NOVA IMS

Information Management School

MGI

Mestrado em Gestão de Informação

Master Program in Information Management

A PROPOSAL FOR THE USE OF BLOCKCHAIN IN THE PORTUGUESE VOTING SYSTEM

Beatriz Ferreira Braz

Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

A PROPOSAL FOR THE USE OF BLOCKCHAIN IN THE PORTUGUESE VOTING SYSTEM

by

Beatriz Ferreira Braz

Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management, specialization in Knowledge Management and Business Intelligence

Supervisor: Professor Doutor Vitor Manuel Pereira Duarte dos Santos

January 2021

ACKNOWLEDGEMENTS

In order to overcome the difficulties faced during the elaboration of this dissertation, I want to thank, in particular to:

The professors of NOVA Information Management School – Nova University of Lisbon who taught me during classes and shared professional and personal experiences that enriched me at the most diverse levels in order to conclude this Information Management master degree.

Professor Vítor Duarte dos Santos for the motivation, guidance and patience during the realization of this dissertation.

Professors and Digital Transformation Adviser for their interest, availability and shared knowledge about this topic in the granted interviews, which were crucial for the elaboration of this dissertation.

My family and friends for all the support, incentive and patience.

ABSTRACT

The key objective of this proposal is to present one of the problems that the Portuguese economy, as well as other European countries, have been facing in regard to the civil society intervention in the democracy: the decrease of turnover rates in the voting system. The main objective is to propose the use of Blockchain technology in the Portuguese Voting System, as a mechanism to counter this trend.

In order to understand how the possible application of a remote e-voting system succeeds, Estonia was selected as the case of study. Its architecture, as well as the legal, social and technological issues and challenges associated are investigated in the light of the information collected in the literature review.

Considering the case analysis and discussion, a set of recommendations that purpose the use of a remote electronic voting system in the Portuguese electoral system are presented and a critical analysis about the introduction of a Blockchain algorithm is made. This dissertation concludes about the advantages and disadvantages from the use of this decentralized system when compared with a system involving a third-party as the one used in the Estonian I-Voting.

The validation is based on interviews and discussions with professors in the area of information systems and law, and also with a contribution of a Digital adviser of the Estonian e-Governance model.

KEYWORDS

Blockchain; E-voting; I-Voting; E-Government; Decentralized institution; Case Study

INDEX

FIGURES INDEX

TABLES INDEX

LIST OF ABBREVIATIONS AND ACRONYMS

AML	Anti-Money Laundering
ASO	App Store Optimization
BOINC	Berkeley Open Infrastructure for Network Computing
BRICS	Brazil, Russia, India, China and South Africa
CRM	Customer Relationship Management
DBMS	Data Base Management System
DLT	Distributed Ledger Technology
DRE	Direct Recording Electronic
DVD	Digital Versatile Disc
EBP	Electronic Ballot Printer
EC	European Commission
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EC-ELGAMAL	Elliptic Curve ElGamal
EDI	Electronic Data Interchange
EGDI	E-Government Development Index
eIDAS	Electronic Identification and Trust Services
EMB	Electoral Management Body
EPROM	Erasable Programmable Read-Only Memory
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
EUDO	European Union Democracy Observatory

EVM	Electronic Voting Machine
FOO92	Fujioka, Okamoto and Ohta
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
ICT	Information and Communications Technology
ID	Identification/Identity/Identifier
IDEA	Institute for Democracy and Electoral Assistance
IT	Information and Technology
IVCA	I-Voting Client Application
IVS	I-Voting Server
KSI	Keyless Signature Infrastructure
LAN	Local Area Network
MEP	Members of the European Parliament
NEC	National Electoral Committee
OMR	Optical Mark Recognition
OSCE	Organization for Security and Co-operation in Europe
OTP	One-Time Password
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	President Machine
PNC	Pittsburgh National Corporation
PO	Purchase Order
POA	Proof of Authority
QR	Quick Response
RN	Random Number
RSA	Rivest-Shamir-Adleman

RSK	RootStock
RVM	Re-Voting Malware
SCOOP4C	Stakeholder Community Once-Only Principle For Citizens
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SIM	Subscriber Identification Module
SMS	Short Message Service
SOA	Service-Oriented Architecture
SSI	Self-Sovereign Identity
STOA	Scientific Foresight Unit
SVM	Self-Voting Malware
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TV	Television
UI	User Interface
UN	United Nations
UNICEF	United Nations International Children's Emergency Fund
USD	Unified Service Desk
UTAUT	Unified Theory of Acceptance and Use of Technology
VCA	Vote Counting Application
VCS	Vote Counting Server
VDC	Voting District Committees
VFS	Voting Forward Server
VMM	Vote Modification Malware
VSS	Vote Storing Server
VVPAT	Verified Paper Audit Trail
VVPT	Verified Voter Paper Trail

WAP	Wireless Application Protocol
XRP	Native currency of the Ripple network

1. INTRODUCTION

1.1. BACKGROUND AND PROBLEM IDENTIFICATION

Nowadays, many nations around Europe have been facing a general decrease of the turnover rates in both National elections and in European elections. The last European elections, on 2019, turn out to be a different case, where the turnout was the highest in the last 20 years. This situation has been discussed by many journalists, critics, commentators, some politicians and even among the general citizens themselves who contribute largely to the increase of abstention. Several analysis and speeches focus on the understanding of its roots and causes but the consequences are what incentivise policymakers to move to the next level and build a new model able to deal with the new circumstances that the modern society is living and express its vision or feeling through the act of not voting and not showing up in the polls. This is one of the concerns that democracies have been facing. Portugal is not and exception and is the priority for this thesis.

According to *Pordata*, a certified statistics database about Portugal, the abstention rate in the European elections has been increasing continuously since the first year after joining the European Union (currently 69.3%). In the case of Portuguese citizens residing outside of the country, this rate goes up to 99%. These data give us a reason for concern regarding the political power sustainability. However, one of the main causes may not be neglected: the difficulty of voting associated to the lack of polling places and long distances to travel in order to be able to vote. Nowadays, but mainly in the near future, this might not be an explanatory variable for the output anymore.

Moreover, another factor that may be take into consideration for the low turnout performance, is the problem of trust between people and institutions due to imperfect information. Lack of trust in the representatives is mentioned as one of the principal causes and it is the time to meet a technological institution, with a high level of enforcement, efficient and capable to provide a solution to the trust crisis just presented.

In this paper, it will be introduced and explained the e-voting and e-government concepts, analysed and some real examples will be given. This way, one may contextualize regarding the last updates in the use of technology in this matter.

In the district of Évora, Portugal, a pilot project of electronic in-person voting was introduced in the last European elections. Despite of its success, people still need to attend the polling places, use a card that enables the unique vote, print it and drop the paper in the poll. The mobility issue for many citizens still does not take advantage of this initiative.

Furthermore, in the case of e-voting, a short number of European countries such as Estonia, Belgium, France, Bulgaria and Germany already used in one way or another, successfully or unsuccessfully, electronic voting machines. Only Estonia became the first country to enact E-voting law, and this country will be a case of study in this paper. However, one may keep in mind that the majority gave up from the official implementation of this mechanism in both National and European elections, due to the possibility of hacking electronic systems, issues with the certification of election results and the existence of software errors. The distrust and consequent fear in becoming this method constitutional have been contributing for the progress delay.

In order to deal with this trust crisis on one hand and with the mobility issue on the other hand, a more complex, cryptographic and revolutionary technique may take place in order to change the paradigm. A more powerful technology with a practical applicability may be explored and purposed: a decentralized trustless voting system developed by the Blockchain technology.

Blockchain technology may become a glove of fresh air in the next future. It started with Bitcoin and quickly an umbrella of possible applications has been developed during the past few years. Departing from the concept, it is known that cryptography makes the records that are splited into blocks a secure process, and tell us that we can trust in the system. An anomaly in one block is easily detected and its detection avoids immediately the propagation of the problem among the rest of the system. The list of records (also called distributed ledger) is decentralized and available for everyone to see and verify. Blockchain goes beyond of how we know Internet nowadays. It is capable to solve the problem of one, and only one, unique identifier, which makes its application highly relevant in the voting system. Last, but not least, the decentralization enables the speed of data processing by allowing the results to be visible in a country as a whole, despite of the possibility of each district operate with its own system for load distribution.

Concluding, one may use the literature review as a contribution for the research development and, in the end, be able to add knowledge to the existing work by making a purpose of the use of this technology in the Portuguese Voting System.

1.2. MOTIVATION & JUSTIFICATION

Departing from the principle that confidence in the institutions and participation in voting are two important variables that measure the life satisfaction of a nation, as well as its development (*Society at a Glance OECD Social Indicators, 2019*), in this thesis one will explore the potential of technology as a mechanism that contributes for social cohesion. Additionally, the fact that Portuguese residents living outside of the country are the main contributors, in a comparison among different society classes, to the abstention rate, one may keep in mind the important role of young people.

Based on the report *European Parliament Spring Eurobarometer 2019* (Schulmeister et al.,2019), a survey was conducted to all European countries. A sample of around 28000 observations was collected and, in the case of Portugal, 1004 people answered to this survey. Hence, the study was able to conclude that among young people (age in the range of 15-24 years old), only 3% manifested high interest in the European elections, showing the most unsatisfying result when compared to young people of the same age questioned in other European countries. At the same time, all the Portuguese citizens aged 15-24 use Internet every day. Furthermore, regarding the general results, in Portugal the main reasons for people not voting are “You believe your vote will not change anything” and “You distrust the political system”. If a correlation between both variables would be calculated, one will be able to resume both in “Distrust”. These results meet the initial considerations presented in the previous chapter, and are, ultimately, a reason of concern for life satisfaction in Portugal.

Considering these results and further analysis and opinions that come to public from the most various sources, one concluded that only a revolutionary and complex technology would be able to deal with some of the factors that influence the problem presented. Some studies have been made about the potential of Blockchain and its introduction and implementation in some areas, especially in the finance and banking systems. It matters to continue its exploration and implementation in further areas in such a way that a whole society can benefit from it (the general civil society who vote, but also the politicians elected). It may take time and resources until this technology to be understood and used by everyone, but one may contribute to the share of this knowledge, as well for its development applied to the Portuguese economy itself. One may be able to purpose by the end of this thesis the use of Blockchain-based voting system in Portugal, taking into consideration social and economic factors.

Another important topic that may be pointed out is the use of this thesis as a mechanism for extension of the existing knowledge of the area, within the limits of assumptions, with a theoretical application in order to explain, predict and understand the phenomena when applied to a real context. This study aims to contribute for breaking the assumption that still exists a long path to the adoption of technology that supports the online voting.

1.3. Study Objectives

The main objective of this study is to purpose the use of Blockchain technology in the current Portuguese voting system.

In order to argument and fundament its use one will need to study the already implemented E-voting systems and projects, the interactivity with the Blockchain technology, as well as the current electoral system in Portugal and retrieve information regarding possible initiatives to apply technological solutions in this environment and how they succeeded. Summing up, it matters to understand the possible beneficial results of a Blockchain-based voting system in Portugal as a solution for the mobility concern and trust crisis. In a secondary level, it is relevant to learn how its use would impact the abstention rate and the trust in the Portuguese political system.

The above paragraph synthesises the main questions that one will seek for response by the end of this thesis.

2. LITERATURE REVIEW

2.1. ELECTRONIC GOVERNMENT

2.1.1. Concepts

To begin with the exploration of concepts, presentation of models and explanation of applications related to the buzzword "E-Government", it is important to understand what this term brings beyond the books and what it implies. E-Government can be considered a building process, similar to the "(…) process of building a bridge" (*Evans, G. (2017)).* The author in his book makes an analogy between the two processes, where all the components of a physical bridge "must be strong and robust". Imagining two towers, both represent the "Business Support and Transformation Services", the main cables are the "Business Requirements and Benefits", the deck, where the roadway is located on the surface reflects the "Targeted Government Services, the headstock right behind the bridge deck, denominated in this analogy by "Interoperability backbone", in which transparency is the key, and, finally, the main anchors representing the Stability of the Infrastructure. In this book, the author states and explains with this terminology the "five fundamental components of our e-Government bridge", which are essential to "bridge the gap between the old governance and the new". According to this statement, two models, adopted by and simply idealised to the United Kingdom government, are explored, explained and compared side by side. The "old governance" corresponding to the past and the "new governance" belonging to the future. In the old model, corresponding to the era before the "Modernising Government" - a white paper where was introduced and listed the programme of reform and modernisation of the UK's government, the ministries, agencies and non-governmental bodies were in the middle, while stakeholders, citizens, communities and businesses were in the periphery. Hence, these surrounding groups "felt their opinions were not valued", citizens were not aware of their benefits and "income went unclaimed", "very difficult to deal with government at any level" and only the "wealthier and computer literate" could gain from this model. One of the main conclusions one can retrieve from this old model was the term "digital divide" and its implications felt within the society, where the discrimination between those who "could access the technology and those who could not" was clear. Consequently, citizens "felt disconnected from the governance process".

Alternatively, the more recent model mentioned above "puts the citizens, stakeholders, communities and businesses at the heart of governance", while agencies and non-governmental bodies working with the ministries support the population in the middle. This is the core of the "e-Government" according to the author. As main results, one may state the citizens becoming "better educated to take advantage of opportunities", higher responsiveness of the government, citizens become aware of the governance process, "services become more targeted", higher flexibility, "cost reductions and efficiency gains" and, overall, "the social and digital divide shrinks". However, it matters to highlight the different results between the old and the new governance models in regard to the voting system: in the first case, people feel discouraged to vote, while in the second, "voting numbers reach all time highs".

Drawing relevant conclusions from this book, the author uses the word “roads” to make an analogy between the bridge example and the E-Government policies necessary to adopt in order “to link our e-Government road system with that of European, and eventually global, networks”. Lastly, E-Government is described as “not just about technology replacing old processes and standards.”, but mainly a “strategy that sought to completely reinvent the way to implement the governance model in the future. It redefined how government should interact with its stakeholders and created a completely new framework for the internal interactions between departments and agencies”.

Despite of the fact that e-Government is considered as a “bridge” for this author between different Governance models, the difference between this concept and e-Governance is clear for other authors and not addressed in this book, creating a limitation to make use of both concepts in a more intelligent and flexible manner.

In the book of Bhatnagar, S. C. (2004), the author retrieves the concept of Governance from a World Bank publication, defined as “the manner in which power is exercised in the management of a country’s economic and social resources for development.” The term “accountability” is important and used to distinguish from “efficiency”, in the matter of management of resources on behalf of public officials without “abuse of power”. Bearing this in mind, the author distinguishes also Governance as “a broader concept that encompasses the state’s institutional arrangements, decision -making processes, implementation capacity and the relationship between government officials and the public”. Hence, E-Governance is defined as “the use of ICT by the government, civil society and political institutions to engage citizens through dialogue and feedback to promote their greater participation in the process of governance of these institutions”. On the other hand, E-Government is considered by the author as a “subset of e-governance”, focused mainly “on improving administrative efficiency and reducing administrative corruption”, and sometimes both terms are confused. Finally, the concept is introduced in a paragraph, where he affirms this buzzword “harnesses information technologies (such as wide area networks, the Internet and mobile computing) to transform relations with citizens, businesses and other arms of government”. This is a good example of a beneficial use of technology to promote better delivery of services to society, create smarter interactions between the government and businesses and contributing to a more efficient management of the government. In the end, the author indicates “less corruption, increased transparency, greater convenience, revenue growth and/or cost reductions” as benefits.

In order to address the voting system thematic, in the article of Alhawawsha, M. (2017), it is studied a new E-Government voting system that supports the government with the election process. Hence, this term considers “the use of electronic mediums to facilitate the services to the public of the country”, making use of the “information and communication technology” and “allows the citizen to engage with the government at all the levels”, helping him/her to “involve in the local and national governance”. Beyond the definition of the use of Information and Communication Technology in the provision of public services to citizens with higher efficiency and effectivity in the management of government, other authors add to the E-Government concept its benefits as well. “E-government is recognized as a tool for improving transparency and openness in the public sector and for combatting corruption”, as stated in Machova, R., Volejnikova, J., & Lnenicka, M. (2018).

2.1.2. Architecture & Tools

In order to implement policies and provide services to citizens through the use of electronic devices, it is required an architecture framework for the e-government adoption that facilitates the understanding of requirements, both technological, as well organizational and governmental. Hence, this framework can support the decision makers and policy makers in their “vision statement and strategic action plan for future direction in the information technology age through identifying key elements and stages of action” (Ebrahim, Z., & Irani, Z. (2005)). In this paper, the authors study an architecture framework for e-government, demonstrating its potential, risks (security issue) and further limitations. For the purpose of this study, one will focus on the framework developed and explain each of the main components.

In the appendix 1, there are four layers (access layer, e-government layer, e-business layer and infrastructure layer), connected, in a sense of flow schema. However, the authors start by defining the meaning of e-government architecture as “the standards, infrastructure components, applications, technologies, business model and guidelines for electronic commerce among and between organizations that facilitates the interaction of the government and promotes group productivity”. Furthermore, they state what this paper contributes for the state of art and adds in regard to other studies already developed and published of the architecture: “provide an integrated architecture framework for e-government that represent the alignment of IT infrastructure with business process management in public sector organizations”. Right after, the indication and description of the four layers is presented, starting by the top level and concluding in the bottom level of the schema.

Firstly, the Access layer is described as “the channels that government users can access the various government services”, and the explanation goes further regarding the access channels as “online and offline channels or routes of distribution through which products, service and information are used, access and communicated by multiple technologies.” Some examples are indicated by the authors such as web sites, kiosks, mobile phones (WAP), Digital TV and call and contact centers. After, the second layer is introduced and gives the name to the architecture: E-government layer. It integrates data of organizations into a “web-portal of government services, in the form of a one-stop e-government portal”. Through a single window, it is visible and accessible all information in one place. The “web-based front-end application” allows different sources of information to be linked among them. According so, the integration, linkage and share of information between different organizations has a big potential for citizens who may benefit of an easier and more efficient way of updating personal details, such as a new address (“citizen moves from his/her residence”), allowing “this cumbersome process to a single step”. In the end, the authors explain some of the reasons and cons that lead to the slow adoption of a web-portal. On one hand, the difficulty in choose the most relevant applications and features, on the other hand, a more technical reason related to the required interconnection of public organizations and the transparency between of their systems (interoperability). It is necessary “comprehensive technology, systems integration and project management skills”. The last issue pointed our is the Security, “through deploying government authentication and privacy standards to secure online transactions and protect the portal contents.”

The third layer is the E-business. It is focused on "using ICT applications and tools to harness a network of trust, knowledge sharing and information processing that takes place both within and between organisations". In another words, the government portal incorporates front-end applications ("online catalogues and transactions interfaces"), with back-end activities ("existing databases and data warehouses"). The authors address the topic by distinguishing from the traditional method, where government bodies maintain "separate databases that are not connected" between each other. It is classified as a challenge for the implementation of an e-government portal, once transmission of data and communication have barriers. However, in this layer is required "computer systems and applications of different public departments and organizations" to being "connected" and/or "communicating with each other". Thereon, a table is presented (appendix 2) and a collection of applications and systems, relevant for the architecture, are indicated as a mean to deliver through different channels information and services to the population.

DBMS (Data Base Management System), CRM (Customer Relationship Management), Enterprise Resource Planning (ERP), Web service application, Data Warehousing, EDI (Electronic Data Interchange) and Document management systems, are some of the applications/systems discussed in this paper that "help determine, assess, and achieve consistent and integrated processes and information systems in public sector organisation".

The fourth and last layer is the Infrastructure. It is represented in the bottom level and "focuses on technologies that should be in place before e-government services can be offered reliably and effectively to the public". These technologies may "support and integrate the operations of information systems and applications in e-business layer organizations", through the use of appropriated network and communication infrastructure: "intranet, extranet, and internet". Another two technologies described is the LAN and Server, which counting the five mentioned, they are powerful technologies used to "support the acquisition, storage, and transformation of data". In the end, the authors mention the biggest issue associated: the security of infrastructure. Once the use of public networks increases, as well the databases holding citizens personal information and government information, it is required major security tools that ensure protection against fraud. "Digital signature and certificate, and sophisticated encryption technique, which secure e-government interoperation, government electronic transactions, and delivery systems" are some technologies capable to protect the system from cyber-attacks, for example.

In the paper "E-Government Based on Cloud Computing and Service-Oriented Architecture" (Cellary, W., & Strykowski, S. (2009)), another two types of architectures are studied by the authors and they defend that the circumstances on that time of computer infrastructure development together with the user's skills and knowledge of computers and Internet, are two good factors to stimulate the adoption of the two new architectures: "cloud computing and service-oriented architecture, in the public sector". Hence, one will describe the two models and arguments for their adoption.

Before that, the main obstacle for the evolution of e-government is introduced: "Interoperability", already addressed by Ebrahim, Z., & Irani, Z. (2005), however in the current paper that is being analysed, this concept is more emphasized. According to the authors, this problem rises "under two conditions": e-government achieves "such a level of development that integrated inter-unit services are required" and "systems providing e-services in different administrative units are incompatible". Also, in this sense, "lack of leadership" is pointed out as the biggest cause for "incompatibility of IT systems providing e-services in different administrative units”. They explain that the “local solutions” created are easily appreciated by “local governments and customers”, once they are “user friendly and efficient”, but only because of the “limited functionality” that leads to “simplicity”. However, once the need for integrated e-services arises, these local solutions are not adapted and even an obstacle. If IT developers would work on the integration of these solutions with other systems, their life would not be easy: “they are not able to cooperate with other systems developed independently under different assumptions”. After that, two solutions are presented: either “replace or rebuilt the local systems” to reach common standards with the non-local systems, or develop “intermediary systems that make cooperation of heterogenous local systems possible”. As an alternative, Cloud computing is mentioned as “a business model of delivering IT resources and applications as services accessible remotely over the Internet rather than locally”. Instead of users purchasing products sold or licensed from a vendor, with cloud computing, “a user purchases remote access” to hardware or software “via the Internet”.

This model has three levels: “Infrastructure as a Service – IaaS” (examples of infrastructure are “servers”, “network equipment and system software like operating systems and database systems”), and IaaS delivers computer infrastructure as a service and “is one of many virtual environments hosted simultaneously on the same physical infrastructure resources”; “Platform as a Service – PaaS” (delivers “application development environment”); “Software as a Service – SaaS” (delivers complete applications such as CRM or ERP over the internet and “a client purchases an access to these applications instead of purchasing licenses and exploiting them locally”). Following the Software as a service concept, the main benefits of cloud computing come “from aggregation that permits to eliminate redundancy”. In this sense, there are two levels of aggregation: “Aggregation at the level of organizational units”, meaning, “hospitals, schools, agencies of local governments”, among other public institutions, have “similar needs of data processing”, mainly due to legal requirements. Hence, these similar units “require the same software functionality to manage their operations”. Cloud computing plays a crucial role in this area. The same center providing SaaS may serve all the units of the same type (hospitals, schools, etc), and knowing that two hospitals are different from one another, the software may be adjusted to meet the specific requirements of each one; regarding the “Aggregation at the level of functional modules”, once the legal regulations may be the same across different units, “some functions performed” are the same. The authors mention some examples such as “management of human resources, payroll, business trips”. Hence, a common function may be used as a SaaS for any unit and, also, cloud computing offers “different software modules” adjusted to customers’ needs. In the end of the exploration of this model, the authors list the advantages of its adoption: “Dynamic load of resources”, meaning a customer can purchase more or less of hardware and software resources, according to its needs in a given moment; “Professional maintenance and administration”, a cloud computing provider manages the hiring process of appropriate staff capable to maintain and administrate with high quality the hardware and software; “Timely software updates”, customers do not need to worry with last versions of software, once the cloud computing system automatically and continuously adapts new updates, as well as changes according to the legal regulations; “Higher security”; “Higher performance”; “Shift from investment cost to operational costs”; “Dissemination of good practices”, meaning with the adoption of cloud computing, local institutions will be more capable to follow e-government initiatives, instead of “purchasing and deploying e-government solutions by themselves”. Summing up, the model described facilitates the dissemination of e-government tools across different units and the data processing in the whole public sector.

In the same paper, another architecture is presented: “Service-Oriented Architecture (SOA)”. According to the name itself, the author considers the “primary building block” the service, at the moment of designing and developing IT solutions. Among many other definitions, service is considered a “container of capabilities associated with a common purpose”. In order to implement services, three technologies are mentioned by the author, which facilitate the development of “service compositions” (“ordered invocation of services to automate executions of a task, or a business or administrative process”), and “service repository” (“collection of services running in an enterprise” and “organized and managed according to a local policy”). Hereupon, the main goal of this architecture is to avoid the existence of “redundancy among services” and that “services can interoperate”. Thus, efficiency and high impact in the life of citizens in the provision of these service compositions can be guaranteed.

Another relevant characteristic worth of mentioning is the “information sharing in and outside the public sector”. This means among public entities and external ones (businesses and citizens). In order to exemplify the features mentioned before, the author shows a figure where the provision of a mix service, “composed of services provided by both governmental and business units”, where these entities are working independently but providing each one its service that, all combined, constitute the final service that the citizen benefits. In an “heterogeneous environment”, suitable for public and private sectors collaboration, the “Enterprise Service Bus (ESB)” tool takes an important role, enabling in this type of environment “application and system connectivity”, taking into consideration the integration of legal requirements and components of the “governmental IT environment”.

In the end, the author concludes that combining the two models, Cloud computing and Service-Oriented architectures, bring many advantages into place, at different spheres: “technical, organizational, social and economical”. However, he alerts to the need of the government understand deeply the importance of electronic government and, as a consequence, reconsider the legislation and adapt to the implementation of these architectures.

In the last paper reviewed for this study (Mosa, A., El-Bakry, H., El-Razek, S., & Hasan, S. (2016)), another architecture is explained, conciliating the Cloud Computing and Service-Oriented models’ benefits, such as interoperability, flexibility, manageability, saving of time, cost and economies of scale, among others. Hence, the main purpose of this paper is to “propose a framework of e-government services that bases on using pros of cloud computing environment” and is “evaluated on deep discussion relative to interoperability and integration”. To start with, the authors write about the Internet as the special form of innovation that e-government can use as a mean to “giving helpful access to administrations and government data”. Therefore, “Web service systems” are understand as a way to “facilitate interactions between government agencies area unit and general public”. Thus, it matters to know the implications to a database system. Its design replicates subsets of the government units’ databases “into the Integrated Central Database” which the main features are “replication and accessibility”, but both of them “suffer from the lack of vital features which are: interoperability, flexibility and manageability”. As a solution, the authors come with another architecture already mentioned: “Service-Oriented Architecture (SOA)”. It is able to achieve the weakness of a typical Web Service Based Architecture with its integrated central database. Hence, experts have tried to become a web service model into a SOA. However, despite of important characteristics as interoperability, flexibility and manageability, it is still missing some relevant ones that a Cloud Computing Architecture is able to overcome: “save time, cost, scale, etc”.

Concluding, the proposed model is based on an e-government application which faces and seeks to solve some challenges as “information management systems, central database, robust infrastructure, interoperability, integrity and much more”. The authors refer that the focus of this study is on “handling quality of service, integrity, delivery status, workflow notification, cost, security and interoperability between different organizations under approved unified government umbrella.” Furthermore, this model is dedicated to solve the issues related to a web service architecture, consisting in “technical issues and functional challenges”. Hence, this web limited architecture is characterized by the “single user profiling”, meaning that in the application there is only a single-entry point for all users. This point makes accessibility restricted and discourages users to access. It is required system stability, data, actions and flows of client’s requests consistent. Hence, synchronization is needed and an important technical issue to be considered. Afterwards, one meets the functional requirements, which are the basis for the creation of the proposed cloud based e-government framework. These requirements are divided in three blocks: “user interface”, “data storage” and “back end” (appendix 3). The User Interface scope is a range of possible entry points of the application and computing terminals. “Web Pages” are known as the “basic entry point”, the “Native App” is the interface for mobile devices, tablets, laptops, and also web page. The third example is the “Cross Platform App”, “fully supported depending on different technologies” and, finally, “Resources”, which focus on the need of sharing resources across these types of user interfaces globally. According to the synchronization challenge and central data storage feature, both are required to keep the UI consistency. In the second block, Data Storage, is able to “satiate one or more instance of database”. These instances are transparent, offering the guarantees required for a strong database repository: “data integrity checks”, “consistency” and “consolidation”. Moreover, synchronization is again mentioned as the key to keep the data up-to-date. “Android SDK”, “Asp.net SDK” and “Other SDK” support “high precision of application development, integrity and compatibility”. In the last block mentioned, management, logistic, among other important tasks are stored. “User management service”, focused on facilitating user authentication and enabling the storage of data in user accounts. This service also makes possible to users authenticate internally through the app or with social networks (Facebook, Twitter and Google+ account). The “Workflow management service” is also useful when it comes to deal with different data formats and, on the other hand, the “Document Management” service dedicates to find files efficiently and effectively, in a short period of time (seconds), enables also concurrent users who seek to access the same file at the same time and free to edit, access further information, manage security, among other settings. “Notification services” is another module, which enforces users to keep up-to-date and track their enquiry.

Summing up, “interoperability”, “integrity”, “transparency”, as well as “accessibility”, “flexibility” and “manageability” are issues and challenges to other models, but according to this authors’ study, they are overcame with this proposal of a Cloud based e-government framework. In the financial and organizational spectrums, investment is considered safe, once the total cost associated “should“ be minimum”.

2.1.3. Case Studies

In order to investigate and understand better the potential of E-government, in this chapter one will present some examples already implemented in different geographies.

In Melin, U., & Axelsson, K. (2009), two e-government projects implemented in Sweden, as main purpose to better understand the chances of success or failure of these type of initiatives. The author explores an "e-government systems development life cycle", claiming based on other studies that typically this cycle consists in five phases: starting in "Project assessment", going to "Analysis of current reality", passing through "Design of the new system", "System construction" and, finally, its "Implementation and beyond". Supported by this development life cycle, the author explores two projects: "the provisional driving licence application project" and "the driving licence web portal project" (appendix 4). The overall idea is that in Sweden anyone who wants to get a driving license, needs to apply firstly for a "provisional driving license". After, the regional County Administration (CoA) will judge the applicant, in order to determine if he/she is able to drive in a responsible manner. This judgement process in order to an applicant get a driving license is a cycle full of requirements and some bureaucracy is needed ("health declaration", "certificate of good eyesight", application that states a "parent is permitted to act as a private instructor", criminal record, among others). Hence, this mix of declarations, information, contacts and responsibilities is considered as a good opportunity to develop the provision of an e-service.

The first project mentioned, "provisional driving license application project", was created in order to automate the decision in more simple applications that do not "call for any extensive handling process". Hence, the resources could be reallocated to more extensive and complex cases. This e-service would be able to check the veracity, quality and accuracy of the data in the filling forms for the driving license application. Also, this service helps citizens to redirect to the right CoA. On the other hand, the "driving license web portal project" would facilitate the share of information and provision of different services by different authorities in order to get a license. This web portal is an "one-stop e-government solution", establishing a bridge between citizens and government agencies and organizations. Further, both projects were analysed and discussed by the author, which reveals the web portal as the most successful one. Different stages of development were pointed out, as the "project assessment" itself, "analysis of current reality", "design of the new system", "system construction" and "implementation and beyond". In the first mentioned stage, two main factors for the development of an application project were cited: "government's commission" to incentivize an e-service development and, then, the fact that this e-government solution is easier to accomplish. In the second stage, some challenges were faced by the parts involved. There was a need to hire external consultancy firms to execute the technical development, as well the project manager required, in a later phase of the project, external help to manage the activities. For the design stage, the lack of knowledge and experience of the staff involved, together with the need of legal regulation's update, this development became more time-consuming than expected. The second last phase identify the problems in the management of customer's needs, once they were "unclear and imprecise", missing the interpretation and expertise of senior consultants to facilitate the communication and meet of expectations. In the end, the implementation was not clear once it was not defined in a raw stage who were the ones responsible for the IT system maintenance. However, the development and implementation of the web portal happened in the other way around. Since the clear objectives from scratch ("only place to find governmental information about driving licenses and the portal should be a joint agency responsibility"), to the relevant experience of the project manager and consequent follow of a well-defined model, the design organization ("focus groups" with citizens to gather different opinions and a way to evaluate the development and performance), the possibility of delivering good results before the deadline and below the initial budget and, finally, in the implementation stage, every steps were well-defined since the beginning: the portal existed at the same time as the remaining former websites in the area. This period of time was used efficiently for testing the user's experience and, in the end, the former sites were closed, making this portal the only one able to provide this type of e-government service.

Sweden is among the top countries in the world that more successfully implemented e-government strategies (the index rating of EGDI – E-Government Development Index in 2018 is 0.89). Although it matters to understand better which factors bring Nordic countries to the top of this ranking evaluated across different nations worldwide.

In the article from Joseph, S. & Avdic, A. (2016), entitled "Where do the Nordic Nations' Strategies Take e-Government?", the authors study the leading nations in Europe (Sweden, Norway, Denmark and Finland) regarding the implementation of e-government strategies. These four countries demonstrate a will to become world leaders in the improvement of efficient and effective public sector services, supported by "electronic information and communication technologies" tools. As main results, in this article is presented a table where is accounted the number of strategic measures adopted by the different governments within different sectors and categories of the economy. From Public sector reforms, to Economic reforms, and without forgetting e-Democracy, the Public sector takes in all countries the major efforts (higher number of measures). Some examples are "legal measures for e-Identification", "service sector reforms" and "public sector integration efforts". "Digitized welfare" is another generic example of public sector reform, focused on the "delivery of welfare services using digital means". Regarding e-Participation, the generic example of e-Democracy, only Sweden and Finland adopted measures. In order to explain more effectively what each nation has been developing, the authors constructed a matrix where the Infrastructure component is presented. In the case of Sweden (already studied in the paper of Melin, U., & Axelsson, K. (2009), the "Government Information portals for citizens and single point portal for businesses" is the main example indicated, as well as the security between government and EU bodies through an "IP-based network". In Denmark, a "single Internet entry point for citizens with self-service and mobile platforms" was developed, and also an "online trading portal and educational materials website with special design for digital illiterates". These progresses are not exclusive to the Danish case. In Norway, further developments were achieved as well. "One-stop service portal to citizens with secured interaction point", as already implemented in Sweden, "point of single contact for businesses, standardization portal, and portal for geo-spatial infrastructure". Finally, Finland is not an exception and a portal with single access point was also developed to citizens to access it. In this portal, they can benefit of e-services provision, "enterprise services" and "geo-data portal". Closer to the end of this article, the authors discuss the results and draw some conclusions as the organization of these Nordic countries, as the government initiatives departing from the ministries and other Public departments. They offer the opportunity and invest strongly in the implementation of measures as the ones already mentioned, incentivizing also the citizens participation, creating conditions that facilitate their involvement in policy making. Another relevant topic addressed in the end is the interoperability offered through the standardization of “software, systems and other e-Government artefacts”.

For this dissertation, it matters to understand what is the position of Portugal regarding the adoption of e-government measures. According to the United Nations E-Government Survey, published in 2018, Portugal is the 29th country performing better in this context. In order to understand better what has been done, in the article from Paiva Dias, G., & Gomes, H. (2014), the authors study the evolution of the Portuguese nation. Hence, a “three-dimensional maturity model” is developed to support the characterization of the “local e-government evolution”. The three dimensions are “access to government information (information)”, “electronic service delivery (services)” and “participation in public decisions (participation)”. They represent three different supply sides of e-government.

For the information dimension, it is evaluated different stages: the general information about the municipality, the possibility to download public documentation (without previous authentication), a search tool to find information in the documents and, also, the possibility to “parametrize searches for documents based on their characteristics”. The second dimension is the services one, as already mentioned. In the website of any municipality, it is provided information about services that citizens may benefit of. They may authenticate in the website in order to monitor the services and, also, it is made available the upload of files, even if the formalization is done in physical interaction. In a final stage, citizens are allowed to “request and complete at least one electronic service provided by the city council” after authentication. Regarding the third dimension mentioned, the participation one, in a first stage, with or without authentication, everyone is free to “submit suggestions and/or complaints”. In a second stage, with or without authentication, anonymously or not, citizens have the freedom to participate more actively in “policy areas of the city council”, through “opinion polls” and “discussion groups”. In a third stage, the city council has the duty to respond and take into consideration the public discussion regarding several matters, and finally, in the fourth and last stage, influence on public budget is included and mechanisms are adopted in order to consider participatory democracy. However, with this methodology adopted and the performance evaluated across different dimensions and different municipalities, “local e-government in Portugal remains substantially underdeveloped”. This conclusion is achieved when comparing the results of 2013 with 2010. Also, the possibility for citizens to participate actively in opinion polls, discussion groups, share their suggestions and complaints, is still very conditioned by municipalities.

In another study about the local e-government in Portugal, from Soares, D., Amaral, L., Ferreira, L. & Lameiras, M. (2019), the performance of 308 municipalities in Portugal is measured and a global ranking is calculated about the provision of online services, conditions created to stimulate citizen’s participation, which topics are addressed via web and searching parameters. The four structural dimensions that are integrated in this study are: Contents (evaluate topics addressed, made available, as well as their continuous update); Accessibility, Searching and Utilization, which focus on the citizen’s experience while surfing on the website; the Online Services, based on the evaluation of them, as well as the authentication and email services and, finally; Participation, where the level of participation is measured and the facilities that each City Council offers to its citizens in order for them to participate more actively in discussion and suggestion polls, as well as specific areas dedicated to transparency, open data and other initiatives (participative budget). Among these dimensions, the most critical ones are the online services and participation. However, in this study from 2019, the authors recognize the general efforts to increase dematerialization, de-bureaucratization and simplification of processes from Public Administration. Hence, greater transparency is visible, even if a gap between municipalities persist.

2.2. E-VOTING

2.2.1. Concepts

In the paper from Zissis, D. & Lekkas, D. (2011), the authors conclude an important fact about citizen participation, already discussed before. According to them, Electronic Voting that complies with all necessary security and it is made available to population, increases citizen participation. The importance of voting is study in schools, remembered by news and recalled in the voting days in order to raise awareness. In this study, it is emphasized the need to become the voting system digital, "offer citizens a timely, location-independent, and transparent means of participation in governance." In this sense, two types of electronic voting are mentioned: the remote e-voting and "Poll-site" e-voting. The first one presents advantages over the second: "cost reductions due to economies of scale and increased participation due to voter geographic independence." Moreover, by complying with all security requirements, together with the cost reductions and mobility issue solved, the turnout may increase.

In this sense, it matters to understand better the concept of E-Voting. According to Al-Ameen, A. & Talab, S. (2013), E-voting is "a voting system in which the election data is recorded, stored and processed primarily as digital information." Furthermore, the authors summarize the main benefits of Electronic voting and why it is better: "E-voting may become the quickest, cheapest, and the most efficient way to administer election and count vote since it only consists of simple process or procedure and require few workers within the process." In this paper, the authors also describe E-Voting as "any type of voting that involves electronic means" and further, they distinguish two types of E-voting: "in-site" and "remote". "The in-site E-voting system" is when voters are identified through their identification card, but "push buttons" on an electronic device instead of the traditional paper form. This way, the citizens still need to mobilize to the polling stations where they can find the electronic devices. The other type is "the remote voting process". Through this system, voters are allowed to choose either to vote "by using computers at remote locations or at polling stations". Both computer and internet are used to vote through an application, where voters go through all the same steps as in-site voters, but remotely, reducing the mobility cost.

In an article written by Bosova, E. & Reut, D. (2019), entitled by "Remote Electronic Voting: search for legislative formalization", the authors investigate the introduction of E-Voting via remote in Russia. They mention the two forms of E-voting: "electronic and remote". Right after, they define the concept of E-Voting as "voting without the use of a ballot made on paper, using a technical means". These "technical means" are later listed under different types of electronic voting: "means of electronic counting of votes", "electronic voting facilities", "voting with the help of terminals installed at polling stations", and "remote voting: via the Internet (using disks and social cards) and mobile communication”. Regarding the “means of electronic counting of votes”, the authors explain the need for “new software and hardware-complexes of processing of ballots”.

In another article written by Abba, A., Awad, M., Al-Qudah, Z., & Jallad, A. (2017), “Security Analysis of Current Voting Systems”, the authors define the concept of Electronic Voting: “a voting procedure that enables voters to cast a safe, secret, and secure ballot over an electronic system”. Furthermore, they distinguish clearly this concept from I-Voting (Internet Voting): “e-voting is different to Internet Voting where voters cast their ballots remotely over the Internet”. Hence, these authors bring a different approach of E-Voting types by not considering the use of Internet as a technical mean of traditional E-Voting. This lack of consensus between different authors leads one to explore further research over the two concepts and how Internet is considered: as a type of Electronic Voting or if an independent concept.

According to the article from Beroggi, G. (2014), “Internet Voting: An Empirical Evaluation”, the author focuses his study in the Internet Voting system. However, he addresses this topic as an important process to be integrated in the “government’s electronics systems”: “E-citizens enable Internet voting to go completely paperless, along with its integration into the government’s electronic systems”. Also, he makes a reference to other electronic government services that are already performed via Internet, voting is an important act that may benefit from internet capabilities as well. Furthermore, he declares that the “True Internet voting should be based fully on digital communication, which means delivering the voting material electronically as well as casting votes in that format.” In another study (Powell, A., Williams, C., Bock, D., Doellman, T. & Allen, J. (2012)), the implementation of Internet Voting as a mean of electronic voting is also point of interest: “With the increased interest in e-voting, it is natural that attention has been given to the potential for implementing online voting via the internet.” In another more recent study (Chondros, N. Zhang, B. et. Al (2019)), the authors base their work in previous literature that mention e-voting systems already introduced, as “the kiosk-based systems” and “internet voting systems”.
For the purpose of this dissertation, one will consider Internet Voting as one type of Electronic Voting, besides of other possible definitions defended by different authors.

2.2.2. Architecture & Tools

In order to understand how the E-Voting schema works, which processes are involved, tools and the methods and characteristics involved that become the system secure, one will explore different Electronic Voting architectures.

Starting with an example of an architecture based on “Elliptic Curve ElGamal (EC-ELGAMAL) cryptography”, explored in the article written by Sodiya, A., Adelani, D., & Onashoga, S. (2011), has as its main principle ensuring the security of all voting process. This security exists once “privacy”, “non-coercion” and “receipt-freeness” (voter cannot prove and reveal his ballot in any bribery circumstance). The idea is, first, encrypt the vote and, in a final stage (tallying phase), decrypt it.

In the figure 1, the Electronic Voting Architecture based on EC-ELGAMAL is put in schema. It is constituted by six phases.

Firstly, the **registration** before the election act is executed. At this moment, voters need to prove their “identity” and “eligibility”. Age and more personal details of each voter are consulted in a national database in order to ensure that is not involved in any crime and is able to proceed. Other relevant features to be included in this registration phase are “fingerprint” or “face recognition”. Then, two details are required: username and a token number generated randomly to log-in in the next phase.

Secondly, the **validation** is done when the voters authenticate by supplying the username and the previous generated random pin number. Hence, the voter is now eligible to vote or, otherwise, his/her access will be denied.

Thirdly, the voting phase takes place and the voter’s choice follows to the tallying one. Cryptography guarantees the following: Privacy or “Anonymity”, “non-coerciveness” and “receipt-freeness”. Privacy implies that a vote cannot be linked to the voter; non-coercion and receipt-freeness, ensure that bribery cannot be committed in the process.

The middle phase between the casting and tallying is the “Election Controller”, more concretely, “EC-ElGamal Encryption”. The main idea is using points “on an elliptic curve for encryption parameters of an ElGamal Encryption except the private key “. A logarithm algorithm is used to determine these points, in which the encryption and decryption is executed.

In the end, all encrypted votes are decrypted while sending them to this phase. The “Audit trail” is where the results are verified and made known to the public.

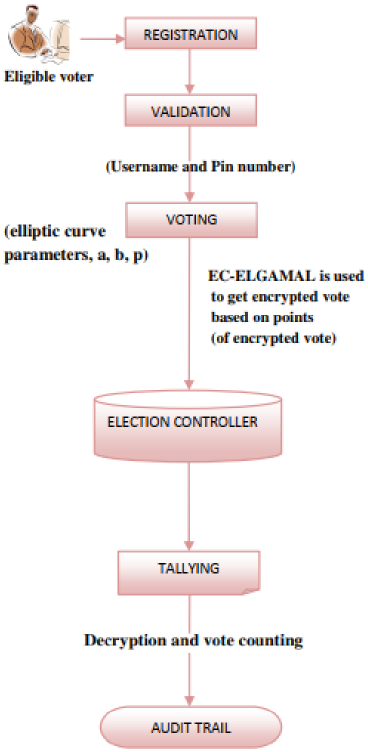


Figure 1 - E-Voting Architecture based on EC-ELGAMAL (Sodiya, A., Adelani, D., & Onashoga, S. (2011))

In another study (Cooke, R. & Anane, R. (2012)), it is presented a different architecture that uses as its basis the FOO92 protocol. According to Kremer, S. & Ryan, M (2005), this protocol works with Blind signatures. Also, it complies with most of the properties which electronic voting protocols may address: “fairness”, “eligibility”, “privacy” and “individual verifiability”.

However, the authors state that this accomplishment is under informal analysis. In this paper, they are able to prove formally three of the four properties: “fairness”, “eligibility” and “privacy”. Fairness is about the fact that no voter is able to access early results, otherwise it would influence his/her decision. Regarding eligibility, only legitimate voters are able to vote (age, criminal record verification, among other requirements), and only once. Then, privacy guarantees the voting is not shared with anyone else.

Theoretically, FOO92 protocol “involves voters, an administrator, verifying that only eligible voters can cast votes.” Furthermore, some cryptographic primitives’ techniques, such as “secure bi-commitment” and “blind signatures”, and, “relies on anonymous channels”.

Returning to the system architecture discussed in Cooke, R. & Anane, R. (2012), the voting process is splited in three main phases:

- Validation: “The voter is known but the vote is unknown”;
- Transmission: the vote is transmitted and, meanwhile, both voter and vote are not known;
- Recording: when the vote is acknowledged but the voter persists unknown.

The process schema which involves these three phases can be visualized in the appendix 5. Firstly, the voter is authenticated by the Administrator and also, this virtual agent retrieves the citizen’s identification information plus the election details themselves. After, a “personal random number” generated and the election details are sent to the “Validator” virtual space. The Validator has the function to sign the message sent by the voter with a “blind signature”, validate the details of the citizen and returns the blinded vote to the voter. This process prevents fraud from “multiple requests for validation from the same voter”.

Secondly, once the validation is successful, the voter unblinds and encrypts the vote that was validated by the Validator in the previous step. With the use of a public key of the Counter (“V={{choice, electionId, RN} val−priv}count−pub”), the encrypted message will be transmitted through a chain of nodes (“routing nodes”) until reach the “Collector”. The Collector will extract the “packaged ballot”, check and validate the message, finishing its role in the chain by forward the message to the Counter.

Thirdly, the Counter checks the ballot waiting for validation, “extracts the vote and adds it to the appropriate tally”. This vote will be also recorded in the database “against the personal random number of the Voter”.

Finally, in order to understand the security of the process and anonymity involved, it matters to know the techniques used. The generation of a RN (Random Number) as a token by the Voter, preventing fraud by not allowing multiple votes by one single voter. Then, the use of blind signatures and symmetric encryption to guarantee the anonymity of the vote when it is sent to the Validator by the Voter. Later, the asymmetric encryption by using a public key (Counter) in order to encrypt the vote and a private one by the Validator. Summing up, the process of encrypting and decrypting the vote is done repeatedly from node to node involved in the process. Decryption is done so the vote is accessed and the encrypted route is made known so the message can follow to the next node, and encryption happens afterwards, in order to guarantee the security.

2.2.3. Case Studies

After understanding how the electronic voting can be processed, one will present a general worldwide overview of the use of Information and Communications Technology (ICTs) in the Voting system, focusing in a higher level of detail in some countries that will be used as case studies.

According to the International Institute for Democracy and Electoral Assistance (International IDEA) survey related to "ICTs in Elections Database", data and information about voting systems in each different country (mainly about the use of technology in the process and the current status about the adoption of electronic means to vote, as well as some existing pros and obstacles for its adoption), was retrieved from a questionnaire done to the many Electoral Management Bodies (EMBs) across the world . The database collects data and information about 183 countries, and major efforts are applied in order to maintain the data up-to-date. The latest updates date back to 2018.

In the table 1 below, some important numbers and percentages are presented in order to understand the status of Electronic Voting in the big picture.

Question	**Answer & Conclusions**	**EU framework**
"Is e-voting currently used in any elections with EMB participation?"	Total #Countries: 176 E-Voting **is used**: 34 countries E-Voting **is not used**: 142 countries E-Voting is used in **19.3%** of countries worldwide E-Voting is **not used in 23 countries of the EU** and only used by 4 (**Belgium, Bulgaria, Estonia and France**)	
"If e-voting is currently being used, what type(s) of technology used?" (E-Voting is <u>used</u> in question 1)	Total #Countries: 33 **Electronic ballot printers – EBPs** (total): 4 **Internet voting systems** (total): 10 **Direct recording electronic – DRE** (total): 16 **Optical Mark Recognition - OMR** (total): 9 **Machines with and without Voter-Verified Paper Audit Trail - VVPAT** (total): 16 **SMS voting system**: 1	**Belgium** uses EBPs, **Bulgaria** uses DRE and VVPAT, **Estonia** uses Internet voting systems and **France** DRE, VVPAT and Internet voting systems.

"If e-voting is currently being used, is it taking place in controlled or uncontrolled environment?" (E-Voting is used in question 1)	Total #Countries: 33 **Controlled** by EMB: 25 countries **Uncontrolled**: 4 countries **Combination**: 2 countries **Both**: 2 countries	E-Voting in **Belgium** and **Bulgaria** is controlled, in **France** both environments rule and in **Estonia** is uncontrolled.
"If e-voting is currently being used, is it available for all voters or only some groups of voters?" (E-Voting is used in question 1)	Total #Countries: 33 **Everyone can vote electronically**: 15 countries **Some groups can vote electronically**: 18 countries	In **Bulgaria** and **Estonia** everyone can vote. In **Belgium** only people in certain constituencies. In **France**, in certain constituencies and voters from abroad.
"If e-voting is NOT currently being used, what is the current status of e-voting in general?" (E-Voting is NOT used in question 1)	Total #Countries: 142 **E-Voting has never been used**: 103 countries (representing 72.5%) **Feasibility studies and/or tests are being carried out**: 26 countries **E-Voting had been used but has been abandoned**: 9 countries **Others status**: 3 countries E-Voting **has never been used in 13 EU countries**, other **6 countries are making tests and studies**, and **4 already used E-Voting and abandoned**.	Finland, Germany, Netherlands and Romania abandoned E-Voting. In Austria, Ireland, Italy, Lithuania, **Portugal** and Spain, feasibility studies and/or tests are being carried out.

Table 1 - Use of E-Voting worldwide (International IDEA survey "ICTs in Elections Database")

Summing up, it matters to explore in more detail the cases of some countries where all population can vote electronically. For purpose of this dissertation, one will focus in the Estonian case, exploring also Belgium (both European Union countries) and one of the BRICS – India.

Estonia:

Since 2002, Estonia introduced the national ID card. This card has a chip "with digital versions of the printed data, two 2048-bit RSA key pairs and certificates for the key pairs." Each pair of keys is used for different purposes. The first one is used for authentication and the certificate associated connects the "citizen's public key" to important personal details (name, national identification number and an email issued by the government). The second pair is used for the digital signature and the certificate associated connects the "citizen's public key to their name and national identification number". In order to make use of the chip, a card reader can be connected to a computer and a custom software.

Three PINs are issued with the card: one to enable authentication, other before generating a digital signature, and a third one used in last case if the card is locked due to the wrong enter of one of the two previous PINs.

Furthermore, there are other two forms of digital identification: “Digi-ID” and “Mobiil-ID”. Digi-ID is a card which contains less personal information than the national one, but still useful for authentication and digital signature. Mobiil-ID is similar to Digi-ID in terms of functionality, but “built into a mobile phone SIM card rather than a chip and PIN card”. Due so, citizens are able to authenticate and digital sign only using a mobile phone. According to a study developed by McKinsey Global Institute intituled *“Digital identification: A key to inclusive growth”* (White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M. & Sperling, O. (2019)), the adoption rate of Digital ID has achieved more than 70%.

After understanding the connection between public key and the Estonian ID card, it matters to analyse the Internet Voting system adopted in this country.

The process is based on the public key cryptography concept. “Voters encrypt their ballots with the public key of the election system, and then digitally sign them with their own private key.” The private key corresponds to the key for signature in the national ID card and, then, the electoral authority associates the voter with his/her public key. In this same book, the system operation is described across 28 steps.

The first step is downloading the platform (“voting client”). Once the voter concludes successfully the installation, he/she will use the ID or Digi-ID card to authenticate. Then, enters the first PIN into the card reader. After, the Voting Forward Service (VFS), determines the list of candidates, the voter’s region, and filter the list of all candidates per region. VFS forwards this information to the Client (platform). The fifth step starts on the voter’s side. He/she chooses a candidate, the voting client generates and encrypted ballot and asks the voter to sign. Hence, the second PIN is entered, the encrypted ballot is signed and sent to VFS. The role of the VFS is again to forward, but to the Vote Storage Server (VSS) this time. In turn, VSS contacts the Validity Confirmation Server (VCS) to certify if the ballot’s signature is valid. At this point, there are two case scenarios: either the signature is invalid and the VSS rejects it, informing the VFS that reaches out the client and the process ends, or the signature is valid and the process continues. In this scenario, VSS stores the encrypted ballot, the voter’s ID number and a ballot’s hash in Log1. This Log1 is stored in the Log server. VSS checks in its turn if the voter has actually voted, stores the hash of the previous ballot, plus the voter’s ID number and the revocation reason in Log2, deleting then the previous ballot. Finished this step, VSS sends to VFS a receipt so it can be received by the voting client. In order to avoid duplication of votes registered by the same citizen, a list of e-voters is printed from VSS for each polling station and the cancelation of the electronic vote occurs in case of duplication (any ballot is deleted). Moving further, VSS acts again and this time removes digital signatures associated to the ballots and stores them as a proof of who voted (hash for each vote in Log3), sorting the ballots by constituency. Then, the encrypted ballots with no signature associated are sent to the Vote Counting Application (VCA) via a physical media object (DVD) with all anonymous votes. The VCA is in its turn attached to a Hardware Security Module (HSM) which has the role to decrypt all the ballots. At the end, VCA sends the decrypted ballots to each constituency. At this point, a final check is done regarding the candidate chosen. If invalid, the vote is not counted and the hash of the ballot is stored in Log4. If valid, the candidate’s tally increases by one and the ballot is stored in Log5. In order to visually summarize all this process, the following flow schema designed by Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. & Halderman, J. (2014) is represented in figure 2.

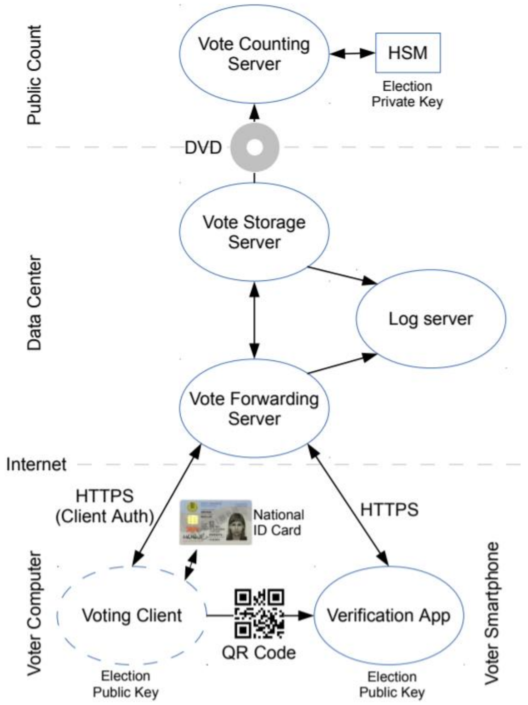


Figure 2 - Estonian I-Voting architecture (Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. & Halderman, J. (2014))

According to the same study developed by White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M. & Sperling, O. (2019), the authors concluded that “more than 30 percent of Estonians vote online, of whom 20 percent say they would not vote at a physical polling place”.

Summing up, Estonia was the first country to announce the electronic voting adoption in 2001 (Binder, N., Krimmer, R., Wenda, G. & Fischer, D. (2019)). This fact increases the responsibility of being the first country establishing a legal procedure in the adoption of E-Voting. In order to comply with legal requirements, the Riigikogu Election Act was introduced in June 2002 and “assumed legal effect on 18 July 2002”. Once this is a technology in continuous development, also the law needed to adapt and change. According so, with the Organization for Security and Co-operation in Europe (OSCE) mission report in 2011 presented a set of recommendations and, at that time, also the Electronic Voting Committee was created. All these events contributed in a way or another to the continuous update of the Act. According to this study, the last time the Act was changed was in 2016, with “legal effect on 1 January 2017”. Many of these changes will “step into force in 2021”. The legal procedures will be described in more detail in chapter 4.2 named “Case Identification”.

Belgium:

Currently in Belgium, two voting methods are in use, according to Cock, D. & Preneel, B. (2007): “electronic and paper-based voting systems”. It matters to understand that “Voting is compulsory and the participation is in practice almost absolute”. This country is complex in terms of governmental organization, for instance, the regionalization leaded to a “three-tiered federation”, where exist “federal, regional, and cultural/political community governments”. Due so, the organization of elections may vary between the three different regions of Flanders, Brussels and Wallonia. According to Smartmatic, the exclusive poll office election technology provider, it was announced in a case-study developed by them – “Belgian elections 2012 - 2019: Customized voting solution for a pioneer in electronic voting” - that the voting machines have been distributed across “185 municipalities in the Flanders region, the Capital Region of Brussels and the German-speaking community”. In the same paper of Cock, D. & Preneel, B. (2007), it is stated that the “Electronic voting was introduced with the federal elections in 1991” and also in June 2007 “44% of the voters have used the electronic system”. Some benefits are the availability of results quickly, the “reduction of costs” and “elimination of spoiled votes”. After, the authors explain the voting scheme of the Electronic Voting Machines.

Once the voter enters the polling station, he/she receives a “blank magnetic stripe card and goes to a voting booth”. There is a computer in the booth and “the voter uses a light pen to select first the party and subsequently the candidates”. Once the voter makes his/her choice, the vote will be recorded in the “magnetic strip of the card”. As in a paper-based system, the vote ballot goes to an urn. In this case, the urn is “driven by a computer”, where the magnetic strip of card is read and counts the vote. At the end, the results “are written to a floppy and brought by courier to the cantonal headquarters”. According to this study, some procedures are followed as tests to the machines (“test votes”) before and after each election, the voting machines and the urn computers have also to comply with some requirements to start up, the voter can check his/her final choice in a different voting booth and, if there’s any failure in the urn computer, all votes can be recounted in a different machine. However, since 2007, some changes have occurred. According to Smartmatic, voters can correct and confirm their choices in an easier way in 2019, the floppies are no longer used, USD pen drives are used, among others innovations. All the equipment required includes “Voting Machines”, “Smart Cards”, (used to access the voting machine and automatically deactivated after the voting moment occurs and when it is delivered to the President Machine), “President Machines” (responsible to “activate smart cards that voters use to access the voting machines; to electronically register and store each vote; to count all votes and store the results; and to generate a polling station report”), “Smart card reader unit” (already two generations, one connected externally via USD, the second one is fully integrated in the President Machine) and, finally, the “e-Urn (electronic ballot box)”, connecting “to the PM via a combined power/USB cable”.

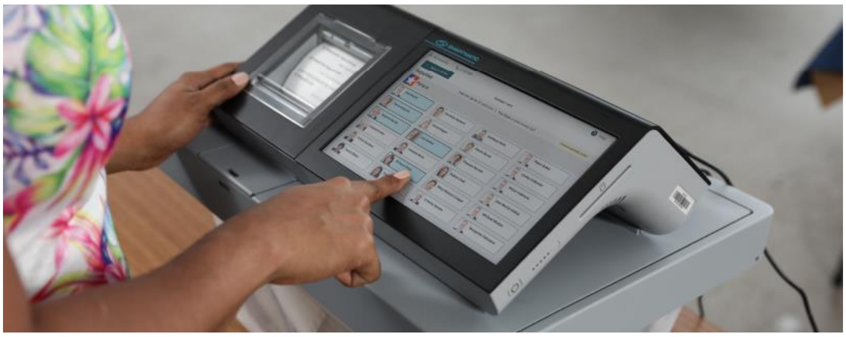


Figure 3 - Voting Machine in during Belgium elections (Smartmatic (2020))

India:

In this emerging economy, Electronic Voting Machine became highly popular after an experiment that took place in three Indian states in 1998, leading to its official adoption in 2004 at a national level. Today, India is one of the few countries where it is possible to the Indian population to cast their vote through an electronic device (Chauhan, S., Jaiswal, M & Kar, A. (2018)). However, since 1989 the law was amended by Parliament in order to spread the use of EVMs around the nation, taking effect in 1998.

According to the study developed by Avgerou, C., Masiero, S. & Poulymenakou, A. (2019), The Electronic Voting Machine in India is constituted by two parts: the ballot and a control unit, connected by a cable. Before the election day, "each key on the ballot unit is marked with the name of a candidate and the symbol of their party". Technically, the design of Indian EVMs is characterized by the software being provided as firmware, "meaning that it is encoded in the EVM's EPROM (erasable programmable read-only memory)". Basically, these machines are used for the voting itself, as well as for the counting. The votes are counted and stored in the machine, moving later forward to counting centres where the votes are "aggregated and tabulated". During the election act, all the process occurs under a controlled environment. Around four officers intervein. The first one checks the "voter's card against the printout register for the booth". After, a second officer "crosses out the voter's name in the printout, asks them to sign the register against their name, and marks their right index finger with an impermeable ink line". A third officer unlocks the machine, following the moment of voting, where the voter presses the button corresponding to the candidate of his/her choice and, in the end, "a sound signal is heard confirming that vote has happened". When the citizen leaves the booth, a fourth officer supervises. In the end, the same officer who unlocks the machine, also locks it, in order to prevent more votes. The machines are transported to a room where a manually aggregation of the outputs of all machines is done in order to determine the final results.

In the paper written by (Chauhan, S., Jaiswal, M & Kar, A. (2018)), a Unified Theory of Acceptance and Use of Technology (UTAUT) model was used to validate a set of hypotheses that the authors intended to test in order to conclude about the main variables that affect the behavioural intention to use an Electronic Voting Machine. In the data collection process, the survey was conducted in the four main metropolitan cities of India, being these results related to an urban population. Despite of the major efforts to gather data from a larger sample of the population, "a total of 638 filled questionnaires were gathered out of which 356 were completely filled".

The variables considered were "Perceived Security", dealing with how citizens perceive the "accuracy and confidentiality of EVMs"; "Trust in Technology", measuring the people's belief in the technology's capability used to design the EVMs (firmware as already indicated before); "Performance Expectancy", measuring at which extent voters consider EVMs useful; "Effort Expectancy", related to the level of complexity and effort amount voters need to apply in the moment of voting, and; "Social Influence", if the important relatives "believe he or she should cast the vote using EVMs". As main conclusions, after the modelling process takes place, "Perceived Security", "Trust in Technology", "Performance Expectancy" and "Social Influence" are the determinants of the voter's intention to use EVMs. In terms of age and gender factors, the authors reached relevant conclusions. First of all, the sample was divided in two groups: the older (citizens with age over 35 years old) and younger groups (citizens with age equal or below 35 years old). Then, for the older stratum of the sample, all measures in the model are significant, while for the youngers, “Effort Expectancy” is not significant. Taking into consideration the culture and literacy rate of the Indian population, female and older stratums are the ones who consider “user-friendliness of EVMs is a major factor of consideration”. “Social Influence” is considered more relevant by men than by women.

2.2.4. Issues & Challenges

In this chapter one introduces the main challenges that the Electronic Voting (both EVMs and Internet Voting) face nowadays.

According to a report published by the European University Institute, Robert Schuman Centre for Advanced Studies, European Union Democracy Observatory – EUDO, Trechsel, A. (2016), when the subject is challenges associated with the E-Voting, one may refer “legal considerations”, “political considerations”, “technological and security challenges” (both human-related and tech-related) and “social challenges”. Below, one can see the considerations and challenges listed by topic:

Legal Considerations:

- Principal of Universal Suffrage (“one voter, one vote”), states that “everyone is entitled to the right to vote”, and it “could only be harmed by the introduction of Internet voting as the only modality of voting”. The “Digital Divide” is introduced here as the critical aspect: people who do not have access to the Internet would not be able to vote;
- Secret voting: ensure that the processes of counting the votes and checking who voted may be independent, ensuring “privacy and security” at its maximum level;
- “Adjustment of existing legal norms”: the implementation of I-Voting needs to comply with all legal requirements. Then, the implementation needs to be “defined, organised and put into operation” by law. It may exist a legal basis for the adoption of this mechanism, so it can be adopted in more member states of the European Union.

Political Considerations:

- The adoption procedure of I-Voting may be “transparent, participatory, and involve all the relevant political actors and stakeholders”, so its implementation can be consensual.
- A strong political consensus about the adoption of this E-Voting mechanism will motivate and increase confidence of citizens in the behavioural intention to use Internet Voting.

- It is required political neutrality about the I-Voting adoption once it may affect directly the results of future elections.

Technological and security challenges – “Human-related technological risks”:

- Citizens with lack of technical competencies to deal with remote I-Voting;
- Electoral officials missing technical skills to be able to control the I-Voting process in an effective way;
- Citizens’ assurance regarding secrecy and privacy of their votes;
- “Lack of transparency when voters cannot be sure whether their votes are correctly counted and stored”;
- Possibility of intimidation or any other kind of enforcement against the voter’s will while casting his/her vote remotely;
- If I-Voting becomes the only way of voting, a significant portion of the population may not be capable to vote and feel discrimination.

Technological and security challenges – “Tech-related technological risks”:

- “Possibility of system attack or breakdown, or connection failure”;
- Correct identification of the voter complexity;
- “Provision of the preventive measures against multiple voting” and “transparency of tabulation”;
- Voter’s personal computer can have virus and affect the system;
- Digital divide and the risk that the electoral population capable of using I-Voting may not represent certainly the different socio-demographic groups (including the ones who are not capable to vote remotely).

Social challenges:

- “Social differences regarding who has a personal computer and internet at home” and “who is sufficiently technologically literate to be able to interact with an online voting platform”. Age, income level and literacy level are key components.

In Beroggi, G. (2014), the question of voter’s personal computer being infected with malware is solved due to “the cryptographic protocol for transmitting encrypted data from the voter’s computer to the electronic ballot is tightly linked to a separate device, which provides sufficient security". However, the trust issue is prevalent. I-Voting may be seen by voters as a secure and trusted option and the belief that the ones who work directly with the system may manipulate the process exists.

In a paper written by Abba, A., Awad, M., Al-Qudah, Z & Jallad, A. (2017), intituled as "Security Analysis of Current Voting Systems", the authors refer the vulnerabilities associated to the electronic voting systems and incorporate them among seven categories.

"Malware Insertion" – someone accesses the machines before entering the polling station, modify or insert the software in order to create a malfunctioning in the machine. Then, the machine could lose, add, mis-record and skip records.

"Wireless and Other Remote-Control Attacks" – Can happen before or in the election day itself. Machines that have wireless components can be hacked ("program the machine to turn on or off, insert a malware, or install something malicious that could attempt to read the information recorded and stored by the voting machines").

"Denial-of-Service Attacks (DoS)" – This attack prevents voters to cast their vote successfully, once the communications between a client platform and a server can be disrupted.

"Attacks on Counting Servers" – Occurs after the closure of the polls, when all votes have been already recorded. Hackers would interfere in the communications between the counting server and the server, making changes to the votes count and "information used to tally the sums of the entire votes".

"Attacks on Ballots or Verified Voter Paper Trail (VVPT)" – "ballot papers and the verified voter paper trail can get damaged when they are being transported to the counting centers or even at the polling unit" and "ballot and VVPT's could even be altered or wholly damaged before they are being audited or recounted at the counting centers".

"Shutting Off Voting Machine Features Meant to Help Voters" – Hack attacks in the features that guide the voters to certify that their votes' cast succeeded may lead to missing recorded votes.

"Social Engineering" - Attacks that entangle misleading individuals into compromising their safety. Phishing emails are a big example of this.

2.3. BLOCKCHAIN

2.3.1. Concepts

Blockchain is the crucial technology that matters for this study and the focus for further developments related to its application in the voting system. Hence, it is required to understand well its concept.

According to the white paper “BlockChain Technology: Beyond Bitcoin” written by Crosby, M., Nachiappan, Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016), Blockchain is described as “a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties.” Furthermore, this technology “contains a certain and verifiable record of every single transaction ever made.”

In other work developed by Osgood, R. (2016), the concept uses the term blocks to the “ever-growing ledger of records (usually transactions)”. Right after, the author describes how this database processes the transactions. Blockchain is “managed by a network of nodes”, being these nodes computers connected all to the network that works and validates all the entries and exits (transactions) under “a set of rules”. Once a transaction is validated by a node, it is added to a block, and in its turn, added to the blockchain. Hence, valid transactions are added to a block, “grouped together and added to the database”. Blocks are added one after the other. Taking into account that this technology is “tamper-proof and secure”, the author describes the algorithm functioning based on the hash function, used to mark every block that enters in the system. For instance, the second block that joins will be “marked with a hash function that contains part of the first block’s hash function”, and so on. Any alteration in the hash function of a block that is about to enter in the system, this anomaly is automatically recognized by the remaining blocks and the update is rejected. Making use of the author’s words applied to the context of this dissertation, “the transactions stored in the database” are votes.

In order to understand better the components that involve this technology, in Ayed, A. (2017), “A Conceptual Secure Blockchain- Based Electronic Voting System”, four fields are mentioned: “Block size”, “Block header” (“encrypted almost unique Hash”), “Transaction Counter” (“the number of transactions that follow”), and “Transaction” (which is saved in the block). According to Ayed, A. (2017), a list of records corresponds to blocks, each one containing transactions. Transactions “can hold different types of data”, and a block “contains a timestamp and a cryptographic link to the previous block.” Hence, security can be implemented through “cryptography” and “hash functions”, examples of “security functions”. In this paper, it is specified two types of Blockchain, depending on the security status: “Open blockchains” and “Closed blockchains”. The first one, as the name indicates, it is opened to everyone who wants to join and contribute to the development of further solutions. Due so, a security model is required in order to guarantee the transactions security and “consensus mechanism”. The closed ones “rely on traditional security mechanisms” in order to guarantee no unexpected change and unwanted access. Examples of open blockchains are “Bitcoin and Ethereum”.

In a more recent study, Zhang, R., Xue, R., & Liu, L. (2019), the authors refer a third type of Blockchain. Starting by defining this technology as “a secure ledger” in which is responsible to organize the growing list of transaction records into a hierarchically expanding chain of blocks”. Each one of these blocks is “guarded by cryptography techniques to enforce strong integrity of its transaction records”. Furthermore, they mention that each block to be added to the chain needs to successfully comply with the “decentralized consensus procedure”. In this paper, the authors defend that this consensus is imposed by the network controlling three fundamental steps: the addition of blocks to the chain, “the read protocol for secure verification of the block chain” and the consistency assurance of the data in each transaction across different nodes in the chain. In this paper, another type of Blockchain is presented apart from the “Public Blockchain”, meaning that is open to anyone ("to read, send, or receive transactions" and participate in the consensus procedure) and, also, apart from the "Private Blockchain" (only one agent can write but everyone or a group of participants can read). This is the "Consortium Blockchain", in which it is open to every participant in the network to read but only a subset has written permissions and can participate in the consensus procedure. Summing up, "speed of consensus" and "trust authority" are what differ between these three types. However, all of them meet mutual properties: "decentralized peer to peer networks for transactions", digital signature per transaction and "each peer node" keeps a full copy of the Blockchain, and, finally, all nodes maintain the consensus (consistency) across the network, so when a new block is created, it is added to every node.

2.3.2. Architecture

In the paper written by Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018), the Blockchain architecture is introduced. The algorithm itself is based on a continuous "sequence of blocks", in which a block contains a "parent block hash" in the "block header". A block that contains no parent block hash is called the "genesis block", meaning, the first block of the chain. Then, a block is not only constituted by a block header, but also a "block body". The block header, apart from the parent block hash, includes also other five features: "Block version" ("block validation rules" that matters to follow); "Merkle tree root hash" ("hash value of all transactions in the block"); "Timestamp" ("current time as seconds"); "nBits" ("target threshold of a valid block hash"); "Nonce" ("4-byte field" increasing for "every hash calculation"); and, finally, "Parent block hash" ("256-bit hash value that points to the previous block").

Regarding the block body, it is composed by a "Transaction counter" and transactions. In figure 4, one can visualize this structure. In this paper, "Digital Signature" is introduced as the way to validate the transactions authentication. This mechanism is composed by two phases: "signing phase" and "verification phase". Also, two types of keys are used in the process: the "private key", which is used by one user to encrypt the data (to sign one transaction), and after, in the validation phase, the "public key" of the first user is used by the second user to validate the message received. Hence, he/she will be able to verify if the data was tempered or not. This concept will be further investigated along this section.

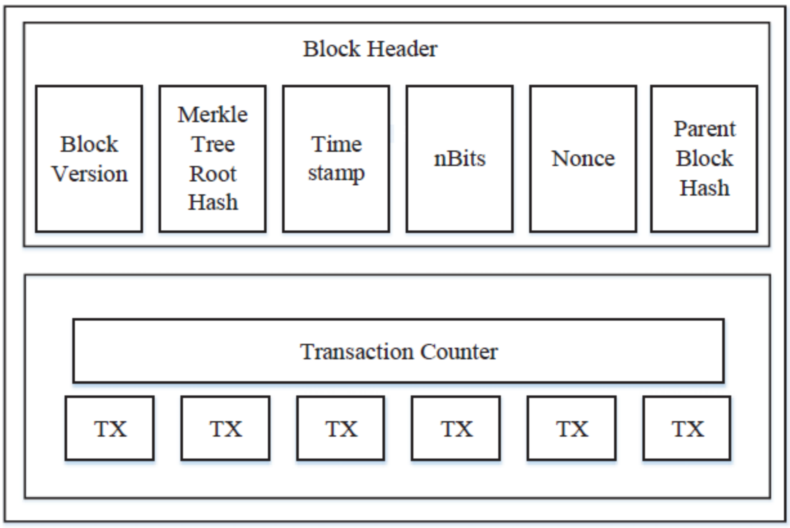


Figure 4 - Block's structure (Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018))

In a work developed by Kolb, J., Abdelbaky, M., Katz, R., & Culler, D. (2020), the authors focus on the basic elements that are adopted across blockchain systems, exemplifying with the Bitcoin case. They introduce the maintenance of a "ledger" by Blockchain, known as the most fundamental capability. "Ledger" is defined as "an append-only log for storing data". Basically, new items (or transactions) are "batched together into a block". Then, only blocks are appended to the ledger, one at a time. In the example of Bitcoin, this creation and addition of blocks to the ledger is done with an interval of 10 minutes. This period of time is one important factor that ensures the security of the Blockchain system, called the "proof of work algorithm" that one will explain later on. Thus, each block contains "an ordered list of ledger entries" and the ledger is formed in its turn by a sequence of blocks. This component is very important in the Bitcoin's Blockchain. For instance, each ledger keeps the record of Bitcoin's ownership, represented by "virtual tokens". They are distributed "among accounts", being each account "uniquely identified by a public key". Every transaction of Bitcoins that occurs within this system is "from one public key to another". As already mentioned above, regarding the study from Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018), in this paper the authors also confirm that each transaction is signed "by the sender's private key", preventing falsification. This is the first intervention of cryptography, where the sender encrypts the data. In this paper, the "parent block hash" is also mentioned and the involved process is explained. The authors call to this block header's component a "cryptographic hash", containing information encrypted regarding the previous block in the chain. Summing up, the cryptographic hash of block 1 is included in block 2. In its turn, the cryptographic hash of block 2 (containing its hash of block 1) is added in block 3. This sequence of integrating the hash of the precedent block into the block header of the following one continues, giving to the chain of blocks a "definitive order and makes their contents immutable". In the white-paper written by Nakamoto, S. (2009), this transactions' sequence and hash function mechanism was explained based on Bitcoin. In the figure 5 one can see how the terms private key, public key, hash and transaction interact between each other.

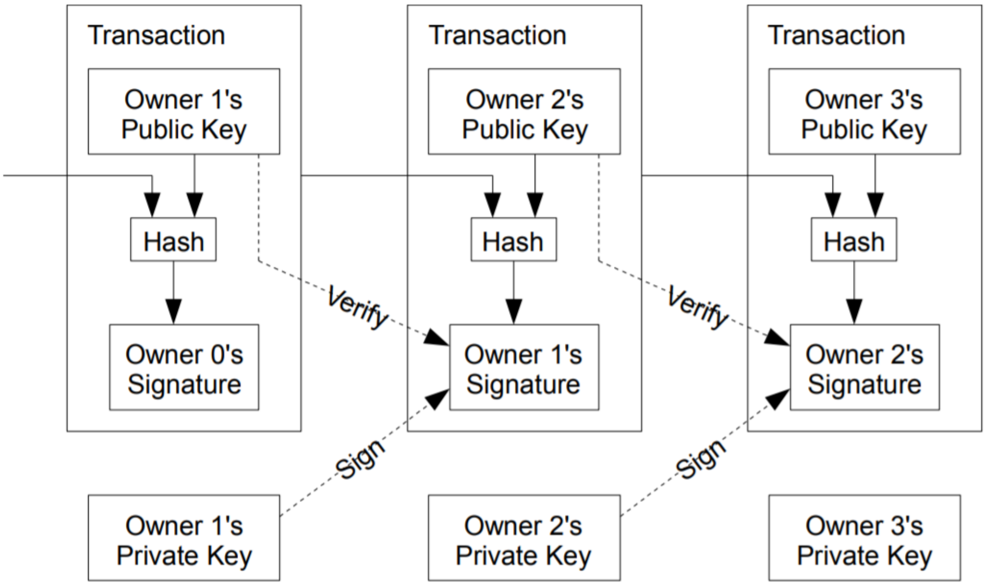


Figure 5 - Signing and Verification of signatures through the use of keys (Nakamoto, S. (2009))

In this mentioned paper, the timestamp component is also described. The "Timestamp server" proves that the data existed before get into the hash function. It works by "taking a hash of a block of items to be timestamped". Hence, each timestamp includes the previous timestamp in its hash. This process is followed from block to block, where each block presents the timestamp that reinforces the previous ones. In this sense, one may describe the "proof of work" concept as already mentioned above.

2.3.3. Areas of Application

In order to understand more concretely how Blockchain is already implemented in markets and governmental institutions, in this section one will identify the main areas of application already in use and the potential ones for further developments in the near future. According to Xu. X, Weber, I. & Staples, M. (2019), in the book "Architecture for Blockchain Applications", the authors mention that "financial transactions" are the first use case but not unique. Nowadays, several private and governmental institutions are investigating the use of blockchain technology in many areas such as "supply chain, electronic health records, voting, energy supply, ownership management, and protecting critical civil infrastructure" (it will be exemplified the different cases ahead in this section).

In short, the Blockchain benefits are divided according to the development level of a country. The authors defend that in countries less developed, the trust in third-party organizations that work as intermediaries is little. "Immutability" ("not changing prior records on the ledger") and "Non-repudiation" ("not being able to disown prior actions on the ledger") are the main benefits of adopting Blockchain and get rid of intermediary agents for these countries. In more advanced countries, the benefits are others: “faster business model innovation”, “reducing the cost of establishing business relationships” and “reducing the cost or risk of transactions”, once the trust in third-party organizations is not so questionable as in undeveloped countries.

Given the different benefits associated with the adoption of Blockchain among different nations around the world, it is important to understand exactly which platforms are in use these days. The first application worth noting is Bitcoin.

Bitcoin:

This buzzword does not only mean a decentralized cryptocurrency but mainly the begin of a technological revolution in the financial markets extending to many other organizations.

In the study presented by Tomov, Y. (2019), entitled as *“Bitcoin: Evolution of Blockchain Technology”,* the author starts by writing about the state-of-the-art of Blockchain, where all evolutionary phases are described until the year 2008 when, “a person or a group of people going under the pseudonym of Satoshi Nakamoto”, presented an article that became rapidly famous due to the working model.

Departing from the year of 1982, David Chaum developed an “untraceable payment system based on blind signatures”. He is considered one of the founders of electronic payments. However, the blind signatures, according to David’s algorithm, preserves the anonymity of transactions that exist between individuals in the system to the bank (the third-party involved and the one that validates the transactions, “unlike in blockchain technologies”). Later, in 1991, despite of not being described in Tomov’s article, it is important to mention the Haber, S. & Stornetta, W. (1991) paper published under the name “How to Time-Stamp a Digital Document”. In this study, the authors depart from the problem “how can one certify when a document was created or last modified?”. In this sense, Time-stamping method is adopted and may comply with two criteria: “time-stamp the actual bits of the document” and “the date and time of the time-stamp must not be forgeable”, meaning they may not be counterfeit. Timestamping became a key feature for the constitution of a block header. In 1997, Adam Black focused his study on a solution to email spam. To do so, hash function and the Proof of Work concept were used. As already studied before, the Proof of Work focus on the validation of the correct hash result and the search of the nonce to reach the appropriate hash target. Then, in the function "VALUE" used by Adam Black, the validation of the hash result is also performed. This function corresponds to the Proof of Work algorithm. Thus, the “Hashcash” method as a solution to the problem of email spam, uses the PoW algorithm which was "later used in many blockchain models". The validation is not performed by any third-party (bank), making "hashcash decentralized”. In 1998, other two important studies, in parallel, came to public and became relevant for the build of Bitcoin. Wei Dai proposed an anonymous distributed cash system named “b money”. The solve of computational problems in order to generate money, the use of public keys and the “copy of the database” that each participant keeps are major common features to Bitcoin. In parallel, Nick Szabo “proposed the Bit Gold model” also in 1998. Despite of applying in its model key features already developed by other computational researchers, as the PoW and Timestamp, the main add-in is “the last created string of bit gold provides the challenge bits for the next-created string”. As already studied before in this dissertation, the feature of a block containing the hash of the previous one in the chain may find its origin in the Bit Gold model.

Hereupon, Bitcoin construction adopted the strengths of these models presented and considered also the main weaknesses and limitations, in order to implement a solid product in terms of process and security. As defined by the author, Bitcoin is "a decentralized peer-to-peer network". The transactions grouped into blocks, added into the system through the mining process, the block's constitution, all these properties described in the Blockchain's architecture chapter are part of Bitcoin. Yavor Tomov mentions the two main objectives of Bitcoin's creation: "create a digital currency" and "to perform financial transactions". Revisiting *"Bitcoin: A Peer-to-Peer Electronic Cash System"* the paper published by Satoshi Nakamoto in 2008, where the Bitcoin's system was introduced, the author starts by mentioning the financial institutions' role as intermediaries for the execution of electronic payments. Banks, for instance, are entitled the "trusted third parties" in the mediation of financial transactions. However, once there are not completely irreversible transactions in this system, they "cannot avoid mediating disputes". Fraud is considered "unavoidable", and only a system which guarantees irreversible transactions may solve this problem. The author defends that the "electronic payment system" may be based on "cryptographic proof" and not "trust" in a third-party.

Following the book edited by Olleros, F., & Zhegu, M. (2016), entitled *Research Handbook on Digital Transformations,* one decided to use the applications examples provided by the authors, exploring in more detail six out of the nine cases presented in the book. To do so, the information was organized in one table for each application.

Sidechain Technology and Smart Contracts			
Definition	**Description**	**Examples**	**Use Cases**
"A sidechain is a secondary blockchain connected to the main blockchain with a two-way peg. Sidechains may have their own consensus protocols, which could be completely different from the mainchain's protocol".	There are a primary blockchain (parent blockchain or mainchain) and a sidechain (secondary). The primary blockchain "operates a cryptocurrency called MainCoin" and "cannot execute non-trivial smart contracts". The sidechain "operates its own cryptocurrency named SideCoin", "has the capability of executing non-trivial smart contracts" and "offers significantly higher transaction rate (i.e. higher transactions per second) than the mainchain".	- Loom; - POA Network; - Liquid; - RootStock (RSK).	**Loom** (Digital Social Interaction (e.g. Delegate call); **Game Development** (e.g. Relentless)) **POA Network** (Swarm City, a decentralized commerce platform; Sentinel Chain; Virtue Poker; Colu Network) **Liquid** (International Exchange) / Advantage: Liquid, introduces improved security and privacy, with lower latency than the Bitcoin network. **RSK** (Retail Payment Systems; Supply Chain Traceability; Digital Identity)

Table 2 - Sidechain Technology and Smart Contracts (Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K. K. R. (2019))

Ethereum			
Definition	**Description**	**Examples**	**Use Cases**
"Ethereum is an open blockchain platform that allows anyone to build and use decentralized applications that run on blockchain technology. Financial interactions or exchanges in the different industry could be carried out automatically and accurately using code running on Ethereum."	Ethereum requires a Virtual Machine (EVM) that executes the "complex algorithmic codes written in friendly programming languages" for each and every node, maintaining the consensus decentralized across the blockchain. This "confirms the extreme level of fault tolerance". In terms of process mining, the algorithm used is "Ethhash". It consists on "finding a nonce input to the algorithm so that the result is below a certain difficulty threshold". On average, it takes 15 seconds to mine a block and the winner miner of a certain block receives 5.0 Ethers.	Many Dapps (decentralized applications) are built on Ethereum, grouped in different categories (at least sixteen, namely Finance, Exchanges, Wallet, Gambling, Marketplaces, Governance, among others)	There are eight principal groups according to Dannen, C. (2017): - **The Internet of Ethereum Things** - **Retail and E-Commerce** - **Community and Government Financing** - **Human and Organizational Behavior** - **Financial and Insurance Applications** - **Inventory and Accounting Systems** - **Software Development** - **Gaming, Gambling, and Investing**

Table 3 - Ethereum (TIFAC-CORE, S.P. (2018); Dannen, C. (2017); State of the DApps (2021))

Gridcoin		
Definition	**Description**	**Sources**
Gridcoin is defined as an "altcoin", meaning, a cryptocurrency build as an alternative to Bitcoin. It is based on "peer-to-peer Internet-based crypto-currency" aiming to reduce the environmental impact caused by Bitcoin (a solution to the "electricity usage problem"), being "more energy efficient".	Currently, more scientific contributions are needed. Due so, users are rewarded when contribute with scientific projects published on the "BOINC project platform", the Berkeley Open Infrastructure for Network Computing.	Grothe, M., Niemann, T., Somorovsky, J., & Schwenk, J. (2017)

Table 4 - Gridcoin (Grothe, M., Niemann, T., Somorovsky, J., & Schwenk, J. (2017); Chohan, U. (2018))

Ripple Labs		
Definition	**Description**	**Use Cases**
Ripple is a tech company in San Francisco, which decided to adopt the potential of Blockchain to revolutionize the financial transactions system. XRP is the cryptocurrency created, allowing "currencies to be converted to XRP back and forth easily". Thus, Ripple system is a big challenge to the current SWIFT system, by enabling "very near to a real-time system" and offering lower cost.	The key components of Ripple System are "distributed ledger" and "cryptocurrency". "Transaction data" and "actual fund" to be transferred are carried out at the same time. In SWIFT words, "messaging flow" and "fund flow" are synchronized. There is more transparency in some information as the "liquidity status" and exchange rates for each member bank of this decentralized peer-to-peer network, comparing to the SWIFT system.	**Popular among banks**. According to Ripple's website, banks as "American Express", "Santander", "Interbank", Personal Banking "PNC", are some of the customers that already joint the Ripple network.

Table 5 - Ripple Labs (Qiu, T., Zhang, R., & Gao, Y. (2019); Retrieved from https://ripple.com/)

Blockchain-Based Digital Identity Providers		
Definition	**Description**	**Use Cases**
The need to share personal details and the security risks associated lead individuals to think about the elimination of the trusted third party and "wait lines for authentication, authorization, and attestation". Hence, individuals would be able to decide which identify details they want to share or not and with whom. Then, it emerges the Self-Sovereign Identity concept, which is defined as the "lifetime portable digital identity that does not depend on any central authority and can never be taken away".	Understanding what means having full control over its own identity implies the identification of Self-Sovereign Identity properties (ten as indicated in Stokkink, Q., & Pouwelse, J. (2018)): "Existence", "Control", "Access", "Transparency", "Persistence", "Portability", "Interoperability", "Consent", "Minimalization" and "Protection". By complying with all these properties, the system has the necessary requirements to implement the self-sovereign identity concept. The architecture of the Self-Sovereign Identity is based on four agents and their relationships mainly, where the user is in the middle. It is based on the distributed ledger of the Blockchain. Then, the full process goes from Identification, to Authentication (use of public/private keys and cryptography), Verifiable claims and, Storage of the user's data (public and private).	**Remote Interaction,** **Automatic Procurement** (offers a widen umbrella of applications for E-Procurement using "Smart Contracts", "Purchase Order (PO)/Supply Chain Visibility (SCV)"), **Authentication, Authorization, and Trust of IIoT User/Devices,** **Part life-cycle support** (industrial machines, management of their components, easier to track its brand and further manufacturing features), **Big Data and Artificial Intelligence** (need for some companies which produce devices to store the huge amount of data generated in a decentralized blockchain-based storage network, and the SSI is used)

Table 6 - Blockchain-Based Digital Identity Providers (Aydar, M., & Ayvaz, S. (2019); Stokkink, Q., & Pouwelse, J. (2018); Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019); Tobin, A. and Reed, D. (2018); Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018)

Social Inclusion in the Developing World		
Definition	**Description**	**Use Cases**
Blockchain features reveal a big opportunity of problem's solving for "people living in poverty" especially in the South economies less developed. Economic, social and political problems are an opportunity for Blockchain's algorithm to "promote transparency, build trust and reputation, and enhance efficiency in transactions".	The main purposes of using Blockchain as a mechanism to promote Social Inclusion in Development Countries are: - "Overtaking institutional weakness through property registry, digital documents, and budget-tracking mechanism"; - "Empowering people and reducing power asymmetry" - "Increasing financial inclusion" (able to create a bank account, once many citizens cannot prove who they are – lack any proof of identity).	**E-Governance** (working on services that require personal interactions and individual identification) **Land titles** ("assignation of private property", e.g. in Ghana) **Identity services** (numerous startups are working on this, e.g. Humaniq's Ethereum blockchain-based app creates user profiles based on biometric data such as facial and voice recognition algorithms) **Anti-Corruption** (increase government transparency – "Blockchain Trust Accelerator project") **Virtual Governments** (e.g. Bitnation) **Electoral Processes** (algorithm applied in order to prevent "frauds and "identity theft") **Aid and Development** (e.g. UN World Food Program's pilot blockchain application to give financial support in Jordan) **Remittances** (e.g. UN Development Programme's remittance pilot project in Serbia and UNICEF's application to reduce child poverty)

Table 7 - Social Inclusion in the Developing World (Mavilia, R., & Pisani, R. (2019); Kshetri, N. (2017))

Some other use cases exist among the following applications: Blockchain Technology for the Banking/Finance Industry; Enhancing the Transparency of Supply/Global Commodity Chains, and, more important for the purpose of this dissertation; Blockchain-Based Voting Systems (one will explore further in the chapter 2.3.5. E-Voting and Blockchain).

2.3.4. Issues and Limitations

The implementation of Blockchain in the most diverse areas, as mentioned in the previous chapter, faces both technical and nontechnical limitations in its construction and adoption. The existent hurdle to commercialize the Blockchain's use is due to these obstacles mainly. According to Drescher, D. (2017), in the book entitled "Blockchain Basics: A Non-Technical Introduction in 25 Steps", the author synthetizes the limitations associated to this algorithm. Below, one presents the set of limitations and a brief description of each one.

Technical limitations:

- “Lack of privacy”:

The Blockchain's level of transparency is not only an advantage, but a disadvantage by itself. On one hand, without transparency, Blockchain cannot "fulfil its duty" as a decentralized network, "purely distributed peer-to-peer ledger", where new transactions are verified avoiding problems of "double-spending" nature and fraud. On the other hand, everyone having access to all transaction details (goods and amount transferred, the accounts involved in each transaction, and the exact time they occur) is a big limitation for the implementation of this algorithm in applications that require a higher level of privacy.

- “The security model”:

The Blockchain's security is strong, using the best cryptographic method known ("asymmetric cryptography"). Identification, authentication and authorization are supported by this method. The use of keys satisfies both the transparency needed and the privacy of each account's owner. The public key corresponds to an account number, visible to anyone in the network, and the corresponding private key, which only the owner possesses it and "can access the property" associated. However, even if the "plan A" is strong, it is not impossible to fail, and there is no "plan B". This inexistence of another privacy method, in case someone loses the private key to someone else, for the most diverse reasons, breaks the "security for that individual account" immediately. The Blockchain's security limitation is due to the absence of a plan B.

- “Limited scalability”:

The capacity of the Blockchain to become larger, by adding to the chain new transactions grouped in blocks, is considered limited. The mining process already presented in the chapter 2.3.2. Architecture prevents attempts that may take place in the network but, as a trade-off, the "processing speed" is reduced and, consequently, the "scalability" is limited. Implementing this algorithm in applications that require "high processing speed, high scalability, and high throughput" turns out a big limitation.

- “High costs”:

To guarantee a high level of security may be expensive. Complicated computational problems are necessary and have higher costs associated. These costs are measured in "computational cycles, physical time, electrical energy, and money". Hence, "the whole blockchain incurs costs".

- “Hidden centrality”:

By solving mathematical computational problems, members of the network can add new blocks to the chain and receive rewards for "contributing to the integrity of the system". However, these members can be divided in two groups: the ones having the "financial resources" to "invest in specialist hardware" and the others which do not have financial capabilities to invest in specialist hardware. This financial discrepancy and consequent division of members causes one "very small group" to detain the computational power, solve almost all problems and receive the majority of rewards. On the contrary, the contribution of the members with worse hardware capability, become unprofitable to the system and, consequently, are discouraged from "contributing computational resources" to the chain. It is notorious that the decentralization is questionable. The system is still decentralized technically, but the integrity is "maintained by only a small number of entities".

- “Lack of flexibility”:

Blockchain is complex in its construction, with well-established procedures (e.g., cryptographic procedures that need to be valid for the "lifetime of the blockchain"). Another important limitation of the Blockchain algorithm is the lack of flexibility in adjusting the protocol and fix bugs that may occur. This immutability avoids people to develop further on the blockchain.

- “Critical Size”:

The size of the peer-to-peer systems is critical to determine the "robustness against manipulations" and how much the "history of transaction data" is trustworthy. In order to a Blockchain system succeed in these two characteristics it is required a majority of honest nodes, so the system can be "resistant to attackers with a lot of computational power". Summing up, the smaller is the system with limited computational power, the robustness is less. Hence, the attack risk is higher.

Nontechnical limitations:

- “Lack of Legal Acceptance”:

One of the major limitations for the adoption of Blockchain in different countries is related to the legal framework and implications. The possibility that users of the peer-to-peer system have to "manage and transfer ownership" collectively leads to debates regarding the "safety, security, and sophistication" of Blockchain.

In order to explore in depth some of the tensions that have been arising due to Blockchain’s features, different from the “centralized approaches” that are currently in law, one decided to clarify the relationship between this technology and the European law described in the thematic report “Legal and regulatory framework of blockchains and smart contracts”, prepared by European Union Blockchain Observatory & Forum. written by Lyons, T., Courcelas, L., & Timsit, K. (2019). In this report, it is explained legal issues associated to the algorithm. As long as it is a decentralized system and is difficult to determine who is the data and network’s owner, hence, to whom the responsibility should be addressed, there are some “hurdles to overcome on the path towards the reconciliation of blockchain and the law”. In order to illustrate six critical legal issues, the following table resumes the main topics to be considered.

Legal value of blockchain as registries	There are many prerequisites that Blockchain needs to comply with in order to be legally accepted. However, among them, one can emphasize the "legal recognition of blockchain based signatures", "timestamps", "validations" and "documents". eIDAS is a term known in Europe for handling the "electronic IDentification, Authentication and Trust Services regulation". In this sense, the issue comes with eSignatures and eSeals, in other words, the signature of a "legal entity as opposed to a natural person". Despite of Blockchains meet the technical criteria, legally their transactions "do not have legal authority by themselves", according to eIDAS.
Territoriality	According to the current European legislation, in case of fraud or practice of any other illegal practice punished at law level, the responsibility is assigned based on the location where the act occurred. In the case of a distributed network as it is Blockchain, this legal responsibility is not clear where and whom to be assigned. Hence, this technology challenges the EU perspective. It is required to revisit the "European private international law". As informed in the Rome II Regulation, the country where the damage occurs is relevant: "the law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs", as stated in the Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). Also, in the Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), the following is also written "in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur".
Enforceability	Another important factor to enforce the law is the identification of the individual(s) identity that break the law. Blockchain supports the "pseudonymity" and "full anonymity" of members. In some circumstances, when both roles are used with criminal purposes, they can lead to the creation of "lawless zones". Governments try to circumvent these issues and adopt techniques to discourage the anonymization in blockchain networks through the Anti-Money Laundering (AML) rules. Another possible measure to be implemented is the use of identification tools, controlled by courts or private sector, in order to enforce the law and responsibility over the individuals behaving illegally in the blockchain space.

Liability	Across law systems, the types of liability imposed on individuals who fails to comply with the obligations and prohibitions, are diverse: "criminal", "administrative", "contractual" and "tort" liabilities. Other specific regulations are more recent and relevant, as it is the case of GDPR (General Data Protection Regulation). In the Blockchain example, it becomes harder to understand who may be the responsible in case of failure in the accomplishment of obligations. Questions regarding the role of Software developers exist: once they are the ones who write the code, understand the features of the algorithm, it matters to determine if they should be the responsible for not creating mechanisms that prevent illegal activities and creating an "open-source code that supports anonymity". According to the report, developers cannot be nominated as the responsible people for the illegal acts just because they are the creators. Governments try to deal with these circumstances and the creation of a "common insurance system" is between the options. This system would cover "damages caused by anonymous actors" or "risks borne by consumers". This measure would imply the rise of costs for the whole system, and the existence of tools to identify the members are preferable over the insurance system, so the liability enforcement could be done directly to the members.
Data protection	The more recent adoption since 2018 of GDPR rules within the European Union member-states, was written based on more traditional and centralized systems, and blockchain was not considered in these norms. There are three principal areas where tensions between GDPR and Blockchain exist: identification of "data controllers and processors" makes quite difficult the enforcement of GDPR's requirements; the anonymization of personal data making totally anonymous under the GDPR; and the GDPR's "right to be forgotten" provisions does not have effect when the data recorded on a blockchain is not "altered or deleted" generally.
Risk to fair competition	New competitors trying to enter in old markets can benefit from the “decentralisation and transparency” that Blockchain enhances. At the same time, there is an “increased risk of competition law infringements” that this technology enhances as well considering some “antitrust domains” as “collusive conduct” and “abuse of dominance”. The first one is related to the transparency in the exchange of information that leads to the reduction of stimulus to compete. Uncertainty between competitors is reduces once information as “prices”, “customers”, “production”, “turnover”, “capacities”, among others, are known. The second one, the abuse of dominance, in the case of permissioned blockchains, the existing members in the network could jointly refuse the enter of new competitors in the market by not giving access and leading to “competition enforcement scrutiny”.

Table 8 - Critical legal issues of implementing Blockchain (Lyons, T., Courcelas, L., & Timsit, K. (2019))

2.3.5. E-Voting and Blockchain

Nowadays, the voting method we find mostly in place is the paper ballot voting. For the purpose of this dissertation, one will consider only the political electoral system which is organized and controlled by the government of each country.

The method mostly known is filling a “ballot sheet and put it in a box”. The counting of votes occurs when the “box is emptied and the ballots are counted in public”. This process brings some problems related with transparency, trust and is time-consuming while counting votes, as is argued in the book of Xu, X., Weber, I., & Staples, M. (2019). Some doubts regarding the number of votes that were counted, the uncertainty if a voter exercised the right to vote only once and, in case a voter claims that his vote was not included in the tallying, it is not possible to verify in this system. Considering all these constraints of paper ballot voting system, new alternatives have been suggested in order to overcome avoidable problems. Electronic voting systems, as already discussed in the chapter 2.2, is ready to release improvements. With E-Voting it is possible to confirm who did not vote and "tallying votes" is faster and more reliable as one already learnt previously. According to Kovic, M. (2017), travel expenses and opportunity costs of a voter being present in the polling place in the election day can be highly reduced due to the introduction of E-Voting. Another important factor is the “mobilization effect” defending that people who had no incentive to vote before, can find a new option and become more enthusiastic, especially young people.

An innovating system brings advantages but also some problems, and it matters to understand why it is not highly used worldwide. All problems are related in one way or another with verifiability. To keep the votes anonymized in E-Voting, for voters to verify if their vote was registered successfully "without revealing who they voted for" and to decide the votes that are valid "without a privileged role", are some of the questions and challenges presented in the book regarding the adoption of Electronic Voting. In the paper written by Kovic, M. (2017), “e-voting carries the greatest risk”. In this sense, some Blockchain technology features were identified as capable to overcome and solve problems presented by E-Voting. In the book Xu, X., Weber, I., & Staples, M. (2019), the author defends “using a blockchain alone is not enough”. The ideal solution is the Blockchain-based E-Voting system. According to Yi, H. (2019), the security of E-Voting is “very urgent” and this article presents some techniques to improve its security through the use of blockchain in a peer-to-peer network.

In this article it is proposed a "blockchain-based e-voting scheme in P2P network", where three techniques are integrated to deliver the best product. The implementation of this product demonstrates that is a "practical and secure e-voting system", solving "the problem on forgery of votes during e-voting".

The first technique is based on "distributed ledger technology (DLT)" by designing a "synchronized model of voting records". This model combats the "forgery of votes". In other words, the blockchain for e-voting is represented not in a different form as the one already described in the Blockchain’s architecture chapter: a sequence of “voting blocks chained to each other”. The composition of each block is technically similar to the one already studied. However, the entire scheme is improved due to the techniques used by the author:

- “Voter’s ID”, which is “randomly assigned” to the voter;
- “Vote” representing the ballot of the chosen candidate by the voter in the voting ballot;
- “Voter’s signature” where the voter signs the hash of the vote by using “his/her private key” in order to keep the vote’s authenticity and its secrecy to other members of the network;
- “Timestamp” representing the block’s time submission to the chain and, in case there are two blocks with the same timestamp, the block that is added is the one “with a higher value of signature”;
- “Hash of the previous block” guarantees the “non-repudiation” and resistance to “modification of the data” by using the SHA-256 algorithm (Secure Hash Algorithm) that computes “the hash value of the previous block”.

The second technique described in the article is the design of a “user credential based on ECC to provide authentication and non-repudiation”. ECC stands for Elliptic Curve Cryptography and non-repudiation means the assurance that the authorship or validity of previous actions performed by the voter cannot be denied by anyone else. The ECC model usage improves the following actions:

- No one is able to see for which candidate a citizen has voted, once the voting ballot is marked with a signature by each voter;
- The authenticity of the vote is guaranteed by the “ECDSA signature” (Elliptic Curve Digital Signature Algorithm). Each voter signs the hash of the vote using “his/her private key”. This way is possible to verify if the voter is who he/she claims to be.

The ECC is defined in Sujatha, K., Arjuna Rao, A., Yejarla, P., & Sruthi, K. J. (2017) as “a public key cryptographic algorithm where it uses couple of keys as private and public”. By using the Elliptic Curve Digital Signature Algorithm (ECDSA), the voter creates his/her private and public keys "to sign his/her vote v". In other words, to create a digital signature. The private key is an integer, which is generated randomly and the public key is computed through the multiplication of the private key with a curve point in the Elliptic Curve (the private key cannot be derived from the public one). In the signing process, despite of all mathematical computations involved in the algorithm, the first step is based on the use of SHA-256 to compute the hash value of the vote. This guarantees the integrity of data by comparing the expected hash value with the actual result. Also, as already discussed before, the case is not different in this voting scheme: the votes are “cryptographically linked block by block”. All miners belong to the same peer-to-peer network and they generate the blocks under the proof of work algorithm.

The third and last technique presented by Yi, H. (2019) is “we design a withdrawal model that allows voters to change their vote before a pre-set deadline”.

In the last chapters of the article, the author discusses why blockchain-based e-voting system is “more secure and anonymous” than the other e-voting systems. According to him, the privacy of the voters is kept due to the decentralized system without a third-party involved and the use of an ID instead of the real identity, the security is ensured by the difficulty of forge the votes due to the DLT model, the non-repudiation due to the ECC model and, the possibility that voters have of changing the final vote due to a withdrawable model. Regarding the initialization of the voting process, one can see it illustrated in the appendix 6 and explained below:

- Firstly, the voter receives a credential by the voting office (another party involved in the scheme), where it is visible the voter's ID and the list of candidates
- The private key is generated by the voter
- The public key is computed by the voter
- Then, the private key is kept by each voter (only the individual voter may keep this key in order to guarantee the ballot secrecy) and the public key is sent to the Public Key Infrastructure (PKI), where the signature of the vote is able to be verified once the public key is known (PKI manages the public-key encryption)
- The miners are elected randomly and they mine the first block to start the voting blockchain (the genesis block)

However, it remains to explain how the voting is processed in the appendix 7.

- ID, the Vote and the Timestamp are included in the argument of the SHA-256 function, generating the hash value;
- The voter uses his/her private key created to generate the digital signature through the use of ECDSA on the hash value
- The voter sends his/her ID, Vote and Timestamp to the miner
- The miner obtains the public key that was sent to PKI previously through the voter's ID and uses it to decrypt the digital signature, getting the hash value
- The integrity of the vote is checked by applying the hash function on the ID, Vote and Timestamp information that miner receives by the voter
- If both hash values match (the one as a result from the decryption of the signature and the one computed with the last application of the hash function), the miner accepts the signature. Otherwise, it is rejected.
- In the end, the miner queries and verifies if "the voter has the right to vote or enough votes".
- This vote details together with the hash of the previous block generate a new block that is added to the chain by the miners.

In blockchain-based e-voting, votes can be counted by everyone but the identity of a voter associated to his/her vote, no one is able to know.

Also, for citizens that vote through an e-voting platform or a blockchain-based e-voting platform, the user experience is similar: the voter access an interface through a device and vote. However, the process behind is completely different between both platforms.

2.3.5.1. Case Studies

Some advantages of the integration of Blockchain technology in electronic voting systems were already explained before. Blockchain is based on immutability and when well implemented, forgery is eliminated. For all these reasons, social technology defined as "ways to communicate, cooperate, compromise, and make consensus with other people" (Jun, M. (2018)), is possible to be implemented through the use of Blockchain and to replace bureaucracy. Having this in mind, in the research article written by Cucurull, J., Rodríguez-Pérez, A., Finogina, T., & Puiggalí, J. (2019), some "electronic voting system projects based on blockchain" are listed. This list includes both private projects and led by the government. For the purpose of this dissertation, one decided to consider the ones that have as application political electoral voting.

In the table below, some of these projects are described.

<table>
<tr><th>Organization</th><th>System</th><th>Technology</th></tr>
<tr><td>Denmark Liberal Alliance</td><td>Follow My Vote</td><td>Graphene Blockchain Framework</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">The Elliptic Curve Cryptography is used for the digital signature as well as the pairs of keys for signing the votes. These elements keep the anonymity and authenticity of voters. It uses a blind signature approach.
Voters can verify if their vote is correctly recorded and counted once votes are added to the chain without encryption, making verifiability and auditability possible.
Two disadvantages associated are the result of the election is possible to determine before the official announcement and "vote selling and coercion" may exist.</td></tr>
</table>

Table 9 - Follow My Vote (Cucurull, J., Rodríguez-Pérez, A., Finogina, T., & Puiggalí, J. (2019))

<table>
<tr><th>Organization</th><th>System</th><th>Technology</th></tr>
<tr><td>Podemos (Spain)</td><td>Agora-Voting</td><td>Bitcoin</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">Encryption and verifiability are provided end-to-end. Immutability is guaranteed in ballots, in its configuration and consensus proofs. Once Bitcoin is the technology implemented in this application, the blockchain immutability exists due to Catena built on top of Bitcoin: an "append-only log".
Anonymity of voters, authenticity and secrecy of votes are supported by the system and its design enables the prevention of "coercion and vote buying".
Regarding verifiability already mentioned, Agora Voting provides all the necessary properties desirable: "Cast-as-Intended, Recorded-as-Cast and Counted-as-Recorded verifiability". Cast-as-Intended is based on a process repeated a certain amount of times until the voter believe and be confident that the system is accurate and a real vote is casted (Cast-or-Challenge is the name of the mechanism used). Recorded-as-Cast occurs when voters verify that the "vote is correctly published in the blockchain". Counted-as-Recorded verifiability is based on the access to the data during the counting of votes and "the availability of the Zero Knowledge Proofs produced by the mixing and the decryption processes".</td></tr>
</table>

Table 10 - Agora-Voting (Cucurull, J., Rodríguez-Pérez, A., Finogina, T., & Puiggalí, J. (2019))

<table>
<tr><th>Organization</th><th>System</th><th>Technology</th></tr>
<tr><td>Texas Libertarian Party</td><td>VoteWatcher</td><td>Florincoin Blockchain</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">Voting system developed by Blockchain Technologies Corp. Transparency and efficiency define this system, as well as all process is “highly auditable”. The QR code is used to prevent duplicated scanned ballots. Voters use paper ballots to vote. Then, OMR (Optical Mark Recognition) is used to scan the filled ballots. Once all ballots are scanned, transactions are created and form the blockchain. Florincoin Blockchain enables more data to be added to a transaction comparing to Bitcoin, so it is the technology used to upload ballot data. The Bitcoin Blockchain supports less data per transaction and is more expensive, but the security is granted. Hence, both technologies are combined and the “resulting hash is posted to Bitcoin’s robust blockchain”.</td></tr>
</table>

Table 11 - VoteWatcher (Cucurull, J., Rodríguez-Pérez, A., Finogina, T., & Puiggalí, J. (2019))

One had mentioned the i-Voting in Estonia in chapter 2.2.3. The Public Key Cryptography useful for the ID-Card and digital signature are concepts that were described, as well as the use of the public and private keys of every voter. The ID-Card is used consequently in i-Voting.

The chip of digital ID cards is built on top of public key encryption and not Keyless Signature Infrastructure (KSI), the “blockchain technology designed in Estonia” as retrieved from KSI Blockchain - e-Estonia. (2019, September 10) website. The National voting system in Estonia is electronic and not a blockchain-based electronic voting system. However, in the working paper Martinovic, I., Kello, L., & Sluganovic, I. (2017), the researchers state blockchain can bring a “revolution in the security and transparency that is needed to enable e-voting”.

Investigating the publication written by Boucher, P. (2016), product of Scientific Foresight Unit (STOA) of European Parliamentary Research Service, the author affirms that Blockchain was already used in elections: “internal elections of political parties” and “shareholder votes in Estonia”. In Ojo, A., & Adebayo, S. (2017), the participants are named: “Tallinn Stock Exchange, Nasdaq and e-Residency Programme”.

In order to understand how this country digitally advanced behaves in terms of adopting Blockchain in various government electronic services in Martinovic, I., Kello, L., & Sluganovic, I. (2017) the authors name the applications: “Estonia’s Digital Court System” (integrity of records is guaranteed by hashing data with KSI Blockchain, enabling “transparent auditability” and records immutable); “Estonian e-Health Authority” (used to protect over a million of health records and enables proof-of-record existence and “database integrity for internal, external and regulatory compliance purposes”; “Estonia Succession Registry” (the records chained have a “provable ordering” and it is not possible to change it without being detected).

3. METHODOLOGY

3.1. CASE STUDY

Before starting with the definition of Case Study and what this methodology implies, it is important to revisit the research questions initially presented in this dissertation: "why" a Blockchain-based voting system in Portugal would be beneficial and a solution to the mobility concern and trust crisis and, on the other hand, "how" its adoption would impact the abstention rate and the trust in the Portuguese political system. Based on these two questions of "why" and "how", one found Case Study as the most suitable methodology to explore, draw conclusions, validate and discuss possible solutions.

In the book from Yin, R. K. (2009) entitled Case Study Research Design and Methods, the author arguments against some social scientist's permissions that Case Studies are "only appropriate for the exploratory phase of an investigation". He explains that some of the most well-known case studies have been explanatory rather than only exploratory. Hence, he defends "an inclusive and pluralistic" vision, and that may exist exploratory, descriptive and explanatory Case Studies. In another chapter, the author arguments under which circumstance(s) the use of this methodology is more adequate. The questions "why" and "how" are the core: "such questions deal with operational links needing to be traced over time, rather than mere frequencies or incidence". When the type of research questions matches with these two, it means the researcher seeks for more "explanatory" reasons and Case Study is preferred over other research methods. Thereupon, the definition that the author of the book gives to this methodology helps one to understand its essence. He departs from other observer's words who considers "decision or set of decisions" the major focus: "why they were taken, how they were implemented, and with what result".

According to Robert K. Yin, the technical concept of Case Study may be divided in two parts (the scope and technical characteristics as data collection and data analysis strategies). The author affirms that a case study is an "empirical inquiry" that focus on a contemporary phenomenon and its position in a real-life context, mainly when what separates the phenomenon from the context is not clear. Regarding the technical definition, "the case study inquiry" technically data points are not only sufficient once there are many other variables to consider in the investigation, having two main results: need for convergence of data in a "triangulating fashion" once there are "multiple sources of evidence", and the definition of "theoretical prepositions" in the start is fundamental to "guide data collection and analysis".

In order to support the use of this methodology for future investigations, the author has in consideration the amin weaknesses defended by scientists and presents contra-arguments.

"Lack of rigor", not following "systematic procedures", allowing equivocal or bias results that conduct the post-analysis of a study is a first prejudice presented. Robert K. Yin alerts for the fact that bias during experiments and in the design of questionnaires for instance also exist, however, in a case study "they may have been more frequently encountered and less frequently overcome". "Little basis for scientific generalization" is the second concern mentioned in the book. The author arguments that Case Studies as Experiments have a common goal: reach generalized theories and analysis and not particular, and both research methods generalize results based on theoretical prepositions and not to populations or universes. The third concern is the long time that takes to produce a study based on this methodology, as well as results most of the times in “massive, unreadable documents”. This is not so linear for him once the long, massive documents and more traditional can be avoided nowadays and in the future by adopting more creative and innovative techniques. Finally, the fourth and last limitation is the impossibility of drawing “causal relationships”. He addresses the complementary role of a Case Study in this point, defending that while another method would provide evidence of success in the efficacy of a certain model, this methodology complements the others by explaining “why” and “how” the model actually works.

As remarked in the book, most of the Case Study researches performed are considered “soft” once they do not follow systematic procedures. The book helps to overcome this constraint by providing to the reader “an array of such procedures”. In this dissertation, one will follow and adapt according to the needs this set of rules, so the model become complex and well-founded.

3.2. Research Strategy

In order to conduct the Case Study methodology, there are a set of steps that may be followed and completed. For any study to succeed while adopting this methodology, the researchers need to have a strategy. In the book from Yin, R. K. (2009), the author describes the important phases.

Firstly, a researcher needs to develop a theory and design it. Once the research questions meet the ideal to do a case study, the "research design" may be defined. According to Robert, there is no "catalog of research designs" that help investigators and contradicts some incorrect thoughts that the case study is "one type of quasi-experimental design", by quoting a sentence of Cook & Champbell, 1979, p.96: "Certainly the case study as normally practiced should not be demeaned by identification with the one-group post-test-only design". Thus, the case study is not only a research method itself as well "has its own research designs".

In order to define the Research Design concept, the author mentions the logical plan like almost a path to be followed from "here" to "there", where "here" means the initial research questions and "there" the answers that one aim to reach. This plan compromises a "process of collecting, analysing and interpreting observations" and deals with four main problems based on "what" and "how" questions: "what questions to study, what data are relevant, what data to collect, and how to analyse the results". Summing up, the researcher may ensure that the evidence addresses the research questions.

To succeed in the planification of a research design, five major components may be addressed: "study's questions", "propositions, if any", "unit(s) of analysis", "logic linking the data to the propositions" and, "the criteria for interpreting the findings".

The study questions were already mentioned in the previous chapter 1.3, the "how" and "why" questions. A good method to go ahead with this set of questions before hand is ensure that exist further studies supporting the ideas mentioned. For instance, finding studies that conclude about the potential of a Blockchain-based voting system as a solution for the mobility concern and trust crisis, provide a good argument to support the theory.

The second component is the "study propositions", the engine that moves the study to another level. By asking "how" and "why" this technology studied in this dissertation can solve existent problems, one may think and elaborate a set of propositions that help to "look for relevant evidence". To the question "why" a Blockchain-based E-Voting system would solve the mobility concern, one may think that it offers to citizens an extra and more flexible way of voting. From this proposition, one may study if this situation is verified in a role model system and taper which options would exist and how they would be reconciled (paper ballot votes versus electronic votes). Through the design of propositions, one may be able to defend successfully a possible judgement of this dissertation.

The third component is the "unit of analysis", which is directly related to the way how the initial research questions were defined. In order to study the Portuguese voting system with the introduction of Blockchain-based E-Voting, one may study and take the best example existent in the world. For the purpose of this dissertation, and taking as an example of what is discussed in the book, one may define the case (a real-life situation of a more advanced way of voting) which is the Estonian I-Voting system. This I-Voting system is indeed a case-study of the potential to implement a Blockchain-based E-Voting system in Estonia. Furthermore, the case has embedded at least one "unit of analysis", for instance the Estonian government policies in terms of electronic voting and citizens' adherence to electronic voting and government digital services. At last, this case-study works as a role model to apply in Portugal.

The fourth and fifth components of the research design correspond to “linking data to propositions” and “criteria for interpreting a study’s findings”, respectively. There is no detailed guidance for these two components, according to the author, but it is based on the combination or calculation of case study’s data “as a direct reflection” of the initial propositions and, on the other hand, the interpretation’s criteria defends that it is important to anticipate rival explanations to the case study’s research design work. In this sequence, the author describes the importance of “theory development” as a part of the design phase. All the five research design components described embody a “theory” of what is being studied. Once for the purpose of this dissertation the case study will be used to develop theory, it matters to distinguish between theory in favour and rival theory. A theory in favour would be the use of the Case Study will demonstrate that Blockchain applied to an E-Voting system is only possible when a government reforms its most traditional public services provision methods by moving towards a digitization process. A rival theory would be that the Case Study will also show how the lack of trust and knowledge towards the technological system are significant barriers for its widely adoption. By defining the theory before the collection and analysis of data will provide guidance on how to succeed in the next steps.

Another important part of this theory development is to which extent is possible to generalize from case study results to theory. The author defends the “analytic generalization”, where a “previously developed theory is used as a template with which to compare the empirical results of the case study”. This analytic generalization can be made based on one single-case study or more than one from which results are reached and inferences are made (policy implication and rival policy implication which are compared with a previous generalized theory granted).

In order to conclude the Define and Design phase, the author describes the matrix shown in figure 6, divided in four quadrants: single-case designs (holistic), multiple-case designs (holistic), single-case designs (embedded) and multiple-case designs (embedded). For this dissertation, one will follow the single-case design with embedded units of analysis. As stated by the author, following a single-case study is advised under certain circumstances. The first one is when it represents a “critical case in testing a well-formulated theory”. The single case is enough to contribute to “knowledge and theory building” and is able to invite for future studies about a field. Estonian digital society is a global example in terms of development of e-solutions.

Another circumstance is when the case is “representative or typical”. It represents a typical project among others, being informative enough about and average “person or institution”. In this sequence, Estonia is a member of European Union and Euro Zone, two common areas with Portugal. Hence, Estonia is aligned with Portugal by sharing identical political and economic objectives, converging to identical development stages. A third reason is because it is a “revelatory case”. Few countries reach the same level of success and recognition regarding the government and society adherence to benefit from public electronic services over more traditional means. The last reason presented is a “longitudinal case”. By looking to different points in time and concluding about how much time it took the transition from the only paper ballot voting method to the implementation of the additional option of I-Voting, could reflect the potential different stages that the Portuguese voting system would go through. Regarding the embedded units of analysis, one finds it preferable, once offers more extensive analysis of the single-case over a holistic one.

In order to collect data, some preparation steps need to be completed. In the book from Yin, R. K. (2009), the author emphasizes the importance of protect human subjects. In case of proceeding to interviews to collect data, for instance, one may ask the participants for volunteerism in participating and aware them about the nature of the study. Besides one may inform the protocol involved and make clear that each one will be protected against any harm. "Privacy" and "confidentiality" may be preserved and do not put any participant in an undesirable position.

As a way to conduct a training agenda for doing the case study, one decided to do a Case Study Protocol template. This protocol includes, further than a simple questionnaire, a set of "procedures and general rules to be followed". The advantages of doing a protocol are various: focus on the topic of the Case Study, foreseeing problems and planning possible solutions ahead, and target the audience even before writing the case study report.

Regarding the Protocol's structure, there are four main sections that may be considered. The first one is an "overview of the case study project". Here, a background information is included about the study, such as the research questions, propositions, the logic model, reference to relevant reading material, the protocol’s role of guiding. The purpose may be explicit so anyone can contextualize and, last but not least, a letter or introduction can be accompanied to send to the potential participants.

The second section is called “field procedures”. They are required, once there is space for open answers and sometimes going out of the questions boundaries initially planned. Making a schedule, with timings and expected activities to be completed, is a way to manage.

Thirdly, the case study questions. They may be formulated based on evidence and their sources and keep one on track as data collection proceeds. Questions can be formulated at five different levels ("questions asked of specific interviewers", "questions asked of the individual case", questions asked of the pattern of findings "across multiple cases", "questions asked of an entire study" and, "normative questions about policy recommendations and conclusions, going beyond the narrow scope of the study".

All different phases of a case-study methodology can be found in figure 7 below.

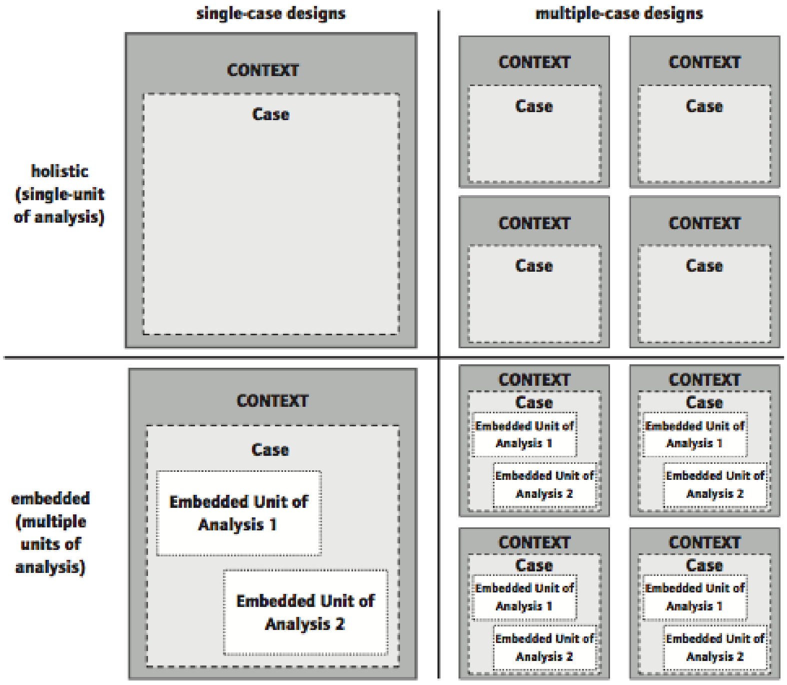

single-case designs
multiple-case designs
holistic (single-unit of analysis)
embedded (multiple units of analysis)
CONTEXT
Case
Embedded Unit of Analysis 1
Embedded Unit of Analysis 2

Figure 6 - Types of designs for case studies (Yin, R. K. (2009))

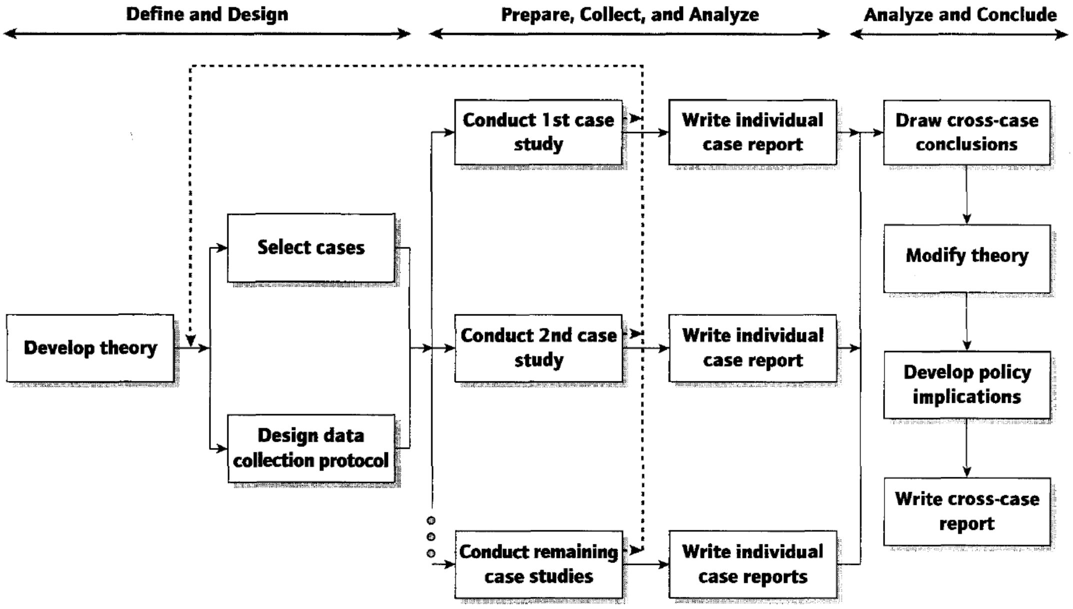

Define and Design
Prepare, Collect, and Analyze
Analyze and Conclude
Develop theory
Select cases
Design data collection protocol
Conduct 1st case study
Conduct 2nd case study
Conduct remaining case studies
Write individual case report
Write individual case report
Write individual case reports
Draw cross-case conclusions
Modify theory
Develop policy implications
Write cross-case report

Figure 7 - Case-Study methodology phases (Yin, R. K. (2009))

4. CASE STUDY – ESTONIA

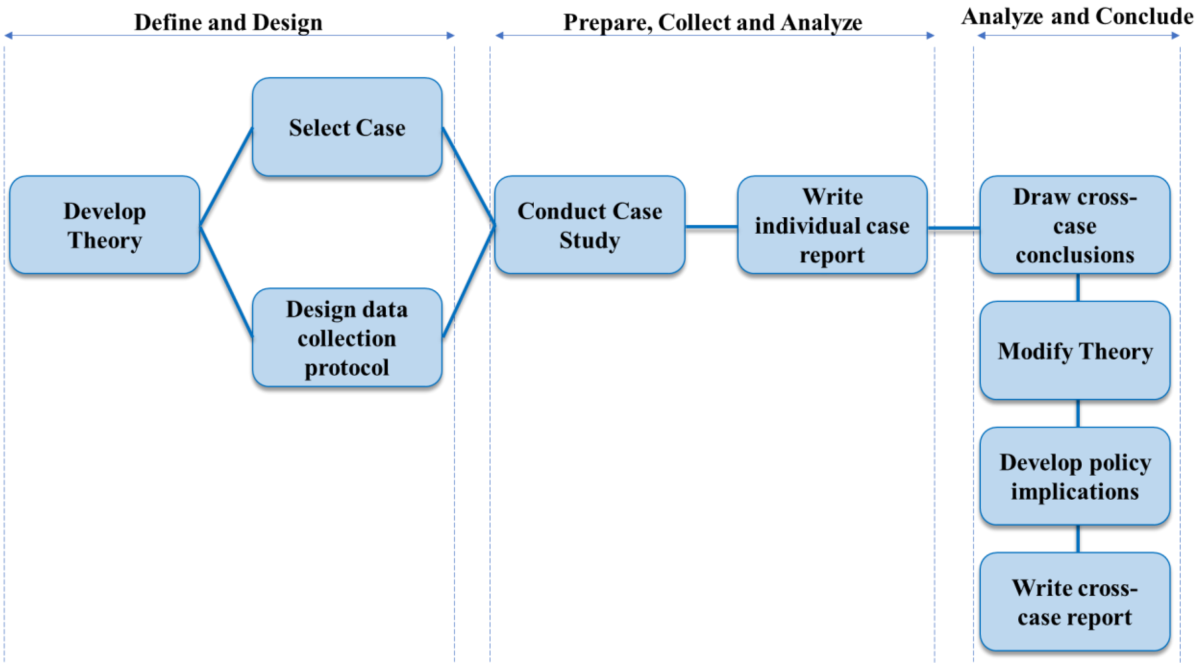

Define and Design
Prepare, Collect and Analyze
Analyze and Conclude
Develop Theory
Select Case
Design data collection protocol
Conduct Case Study
Write individual case report
Draw cross-case conclusions
Modify Theory
Develop policy implications
Write cross-case report

Figure 8 - Different phases inspired from Yin, R. K. (2009) and adapted to this dissertation

4.1. CASE SELECTION

Generally speaking, Estonia and Portugal follow a set of rules and rights that are common to these two countries: European Union law (European Union treaties and European Union legislation, for instance). Also, in political terms, they are a Democratic Republic, even with some differences across national executive and legislative branches. The fact that they are both EU member-states, there is a political framework convergence and enables one to wonder about the existent gap about the technology adoption in e-government services in Portugal when compared to the Estonian strategy. In this chapter will be pointed out arguments for choosing Estonia as the Case Study of this dissertation. Also, one will take into consideration the different acts and politics existent between both nations, despite of considering the integration of electronic voting and the Blockchain application perspective by Estonia a good opportunity and example to mirror in the future development of electoral law in Portugal. This last topic will be developed in chapter 4.5.

According to SCOOP4C, that stands by Stakeholder Community Once-Only Principle For Citizens, a project funded by the European Union, the Estonian Internet Voting is studied and is concluded that this country "became the first nation to hold legally binding general elections over the Internet for the municipal elections in 2005". Two years later, Estonia became the first country worldwide to use internet voting in the Parliamentary Election. In Maurer, A. D., & Esteve, J. B. (2016) book, the authors mention that the major principles of traditional voting are followed by I-Voting, as "freedom, universality, uniformity and secrecy (anonymity) of the vote". In other words, the adaptability of the new system with the traditional one in order to facilitate the voter's understanding of its process is relevant to notice. Also, the Parliament's liberal approach to voting that states the voter has the option to vote either via Internet or in the traditional way in a polling station, and, not less important, the Estonian system is a pioneer of internet voting. These three subjects are good arguments to choose this country as a case study.

Departing from the literature review, one concluded that before binding elections over Internet in 2005, Estonia announced previously in 2001 the adoption of electronic voting as stated in Binder, N., Krimmer, R., Wenda, G. & Fischer, D. (2019). Due so, this fact increased responsibility to this nation become the first one establishing a legal procedure in the adoption of Electronic Voting. One year later, in 2002, the Riigikogu Election Act was introduced and assumed legal effect in the same year (will be further discussed in the next chapter 4.2). There were amendments at the same time the technology was developing, the act was updated and today many changes will step into force in 2021, for instance. In order to become legally accepted, the Organization for Security and Co-operation in Europe (OSCE) mission report in 2011 presented a set of recommendations regarding e-voting and the Estonian Electronic Voting Committee was created. Hence, the need to legislate and document both the technology used as well as all the process, shows transparency, convergency in adoption steps, a clear cooperation between public and private sectors, are crucial factors for successful citizens acceptance and accession to the new way of voting, as well as worldwide recognition as a country that is a step ahead in the introduction of technology in national elections.

Furthermore, it was investigated in the literature review that currently Estonia does not integrate Blockchain technology in the National internet voting system architecture. However, as defended in the working paper Martinovic, I., Kello, L., & Sluganovic, I. (2017), blockchain can bring a "revolution in the security and transparency that is needed to enable e-voting".

In the Issues & Challenges – chapter 2.2.4, some E-Voting constraints are identified, according to a report published by the European University Institute, Robert Schuman Centre for Advanced Studies, European Union Democracy Observatory – EUDO, Trechsel, A. (2016). E-Voting faces "legal considerations", "political considerations", "technological and security challenges" (both human-related and tech-related) and "social challenges". While several aspects can be handled according to the increase of legal acceptance and convergence in the European Union (Legal Considerations), increase of transparency and communication from the government side to citizens so they feel confident to vote electronically (Political Considerations), Technological and security challenges are the ones that are still more critical and reason for not existing a broader adoption in other European countries. Further on, in "E-Voting and Blockchain" - chapter 2.3.5, it is indicated why E-Voting is not widely used and a Blockchain-based E-Voting system solution (not blockchain alone once it is not enough) is introduced as capable to overcome and solve problems presented by E-Voting. Although one describes in this chapter a theoretical model where are presented Blockchain techniques that can overcome issues of the current system ("synchronized model of voting records", "user credential based on ECC to provide authentication and non-repudiation" and "withdrawal model that allows voters to change their vote before a pre-set deadline", according to Yi, H. (2019)), one defends that a blockchain-based e-voting system is "more secure and anonymous" than the other e-voting systems. According to the author Yi, H. (2019), the privacy of the voters is kept due to the decentralized system without a third-party involved and the use of an ID instead of the real identity, the security is ensured by the difficulty of forge the votes due to the DLT model, the non-repudiation due to the

ECC model and, the possibility that voters have of changing the final vote due to a withdrawable model. Moreover, in blockchain-based e-voting, votes can be counted by everyone but the identity of a voter associated to his/her vote, no one is able to know. For all these technical fundamentals, Blockchain is promising for technological development at the election level.

In Estonia, there are private elections ("internal elections of political parties" and "shareholder votes in Estonia") and government electronic services ("Estonia's Digital Court System", "Estonian e-Health Authority" and "Estonia Succession Registry") that use currently Blockchain.

4.2. Case Identification

Estonia, officially the Republic of Estonia, is a Parliamentary Republic. Like Portugal, there is a head of government, the prime minister, and a head of state, the President of Republic. In 1st of May 2004, this country became an EU member state. In electoral terms, the President in Estonia is elected every five years, the Parliament deputies are elected every four and the European Parliament deputies are elected every five years. Summing up, this political system is highly defined by the National elections results that are obtained either by Estonian citizens going physically to the voting polls or voting via internet, as one already mentioned. As part of this Case Study, it matters to understand the existent Electoral Acts in the Estonian Constitution: Riigikogu Election Act (most commonly known as the Estonian Parliamentary election), Local Government Election Act (municipal councils), European Parliament Election Act (Estonian members of the European Parliament - MEPs), Referendum Act ("the Riigikogu shall submit any amendment of Chapters 1 and 15 of the Constitution to a referendum. The Riigikogu may submit other draft Acts that amend the Constitution, and other draft Acts or other national issues to a referendum") and President of the Republic Election Act, according to the official elections website of *Riigi Teataja*.

As defined in the Maurer, A. D., & Esteve, J. B. (2016) book "E-Voting Case Law: A Comparative Analysis", the members of the Riigikogu, government and European Parliament are elected in "free, general, equal and direct elections", as well as "voting shall be secret". There is a legal framework for I-Voting in all electoral acts mentioned above, but it is in the Riigikogu Election Act that the stipulated provisions are more described. Hence, one will focus on this act (English translated version and in force until 31.12.2020) and understand what is documented regarding Electronic Voting.

In the chapter 7^1 *Electronic Voting* of the Riigikogu Election Act, that entered into force on 11.11.2012, the following set of provisions are documented: "General principles of electronic voting", "Preparation of electronic voting", "Electronic voting procedure", "Change of electronic votes", "Verification of electronic votes", "Taking into account of electronic votes" and "Suspension, termination and not starting electronic voting". In each of these seven provisions blocks, it is explained all the procedures that may be followed prior and during the electronic voting.

Chapter 7^1 ELECTRONIC VOTING of the Riigikogu Election Act **(*entry into force 11.11.2012*)**	
"General principles of electronic voting"	The right of the voter to change his or her vote cast by electronic means is enunciated in this provision. Right after, the roles of the Electoral Organizers, the National Electoral Committee and State Electoral Office, respectively, are identified through the intervention in ensuring the proper application of the Electronic Voting. The National Electoral Committee is responsible to "establish by a resolution" the organization of electronic voting through technical requirements principles assurance and its description. Regarding State Electoral Office
"Preparation of electronic voting"	In this phase, the State Electoral Office has a crucial role. This organizer receives the amendments to the list of voters at least once a day and must organize these entries at the same time frequency. Moreover, it is responsible for all the technical set-up prior to any election: ensure and inform about the operating systems compatible with the voter application; creation of the encryption key for electronic votes and the vote-opening key; guarantee support to visually impaired citizens in the voter application usage; make publicly available (publish) the voter application, votes verification application and the authenticity and integrity of the website information. All these required procedures may be finished "not later than by the thirteenth day before election day".
"Electronic voting procedure"	The electronic voting may be done between the tenth and fourth days before the election day, twenty-four hours a day and closing at 6 p.m. on the fourth day before election day, following the proper organization of the E-Voting as established by the National Electoral Committee. The list of candidates is then displayed to the voter after his/her identification. The candidate is chosen, the vote is encrypted with the vote-encryption key and the digital signature is used to confirm the vote ("in conformity with the requirements of the Electronic Identification and Trust Services for Electronic Transactions Act"). The E-Voting procedure ends with the notice displayed to the voter, confirming the voting is done.
"Change of electronic votes"	The voter has the right to change his/her vote during the seven day-period mentioned before. It is also possible to change from Electronic Voting to ballot paper voting, during the same seven day-period for the cases of Advance voting, "Voting in custodial institutions, hospitals and twenty-four hour social welfare institutions" and voting of voters residing in foreign countries (40–43, 45 or 47 of Riigikogu Election Act).

"Verification of electronic votes"	The verification of votes is possible. Any voter has the opportunity to verify if the application has transferred the vote correctly (this verification is only possible since 2015). The vote verification application is developed by the State Electoral Office as already mentioned and, this is only possible to be checked by the voter "for a limited time a limited number of times".
"Taking into account of electronic votes"	In this provision, the conciliation between electronic voting and paper ballot voting systems is reached. First of all, in case of several electronic votes submitted by the same voter, only the last one is taken into account. Then, in order to avoid misleading information, the State Electoral Office may send not later than two days before the election day to all "rural municipality or city secretaries" the list of voters who voted electronically by voting district. One day before the election day, all district committees may have access to this list. Regarding the electronic voting and traditional voting, the Act sets some rules to ensure the unique vote, based on a "nested if's" relationship: **Voter voted electronically** → his/her name is notated; **Voter voted electronically + ballot paper** → ballot paper vote is the only taken into account; **Voter voted electronically + voted several times outside of his/her voting district** → any vote is taken into account.
"Suspension, termination and not starting electronic voting"	**Suspension** of electronic voting → the National Electoral Committee must notify voters and ask to restart the electronic voting; **Not starting or termination** of electronic voting → the National Electoral Committee must notify voters and provide the alternative to electronic voting; **Suspension or termination** of electronic voting → the National Electoral Committee must notify voters about the necessity to vote again and provide the alternative to electronic voting.

Table 12 - Electronic Voting articles in Riigikogu Election Act (Riigikogu Election Act (2002))

4.3. CASE INFORMATION RETRIEVING

In order to proceed with the case analysis in the next chapter, one retrieved information from different data sources – official electoral website from Estonia, where could access official documents and papers regarding the Internet Voting architecture published by people responsible for the development of the system (Cybernetica company) and further data and information regarding the adoption behaviour of I-Voting among the Estonian population across last years. The paper written by Heiberg, S., Laud, P., & Willemson, J. (2011) was analysed regarding the security challenges of this online system deployment.

Furthermore, one conducted an interview with Florian Marcus, the Digital Transformation Adviser in e-Estonia Briefing Centre about the Internet Voting in Estonia and also attended a conference ("e-Estonia Live: i-Voting as key to future elections") where it was asked the opinion and perspective about the use of Blockchain integrated in Estonian I-Voting. Steven Heiberg, I-Voting Product Manager Cybernetica AS (company also known for the Internet Voting development) shared his thoughts about this integration.

4.4. CASE ANALYSIS

In this chapter, one will start by revisiting the three pillars addressed in the literature review: E-government, E-voting and Blockchain (namely the Blockchain-based E-voting system). It is important to indicate on this phase the most relevant parameters, data and information in the Estonian framework.

In the E-Government pillar, one studied the importance of implementing policies and providing services to citizens through the use of electronic devices. It was defended that a well-structured E-government architecture is capable to improve transparency and openness in the public sector, as well as combatting corruption. Greater efficiency and cost reductions are mentioned also. According so, it matters to understand in the Estonian case if the same is verified. In the paper "Estonian e-Government Ecosystem: Foundation, Applications, Outcomes", Vassil, K. (2015), the author explains how the modernization of ICTs of the public sector and governance contribute to "provide transparent governance", "offer efficiency in terms of money and time saved" and, last but not least, the electronic services provided are considered "trustworthy and reliable".

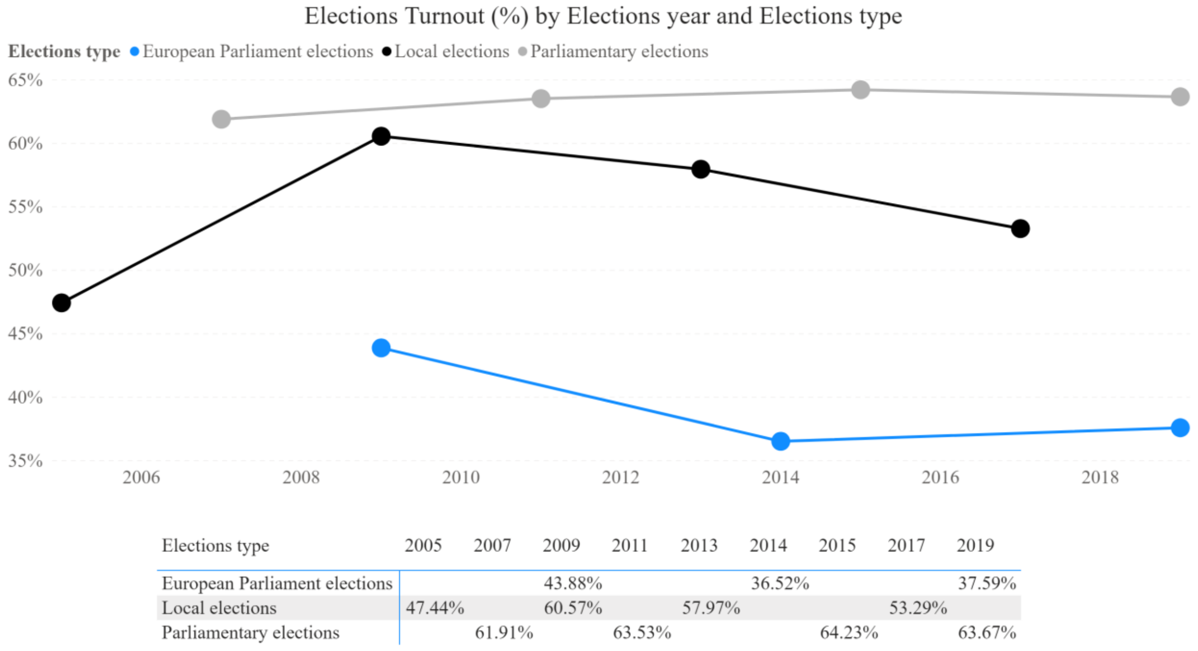
Right after, one puts in perspective two models, an E-Government architecture model studied in the literature review from Ebrahim, Z., & Irani, Z. (2005) side by side with the Estonian E-Government technical architecture that is defended in the article from McBride, K., Kütt, A., Yahia, S., & Draheim, D. (2019).

Framework of E-Government Architecture (*Ebrahim, Z., & Irani, Z. (2005)*)	**Estonia's Technical Architecture** (*McBride, K., Kütt, A., Yahia, S., & Draheim, D. (2019)*)
Access Layer	**Electronic identity**
"The channels that government users can access the various government services"	"Allows for citizens to be able to identify themselves in order to access the delivered services." Based on a chip-based ID card, a SIM-based MobileID application and SmartID.
E-Government layer	**Delivery channels**
"Web-portal of government services, in the form of a one-stop e-government portal", "integration, linkage and share of information between different organizations"	They are a "combination of a centralized "single window" portal in conjunction with private services offerings by public service providers". A single portal.
E-Business layer	**Interoperability**
Government portal incorporates front-end applications ("online catalogues and transactions interfaces"), with back-end activities ("existing databases and data warehouses").	"Distributed service bus called X-Road which allows for different agencies to provide and consume services". X-Road provides services that are accessible via the "Information System Registry which lists all datasets in Estonia, and the services available for accessing them".
Infrastructure layer	**Infrastructure**
"Focuses on technologies that should be in place before e-government services can be offered reliably and effectively to the public". It is the "Network Infrastructure".	"Consists of three main components": "network solution called ASO, data embassies, and a private cloud solution".

Table 13 - E-Government architecture model adapted to Estonia's Technical Architecture

Moving from the E-Government pillar to the E-Voting one, the concept of E-Voting was given based on different sources and authors. In the literature review, E-Voting and I-Voting concepts were distinguished from one another: "e-voting is different from Internet Voting where voters cast their ballots remotely over the Internet", as quoted from Abba, A., Awad, M., Al-Qudah, Z., & Jallad, A. (2017). Regarding the Estonia case, it is known that is used Internet Voting as one mean of voting beyond the traditional method. Hence, according to Zissis, D. & Lekkas, D. (2011), the remote e-voting offers advantages over the "poll-site" e-voting (in the case of Estonia, I-Voting over the paper-ballot voting): "cost reductions due to economies of scale and increased participation due to voter geographic independence" and, "by complying with all security requirements, together with the cost reductions and mobility issue solved, the turnout may increase". Hence, it is important to understand if these advantages are verified in Estonia.

Regarding the increase of total turnout in Elections, one considered data from the Valimised website (the official Estonian elections website). The participation in voting (%) since 2005, year when I-Voting started being used in this country, did not increase consistently as verified in the visualization below.



Elections type	2005	2007	2009	2011	2013	2014	2015	2017	2019
European Parliament elections			43.88%			36.52%			37.59%
Local elections	47.44%		60.57%		57.97%			53.29%	
Parliamentary elections		61.91%		63.53%			64.23%		63.67%

Figure 9 - Elections Turnout in Estonia (Valimised website)

However, the evolution of the proportion of I-Voters is a different scenario. In the line charts in appendix 8, one can see that since 2005, the percentages of eligible, advance and participant I-Voters have been increasing consistently. In the European Parliament elections of 2019, the total number of I-Voters reached almost 50%, as it is visible in the figure 10. The I-Voting adoption rates are evidence that the trust and willingness of more and more Estonians to use I-Voting as the preferable way of voting, are increasing.

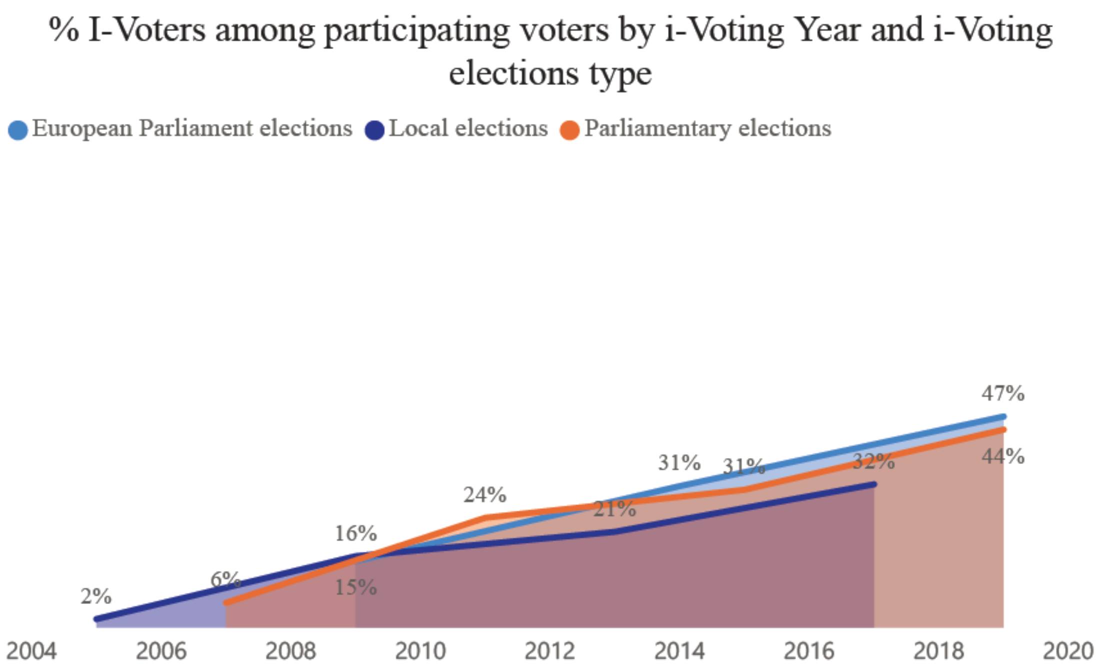
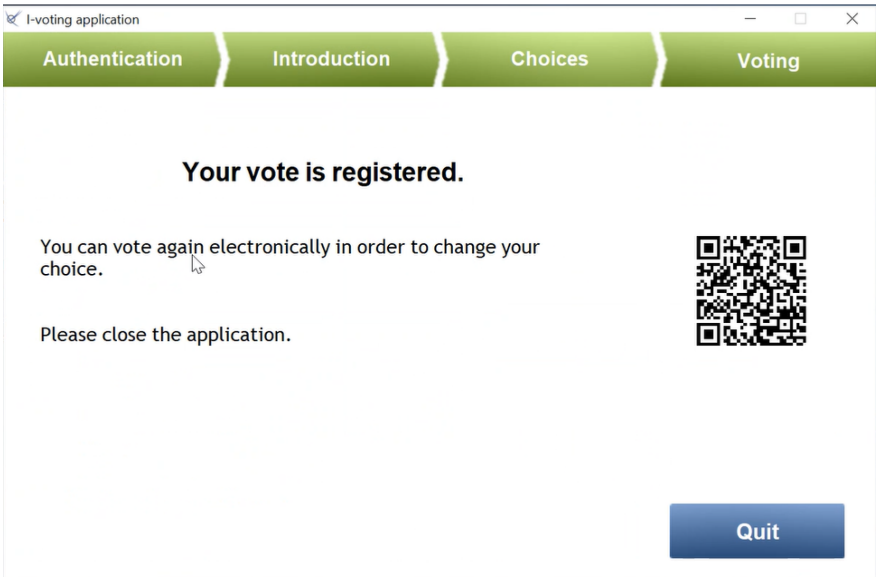


Figure 10 - Percentage of I-Voters in Estonia (Valimised website)

In order to validate the cost reductions of using I-Voting as the preferable channel to vote, one will reference the values calculated in Krimmer, R., Dueñas-Cid, D., Krivonosova, I., & Vinkel, P. (2018), a paper where the cost differences between the existent voting channels in Estonia were investigated and accounted, allowing researchers to conclude with greater accuracy about the administrative costs associated to each channel. Relying on the Local elections of 2017, the authors were able to achieve that the cost per ballot, in Euro, is around 2,32 through I-Voting channel, the cheapest one when compared to the remaining voting channels considered in this analysis: "Early Voting in country centres" (5,07), "Advance Voting in country centres" (6,24), "Election Day Voting in country centres" (4,61), Advance Voting in Voting District Committees (VDC) (20,41) and "Election Day Voting in VDC" (4,37).

Since 2002, Estonia introduced the national ID card. Furthermore, there are other two forms of digital identification: "Digi-ID" and "Mobiil-ID". Digi-ID is a card which contains less personal information than the national one, but still useful for authentication and digital signature. Mobiil-ID is similar to Digi-ID in terms of functionality, but "built into a mobile phone SIM card rather than a chip and PIN card". According to the official Estonian election's website, the proportion of Mobile-ID I-Votes among all I-Votes have been increasing consistently election after election, from 1.9% in the Parliamentary elections in 2011, year of Mobiil-ID introduction, reaching 30.1% in the European Parliament elections of 2019.

In the E-Voting case of Estonia explored in the section 2.2.3, it was studied the architecture of the system, how the different components are associated from the moment when the citizen opens the voting client application until the moment when the vote is successful registered for tallying and the voter can verify his/her vote by reading the QR Code with the smartphone in the verification application. In this section, one will analyse the experience of the end user which goes through four different stages: “Authentication”, “Introduction”, “Choices” and “Voting”. In order to understand how the vote is registered in practice, one went to the same Estonian website already referred and watched a demonstration by Florian Marcus, Digital Transformation Adviser in e-Estonia Briefing Centre. In the “Stages of i-Voting in voter application” session, the “Authentication” tab goes through all steps to identify the voter - choose the ID-card (enter PIN1 code) or Mobile-ID (mobile phone number and personal identification code) for voting. After sending, the verification code is displayed. The system checks if the person has already voted and the list of candidates are loaded. The “Introduction” stage starts and its main goal is to display the voter’s name and proof of how it was correctly identified in the previous stage and it is also informed if any i-vote was already registered previously by the voter. Moving to next stage, “Choices”, the list of political parties and candidates is displayed in drill down hierarchy (the political parties are displayed first and only after selecting one party, the list of candidates associated are visible). There is also a search box to type the candidate names (results are filtered when are typed at least two symbols). After click on “Vote”, the last stage “Voting” is designed to confirm the choice with digital signature. In order to so, the voter can go back to the previous stage or click in the “Confirm” button. Once the click is done on Confirm, the vote is encrypted and the digital signature is required (in the case of ID-card, voter just needs to insert the PIN2; with Mobile-ID, the PIN2 needs to be inserted as well but the voter needs to guarantee that the verification code displayed on the computer screen is identical to the one displayed on the phone screen first). If everything is fine, the final window informs about the registration of the vote and exhibits a QR code. From the demo that one followed, a screenshot of this last window was taken and is visible in figure 11, and about which Florian Marcus informed that the QR code is made available for the voter to use it through his/her mobile phone in order to verify that the vote was correctly received through a different communication channel. This QR code is only valid for few minutes so by sharing it on the internet for everyone to see who the citizen voted for is not possible. Furthermore, to generate a new QR code, a new vote needs to be submitted.



Your vote is registered.

You can vote again electronically in order to change your choice.

Please close the application.

Figure 11 - Screenshot took during Florian Marcus’ demo of how to register an I-Vote through the I-voting application

In this process described above, the public key cryptography concept is present. As concluded in White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M. & Sperling, O. (2019), a study aborded in the literature review, “Voters encrypt their ballots with the public key of the election system, and then digitally sign them with their own private key.” The private key corresponds to the key for signature in the national ID card (PIN2 as mentioned) and, then, the electoral authority associates the voter with his/her public key.

In the last topic of E-Voting investigated in the literature review, some issues and challenges were listed. They were divided in "Legal Considerations", "Political Considerations", "Technological and security challenges – Human-related technological risks", "Technological and security challenges – Tech-related technological risks”, "Social Challenges", and other possible vulnerabilities that an electronic voting system can face. In order to comprehend how the Internet Voting system in Estonia adapted, one had the opportunity to have a conversation with Florian Marcus from the e-Estonia Briefing Centre and collect further information from a technical document "Mobile voting feasibility study and risk analysis" (Buldas, A., Heiberg, S., Krips, K. & Willemson, J. (2020)) and from a technical paper explaining the security considerations regarding the system (Heiberg, S., Laud, P., & Willemson, J. (2011)), published in the year when the number of votes cast in the Parliamentary elections over the internet among all votes reached 24.3%. Below, you can find a table where the issues and limitations of internet voting mentioned in the literature review are put side by side with the Estonian case.

European University Institute, Robert Schuman Centre for Advanced Studies, European Union Democracy Observatory – EUDO, Trechsel, A. (2016)	**Estonian I-Voting**
“Legal Considerations”	
“Digital Divide” is introduced here as the critical aspect: people who do not have access to the Internet would not be able to vote	People who do not have access to the Internet are able to vote on site (paper ballot voting).
Processes of counting the votes and checking who voted may be independent, ensuring “privacy and security”	There are two servers: Vote Storing Server (VSS) which stores the i-votes and anonymization of the i-votes before the tabulation. The Vote Counting Server (VCS) does the tabulation and is offline.
It may exist a legal basis for the adoption of this mechanism, so it can be adopted in more member states of the European Union.	In the chapter 7^1 *Electronic Voting* of the Riigikogu Election Act, that entered into force on 11.11.2012, a set of provisions are documented about the electronic voting. In the European Commission website, I-Voting in Estonia is recognized as a pioneer case.

“Political Considerations”	
Procedure of I-Voting may be “transparent, participatory, and involve all the relevant political actors and stakeholders”, so its implementation can be consensual and strong political consensus will motivate and increase confidence of citizens to use Internet Voting	The Estonian Election Acts have already a chapter dedicated to the all the procedures of voting and counting of I-votes. In 2019, for the European Parliamentary Elections, almost half of the voters used I-Voting to choose the Estonian members of the European Parliament.
Technological and security challenges – “Human-related technological risks”	
Citizens with lack of technical competencies to deal with remote I-Voting	The number of internet users in Estonia is significantly high, around 90% in 2017 (according to The World Bank), where internet users have used the Internet (from any location and any device) in the last 3 months). This relevant majority of the Estonian population who are familiar with Internet, makes the I-Voting process easier to understand and enhances its use.
Electoral officials missing technical skills to be able to control the I-Voting process in an effective way	The anonymization of i-votes can only occur in the presence of at least 2 election officials, an auditor and possible external observers. All procedures are defined beforehand in written form, and all actions and outcomes are recorded on tape. Without enforcing those regulations, the IVS owner could manipulate the election results on a large scale by adding or removing votes from the digital ballot box without getting caught.
Citizens’ assurance regarding secrecy and privacy of their votes	The citizen cannot assure by himself/herself the secrecy of the vote. However, the system uses the asymmetric encryption to guarantee the secrecy of voting. The use of the public key to encrypt the vote (but with no power to decrypt it) and the private key used to decrypt the anonymous votes, not associated to personal details of the voter, and never before the counting process, ensure the secrecy.
“Lack of transparency when voters cannot be sure whether their votes are correctly counted and stored”	A QR Code is made available for the voter to use it through his/her mobile phone in order to verify that the vote was correctly received through a different communication channel. This QR code is only valid for few minutes so by sharing it on the internet for everyone to see who the citizen voted for is not possible.

Possibility of intimidation or any other kind of enforcement against the voter’s will while casting his/her vote remotely	The solution is “You can vote again electronically in order to change your choice.” According to the *Riigikogu Election Act*, chapter 71, the “Change of electronic votes” provision states that the voter has the right to change his/her vote during a seven day-period.
If I-Voting becomes the only way of voting, a significant portion of the population may not be capable to vote and feel discrimination.	Paper ballot voting is another alternative to participate in elections.
Technological and security challenges – “Tech-related technological risks”	
“Possibility of system attack or breakdown, or connection failure”	The voting application is executed in malicious environment, where malware could manipulate its behaviour. Several weaknesses present in Estonian i-voting scheme were materialized. The analyzed events indicate real-life attacks that an i-voting system has to withstand. From these events we conclude that it is necessary to work toward new, more secure i-voting protocol. We need to reduce the level of trust required in the voter’s computer and provide the NEC with means to show that it could not act malicious even if it wanted to. It is possible that i-voting related legislation may be refined to meet these requirements.
Correct identification of the voter complexity	Voter’s identification is confirmed by asking the voter to submit his/her personal identification code. The credentials users by the citizen to authenticate can be “knowledge-based” – username/password and PIN, or physical authentication token (“chip card, SIM-card, etc.”) combined with a knowledge-based PIN. The identity of the voter is proven by the digital signature, and consists on the basis to take the i-vote into account.
“Provision of the preventive measures against multiple voting” and “transparency of tabulation”	The conciliation between electronic voting and paper ballot voting systems is reached. First of all, in case of several electronic votes submitted by the same voter, only the last one is taken into account. Then, in order to avoid misleading information, the State Electoral Office may send not later than two days before the election day to all "rural municipality or city secretaries" the list of voters who voted electronically by voting district. One day before the election day, all district committees may have access to this list. Regarding the electronic voting and traditional voting,

	the Act sets some rules to ensure the unique vote.
Voter’s personal computer can have virus and affect the system	As with the IVS (I-voting system) server’s side problems, there exist i-voting protocols which handle the problem of trusting voter’s computer. The Estonian i-voting scheme relies on the assumption that we can trust the owner of the IVS and we can trust voter’s computer. However, some measures to reduce the necessary trust have been taken. A detection system for known attack-vectors is built into IVCA (I-voting client application) and methods are used to complicate reverse engineering.
Social challenges	
“Social differences regarding who has a personal computer and internet at home” and “who is sufficiently technologically literate to be able to interact with an online voting platform”. Age, income level and literacy level are key components	Elderly people are actually using I-Voting (according to statistics available in the Valimised website, retrieved from *https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia*, 17% of I-Voters in the European Parliament elections 2019 belong to the age group >65 years old, for instance). The number of internet users in Estonia is significantly high, around 90% in 2017 (according to The World Bank, as mentioned previously).

Table 14 - Estonian I-Voting and how it overcomes issues and limitations identified in e-voting

The third and last pillar presented in the literature review was Blockchain and Blockchain-based E-Voting system. This algorithm architecture was studied as well as some issues and limitations. Regarding the application of Blockchain to an E-Voting system, one started by defining what the integration of this solution could add to a current existent electronic voting. It is known that in E-Voting the process to confirm who did not vote and tallying votes is faster and more reliable, at the same time that travel expenses and opportunity costs of a voter being present in the polling place in the election day can be highly reduced due to the introduction of E-Voting. Another important factor mentioned was the “mobilization effect” - people who had no incentive to vote before, can find a new option and become more enthusiastic, especially young people. However, the existent problems are associated with verifiability. To keep the votes anonymized in E-Voting, for voters to verify if their vote was registered successfully "without revealing who they voted for" and to decide the votes that are valid "without a privileged role", are some of the questions and challenges. In the paper written by Kovic, M. (2017), “e-voting carries the greatest risk”. In this sense, some Blockchain technology features were identified as capable to overcome and solve problems presented by E-Voting. In the book Xu, X., Weber, I., & Staples, M. (2019), the author defends “using a blockchain alone is not enough”. The ideal solution is the Blockchain-based E-Voting system.

In order to see the three mentioned challenges applied to the Estonian case scenario, one based the analysis over the paper written by Heiberg, S., Laud, P., & Willemson, J. (2011).

Keep the votes anonymized in E-Voting - ballot secrecy relies heavily on organizational procedures in the Estonian i-voting scheme. It is theoretically possible for the NEC (National Electoral Committee) not to anonymize i-votes and use a modified VCS to break the secrecy of all ballots. To break the secrecy of one ballot, it is sufficient to decrypt it separately from others and later analyse audit log-files.

Ability of voters to verify if their vote was registered successfully "without revealing who they voted for" – during the verification process, the application downloads the QR code information from the voting server, decrypts the votes so it can display the name of the candidate the voter voted for. Some attacks may occur at this stage, but by verifying the vote with the QR code together with the new verification method (smart card readers with PIN-pads and PIN-firewalls), malware attacks are avoided.

Decide the votes that are valid "without a privileged role" - The fact that the IVS auditing logfiles can link original voters to the hashes of the encrypted ballots means that if the invalid i-vote was indeed decrypted separately from other i-votes, the ballot secrecy would be protected only by organizational means. An IVS implementing a mix network-based anonymization system would have reduced the required trust in the NEC and allowed the analysis of invalid i-vote in a secure manner with respect to ballot secrecy.

Also, in order to understand what is the current opinion and perspective about the use of Blockchain integrated in Estonian I-Voting, in the conference “e-Estonia Live: i-Voting as key to future elections”, that took place on 18th June 2020, Florian Marcus, Digital Transformation Adviser e-Estonia Briefing Centre, made a question to Sven Heiberg, I-Voting Product Manager Cybernetica AS (company also known for the Internet Voting development):

While Estonia started to using Blockchain on a national level almost 10 years ago, I-Voting is not really associated with Blockchain implementation. Was there ever the thought of implementing Blockchain for I-Voting, maybe even right now, or for the future, and if not, why do you think is not necessary?

To this question, Steven Heirberg confessed that “using Blockchain on top of Online Voting system definitely crossed our minds”. Also, “we have looked into the properties and capabilities of Blockchain applications, such as Etherium or Bitcoin, and we have determined that it is not suitable for Online voting at this stand”. They are currently investigating a different model based on “private permissions”. However, a major argument for retarding the adoption of Blockchain is the fact that currently the Online Voting system relies on a “single component to store the information” and exists a “separation of duty and distribution of tasks” which is crucially in the current implementation architecture. Blockchain does not rely on a single component. Another important topic discussed was regarding Blockchain encryption. As stated by Steven Heirberg, “to go through Blockchain, we need a different kind of encryption and we need to consider every last thing towards we publish into the Blockchain” once exists the risk of the key length being “approachable to hackers” and, then, “we might be linking historical voting results is possible to make a link once this key is saved for years”. The remaining discussion can be read in appendix 9.

4.5. Discussion/ Key Learnings

As a matter of fact, Estonia was the first country to announce the electronic voting adoption in 2001. This achievement brings great responsibility and it was the first country to establish a legal procedure in the adoption of E-Voting. In order to comply with legal requirements, the Riigikogu Election Act was introduced in June 2002 and "assumed legal effect on 18 July 2002". Once this is a technology in continuous development, also the law needed to adapt and change. According so, with the Organization for Security and Co-operation in Europe (OSCE) mission report in 2011 presented a set of recommendations and, at that time, also the Electronic Voting Committee was created. All these events contributed in a way or another to the continuous update of the Act. According to this study, the last time the Act was changed was in 2016, with "legal effect on 1 January 2017". Furthermore, the Electronic Voting discussed during this dissertation makes part of one of the public services provided by the government. Generally speaking, one considered the E-Government Development Index (EGDI) from 2020, that assesses the e-government development at national level, calculated based on the average value between three components (Online Service Index, Telecommunication Infrastructure Index and Human Capital Index). In the year of 2020, Estonia is in 3rd place in the world ranking and in 2nd place in the European ranking, a notable very high EGDI, according to this mentioned report issued by the Department of Economic and Social Affairs of United Nations. Estonia was also the country at world scale which recorded the most significant increase since the EGDI registered in 2018. Regarding the e-Participation Index 2020, Estonia is considered the country in the world that performs better in the provision of information to citizens, consultation and decision-making, knowing how to promote socially inclusive governance.

Being a pioneer of I-Voting adoption worldwide, together with the fact that it is considered one of the fastest raising countries for digital transformation in the world, one believes that this country is a good case-study for Portugal. However, there are factors that may be reflected and analysed in a possible application in the Portuguese framework. Before starting with the set of recommendations in this sense, that will be highlighted in the chapter 5.2, one will focus on the discussion of the I-Voting limitations.

In order to create trust and confidence in such a way that citizens take the initiative to adopt Internet Voting, there are several factors to be taken into account. Existing adequate and transparent voting procedures, good coordination between different voting bodies involved, technical requirements that guarantee all the credibility of the system from the front to back end ("end-to-end verifiable"), are basic requirements that will influence the propensity of citizens to vote online. However, keeping the anonymization of i-votes, guarantee the verifiability of the successful registration of the i-vote without revealing the output, tallying the votes that are valid without privileges usage, and susceptibility to system attack, breakdown or connection failure, are the limitations that were not completely overcame and may lead to lack of confidence on citizens behalf. This affirmation is based on the paper "The Application of I-voting for Estonian Parliamentary Elections of 2011", Heiberg, S., Laud, P., & Willemson, J. (2011), where two real problems related to the i-Voting application were reported and are analysed. The first one was related to an "Invalid I-vote" in 2011, during the tabulation phase of the Riigikogu Elections. In paper voting there are plenty of invalid votes, while in the case of the I-Voting Client Application, the casting of one invalid vote means that the application was manipulated. Possible causes were raised, such as a bug (either in the Client Application, or Forwarding Server, or Vote Counting Server), a human mistake (incompatible candidate lists on the counting server and forwarding server), or someone that intentionally casted an invalid i-vote. After reviewing the code and performing some tests, the bug possibility was disregarded, and the possible cause of an intentional spoiled vote was considered. However, the root cause is unknown. Also, the involvedness of the NEC (Estonian National Electoral Committee) and the fact that the ballot secrecy is highly dependent from this body (it is technically possible for them to do not anonymize these votes and break the secrecy). Another real problem faced was the "Student's attack". A student named "P." emailed NEC claiming that designed a prototype of an election rigging malware, capable of manipulating the voter to believe that he has voted for his election candidate, although the malware actually voted for another candidate. By analysing the election logs, the longest session registered came from P. Also, all sessions created while P. was voting, were marked as suspicious. Later on, the source code was made available by P. at the same time the Electoral Committee claimed that the malware was detected. Without giving up, P. claimed that was able to do the same procedure, but for selected candidates in order to favour one over the others. NEC replied again stating that no attempts to attack the I-Voting Server have occurred. Summing up, this potential attack brought up the fact that the detection system implemented is not enough and only indicates if some kind of malware is occurring, it doesn't prevent it. There are several alerts detected and visible in the logs, but the absence of countermeasures against voter disenfranchisement attack (taking away the right to vote from a citizen) is the main weakness of this detection system. Also, nobody from the NEC analysed the logs timely.

In a paper named "Secure I-Voting System with Modified Voting and Verification Protocol", by Ajish, S., & Anil Kumar, K. S. (2020), the security weakness of relying only on the PIN stored in the national ID card is identified. The attacker can easily re-vote by using Re-voting Malware (PIN in the national ID card is collected and later when the voter uses the ID card for other use, the malware casts the vote), and can cast any vote from any voter he/she wants by using Self-voting Malware (once the voter's device makes part of a botnet, administrated by the malware, it records the PIN code and then cast the vote without the voter's awareness). Also, the vote change is not reflected in the vote verification application – Vote Modification Malware. For these two situations, the authors tested the inclusion of OTP, One-Time Password, to prevent the Re-voting and Self-voting malwares. On the other hand, to prevent a fake verification of the vote, they also propose the use of the private key of the server to digitally sign the vote. In order to present a product that is more secure than the current Estonian I-Voting system, the authors analysed theoretically and technically the major client-side attacks in the Estonia i-voting system: Vote Modification Malware (VMM), Re-Voting Malware (RVM) and; Self-Voting Malware (SVM). Consequently, they tested and validated the security of a modified voting and verification protocol.

Modified Voting Protocol	Once the candidate list is made available in the app, the voter makes his/her choice and it is generated a random number. The Modified protocol uses instead an OTP that is sent to the voter's phone by the VSS. Then, once the voter inserts the OTP in the application, the voter applications pads the OTP and the candidate, and encrypts it with the server's public key. Prevents the Re-Voting and Self-Voting Malware attacks. In this modified protocol, the vote is not casted in the background. In case of attack, with the OTP, the voter knows that the malware is present.
Modified Verification Protocol	The encrypted vote is digitally signed by the VSS's private key before it is sent to the verification application, so the hacker cannot modify the vote at this stage. In this modified protocol, the voter should verify the vote so it can be accounted in the VSS. Also, the VCA and verification application may run on different devices. There is a two-level security offered by the VCA: using the PIN and OTP. The cryptogram includes the OTP, so the voter can check it and make he/she is verifying the vote and make sure it belongs to him/her. A third-level is ensured by the encryption of the cryptogram by using the private key of the server before it is forwarded to the verification application.

Table 15 - Modified Voting and Modified Verification Protocols (Ajish, S., & Anil Kumar, K. S. (2020))

Learning from the known Estonian success case, not only about the growing I-Voting adoption rates among the voting population, but because of what triggers it: transparent voting procedures, good coordination between different bodies involved and technical requirements that guarantee system's credibility. Moreover, learning from the potential security weaknesses presented and from academics and other experts that suggest system development improvements, Portugal can take a step forward in the implementation of a solid and credible solution that will incentivise and benefit the population.

5. RECOMMENDATIONS FOR PORTUGAL

So far, the select case, design data collection protocol, conduct case study and write individual case report phases were fulfilled across the previous chapter. Right after, one may draw cross-case conclusions, modify theory, develop policy implications and, finally, write the cross-case report. These last phases will be developed across this chapter exclusively for the Portuguese case.

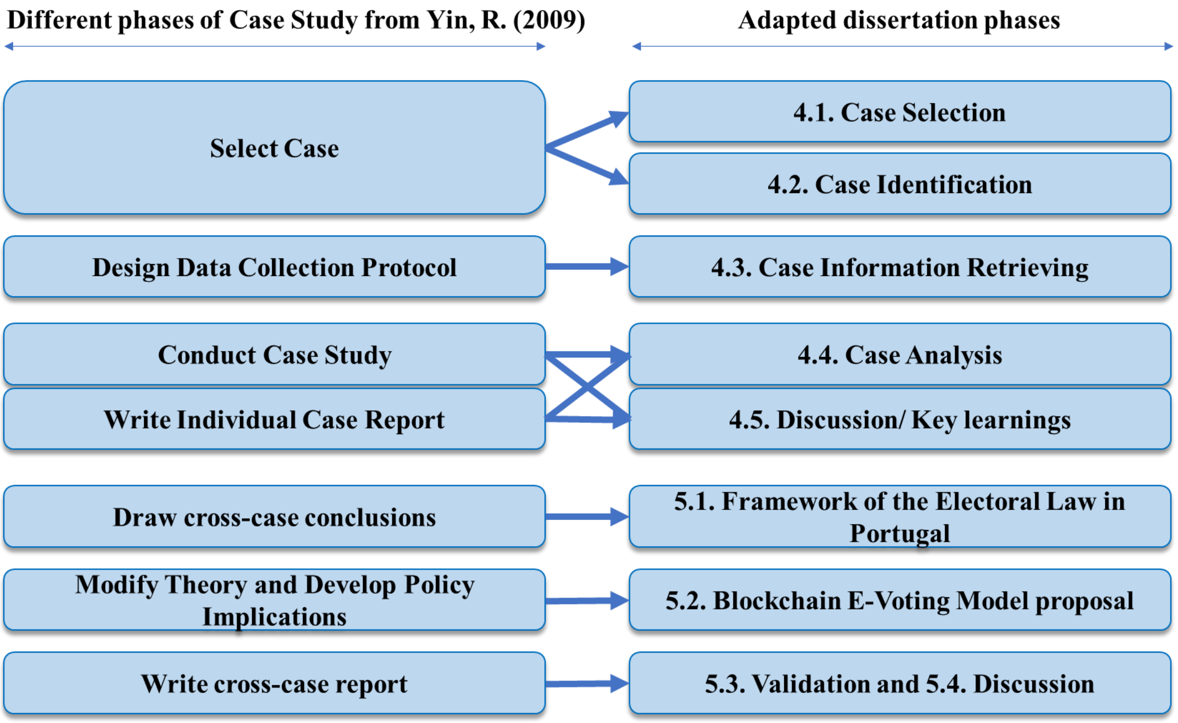

Different phases of Case Study from Yin, R. (2009)
Adapted dissertation phases
Select Case
4.1. Case Selection
4.2. Case Identification
Design Data Collection Protocol
4.3. Case Information Retrieving
Conduct Case Study
Write Individual Case Report
4.4. Case Analysis
4.5. Discussion/ Key learnings
Draw cross-case conclusions
5.1. Framework of the Electoral Law in Portugal
Modify Theory and Develop Policy Implications
5.2. Blockchain E-Voting Model proposal
Write cross-case report
5.3. Validation and 5.4. Discussion

Figure 12 - Dissertation phases based on Yin, R. K. (2009) methodology

5.1. Framework of the Electoral Law in Portugal

As already explored previously, the lack of legal acceptance is considered a major limitation regarding the adoption of Blockchain. In the "E-Voting and Blockchain" chapter, some of the problems in the paper ballots are solved with the introduction of Electronic Voting devices and, in its turn, Blockchain is capable to overcome security issues related E-Voting as studied before.

In Portugal, despite of some initiatives for the exploration of Blockchain applications and modernization of the current electoral procedures, the political legislation and electoral law are still resistant to the technological potential. For the purpose of this dissertation, it matters to understand the critical articles documented in the Electoral Legislation, divided according to the political body to be elected (Electoral Law for the Republic President, Republic Assembly, Local Authorities and European Parliament elections, mainly). From this documentation, one will explore the articles that may describe better how the Portuguese electoral law works and if exists any challenge to the adoption of and Electronic Voting system and/or Blockchain. They are grouped by the corresponding theme: early vote; localization; voting method; vote secrecy; requirements to exercise the right to vote; supervision at polling stations; counting of votes; disabled voters; doubts, complaints, protests and against protests and, last but not least; legal violations when voting and associated punishment. The paragraphs below resume important topics about the crucial articles that matter to be analysed for the purpose of this dissertation. It is a similar analysis as the one performed in the sub-chapter 4.2. Case Identification, where the provisions with all the procedures that may be followed prior and during the electronic voting in Estonia were documented.

In the table below, one took as example the Assembly of the Republic Electoral Law. The President of the Republic Electoral Law is similar in most of the articles referenced.

Nº	Article	Description
40	Polling stations	One polling station per parish. (>1500) electors: number of electors shall be divided into polling station sections Details may be communicated by the mayor to the parish council by the thirty-fifth day before election day
40.B	Mobile advance polling stations	At least one station in the chief municipality of a constituency (in Autonomous Region of Madeira two stations, in Autonomous Region of Azores, nine stations, one per island). If no voters have been registered in one municipality, the mayor may order that it will be exempted from operation. The number of voters per station if significantly exceeds 1500, the mayor may determine the necessary divisions so this number doesn't exceed too much.
42	Location of polling stations	Public buildings (schools or seats of municipal councils or parish councils) offering capacity, security and access. Private buildings shall be requisitioned in case needed.
79	Casting a vote	Only the registered elector has the right to cast his/her vote. The vote can only be casted in person or by post (in the case of electors residing abroad).
79.B	Advance voting	Not everyone can vote in advance. There is a list in which circumstances an elector can cast his/her vote in advance.
82	Secret ballot	Nobody can be obliged to disclose their vote or be asked about it by any authority (save in the case of unidentifiable statistical data collection). No one may reveal which list they voted or are going to vote for (both inside and outside of the polling station, withing a distance of five hundred meters outside).
83	Requisites for exercise of the right to vote	The voter may be registered in the electoral roll book and his/her identity must be recognized by the board of officers.
84	Location in which the right	The vote only be exercised at the electoral station that corresponds to the location for which the elector is registered (save in the case of advance voting).

	to vote is exercised	
88	Voting order	Electors vote in the order in which they arrive at the polling station and may exercise their right to vote as soon as they present themselves and display the respective writ of appointment or credential.
89	Continuity of electoral operations and closure of voting	Voting operation is concluded as soon as all the registered electors have voted or, if it is past 7 p.m., as soon as all the electors who are present inside the polling station have voted.
95	Voting slips and templates in Braille	Voting slips shall present all the lists that are being put to the vote in each constituency to fit on them, and shall be printed on a blank sheet of paper. Braille templates of the voting slips, in all respects identical to these and with spaces corresponding to the squares of the competing lists, are produced.
96	Manner in which each elector votes	First, the voter gives his/her identification document to the president of the table (can an identification document other than the citizenship card). Secondly, once the voter has been identified, the presiding officer says the name and civil identification number aloud and, after checking the registration, gives them a voting slip. Voter, alone in the polling station, marks a cross in the respective square of his/her choice. In the ballot table, voter gives the paper to the president who puts in the ballot right after and other officer registers in the paper that that elector had voted. If a voter accidentally spoils the voting slip they must ask for another one from the presiding officer, and give back the first one.
97	Voting by disabled persons	Elector who is affected by an obvious illness or physical disability shall vote while accompanied by another elector of his choice.

98	Blank and null votes	Blank votes - no mark of any kind has been made on the voting slip. Null votes - more than one square has been marked or there are doubts about which square was marked; when the voter votes for a list that is no longer running in the elections; any cut, drawing, written words or tear has been made. In the case of advance voting or by post, votes are considered null when they do not arrive to the destination or the envelope has not been properly closed.
99	Doubts, challenges, protests and counter-protests	Any elector who is registered at a polling station and any of the delegates for lists may raise doubts and lodge written challenges, protests or counter-protests
101	Counting voters and voting slips	The electors that were marked in the electoral roll books along the day are counted. Once the number is known, the presiding officer shall order the opening of the urns and the counting of the slips. In case number of electors is different than number of slips, the latter number must be considered for counting purposes. The number of voting slips may be of public knowledge.
102	Counting votes	One of the scrutineers shall unfold the slips one by one, and shall announce out loud which list has been voted for. The other scrutineer shall separately record on a blank sheet of paper or preferably on a clearly visible board. The presiding officer together with another scrutineer group the votes into separate batches corresponding to each of the lists that have received votes, blank votes, and null votes. The presiding officer counter-check the counting of the votes in each batch after the steps above. Delegates for lists have the right to subsequently examine the separate batches of voting slips and ask for clarifications and/or protest before the presiding officer. Once the final count is concluded, the results may be known and affixed to the main door.
146	Violation of voting rights	Anyone who is not eligible to vote and presents himself/herself voting, will be punished with a fine of 500 to 5,000 escudos. If a citizen takes the identity of a registered elector will be punished with six months to two years imprisonment and a fine ranging from 20,000 to 200,000 escudos.

150	Disloyal agents	Anyone who accompanies a blind or disabled person to vote and willfully expresses the latter's wish in a manner that is not faithful thereto shall be punished by a prison term of between six months and two years and a fine of between five thousand and twenty thousand escudos.
151	Breach of voting secrecy	Anyone who in, or within the five hundred meters immediately around, a polling station enforces another voted to get to know in which list he/she voted for, shall be punished by a prison term of up to six months. Anyone who says who voted for in or within the 500m immediately around the polling station shall be punished by a fine of between one hundred and one thousand escudos.
152	Coercion and fraudulent artifice in relation to electors or candidates	In case anyone who employs any kind of violence or threat over an elector in order to persuade him to vote for a given list or to withdraw from standing for a given list shall be punished by a prison term.

Table 16 - Assembly of the Republic Electoral Law main articles for this dissertation (Lei Eleitoral da Assembleia da República 2020 (LEAR))

After getting to know more about the Portuguese electoral law, some questions regarding the Internet Voting procedure are raised. The following questions are based in some of the main articles described above and the respective answers are based on the information presented in the table of chapter 4.2. Case Identification. The purpose of this table is mainly to do a cross information about legal aspects between the Portuguese articles and how they are transcribed in the Riigikogu Election Act, specifically in the Electronic Voting articles.

Article	Question	Answer
Polling stations	What details are communicated/prepared prior to any election in the case of I-Voting?	State Electoral Office has a crucial role as organizer: receives the amendments to the list of voters at least once a day and must organize these entries at the same time frequency; ensure and inform about the operating systems compatible with the voter application; creation of the encryption key for electronic votes and the vote-opening key; guarantee support to visually impaired citizens in the voter application usage; publish the voter application, votes verification application and the authenticity and integrity of the website information. All these procedures may be completed not later than by the thirteenth day before election day.
Location of polling stations	Where is the location of polling stations in I-Voting and paper voting?	Any voter's computer with an operating system compatible with the Voter application. Also guarantee the installation of the vote's verification application and the authenticity and integrity of the website information. Voting in custodial institutions, hospitals and twenty-four-hour social welfare institutions, in the case of in person voting.
Advance voting	How is advance voting processed in the case of I-Voting and paper voting?	Any voter who installs the required applications to cast the vote can do it between the tenth and fourth days before the election day, twenty-four hours a day and closing at 6 p.m. The voter has the right to change his/her vote during the seven day-period mentioned before. It is also possible to change from Electronic Voting to ballot paper voting, during the same seven day-period for the cases of Advance voting
Exercise of the right to vote	What are the requisites to exercise the right to vote?	State Electoral Office, as organizer, receives the amendments to the list of voters at least once a day and must organize these entries at the same time frequency. This is done prior to the election day.

Voting order	What is the voting order and the manner in which each elector votes?	The list of candidates is then displayed to the voter after his/her identification. The candidate is chosen, the vote is encrypted with the vote-encryption key and the digital signature is used to confirm the vote. The E-Voting procedure ends with the notice displayed to the voter, confirming the voting is done.
Manner in which each elector votes	In case there are any problems with electronic voting, what are the procedures to be followed by the National Electoral Committee?	Suspension of electronic voting à the National Electoral Committee must notify voters and ask to restart the electronic voting; Not starting or termination of electronic voting à the National Electoral Committee must notify voters and provide the alternative to electronic voting; Suspension or termination of electronic voting and the National Electoral Committee must notify voters about the necessity to vote again and provide the alternative to electronic voting.
Counting votes	How is processed the counting of votes?	The conciliation between electronic voting and paper ballot voting systems is reached. First of all, in case of several electronic votes submitted by the same voter, only the last one is taken into account. Then, in order to avoid misleading information, the State Electoral Office may send not later than two days before the election day to all "rural municipality or city secretaries" the list of voters who voted electronically by voting district. One day before the election day, all district committees may have access to this list. In case a voter voted electronically and ballot paper, only the ballot paper vote is taken into account.

Table 17 - Portuguese articles and how they are transcribed in the Riigikogu Election Act

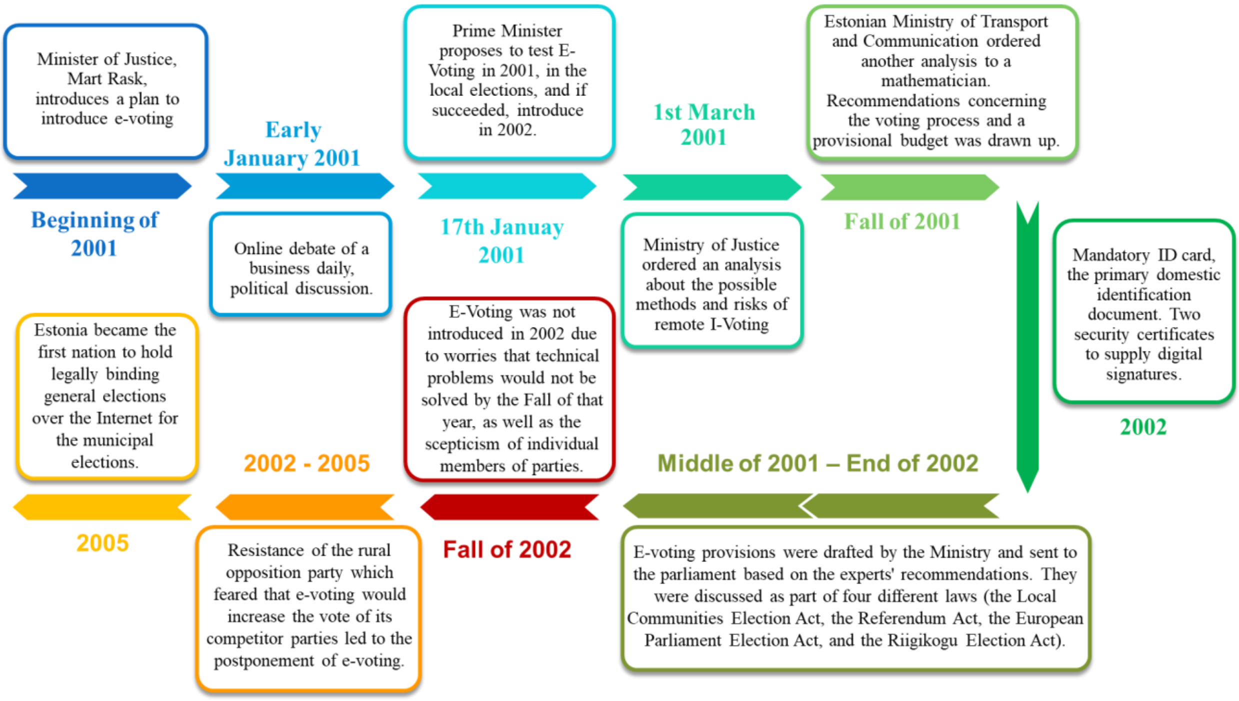
5.2. Recommendations and/or Blockchain E-Voting Model Proposal

In the previous sub-chapter, one presented the main articles documented in the Portuguese Assembly of the Republic Electoral Law. Consequently, it was possible to do a cross information between the Portuguese and Estonian electoral law on the main articles. Hereupon, it remains to analyse and describe how and if a Blockchain E-Voting Model could be implemented in the Portuguese framework.

First of all, independently of the technology used, the possibility of voting remotely (via Internet), implies by itself major changes and several amendments and adaptations to the Portuguese scenario.

Currently, as already mentioned before, it is only allowed paper voting, by post (in the case of residents abroad) and the last pilot project conducted in the district of Évora where voting machines were made available for the first time in the polling stations. The possibility of voting anywhere, only by turning on a computer and submitting the vote through an application, requires not only legal changes, as well as political agreement, social knowledge and engagement, technical expertise and consequent technical development. All of these aspects are addressed in the sub-chapter 4.4. Case Analysis, where the issues and limitations of internet voting mentioned in the literature review are put side by side with the Estonian case. We may depart from these examples but adapted to the Portuguese scenario. Thus, one may be able to understand upfront what major aspects may be taken into consideration in the implementation of a solution and make recommendations based on the success and failure points of the case study of this dissertation. At the same time, in the sub-chapter 4.5. Discussion/ Key Learnings, two real problems faced in Estonia were described, as well as two possible solutions presented in the paper named "Secure I-Voting System with Modified Voting and Verification Protocol", by Ajish, S., & Anil Kumar, K. S. (2020). The proposed protocols are integrated in the set of recommendations.

First of all, one may reflect about the genesis of E-Voting in Estonia, the case-study of this dissertation. In the sub-chapter 4.1 Case Selection, it was already mentioned that Estonia announced in 2001 the adoption of electronic voting and the increased responsibility to this nation become the first one establishing a legal procedure in the adoption of Electronic Voting that was introduced one year later: the Riigikogu Election Act. Considering the technology subject to frequent maintenance and development, the legal act has been amended and many changes will step into force in 2021. These events are important to understand before introducing a similar technology in Portugal. Hence, the following chronology figure resumes the important events taken until the implementation of I-Voting, legally, politically and technically.



Beginning of 2001

Minister of Justice, Mart Rask, introduces a plan to introduce e-voting

Early January 2001

Online debate of a business daily, political discussion.

17th Januay 2001

Prime Minister proposes to test E-Voting in 2001, in the local elections, and if succeeded, introduce in 2002.

1st March 2001

Ministry of Justice ordered an analysis about the possible methods and risks of remote I-Voting

Fall of 2001

Estonian Ministry of Transport and Communication ordered another analysis to a mathematician. Recommendations concerning the voting process and a provisional budget was drawn up.

2002

Mandatory ID card, the primary domestic identification document. Two security certificates to supply digital signatures.

Middle of 2001 – End of 2002

E-voting provisions were drafted by the Ministry and sent to the parliament based on the experts' recommendations. They were discussed as part of four different laws (the Local Communities Election Act, the Referendum Act, the European Parliament Election Act, and the Riigikogu Election Act).

Fall of 2002

E-Voting was not introduced in 2002 due to worries that technical problems would not be solved by the Fall of that year, as well as the scepticism of individual members of parties.

2002 - 2005

Resistance of the rural opposition party which feared that e-voting would increase the vote of its competitor parties led to the postponement of e-voting.

2005

Estonia became the first nation to hold legally binding general elections over the Internet for the municipal elections.

Figure 13 - Events that marked the implementation of I-Voting in Estonia (Drechsler W., Madise Ü. (2004))

The Constitution of 1992 was revised with the drafts and amendments done to the four different electoral laws. Also, in this case-study, it matters to say that was the political elite which started with the e-voting initiative and not the general population.

Right below, a set of Recommendations are listed based on the Legal Considerations, Political Considerations, Technological and security challenges – Human-related technological risks, Technological and security challenges – Tech-related technological risks and Social challenges, that were previously presented in the case discussed in this dissertation.

"Legal Considerations"	
"Digital Divide" is introduced here as the critical aspect: people who do not have access to the Internet would not be able to vote	**Portuguese Reality**
	Currently, only paper ballot voting and by post (in the case of electors residing abroad) are allowed.
	Recommendation
	Similar to the Estonian case, people who do not have access to the Internet would be able to vote on site (paper ballot voting).

Processes of counting the votes and checking who voted may be independent, ensuring “privacy and security”	**Portuguese Reality**
	According to the “Counting voters and voting slips” and “Counting votes” articles, under the Portuguese Electoral Law, the electors that were marked in the electoral roll books are counted after the voting closure. After known the number of voters, the slips are counted. For counting purposes, only the number of slips is considered and it may be publicly known. Regarding the counting votes process, the voting slips are separated into batches according to the different lists. These storing and counting processes (number of electors and voting slips, as well as votes per list) can be translated in two different servers.
	Recommendation
	In the case of Estonia, Vote Storing Server (VSS) which stores the i-votes and anonymization of the i-votes before the tabulation and the Vote Counting Server (VCS) does the tabulation and is offline.
It may exist a legal basis for the adoption of this mechanism, so it can be adopted in more member states of the European Union.	**Portuguese Reality**
	The electoral procedure in Portugal is supported by the different Electoral Law acts published in the Portuguese Electoral National Committee website. In the case of adopting electronic voting, a set of articles and/or chapter(s) shall be documented in the respective legal acts.
	Recommendation
	An English version shall be available, as well as a communication about the E-voting adoption to the European authorities.
“Political Considerations”	
Procedure of I-Voting may be “transparent, participatory, and involve all the relevant political actors and stakeholders”, so its implementation can be consensual and strong political consensus will motivate and increase confidence of citizens to use Internet Voting	**Recommendation**
	A legal revision of the Portuguese Electoral Law may be executed and some articles and amendments may be drafted in order to present a plan to the Government. An analysis about the provisional budget and possible methods and risks may be drawn up. After both legal, economic, social and technological considerations, a plan may be debated and voted in the Parliament. A strong consensus between different political parties and a clear communication to the Portuguese citizens about the process may be outlined.

Technological and security challenges – "Human-related technological risks"	
Citizens with lack of technical competencies to deal with remote I-Voting	**Recommendation**
	The percentage of internet users in Portugal was around 75% in 2019 (according to the World Bank), where internet users have used the Internet (from any location and any device) in the last 3 months). This relevant majority of the Portuguese population who are familiar with Internet, makes the I-Voting process easier to understand and enhances its use.
Electoral officials missing technical skills to be able to control the I-Voting process in an effective way	**Portuguese Reality**
	In the case of the Assembly of the Republic Electoral law, the candidates or agents of the different lists shall send to the mayor of the city details of the delegates and alternates for the respective assemblies and polling stations. Therefore, an officer is nominated by each list to the polling station and section. These delegates and officers nominated do not require any technical and/or technological specialized skill to control the voting process.
	Recommendation
	In case of introducing Electronic Voting, the technical skills required to deal with informatic systems and manage the E-Voting process demand different or more skilled human resources. Observing E-Voting requires these computational skills and understanding of the cryptographic protocol. In the example of Estonia, the anonymization of i-votes occurs in the presence of at least 2 election officials, an auditor and possible external observers. All procedures are defined beforehand in written form, and all actions and outcomes are recorded on tape. Without enforcing those regulations, the IVS owner could manipulate the election results on a large scale by adding or removing votes from the digital ballot box without getting caught.

Citizens’ assurance regarding secrecy and privacy of their votes	**Portuguese Reality**
	In the current Portuguese electoral process, the paper ballot voting also carries the risk of keeping citizens’ secrecy and privacy of their votes. They can both be violated in case the voter decides to reveal which list he/she voter for, when an authority agent asks or tries to obligate the voter to reveal who voted for, and/ or anyone who employs any kind of violence or threat over an elector in order to persuade him to vote for a given list or to withdraw from standing for a given list. All these scenarios (breach of voting secrecy and violation of privacy through violence or threat over electors), is punished by a fine or a prison term, respectively. However, the fact that in the paper ballot voting the citizen is isolated in the moment that votes and is observed when inserts the paper in the urn is undoubted. This situation provides confidence and helps the voter to assure the secrecy of voting.
	Recommendation
	In E-Voting, the citizen cannot assure by himself/herself the secrecy of the vote. Further knowledge about how the system works (asymmetric encryption and the use of the public and private keys) is required in order to know how the secrecy is ensured. A simple notation may be used in order to explain the general population how the e-vote will not be associated to any personal details, ensuring the secrecy.
“Lack of transparency when voters cannot be sure whether their votes are correctly counted and stored”	**Portuguese Reality**
	According to the current Portuguese voting system, this lack of transparency is present once the counting and storage is executed at closed doors. The number of votes and the election results are publicly known, but if a citizen wants a guarantee that his/her vote was correctly counted, it is not possible.

	Recommendation
	Taking as example the Estonian case, a QR Code is made available for the voter to use it through his/her mobile phone in order to verify that the vote was correctly received through a different communication channel. This QR code is only valid for few minutes so by sharing it on the internet for everyone to see who the citizen voted for is not possible. This way, any citizen can verify if his/her vote was correctly stored. According to Ajish, S., & Anil Kumar, K. S. (2020), the Modified Verification Protocol would be able to add another level of security while the voter verifies its vote with the QR code.
Possibility of intimidation or any other kind of enforcement against the voter's will while casting his/her vote remotely	**Portuguese Reality**
	It is only possible to intimidate or threat a voter in order to change his/her intention to vote before or after voting. The truth is that only the citizen can cast the vote in private, choosing the list/candidate he/she actually wants to vote for. Also, this kind of intimidation behaviour over another is punishable in the eyes of the electoral law, as discussed earlier.
	Recommendation
	In the case of voting remotely, the possibility of changing the electronic vote during a seven-day period guarantees that the voter can vote safely in another time. Also, the voter can always go to the polling station on the election day. In Portugal, the advance voting period (between the 14th and 10th days prior to that of the election) could coincide with the remote voting period, so the election day would be exclusively dedicated to the voting in polling stations.
If I-Voting becomes the only way of voting, a significant portion of the population may not be capable to vote and feel discrimination.	**Recommendation**
	Paper ballot voting is another alternative to participate in elections.

Technological and security challenges – “Tech-related technological risks”	
“Possibility of system attack or breakdown, or connection failure”	**Portuguese Reality**
	There is no technology involved in the voting and counting processes. However, both can be attacked or suffer any kind of irregularity (wrong counting of votes, a person votes on behalf of another, either on purpose by making use of the citizen card and voter number, or due to an error in the registration of the elector name by an officer).
	Recommendation
	In the case of remote voting, all anomalies are related to technology. It can happen that the voting application is executed in malicious environment, where malware could manipulate its behaviour. Through logs, it is possible to analyse events that indicate real-life attacks. From these events, the responsible people for the application maintenance can work toward new, more secure protocols. Other important topics are to find mechanisms to reduce the level of trust required in the voter’s computer, and provide the Electoral Committee with means to show that it could not act malicious even if it wanted to. The electoral legislation may be updated with these requirements.
Correct identification of the voter complexity	**Portuguese Reality**
	According to the article “Requisites for exercise of the right to vote”, the voter may be registered in the electoral roll book and his/her identity must be recognized by the board of officers. His/her identify is recognized by presenting and displaying to the officer the respective writ of appointment or credential (citizen card).
	Recommendation
	The voter may also be registered in the electoral roll book and his/her identification is confirmed by asking the voter to submit his/her personal identification code. The credentials users by the citizen to authenticate can be “knowledge-based” – username/password and PIN, or physical authentication token (“chip card, SIM-card, etc.”) combined with a knowledge-based PIN. The identity of the voter is proven by the digital signature, and consists on the basis to take the vote into account.

“Provision of the preventive measures against multiple voting” and “transparency of tabulation”	**Portuguese Reality**
	According to the article 84 “Location in which the right to vote is exercised”, Portuguese electors can only exercise the vote at the electoral station that corresponds to the location for which the elector is registered (save in the case of advance voting). It is required coordination between bodies that manage the voters enrolled to vote in advance and the ones enrolled to vote on the election day, so double voting is impossible.
	Recommendation
	Under the Estonia’s electoral law, the conciliation between electronic voting and paper ballot voting systems is reached. First of all, in case of several electronic votes submitted by the same voter, only the last one is taken into account. Then, in order to avoid misleading information, the State Electoral Office may send not later than two days before the election day to all "rural municipality or city secretaries" the list of voters who voted electronically by voting district. One day before the election day, all district committees may have access to this list. Regarding the electronic voting and traditional voting, the Act sets some rules to ensure the unique vote. According to Ajish, S., & Anil Kumar, K. S. (2020), with the Modified Voting Protocol, the re-voting is also prevented with the introduction of an OTP that is sent to the voter’s phone by the VSS. The voter inserts right after the OTP in the application, the voter’s application pads the OTP and the candidate and encrypts it with the server’s public key.
Voter’s personal computer can have virus and affect the system	**Recommendation**
	As with the IVS (I-voting system) server’s side problems, there exist i-voting protocols which handle the problem of trusting voter’s computer. The Estonian i-voting scheme relies on the assumption that we can trust the owner of the IVS and we can trust voter’s computer. However, some measures to reduce the necessary trust have been taken. A detection system for known attack-vectors is built into IVCA (I-voting client application) and methods are used to complicate reverse engineering. With the same modified protocol presented in the previous recommendation, the Self-Voting malware can also be avoided with the OTP usage.

Social challenges	
“Social differences regarding who has a personal computer and internet at home” and “who is sufficiently technologically literate to be able to interact with an online voting platform”. Age, income level and literacy level are key components	**Portuguese Reality**
	The number of internet users in Portugal is significantly high, around 75% in 2019 (according to The World Bank, as mentioned previously). Also, according to Pordata, around 84.5% of the Portuguese households have an internet connection at home, while 71.5% have a computer (2020). Regarding age, over 90% of citizens between 16- and 44-years old use internet, while in the age group of between 55 and 64 years old this number decreases to 65.3% and to 39% in citizens older than 64 years old (2020). When it comes to the percentage of those who use a computer, the numbers are lower in all groups (2017).
	Recommendation
	Considering that the majority of Portuguese citizens have access to a computer and internet connection, one can say that are social and technological conditions to proceed with the implementation of an Electronic Voting system in Portugal.

Table 18 - Recommendation for Portugal based on the Estonian experience

5.2.1. Critical Analysis considering Blockchain Architecture

So far, the discussion, key learnings and recommendations regarding the Portuguese framework were based on the case-study’s methodology developed in this dissertation. The Estonia’s I-Voting system was selected as the case of study due to three main arguments: the first nation to hold legally binding general elections over the Internet for the municipal elections in 2005, the first country worldwide to use internet voting in the Parliamentary Election and, finally, the adaptability of the new system with the traditional one in order to facilitate the voter’s understanding of its process. However, one has learnt about the Blockchain architecture, its applicability in e-voting, the blockchain applications in Estonia (apart from the e-voting system), and it matters to analyse its viability to integrate in a possible Portuguese e-voting solution.

First of all, one may analyse if and why a Blockchain-based e-voting system is “more secure and anonymous” than other voting systems. As investigated in the chapter 2.3.5. E-Voting and Blockchain, the privacy of the votes is kept due to the decentralized system without a third-party involved and the use of an ID instead of the real identity. Another reason is the difficulty of forge the votes due to the Distributed Ledger Technology (DLT) model that ensures security. Not less important, the ECC model guarantees non-repudiation, and, finally, the possibility of changing the final vote is also possible due to a withdrawable model as designed and defended in Yin, H. (2019), which is similar to the voting model.

Secondly, one will revisit what happens in the Estonian model. Regarding decentralization, this system is not decentralized, as well as there is a third-party involved (the National Electoral Committee). Also, each voter may use his/her PIN1 and PIN2, besides the ID-card or mobile-ID. In the case of Blockchain integration, there is also an ID as said before, but this is randomly assigned to the voter, and in order to proceed with the asymmetric encryption, the private key is generated by the voter and the public one is computed also by the voter. Then, no ID-card is used in order to the voter authenticate (no real identity). On the other hand, this technology does not depend from the trust in an electoral body (third-party) involved, once it is a decentralized network. Both facts are also capable of overcoming two of the limitations mentioned in chapter 4.4. Case Analysis: “Keep the votes anonymized in E-Voting” and “Decide the votes that are valid without a privileged role”.

Concerning non-repudiation and difficulty of forgery of votes that are avoided by the ECC model and DTL model, respectively in the Blockchain technology, in the case of the Estonian’s system both security properties are not guaranteed at the same level.

On one hand, the potential of forgery is mitigated due to the digital signature infrastructure. During the tabulation phase, forgery of the voting result can be identified. There is a countermeasure based on the audit procedure, “which involves retabulating the votes and comparing the result with the published one”. However, taking into consideration a possible attack that starts in the VSS while it is online (during the voting period, and not during the tabulation phase when it is offline), the set of encrypted votes sent to tabulation can be replaced by the malicious VSS. Right after, the set of forged votes would be used as basis for audit log forgery. According to Heiberg, S., Martens, T., Vinkel, P., & Willemson, J. (2017), there is no audit implemented that detects this type of forgery. On the other hand, during the same conference paper, the authors propose several improvements to achieve the end-to-end verifiability of Estonian Internet voting. In particular, the tabulation integrity improvement.

Regarding non-repudiation, it is a situation when a “user cannot deny (repudiate) having performed a transaction”. This concept combines “authentication and integrity: non-repudiation authenticates the identity of a user who performs a transaction, and ensures the integrity of that transaction” (Conrad, E., Misenar, S., & Feldman, J. (2016)). Hence, by simply entering other voter’s identification number (PIN1, PIN2 and ID-card or mobile-ID), people can vote on behalf of someone.

From the two previous paragraphs, one can understand that avoiding forgery and ensuring non-repudiation are subject to different procedures in an I-Voting system as the one used in Estonia than in a e-voting system where Blockchain is integrated.

By revisiting the chapter 2.3.4. Issues and Limitations, some technical and nontechnical limitations may be considered and highlighted for this Blockchain analysis’ chapter. Below, one can read more about them and their contextualization in a Blockchain-based e-voting system.

Lack of Privacy: If on one hand Blockchain is a decentralized network "purely distributed peer-to-peer ledger" and transparency is required, on the other hand it presents a big limitation for the implementation of this algorithm in applications that require a higher level of privacy. According to Yi, H. (2019), as discussed in chapter 2.3.5. E-Voting and Blockchain, the author presents techniques that improve the security in a Blockchain-based e-voting system. The Blockchain's architecture is similar but the entire scheme is improved. Consequently, in blockchain-based e-voting, votes can be counted by everyone but the identity of a voter associated to his/her vote, no one is able to know, as well as no one is able to see for which candidate a citizen has voted, once the voting ballot is marked with a signature by each voter.

The Security Model: The Blockchain's security is strong and based on asymmetric encryption. The problem comes in case the private key of a user is lost to someone else: the security of the first user's account is compromised immediately. There is no "plan B" for this situation. In fact, in chapter 2.3.5. E-Voting and Blockchain, the proposed model by Yi, H. (2019) also states that the private key generated by the voter may be kept, once it guarantees the ballot secrecy. Hence, the lack of an efficient mechanism to recover a lost key is a possible bottleneck of the system. Proposed solutions are already published, as in this study from Aydar, M. Çetin, S., Ayvaz, S., & Aygun, B. (2019), where two bottlenecks related to keys are mentioned and object of study: "users not having an efficient and secure way to store their keys" and "no efficient recovery mechanism exists in case the keys are lost". From this study, the authors make use of "concepts of revocable fingerprints and erasure codes for key encryption, and distributed secret sharing scheme for key recovery".

Limited Scalability: The capacity of Blockchain of adding to the chain new transactions grouped in blocks has as a trade-off processing speed that is reduced and scalability which is limited. Applications that need high processing speed and high scalability face a big limitation by using Blockchain. Also, in the case of a Blockchain-based e-voting solution, storing large volumes of historical data is not desirable in case of an eventual hacker attack in the future.

Lack of Flexibility: Immutability of the algorithm avoids people to develop further on the blockchain. Then, a Blockchain-based e-voting solution requires to be built on top of a protocol that is very robust and bugs may be detected and corrected since the very beginning.

Critical Size: Ensure "robustness against manipulations" and that the "history of transaction data" is trustworthy, are the principal characteristics of a peer-to-peer system that guarantees a majority of honest nodes and becomes more resistant to attackers with a lot of computational power. Building an e-voting system on top of Blockchain, working in an uncontrolled environment, leaves the system vulnerable to attackers trying to take control of the system.

Although all mentioned limitations are worth of attention, the next two are considered especially critical for this analysis:

Hidden Centrality: Not everyone has the required financial resources and computing skills to invest in specialist hardware. Considering the basis of Blockchain, the more mathematical computational problems members are capable of solving, the more blocks they add to the chain and receive rewards for "contributing to the integrity of the system". As long as users do not have all the same computing skills, the decentralization is questionable, once the integrity ends up to be managed by a small number of users. In the case of voting, this logical cannot be replicated. Each user shall have one and only one vote associated in the end (considering also the possibility of the withdrawable model as defended in chapter 2.3.5), and candidates shall not be elected based on who computes the most and the best.

High Costs: To guarantee the high level of security desirable, it implies powerful pieces of hardware, high electrical energy consumption and money. Not every user will have in his/her position a computer capable of solving the computational problems in short-time, neither he/she has the technical skills to deal with this algorithm. Another important factor is the energy consumption which is not desirable especially during an era that people are investing resources in reducing the carbon footprint.

In the case of Portugal, the lack of Legal Acceptance is also an impediment.

The fact that is a decentralized system, different from the "centralized approaches" that are currently in the European law (European Union Blockchain Observatory & Forum. written by Lyons, T., Courcelas, L., & Timsit, K. (2019)) and, also, five of the six critical legal issues presented in chapter 2.3.4. Issues and limitations, are the basis to explore the legal acceptance of this algorithm in Portugal, at a national perspective.

The **legal value of Blockchain as registries** (the transactions do not have legal authority by themselves, according to eIDAS); **territoriality** (in case of fraud, the responsibility is assigned based on the location where the act occurred, and considering this distributed network, the legal responsibility is not clear where and whom to be assigned); **enforceability** (the individual who breaks the law may be identified. As known, this algorithm ensures the full anonymity of members. Identification tools could be used by courts in order to enforce the law and responsibility over the individuals); **liability** (assign the responsibility to software developers for illegal acts committed by members in the network, only because they are the creators, is not correct) and, finally; **data protection** (since GDPR rules within EU member-states entered into force, blockchain was not considered in these norms).

Summing up, despite of bringing security and anonymity to an electronic voting system, Blockchain is still a technology which requires not only more powerful hardware and software resources, but also higher technical skills from a common citizen. In a country where not everyone has neither a computer or access to the internet, some steps may be taken first in order to build the necessary conditions to implement this technology in a national e-voting procedure.

5.3. VALIDATION

In order to discuss the possible implementation of a national electronic voting system in Portugal and collect some opinions and points of view to take into consideration for this analysis, three questions were made to Professor Luís Alfredo Amaral, Associate Professor at Department of Information Systems in the School of Engineering of University of Minho, and to Miguel de Azevedo Moura, Professor at Private Law in NOVA School of Law.

After a brief introduction about the subject and objectives of this dissertation, the three questions indicated below were made to the participants for them to answer according to their personal and professional experiences:

1 – "Do you consider that the introduction of an electronic voting system in Portugal would be beneficial, taking into account the current social, political, legal and technological framework?"

2 – "Do you consider that adapting and/or replicating an identical system to Estonia would be a good option?"

3 – "Do you think that an algorithm as Blockchain could add confidence to the electronical voting system?"

Regarding **question 1**, the answers were as follow:

LA: Me and some colleagues of mine had the opportunity to follow and review some years ago the Portuguese national elections (Parliamentary, Presidential, European and Local elections). My opinion is based on the technology and organizational advancements (not judicial). In another words, it is based on the information systems of the national electoral system, but not in the legal and political components.

In order to share my opinion about the electronic voting I need first to clarify if we are talking about the electronic voting machines or Internet voting. Regarding the electronic voting machines, I am against, I think it is a bad investment, a waste of money, time and opportunity. Curiously, in the last European elections, these machines were used in the district of Évora. It would be necessary to appear accounts that justify the investment and associated risk, balanced with the benefit. Currently, the paper ballot voting is a process that goes well, without economic problems, and substitute this process by electronic voting machines (where millions would be invested), it would be a waste. About the electronic voting via Internet, I am totally in favor. Several years ago, when me and my colleagues sent the elections' reports to the Prime Minister, the last paragraph was always appealing to the need of the Portuguese electoral system's modernization, namely the use of I-voting. We have had the opportunity to speak to the person in the government responsible for these matters and we always pass this message.

Everybody is concerned about the abstention rate increase, with the disinterest especially by the youngest, and it can only get worse once these younger citizens socialize through the use of a smartphone, study and work under the use of technological equipment, consume culture through the digital devices, but when it comes to the time to vote, they need to travel to a place in their parish in order to vote. It goes against what is natural nowadays, and people will distance themselves from this process. The only way to appeal to the votes of the youngest is to give the possibility of voting in the "place where they live", so to speak, through the digital devices.

However, when this subject is debated in the Parliament, I see a big reaction, not rational in my perspective.

Answering to your question, I am in favor of Internet Voting and I consider retrograde the blocking of electronic voting advancement nowadays. The technology is there, other countries are already doing it as it is the Estonian case (started with low participation rates, but in the last elections it reached 49%), proving that people are more confident about this system. There is not the guarantee of voter uniqueness, but the weaknesses also exist in the traditional system. After these years, I reached the conclusion that everybody acknowledges the paper ballot voting falls, but when it comes to the time to change to the electronic voting via Internet, it needs to be perfect, without failures. This is not rational; it would be enough to be equal or better. Here I give reason to one of the conservatives' arguments: there is no guarantee that one person will use another person's credentials to vote on behalf of the second.

However, there are some mechanisms capable to minimize the risks: vote multiple times and counts only the last vote, as it is in the case of Estonia; give two credentials, one dummy and other real, where only the voter knows what are they. There are several methods capable to overcome this problem presented and being truth that is not perfect, the same happens in a traditional system. The truth is that any political party, either right or left-wing, are not comfortable to make a change in this topic. However, in my opinion, it will be inevitable. As sooner the better but there is no political will to advance for this experimentation. But we need to keep in mind that the technology is there and I don't believe the costs are higher than the current system (just in postage to send the ballot papers to emigrants, it was more than one and a half million euros, excluding the remaining associated costs). It is not due to the costs of Internet voting that it does not move forward.

MM: In my point of view, and maybe I will give an antagonistic opinion, Portuguese citizens see with good eyes the technologic advancement, the debureaucratization, the technical progress of daily activities, such as the MBWay massification and Via Verde. Nowadays, also due to Covid, there has been an advancement for carrying out online activities. This is to say that, on one hand there is trust (an important word for this subject) in the demand of technological solution. The electronic vote only, without thinking about the technology and/or language behind, it seems to me that would be welcome in the electoral act.

There will always be a percentage of the political population that will criticize, think that it is a way to control the votes, it is inevitable. However, it is a small percentage of the Portuguese population when compared to the Blockchain case.

Answering briefly, the electronic vote seems adequate and the Portuguese welcome it, and I believe that would lead to a reduction in the abstention rate.

There is nothing in the law that prohibits it, that restricts it or that we have to make a very profound constitutional or legislative change. No. There will have to be legislative changes, but it is from the point of view of changing ordinary and non-constitutional law, which would be more difficult to make (by qualified majority in parliament). The change would be made by the government or Republic Assembly behalf and the implementation process of this system would be much swifter and more welcome.

Question 2:

LA: I think copying models never leads to a good result. I support inspiration, not reinventing the wheel, but inspiration in the good practices. I am not an expert in the Estonia's technological solution but it seems like a solid one, more proven, more tested, and would work as a good starting point for a process in Portugal. However, all processes need to be adjusted, taking into consideration the cultural specificities, for example. Estonia is a smaller country, with a population more concentrated and less inequality in digital literacy of the population (in Portugal, we have an illiterate population on the one hand and a highly qualified population on the other). The realities are not the same. But a solution as the one implemented in Estonia would certain be a great starting point for Portugal.

MM: Even for a population a little uninformed and confused, as it can be the Portuguese one, the Estonian system as it is presented to me, is adaptable. If I do not have a computer, I can vote in the polls, if I am in doubt, I can always change, if I do not have trust in the system, I can always go to the polls and vote. However, there will always exist people who are in doubt and question about the eventual vote duplication. This system can only exist if there will be confidence that when someone goes to the polls voting in paper, that vote will override the last electronic vote, and Portuguese people will tend to considerate a problematic topic: how does the electoral body guarantee, in an independent manner, this system? Only through the integration of all intervenient bodies in the electoral act, making part of the commission, approving all the technical aspects and following and monitoring this process, then they would be able to transmit confidence to people vote.

Finally, **question 3**:

LA: I can answer to this question in two or three parts.

There are other technologies other than Blockchain which guarantee the anonymity of votes: e-Vote, used in University of Minho for several years ago, with a duly thought out and improved architecture, following international standards on the best way to do it. Through this system, whenever I vote, I can verify my vote (not in who I voted for but if the vote was well counted or not), and I can guarantee (the system is audited) that nobody knows who voted for whom and all votes are counted. This solution has nothing to do with Blockchain, so there are further alternatives.

Regarding Blockchain itself, I have some animosity. I know reasonably how it works and I believe that in its more transparent purpose is competent. However, it has some weaknesses: if there are a majority of miners in the network, the balance of a group that verify the others can be taken apart. In case the network is balanced, everyone can verify the other's actions. But if a majority of machines controls the network, it is not balanced anymore. One of the principal advantages and its robustness ends with this lack of balance. In the example of cryptographic coins this situation happens when we have a set of machines operating in one place and controlling the system, becoming centralized, and at that moment we questioned about where is the virtue of Blockchain. We must fear about this.

In the democracy and elections spectrum, this manipulation and centralization of power is very desirable, such as in the Brexit referendum and Trump elections examples. It is always possible, even with the Blockchain capabilities, to "trick the game". Another topic is the Blockchain's carbon footprint that continues to be very significant. It needs hard work, a great computational power, energy consumption, heat, so everything works fine. It requires a lot of money, not only in computation, but also in ecological terms once it is a technology not environmentally friendly. Each transaction has the "history" of every previous transaction, forming the chains, which is its strength, but on the other hand, associated with each bit is a transmission and computing energy.

This bit of energy times billions and billions has a very high and energetic footprint and negative. I am not aware at the moment if there were already improvements to reduce this energy consumption, but according to its principals it is not even possible so it is able to prove the history in chain at any time and, in case it is not solvable, it is not a future solution. Although safe it will be very expensive. And in case yes, it cannot be a good engineering solution. This technology can be used in contexts where security is extremely crucial, but in a national electoral system, with millions of voters, I have difficulties to understand that this technology has a space. The truth is, after all these years, we still have no national systems based on Blockchain. Theoretically, it works well, but it raises several problems in practice.

MM: On the one hand, the Blockchain technology guarantees confidence and timelessness, undoubtedly. The anonymity question I do not think it would be that relevant because, if it is true that we want the anonymity of the vote, it is also true that we do not question the eventual non-anonymity in the paper voting at the polls. The topic of non-anonymity can be considered a "known issue". Another point is the timelessness and the fact that it is possible to save the data in a safely manner would be an advantage certainly. Furthermore, Blockchain allows an intercommunication with other data, as I think it is in the case of Estonia, where there is an associated number to the citizen card that represents the person and this key that no one can link to the citizen besides the technology itself, replicates the data. I do not have technical knowledge about Blockchain to say if a hacker would be able to do a match between the citizen's keys with the physical person, but in case no, it seems to me a positive point.

My problem with Blockchain is not related to the technology itself, but to the social awareness. If I say to the voters that we have Blockchain, I do not have any doubt that people would start to investigate and ask about it, to associate Blockchain to money laundering, Bitcoin, dark payments, cryptocurrencies, and that still has a negative connotation in terms of sensitivity nowadays and could cause some noise in the electoral process. If I was the responsible for the implementation, unless someone asks me, I would not say to the electorate that the technology behind the electronic voting system is Blockchain (I would not hide it but would not make a campaign about it). I have no doubt that the Portuguese would quickly associate to something negative. There isn't neither enough culture or a solid education (at Academy level) regarding this technology. My only fear in case the Blockchain would be implemented in the E-Voting is that no campaign could be made, otherwise the Portuguese people would not accept due to lack of culture regarding this topic. It could be a good trigger to start a discussion and to explain to the citizens what the technology is, what are the advantages, what are the disadvantages in the national panorama, and that would be the "best of both worlds", but I am certain that in a near future I would not be able to do this implementation because of the social fear and negative connotation given to the algorithm. But I hope it will change.

5.4. Discussion

In this section, three analysis will be made. The first one concerns the introduction of an electronic voting system in Portugal, if it would be beneficial and what are the social, political, legal and technological factors that may be taken into account. The second analysis is related to the case-study of this dissertation, the Estonia's I-Voting system and if a similar solution would be reasonable to adapt and/or replicate in Portugal. The third and last analysis is about the Blockchain algorithm and its place in an e-voting system regarding confidence. This discussion will be based on the interviewees' perspective and opinions as a way to validate the conclusions and recommendations that were obtained after the Case Study's analysis and discussion, and Recommendations for Portugal chapters of this dissertation.

Regarding the first topic, both Professors interviewed consider beneficial and agree with the introduction of an electronic voting system in Portugal. Important opinions and conclusions were collected, from the different spectrums (legal, social, political and technological):

- **Associated costs:** Electronic voting machines (kiosks) may be differentiated since the very beginning from Internet voting. The first one implies an opportunity cost (time and money) very high when compared to the benefit that brings to the electoral population. The investment done in e-voting shall consider the balance between risk and benefit and, in that logic, Internet voting is beneficial in opposition to kiosk voting. Also, the associated costs are not higher when compared to the traditional system and it may not be used as an excuse to block its advancement.
- **Abstention rate:** Another topic discussed was the participation of electors and what incentive e-voting could bring to the population (especially to the youngest). There is a political and social concern in regard to the uninterest and abstention of the youngest

electors to vote in elections. Nowadays, they socialize, study and work under the use of a technological equipment but, when it comes to the time of voting, most of them need to travel long distances. Summing up, both interviewees agree that an electronic internet voting system would impact the abstention rate positively.

- **Legal amendments:** There is nothing in the Portuguese Constitution that blocks the implementation of E-Voting in Portugal. There will have to be legislative changes, but it is from the point of view of changing ordinary and non-constitutional law.
- **Social perspective:** Portuguese citizens see with good eyes the technologic advancement, the debureaucratization and the technical progress of daily activities. Covid-19 pandemic proves even more the importance of these changes.
- **Technology intervention:** Its retrograde to block the implementation of a national electronic voting system in Portugal once the technology exists. The traditional system weaknesses also exist, however, at the time of creating a system under the use of internet, it needs to be perfect, without falls (according to political debates), and this is not rational.

The second question was simple: if adapting or replicating an identical system to that of Estonia would be a good option to the Portuguese electoral system. Both interviewees agree that would certain be a great starting point for Portugal and it is also adaptable which is a great advantage (if an elector does not have a computer, or if he/she doesn't trust the e-voting system, or is in doubt for any possible reason, can always go to the urns and vote personally). Other two topics were discussed:

- **Cultural perspective:** In the case of Portugal, a system as it is presented in Estonia, would need to be adjusted accordingly. Estonia is a smaller country, with a higher population density and lower literacy inequality. Both realities are different and replicating an identical system would not be correct.
- **Trust:** In case of replicating the possibility of an elector to choose if he/she prefers to vote personally in the polls or through the internet, confidence becomes a sensitive topic when someone asks about the independency and integrity of the system, and if the problem of double voting is mitigated indeed. Only through the integration of all intervenient bodies in the electoral act, making part of the commission, approving all the technical aspects and following and monitoring this process, then they would be able to transmit confidence to people vote.

The third and last topic discussed was about the inclusion of Blockchain and if it would add confidence to the e-voting system. This question raised up different opinions and perspectives about its possible integration in an e-voting solution. However, both Professors interviewed presented some animosity and disbelief about the algorithm itself and its use as the basis technology for the voting system in the short- and medium-run. Below, one writes more about the opinions and conclusions collected during both interviews:

- **Confidence, anonymity and timelessness:** This algorithm guarantees confidence and timelessness (the possibility of saving data in a safely manner would be an advantage certainly). Another positive aspect to note is how difficult it is to find a match between citizen's keys (private and public) and the physical person itself.

- **Technology weaknesses:** There are other alternatives to Blockchain and some animosity was presented. If a majority of machines start to control the network, it is not balanced anymore. One of its major advantages and robustness ends with this lack of balance. This problem could influence democracy and the election spectrum in a way that manipulation and centralization of power is very desirable for some parties and could benefit from this.

- **Energy cost:** One of the interviewees mentioned the concern with the energy consumption, which is very high the energetic footprint associated. Hence, it cannot be considered a good engineering solution once we are dealing with millions and millions of transactions. Although it is safe, it becomes very expensive.

- **Social awareness:** The word Blockchain itself brings a negative connotation to the most common citizen and would cause some noise in the electoral process: Bitcoin, money laundering, dark payments and cryptocurrencies. There isn't neither enough culture or a solid education (at Academy level) regarding this technology. The interviewee also believes that due to these reasons, Blockchain might not be used as the basis technology for a national e-voting system.

Summing up, the possibility of voting anywhere, from home, by only accessing an application, it is a solution with potential and worth of investment. The mobility problem and abstention concern could be mitigated, not only, but also with this technological solution (considering other factors that may explain both issues). However, the introduction of Blockchain as the technology behind this application, presents some disadvantages and fears that may prevent its use. In an economic analysis of the opportunity cost associated to the investment in a Blockchain-based e-voting schema, it is sufficiently high. The non-repudiation and difficulty of forgery of votes are not enough to make people accept that this is the solution for the next elections. Also, this technology does not depend from the trust in an electoral body (third-party) involved, once it is a decentralized network, and in a country that is used to a National Electoral Committee that manages the electoral process in rigorous and transparent way, its absence would generate untrust and doubts about its integrity and credibility.

6. CONCLUSIONS

6.1. SYNTHESIS OF THE DEVELOPED WORK

In order to conclude this dissertation and the recommendations associated to the proposal of a Blockchain-based e-voting system in the Portuguese electoral law, it is important to mention that the initial presented questions were studied and answered throughout this work.

First of all, some E-Voting solutions already implemented in other countries were studied. From this sample, Estonia was the country selected as the case of study of this dissertation (the methodology that was chosen in order to conclude on the recommendations for Portugal). By becoming the first country worldwide to use internet voting in the Parliamentary Election, the adaptability of the new system with the traditional one in order to facilitate the voter's understanding of its process and the fact that this country was a pioneer of Internet Voting were the arguments presented to defend the choice. Regarding the study method chosen, the set of research questions initially presented in this dissertation are of type "why" and "how". "Why" a Blockchain-based voting system in Portugal would be beneficial and a solution to the mobility concern and trust crisis and, on the other hand, "how" its adoption would impact the abstention rate and the trust in the Portuguese political system. Based on these two questions of "why" and "how", one found Case Study as the most suitable methodology to explore, draw conclusions, validate and discuss possible solutions.

After selecting the I-Voting system of Estonia as the case of study, some important conclusions were achieved from the case analysis chapter, where the Estonian E-Government technical architecture was studied in the light of a model documented in the literature review. Still in connection with the same chapter, the architecture of the I-Voting system was revised (how the different components are associated from the moment when the citizen opens the voting client application until the moment when the vote is successful registered for tallying and the voter can verify his/her vote by reading the QR Code with the smartphone in the verification application), so the voter's experience could be analysed from the end user's perspective. Right after, a list of issues and limitations (legal, political, social and technological), reported in the literature review, were put side by side with the Estonian case. From this analysis one was able to understand that this system is capable to overcome most of the challenges documented in the bibliography, which makes it highly accepted by the European Commission, Estonian's government and Estonian citizens in general. In the end, the possible integration of a Blockchain-based E-Voting system was discussed and in order to understand the current vision of this country regarding this topic, one have asked Florian Marcus, Digital Transformation Adviser e-Estonia Briefing Centre, to make a question to Sven Heiberg, I-Voting Product Manager Cybernetica AS (company also known for the Internet Voting development), as we can read in appendix 10. This question was focused on the thought of implementing Blockchain for I-Voting, in the present, future or if not, a possible explanation why it is not necessary. The Product Manager affirmed that the possibility of integrating Blockchain was considered and investigated. However, the major argument for retarding the usage of this technology is the fact that currently the Online Voting system relies on a "single component to store the information" and exists a "separation of duty and distribution of tasks" which is crucially in the current implementation architecture. Blockchain does not rely on a single component, or, in another words, it is a decentralized system that does not involve a third-party.

In the end, a set a of recommendations concerning the Portuguese framework and based on the Estonian experience were listed. Departing from the main Portuguese electoral law articles that were studied and documented in this dissertation, the principal differences and what is missing in the electoral acts to implement an e-voting solution in Portugal were identified. Also, two interviews were conducted in order to understand the vision of two professors regarding the implementation of an E-Voting solution in Portugal. From this validation, one was able to conclude from both interviews that exists some animosity and disbelief about the algorithm itself and its use as the basis technology for the voting system in the short- and medium-run.

Summing up, the mobility problem and abstention concern could be mitigated, not only, but also with a technological solution (considering other variables that may explain both issues). However, the introduction of Blockchain as the technology behind this application, presents some disadvantages and fears that may prevent its use. This technology does not depend from the trust in an electoral body (third-party) involved, once it is a decentralized network, and in a country where the National Electoral Committee manages the electoral process in a rigorous and transparent way, its absence would generate untrust and doubts about its integrity and credibility in the voter's point of view.

6.2. RESEARCH LIMITATIONS

Despite of recommending the investment in an Electronic Voting system, through the Internet (instead of kiosks), based on a case study analysis and issues and limitations that may exist, no practical application was developed and tested by a sample of electors.

Other limitation is the inexistence of a country nowadays that uses Blockchain integrated in a national electronic voting procedure. Hence, no real case scenario was explored and its possible integration was based exclusively on existing papers and researchers' conclusions.

Last but not least, Blockchain technology is not recommended as the solution most feasible in the short-medium run due to the reasons presented. However, this study aims to contribute for breaking the assumption that still exists a long path to the adoption of technology that supports the online voting.

6.3. FUTURE WORK

During the validation phase and in line with what was mentioned in the previous sub-chapter, some topics and questions were raised. One believes that the development of a practical e-voting application, for testing purposes, and share it with a set of potential Portuguese voters (a sample), would make it possible to assess, receive opinions, vision and perception of its security by the end-users. At the same time, some blockers suggested during the validation phase would be confirmed whether they are indeed a cause for concern. The manipulation and centralization of power, energy consumption and social perception would be studied and measured when introducing Blockchain as the technology behind the user's experience.

This application should be used for testing purposes and its usage in a real-life scenario should be done exclusively under further coordination and agreement with the competent authorities.

REFERENCES

(2019). Society at a Glance 2019. In Society at a Glance. OECD. https://doi.org/10.1787/soc_glance-2019-en

Abba, A. L., Awad, M., Al-Qudah, Z., & Jallad, A. H. (2017, November). Security analysis of current voting systems. *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).* https://doi.org/10.1109/icecta.2017.8252006

Agora (2017). Agora: Bringing our voting systems into the 21st century [White Paper]. https://agora.vote/Agora_Whitepaper_v0.1.pdf

Ahmad Mosa, Hazem M. El-Bakry, Samir M. Abd El-Razek, & Sajjad Q. Hasan. (2016). A Proposed E-government Framework Based on Cloud Service Architecture. *International Journal of Electronics and Information Engineering*, 5(2). https://doi.org/10.6636/IJEIE.201612.5(2).05

Ajish, S., & Anil Kumar, K. S. (2020). Secure I-Voting System with Modified Voting and Verification Protocol. *In Lecture Notes in Electrical Engineering* (pp. 189–200). Springer Singapore. https://doi.org/10.1007/978-981-15-5558-9_19

Al-Ameen, A., & Talab, S. (2013). The technical feasibility and security of e-voting. *Int. Arab J. Inf. Technol*., 10, 397-404.

Alhawawsha, M. (2017). Developing of the E-government system based on Java for online voting. *Technology Audit and Production Reserves*, 3(2(35)), 9–13. https://doi.org/10.15587/2312-8372.2017.104033

Avgerou, C., Masiero, S., & Poulymenakou, A. (2019). Trusting e-voting amid experiences of electoral malpractice: The case of Indian elections. *Journal of Information Technology*, 34(3), 263–289. https://doi.org/10.1177/0268396218816199

Aydar, M., & Ayvaz, S. (2019). Towards a Blockchain based digital identity verification, record attestation and record sharing system. ArXiv, abs/1906.09791.

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019, September). Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT. *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).* https://doi.org/10.1109/etfa.2019.8869262

Ben Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*, 9(3), 01–09. https://doi.org/10.5121/ijnsa.2017.9301

Bhatnagar, S. C. (2004). E-government: from vision to implementation: a practical guide with case studies /. Sage Publications.

Bosova, E. N., & Reut, D. A. (2019). Remote electronic voting: search for legislative formalization. *Law Enforcement Review*, 3(3), 53–62. https://doi.org/10.24147/2542-1514.2019.3(3).53-62

Boucher, P. (2016, September). *What if blockchain technology revolutionised voting?* Retrieved from Scientific Foresight Unit (STOA) - European Parliament: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2016)581918

Braun Binder, N., Krimmer, R., Wenda, G., & Fischer, D.-H. (2019). International Standards and ICT Projects in Public Administration: Introducing Electronic Voting in Norway, Estonia and Switzerland Compared. *Administrative Culture*, 19(2), 8–22. https://doi.org/10.32994/hk.v19i2.215

Buldas, A., Heiberg, S., Krips, K. & Willemson, J. (2020, April). *Mobile voting feasibility study and risk analysis*. *Cybernetica report T-184-5. Tallin: Cybernetica*. Retrieved from https://www.valimised.ee/sites/default/files/uploads/eng/2020_m-voting-report.pdf

Cellary, W., & Strykowski, S. (2009). e-government based on cloud computing and service-oriented architecture. *Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance - ICEGOV '09. the 3rd International Conference*. https://doi.org/10.1145/1693042.1693045

Chauhan, S., Jaiswal, M., & Kumar Kar, A. (2018). The Acceptance of Electronic Voting Machines in India: A UTAUT approach. *Electronic Government, an International Journal*, 14(3), 1. https://doi.org/10.1504/eg.2018.10011841

Chohan, U. (2018). Environmentalism in Cryptoanarchism: Gridcoin Case Study*. SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3131232

Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., Delis, A., Kiayias, A., & Roussopoulos, M. (2019). Distributed, end-to-end verifiable, and privacy-preserving internet voting systems. *Computers & Security*, 83, 268–299. https://doi.org/10.1016/j.cose.2019.03.001

Conrad, E., Misenar, S., & Feldman, J. (2016). Domain 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity). *In CISSP Study Guide* (pp. 11–79). Elsevier. https://doi.org/10.1016/b978-0-12-802437-9.00002-3

Cooke, R., & Anane, R. (2012). A service-oriented architecture for robust e-voting. *Service Oriented Computing and Applications*, 6(3), 249–266. https://doi.org/10.1007/s11761-012-0108-0

Cucurull, J., Rodríguez-Pérez, A., Finogina, T., & Puiggalí, J. (2019). Blockchain-Based Internet Voting: Systems' Compliance with International Standards. *In Business Information Systems Workshops* (pp. 300–312). Springer International Publishing. https://doi.org/10.1007/978-3-030-04849-5_27

Dannen, C. (2017). Use Cases. *In Introducing Ethereum and Solidity* (pp. 165–172). Apress. https://doi.org/10.1007/978-1-4842-2535-6_10

De Cock, D., & Preneel, B. (2007). Electronic Voting in Belgium: Past and Future. *In Lecture Notes in Computer Science* (pp. 76–87). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-77493-8_7

Dias, G. P., & Gomes, H. (2014, June). Evolution of local e-government maturity in Portugal. *2014 9th Iberian Conference on Information Systems and Technologies (CISTI).* https://doi.org/10.1109/cisti.2014.6877041

Drechsler, W., & Madise, Ü. (2004). Electronic Voting in Estonia. *In Electronic Voting and Democracy* (pp. 97–108). Palgrave Macmillan UK. https://doi.org/10.1057/9780230523531_6

Drescher, D. (2017). Blockchain Basics. Apress. https://doi.org/10.1007/978-1-4842-2604-9

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, 11(5), 589–611. https://doi.org/10.1108/14637150510619902

e-Estonia. (2020, June 18). e-Estonia Live: i-Voting as key to future elections [Video file]. Retrieved from https://fb.watch/2Hqw4VL5wU/

Evans, G. (2017). Implementing E-Government: An Executive Report for Civil Servants and Their Advisors. Routledge.

E-Voting: What Do Judges Say? (2016). *In E-Voting Case Law* (pp. 31–50). Routledge. https://doi.org/10.4324/9781315581385-8

Grothe, M., Niemann, T., Somorovsky, J., & Schwenk, J. (2017). Breaking and Fixing Gridcoin. WOOT.

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2). https://doi.org/10.1007/978-3-540-31987-0_14

Heiberg, S., Laud, P., & Willemson, J. (2012). The Application of I-Voting for Estonian Parliamentary Elections of 2011. *In Lecture Notes in Computer Science* (pp. 208–223). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32747-6_13

Heiberg, S., Martens, T., Vinkel, P., & Willemson, J. (2017). Improving the Verifiability of the Estonian Internet Voting Scheme. *In Electronic Voting* (pp. 92–107). Springer International Publishing. https://doi.org/10.1007/978-3-319-52240-1_6

ICTs in Elections Database. (2017, March 04). Retrieved from https://www.idea.int/data-tools/data/icts-elections

Internet Voting: An Empirical Evaluation. (2014). *Computer*, 47(4), 44–50. https://doi.org/10.1109/mc.2013.224

Joseph, S., & Avdic, A. (2016). Where do the Nordic Nations' Strategies Take e-Government? *Electronic Journal of E-Government*, 14(1), 3.

Jun, M. (2018). Blockchain government - a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity*, 4(1). https://doi.org/10.1186/s40852-018-0086-3

Kolb, J., AbdelBaky, M., Katz, R. H., & Culler, D. E. (2020). Core Concepts, Challenges, and Future Directions in Blockchain. *ACM Computing Surveys*, 53(1), 1–39. https://doi.org/10.1145/3366370

Kovic, M. (2017). Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system. *Center for Open Science*. https://doi.org/10.31235/osf.io/9qdz3

Kremer, S., & Ryan, M. (2005). Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. *In Programming Languages and Systems* (pp. 186–200). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-31987-0_14

Krimmer, R., Duenas-Cid, D., Krivonosova, I., Vinkel, P., & Koitmae, A. (2018). How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. *In Electronic Voting* (pp. 117–131). Springer International Publishing. https://doi.org/10.1007/978-3-030-00419-4_8

Kshetri, N. (2017). Potential roles of blockchain in fighting poverty and reducing financial exclusion in the global south. *Journal of Global Information Technology Management*, 20(4), 201–204. https://doi.org/10.1080/1097198x.2017.1391370

KSI Blockchain - e-Estonia. (2019, September 10). Retrieved from https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

Lei Eleitoral da Assembleia da República 2020 (LEAR) Lei n.º 14/79 (Prt.). Retrieved from https://dre.pt/web/guest/pesquisa/-/search/382590/details/normal?q=Lei+n.%C2%BA%2014%2F79%2C%20de+16+de+maio

Lyons, T., Courcelas, L., & Timsit, K. (2018). Blockchain for government and public services. Retrieved from European Commission. European Union Blockchain Observatory & Forum website: https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf

Machova, R., Volejnikova, J., & Lnenicka, M. (2018). Impact of E-government Development on the Level of Corruption: Measuring the Effects of Related Indices in Time and Dimensions. *Review of Economic Perspectives*, 18(2), 99–121. https://doi.org/http://www.degruyter.com/view/j/revecp

Martinovic, I., Kello, L., & Sluganovic, I. (2017, December). Blockchains for Governmental Services: Design Principles, Applications, and Case Studies (Working Paper No.7). Retrieved from https://www.ctga.ox.ac.uk/article/blockchains-governmental-services-design-principles-applications-and-case-studies

Maurer, A. D., & Esteve, J. B. (2016). E-voting case law: A comparative analysis. London: Routledge, Taylor & Francis Group.

Mavilia, R., & Pisani, R. (2019). Blockchain and catching-up in developing countries: The case of financial inclusion in Africa. *African Journal of Science, Technology, Innovation and Development*, 12(2), 151–163. https://doi.org/10.1080/20421338.2019.1624009

McBride, K., Kütt, A., Ben Yahia, S., & Draheim, D. (2019, November 12). On Positive Feedback Loops in Digital Government Architecture. *Proceedings of the 11th International Conference on Management of Digital EcoSystems*. https://doi.org/10.1145/3297662.3365817

Melin, U., & Axelsson, K. (2009). Managing e-service development – comparing two e-government case studies. *Transforming Government: People, Process and Policy*, 3(3), 248–270. https://doi.org/10.1108/17506160910979351

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System [White paper]. Bitcoin Project. https://bitcoin.org/bitcoin.pdf

Ojo, A., & Adebayo, S. (2017). Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries. *In Public Administration and Information Technology* (pp. 283–298). Springer International Publishing. https://doi.org/10.1007/978-3-319-63743-3_11

Olleros, F., & Zhegu, M. (2016). Research Handbook on Digital Transformations. *Edward Elgar Publishing*. https://doi.org/10.4337/9781784717766

OSCE Annual Report 2011 (2012, March). OSCE Annual Report 2011. Retrieved from Organization for Security and Co-operation in Europe website: https://www.osce.org/secretariat/89356

Osgood, R. (2016). The future of democracy: Blockchain voting. COMP116: Information security, 1-21.

Paiva Dias, G., & Gomes, H. (2014). Evolution of local e-government maturity in Portugal. *2014 9th Iberian Conference on Information Systems and Technologies (CISTI) Information Systems and Technologies (CISTI), 2014 9th Iberian Conference On*, 1–5. https://doi.org/10.1109/CISTI.2014.6877041

Powell, A., Williams, C. K., Bock, D. B., Doellman, T., & Allen, J. (2012). e-Voting intent: A comparison of young and elderly voters. *Government Information Quarterly*, 29(3), 361–372. https://doi.org/10.1016/j.giq.2012.01.003

Qiu, T., Zhang, R., & Gao, Y. (2019). Ripple vs. SWIFT: Transforming Cross Border Remittance Using Blockchain Technology. *Procedia Computer Science*, 147, 428–434. https://doi.org/10.1016/j.procs.2019.01.260

Riigikogu Election Act (2002) Chapter 71 Electronic Voting (Est.). Retrieved from https://www.riigiteataja.ee/en/eli/ee/510032014001/consolide

Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K.-K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149, 102471. https://doi.org/10.1016/j.jnca.2019.102471

Smartmatic. (2020). Belgian elections 2012 - 2019: Customized voting solution for a pioneer in electronic voting. Retrieved from https://www.smartmatic.com/case-studies/article/belgian-elections-2012-2019-customized-voting-solution-for-a-pioneer-in-electronic-voting/

Soares, D., Amaral, L., Ferreira, L. e Lameiras, M. (2019). Presença na Internet das Câmaras Municipais Portuguesas em 2019: Estudo sobre Local e-Government em Portugal. GÁVEA – Observatório da Sociedade da Informação. Universidade do Minho, Guimarães.

Sodiya, A. S., Onashoga, S. A., & Adelani, D. I. (2011, April). A Secure e-Voting Architecture. *2011 Eighth International Conference on Information Technology: New Generations (ITNG).* https://doi.org/10.1109/itng.2011.67

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November 3). Security Analysis of the Estonian Internet Voting System. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/2660267.2660315

State of the DApps (2021). Retrieved from https://www.stateofthedapps.com/rankings/platform/ethereum?page=1

Statistics about Internet voting in Estonia. Retrieved from https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

Statistics. Retrieved from https://www.valimised.ee/en/archive/statistics

Stokkink, Q., & Pouwelse, J. (2018, July). Deployment of a Blockchain-Based Self-Sovereign Identity. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. https://doi.org/10.1109/cybermatics_2018.2018.00230

Sujatha, K., Arjuna Rao, A., Yejarla, P., & Sruthi, K. J. (2017). Voter Authentication Using Modified Elliptic Curve Cryptography. *In Smart Computing and Informatics* (pp. 497–504). Springer Singapore. https://doi.org/10.1007/978-981-10-5544-7_48

Sutardja Center for Entrepreneurship and Technology. (2016). BlockChain Technology: Beyond Bitcoin [White paper]. Berkeley. http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

The World Bank. Individuals using the Internet (% of population). Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS

TIFAC-CORE, S.P. (2018). On Blockchain Applications: Hyperledger Fabric And Ethereum.

Tobin, A. and Reed, D. (2018). Sovrin ™: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust. Sovrin Foundation

Tomov, Y. K. (2019, September). Bitcoin: Evolution of Blockchain Technology. *2019 IEEE XXVIII International Scientific Conference Electronics (ET)*. https://doi.org/10.1109/et.2019.8878322

Trechsel, A., Kucherenko, V., & Silva, F. (2016). POTENTIAL AND CHALLENGES OF E-VOTING IN THE EUROPEAN UNION. Policy Department for Citizens' Rights and Constitutional Affairs

United Nations Department For Economic And Social Affairs. DESA. (2020). United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development. S.l.: United Nations.

Vassil, K. (2015, June). Estonian e-Government Ecosystem: Foundation, Applications, Outcomes. Retrieved from World Bank's World Development Report 2016 Digital Dividends: http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf

White, O., et al (2019, April). Digital identification: A key to inclusive growth. Retrieved from McKinsey Global Institute: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Cham: Springer.

Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, 2019(1). https://doi.org/10.1186/s13638-019-1473-6

Yin, R. K. (2009). Case Study Research: Design and Methods (Ilustrada ed., Vol. 5). Thousand Oaks: Sage.

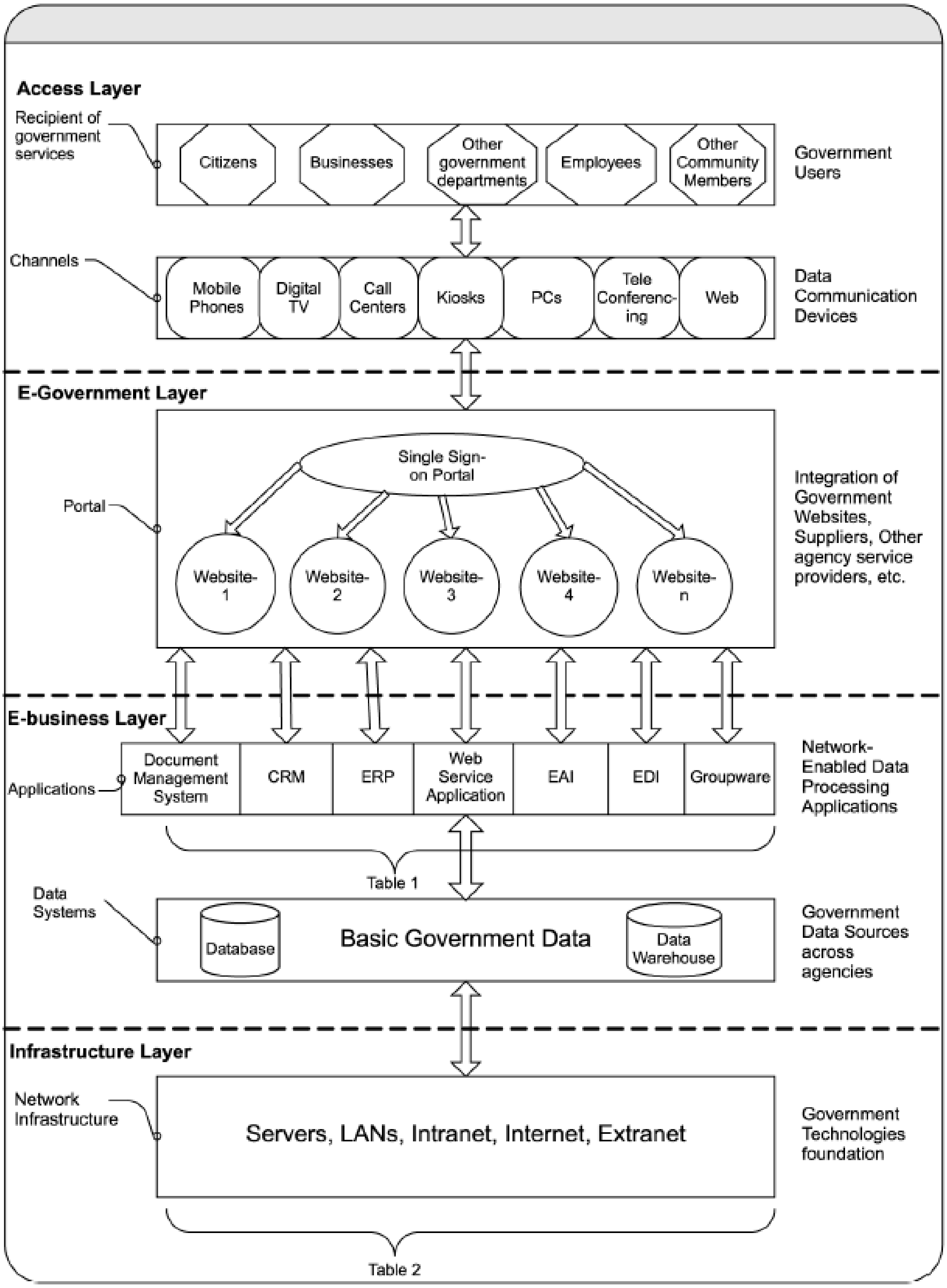
Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, 52(3), 1–34. https://doi.org/10.1145/3316481

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352. https://doi.org/10.1504/ijwgs.2018.095647

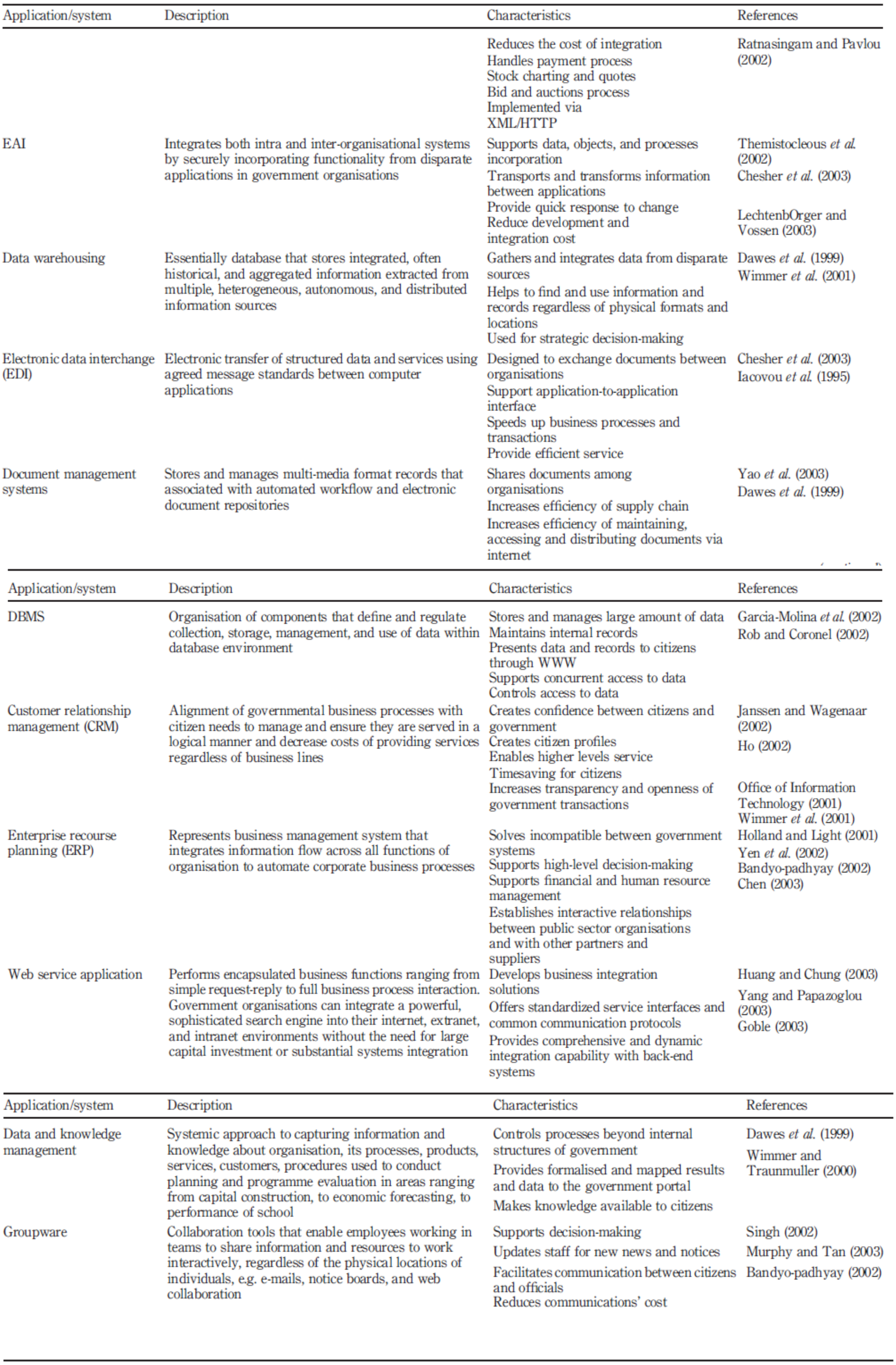
Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), 239–251. https://doi.org/10.1016/j.giq.2010.05.010

APPENDICES

Appendix 1 – Framework of E-Government Architecture (*Ebrahim, Z., & Irani, Z. (2005)*)

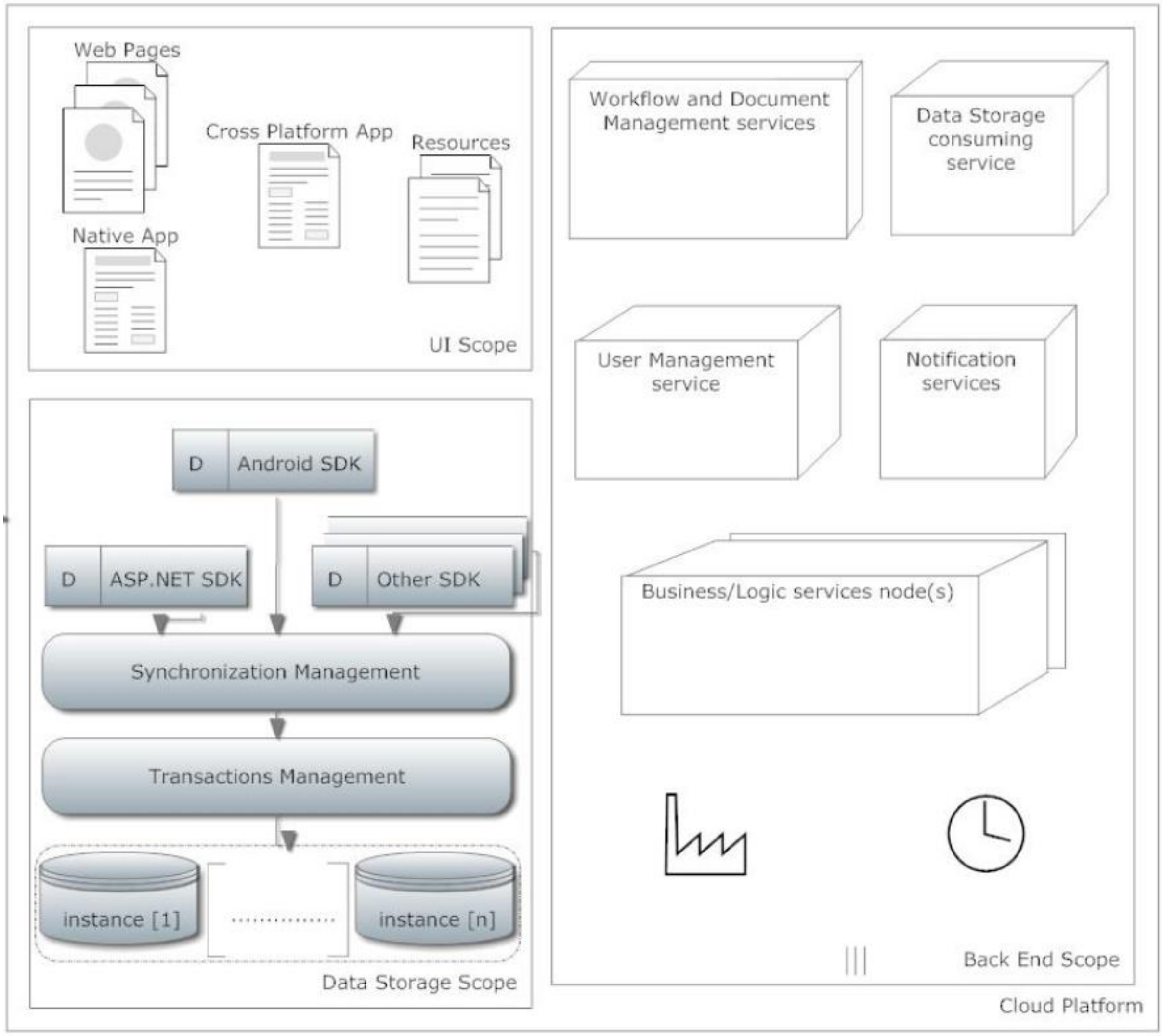


Appendix 2 – E-Business Layer Applications and Systems (*Ebrahim, Z., & Irani, Z. (2005))*

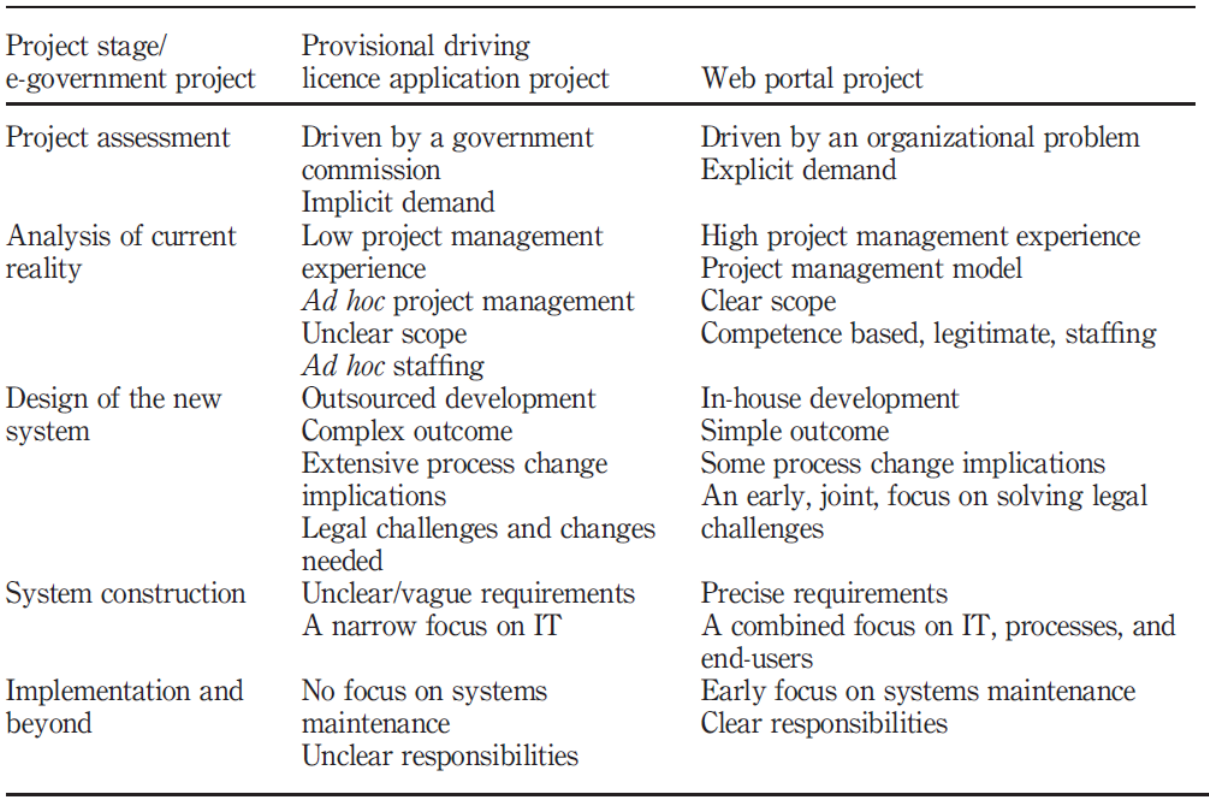


Application/system	Description	Characteristics	References
		Reduces the cost of integration Handles payment process Stock charting and quotes Bid and auctions process Implemented via XML/HTTP	Ratnasingam and Pavlou (2002)
EAI	Integrates both intra and inter-organisational systems by securely incorporating functionality from disparate applications in government organisations	Supports data, objects, and processes incorporation Transports and transforms information between applications Provide quick response to change Reduce development and integration cost	Themistocleous *et al.* (2002) Chesher *et al.* (2003) LechtenbOrger and Vossen (2003)
Data warehousing	Essentially database that stores integrated, often historical, and aggregated information extracted from multiple, heterogeneous, autonomous, and distributed information sources	Gathers and integrates data from disparate sources Helps to find and use information and records regardless of physical formats and locations Used for strategic decision-making	Dawes *et al.* (1999) Wimmer *et al.* (2001)
Electronic data interchange (EDI)	Electronic transfer of structured data and services using agreed message standards between computer applications	Designed to exchange documents between organisations Support application-to-application interface Speeds up business processes and transactions Provide efficient service	Chesher *et al.* (2003) Iacovou *et al.* (1995)
Document management systems	Stores and manages multi-media format records that associated with automated workflow and electronic document repositories	Shares documents among organisations Increases efficiency of supply chain Increases efficiency of maintaining, accessing and distributing documents via internet	Yao *et al.* (2003) Dawes *et al.* (1999)
DBMS	Organisation of components that define and regulate collection, storage, management, and use of data within database environment	Stores and manages large amount of data Maintains internal records Presents data and records to citizens through WWW Supports concurrent access to data Controls access to data	Garcia-Molina *et al.* (2002) Rob and Coronel (2002)
Customer relationship management (CRM)	Alignment of governmental business processes with citizen needs to manage and ensure they are served in a logical manner and decrease costs of providing services regardless of business lines	Creates confidence between citizens and government Creates citizen profiles Enables higher levels service Timesaving for citizens Increases transparency and openness of government transactions	Janssen and Wagenaar (2002) Ho (2002) Office of Information Technology (2001) Wimmer *et al.* (2001)
Enterprise recourse planning (ERP)	Represents business management system that integrates information flow across all functions of organisation to automate corporate business processes	Solves incompatible between government systems Supports high-level decision-making Supports financial and human resource management Establishes interactive relationships between public sector organisations and with other partners and suppliers	Holland and Light (2001) Yen *et al.* (2002) Bandyo-padhyay (2002) Chen (2003)
Web service application	Performs encapsulated business functions ranging from simple request-reply to full business process interaction. Government organisations can integrate a powerful, sophisticated search engine into their internet, extranet, and intranet environments without the need for large capital investment or substantial systems integration	Develops business integration solutions Offers standardized service interfaces and common communication protocols Provides comprehensive and dynamic integration capability with back-end systems	Huang and Chung (2003) Yang and Papazoglou (2003) Goble (2003)
Data and knowledge management	Systemic approach to capturing information and knowledge about organisation, its processes, products, services, customers, procedures used to conduct planning and programme evaluation in areas ranging from capital construction, to economic forecasting, to performance of school	Controls processes beyond internal structures of government Provides formalised and mapped results and data to the government portal Makes knowledge available to citizens	Dawes *et al.* (1999) Wimmer and Traunmuller (2000)
Groupware	Collaboration tools that enable employees working in teams to share information and resources to work interactively, regardless of the physical locations of individuals, e.g. e-mails, notice boards, and web collaboration	Supports decision-making Updates staff for new news and notices Facilitates communication between citizens and officials Reduces communications' cost	Singh (2002) Murphy and Tan (2003) Bandyo-padhyay (2002)

Appendix 3 – The proposed Cloud based e-government framework (*Mosa, A., El-Bakry, H., El-Razek, S., & Hasan, S. (2016)*)

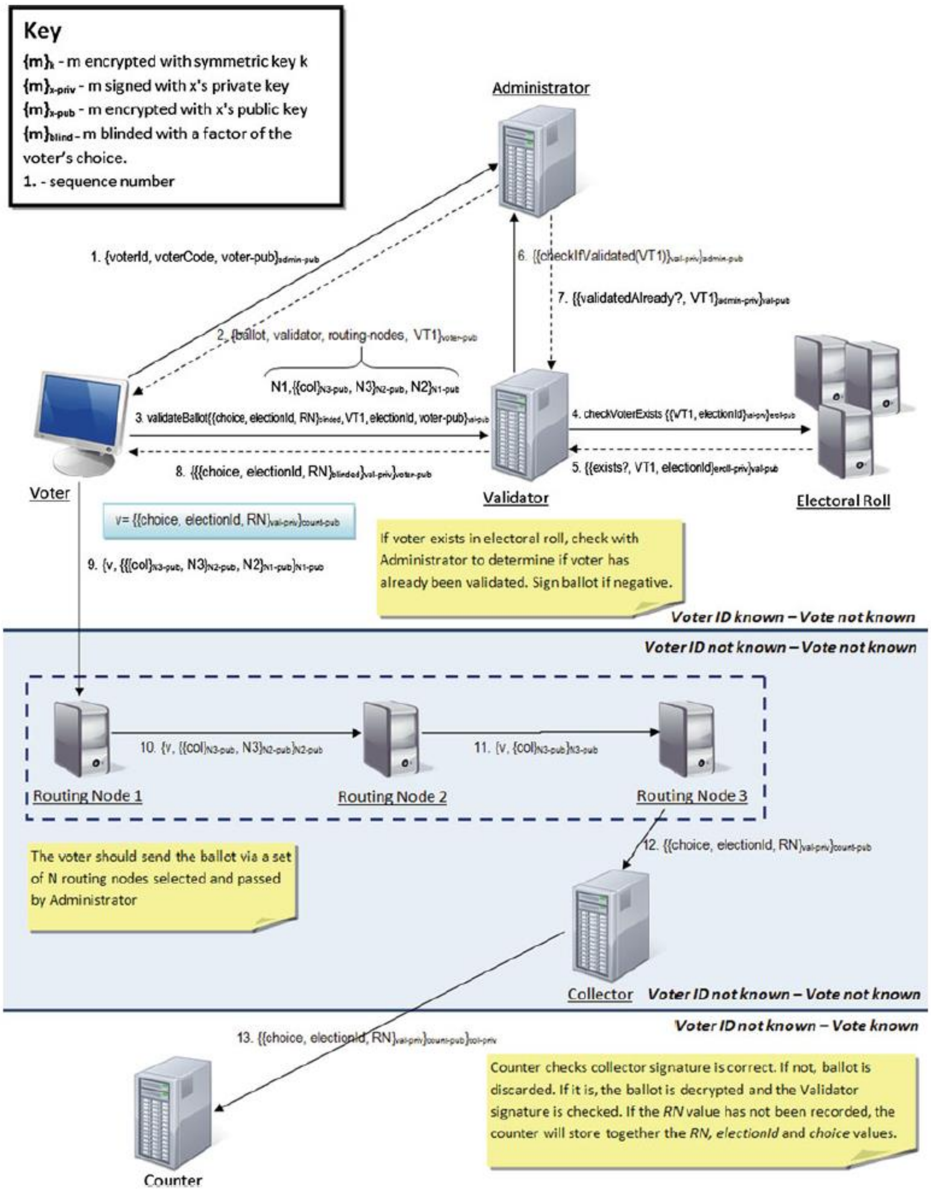


Appendix 4 - Revised/developed project stage and analysis grid (Melin, U., & Axelsson, K. (2009))



Project stage/ e-government project	Provisional driving licence application project	Web portal project
Project assessment	Driven by a government commission Implicit demand	Driven by an organizational problem Explicit demand
Analysis of current reality	Low project management experience *Ad hoc* project management Unclear scope *Ad hoc* staffing	High project management experience Project management model Clear scope Competence based, legitimate, staffing
Design of the new system	Outsourced development Complex outcome Extensive process change implications Legal challenges and changes needed	In-house development Simple outcome Some process change implications An early, joint, focus on solving legal challenges
System construction	Unclear/vague requirements A narrow focus on IT	Precise requirements A combined focus on IT, processes, and end-users
Implementation and beyond	No focus on systems maintenance Unclear responsibilities	Early focus on systems maintenance Clear responsibilities

Appendix 5 – E-Voting process and architecture (Cooke, R. & Anane, R. (2012))



Key

$\{m\}_k$ - m encrypted with symmetric key k

$\{m\}_{x\text{-priv}}$ - m signed with x's private key

$\{m\}_{x\text{-pub}}$ - m encrypted with x's public key

$\{m\}_{blind}$ - m blinded with a factor of the voter's choice.

1. - sequence number

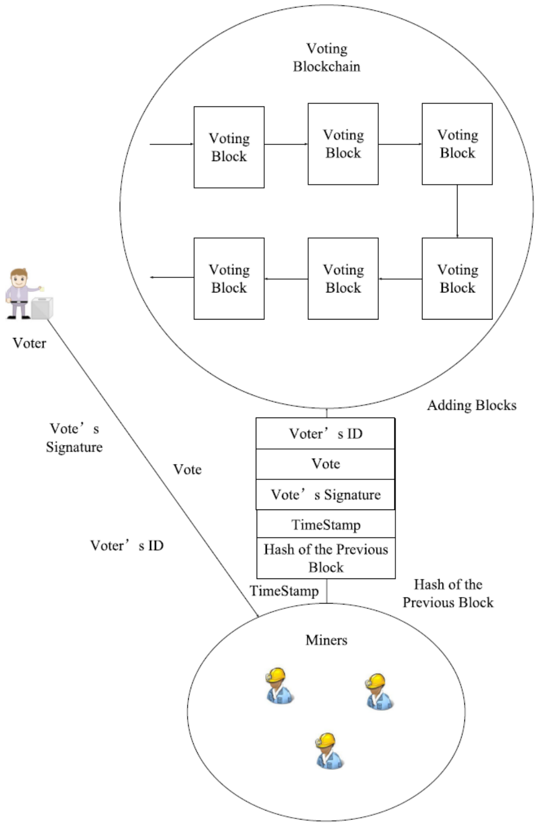
If voter exists in electoral roll, check with Administrator to determine if voter has already been validated. Sign ballot if negative.

The voter should send the ballot via a set of N routing nodes selected and passed by Administrator

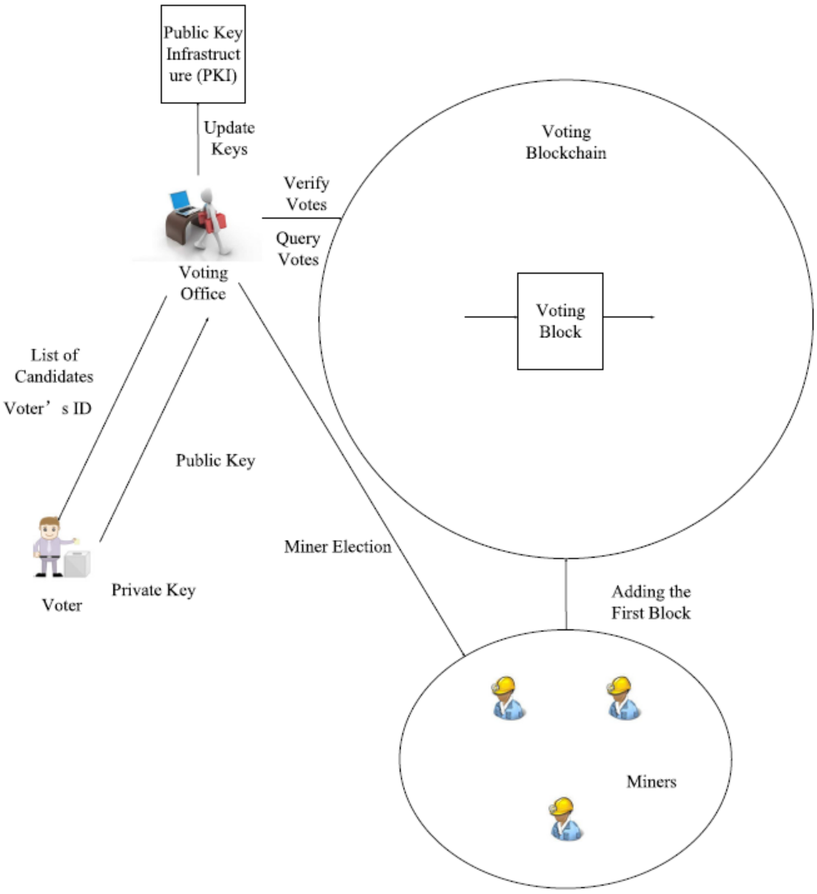
Counter checks collector signature is correct. If not, ballot is discarded. If it is, the ballot is decrypted and the Validator signature is checked. If the *RN* value has not been recorded, the counter will store together the *RN, electionId* and *choice* values.

Administrator
1. $\{voterId, voterCode, voter\text{-}pub\}_{admin\text{-}pub}$
2. $\{ballot, validator, routing\text{-}nodes, VT1\}_{voter\text{-}pub}$
$N1, \{\{col\}_{N3\text{-}pub}, N3\}_{N2\text{-}pub}, N2\}_{N1\text{-}pub}$
3. $validateBallot(\{\{choice, electionId, RN\}_{blinded}, VT1, electionId, voter\text{-}pub\}_{val\text{-}pub}$
4. $checkVoterExists \{\{VT1, electionId\}_{val\text{-}priv}\}_{ercll\text{-}pub}$
5. $\{\{exists?, VT1, electionId\}_{ercll\text{-}priv}\}_{val\text{-}pub}$
6. $\{\{checkIfValidated(VT1)\}_{val\text{-}priv}\}_{admin\text{-}pub}$
7. $\{\{validatedAlready?, VT1\}_{admin\text{-}priv}\}_{val\text{-}pub}$
8. $\{\{\{choice, electionId, RN\}_{blinded}\}_{val\text{-}priv}\}_{voter\text{-}pub}$
Voter
Validator
Electoral Roll
$v = \{\{choice, electionId, RN\}_{val\text{-}priv}\}_{count\text{-}pub}$
9. $\{v, \{\{\{col\}_{N3\text{-}pub}, N3\}_{N2\text{-}pub}, N2\}_{N1\text{-}pub}\}_{N1\text{-}pub}$
Voter ID known – Vote not known
Voter ID not known – Vote not known
10. $\{v, \{\{col\}_{N3\text{-}pub}, N3\}_{N2\text{-}pub}\}_{N2\text{-}pub}$
11. $\{v, \{col\}_{N3\text{-}pub}\}_{N3\text{-}pub}$
Routing Node 1
Routing Node 2
Routing Node 3
12. $\{\{choice, electionId, RN\}_{val\text{-}priv}\}_{count\text{-}pub}$
Collector
Voter ID not known – Vote not known
Voter ID not known – Vote known
13. $\{\{choice, electionId, RN\}_{val\text{-}priv}\}_{count\text{-}pub}\}_{col\text{-}priv}$
Counter

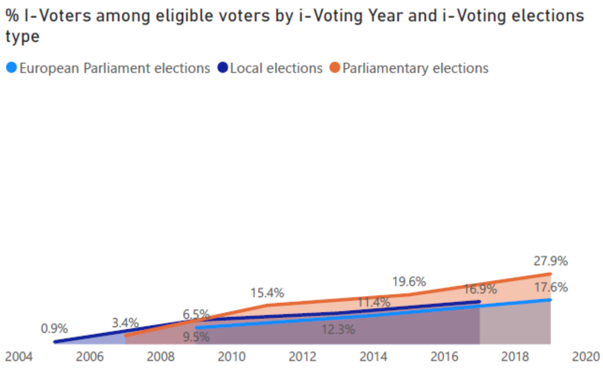
Appendix 6 – Initialization of the e-voting system (*Yi, H. (2019)*)

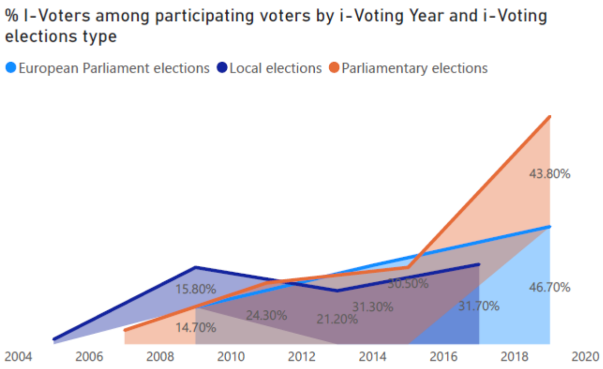


Appendix 7 – Voting process *(Yi, H. (2019))*



Appendix 8 – Questions from Florian Marcus, Digital Transformation Adviser e-Estonia Briefing





Appendix 9 – Discussion with Florian Marcus, Digital Transformation Adviser in E-Estonia.

Firstly, it was mentioned that elderly people are actually using I-Voting (according to statistics available in the Valimised website, retrieved from *https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia*, 17% of I-Voters in the European Parliament elections 2019 belong to the age group >65 years old, for instance);

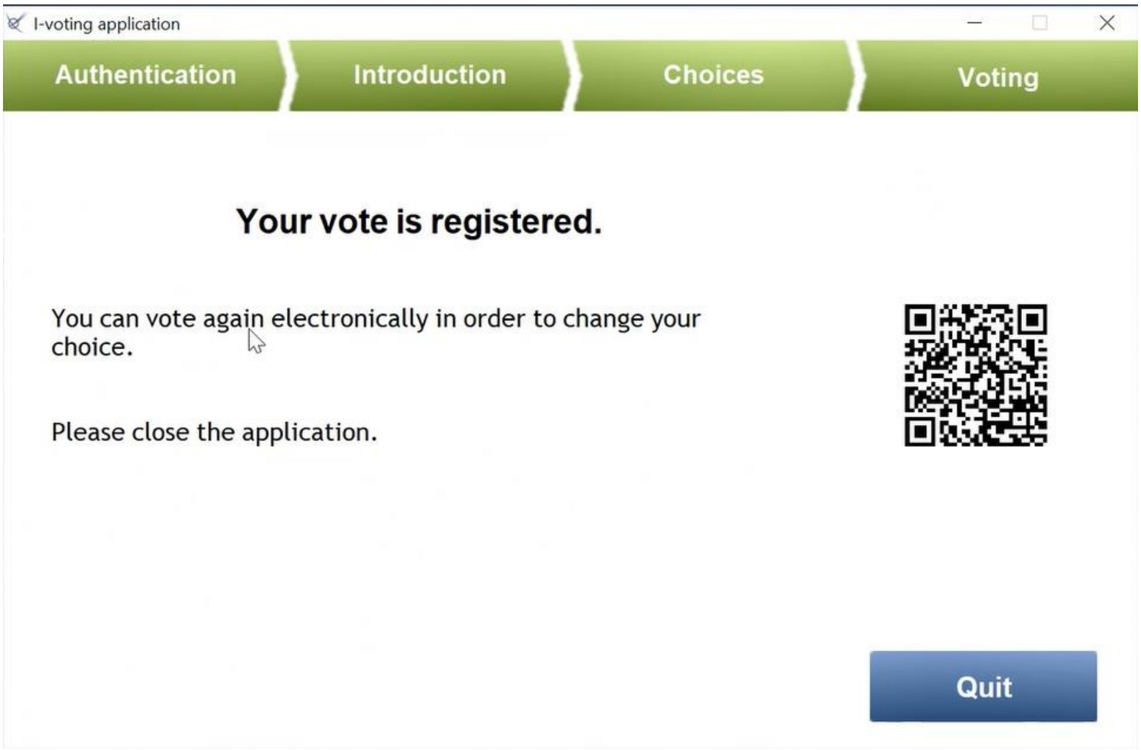
Secondly, the number of internet users in Estonia is significantly high, around 90% in 2017 (according to The World Bank, retrieved from *https://data.worldbank.org/indicator/IT.NET.USER.ZS*, where internet users have used the Internet (from any location and any device) in the last 3 months). This relevant majority of the Estonian population who are familiar with Internet, makes the I-Voting process easier to understand and enhances its use.

Thirdly, it was mentioned the digital identity that is issued to every citizen. Estonians are able to identify themselves through a digital signature, using an ID-Card, Mobile-ID and/or Smart-ID. It's not technically illegal to give citizens ID and PINs away, but the person who abuses the ID and PINs does something illegal. Just like in the physical world, where someone shows to another person his/her paper signature is not illegal but the one who gets to know about the signature will do something illegal by forging the same signature for another document. Regarding the ID-Card and PIN code, this issue is considered more of a matter of awareness raising rather than jailing people.

To the question related to Malware attacks and Social Engineering: the voting application is download from a unique place, reducing the chance for hacking attacks, as well as any other application downloaded from a malicious website, will not be able to access the same points, server and data as the official one. Also, the vote is not submitted through email, against what is verified in other voting systems, in other countries.

A **demo** of how a voter can cast his/her vote was presented. It is a process that goes from

- Authentication --> Introduction --> Choices --> Voting.



Your vote is registered.

You can vote again electronically in order to change your choice.

Please close the application.

The voter's identification details are confirmed (authentication), the favourite party is selected, the voter needs to confirm that the selection was correctly done and, finally, the vote is registered. A **QR Code** is made available for the voter to use it through his/her mobile phone in order to verify that the vote was correctly received through a different communication channel. This QR code is only valid for few minutes so by sharing it on the internet for everyone to see who the citizen voted for is not possible. Also, to generate a new QR code, a new vote needs to be submitted.

How does the government know that every citizen does not vote under intimidation or any other kind of enforcement against his/her will while casting the vote remotely? For that situation, the solution is **"You can vote again electronically in order to change your choice."** According to the *Riigikogu Election Act*, chapter 71, the "Change of electronic votes" provision states that the voter has the right to change his/her vote during a seven day-period.

Regarding Blockchain:

Florian is not so confident that it might be used in the near future once contains a certain and verifiable record of every single transaction ever made, and this might be critical while dealing with voting secrecy and citizens personal data. On the other hand, KSI Blockchain is already used in Estonian e-Health Authority, for instance.

Appendix 10 – Questions from Florian Marcus, Digital Transformation Adviser e-Estonia Briefing Centre on 18th June 2020 to Sven Heiberg, I-Voting Product Manager Cybernetica AS, in the conference "e-Estonia Live: i-Voting as key to future elections", minute 22:07.

FM: *While Estonia started to using Blockchain on a national level almost 10 years ago, I-Voting is not really associated with Blockchain implementation. Was there ever the thought of implementing Blockchain for I-Voting, maybe even right now, or for the future, and if not, why do you think is not necessary?*

SH: *Using Blockchain on top of Online Voting system definitely crossed our minds. We have looked into the properties and capabilities of Blockchain applications, such as Etherium or Bitcoin, and we have determined that it is not suitable for Online voting at this stand. At the same time, we are researching an approach to integrate Online voting with Blockchain using a different model which is "private permissions" blockchain and see if we can add value to the observers through this way. The important thing in case of Blockchain is that you are not relying on a single component to store your information so this kind of separation of duty and distribution of the tasks is a key element in the online voting system architecture and is actually also present in the current Estonian Online Voting system, meaning that each vote that is stored in the digital ballot box is also registered in the external ledger system and there is a later audit step to verify that all of these views match and, of course, if there are any differences, than these steps already taken to sort out those differences where, purely because of technical reasons: "Do we have to reboot?" or "Do we have major cross issues?"*

FM: *Public Blockchain – distribution of the data, would be also a philosophical question whether if ballot secrecy would be still given because is technically everywhere (the vote transaction, across different chains, several copies), if you wanna put it like that.*

SH: *That's a perfect point. Currently, in I-Voting system, the kind of encryption we rely on, this is asymmetric encryption, its security depends on the Key length. We publish some encrypted information so there is the risk that, in a period of time like 30 years, this key length is already approachable to hackers so we might be linking historical voting results is possible to make a link once this key is saved for years, which is a risk assessment to question it, to see if it is risk acceptable or not. To go through Blockchain, we need a different kind of encryption and we need to consider every last thing towards we publish into the Blockchain.*

FM: *Blockchain probably will not come for the next 30 years. Nowadays, we are not in the situation where half of the population have a super computer or quantum computer but one day we will have a lot more computation power than we have right now.*