legitimacy-as-perception at the macro level. Such an effort would imply the use of vast -both material and time- resources not available to the authors of this master thesis.

Finally, as stated in Section 5, while we were not lucky on finding matching literature on how Semi-centralized systems work, the Professor of Communications Systems provided an extensive technical explanation that we considered to be interesting as a matter of future research, beyond the scope of this master thesis.

8 References

Abuidris, Y., Kumar, R., Yang, T., & Onginjo, J. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *Etri Journal*, *43*(2), 357-370. https://doi.org/10.4218/etrij.2019-0362

Adams, N. (2022). The Concept of Legitimacy. *Canadian Journal of Philosophy*, *52*(4), 381-395.

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet voting in comparative perspective: the case of Estonia. *PS: Political Science & Politics*, *42*(3), 497-505.

Amelin, R., Channov, S., Lipchanskaya, M., Tsybulevskaya, O., & Zametina, T. (2019). Blockchain technologies for electronic voting: Legal aspects. *Journal of Advanced Research in Law and Economics*, *10*(5), 1382-1389. https://doi:10.14505/jarle.v10.5(43).04

Anitha, V., Marquez Caro, O., Sudharsan, R., Yoganandan, S., & Vimal, M. (2023). Transparent voting system using blockchain. *Measurement. Sensors*, *25*, Article 100620. https://doi:10.1016/j.measen.2022.100620

Avital, M. (2007). Innovation through generative systems design. In *Cleveland, OH, USA, NSF Science of Design Workshop–technical report*.

Bhadoria, R., Das, A., Bashar, A., & Zikria, M. (2022). Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections. *Electronics (Basel)*, *11*(20), 3359. https://doi:10.3390/electronics11203359

Bryman, A. (2011). *Samhällsvetenskapliga metoder* [Social science methods] (3rd ed.). Liber: Stockholm.

Chohan, U. W. (2022). A history of bitcoin. Available at SSRN 3047875.

Cserny, Á., & Nemeslaki, A. (2018). The challenges of e-voting. *Public policy and administration*, *17*(4), 497-509. https://doi:10.13165/VPA-18-17-4-01

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*, 147-160.

Gebhardt Stenerud, I. S., & Bull, C. (2012). *When reality comes knocking norwegian experiences with verifiable electronic voting*. Gesellschaft für Informatik eV.

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The Discovery of Grounded theory; strategies for qualitative research. *Nursing research*, *17*(4), 364.

Government Trust Index OECD 2021 https://data.oecd.org/gga/trust-in-government.htm

Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR), 54(3), 1-28.*

Jost, J., & Major, B. (2001). *The psychology of legitimacy: Emerging perspectives on ideology, justice, and intergroup relations*. Cambridge: Cambridge University Press.

Langwagen Elfström, A. (2018). *Blockchain organizations - Decentralized autonomous organizations and the law.* [Master's thesis, University of Gothenburg]. Gothenburg University Publications Electronic Archive. http://hdl.handle.net/2077/57602

Larsen, K. A. (2018). Metod helt enkelt – En introduktion till samhällsvetenskaplig metod [Method simply – An introduction to social science method] (2 uppl.). Gleerups: Malmö

Lindman, J., Berryhill, J., Welby, B., & Barbieri, M. (2020). The uncertain promise of blockchain for government. *OECD Working Papers on Public Governance*, (43), 0_1-63. https://doi:10.1787/d031cd67-en

Merton, R. K. & Barber, E. (2004) The travels and adventures of serendipity: A study in sociological semantics and the sociology of science. Princeton University Press.

Moogk, D. R. (2012). Minimum viable product and the importance of experimentation in technology startups. *Technology Innovation Management Review*, *2*(3).

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

Natarén, C., & Herran, A. (2019). Restoring Trust in Mexican Government. Preliminary Assessment of DLT Implementation. *ACM International Conference Proceeding Series*, *148153*, 24-29. https://doi:10.1145/3320154.3320158

Organization for Economic Co-operation and Development (2023, August). *Government Trust Index OECD*. https://data.oecd.org/gga/trust-in-government.htm

Park, S., Specter, M., Narula, N., & Rivest, R. (2021). Going from bad to worse: From Internet voting to blockchain voting. *Journal of Cybersecurity*, *7*(1). https://doi:10.1093/cybsec/tyaa025

Piazza, F. S. (2017). Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses. *Bocconi Legal Papers*, *9*, 125-156. https://heinonline.org/HOL/Page?handle=hein.journals/bocclp9&div=11&g_sent=1&casa_token=&collection=journals

Popovski, L., Soussou, G., & Webb, P. B. (2018). A brief history of blockchain. *Online access: February*, *1*, 2019.

Sanka, A., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications*, *169*, 179-201. https://doi:10.1016/j.comcom.2020.12.028

Schon, D. A. (1983). *The Reflective Practitioner: How professionals think in action*. New York: Basic Books.

Shahzad, B., & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access, 7*, 24477-24488. https://doi:10.1109/ACCESS.2019.2895670

Stebbins, R. A. (2001). *Exploratory Research in the Social Sciences* (Vol. 48, Qualitative Research Methods). Los Angeles: SAGE Publications.

Suchman, M. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review, 20*(3), 571-610.

Suddaby, R., Bitektine, A., & Haack, P. (2017). Legitimacy. *Academy of Management Annals, 11*(1), 451-478. https://doi.org/10.5465/annals.2015.0101

Swedberg, R. (2020). Exploratory research. *The production of knowledge: Enhancing progress in social science*, 17-41.

Trieflinger, S., Münch, J., Heisler, B., & Lang, D. (2021). Essential approaches to dual-track agile: results from a grey literature review. In *Software Business: 11th International Conference, ICSOB 2020, Proceedings 11. Karlskrona, Sweden. November 16–18, 2020*. (55-69). Springer International Publishing. https://doi.org/10.1007/978-3-030-67292-8_5

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annu. Rev. Psychol., 57*, 375-400.

U.S. Vote Foundation. (2015). *The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study.* https://www.usvotefoundation.org/E2E-VIV

Valmyndigheten (2023, March 18). *Valsystemets grunder* [Basics of the electoral system]. https://www.val.se/val-och-folkomrostningar/det-svenska-valsystemet/valsystemets-grunder.html

Vijayakumar, K., Sriramasivam, T., Vigneshkumar, G., Senthil Kumar, G., Angel, T. S., & Snehalatha, N. (2022). Secure E-voting system using blockchain based on solidity technology. In *AIP Conference Proceedings, 2516. November 30, 2022.* (260005-1–260005-6). AIP Publishing LLC. https://doi:10.1063/5.0109146

Von Hippel, E., & Tyre, M. J. (1995). How learning by doing is done: problem identification in novel process equipment. *Research policy*, *24*(1), 1-12.

Von Hippel, E., & Von Krogh, G. (2016). Identifying Viable "Need–Solution Pairs": Problem Solving Without Problem Formulation. *Organization Science (Providence, R.I.)*, *27*(1), 207-221. https://doi:10.1287/orsc.2015.1023

Walpole, H. (1960) To Mann, Monday 28 January 1754. Lewis WS, ed. The Yale Editions of Horace Walpole's Correspondence, With Sir Horace Mann, IV, Vol. 20 (Yale University Press, New Haven, CT), 407–411.

9 Appendices

9.1 Appendix 1 – Original Interview Questions

First question for everyone

- What is blockchain for you?

Researchers:

- *What are the most basic characteristics a blockchain would need in an electoral voting system?*
- *Could blockchain make electoral processes more transparent and trustworthy?*
- *Are there any potential benefits of implementing blockchain technology for electoral voting system?*
- *Could blockchain increase the accuracy and speed of the vote counting system?*
- *What could be some of the key technical challenges associated with implementing blockchain in electoral voting system?*
- *Are there any potential limitations associated with implementing blockchain in an electoral voting system, that you could think of?*

Practitioners:

- *What are some of the operational challenges associated with implementing blockchain in an electoral voting system?*
- *What kind of infrastructure would you believe is necessary to support a blockchain-based electoral voting system?*
- *Could we ensure that all eligible voters are able to participate in the voting process, regardless of their technological literacy?*

- *How would addressing concerns about the potential cost of implementing blockchain in an electoral voting system?*

- *How would we educate the public about the benefits and limitations of using block-chain technology in electoral voting systems?*

Electoral officials:

- *What potential security risks exist with implementing blockchain in an electoral voting system? How can those security risks be mitigated?*

- *Are there any ethical considerations to acknowledge when implementing blockchain in an electoral voting system?*

- *Are there any potential legal or regulatory barriers to implementing blockchain in an electoral voting system?*

Last question for everyone:

- Is there anything you see that we have overlooked?

9.2 Appendix 2 - History of Blockchain

Most people agree that the first application of modern day Blockchain technology originated with Bitcoin and Satoshi Nakamoto.

In a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System", Nakamoto (2008) proposed a direct online payment from one party to another without the involvement of a third-party intermediary (such as banks). Nakamoto's (2008) article addressed the issue of *double spending* ("spending the same digital token more than once"), which was the main challenge that made digital currency impossible to adopt previously (Popovski et al., 2018). This issue was resolved by *tamper-resistant* links between each transaction and the transactions that came before that. Nakamoto's (Popovski et al., 2018) method was made "tamper-proof" by making all the trans-actional history of any electronic coin available for verification by anyone in the network. Ver-ifying transactions is done by solving complex mathematical problems, this process is referred to as mining.

Following the publication of the paper (Nakamoto, 2008), the first open-source Bitcoin-Client was made available (where the first Bitcoins was eventually created). This Bitcoin-Client created the actual underlayer for Bitcoin transactions. Nakamoto mined the first block of Bitcoins (containing 50 Bitcoins) that would frequently be known as the "*genesis block*" (Chohan, 2022). In other words, a block is a collection of verified transactions and unique digital signature, and blockchain is made up of blocks that are connected to one another chronologically after verification (mining).

The first Bitcoin transaction in history took place when Hal Finney (an American computer scientist) downloaded the Bitcoin client and acquired the first 10 Bitcoins from Nakamoto.

Before stopping the involvement with the Bitcoin movement and vanishing completely, Nakamoto mined roughly 1 million Bitcoins himself. Gavin Andresen (an American software developer) rose to the position of main developer at the Bitcoin Foundation and later would be seen as the 'public face' of Bitcoin (Chohan, 2022).

Few people were aware of Bitcoin when it first joined the market in 2009 at a value of $.06 per coin. In December 2017, when the price of one Bitcoin surpassed $19,000, "Blockchain" technology had become the newest buzzwords and took the world by storm. The word "blockchain" alone seemed to produce value just by being adopted.

Blockchain initially attracted attention due to its capacity to remain anonymous, as is the case with cryptocurrencies like Bitcoin, but its true strength lied in the complete transparency it provided. Blockchain could be applied to every subject that involves transactions and could therefore be implemented in almost every field, making its technological advancement arguably similar to the creation of the Internet (Popovski et al., 2018).

But on the other hand, despite the fact that many people have bought Bitcoin, very few people truly have the knowledge about the actual blockchain technology that powers crypto currencies.

9.3 Appendix 3 - Glossary

- ***End-to-end (E2E) verification***: voters can check if their vote is counted correctly. (Shahzad & Crowcroft, 2019).
- ***Homomorphic Encryption*** – Is an advanced algorithm that makes possible to process all the content of a set of certain encrypted messages without decrypting the messages (U.S. Vote Foundation, 2015).

- ***Immutability***: each vote is recorded and cannot be changed, if a person has to re-vote the previous vote can be invalidated (Shahzad & Crowcroft, 2019).
- ***Legitimacy*** –when considering political matters, the concept of legitimacy relates to the perception of what is appropriate or not, and the need to the public opinion to see this need satisfied. (DiMaggio & Powell, 1983).
- ***Need-Solution Pairing*** – A research approach proposed by Von Hippel & Von Krogh (2016) where problem definition and solution (s) are found parallelly (Von Hippel & Von Krogh, 2016).
- ***Transparency***: Each transaction on the ledger is visible to all parties- but probably encrypted for security purposes (Shahzad & Crowcroft, 2019).
- ***Proof of Concept (PoC)*** Relates to the verification process of the feasibility of an implementation idea in a real scenario (Abuirdris et al., 2021).
- ***Proof-of-person*** **(PoP)**: Relates to the identification that someone is a real person and not a robot or electronic tool (Shahzad & Crowcroft, 2019).
- ***Proof-of-Stake*** Relates to the consensus protocol of Blockchain driven by users and miners on validating the accuracy of new blocks (Abuirdris et al., 2021).
- ***Proof of Work (PoW)*** Relates to the verification mechanism on adding new transactions, it was introduced originally on Bitcoin protocols but has rapidly expanded to other Blockchain applications (Abuirdris et al., 2021).
- ***Zero-knowledge (ZK) proof*** is a protocol between two parties, called the prover and the verifier, that is associated with a language $L = \{x \mid \exists w : R(x,w)\}$, where R is a polynomial-time predicate in a parameter k and x and w are strings of length k. The protocol enables the prover to convince the verifier that she is in possession of a "witness". In plain English, I can prove to someone else that I know something without showing how (U.S. Vote Foundation, 2015).

9.4 Appendix 4 - The Swedish Elections

The Basis

The Swedish electoral system is based on *equal voting rights* and on freedom, secrecy and direct parliamentary voting. It is *free* in the sense that no one else can decide the voter`s choice rather than the voter itself, it is *secret* since there is no need of disclosure of how the voter voted, and it is *direct* since voter chooses which candidate(s) will be elected to the parliament (Valmyndigheten, 2023). Likewise, the Swedish electoral system is described by the authorities as man

ual, decentralized, and transparent. Both the voting reception and voting counting are performed *manually* by both election workers and volunteers. The process of vote reception and vote counting is done locally at local polling stations, which is why the authorities claim the process to be *decentralized*. Another big pillar of the electoral process is *transparency*, the average citizen is allowed to go to any polling station to observe the counting, reception and counting process making the authorities to call the process *transparent* by nature (Valmyndigheten, 2023). These are the foundational pillars the Swedish elections are built upon.

Frequency of voting

Every four years, on the second Sunday in September, ordinary elections are held for the Swedish Parliament as well as regional and municipal governments.

Elections for the European Parliament are held every five years. Each EU member states national electoral law governs how the elections are conducted, and in Sweden, the electoral law demands that election day must always fall on a Sunday.

Sweden conducts *four general elections*:

- The Parliament – 349 members of parliament, legislating for major public issues such as budget, are elected every 4 years.
- Regional councils – Regional counselors, legislating for local issues such as health care, are elected every 4 years.
- Municipal councils – Municipal counselors, legislating for local issues such housing, are elected every 4 years.
- The European Parliament – European Parliamentarians, legislating for major European issues such as budgets, are elected every 5 years (Valmyndigheten, 2023).

Different Constituencies

Constituencies (“election circuits”) are a division of geographical areas in Sweden. In the different constituencies, parties choose running candidates for a seat at the European parliament, Swedish Parliament, regional or local council.

Parliamentary constituencies

Sweden is divided into 29 constituencies for the purposes of elections for the Parliament. There are 349 seats in the Parliament, 310 of which are assigned to fixed constituencies.

Regional constituencies

The regional council decides how many seats the entire council should have as well as whether the region should be divided into one or more constituencies.

Municipal constituencies

The municipal council decides how many seats should be on the full council as well as if the municipality should be divided into one or more constituencies.

European Parliament

Sweden itself represents a constituency for the European Parliament elections. According to every EU Member State's population, seats are allocated among the different members.

Secrecy of Vote

Citizens, without interference from others, can go behind a screen by themselves where they independently collect their ballot papers. Then can enclose votes in envelopes to ensure the vote's confidentiality.

Identification process

Poll workers check the voters' names against a nominal electoral roll and collecting their ballots, in addition they are trained to answer voters' questions and help those who require it.

An accessible electoral system

Legislation in Sweden makes it possible for us to have a very open and accessible electoral process. This indicates that there are numerous ways and locations where you can cast your vote. For instance, you can cast your ballot earlier than on election day almost anywhere in Sweden, on election day you can cast your ballot at your polling station, if you are unable to cast your ballot in person, you can vote by courier or at a mobile polling station, and if you are abroad, you can also cast your ballot from abroad at the Swedish Embassy.

Election results and re-count.

Votes are counted twice: The first on election night in a preliminary count at the local poll stations, and the second counting on the next day by the county council as final count. The election results for the Parliament and the county councils for elections, to regional and municipal councils, are then validated by the election authority i.e., Valmyndigheten.

Corrections may be made up to the time that the county council or the electoral authority has decided on the outcome. The ballots are kept in the county council, and the entire vote-counting process is public. The votes can be recounted multiple times if necessary, repeating the same procedure.

Security

Election security refers to all the election administration's organized efforts to protect the elections through election-related laws. Measurements include physical security, operational security, accident prevention, *information security*, crisis preparation, and continuity management. The Swedish Election Authority and other regulatory bodies have declared the presence of more threats, sabotage attempts, and disinformation campaigns aimed to influence general elections since the 2018 elections. As a result, the Swedish Election Authority started a project to "strengthen the elections" in the spring of 2020 which ran until the end of 2022.

The framework of the project included in one of its points:

"Create a digital introductory course on electoral security and conduct follow up workshops for all municipalities and county administrative boards in the country". (Valmyndigheten, 2023)

Election observation in Sweden

The Organization for Security and Cooperation in Europe (OSCE) is a security cooperation body with 57 participating States that sends international observers to the Swedish elections.

Personal data processing and EU GDPR

Any information that can be directly or indirectly linked to a living person is considered personal data. General Data Protection Regulation is the meaning of the acronym GDPR. The Personal Data Act (PuL), which was formerly in effect in Sweden, is replaced by the legislation. A universal and equal level of protection for personal data is what the General Data Protection Regulation aims to achieve.

The Swedish election Authority is responsible for the *processing* of personal data which involves collecting, transmitting, combining, storing, and erasing the personal data.

Information Control directionality

Election Authority may, in certain circumstances, take steps to protect information in documents to prevent the disclosure of specific personal information. The Public Access to Information and Secrecy Act governs what information the Election Authority is permitted to keep private.