UNIVERSITY OF TARTU

School of Economics and Business Administration

Institute of Computer Science

Johan Skytte Institute of Political Studies

Master of Arts in Social Sciences

Innovation and Technology Management Curriculum (2017-19)

Rahul Puniani

Conceptualization of a Blockchain Based Voting Ecosystem in Estonia

Master's Thesis (20 ECTS)

Supervisor(s): Mr. Fredrik Milani

Dr. Mihkel Solvak

Tartu | 2019

Conceptualization of a Blockchain Based Voting Ecosystem in Estonia

Abstract: Democracy is an age-old concept coined by the ancient Greeks meaning, 'Rule by People'. World has come far from that, from empires, to kingdoms to finally democracy as we know it. In current democracies, the exercise conducted to be 'Ruled by People' is based up on periodic elections and those elections are conducted via voting, direct or indirect. The ways of voting have been consistent up until the 20th Century with the use of ballot papers and physical counting. The age of technology and engineering since, have brought about changes to the status quo, with introduction of Electronic Voting Machines such as, in India and Electronic Voting via Internet such as, in Estonia which are practiced in every election. But in all of this, something still remains unresolved. When candidates or in turn a government is elected, they are meagre obliged to perform their duties correctly, with little or no accountability and oversight. Even after elections, a government might be unpopular among its citizens, but the citizens don't have means to change anything, before the next elections. This thesis helps to fill this gap with use of newly introduced technology of Blockchain and Distributed Ledgers, and also with the help of newly conceptualized innovative concepts.

Plokiahelapõhise hääletamise ökosüsteemi kontseptsiooni loomine Eestis

Lühikokkuvõte: Demokraatia on iidsete kreeklaste poolt välja töötatud mõiste, mille tähendus on "inimeste valitsemine". Maailm on arenenud sellest ajast kaugele edasi – impeeriumidest kuningriikideni ning lõpuks jõudnud demokraatiani nagu me seda tänapäeval teame. Praegustes demokraatlikes riikides põhineb rahva poolne juhtimine perioodilistel valimistel, mis viiakse läbi otsese või kaudse hääletamise teel. Hääletamisviisid on olnud kuni 20. sajandini ühtsed, kasutades hääletamissedeleid ja füüsilist loendamist. Tehnoloogia ja tehnika on sellest ajast alates olukorda muutnud, juurutades elektroonilised hääletamismasinad, näiteks Indias, ja elektroonilised hääletamisvõimalused Interneti kaudu, nagu näiteks Eestis, mida kasutatakse järjepidevalt. Kuid kõige selle juures jääb midagi ikkagi lahendamata. Peale kandidaatide või valitsuse valimist võivad ja saavad nad oma kohustusi ja ülesandeid täita ebapiisava korrektsuse, vähese või puuduva vastutuse ning järelevalveta. Isegi pärast valimisi võib valitsus olla oma kodanike seas ebapopulaarne, kuid enne järgmisi valimisi ei ole kodanikel võimalust midagi muuta. See väitekiri aitab selle lünga täita värskelt kasutusele võetud plokiahela ja hajusraamatu tehnoloogia kasutamisega ning ka äsja väljatöötatud uuenduslike kontseptsioonide abil.

Table of Contents

1. Introduction

An aggregate of people living together can be termed as a 'Society'. This society grows together as a community (Cambridge Dictionary, 2019). For a society to survive, it needs consensus on issues. From societies to cities to countries at world level, taking consensus refers to democracy and the means of consensus is called voting (Cambridge Dictionary, 2019). The process of recording the consensus can be referred as elections (Cambridge Dictionary, 2019). Therefore, Voting and elections can be termed as a cradle of democracy. Both of the fields, unique but inter-related require both transparency and anonymity. Also, at the same time they must be auditable, such that the method applied in both can be re-assured to be without corruption.

Several methods have been deployed for elections as well as voting. With this age of technology, it is clear to digitalize the pillars of technology to make them more efficient. In many countries, all around the world, voting and elections make use of technology in one way or another. The best use has been recorded in the country of Estonia, where its citizens are able to vote electronically called as I-Voting or Internet Voting (Enterprise Estonia, 2018). But even with nationwide adoption, I-Voting has been sceptic over the lack of conclusive evidence regarding whether the new voting technology had diffused homogenously among the voting population or has remained a channel for the resourceful and privileged (Vassil, Solvak, Vinkel, Trechsel, & Alvarez, 2016). Therefore, going to the level next, is to explore another technology on horizon which has the potential to radically change the functioning processes of the world, i.e. Blockchain Technology, which could assist or overtake the idea of voting electronically which could be accessible and auditable by all.

Blockchain technology in sense, is based upon principles to simplify processes, and staying secure at the same time with multi-node accessible ledger. Therefore, currently implemented electronic voting methods could take a partial or overall assistance from technologies like blockchain to further their case to replace the paper-based methods. Blockchain Technology having benefits of security and consensus, could work in the fields of increasing Election Transparency and Voter Confidence. (Moura & Gomes, 2017).

Technology has already been applied in the fields of supply chain, logistics, healthcare and much more. Many start-ups and national entities are also therefore, looking at the scope of blockchain based or assisted electronic voting methods to conduct their respective elections (Renming, Chen, Zheng, & Mrad, 2017). The blockchain technology is maturing, and collaboration with current voting methods in elections is also increasing. Several countries are conducting trials, and in some countries, Blockchain based electronic voting has already been tested and used successfully. South Korea has planned to conduct trials in the country pertaining to use of blockchain in Voting (Mu-Hyun, 2017) and West Virginia state of United States of America (USA), has already successfully used a blockchain based electronic voting method via mobile app for, its overseas citizens in 2018 (Kelly, 2018). Approximately 150 people successfully voted for the USA mid-term 2018 elections via the app.

In case of Estonia, I (Internet) -Voting has been revolutionary. Garnering almost 44% percent of the total casted votes in the 2019 general elections (the highest proportion since its inception) serves as a proof that, technology and voting can coexist (Valimised, 2019). Maybe there is a need to look at exploring and comparing ways blockchain technology can assist or enable parts of the I-Voting system. Estonia has been chosen as a base for a proposed system as only it has the infrastructure and history to conduct online internet voting nationwide, than any other country.

This thesis aims to look over the possibilities, for the use of blockchain technology in the assistance of voting system in Estonia, conceptually. It looks over the opportunities and challenges relating to the topic, comparing the current internet voting method of Estonia with a blockchain powered voting method.

1.1. Research Questions

The thesis aims to provide a conceptual overview of a new system which could be upheld by the scope of adoption for blockchain technology in Estonia. Following are the research questions formulated:

RQ1: How can Blockchain Technology based voting eco-system transform voting in Estonia?

RQ2: What additional value would a Blockchain Technology based voting ecosystem would deliver compared to the existing one? These values are to be assessed based on standards adapted by Council of Europe E-Voting Standards (Council of Europe, 2017):

- *Legal:* Universal Suffrage, Equal Suffrage, Free Suffrage, Secret Suffrage
- *Procedural:* Regulatory and Organizational Requirements, Transparency and Observation, Accountability, Reliability and security of the system

In RQ1, the capabilities and potential of the proposed system are to be explored over, how it can transform the voting methods, and in turn the elections, and in turn the democratic principles of the country, Estonia. It is to be explored that how can the proposed system fill in the current governance gaps and citizen to government relations.

In RQ2, the proposed system is to be compared with the current system, on the basis E-Voting standards, to explore the additional values it can or cannot deliver than the current one. The overall system is to be compared with each sub-standard, to better understand the benefits and limitations.

1.2. Research Methodology

The research method followed is of a theoretical independent study, being inspired by a case study structure. The approach and structure have been slightly divergent, according to author's frame of reference. The primary objective has been kept as an 'Exploratory' analysis of the current system with the primary data being 'Qualitative'. Basic concepts are outlined as a prelude to the information and research following it, to have a common understanding with the perspective of the author. Figure 1 shows the master thesis structure.
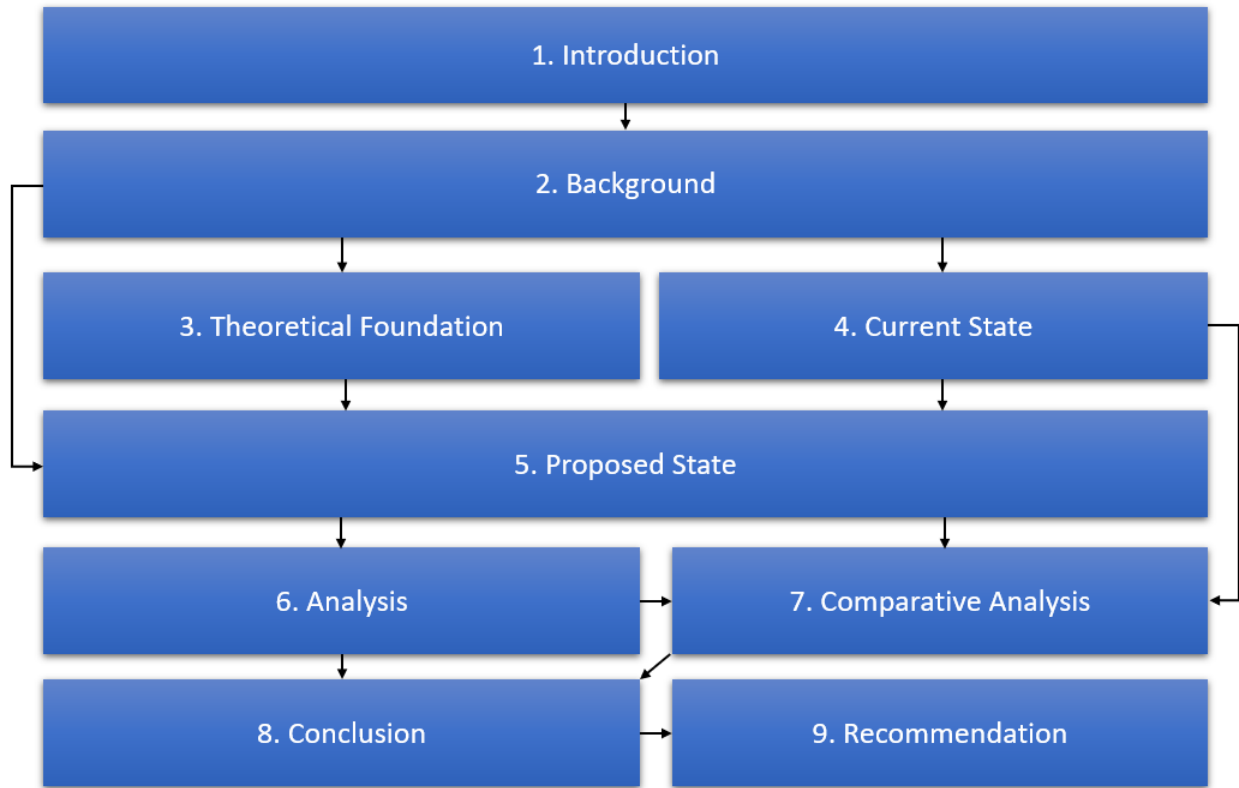
Figure 1 Master Thesis Structure. Source: Author

The basic concepts related to the topic are listed down in background, with the motivation behind the need for change. Then, an extensive Literature Review is conducted via summarizing peer-reviewed articles, reports and conference papers published in the domain of voting and blockchain. The literature is extracted, analysed and synthesised to be a foundation for the proposed system.

Research is then conducted via analysing the current state of electoral system and Internet (I) – Voting method conducted in the country of Estonia. The resources are extracted from official website of the government, and related sources. Followed by the mapping of the current I-Voting system, information is compiled.

At the same time, the limitations of current political systems are listed and informed. With theoretical mapping and research, the proposed concepts to overcome these limitations with the help of blockchain technology are outlined. The scope has been limited to the theoretical research and not developing an own blockchain based technical system. Analysis has been conducted independently with use of analytical tools supported by author's interpretation.

With all the information and research in hand, certainties are drawn out for the scope of answering the research questions. At the same time, with continual feedbacks with supervisors, research is be compiled, and conclusions are made, followed by further recommendations. Thereafter, references are cited and open license for this thesis as appendix.

The author's contribution to the thesis is coherent to disrupt governance models and elections by introducing innovative concepts for the proposed system which would offer a new way of defining voting and democracy. The contribution is also to synthesize two different streams of political science and computer science into one. The solution proposed would benefit researchers working in the similar fields, and in a long run, citizens and the government, to look over their relationship with a different point of view. The thesis has been limited in scope over the vastness of the topics. Information has been kept condensed and in brief.

2. Background

2.1. Voting

Voting can be defined as an action or process of indicating choice, opinion or will on a question, such as unanimously choosing a candidate for a position or choosing a policy (Cambridge Dictionary, 2019). Voting can be conducted at various levels. Either related to the rule of law such as Voting for representative delegate for at local or national levels, Or unrelated to the rule of law such as within a board room meeting.

Voting (Electoral) System and Voting Methods are distinct terms. The former might refer to the electoral system deployed by the conducting organization such as plurality system, majoritarian system, proportional system among others. Whereas the latter, refers to the procedure of voting performed by the designated voters which assists the system (Encyclopaedia Britannica, 2019) . Current voting methods include;

2.1.1. *Paper-based methods*: These methods consist of paper-based voting. The most prevalent method is by using paper ballots on which the voters can mark their preferences before putting into a secure box. This procedure may include marking down a symbol or name of a political party or a person (Ballotpedia, 2018). The most common voting method uses paper ballots on which voters mark their preferences. This may involve marking their support for a candidate or party listed on the ballot, or a write-in, where they write out the name of their preferred candidate if it is not listed. Most countries around the world use, some sort of Paper-based method including Optical Scanning Voting Machine (Ballotpedia, 2018).

2.1.2. *Electronic methods*: These methods of voting can be defined which are conducted via use of softwares, hardware such computers or machines. This could be done via Internet, in case of Estonia (Enterprise Estonia, 2018), via EVMs (Electronic Voting Machines), in case of India (Election Commision of India, 2018), or via Direct Recording Electronic (DRE) Methods, in case of several states of United States of America. (Ballotpedia, 2018). Other countries to use some sort of electronic voting method include Brazil, Canada, Peru and Argentina (Laukkonen, 2018).

2.1.3. Use of *Electronic* methods over *Paper-based* methods: Use of electronic based methods for use in elections is relatively new. While there have been noted vulnerabilities found in the use of electronic methods, there is an inevitable historical bias towards trust in paper-based voting (Willemson, 2017). Electronic methods have been proven to be cost-effective when done on the large scale as they decrease the sheer amount of resources need to run elections or voting via paper-based alternatives, as it is, in case of Estonia (Enterprise Estonia, 2018). Schemes and modifications in electronic voting can offer mobility and convenience to cast vote securely in any location, which can further raise potential voter turnout (Zhen-Yu, Ju-Chuan, Lin, & Wang, 2014).

2.2. Elections in Estonia

According to the *Riigikogu* Election Act (Parliament Election Act), the parliament is constituted of 101 elected members. Each voter has one vote. The election results are determined based on the principle of proportionality. In elections, candidates can run via Political parties, which are registered as NGO or as an independent candidate. The voting procedure is carried out offline via polling booths which have all the necessary distribution of ballot papers, ballot box and voting booths. The ballot is always ensured to be secret (RiigiTeataja, 2019).

At the same time, electronic voting or Internet (I) - Voting is administrated by the State Electoral Office. In this case, the voter is allowed to vote by herself or himself via electronic means. The information security policy of the electronic voting system, protocol and guidelines are approved by the State Electoral Office. Several tasks are completed prior to the start of the electronic voting phase. State Electoral Office also creates encryption key for the electronic votes and decryption key for opening the votes. The decryption key is distributed among the members of the State Electoral Office and National Electoral Committee (RiigiTeataja, 2019).

The office is also responsible to determine the operating systems in which application can be run, based on the data of most widespread used operating systems. Then, in the voting phase, the voters are allowed to vote electronically in an organized manner. They are lead step by step to vote and confirm their vote to the respective candidate of respective political party or independent. Voters are allowed to vote as many times as possible, but in this case, only the last vote is counted as the corrected vote. The voters also have the option to verify their vote via a smartphone app (RiigiTeataja, 2019).

In case of some mishaps or fraud, the National Electoral Committee can suspend the electronic voting and also has the responsibility of notifying the voters about any suspension or restarting of the electronic voting phase. The system is designed in a way that, electronic voting phase is generally before the actual offline voting day. In case of suspension of Electronic votes / voting, voters still have a chance to vote for their favourable candidate offline via paper ballot in the voting booths (RiigiTeataja, 2019).

2.3. Government and Accountability

Each job pertains accountability. When elections are conducted after each fixed term, political parties and candidates call for votes in return for promises in policies. But after elections, it is always a position term pass, when they can't be held accountable, and have the job fixed of running a country. A government is for the people and by the people, but unfortunately controlling the government is a periodic process and not a continual one.

The rise of populism, stagnant growth, dissatisfaction with the national governments worldwide leads to peaceful or sometimes violent protests, revolutions and helplessness of citizens towards their government. (Economist, 2015). It is regularly possible to see, that after voting, in elections or referendums or otherwise, citizens change their mind but they are not able to do anything, for example, the stalled case of Brexit (BBC, 2019) or formation of a political movement formed by Estonians after the election results called '*Kõigi Eesti*' for greater positive civil society in Estonia (ERR, 2019).

The current system which involves cumbersome organization of elections once every 4/5 years is hard to replicate more periodically. But the power of Technology and moreover Internet allows us to think beyond and re-think democracy. With the use of Internet Voting System, and with the assistance of blockchain technology, we could foresee a future where the citizens are able to control/change/affect their national government/leaders promptly and securely. The silent majority can have their voices heard in real-time. This is inspired by following opinion: A government is made by its citizens, and hence the citizens must be able to control it.

2.4. Blockchain Technology

Blockchain can be defined as a technology used to create a digital database (ledger) containing blocks of information that can be simultaneously used and shared within a large decentralized, publicly accessible network with use of cryptography (Swan, 2015). The blockchain technology was envisioned by a paper published under the pseudonym of Satoshi Nakamoto in March 2009 (Nakamoto, 2009). The paper introduced the world to the concept of Bitcoin, and in-turn, Blockchain Technology. The paper established solving trust issues in online payments by eliminating third parties and taking it to peer-to-peer network. The proposed solution, proposed hashing of the network timestamps transactions on to a chain of hash-based records, which cannot be changed or tampered with, without consensus (Nakamoto, 2009). The technology, fairly new, has sprung up ideas of applications in several domains such as supply chain, banking, transportation etc. Blockchain powers automation and security. Permissioned blockchains have seen a larger growth with institutions implementing the technology in the fields of the food safety in cooperation with government agencies, financial institutions, smart properties etc. (Renming, Chen, Zheng, & Mrad, 2017).
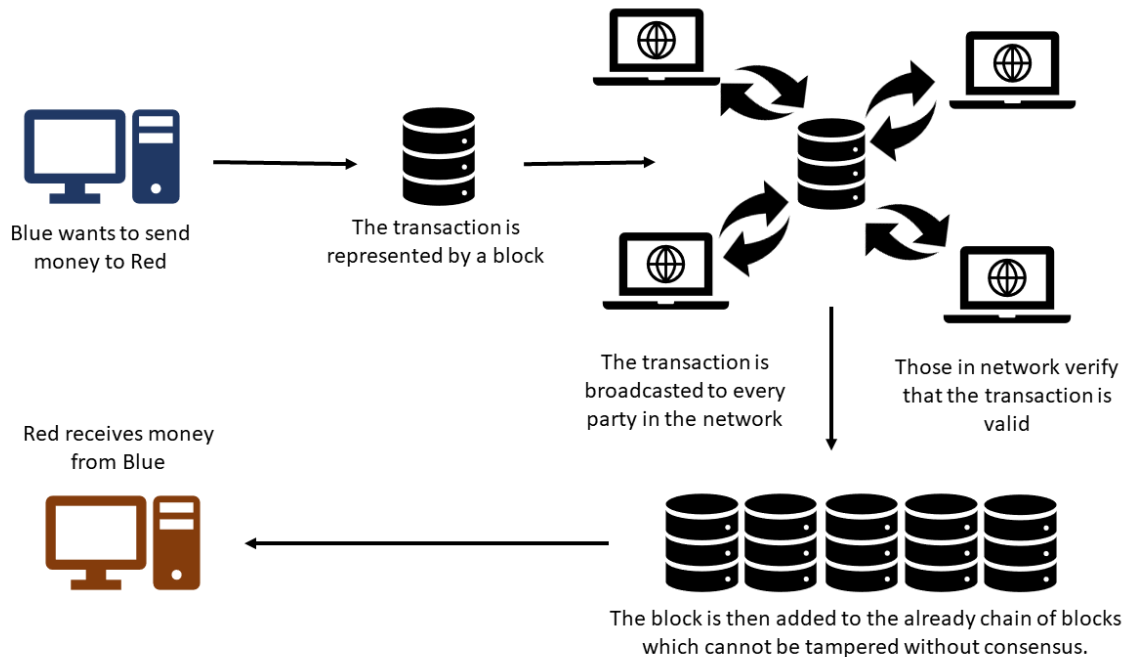
Figure 2 A visual representation of blockchain. Source: Author

Overall blockchain technology works on the principles of Distributed ledger technology (DLT) which basically offers a validation mechanism based on consensus through multiple channels of computers which facilitate peer-to-peer transactions without the need of a central authority to regularly update or maintain the information generated by the transactions.

As depicted in Figure 2, blockchain works on peer-to-peer trust and consensus. Once transaction conducted on a block has to be verified by each node on the network. When the transaction is verified, then it is accepted in the blockchain. This chain is termed as 'Blockchain' to the basics. The more transactions that occur, have to verified by each node, and overall then, the size of the blockchain also increases. Therefore, the bigger the blockchain, more-time is consumed in verifying the block and more energy is also consumed (Voshmgir, 2019).

A block can have several transactions, but it is important to limit the number of transactions in a single block. This can be achieved by the infrastructure of the blockchain, it can be decided that, how many transactions can each block have. Hence, the number of blocks depend upon the set of blockchain (Voshmgir, 2019).

'Hashing' is another import element of the Blockchain Technology System. Hashing basically refers to masking of the transactions cryptographically. It is achieved using a mathematical function. Input string of any length is converted to an output of a fixed length. In Bitcoin, the input transactions are run through a hashing algorithm called SHA (Securing Hash Algorithm) - 256 which gives out an output of fixed length (Nakamoto, 2009). The hash function makes sure that the output has a random yet, auditable masked output with set of keys. A transaction is always

11

added after running through a hash algorithm, and hence, a single block in general would contain transactions masked as hash functions (Rennock, Cohn, & Butcher, 2018). Examples of inputs after hashing would be as following,

For 'John Doe', it would be '6cea57c2fb6cbc2a40411135005760f241fffc3e5e67ab99882726431037f908' and,

For 'Janie Doe' it would be '775be8f1663e5902fe8044312e2be936a129d1b9f5152f296d08f86edfdf0161' (Xorbin, 2019). As observable, the output hash is of fixed length even though inputs were of different lengths. We can say that similarly, with use of time-stamps even with unique names, the output would always be unique.

All the transactions and the identities of the participants are secured by hashing, which is to secure via use of cryptography. Once information has been put on the ledger, it cannot be tampered with, without the consensus of the network (Rennock, Cohn, & Butcher, 2018). There are two types of blockchain networks:

- *Permissionless or public blockchains*: Following the core concept of blockchain, access to these networks is opensource and anyone can access or conduct transactions. For example, Bitcoin (Rennock, Cohn, & Butcher, 2018).
- *Permissioned blockchains*: These networks are exclusively owned and by-large extent, centralized where specific group of participants have the access to the blockchain network and permissions to conduct the transactions. For example, a consortium processing transaction among its entities (Rennock, Cohn, & Butcher, 2018).

Table 1: Major Differences between Public (Permissionless) and Private (Permissioned) Blockchain (Voshmgir, 2019):

	Public (Permissionless)	**Private (Permissioned)**
Access (Read and Write)	Public to anyone	Upon Invitation only
Network Actors	Unknown	Known to each other
Native Token	Yes	Not Necessary
Security	Economic Incentives via Proof of Work, Proof of Stake, Proof of Space, Proof of Burn etc.	Legal Contracts, Proof of Authority
Speed	Slow	Fast

Examples	Bitcoin, Ethereum, Litecoin etc.	R3 (Banks), EWF (Energy), B3i (Insurance)
Advantage	Lower Infrastructure Costs	Reduces Transaction Costs.

2.4.1. Smart Contracts

A smart contract is a digital self-enforcing contract that is managed by a Peer-to-Peer Network. Smart contacts are electronic authorization tools for parties to provide an enforcement and coordination framework for agreements between network participants. Two parties can use them to formalize agreements between them (Voshmgir, 2019).

These self-enforcing agreements are embedded in computer code managed by a blockchain. A set of rules are contained in the computer code which the parties agree upon before. If and when the conditions of the rules are met, the agreement is automatically enforced. This ensures the parties of the authenticity and transparency of the process. Since, only the matching of the rules will let the contract to be executed, each party takes care that the conditions are correctly met. The set of rules and access rights are stored on the blockchain which is a shared ledger, preventing the data from deletion or tampering. The smart contracts are also auditable, as they provide a possibility embed business rules and governance knowledge with computer code (Voshmgir, 2019).

Aspects of Smart Contracts (Voshmgir, 2019):

- *Technical Aspects*: Smart Contracts are self-verifying, self-executing and tamper resistant.
- *Legal Aspects*: Smart Contracts can map legal obligations into an automated process. They also provide a greater degree of contractual security, if implemented correctly.
- *Economical Aspects*: Smart Contracts have higher transparency, less intermediaries and lower transaction costs.

3. Theoretical Foundation

3.1. Literature Review Method

From the University Library's Database, reputable sources were used such as:

- EBSCO Discovery Database search engine for University of Tartu
- Science Direct Portal (www.sciencedirect.com)
- Scopus Portal (www.scopus.com)
- Google Scholar (scholar.google.com)
- Web of Science
- E-journals and e-books Publication Finder for University of Tartu
- IEEE Explorer

The access to the databases and portals was conducted ethically and legally via University of Tartu's Computer Network and its relevant subscriptions to the sources. Portals related to Science, Information Technology were chosen as a priority because of their closeness with the chosen topic.

Search Strings used to search were:

- "Blockchain OR Blockchain Technology"
- "Voting OR Electronic Voting OR Internet Voting"
- "Blockchain AND Voting"
- "Technology AND Voting"
- "Internet Voting AND Estonia"
- "Internet AND Democracy"

Criteria for inclusion of Article/Publication were:

- Relevance to the topic – The article must be directly related to the area of research which is related to Blockchain, Voting and Technology.
- Age – Article must not be more than 10 years old. i.e. Publication date must not be later than 2009, as the first published material about Blockchain was published in 2009, and only then the research has continued and spiked in recent years.
- Peer review – The articles or publications must be extracted from reputable peer-reviewed sources. Peer-reviewed articles go through hard quality checks, also they add the credibility to the opinions as they have been reviewed extensively.
- Attributes – Qualitative data is preferred as this thesis is also qualitative. This is assessed by choosing publications which have more to say on theoretical than technical aspects.

3.2. Literature Review

Since the inception of electronic voting, there have been several different methods to pursue it. Research has been conducted accordingly. The topic of blockchain technology in voting is a specific interested topic as of today in 2019. Several papers have been published, either being white-papers from private organizations working in the field or conference proceedings happening all around the world. Tracking the information, the idea of blockchain and voting is advancing at a fast pace. There have numerous schemas or protocols that have been published to standardize and streamline the use of technology.

Models have been created on the protocols of PHANTOM (Srivastava, Dwivedi, & Singh, 2018) to showcase, how the protocol could be established even with use of current EVMs (Electronic Voting Machines and not with browsers or apps on hand-held devices. This would help countries which are developing and many of the citizens do not have the access to technology and literacy.

This could be an active replacement of current EVMs. Same paper establishes that sustainable energy consumption and high computational speeds can be achieved at the same time. They also suggested Borda method of counting votes, such that, to avoid cases of forced voting or booth capturing. Much of the research and study conducted in the sphere is also linked to the use of Ethereum based blockchain voting solutions (Yavuz, Kaan Koc, Can Cabuk, & Dalkılıç, 2018) and in general Bitcoin based solutions.

Talking about under-developing countries and their implementation of electronic style of voting, another paper outlines the risks and dangers posed by relying on blockchain technology. (Harris, 2018). At one hand, the technology does have a potential to help assist in transparency and facilitate overall trust but problems such as rigging of elections, bribery, and overall corruption is quite high in countries with low Human Development Index. For those countries, they would first need to have state confidence in authorities and the state authorities have to create an environment of political peace, then only electronic voting would be successful (Harris, 2018).

In a survey conducted over remote electronic voting methods, (Schneider, Meter, & Hagemeister, 2017), it showcases different attributes influencing the use of the method, such as Availability, Eligibility, Integrity, Anonymity, Transparency among others. It is very important the voting method is practical and could be applied within limits of the budget and the infrastructure of the place to be conducted in.

Also, to prevent from attacks and coercions, remedies should be in place such as cryptographic shuffles, different level of encryptions. The paper surveyed several protocol systems of remote electronic voting including, 'Public Key Encryption', 'Homomorphic Encryption' and 'Blind Signatures + Secret Sharing' and alas, it pointed out that remote voting is still a topic to be researched about in case of large scale national elections but could already be used for low-coercion environments such as student elections in a university (Schneider, Meter, & Hagemeister, 2017).

But not everyone is convinced such that, going through published white-papers of several companies trying to make Blockchain Voting a reality, (Agora, 2018) (Votem, 2017) (Polys, 2018) among others, gives a positive outlook. They claim to promise enhanced and complete transparency with voter anonymity and to reduce costs. They mostly compare themselves with traditional voting methods such as ballot paper and EVMs.

Although, each over a slightly different way of protocol such as Agora, proposes a bulletin board based permissioned blockchain and Votem would use a private blockchain with additional public blockchains for verification and audit. The companies tend to be on the optimistic outlook over the risks posed by remote electronic voting (Puiggali, Choliz, & Guasch, 2010). If the votes are casted over the network or the internet, encryption and decryption is a major challenge to be solved. The risks of voter fraud and deletion, could be mitigated by cryptographic voting receipts. But at the same time it has been noticed that, the it could violate privacy as a vote could be tracked back to the voter.

One of the recent successful attempts to apply blockchain based internet voting was applied in West Virginia, USA for its 2018 Mid-Term Elections. (Voatz, 2019). A total of 144 votes were taken into account, and it made historical use of the blockchain technology for voting at a national government level. The voters voted via an App among other steps. The process has been audited and declared as a success to follow up. This has demonstrated the future use and case study of use of Blockchain based-internet voting.

Certain proposed conceptual protocols would also include features which are seen rarely in current methods, such as allowing the voter to have a protest vote, where the voter may have a blank vote representing the dissatisfaction with the current political system or election (Ayed, 2017).

If Blockchain is not enough, Quantum Blockchain is another domain which might have a scope. In a published article, (Sun, Wang, Kulicki, & Sopek, 2019), the authors demonstrate and propose a voting protocol which they term as simple, based on Quantum Blockchain. The protocol would offer enhanced anonymous, binding, eligible, verifiable, fair and self-tallying voting. The major advantage of this protocol to the traditional blockchain would be non-reusability.

Another interesting concept was published in a paper which describes the use of intelligent agents and multi-agent system concept for Auditable Blockchain Voting System (ABVS). (Pawlak, Poniszewska-Maranda, & Kryvinska, 2018). The ABVS system in general is a non-remote and rather supervised voting method where the use of internet is done in order to transfer votes to store them into a blockchain.

Thus, it does include the traditional way of voting in a polling station, but it adds a layer of electronic authorization. Each voter has a VIT (Vote Identification Token) which is used to identify and confirm the voter in several steps. After the vote has been done, the vote is confirmed by a VVPAT (Voter-Verified Paper Audit Trail). Since, the system has several steps, the paper proposes to modify its node structure, with multi-agent system which is distributed and

decentralized, to have intelligent nodes for better communication (Pawlak, Poniszewska-Maranda, & Kryvinska, 2018).

In a paper published to compare the tradeoffs of applying blockchain technology compares over what we can lose and what we can gain from the use of it. (Heiberg, Kubjas, Siim, & Willemson, 2018). Some solutions are pointed to be only beneficial to be used at small scale such as board room meetings than large scale such as national elections. Complexity would increase dramatically in light of the stakes of the elections. To have a simple interface, there might be a very complex structure and back office behind. Although trust might be high, the costs pertaining to it might be higher. For an election, depending upon the numbers, high costs would incur as energy costs to run the big rig machines. Usability at individual level is also pointed out (Heiberg, Kubjas, Siim, & Willemson, 2018).

Using the technology would also mean increased times of processing the vote. The research states that use of smart contracts and related protocols would be highly beneficial in addition with blockchain technology. (Heiberg, Kubjas, Siim, & Willemson, 2018). And perhaps studies have been conducted over the use of smart contract and blockchain for voting. In the paper published, (Hsiao, Tso, Chen, & Wu, 2017) authors showcase that use of smart contracts can enhance the voter's confidence and reduce consumption of resources.

Another proposal of a Blockchain Based E-Voting System proposes the use of permissioned blockchains, which would be a variation of consortium-based blockchains. They would use the consensus algorithm of Proof-of-authority (POA) which means, the transactions would be validated by approved accounts. Votes would be casted a ballot smart contracts and then added on the blockchain. When a voter casts the vote, the ballot smart contract interacts with the blockchain, and after receiving consensus, each vote is added as a transaction on the blockchain and each voter would receive a transaction ID for auditing (Hjálmarsson, Hreiðarsson, Hamdaqa , & Hjálmtýsson, 2018).

For any electronic method of voting, security is always a risk. The main hindrance to the advancement of such methods is the trust over the security. A study done to analyze blockchain and internet voting, the authors conclude that security should not be an excuse to move forward to modernize our way of life (Akbari, Wu, Zhao, R. Arabnia, & Qu Yang, 2017).

3.3.Literature Summary

Summarized from the literature, in the author's opinion, the use of technology and specific blockchain technology can be different in different methods. For some, it's a mix of traditional and blockchain method, whereas for others, it's a total overall blockchain solution. The blockchain technology can be noted to be applied at different stages of different processes. It can be actively used to assist the current methods to enhance their attributes of privacy and transparency. Several secure transactions also take place over the internet today, which would have been unimaginable 50 years ago. Other issues such as scalability could be resolved by using parallel processing.

The main advantage that comes from blockchain and distribution ledger technology is that, it is tamper-proof or as can be said, it is very difficult to be tampered with. Even, a small change in a hash in one block, will raise automatic concern to the other partners of the blockchain, and a simultaneous effort to change the same hash in multiple ledger will require humongous resources. Electronic voting powered by distributed ledger would uphold not only the basic principles but also, ensure active participation from the citizens who elect their leaders.

At the same time, use of blockchain technology gives transparency to the stakeholders. When talked in the context of elections, depending upon who all will be the partners in a permissioned ledger, the voters, the elected representatives and the election body could have the power to see real time changes in the votes.

This would be ultra-beneficial when we think about the idea of continual voting. Realtime changes and fluctuations to the voting number could tell us the satisfaction among the citizens for its government. Citizens would be able to change their vote depending on the enacted law, but ledger technology will make it possible and securely.

4. Current State

4.1. Voting System in Estonia

The general election which is conducted nationwide to elect the '*Riigikogu*' (Parliament) and in turn the government every 4 years. Estonian citizens who have attained the age of 18 or over up till the month of March of the Election can vote. Estonian citizens who have attained the age of 21 or over, can stand in election as candidates. Non-Estonians cannot vote in the National Elections regardless of their stay in the country. Estonians living abroad are also able to via Postal votes or Voting at a foreign representation of Estonia or Online. (ERR, 2018).

Estonia is divided into 12 electoral districts according to the population distribution. Tallinn has 3 districts and Tartu is the only city with own electoral district. The other cities are falling into respective districts. Each of the electoral district have definite number of mandates (seats) which can be achieved by the parties. The combination of the seats equates to 101, which is the number of members of the Estonian Parliament (*Riigikogu*). Voting is conducted either in person at a polling station or in advance online. The most popular option, increasing with each election is the method of Internet-Voting where citizens are able to vote in advance using their chip-enabled ID Cards. Citizens are free to choose the voting method they desire (ERR, 2018).

A political party is a legal entity with at least 500 members nationwide in order to be legal. These political parties are able to participate in an electoral district with a list of candidates. A list would have the same number of seats available in a district, plus two. (If a district has 8 seats, a party list can have 10 candidates). Independent candidates can also run in the elections but they have to follow same system as a party list. But voters do not vote for a political party but are able to vote for specific candidates. But these votes garnered are later divided and distributed amongst the political party lists (ERR, 2018).

The results are calculated combining the votes and distributing among the party lists in 3 batches, Personal mandates, district mandates and compensation mandates. Each district has set number of these batches, but in total there are 22 compensation mandates, 12 personal mandates and 66 district mandates, making the total of 101 mandates. There is a threshold of 5% of total votes, which should be taken in an electoral district. Overall, these mandates are distributed using a modified d'Hondt method which ensures each political party would get proportional representation in the parliament. But at the same time this system has only lead to coalition governments, as getting a majority in the mandates is a very difficult task. The current system of distributing the votes has an advantage for smaller parties who have received less votes in proportion to have a greater representation. But at the same time, the system is rigged for the most popular party, as they end up receiving less mandates, even being most voted (ERR, 2018).

Therefore, political parties with different ideas and poll promises, who are running against each other, have to compromise and come together to form a government, leaving their own promises behind (ERR, 2018).

4.2.Internet (I) – Voting System

To make a distinction between other electronic means of voting and its own system, Estonia designates itself to be using 'Internet Voting' or 'I-Voting'. This also means that, internet voting can be done through any device over the internet connection albeit with active personal ID cards. In Estonia, I-Voting has been in use since 2005. Each person who has the right to vote in the country also has the right to vote via the internet at the elections and referendums. This has been possible because, the country has a legal basis of digital signature and all acts concerning conducting an online election. Also, most of the voters possess the ID card which enables them to securely identify themselves and vote (State Electoral Office of Estonia, 2017). It should be also understood that, currently, electronic means of voting is just additional or optional way of voting.

Internet Voting is part of the whole voting process of the election. Therefore, the scope of the use of Internet Voting System covers the stages of, casting the votes via Internet, the counting of votes and the after the election results, the destruction of the necessary key which is used for counting votes. There are separate pre-requisites for the Internet system to work such as availability of the list of voters and the list of candidates, calibrated properly, such that they are correctly presented with respective polling division and electoral district (State Electoral Office of Estonia, 2017).

Also, the votes casted over the internet are counted separately and the results of which are added to the results of counting of paper votes, such that duplicated votes aren't counted twice. The voting period of Internet Voting is generally before the election day itself as prescribed by the law. Therefore, in practice a voter can change vote casted several times until the deadline. This provides the flexibility for the voter to be better decisive and in case, the person change mind. I-Voting is also done before the election day, such that, if any virtual attacks do happen or something hampers the I-voting system, then those who have voted during the I-voting phase could vote again at a polling station (State Electoral Office of Estonia, 2017).
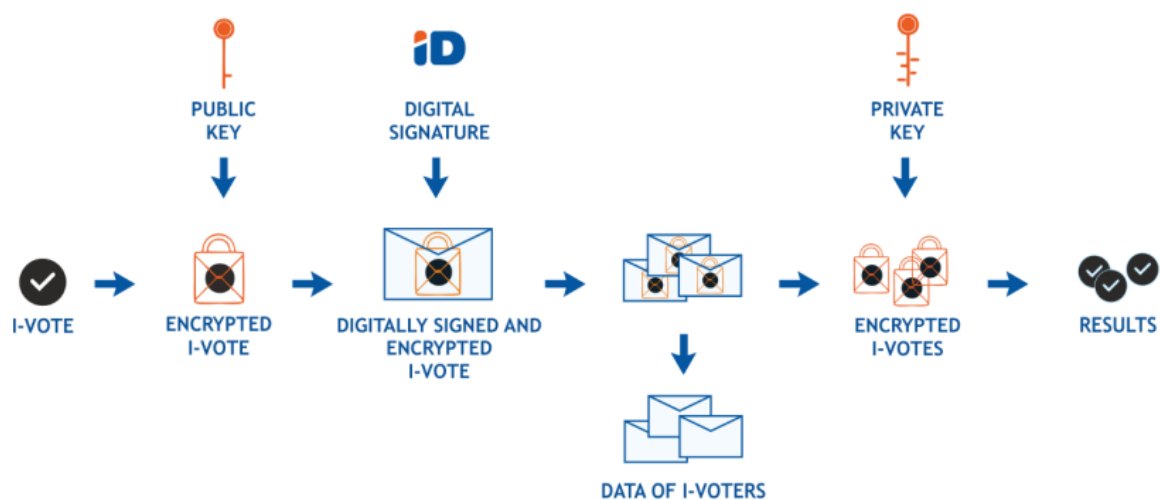

Figure 3 Envelope Scheme of I-Voting (State Electoral Office of Estonia, 2017)

The security of the I-Voting is preserved by the use of legally accepted digital signature. This is a function of the state ID card, whereby one can authenticate digital signatures at various levels. This also lets the state authorities fulfil the criteria of personal identification of the voters voting. A voter also has the chance to verify whether their I-vote has been casted successfully. This can be done by using a device separate than the one used for voting (State Electoral Office of Estonia, 2017).

The I-Voting system works on principles of so-called 'envelope scheme' as depicted in the figure 3 whereby the votes are held in form of virtual envelopes and forwarded along. This helps to maintain the security and integrity of the system. The steps as depicted show that, a voter when I-voting encrypts the vote with a random number generated with a specific public key which forms an 'inner envelope' then, signs the encrypted vote by using the digital signature method of the ID card making it the 'outer envelope' (State Electoral Office of Estonia, 2017).

The vote encrypted with the public key can only be decrypted by the private key which reassures security in the system. Among other processes, during the counting of the votes for the results, mixed and anonymous votes are decrypted with the elections-specific private key, and then the summarized results of the I-Voting are issued. (State Electoral Office of Estonia, 2017).

The current system is organized in such a way that there are principle parties which are responsible in the whole voting process and then, secondary parties which are responsible for support to the principle parties. The voting system has four distinct principle parties as seen in the figure 4, which each having the following functions:
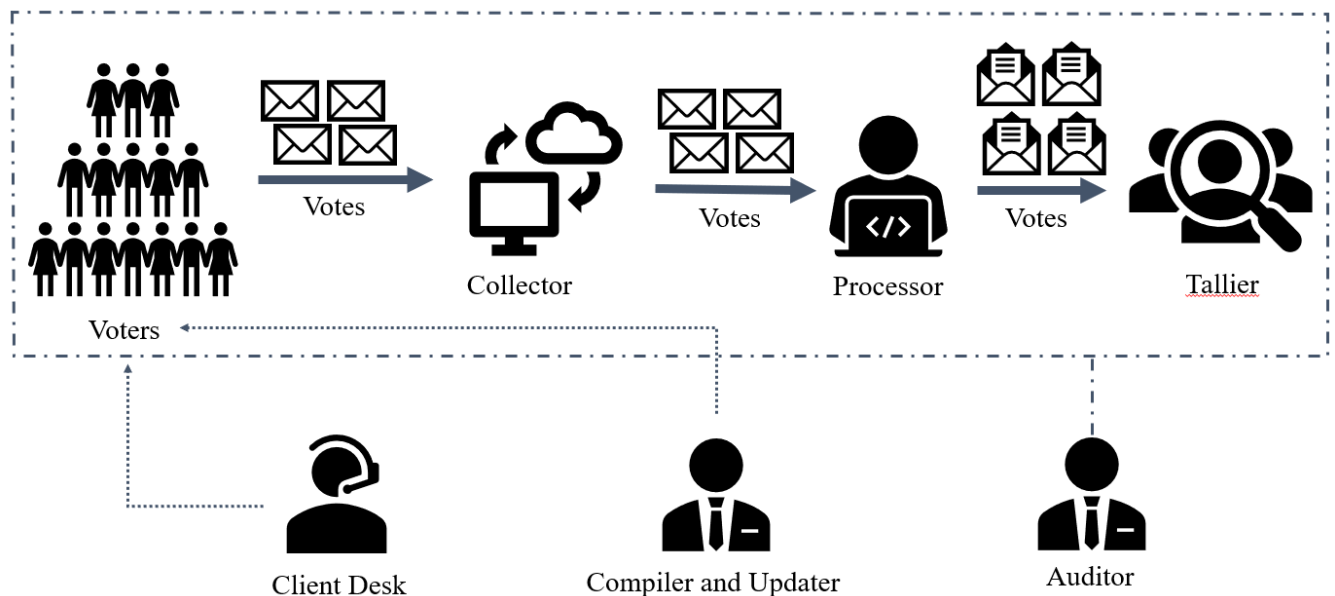

Figure 4 Internet (I) Voting System in Estonia (State Electoral Office of Estonia, 2017)

(i) *Voters*: Voters are responsible to vote according to their preference through voter application in the computer over the web. With the help of the application, the voter makes their choice, encrypts it and then after signing digitally, sends it to the collector. The voter also can verify if the vote has not been tampered with, and is securely sent via a separate smartphone application.

(ii) *Collector*: Collector here is a virtual server system which assists the voters in voting and accepts the encrypted I-votes. The collector is also responsible for the answering any queries related to verification and integrity of the vote. The provider of the collection service then, signs the overall votes and logs and then forwards them to the processor at the end of voting period.

(iii) *Processor*: The processor with help of the system processes the votes casted over the voting period and verifies the integrity and authenticity of the digital signatures. The processor is responsible for deletion of duplicate voting, parallel voting and those who voted at a polling station. (Only the last vote counts). Then the processor removes the personal signatures (identification) in order to anonymise, from the votes and sorts them by electoral districts. A sub-role of mixer can be counted in this process, where the votes are randomly mixed and then forwarded for final counting.

(iv) *Tallier*: The Tallier is the final step for the voting process. Tallier holds the private key and is responsible for adding the anonymized votes to the final results.

Then, there are secondary parties in the voting system with responsibilities as follows:

(i) *Compiler and Updater*: Its job is to compile and update the voter list according to the law/elections stipulated. The list is susceptible for change during voting.

(ii) *Client Desk*: Client desk is the point of contact for the voters in case of any issues and helps them to bridge communication with the collector and its queries. All the queries are later logged into a database.

(iii) *Auditor*: Auditor is responsible for auditing the whole system and process within the principle parties and check the integrity of the functions performed.

Some important external services are Identification, Signature and Registration Services respectively. And all of the role of the parties are done using several tools including, Voter Application, Verification Application, Key Application, Collection Service, Processing Application, Mixing Application and Audit Application (State Electoral Office of Estonia, 2017).

4.3. Characteristics of Current System

(i) *Flexibility*: The Voting System works in Estonia in a way that, voters have an option to either choose to vote online via internet or ballot paper. Therefore, Internet Voting system is just an additional and optional for voters to use. Voters are allowed to vote via ballot paper even after voting online. In this case, duplicate votes are annulled and the final vote is counted in the results. But overall, the current system provides flexibility to the voter in terms of voting for their favourite Candidate.

(ii)   *Trustworthy*: Each election period, people choosing to vote online is increasing. This refers to the idea that citizens are becoming more confident in voting online, because of accessibility among other reasons. The 2019 Parliament elections and European Parliament elections in Estonia saw an increased more than 40% participation by internet voting. Although the overall voter turnout hasn't increased much, but the internet voters have increased proportionally (Valimised, 2019). Anyhow, the increased voting numbers would refer to the increase in trust of voters for switching from their old voting method, among other factors. This trend serves to prove that among people who already vote, are increasing adopting the internet voting.

(iii)   *Security*: The security of internet voting is ensured via several stakeholders. Firstly, the encryption model and the envelope scheme makes sure that votes are secured from the point where voters confirm their participation to the point, results are announced. State Electoral Office upholds the principles of information security and transparency along the process.

4.4. Limitations of Current State

4.4.1. *Just a supplement to ballot paper*

Although there are several positive characteristics of the current system of ballot paper voting + electronic voting. The Electronic voting is a meagre supplement to the current system of voting. i.e. Internet voting is step by step comparison of a traditional mode of voting via ballot paper. This leaves little room for innovation. Being just a supplement in the end, leaves the internet system to be helpless to innovate in a bigger sphere. The best case scenario under current circumstances would be to increase the vote share of Internet voters among overall voting.

There is a noted case, that the Internet Voting overall hasn't influenced the actual voting turnout which still remains low at around 60% on average in parliamentary elections (Vassil, Solvak, Vinkel, Trechsel, & Alvarez, 2016) . The greatest impact currently noted is among foreign voters i.e. Estonians who are living abroad and who wants to vote. At the same time, researchers have found that voters who have used internet voting in one election are likely to repeat the same way of voting in the elections (Vassil, Solvak, Vinkel, Trechsel, & Alvarez, 2016).

4.4.2. *Limited options to vote*

There are only limited options to vote from via electronic means. For examples, at the time of writing, there is no way of voting via smartphone which has also increased usability among citizens (Statistics Estonia, 2018). Currently, voting can only be carried out in designated operating systems via computers. It has been assumed that people who have access to smartphone also have the access to a computer system, which might be disputable.

4.4.3. Means of Vote

Currently, it is allowed to vote in several ways including advance voting, electronic voting, vote at home, and via ballot paper. In all cases except electronic voting, the electoral board provides means and infrastructure for voting. For example, in case of polling booth, the ballot paper, means of voting is provided clearly. In case of Internet Voting, it is up to the responsibility of the voter to have access to internet and the access to a computer with desired operating system. For voters who would like to vote electronically and would trust it more, but lack the means, it is not possible to vote like that. It is understandable that Internet Voting is optional but at the same time, any means should be universally accessible by everyone.

4.4.4. Impact on election system

As mentioned above that electronic/internet voting remains to be a supplement of the current voting election system. The issues of accountability and trust come with it. For example, no system currently facilitates actions of voters after elections. If a voter or group of voters are dissatisfied by the government which is formed or in the middle of tenure by its functioning, there is no means, but to wait for next elections for a change. The government and elected candidates should be responsible and accountable to their electors.

4.4.5. Accountability

The accountability issue is quite huge than it is maybe realised. Current system of parliamentary elections in Estonia facilitates and promotes election of coalitions to the government. It is rather impossible for a single political party to be able to rule independently and make decisions. Currently, the political parties are at the behest of each other, who they are against in the elections to form a government with. Although, no system is perfect, a directly majority system of elections, would let one political party to dominate their policies to the whole country. Any kind of government maybe into place, but none is directly accountable for their tasks and policies. They can surely assume the citizens and voter confidence, but there is currently no way of validating that in real time except third party surveys.

In any case, there should be possibility of direct communication between the selected few (candidates) and the selectors (citizens), to ensure that the policies made by the government are sound to the whole population, to be directly accountable for the actions.

5. Proposed State

Disclaimer: Such a proposed system at this stage is just conceptual, therefore, there might be technical and legal discrepancies.

The proposed state is a blockchain based voting eco-system which has the possibility to disrupt the election and voting as a whole. The proposed system of voting would consist of 2 components, namely Blockchain Based Continual (I) – Internet Voting System or in short 'Continual Voting' and accountability tool for the citizens and the government called as 'Confidence Assessment Meter'. This proposed system takes into account the digital infrastructure already present in the country of Estonia and the disruption done so far. Also, the continual use of e-governance and e-government services by Estonians would make this possible, as the confidence has rather increased in the use of E-Systems because of their accessibility and security.

5.1. Pre-requisites

(i)   The system takes into consideration of already present digital tools present in the Estonian E-government ecosystem, such as access of ID Card and Digital Signatures by the citizens of the country. Therefore, they will continue to play an important role in building and functioning of such a system.

(ii)   The system would require 100% support from the State Electoral Board for the implementation. In this case, the electronic method of voting has to be the only method of voting in the election. This could achieved by user access at personal level, and polling booth access to system and internet by the Electoral Board.

(iii)   The blockchain infrastructure would have to be created or modified via already present protocols. The best case scenario would include the use of permissioned blockchain and distributed ledger technology. It would ensure the security and transparency of the elections.

(iv)   Legal aspects would have to be discussed and presented carefully, before a law is passed regarding the same. Some aspects of the system are new, and not covered with existing election law.

(v)   Citizen and Civil Society participation in technical know-how and legal matters is necessary, before implementation of such a system at national level.

(vi)   The voting currently done to the candidates should shift towards voting for a political party. In case of independent candidates, the current law is sufficed.

5.2. Blockchain Based Continual (I)-Voting System

The proposed state of system would include the use of permissioned blockchain solution, such that although the organizing body is still centralized, but the verification of the same can be broadcasted and verified via several nodes. This system of voting would aim to make the elections and voting procedures real time and continual.

As depicted below in figure 5, it shows the conceptual overview of such a system.
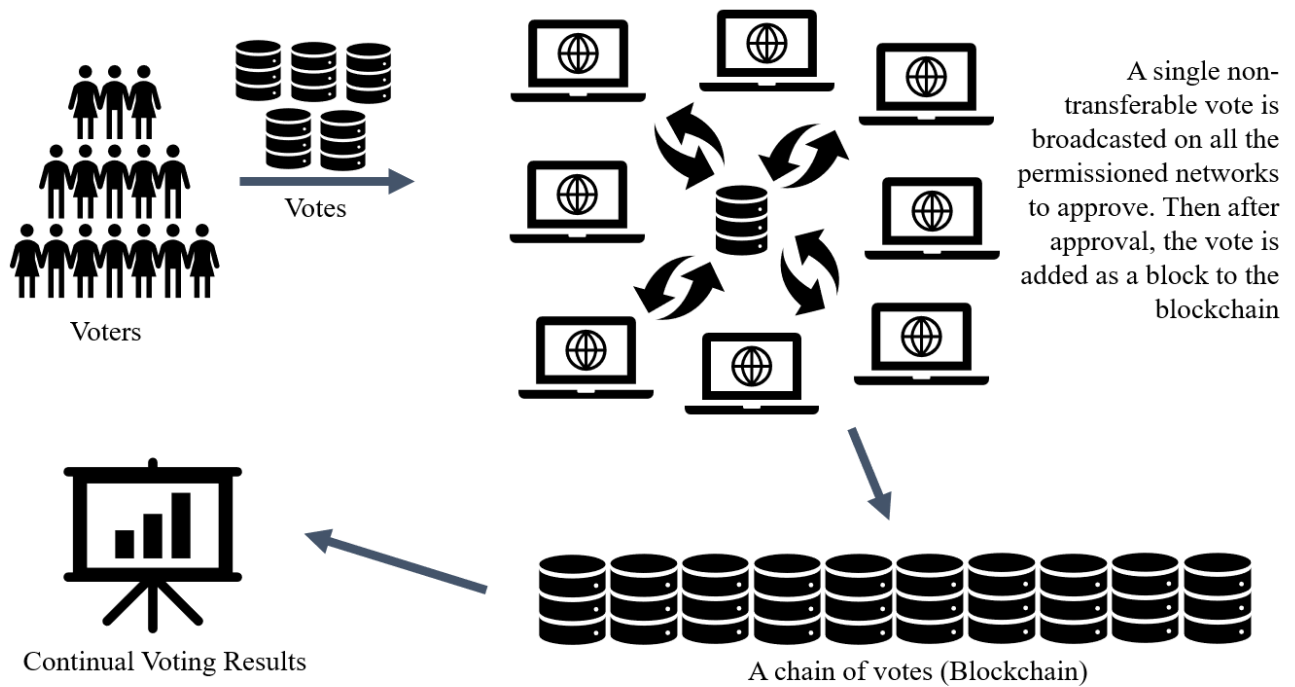
A single non-transferable vote is broadcasted on all the permissioned networks to approve. Then after approval, the vote is added as a block to the blockchain

Voters

Votes

Continual Voting Results

A chain of votes (Blockchain)

Figure 5 Conceptual overview of the system

The proposed state could be reached by using a modified system based up the paper published, 'Blockchain based E-Voting System', (Hjálmarsson, Hreiðarsson, Hamdaqa , & Hjálmtýsson, 2018), where the authors propose to use smart contracts in the e-voting system. In the paper, they proposed to use smart contracts for each electoral district node where a voter could vote from, and when a voter casts his/her vote, the contract executes to add that transaction to the blockchain after broadcasting it on other district nodes. The paper established to use Go-Ethereum system which is a permissioned Proof-of-Authority (PoA) blockchain. A proof of Authority is system where transactions are done relatively faster with the consensus based on identity.

Each voting district will present a district node with a smart contract. Each node would have a software agent that would interact with a bootnode and manage the life-cycle of smart contract. When elections are announced by the Electoral Authority they would distribute a ballot as smart contract for each district. When a voter would cast vote, the smart contract would trigger and the voting transaction would be verified by other nodes. After verification it would be appended to the blockchain. In this case, a boot node would be a network which has the permissioned access to the network. This would act as a service to help the district nodes (Hjálmarsson, Hreiðarsson, Hamdaqa , & Hjálmtýsson, 2018).

Voters would be able to authenticate in the same way with the help of ID card and digital signature. After each vote, the voter will have a transaction ID to correspond to which will act as a medium to confirm and verify the vote later if needed. The vote casted with the help of a smart contract will be added to the blockchain. Accordingly, to calculate the results, the number of votes would have to be counted district-wise and then country wise, to map out which political parties won the most votes.

A blockchain system compared with a traditional one will deliver something much more important. It would be possible to have a continual voting period. The current system follows the pattern of normal voting procedure where ballots are collected, counted and then destroyed. To over hall the system, things need to be automated, but at the same time securely. In this proposed system, the distribution ledger will keep the votes casted by the voters until the election phase is over, like regular elections.

But when a government is formed in the centre, politicians might change their behaviour and aims in order, just to build a collation and come to power. Whichever situation is concluded, voters would have the possibility to do something about it. Therefore, as with any other job, a 'Grace' or 'Probation Period' of 6 months is recommended after the formation of the government.

This probation period will refer to any initial period an employee faces when joining a new job. Governing a country is a significant job, and the responsibility must always lie with the employers, in this case the citizens, voters. Therefore, in this period, the citizens must have an option to re-vote if any voter would want to. If a voter would feel, the government created is not up to the standards, the voters would be allowed to vote again.

In this case, only the voters who have voted before, will have the chance to vote again. This elongated voting period is not a mandatory course to follow, so it would be up to an individual voter who would like to vote again. This would be an entirely optional phase. This period is added, because after overseeing the functioning of the country for 6 months, it would give an idea to the voters if the government elected is a worthy one.

This elongated period of re-thinking would only be possible via blockchain technology and distributed ledger, as it would automate several processes to count. Daily, there could be an electronic bulletin board collecting the data. With applying similar format with the current I-Voting system, the encrypting in envelope, and decrypting via private key, wouldn't allow to have such a continual real-time process.

After the 6 months, so called 'Probation Period', final results would be declared, and hence, if the current government still has the absolute majority, they would be allowed to rule the country until the next term. This system would enhance the accountability of a government to their citizens. The 6 month period would also give the chance to elected government to not disappoint their voters.

5.3.Confidence Assessment Meter

But even elongated 6 period 'probation time' would not help, if the voters still seems not to be satisfied by their current government. Also, there can be a case, where voters who didn't cast the vote for the first time, won't be able to case their vote in the probation period. For this reason, and perennial oversight of the government, there is a proposal for a Government 'Confidence Assessment Meter'. It is important to establish that, in case of functioning of a country, citizens are the most important stakeholders, and they should be able to opt-out of the government, if they are not satisfied.
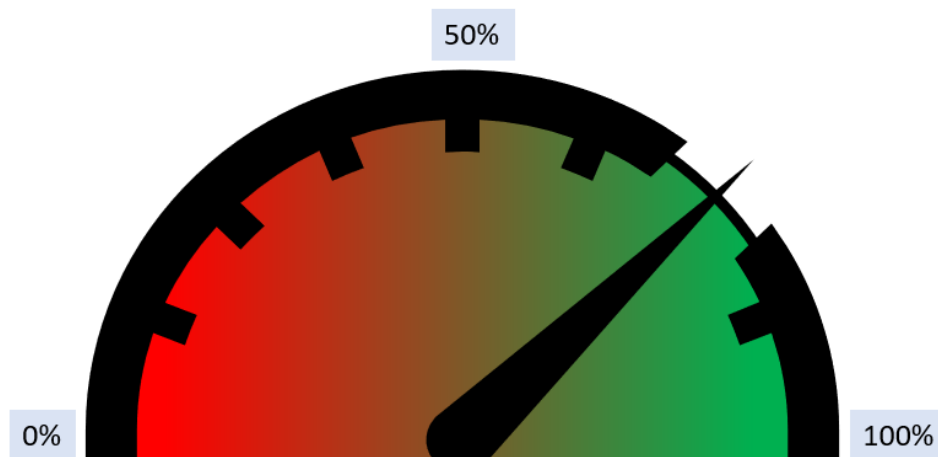

Figure 6 An artists' impression of the confidence meter. Source: Author

This meter would work in a way that, after 6 months, when the government is finalised from the interim government, there would be a virtual assessment meter calculated to 100%. This 100% would recognize all the voters in the voter database, and those who are eligible to voting, are added to this voter list. Then, via an application from the State Electoral Board, the voters would have a possibility to opt-out from their current government. This assessment meter would work real time for better results.

For example, total eligible voters, regardless who voted and didn't vote for the election was 800,000. The assessment meter is set to 100% from day 1 of functioning of the government. After 1 month, 100,000 voters decide to opt-out from the government because they might think, government is working in the wrong direction. Then, the total number would come down to 700,000, hence effectively the confidence meter would come down to 87.5%. Depending upon the popularity of the government, the confidence can increase or decrease, if people are back satisfied, number would increase, and if more are dissatisfied, the number will decrease.

In this way, it is much easier to track if the primary stakeholders of the country are happy with the working of the country. With such a system, there would be no need for referendums, because this will ensure continual democracy. If the elected leaders make a wrong decision, it would be outlooked in their confidence assessment meter.

This system would also make period terms and elections of government obsolete, as it will let the smart-citizens to choose when the government is not functioning properly. In an ideal system, if the binding confidence meter is in place, the government could stay in power as long as it is supported free and independently by the citizens of the country.

The question of making the confidence meter binding and non-binding, depends on the design. If all the eligible voters are allowed to opt-out or opt-in, then, the confidence meter should be non-binding to the government, as more people who didn't vote before can influence the working of the government. But still, it would keep as a healthy or unhealthy indicator, depending on the government and will make democracy more transparent.

The Confidence Assessment Meter could be made binding, which means, if the threshold comes down to less than 40%, the government is bound to resign, and new elections should be organized at the earliest. But this case could only be applied if only the voters who voted for the government will have their option to opt-out or opt-in. This would lead to much more direct democracy, but at the same time, might leave out the voters who couldn't vote before or the voters who have attained the age of voting only in the current term of the government.

This system could be implemented together with previous proposed system could be termed as a 'Blockchain Based Voting Ecosystem'.

5.4. Proposed State Summary

The current system which is a combination of ballot paper and electronic voting, is a one-time affair which is held periodically. As mentioned above, this gives less options for the citizens to exercise their rights as stakeholders of the government before the end of a term.

The formed government after an election, gets a straight pass until the next elections to do as they please. At the same time, the government might stall work for few years until the end of term, where there are accelerated change to affect voter behaviour for next elections. This makes a country in return, vulnerable for non-functioning or policies which are not good, or some good policies which are not implemented until the end.

In the proposed system of change where there would be just one Blockchain based voting ecosystem, not only it will make the process transparent but also make sure it possible to implement aspiring positive changes. The government elected firstly, would be subjected to a 6 month probation period, in which period, the voters will be able to change their vote, if they deem necessary. Then, the horse trading, resignations etc. which are done when forming a government, could be reduced. The possibility of changing the vote would bring more credibility to the choices made by the voters in the elections.

If voters are dissatisfied with the elected government, they would be able to exercise their right of changing it. It is a very normal process, whereto a new employee joins a position of work. In this case, the employee is the government for running the country.

After 6 months, the final results would come in, where if the current government settles down well with the voters, it would be able to stay. If not, there would always be a scope of changing of government. Then, there would be more bases of choices and coalition.

At the same time, the dissatisfaction and purported malice of a government can never be predicted. To keep this into check the confidence assessment system will kick into place. The voters will be able to give direct feedback in terms of support to their government, which could be tracked in real-time basis.

Voters will always have the option of opting out or opting in for the confidence towards their government and their respective policies.

6. Analysis

The analysis of the proposed system is carried out via analysis tools such as SWOT and PESTEL. In general, these tools are significant for analysis of an organization or a system. With author's perspective, proposed solution will work as a newly independent system, and hence, these tools would be useful to analyse its impact.

6.1. SWOT

SWOT is an analysis and strategic planning tool for a project or a system or an organization. It helps to identify important components such as, Strengths, Weaknesses, Opportunities, and Threats.

6.1.1. Strengths

- This ecosystem will allow the voters to act directly on their grievances in real time. This will give them a chance to think over the government elected, and would have a direct say in the functioning of the government.
- The system will allow the government to settle down in its initial months, to be aligned with the voters expectations. The government will make sure to reach their voters in case of important decision making or support.
- The government and the politicians will be directly accountable to their citizens. This system would give time to the leaders to re-evaluate their policy choices, which reflect the minds of the citizens.
- This will reduce the public menace, if any, caused by protests. As, every voter will have the power in their own hand to do something and change. If they don't like a policy, they can express their concern by opting out of the government.
- The political party(s) elected to be the government, would be less likely to pass their extreme unpopular agendas in the parliament or to make such laws. If highly unpopular, it could be seen in the confidence meter.
- Strong coalitions would be made, as after the 6 month probation period, the government is likely to be popular and permanent.
- The automated system via blockchain will help to make everything possible. It will decrease the cost of having such an exercise on a large scale. The backend technology will help to make the information confidential and secure.
- The number of election exercises could be decreased as if the government is popular and wanted among its citizens, there might not be a need to call re-election. Citizens would be happy with a functioning stable government.

6.1.2. Weaknesses

- Every system is susceptible to weaknesses. As with this, there could be a case, where voters are undecided after the voting. For example, there is a daily spike of votes from one side to another.

- The system although secure, has to be made more secure. Any try for breach or fraud has to be detected. As the system is electronic, there might be attacks from other non-friendly elements or countries.
- The government in this case has to make sure that the voters have unrestricted access to the voting applications all-round the year.
- The government also has to operate few centres of excellence where people can be made aware of this system, and functioning of the system, as this would be new to whole society. Digital literacy will be the responsibility of government. This is not a weakness but an opportunity too.
- Instability of the government is also an issue. If the government is taking right steps, but the voters are not ready for the changes, then the government would always find themselves in low confidence and could conclude in government changes much faster.
- Such a system would want regular up-keep and check for failures.

6.1.3. Opportunities

- The biggest opportunity with this system is to create a direct democracy scenario where the citizens of the country always have the power over their government.
- It is an opportunity to be a model for other countries, which have polarising views among the voters.
- The continual voting system and confidence meter would increase a government/political party to work positively for the working of the country, instead of working on their political agendas.
- This system will allow further opportunities in the phase of smart government, such as smart government policies, where the candidates/political party would participate in elections directly with policies which could be triggered automatically after forming the government.
- There is an opportunity to process the government working faster than usual. If the voters are not content with their selection or government, instead of protesting or waiting for changes to happen, they could remove their support from the government. This gives opportunity for concerned citizens to be more active towards their government.

6.1.4. Threats

- Threats from the cyber or digital point of view would remain an issue. As the whole system would work electronically, it is important to ensure the security to the digital infrastructure of the country
- There could be mass-hysteria fuelled polarisation and populism attempts by extreme individuals/parties. Even a small trigger might have the impact on the functioning of the government. In case of no-confidence in probation period or binding low confidence, the government would be obliged to fall. Therefore, as a society, it should be ensured that

information spread is free from any elements that can polarize a specific topic in a wrong way.

- There would be spawning of several civic societies with different agendas. This would make the society much more segmented and segregated. These groups would be a threat, as they could aggregate voters from their supporters.

- Technology sceptic population would dismiss of having such an idea, but then, the deployment of such a system would require special survey and support from all the citizens of the country. People who do not trust the government or elections are to be termed as sceptics. This system would ensure to bring up more transparency to tackle these kind of problems.

6.2. PESTEL

Another tool helpful to analyse is PESTEL, which is a tool for strategy and analysis of a system. Its components/factors are namely, Political, Economic, Social, Technological, Environmental, Legal. It is generally used for measuring an impact of business model, but in this case, a modified version of the same tool might be helpful measuring the impact of the new system.

6.2.1. Political

Political factor would be very crucial in order to implement such a system. There might be opposition from the elected individuals already, as this will limit their power to rule aimlessly and without any accountability. The major impact will be political. It will change the way political parties work, and the whole political ecosystem of the country.

The other political impact will be inside the political parties, as the votes will be casted to directly political parties rather than candidates. The internal working of the political parties would have to be closely monitored. The way they allocate the leaders, candidates and the policies they might take out could be monitored.

This political system would be one-of-a kind ever implemented in a democracy would have major impact on the politics of the country.

6.2.2. Economic

The economic impact forecasted is to be neutral in author's opinion. Since, building new system would require upfront costs and then maintenance costs included, it will oversee the savings made by it. At the same time, money would be saved by removing some manual tasks, but overall the automated task would require some resources.

The other economic impact would come from any faster than periodical elections, if conducted.

6.2.3. Social

By far the most impact would be socially, where society would be made aware of their rights of controlling their government directly. The attitude of the society would change towards their government. They would be able to feel part of the government elected. There would be greater participation of the civil society. The social impact would also be impacted by the real-time changes and transparency which this system would bring.

The importance of this impact is rather critical as the usage of such a system by the society would have direct impact with the day to day life. The social impact could be increase of voting turnout, after seeing changes to the government, election-sceptics might be motivated to opt for voting.

Society could be build together stronger with this. The common issues pertaining to the government could be identified quickly and thus the action points could be mapped out quickly as well.

6.2.4. Technological

With the application of the Blockchain Technology, is by far the factor for the technological impact. Blockchain based infrastructure would have to be created. Either by using already present protocols or by innovating own ideas for it. Technological factors would depend upon the type of blockchain system chosen, but there would be a major impact thereof.

One of the impacts is the adoption of the technology among the voters and society. The adoption and acceptance of blockchain based solutions to vote would have to be overcome by digital literacy programs.

As Elections are one of the most important pillars of democracy and the country itself, the utmost priority would be to have the technology at par level before implemented. The margin of error has to be at its minimum. The technological impact would also factor in the maintenance of such a system. There should always be qualified people to run these systems.

Also, in case of threats or fraud, a plan B system should always be in place. The technology impact would bring in more threats from external sources.

6.2.5. Environmental

Environmental factors affecting this system would be the use of resources to build and run such a system. The environmental aim of the proposed system would be to ensure carbon-neutral approach towards implementation and maintenance.

The use of blockchain and computers instead of paper, would reduce the paper and physical stationary requirement but it would require resources to process the big machines and servers doing the automated calculations. The environmental impact of implementing the proposed system would aim to be neutral to its predecessor.

6.2.6. *Legal*

Implementing systems like continual voting and confidence meter would require laws to pass in order for them to be relevant. Currently, there are no laws regarding these topics, as these not have been considered.

Laws have to be passed for use of such a system at country level, not just for the technology but also for the voters. As this proposed system would work if everyone could vote digitally and several times in a long span of time.

Other legal aspects would be to change the elections act, which is by no means would be easy. The government itself would have to pass a law making this kind of system relevant and legal.

Other legal issues may arise up if the non-binding confidence assessment hit its lowest levels. What steps would the government take to save itself, and the procedure of changing the government in case of no-confidence by the citizens.

7. Comparative Analysis

Blockchain based Voting ecosystem has potential to disrupt elections and the democracy infrastructure. The traditional way of voting and elections, as mentioned before. This section will compare and analyse the current Internet (I) – Voting Method referred from now as 'I-Voting' and proposed Blockchain based Continual Internet (I) – Voting Method referred from now as 'Continual I-Voting'. This aims to answer the RQ2 of, 'What additional values would Blockchain based Voting Ecosystem would deliver comparing to the existing one?'. This would be assessed based on standards adapted by Council of Europe E-Voting Standards (Council of Europe, 2017):

7.1. Legal

7.1.1. *Universal Suffrage*: According to the standard, this refers to the characteristic that the voting interface should be easy to understand and use by all voters. The e-voting system must be designed in a way that, citizens with disabilities and special needs are able to vote independently. The e-voting system should only be an optional or additional means if it is not universally accessible. Also, voters should be aware that e-voting system is legitimate means of voting in election or referendum (Council of Europe, 2017).

   (i) *I-Voting*: The current I-Voting system upholds this standard. According to the constitution of Estonia, Voting digitally is a legitimate form of voting in an election or a referendum. It is also an optional or additional means where there is always the possibility of voting via ballot paper in a voting booth.

   (ii) *Continual I-Voting*: The proposed Continual I-Voting system will uphold the standard with similar conditions as the traditional one. Voting digitally stays to be a legitimate form of voting in an election or a referendum. But since, continual voting would require means of voting by everyone, at any given point of time, it will not be an additional or optional form of voting. Instead, it would be universally accessible. The government shall make sure, that there are enough public institutions that will help to make this possible. So, the enhancement would be to universally accessible.

7.1.2. *Equal Suffrage*: According to this standard, all the voting information is to be broadcasted equally among various voting channels. Where both non-electronic and electronic voting methods are used, there must be a secure way of combining the voting and get the results. There should be an assured way of unique identification of voters, such that they are able to be distinguished from other voters. The e-voting system should be used by only the voters who have been authenticated with a right to vote (Council of Europe, 2017).

   (i) *I-Voting*: I-Voting upholds this standard as well. All the official voting information is broadcasted across all channels. Since, currently I-voting is just an additional or optional way of voting, the results are calculated securely and

reliably. Only after the I-Voting period is over, then the offline voting happens and then duplicate votes are counted only once. Estonian Citizen's ID number ensures that each voter has a distinguishable mark. With digital signature, the I-Voting system ensures that voters (users) can authenticate who have the right to vote.

(ii) *Continual I-Voting*: In the proposed system of Continual I-Voting, the characteristics would be similar as the I-Voting system. The ID Card and the Digital Signature will help to ensure only the citizens with right to vote are able to vote. Integrity of the voting process will be protected with the same. Since, proposed system will include just one electronic voting channel which would be distributed ledger based, there shall be secure and reliable way to add and aggregate all the vote simultaneously for calculating the result.

7.1.3. *Free Suffrage*: According to this standard, the system itself should be free of influencing voter's decision to vote and voter's intention should not be affected, directly or indirectly by the system. The system shall ensure that information broadcasted to the voter about ballot is true, and the voters are duly guided for the whole e-voting process leading to confirmation of vote. The voting system should also be responsible to tell to the voter if the vote casted was invalid. The voter should be able to verify that the vote is accurately counted in the ballot and is not altered with. The system shall ensure that only eligible votes have been included in the final result and the evidence should be verifiable independent from the e-voting system (Council of Europe, 2017).

(i) *I-Voting*: The current I-Voting system ensures free suffrage. The system is built in a way that, voters are presented with the ballot and voting options in a specific order that it does not influence their voting behaviour. By the system itself, the voter (user) is guided fully by the interface until the vote has been confirmed. The voter also has the possibility to re-verify his/her vote with use of a smart phone application, to track if the vote was given to the right candidate. The voting system can be verified too.

(ii) *Continual I-Voting*: The proposed system of voting shall ensure the free suffrage in the similar principles. The interface will guide the voters over the whole process of voting until the casted vote is confirmed. The voters (users) will be able to verify their vote by checking through the system, the hash protects the vote, but could be revealed to the voter in case the voter wants to recheck their choice of vote.

7.1.4. *Secret Suffrage*: According to this standard, the secrecy should be the utmost priority in case of e-voting. It also deals with the use of personal data, this standard vows to protect the personal data of the voters, for only when it is needed. This standards also states to protect and limit the use of personal data such that unauthorised parties are not able to intercept, modify or misuse the data to gain knowledge. This standard also maintains to prohibit giving data to third parties about voter proof of vote casted. The e-voting system should ensure to erase the previous options, if voter has casted vote multiple times. This standard wants to make sure that it is not possible to re-construct a link between an unsealed vote and a voter, at the counting stage. At all times, the voters identity should be anonymous (Council of Europe, 2017).

(i) *I-Voting*: The current system follows this system to the context. When the votes are casted by voters, they are sealed in an envelope with a public key. There is no vote which is not encrypted passes through. The envelope system ensures the privacy and secrecy. When in the phase of counting, the votes are separated from their envelopes and in this way, they cannot be traced back to the voter. The voter's identity cannot be linked, as even after separation, the votes are later shuffled and mixed in random order.

(ii) *Continual I-Voting*: The proposed system also values to uphold this standard, albeit, in another way. Since, with the use of distributed ledger, the votes casted will be encrypted and then only added to the chain. It would not be possible to link back to the identity of the voter, without decryption. In this proposed system, votes would be counted as timestamp, and the identity of the voter would be publicly hidden. The previous choices would be annulled, counting only the final vote.

7.2. **Procedural**

7.2.1. *Regulatory and organisational requirements*: According to this standard, the member states are required to introduce the form of electronic voting in a progressive and gradual way. Before the introduction of electronic voting, the states should bring in required and important changes to the law and legislation. The legislation should be able to convey that the national electoral authority has control over the system. The legislation should establish the responsibility of the working of electronic voting system. The counting process must be managed by the central electoral authority, and any observer should be able to make observations over the counting of votes (Council of Europe, 2017).

(i) *I-Voting*: The current system provides the regulatory framework for running the electronic voting. The Riigikogu Act establishes the use and functioning of the electronic voting system. Currently, in Estonia, the spread of electronic voting is gradual, as it has always been the optional or additional way of

voting. The current also establishes the roles of the primary owners of the processes such as State Electoral Board. The observation of counting of votes can also be observed by anyone with required permission (RiigiTeataja, 2019).

(ii) *Continual I-Voting*: In the proposed system, there would be a need to pass a relevant legislation as the current legislation would not cover all the aspects of the system. The deployment of continual I-voting could be done in a progressive manner by firstly doing testing in comparison to the current system. Overall, the continual I Voting system deems to replace the voting method for all, therefore, the progressive way to do it would be testing rigorously and at the same time training the voters and citizens to prepare for the same. Since, the blockchain ledger counting is automated, any would be able to observe the counting of votes without any problems.

7.2.2. *Transparency and observation*: According to this standard, transparency should be maintained at every step of electronic voting. The voters should be well informed in advance about the steps of participation, the correct use of the electronic voting system and its functioning. The voters should be well informed about the time phase and stages of elections and electronic voting. The components must be disclosed for certification and verification publicly. Observers should be able to observe and comment upon the electronic voting process, for the whole process from start to the end results. The standards build for the electronic system should be open and could be derived from several sources (Council of Europe, 2017).

(i) *I-Voting*: The current system applies the principle of transparency and digital literacy. The voters are well-informed from the government resources about the use, time phase and process of voting via internet voting. The voters are guided by text, informational videos. The components are disclosed publicly in Estonian as well English language, for any and all international observers. International observers are also given access with permission, to review the electronic voting process from start to end. The standards used for building electronic voting system are publicly available. Any country/individual can have the access to it.

(ii) *Continual I-Voting*: The blockchain based system would also follow this standard. The distributed ledger and counting would be transparent to everyone. The voters would be well-informed about the changes incoming to the current system and the procedure, time phase to vote would disclosed well in advance to the voters. All observers will be able to observe the electoral process as it would be transparent. Standards would be made transparent, so better auditability.

7.2.3. *Accountability*: According to this standard, the certification, technical and evaluation requirements should be formed in such a way that they would follow the democratic and legal principles. It is the responsibility of the government to keep the requirements up to date. Also, there is a scope of international independent evaluation of the system at appropriate intervals, such as some significant changes made to the system. This would be concluded in a certification or something similar. The electronic voting system must be auditable, the system should be open to investigations in regards to any weaknesses and threats (Council of Europe, 2017).

   (i)   *I-Voting*: The current system maintains accountability to its stakeholders. There are regular evaluations of the current system to evaluate any potential threats and weaknesses. Only after proper requirements and testing, new functionalities to the system are introduced. The current system is accountable to any independent body, and then it works for the threats, if identified any.

   (ii)   *Continual I-Voting*: The proposed system, would be open to evaluation as it aims to be a transparent system. It would uphold the relevant legislation and democratic principles. This process would make the whole election system more democratic than every before, as the voters will have option to make their choices again, after seeing the working of the government.

7.2.4. *Reliability and security of the system*: According to this standard, the electoral body conducting the electronic voting must be responsible for compliance with all the requirements in case of emergencies, attacks or failures. The electoral body is responsible for the security, reliability, usability and availability of the electronic voting system. Only authorised individuals must have access to the critical central infrastructure, servers and data. Before the actual voting, the electoral body has to ensure via testing that the system is working properly and correctly. Votes should be encrypted in case, they are stored externally. Voter and voting information must be kept securely before counting. There should be a procedure for regulating the installing, updating or corrections in any software. The electoral body is also responsible for handling the cryptography material with utmost care. In case of any incidents with voters who are affected by irregularity, the electoral body should ensure the cases are resolved. If there is an observance of a threat or failure, the operators of the system must inform the electoral authority at the earliest. The voters list, candidate list should be authenticated, and their integrity should be maintained. The data protection laws should be followed accordingly (Council of Europe, 2017).

   (i)   *I-Voting*: The current system follows this standard. The electoral body is responsible for the whole process of electronic voting. The electoral body has the power to pause or annul the electronic voting in case of detection of any threat or emergencies. Only authorised individuals, in this case, Tallier has the access to the private keys to the votes. Other critical infrastructure is also well

protected. Procedure of installing an update or new software is the responsibility of the electoral board. The keys are taken care of in a careful manner. The authority also checks if there are any discrepancies found or if some voters are facing a problem while using the electronic voting system.

(ii)   *Continual I-Voting*: In the proposed system, the security of the system will be protected by the blockchain protocol, which is one the safest algorithms available. The electoral authority will ensure to give permission of decryption to selected few. The list of candidates and voters would be taken care of, following the data protection rules. The reliability of the system is maintained, as several ledgers are maintained simultaneously, even a small change in one, will be helpful to detect a malice behaviour.

8. Conclusions

With the introduction of a blockchain based voting ecosystem, it would have the potential to change the functioning of the democracy, making it more transparent and accountable. While drawing comparisons from the current e-system to the proposed blockchain based e-system, there are definite ups and downs. While in terms of transparency and security, the new system would have a greater advantage but at the same time, in terms of legislation and procedural requirements, the current system has the advantage. In case of universal, equal, free and secret suffrage, both of the systems have similar approaches and will make sure to uphold those standards.

This thesis prefers the blockchain based system to overtake the current system of voting, as the current e-voting system is an exact replica of the offline ballot and polling booth procedure. Thus it would not support for the ideas of continual voting and ideas thereof.

The new eco-system would bring out revolutionary aspects of democracy to general public. The society and in turn, voters will be able to make their government more accountable and answerable with this approach. The confidence meter will give them a factual approach towards the government policies. If there is a massive backlash over the government, the voters will be able to opt out and decrease in the confidence. Depending upon the decision being binding or non-binding, actions could be taken faster with no public distress and damage.

This thesis aimed to give a theoretical overview and impact of adopting a new system of governance. With this thesis, the aim is to change democracy to be more direct and interactive with the citizens.

9. Recommendations

General Recommendation is to take such type of governance into account, where the accountability is transparent and more direct. The factual nature of confidence assessment could also be applicable without the use of proposed system. Confidence Assessment meter could be already applied in general life, which existing infrastructure. This would already be a new step towards direct democracy and a pillar for e-governance.

9.1. Further Research

Based on this thesis, a technical framework for the blockchain which would make it possible could be formulated. Deploying such a project might be a shock to the voters who are not used to exercise power regularly. Further areas of research regarding the same topic would be go deeper into the social aspect of deploying such a project. If successful, this approach could also lead to a level step up to policy-based elections where voters could be voting for policies rather than politicians.

9.2. Related work

- Almeida R.L., Ricci L., Camarinha-Matos L.M. (2019) voteChain: Community Based Scalable Internet Voting Framework. In: Camarinha-Matos L., Almeida R., Oliveira J. (eds) Technological Innovation for Industry and Service Systems. DoCEIS 2019. IFIP Advances in Information and Communication Technology, vol 553. Springer, Cham
- Al-Rawy M., Elci A. (2019) A Design for Blockchain-Based Digital Voting System. In: Antipova T., Rocha A. (eds) Digital Science. DSIC18 2018. Advances in Intelligent Systems and Computing, vol 850. Springer, Cham

10.   References

Agora. (2018). *White Paper 2.0 Bringing our voting systems into 21st Century.* https://agora.vote/.

Akbari, E., Wu, Q., Zhao, W., R. Arabnia, H., & Qu Yang, M. (2017). From Blockchain to Internet-Based Voting. *2017 International Conference on Computational Science and Computational Intelligence.* IEEE.

Ayed, A. B. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. *International Jounal of Network Security and its applications (IJNSA) Vol.9, No.3.*

Ballotpedia. (2018). *Voting methods and equipment by state*. Retrieved from Ballotpedia: https://ballotpedia.org/Voting_methods_and_equipment_by_state

BBC.   (2019,   August).   *Brexit*.   Retrieved   from https://www.bbc.com/news/politics/uk_leaves_the_eu

Cambridge   Dictionary.   (2019).   Retrieved   from https://dictionary.cambridge.org/dictionary/english/

Council of Europe. (2017). Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting. *1289th meeting of the Ministers' Deputies.*

Economist. (2015, January 20). *Democracy on the edge: Populism and Protest.* Retrieved from The Economist Intelligence Unit: https://ifuturo.org/documentacion/Democracy-on-the-edge.pdf

Election Commision of India. (2018). *Home page*. Retrieved from Election Commision of India: https://eci.gov.in/

Encyclopaedia   Britannica.   (2019).   *Electoral   System*.   Retrieved   from https://www.britannica.com/topic/electoral-system

Enterprise Estonia. (2018). *e-Governance - i-Voting*. Retrieved from e-Estonia: https://e-estonia.com/solutions/e-governance/i-voting/

ERR. (2018, October 9). *How does the electoral system in Estonia work?* Retrieved from Eesti Rahvusringhääling: https://news.err.ee/867523/how-does-the-electoral-system-in-estonia-work

ERR, N. (2019, 03 23). Retrieved from ERR News: https://news.err.ee/922982/koigi-eesti-movement-launched-by-concerned-residents

Harris, C. G. (2018). The Risks and Dangers of Relying on Blockchain technology in Underdeveloped Countries. *IEEE/IFIP Network Operations and Management Symposium.* Taipei: IEEE.

Heiberg, S., Kubjas, I., Siim, J., & Willemson, J. (2018). On Trade-offs of Applying Block Chains for Electronic Voting Bullentin Boards. *E-Vote-ID.*

Hjálmarsson, F., Hreiðarsson, G., Hamdaqa , M., & Hjálmtýsson, G. (2018). Blockchain-Based E-Voting System. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*.

Hsiao, J.-H., Tso, R., Chen, C.-M., & Wu, M.-E. (2017). Decentralized E-Voting Systems Based on the Blockchain Technology. *Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering, vol 474.* Springer, Singapore.

Kelly, M. (2018, November 10). *Nearly 150 West Virginians voted with a mobile blockchain app*. Retrieved from The Verge: https://www.theverge.com/2018/11/10/18080518/blockchain-voting-mobile-app-west-virginia-voatz

Laukkonen, J. (2018, September 25). *Which Countries Use Electronic Voting?* Retrieved from Lifewire: https://www.lifewire.com/which-countries-use-electronic-voting-4174877

Moura, T., & Gomes, A. (2017). Blockchain Voting and its effects on Election Transparency and Voter Confidence. *dg.o '17.* Staten Island, New York: Authors.

Mudliar, K., Parekh, H., & Bhavathankar, D. (2018). A Comprehensive Integration of National Identity with Blockchain Technology. *International Conference on Communication, Information and Computing Technology (ICCICT).* Mumbai.

Mu-Hyun, C. (2017, November 28). *South Korea to develop blockchain voting system*. Retrieved from ZDnet: https://www.zdnet.com/article/south-korea-to-develop-blockchain-voting-system/#ftag=RSSbaffb68

Nakamoto, S. (2009, March). *Bitcoin Resources*. Retrieved from Bitcoin: https://bitcoin.org/bitcoin.pdf

Pawlak, M., Poniszewska-Maranda, A., & Kryvinska, N. (2018). Towards the intelligent agents for blockchain e-voting system. *The 9th International COnference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018).* Elsevier.

Polys. (2018). *Whitepaper.* https://polys.me/.

Puiggali, J., Choliz, J., & Guasch, S. (2010). Best Practices in Internet Voting. *Workshop on UOCAVA Remote Voting Systems.* Washington DC.

Renming, Q., Chen, F., Zheng, L., & Mrad, N. (2017). Blockchain-Powered Internet of Things, E-Governance and E-Democracy. In T. V. Kumar, *E-Democracy for Smart CIties.* Singapore: Springer Nature.

Rennock, M., Cohn, A., & Butcher, J. (2018, February/March). Blockchain Technology and Regulatory Regulations. Thomas Reuters.

RiigiTeataja. (2019). *Riigikogu Election Act*. Retrieved from Riigikogu Election Act: https://www.riigiteataja.ee/en/eli/ee/501092014005/consolide/current

Schneider, A., Meter, C., & Hagemeister, P. (2017). *Survey on remote electronic voting*. Retrieved from https://arhiv.org/abs/1702.02798

Srivastava, G., Dwivedi, D. A., & Singh, R. (2018). Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. *15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT*. Porto.

State Electoral Office of Estonia. (2017). *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia.* Tallinn: State Electoral Office of Estonia.

Statistics Estonia. (2018, June 29). *Eesti Statistika Kvartalikiri. 2/18. Quarterly Bulletin of Statistics Estonia (e-publication).* Retrieved from https://www.stat.ee/publication-2018_quarterly-bulletin-of-statistics-estonia-2-18

Sun, X., Wang, Q., Kulicki, P., & Sopek, M. (2019). A simple Voting Protocol on Quantam Blockcahin. *International Journal of Theoretical Physics*, 275-281.

Swan, M. (2015). *Blockchain: Blueprint for new economy.* O'Reilly.

Valimised. (2019). *Statistics about Internet voting in Estonia*. Retrieved from https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly*, 453-459.

Voatz. (2019). *Under the hood- The West Virginia Mobile Voting Pilot.* Voatz, Inc.

Voshmgir, S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy.* BlockchainHub Berlin.

Votem. (2017). *White Paper.* Votem.io.

Willemson, J. (2017). Bits or paper: Which should get to carry your vote? *Journal of Information Security and Applications*, 124-131.

Xorbin. (2019). *SHA-256 hash calculator*. Retrieved from Xorbin: https://www.xorbin.com/tools/sha256-hash-calculator

Yavuz, E., Kaan Koc, A., Can Cabuk, U., & Dalkılıç, G. (2018). Towards secure e-voting using ethereum blockchain. *6th International Symposium on Digital Forensic and Security (ISDFS).* Antalaya: IEEE.

Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Ho Au, M. (2018). Platform-Independent Secure Blockchain-Based Voting System. *ICS 2018: Information Security* (pp. 369-386). Springer.

Zhen-Yu, W., Ju-Chuan, W., Lin, S.-C., & Wang, C. (2014). An electronic voting mechanism for fighting bribery and coercion. *Journal of Network and Computer Applications*, 139-150.

Appendix A: License