PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO – PUCSP
PROGRAMA DE ESTUDOS PÓS-GRADUADOS EM TECNOLOGIAS DA INTELIGÊNCIA E DESIGN DIGITAL

RODRIGO CARDOSO SILVA

PROPOSTA DE APLICAÇÃO PARA VERIFICAÇÃO DO VOTO COM TECNOLOGIA BLOCKCHAIN: A ABORDAGEM DE UM MODELO E2E VERIFIABILITY PARA INTERNET VOTING DA ESTÔNIA

DOUTORADO EM TECNOLOGIAS DA INTELIGÊNCIA E DESIGN DIGITAL

SÃO PAULO
2020

RODRIGO CARDOSO SILVA

PROPOSTA DE APLICAÇÃO PARA VERIFICAÇÃO DO VOTO COM TECNOLOGIA BLOCKCHAIN: A ABORDAGEM DE UM MODELO E2E VERIFIABILITY PARA INTERNET VOTING DA ESTÔNIA

Tese apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de Doutor em Tecnologias da Inteligência e Design Digital - área de concentração em Processos Cognitivos e Ambientes Digitais, sob a orientação do Prof. Dr. Demi Getschko.

SÃO PAULO
2020

BANCA EXAMINADORA

Prof. Dr. Jorge Stolfi (UNICAMP)

Prof. Dr. Klaus Steding-Jessen (CERT.br)

Profa. Dra. Cristine Hoepers (CERT.br)

Profa. Dra. Edith Ranzini (PUC-SP)

Prof. Dr. Daniel Couto Gatti (PUC-SP)

Autorizo exclusivamente para fins acadêmicos e científicos, a reprodução total ou parcial desta Tese por processos de fotocopiadoras ou eletrônicos.

Assinatura: _____

Data: _____/_____/_____

E-mail:_____

FICHA CATALOGRAFICA

Sistema para Geração Automática de Ficha Catalográfica para Teses e Dissertações com dados fornecidos pelo autor

SILVA, RODRIGO CARDOSO
PROPOSTA DE APLICAÇÃO PARA VERIFICAÇÃO DO VOTO COM TECNOLOGIA BLOCKCHAIN: A ABORDAGEM DE UM MODELO E2E VERIFIABILITY PARA INTERNET VOTING DA ESTÔNIA / RODRIGO CARDOSO SILVA. -- São Paulo: [s.n.], 2020.
156p. il. ; cm.

Orientador: DEMI GETSCHKO.
Tese (Doutorado em Tecnologias da Inteligênciae Design Digital)-- Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós-Graduados em Tecnologias da Inteligênciae Design Digital, 2020.

1. Verificação de Ponta a Ponta. 2. Sistema de Votação pela Internet. 3. Tecnologia Blockchain. 4. Algoritmo Monero. I. GETSCHKO, DEMI. II. Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós-Graduados em Tecnologias da Inteligênciae Design Digital. III. Título.

CDD

Dedico esta pesquisa à minha filha Sarah Donda Silva.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior- Brasil (CAPES) - Códigos de Financiamentos 88887.150078/2017-00 (PROSUP) e 88881.189182/2018-01 (PDSE).

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior- Brasil (CAPES) - Finance Codes 88887.150078/2017-00 (PROSUP) and 88881.189182/2018-01 (PDSE).

O presente trabalho foi realizado com apoio do Fundo de Desenvolvimento Regional Europeu – Programa de Doutorado Visitante (*DORA Plus*).

This study was financed in part by the European Regional Development Fund - Visiting DoRa Doctoral Fellowship (DORA Plus).

AGRADECIMENTOS

Quero expressar a minha gratidão ao Prof. Dr. Demi Getschko, porque desde a primeira reunião de orientação no NIC.br, ele acredita no potencial da pesquisa e na minha capacidade de resolver os desafios que a investigação acadêmica impôs durante toda a jornada científica. Com a mentoria e orientação do notório professor, a pesquisa alcançou respostas inéditas para a comunidade acadêmica e científica, ambas relacionadas à sistemas de votações digitais.

Aos professores da banca de qualificação e examinação, é uma honra tê-los na minha defesa de doutorado. A contribuição dos doutos professores é o momento enriquecedor para a posteridade do trabalho científico.

Ao Cardeal Dom Odilo Pedro Scherer, Arcebispo Metropolitano de São Paulo, e Presidente da Fundação São Paulo - mantenedora da Pontifícia Universidade Católica de São Paulo (PUC-SP).

À Profa. Dra. Maria Amália Pie Abib Andery, Reitora da Pontifícia Universidade Católica de São Paulo (PUC-SP).

Ao Prof. Dr. Márcio Alves da Fonseca, Pró-Reitor de Pós-Graduação (PUC-SP).

Ao Prof. Dr. Daniel Couto Gatti, Diretor do Campus Consolação - Marquês de Paranaguá (PUC-SP).

À Profa. Dra. Maria Lucia Santaella Braga, Coordenadora e o Prof. Dr. Hermes Renato Hildebrand, Vice-Coordenador, ambos gestores acadêmicos do programa de Pós-Graduação em Tecnologias da Inteligência e Design Digital (TIDD), agradeço o apoio e a confiança depositada para eu representar o programa TIDD no país e exterior.

À Edna Conti que, com dedicação e paciência, buscou me ajudar desde o meu primeiro dia como doutorando com as atividades acadêmicas (bolsista) e o cumprimento das regras administrativas do programa TIDD.

À Vera Braz que, além de colega do programa TIDD, ajudou-me bastante com as agendas e tarefas para serem entregues ao Prof. Dr. Demi Getschko.

Aos professores e colegas (alunos) do programa TIDD da PUC-SP.

Ao Prof. Dr. Dr. Robert Krimmer *at Tallinn University of Technology (TALTECH) in Technology Governance – Public Administration, Post Graduate Program of the Ragnar Nurkse Department of Innovation and Governance*, que acreditou na minha capacidade de aprender sobre tecnologias novas de votação e a confiança depositada para eu conhecer pessoas importantes do poder público e privado que estão relacionadas com a transformação digital na administração pública e o sistema de votação pela Internet na Estônia.

Ao Prof. Dr. Erkki Karo, Diretor do departamento *Ragnar Nurkse* na *TALTECH*.

Aos professores, doutorandos e colaboradores do departamento *Ragnar Nurkse* na *TALTECH*, agradeço pela acolhida amigável, cordial e respeitosa que auxiliaram bastante durante os dez meses de convivência na cidade de *Tallin*, Estônia.

Aos meus pais, Sr. Benedito Silva e Sra. Valéria Carvalho, que sempre me apoiam nos meus projetos pessoais e profissionais.

À minha esposa Eliza Donda.

RESUMO

O processo de votação pela Internet ou *Internet voting (i-voting)* é um fenômeno emergente no cenário político internacional. A República da Estônia é o paradigma com maior tempo de experiência dentre os países que já utilizaram o voto pela Internet. Durante a investigação, a experiência estoniana prova que o sistema de *i-voting* é a evolução do processo democrático no campo político, social, jurídico e tecnológico. Todavia, o sistema de votação pela Internet é suscetível à fraudes e vulnerabilidades, fatos que prejudicam a confiança no sistema. A aplicação para verificação de ponta a ponta ou *end-to-end verifiability (E2E)* é apenas do tipo individual no sistema de *i-voting,* resultando na transparência parcial do processo de votação para o eleitor. Neste sentido, a hipótese encontrada pelo trabalho é a recomendação de utilização da tecnologia *public permissioned blockchain* – adaptada e customizada pelo algoritmo *Monero*, para aperfeiçoar a verificabilidade individual e universal atendendo os princípios disciplinados pela *OSCE/ODIHR*, como o anonimato, a integridade e a transparência no pleito eleitoral pela Internet. É importante enfatizar que a abordagem da pesquisa não está diretamente relacionada com os aspectos de segurança da informação das eleições pela Internet na Estônia, pois a pesquisa entende que a aplicação de normas e boas práticas de segurança são um conjunto de fatores que envolvem pessoas, processos e tecnologias. A finalidade da investigação acadêmica é potencializar a confiança no sistema de votação pela Internet com uso da tecnologia *blockchain* dentro de um modelo novo de verificação de ponta a ponta da cédula eletrônica que pode ser auditada pelo eleitor, partidos políticos e membros responsáveis pelo processo eleitoral estoniano.

Palavras-chave: Verificação de ponta a ponta; Sistema de votação pela Internet; Tecnologia blockchain; Algoritmo Monero; República da Estônia.

ABSTRACT

The process of Internet voting (i-voting) is an emerging phenomenon in the international political scenario. The Republic of Estonia is a paradigm with the most extensive experience among the countries that have used i-voting. During the investigation, the Estonian experience proves that the i-voting system is the evolution of the democratic process in political, social, legal, and technological fields. However, the Internet voting system is susceptible to fraud and vulnerabilities, facts that undermine the system's confidence. The application for end-to-end verifiability (E2E) is only of the individual type in the i-voting system, resulting in partial transparency of the voting process for the voter. n this sense, the hypothesis found by the work is the recommendation to use public *permissioned* blockchain technology - adapted and customized by the Monero algorithm, to improve individual and universal verifiability in compliance with the principles disciplined by OSCE/ODIHR, such as anonymity, integrity and transparency in an election by the Internet. The research approach is not directly related to the information security aspects of Internet elections in Estonia, as the research understands that security is a set of factors that involve people, processes, and technologies. The purpose of academic research is to enhance confidence in the i-voting system with the use of blockchain technology for the new model of end-to-end verifiability electronic ballot (e-ballot) by voters, political parties, and members responsible for the Estonian electoral process.

Keywords: End-to-End verifiability (E2E); Internet Voting System; Blockchain technology; Monero Algorithm; Republic of Estonia.

RESUMÉ

Le processus de vote par Internet est un phénomène émergent dans le scénario politique international. La République d'Estonie est un paradigme avec l'expérience la plus étendue parmi les pays qui ont utilisé le vote électronique. Au cours de l'enquête, l'expérience estonienne prouve que le système de vote électronique est l'évolution du processus démocratique dans les domaines politique, social, juridique et technologique. Cependant, le système de vote par Internet est vulnérable à la fraude et aux vulnérabilités, des faits qui sapent la confiance du système. La demande de vérifiabilité de bout en bout n'est que de type individuel dans le système de vote électronique, ce qui entraîne une transparence partielle du processus de vote pour l'électeur. Dans ce sens, l'hypothèse trouvée par l'ouvrage est la recommandation d'utiliser la technologie blockchain autorisée par le public - adaptée et personnalisée par l'algorithme Monero, améliorer la vérifiabilité individuelle et universelle conformément aux principes disciplinés par l'OSCE/ODIHR, tels que l'anonymat, l'intégrité et la transparence dans un élection par Internet. L'approche de la recherche n'est pas directement liée aux aspects de sécurité de l'information des élections par Internet en Estonie, car la recherche comprend que la sécurité est un ensemble de facteurs qui impliquent les personnes, les processus et les technologies. L'objectif de la recherche universitaire est de renforcer la confiance dans le système de vote électronique grâce à l'utilisation de la technologie de la chaîne de blocs pour le nouveau modèle de bulletin électronique de vérification de bout en bout (bulletin électronique) par les électeurs, les partis politiques et les membres. responsable du processus électoral estonien.

Mots-clés: Vérifiabilité de bout en bout; Système de vote par Internet; Technologie blockchain; Algorithme Monero; République d'Estonie.

LISTA DE FIGURAS

TABELAS

LISTA DE ACRÔNIMOS

BDTD - Biblioteca Digital de Teses e Dissertações

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CIO – *Chief Information Oficer*

CoDe - *Cost of Democratic Elections*

EVC - *Electronic Voting Committee*

ECC - *Electronic Couting Committee*

EUA – Estados Unidos da América

RIA - *Information System Authority* ou *Riigi Infosüsteemi Amet*

BPMN - Business Process Model and Notation

NEC - *National Election Committee*

NIIS - *Nordic Institute for Interoperability Solutions*

NATO - *North Atlantic Treaty Organization*

OTAN - Organização do Tratado do Atlântico Norte

OEA – Organização dos Estados Americanos

OATD - *Open Access Theses and Dissertations*

OEA – Organização dos Estados Americanos

OECD - *Organisation for Economic Co-operation and Development*

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

OSCE - *Organization for Security and Co-operation in Europe*

ODIHR - *Office for Democratic Institutions and Human Rights*

PUC-SP – Pontifícia Universidade Católica de São Paulo

RMCS - *Rural Municipality ou City Secretaries*

SEO - *State Electoral Office*

TALTECH – *Tallin University of Technology*

UE - União Europeia

SUMÁRIO

1. INTRODUÇÃO

"O trabalho científico não deve ser considerado do ponto de vista de sua utilidade direta. Deve ser feito por si, pela beleza da ciência, e depois há sempre a chance de que uma descoberta científica poder tornar-se como o rádio, um benefício para a humanidade"
Marie Curie

O novo milênio da era digital é uma realidade híbrida no ambiente imersivo e interativo da Internet, onde se promovem habilidades cognitivas emergentes de forma tangível, ubíqua e pervasiva.

Neste sentido, a busca por inovações[1] na área da tecnologia da informação e comunicação se tornaram um dos principais negócios desafiadores dos setores privado e público.

A indústria dos bens e consumos do setor empresarial está inter-relacionada com a automação, controle e a troca de informações em sistemas digitais no meio ambiente da Internet, e estão consubstanciadas em diversas tecnologias computacionais, como por exemplo, sistemas de informação, plataformas sociais e de comunicação digital, criptografia computacional, computação em nuvem, Internet das coisas, *blockchain* e etc., tornando-as protagonistas da transformação digital no processo de inovação tecnológica[2].

De outro lado, o perfil governamental não é impulsionado pela disputa de mercado. Na maioria dos casos, o governo depende de propostas acadêmicas, projetos científicos privados, indicadores nacionais[3] e internacionais[4] e, principalmente, bastante vontade política para que a inovação digital no governo seja cada vez mais aconselhável e explorada para atender a necessidade da sociedade e viabilizar o desenvolvimento dos serviços públicos pela Internet.

Para a pesquisa o comportamente de ambos os setores não é diferente no tocante às tecnologias novas em processos de votação. Por exemplo, após o surgimento da votação eletrônica ou *electronic voting* (*e-voting)* em 1836, a ideia de votação pela Internet ou *Internet*

---

[1] Teoria da Difusão de Inovações por Everett Roger (1962).

[2] A tecnologia hoje ter maior poder computacional do que em meados de 1965. Gordon Earl Moore, co-fundador da empresa *Intel Corporation*, estipulou que a tecnologia de *transistors* para computadores da época evoluiriam sob o mesmo custo. As inovações para dispositivos computacionais têm demonstrado que a teoria é válida.

[3] TIC Governo Eletrônico - Cetic.br.

[4] *UN E-Government Survey*.

voting (i-voting) ganha *status* no ano de 1978 com o projeto *Televote*[5], tornando-se o primeiro sistema de *e-voting* híbrido com conexão remota de dados. Consequentemente, no ano de 1982 a terminologia *i-voting* é potencializada com adoção de técnicas de criptografia computacional para manter o sigilo do voto[6] (KRIMMER, 2012, pp.18-23).

Anos mais tarde, o advento da Internet na década de noventa estimula a votação pela Internet para se tornar um fenômeno natural e emergente para a sociedade global. Em 1999, segundo Hall e Alvarez (2004, pp. 4-5), o ex-presidente Bill Clinton escreve em memorando para a *National Science Foundation* aplicar pesquisas científicas com sistemas de *i-voting* para as eleições nos Estados Unidos da América (EUA), porém estudiosos no assunto afirmam que um processo de eleição pela Internet é bastante arriscado. No ano 2000, as eleições são marcadas pelas vulnerabilidades encontradas no modelo de *e-voting Votomatic.*

De acordo com o mapa de tecnologias para sistemas de votação da *Competence Center for Electronic Voting - E-Voting.CC*, os anos entre 2009, 2011 e 2015 mostram os países que adotam ou projetam um modelo de votação eletrônica ou votação pela Internet para eleições locais ou nacionais. Não obstante, o mapa também exibe as nações que renunciaram algum modelo tecnológico de votação adotado em determinado tempo e governos que não discutem qualquer forma de implementação no futuro.

Em face dos avanços tecnológicos que perduram anos de tradições em eleições – desde Atenas 507 a.C., a pesquisa entende que os sistemas de *e-voting* e *i-voting* são parte do processo de transformação digital dos governos que, em tempo, podem encontrar um modelo híbrido para tornar o processo democrático mais transparente para sociedade civil e, ao mesmo tempo, coibir comportamentos maliciosos nas eleições.

1.1 A PESQUISA

1.1.1 Motivação

A motivação da pesquisa é entender a votação pela Internet como tecnologia emergente e incipiente no processo político de votação e impulsionar a pesquisa científica em torno do tema para buscar uma perspectiva duradoura.

---

[5] *Researchers Ted Becker and Christa Slaton conducted Televote project where they conducted votes with hundreds of participants despite using only the telephone.*

[6] *David Chaum presented the idea of blind signatures, which allows officials to validate the identity and authenticity of a voter and still keep a vote secret.*

1.1.2 Razão

A razão da pesquisa é o desafio de empreender a aplicação de verificação de ponta a ponta na votação pela Internet com a tecnologia *blockchain.*

1.1.3 Escopo

De acordo com as comunidades acadêmicas e científicas[7], a experiência dos processos de votação eletrônica e votação pela Internet tornam o sufrágio mais acessível, célere e pragmático, mas parcialmente seguro e confiável para o eleitor e a instituição responsável pelo processo eleitoral.

Isto se deve ao fato de que sistemas de *e-voting* são complexos por natureza tecnológica e, consequentemente, a construção formada de numerosos elementos tecnológicos e interligados pela Internet faz com que sistemas de *i-voting* sejam classificados com maior complexidade.

O tema é abordado, aconselhado e estudado por organizações internacionais nos continentes europeu e americano.

Por exemplo, a *Organization for Security and Co-operation in Europe (OSCE) and Office for Democratic Institutions and Human Rights (ODIHR)* ou Organização para a Segurança e Cooperação na Europa e o seu Gabinete das Instituições Democráticas e dos Direitos Humanos (OSCE/ODIHR, 2013) que, na qualidade de observador de processos eleitorais, apresenta um estudo de boas práticas sobre tecnologias novas para sistemas de votação no continente europeu e Estados Unidos da América (EUA), demonstrando, assim, a importância em saber lidar com as transformações digitais no mundo contemporâneo que impactam diretamente no sistema político democrático.

No mesmo sentido, a Organização dos Estados Americanos (OEA, 2010) também possui um Departamento para Cooperação e Observação Eleitoral que exerce semelhante

[7] Cf. Capítulo 2.

função nas missões de fiscalização dos processos eleitorais dos três continentes americanos com o objetivo de analisar as tecnologias de votação.

Em vista disto, o cenário da pesquisa está concentrado em tecnologias para o processo de votação eleitoral pela Internet em processos políticos para democracias indiretas ou representativas.

Neste caso, a República da Estônia é o único paradigma que há quinze anos exerce a votação pela Internet para o sufrágio nacional *(the Riigikogu elections)*, local *(the local government councils elections)*, Parlamento Europeu *(the European Parliament election)* e plebiscito *(referendum)*, demonstrando alinhamento entre a infraestrutura tecnológica, jurídica, sócio-política e cultural.

É importante observar que a votação pela Internet na Estônia ensina que se deve ter consciência de que a tecnologia em si é parte desse macroprocesso evolutivo e que, apesar dos obstáculos no ambiente governamental e privado[8], ela oferece meios resilientes de superação para promover o desenvolvimento coletivo entre todos os atores da sociedade.

Para o professor Robert Krimmer, a observação do modelo de interoperabilidade tecnológica da Estônia é necessária para a pesquisa ter uma visão holística sobre o sistema de votação pela Internet, pois os mecanismos para as eleições não são apenas métodos pelos quais as sociedades podem expressar as suas opiniões, mas também são indicadores de como um governo utiliza a tecnologia no geral. Ao longo da história, são numerosas as eleições que fizeram o uso das tecnologias emergentes de uma forma ou de outra, mas é preciso ter consciência de que o processo é formado com a sociedade, o direito, a política e a tecnologia (KRIMMER, 2012, pp. 5-16).

No caso do governo estoniano, ele possui um ambiente de governança eletrônica ou *electronic governance (e-governance)* que opera sob uma plataforma *middleware* - *X-Road,* para aplicações distribuídas sob camadas de segurança de dados.

O objetivo da plataforma é que um único dado eletrônico deve ser acessado apenas uma vez de uma única base de dados *(once-only)*, produzindo, assim, uma interoperabilidade de

[8] A parceria público-privada é um processo a longo prazo.

custo-benefício eficiente e eficaz e performance de noventa por cento dos processos burocráticos entre os sistemas públicos e privados para os cidadãos.

Toda essa infraestrutura contribui para a utilização de uma identidade digital única nos processos de governança eletrônica, especialmente, para a votação pela Internet[9].

De outra parte, a investigação *in loco* observa que a arquitetura do sistema de *i-voting* não é cem por cento pela Internet. Há problemas de transparência no processo eleitoral semelhantes a outros sistemas de votação em eleições eletrônicas.

Além disso, o *slogan E-Estonia* também é observado pela pesquisa como uma estratégia de marketing estatal para os serviços públicos do governo estoniano, inclusive, a votação pela Internet e o modelo do sistema de segurança da informação do país[10].

Neste caso, o objetivo da pesquisa é utilizar a tecnologia *blockchain* para potencializar as relações de confiança no ambiente de votação da Estônia.

1.2 PROBLEMA

A investigação entende que apesar do sistema de *i-voting* não ser mais um tema emergente e incipiente na democracia eletrônica ou *electronic democracy (e-democracy)*, o processo de votação pela Internet é um campo ainda incompreensível para o eleitor comum, pois abrange uma gama de assuntos específicos e conhecimentos adicionais sobre ciência computacional.

Isto faz com que os métodos aplicados no processo das cédulas eletrônicas sejam questionados, promovendo-se, assim, um dilema entre os princípios do anonimato, integridade e transparência, todos consubstanciados pela *OSCE/ODIHR* (2013, pp. 9-12) para garantir a consecução plena no processo de votação pela Internet.

Não se pode negar que o dilema em si faz objeção ao nível de medidas tecnológicas que são necessárias para buscar uma ou mais saídas que não sejam contraditórias e igualmente insatisfatórias do ponto de vista da segurança da informação no sistema de *i-voting*.

---

[9] Cf. Capítulo 4.
[10] Id. cit. 9.

Importante se faz ressaltar também que no contexto dos dilemas principiológicos do processo de votação, o anonimato é para ocultar o voto da inter-relação com o eleitor (sigilo do voto), e não o eleitor propriamente dito – *one person, one vote*; a integridade é o fato de que a cédula eletrônica não deve ser adulterada por qualquer pessoa durante todo o processo eleitoral; e a transparência é o poder de observar o curso regular da votação pela Internet de ponta a ponta para ter certeza de que o anonimato e a integridade estão incólumes.

Neste caso, a pesquisa observa *in loco*[11] que o dilema mencionado acima está presente no sistema de votação pela Internet da Estônia, contudo, há parcial fragilidade no sistema que pode comprometer o processo eleitoral do país nórdico por causa da arquitetura lógica e infraestrutura do seu ambiente tecnológico.

Para a pesquisa são três estágios de falhas ou vulnerabilidades que podem ocorrer nas eleições estonianas pela Internet:

a) Servidor de dados é centralizado para o registro das cédulas eletrônicas (Figura 22);
b) Identificação do eleitor é por fator único, e não autenticação em duas etapas (Figura 17);
c) Processamento e contagem das cédulas eletrônicas são realizados em ambiente *off-line:*
    i. Sistema de *i-voting* não fornece prova (recibo) da eliminação da última cédula eletrônica registrada durante o processo de votação múltipla (Figura 20);
    ii. Operação manual de votação paralela (cédula eletrônica e papel) dispõe de informações em arquivo de extensão *portal document format (pdf)* que podem infringir o sigilo da cédula eletrônica (Figura 20); e
    iii. Após as cédulas eletrônicas serem armazenadas em servidor de dados no período *on-line* de votação, os votos eletrônicos são transferidos manualmente para um *memory flash card* que, na sequencia, é encaminhado para um *hardware security module (HSM)* para realizar a anonimização das cédulas com a chave de criptografia privada. Posteriormente, os votos anônimos são processados para a contagem e publicação resultado (Figura 22).

O cenário exposto acima torna o sistema de votação pela Internet estoniano sucetível a interferências indevidas, como interrupções ou manipulações indesejadas de agentes internos

[11] Do latim significa “no local”.

ou externos – ataque computacionais de *Insider threat, Phishing, Man-in-the-middle, Spoofing, Sybil, Botnets* e *DDoS*, comprometendo, assim, o resultado final da eleição *on-line*.

A pesquisa também observa que o sistema de *i-voting* atende parcialmente a verificabilidade de ponta a ponta nas eleições estonianas (Figura 21):

d) Aplicação de verificação de ponta-a-ponta ou *end-to-end verifiability (E2E)*[12] ocorre apenas no ambiente *on-line*, sendo limitada a consulta para o eleitor (três vezes a cada trinta minutos); e
e) Aplicação da verificação de ponta-a-ponta é individual, e não universal.

Notadamente o sistema estoniano não contribui com a transparência do processo de votação pela Internet, pois não realiza a apuração de ponta a ponta, registrando somente o armazenamento correto do voto no servidor de dados em ambiente *on-line,* ignorando os demais processos no sistema de *i-voting*.

Logo, a pesquisa observa que no sistema de votação pela Internet da Estônia não há a verificação *E2E* das cédulas eletrônicas na contagem inicial e final dos votos para a verificabilidade *double-check* ou dupla verificação do resultado da eleição.

1.3 HIPÓTESE

A investigação propõe um modelo novo de aplicação para verificação de ponta-a-ponta em parte do sistema de votação pela Internet estoniano para resolver:

I. As falhas e vulnerabilidades do estágio da letra *c)* e itens *i, ii* e *iii* através do uso da função *hash* com a tecnologia *blockchain*;
II. Abordar o uso da tecnologia *blockchain* para aplicação da verificabilidade *E2E* nos itens que correspondem as letras *d)* e *e)* para que os eleitores, partidos políticos e organizadores do pleito possam apurar a eleição de forma individual e universal.

É importante ressaltar que os estágios mencionados como falhas e vulnerabilidades - itens *a)* e *b),* são ambientes críticos que estão fora do controle da prospota, requerendo, assim, uma abordagem específica *in loco*, portanto, não são objetos de pesquisa da tese.

---

[12] Id. cit. 7.

1.4 DESAFIO

No tocante à tecnologia *blockchain,* o objetivo de utilizá-la não é para fornecer apenas mais segurança da informação ao sistema de *i-voting* da Estônia, mas buscar fortalecer as relações de confiança no processo de votação pela Internet.

Para a pesquisa, a afirmação é importante para diferenciá-la do *buzzword*[13] existente sobre a aplicação da tecnologia *blockchain* para determinadas atividades de meio e fim das corporações[14].

Pode-se dizer que a maioria dos projetos mencionados no Capítulo 2 utilizam o conceito original de Satoshi Nakamoto (2008) - *public permissionless blockchain*, o que proporciona para a pesquisa um indicador positivo na hipótese de implementação da aplicação *E2E* em parte do sistema de votação pela Internet da Estônia.

Por outro lado, a investigação entende a necessidade da customização para uma tipologia *public permissioned blockchain* – Capítulos 5 e 6.

Também é preciso reconhecer que não é tarefa fácil empreender a hipótese diante dos desafios que a própria tecnologia impõe, especialmente com relação aos limites técnicos decorrentes dos *trade-offs*[15] encontrados durante o processo de investigação.

É importante mencionar que apesar da tecnologia *blockchain* ainda ser um tópico emergente e incipiente para sistemas de votação pela Internet, quanto maior for o número de pesquisas, menor será a possibilidade de cometer falhas no futuro e, consequentemente, poder-se-á chegar a uma perspectiva duradoura para o cenário de novas tecnologias de votação.

Aludem a mesma afirmação os estudiosos Alvarez e Hall (2004, p. 10), pois para eles não há como saber se qualquer proposta inovadora relacionada à votação pela Internet esteja correta a menos que elas sejam pesquisadas - mesmo que sejam em pequenas escalas, para que seus sucessos e fracassos possam ser avaliados e validados.

---

[13] Falácia.
[14] Id. cit. 7.
[15] No sentido do equilíbrio entre o risco e o potencial retorno do objeto estudado.

Neste sentido, o tema da pesquisa é emergente, inédito e desafiador.

A proposta busca provar que a hipótese de utilizar a tecnologia *blockchain* para aplicação da verificação *E2E* contribui para tornar mais confiável e transparente o processo de votação pela Internet na Estônia.

A estrutura do trabalho acadêmico foi dividido em sete partes: a) Introdução que aborda o objetivo e a justificativa da tese; b) Capítulo 2 que retrata o estado da arte e a revisão de trabalhos científicos teóricos e práticos; c) Capítulo 3 que aduz sobre a metodologia aplicada na investigação; d) Capítulo 4 que apresenta o cenário evolutivo da administração pública na era digital com enfoque na experiência estoniana; e) Capítulo 5 que explica o sistema de votação pela Internet da Estônia; f) Capítulo 6 que apresenta a proposta de aplicação para verificação ponta a ponta em parte do sistema de *i-voting* com a tecnologia *blockchain*, trabalhos futuros e lições aprendidas; g) Conclusão que faz o fechamento da pesquisa com as últimas observações analíticas. Por fim, a bibliografia, *websites* acessados, glossário e o apêndice.

2. ESTADO DA ARTE

"We can only see a short distance ahead, but we can see plenty there that needs to be done"
Alan Turing

A tese faz o levantamento dos estudos que alcançaram o alto nível de desenvolvimento para retratar o estado da arte sobre os objetos da investigação: *e-voting, i-voting, end-to-end verifiability* e tecnologia *blockchain*. Neste sentido, há necessidade de ir ao encontro de teses, dissertações, artigos científicos, outros meios científicos de publicação e o material disponível *in loco* na República da Estônia.

Na sequência, amplia-se a busca por conteúdos em outras universidades e periódicos como a Biblioteca Digital de Teses e Dissertações (BDTD), *Networked Digital Library of Theses and Dissertations*, *Open Access Theses and Dissertations (OATD)*, Plataforma Sucupira e Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), Google Acadêmico, do país e exterior.

Ressalta-se que a pesquisa se utiliza do programa Zotero para gerenciar os dados bibliográficos e materiais relacionados a tese.

2.1 REVISÃO DA LITERATURA

Inicia-se a pesquisa pela coleta de informações na biblioteca digital da Pontifícia Universidade Católica de São Paulo (PUC-SP)[16], Universidade Tecnológica de Talín ou *Tallinn University of Technology* (*TALTECH)*[17, 18], *National Library of Estonia*[19] ou Biblioteca Nacional da Estônia, conferências *ad hoc* sobre sistemas digitais de votação e empresas nacionais ou internacionais especializadas no mercado do sistema de *i-voting*.

No banco de dissertações e teses da PUC-SP são encontradas a tese: a) Facundo Guerra Rivero - "Tecnologia e política: o voto e seu suporte"; e a dissertação de mestrado: b) Daniel

[16] Disponível em: http://biblio.pucsp.br/.
[17] Até a primeira quinzena do mês de setembro de 2018, a universidade se utilizou do acrônimo *TTÜ* (estoniano) ou *TUT* (inglês). A partir do dia 14/09/2018 ela adotou a marca *TALTECH*.
[18] Disponível em: https://old.taltech.ee/institutes/library-3/for-students/databases-5/
[19] Disponível em: https://www.ester.ee/search~S1.

Márcio de Medeiros – "Mecanismo de consenso em uma rede ponto a ponto distribuída para validação e registros de diplomas universitários".

Para cada tema a pesquisa entende que:

- Rivero (2012): o trabalho analisa o panorama eleitoral incompleto da história das urnas eletrônicas brasileiras, incluindo seus obstáculos no cenário nacional e global, como também reflete superficialmente sobre o sistema de votação pela Internet. No final, a pesquisa não avança em tópicos como, por exemplo, protocolo de criptografia computacional ou tecnologia *blockchain*, mas somente aborda o âmbito jurídico nacional. Não há contribuição para a tese;

- Medeiros (2019): a dissertação analisa a utilização no futuro de mecanismos de consenso com a tecnologia *blockchain* para o processo de validação, emissão e registro de diplomas acadêmicos pelas Instituições de Ensino Superior (IES) brasileiras. A parte que discorre sobre o *blockchain* contribui de forma parcial para a pesquisa.

Na *TALTECH*, o Departamento de Inovação e Governança *Ragnar Nurkse* ou *Ragnar Nurkse Department of Innovation and Governance* foi o laboratório para a pesquisa *in loco* durante dez meses entre maio de 2018 a fevereiro de 2019, e que forneceu um repositório de literatura importante, especialmente em relação à parceria da universidade com a conferência internacional sobre *E-voting* e *E-Vote-ID*[20].

Na biblioteca da *TALTECH* encontra-se quatro dissertações de mestrado dos seguintes autores: a) Tanel Torn – *Security* A*nalysis of Estonian I-voting System Using Attack Tree Methodologies;* b) Nisham Kizhakkedathil - *A Study Into The Prospects of Implementing End-to-End Verifiability in Estonian I-voting*; c) Crystal Cushing La Grone - *Engaging Youth Voter Participation with Internet Voting in Estonia*; and d) Radu Antonio Serrano Iova - *I-Voting Costs: A Case Study of the 2019 Estonian Parliamentary Elections;* e duas teses de doutorado: a) Robert Krimmer - *The Evolution of E-voting: Why Voting Technology is Used and How it*

[20] A conferência existe desde o ano de 2004, sendo que de 2004 a 2015 era conhecida como *E-Voting and Identity (Vote-ID)* e do ano de 2016 até os dias atuais o nome foi alterado para *The International Conference on Electronic Voting (E-Vote-ID).*

Affects Democracy; b) Priit Vinkel – *Remote Electronic Voting in Estonia: Legality, Impact and Confidence.*

Para cada assunto abordado a pesquisa entende que:

- Torn (2014): o estudo se baseia na análise de segurança do sistema de *i-voting* com a propositura de três métodos de ataques simulados em aplicações diferentes, mas sem relação *in loco* com o sistema de votação. É uma contribuição parcial para o doutorado;

- Kizhakkedathil (2016): o autor analisa o cenário estoniano de votação pela Internet sob a perspectiva do risco de segurança no processo eleitoral e o sistema de verificação de ponta a ponta. O trabalho contribui parcialmente para a pesquisa do doutorado em razão da superficialidade das informações coletadas e a falta de clareza da investigação com as recomendações aludidas ao objeto estudado;

- La Grone (2016): o objetivo da dissertação é entender a participação dos eleitores estonianos no processo de votação pela Internet entre 2005 e 2015 para o pleito nacional. Apesar da relevância do tema não é o ponto central da pesquisa;

- Iova (2019): estuda os trâmites administrativos do pleito eleitoral de 2019 com foco na análise dos custos em atividades individuais do processo de votação pela Internet. A dissertação é inspirada ou parte do resultado de pesquisas do grupo de estudos denominado *the Cost of Democratic Elections (CoDE)*, *TALTECH.* Há contribuição para a tese no âmbito de entender a função dos atores no processo de *i-voting;*

- Krimmer (2012): apresenta a visão holística sobre a aplicação, evolução, motivação e impacto da tecnologia no processo de *e-voting* e *i-voting*. A relevância do trabalho contribui de forma parcial para a tese com relação ao conteúdo histórico e inferência holística do tema;

- Vinkel (2015): o autor analisa a segurança jurídica, o impacto político-social e a credibilidade no sistema de votação pela Internet pelos eleitores estonianos. É um tema relevante na ótica social, mas também contribui parcialmente para a pesquisa.

No acervo digital da Biblioteca Nacional da Estônia, a pesquisa encontra duas dissertações de mestrado e um livro na *Tartu University* ou Universidade de Tartu: a) Ülo Leppik - *Casting Votes Digitally: Examining the Latvian National Position on Internet Voting;* b) Anna Beitane - *Casting Votes Digitally: Examining the Latvian National Position on Internet Voting;* e a) Mihkel Solvak e Kristjan Vassil - *E-voting in Estonia:Technological Diffusion and Other Developments Over Ten Years (2005 - 2015).*

- Beitane (2016): o trabalho faz a análise documental do processo de evolução da votação pela Internet na Letônia entre 2012 e 2015 em comparação com o sistema de *i-voting* estoniano;

- Leppik (2015): analisa o processo de *i-voting* estoniano entre 2007 e 2011 para entender os custos e a participação do eleitor no processo de votação pela Internet;

- Solvak e Vassil (2016) e co-autores Priit Vinkel, Mihkel Solvak e Taavi Unt: o livro expõe reflexões a respeito do sistema *i-voting* estoniano entre 2005 e 2015 sob a perspectiva política, regulatória, social e tecnológica.

Em todos os trabalhos, há parcial contribuição na literatura acima para a tese com destaque para o cenário estoniano de votação pela Internet, o sistema de *e-governance* e os impactos no processo democrático.

2.2 DISCUSSÃO

Neste capítulo, a pesquisa discute a adoção da tecnologia *blockchain* para verificabilidade de ponta a ponta em eleições com voto pela Internet.

Em primeira análise, a tese faz um panorama conceitual sobre *e-voting, i-voting, E2E verifiability* e *blockchain* para em seguida iniciar a discussão de estudos anteriores para cada tema especificamente.

2.2.1 Breve História da Votação por meios Eletrônicos

Em Krimmer (2012, pp. 16-28), o trabalho apresenta a linha do tempo histórica da votação expondo o surgimento dos procedimentos, processos e tecnologias rudimentares que são a base para o cenário atual.

É interessante observar que no início o voto público (aberto) é o mais usual e também bastante criticado, mas com o passar do tempo e a particularidade para tomar certas decisões, o voto secreto ganha força no decorrer da história da humanidade, tornando-se o fator preponderante para a utilização das tecnologias com o objetivo de garantir o sigilo do voto.

Após a primeira aparição da tecnologia para votação em meados de 1836 - Inglaterra, a ideia de utilizar meios eletrônicos para o processo democrático tem mais importância após o fim da Segunda Guerra Mundial em 1945, obviamente, em razão da possibilidade de ampliar a participação dos cidadãos na escolha de líderes políticos. (FULLER, 1967, p. 03-05).

Desde então, o uso de meios eletrônicos para o processo de votação passa por transformações que perduram até os dias de hoje, sendo adaptado de acordo com os avanços tecnológicos e as necessidades econômicas, jurídicas, políticas e sociais de cada pleito durante uma eleição eletrônica ou *electronic election (e-election)*.

2.2.2 Votação Eletrônica ou Electronic Voting (e-voting)

De acordo com o *Council of Europe* (2017), há trê reflexões sobre o tema. Primeiro, o voto eletrônico ou *electronic vote (e-vote)* é a maneira do eleitor expressar a sua opção de voto eletronicamente. Segundo, a votação eletrônica é o uso dos meios eletrônicos para registrar ou contar o voto. Por fim, o sistema de *e-voting (system)* é a composição de *hardware, software* e processos que permitem ao eleitor votar eletronicamente em um pleito eleitoral.

É possível observar que os conceitos acima dizem respeito à cédula eletrônica ou *electronic ballot (e-ballot),* processo eletrônico ou *eletronic process (e-process)* e sistema computacional. Apesar de que o termo “sistema” também pode ser compreendido como o conjunto de regras e leis que fundamentam a votação eletrônica.

De acordo com Krimmer (2012, p. 25) há doze formas de tecnologias de votação para eleições governamentais classificadas em seis categorias operacionais: registro, contagem, votação aberta, votação secreta, ambiente controlado e ambiente não controlado.

Das dozes formas acima, a pesquisa lista os três modelos eletrônicos mais contemporâneos (FISCHER, 2006; NORDEN, 2015; EUROPEAN COMISSION, 2017):

a) *Optical Scan* ou *Punch Card*: leitura com digitalização ótica ou cartão perfurado;
b) *Direct Recording Electronic (DRE)* ou *Touch Screen E-Voting Machine:* registro direto com o uso dos teclados ou com toque digital na tela do computador que também pode se tornar um *DRE with Voter Verified Paper Trail (VVPT)* – com dispositivo de impressão do comprovante do voto;
c) *Internet Voting* ou *Remote Voting*: votação pela Internet.

Com base na classificação de Krimmer (2012), o item *a)* opera em ambiente controlado com voto aberto ou secreto; e os itens *b)* e *c)* operam em ambiente controlado ou não controlado com voto aberto ou secreto. Todos realizam a contagem dos votos eletronicamente.

Para a pesquisa, é conjecturável dizer que qualquer sistema computacional está suscetível à fraude e vulnerabilidade. E, independente do sistema de *e-voting*, o maior desafio imposto até os dias atuais é a segurança das informações antes e durante o dia da eleição.

De acordo com o relatório da *DEF CON*[21] (2017) - *Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure,* sistemas de votação digitais são sucetíveis a falhas *(bug)* ou vulnerabilidades de *hardware*, sistema operacional e em programas de computador. Em exemplo prático, o caso de substituição dos sistemas *e-voting* do tipo *DRE* no estado da Virgínia, Estados Unidos da América (EUA), por causa da vulnerabilidade exposta meses antes da eleição (ITU COPENHAGEN, 2017).

Em razão disso, alguns estudiosos dedicam-se para dirimir os problemas de segurança das informações nos sistemas de *e-voting* e, paralelamente, elaborar um modelo menos sucetível a fraudes ou invasões de agentes maliciosos. Dentre eles podemos mencionar os trabalhos de Fisher, Carback e Sherman (2006) e Benaloh, Byrne, Eakin, Kortum, McBurnett, Pereira, Stark, Wallach, Fisher, Montoya, Parker e Winn (2013), que propõem modelos novos de sistemas de votação eletrônica, em especial, para os protocolos de chaves criptográficas.

[21] Convenção de *hackers* criada em 1993.

O termo *e-voting* é considerado na comunidade acadêmica como uma terminologia genérica para outros meios de votação eletrônica, pois é possível associar parte do processo do sistema de *e-voting* à Internet, tornando-se um sistema de votação híbrido.

Neste caso, a cédula eletrônica não é mais armazenada na urna eletrônica ou *electronic ballot box (e-ballot box)* localmente, mas é enviada remotamente em *link* de comunicação dedicado para um servidor de dados central do sistema de *i-voting.*

É necessário afirmar que os riscos do ambiente de segurança das informações são potencializados quando o assunto aborda o processo de votação pela Internet.

2.2.3 Votação pela Internet ou Internet Voting (i-voting)

A pesquisa entende que a votação pela Internet ou *i-voting* é um fenômeno natural emergente para a sociedade global.

Para os estudiosos Alvarez e Hall (2004, p. 04), a *Remote Internet voting* ou votação Remota pela Internet é o processo eleitoral realizado através de uma conexão com a Internet mediante o auxílio de um microcomputador pessoal que não está sob o controle físico do responsável pela eleição. Segundo eles, há três modelos conceituais de *i-voting* ou *remote Internet voting*: a) *kiosk Internet voting;* b) *polling place Internet voting;* e c) *(own) precinct Internet voting.*

De acordo com os autores, os itens *a)* e *b)* referem-se ao uso de um microcomputador em local supervisionado pela autoridade eleitoral, sendo que o lugar poderá ser específico ou genério dentro do perímetro de segurança física estabelecido pelo órgão responsável. Já no tocante ao item *c)* ele está relacionado ao fato do eleitor votar pela Internet em qualquer lugar e sem controle físico do órgão competente, por exemplo, residência, escritório laboral, praça pública e etc.

Ambos os autores seguem a mesma linha conceitual do relatório *California Internet Voting Task Force* (EUA, 2000, pp.02-03)[22] – um relatório criado para estudar o uso da votação

[22] *Definitions of Internet Voting: a) For the purposes of this report, an* ***Internet Voting System*** *is defined as an election system that uses electronic ballots that would allow voters to transmit their voted ballot to election officials over the Internet; b)* ***Internet Voting*** *means the casting of a secure and secret electronic ballot that is transmitted to election officials using the Internet; c) An* ***Internet Voting Machine*** *is defined as the computer hardware that allows an electronic ballot to be cast over the Internet; d)* ***Polling Place Internet Voting*** *is defined*

pela Internet na Califórnia (EUA), que pode ser considerado um dos precursores na definição dos termos que envolvem sistemas de *i-voting.*

No *Handbook For the Observation of New Voting Technologies* ou Manual para Observação das Novas Tecnologias de Votação da *OSCE/ODIHR*, a votação pela Internet tem o seguinte conceito:

> Permitir que os eleitores votem em qualquer lugar e em ambiente não controlado. Os votos são armazenados e agregados eletronicamente em um local centralizado. Atualmente, a Internet é o principal canal de votação em uso em sistemas remotos de votação eletrônica (OSCE/ODIHR, 2013, p. 06).

Em consonância com reflexões acima, a tese pode concluir que o sistema de *i-voting* é quando o eleitor tem acesso autorizado e seguro ao *website* oficial da eleição para que através de um microcomputador ou *laptop* ele tenha condição para escolher o candidato e o partido político durante o processo de votação pela Internet.

Não obstante, a segurança da informação também está relacionada ao cenário rudimentar e atual dos sistemas de *i-voting.* Com base na acepção de Robert Krimmer:

> Em 1978, os pesquisadores Ted Becker e Christa Slaton conduziram o projeto *Televote*, onde realizaram votos com centenas de participantes, apesar de usar apenas o telefone (Slaton, 1992). Quatro anos depois, David Chaum apresentou a idéia de "assinaturas cegas", que permitem que os funcionários validem a identidade e autenticidade do eleitor e ainda mantenham o voto em segredo (Chaum, 1982). Esta invenção permitiu implementar uma eleição eletrônica integrada que consiste em todas as etapas de uma eleição em uma rede pública, incluindo verificações de elegibilidade, votação e contagem de votos, introduzindo assim a forma mais complexa de votação eletrônica: votação pela Internet (KRIMMER, 2012, p.23).

A partir disso surgem trabalhos de destaque como, por exemplo, Cramer, Gennaro e Schoenmakers (1997); Chaum (2001); Adida (2008); Clarkson, Chong e Myers (2008); e Gjøsteen (2013), com o propósito de inovar ou melhorar o modelo de *i-voting*, principalmente

---

as the use of Internet Voting Machines at traditional polling places staffed by election officials who assist in the authentication of voters before ballots are cast.; e) ***Remote Internet Voting*** *means the unsupervised use of an Internet Voting Machine to cast a ballot over the Internet using a computer not necessarily owned and operated by election personnel. Authentication of the voter would rely on procedures outlined later in this report, but must include some form of identity verification that is at least as secure as existing voting procedures.*

no que se refere à anonimização de dados que, em certos casos, tornam-se buscas científicas "incessantes" para criar a criptografia de chaves "perfeita".

Muito embora isso seja bastante louvável para a academia na área computacional e mercadológica, a pesquisa entende que o uso do protocolo de criptografia de chaves é apenas um dos garantidores do sistema de votação pela Internet e a tecnologia não é suficiente para combater fraudes acometidas por comportamentos sociais que estão fora do controle tecnológico.

É importante ressaltar que as comunicações através da Internet envolvem não apenas às duas partes conectadas, mas também há intermediários controlados por terceiros que podem ou não compor o órgão responsável pela eleição (ambiente não controlado). Assim, o sistema de *i-voting* precisa impedir que esses intermediários se tornem a falha ou a vulnerabilidade para o processo de votação pela Internet.

Segundo o *California Internet Voting Task Force* (EUA, 2000, p.18), os problemas técnicos em relação à segurança da informação no sistema de *i-voting* são: a) autenticação eletrônica do eleitor; b) integridade da cédula eletrônica; c) confiabilidade do meio de transmissão e armazenamentos dos votos eletrônicos; d) votação múltipla segura; e) defesa do sistema de votação pela Internet no ambiente dos eleitores e do governo responsável pelo pleito contra ataques de agentes maliciosos.

Para a pesquisa, conclui-se que qualquer sistema de votação eletrônica ou votação pela Internet deve ter um sistema ou aplicação de verificação de ponta a ponta. Em especial, que ela seja um *software* independente (RIVEST e WACK, 2006) ao sistema de votação para potencializar a confiança e a participação no processo eleitoral.

2.2.4 Verificação de Ponta a Ponta ou End-to-End Verifiability (E2E)

Os sistemas ou aplicações para verificação de ponta a ponta ou *End-to-End verifiability (E2E)* não são novidades em ambientes de votação eletrônica, pois são estudados há aproximadamente uma década.

Desde 2010, os estudiosos David Chaum, Manuel Krip, Melanie Volkamer e Rüdiger Grimm observam que estudar metodologias para aplicação da verificabilidade de ponta a ponta em eleições eletrônicas é uma maneira de aperfeiçoar as observações no processo de votação (KRIMMER, 2012, p. 08).

Segundo a *OSCE/ODIHR* (2013, p. 68), a verificabilidade de ponta a ponta é uma funcionalidade dos sistemas com novas tecnologias de votação eletrônica que permitem a validação dos resultados de maneira universal - por meio de verificações manuais ou matemáticas; e/ou de forma individual - através da verificação do registro e contagem do voto pelo eleitor.

Para a pesquisa é importante analisar a literatura sobre a verificabilidade de ponta a ponta em eleições eletrônicas para entender os avanços e os desafios que a tecnologia impõe a partir do uso de tecnologias específicas ou emergentes, como é o caso da tecnologia *blockchain.*

As limitações e os *trade-offs* escolhidos são uma amostragem das pesquisas que adotaram na prática algum tipo de sistema ou aplicação para verificabilidade *E2E* em votações eletrônicas.

1. A ideia de usar dois canais de autenticação (sistema *web* e *e-mail)* para acessar a *public bulletin board* ou "boletim da urna", em *website* e verificar o resultado de uma eleição é muito atrativo em primeira análise, por exemplo: a) *Rijnland Internet Election System (RIES)* (HUBBERS, BART, JACOBS e PIETERS, 2005); (GONGGRIJP, 2009); b) *Prêt à Voter* (BISMARK, 2009); (BURTON, 2012); (CHAUM, RYAN e SCHNEIDER, 2005); (RYAN *et al.*, 2009); c) *Punchscan* (ESSEX, 2007); (POPOVENIUC e HOSP, 2006 e 2010); d) *Scantegrity II* (CARBACK, 2010); (CHAUM, 2008 e 2009); e) *Remotegrity* (ZAGÓRSKI, 2013); f) *Helios* (ADIDA, 2008 e 2009); (BULENS, GIRY E PEREIRA, 2011); (TSOUKALAS *et al.*, 2013); (UNIVERSITY OF WASHINGTON COMPUTER SECURITY, 2009); g) *Wombat* (WOMBAT VOTING SYSTEM, 2011); h) DEMOS (DELIS *et al.*, 2014); i) D-DEMOS (CHONDROS, ZHANG, ZACHARIAS, DIAMANTOPOULOS, MANEAS, PATSONAKIS, DELIS, KIAYIAS e ROUSSOPOULOS, 2016); j) *A peered bulletin board for robust use in verifiable voting systems* (CULNANE e SCHNEIDER, 2014). No entanto, é possível notar que a utilização de dois canais não oferece transparência no processo de votação, pois é iminente a possibilidade de um agente malicioso - interno ou externo, ou um procedimento errôneo do eleitor oferecer um meio de violar o sigilo do voto eletrônico ou impresso. Consequentemente, a utilização de *bulletin board* também torna o sistema de votação suscetível a ataques de *spoofing* e *Denial of Service (DoS)*.

2. Em *Norwegian System* (GJØSTEEN, 2012); (CARTER CENTER, 2014) o sistema utiliza três combinações para registrar e verificar o voto: *e-mail,* Internet e mensagem de texto via aparelho de telefonia celular *(SMS text messaging)*. No entanto, a aplicação *E2E* fornecido pela *Scytl* não dispõe de verificação universal (contagem ou totalização) das cédulas eletrônicas e não há contra-prova do descarte da última cédula durante a votação múltipla. Logo, o sistema não é verificável de ponta a ponta e, também, não contribui com a transparência do pleito eleitoral. Além disso, é passível de ataque de programa de computador malicioso.

3. A combinação dos conceitos já existentes na segurança computacional que está por detrás da tecnologia *blockchain* são aplicadas em pesquisas acadêmicas que, no todo ou em parte, buscaram soluções para os sistemas de votação eletrônica com o uso de *hash function* para assegurar a integridade das cédulas eletrônicas nos recibos dos eleitores, por exemplo: a) *Castin Votes in the Auditorium* (SANDLER e WALLACH, 2007); b) *VoteBox: A Tamper-evident, verifiable electronic voting system* (SANDLER, DERR, e WALLACH, 2008); c) *The trash attack: An attack on verifiable voting systems and a simple mitigation* (BENALOH, LAZARUS, 2011); d) *STAR-Vote: A secure, transparent, auditable, and reliable voting system* (BELL, BENALOH, BYRNE, DEBEAUVOIR, EAKIN, FISHER, KORTUM, MCBURNETT, MONTOYA e PARKER, *et al.*, 2013). O resultado de cada pesquisa é um complemento ou um concatenado de outras técnicas em sistemas de *e-voting.* Não são pesquisas com *status* de tecnologia *i-voting.* A verificabilidade *E2E* universal é parte das pesquisas, mas sem abordar a verificação individual para fortalecer a transparência do processo.

4. Em outras pesquisas, a tecnologia *blockchain* é o tema central na busca de soluções em processos eleitorais eletrônicos, por exemplo: a) *CommitCoin: carbon dating commitments with Bitcoin* (CLARK e ESSEX, 2012); b) *An End-to-end Voting-system Based on Bitcoin* (BISTARELLI, MANTILACCI, SANTANCINI e SANTINI, 2017); c) *Buying Votes in the 21st Century: The Potential Use of Bitcoins and Blockchain Technology in Electronic Voting Reform* (BOGUCKI, 2017); d) *Transparent Voting Platform Based on Permissioned Blockchain* (FAOUR, 2018); e) *Votebook: A proposal for a blockchain-based electronic voting system* (KIRBY, MASI e MAYMI, 2016); f) *Towards Secure E-Voting Using Ethereum Blockchain* (KOÇ, YAVUZ, ÇABUK, e DALKILIÇ, 2018); g) *Electronic voting service using block-chain* (Lee, James, Ejeta e

Kim, 2016); h) *Design of Distributed Voting Systems* (METER, 2015); i) *Blockchain electronic vote* (NOIZAT, 2015); j) *Using Blockchain and smart contracts for secure data provenance management* (RAMACHANDRAN e KANTARCIOGLU, 2017); k) *An anonymous distributed electronic voting system using Zerocoin* (TAKABATAKE, KOTANI e OKABE, 2016); l) *An E-voting System based on Blockchain and Ring Signature* (WU, 2017); m) *How to Vote Privately Using Bitcoin* (ZHAO e CHAN, 2016). A pesquisa observa que a maioria dos trabalhos optaram pela tecnologia *public permissionless blockchain* com base no protocolo *Bitcoin* e aplicação de *bulletin board* para propor um sistema de votação "completo". É importante ressaltar que o papel da *Bitcoin* de Satoshi Nakamoto (2008) é realizar a transferência de dados de forma anônima. Em uma *e-election* é o oposto, pois os eleitores precisam ser identificados para garantir a uniformidade do voto, ou seja, um serviço externo de autenticação para autorizar e regularizar o eleitor. É comum nesta categoria de *ledger* uma cadeia de blocos limitada em frequência e tamanho. Isto quer dizer que o número de transações por segundo para validar a *blockchain* é muito baixo, ou seja, dependendo da escalabilidade e multiplicidade de votos permitidos durante o pleito eleitoral, um *ledger* desse tipo torna o tempo de resposta do processo eleitoral impraticável e moroso, ainda mais se tiver que também verificar a elegibilidade dos nós da rede. Em um caso isolado do tipo *private permissioned blockchain*, também não é a melhor opção, pois um sistema com integridade de dados via *hash function* poder ser mais trivial.

5. No viés mercadológico da *e-election*, a tecnologia *blockchain* e demais métodos também estão presentes, contudo, as informações são parcialmente publicadas. Não obstante o caráter "revolucionário" das arquiteturas em *blockchain* para *i-voting* ou *e-voting*, a pesquisa observa que cada aplicação ou plataforma requer muito poder de processamento para sustentar o processo de votação. A autenticação do eleitor é uma vulnerabilidade latente, seja realizada via *e-mail, SMS, eID, mID, biometric* e etc. Por último, a verificabilidade de ponta a ponta, individual ou universal, não é transparente em todo o processo de votação. Abaixo segue a lista de cada modelo analisado:
    a. *Agora* (https://agora.vote): a empresa *Agora* publicou oficialmente no dia 07 de março de 2018, na capital *Freetown*, Serra Leoa (África), a realização das "primeiras eleições com a utilização da tecnologia *blockchain* no mundo". Todavia, a metodologia do projeto não oferece vantagem para a verificação ponta a ponta em eleições eletrônicas. Na verdade, a auditoria do sistema utiliza

como ferramenta uma recontagem tradicional (voto "cantado em voz alta") para serem calculados (via planilha eletrônica) e depois registrados no sistema da *Agora* com tecnologia *blockchain*. Diante da controvérsia sobre a suposta "inovação" no setor, a equipe da empresa *Agora* exclui a publicação oficial do seu sítio da Internet (https://agora.vote/pdf/Agora_Press-release_SL2018.pdf), mas ainda é possível encontrá-la no cache da empresa *Google* (https://medium.com/agorablockchain/agora-official-statement-regarding-sierra-leone-election-7730d2d9de4e);

b. *Boulé* (https://www.boule.one/): a empresa oferece a autenticação do eleitor pelo modo de reconhecimento facial na *blockchain.* O *website* e o artigo científico estão *off-line*, ofuscando qualquer informação a mais sobre a plataforma. Apenas há um *link* disponível (https://www.newswire.com/news/introducing-boul-blockchain-based-online-voting-technology-19975015);
c. *Coalichain* (https://www.coalichain.io/): segundo os criadores é uma plataforma em *Ethereum public blockchain* com o objetivo de utilizar a ideia da *liquid democracy* ou democracia líquida para o processo de votação pela Internet. Apesar ser um tema atrativo para a ideologia democrática, é impraticável a sustentação computacional em *blockchain* e os riscos de segurança são iminentes no *website*;
d. *Democracy.Earth* (https://www.democracy.earth/): é uma plataforma em *Distributed Autonomous Organization (DAO)* elaborada com *smart contract Ethereum blockchain.* A arquitetura e o propósito da ferramenta de votação são semelhantes ao *Coalichain*;
e. *e-Vox: Open e-Democracy Platform* (http://e-vox.org/): o projeto é um sistema de *e-voting* criado por entusiastas e especialistas em *blockchain* na Ucrânia, sendo iniciado em 2016. De acordo com o organismo não-governamental, as informações somente podem ser fornecidas mediante uma consulta agendada. Não há notícia de algum caso testado com esta plataforma pelo governo ucraniano;
f. *Follow My Vote* (https://followmyvote.com/): é uma plataforma em *blockchain* proveniente dos EUA que, apesar de ser *open source,* não fornece muita informação sobre a arquitetura;
g. *Polys* (https://polys.me/): é uma arquitetura em *blockchain* proveniente da Rússia que, apesar de ser *open source,* também não fornece muita informação

sobre a plataforma *web*. Existe uma versão *beta* do produto que está disponível *on-line* (https://polys.me/admin/create-vote/1591467678528);

h. *SecureVote* (https://secure.vote/): a plataforma *web* (*app* via *smartphone*) australiana é baseada em tecnologia *blockchain* com um sistema de governança chamado de *blockchain agnostic scalability layer (BASL)*. Não fornece muita informação sobre o sistema de votação;

i. *TIVI* (https://tivi.io/): é uma plataforma *web* da *Smartmatic-Cybernetica Centre of Excellence for Internet Voting*[23]. De acordo com o *website* é baseado em *blockchain-based digital time stamping.* Em Krips, Kubjas e Willemson (2018), a plataforma é reportada na eleição de 2016 para o Partido Repubicano no estado de *Utah* (EUA) para testar verificabilidade *E2E*. Utiliza-se da ferramenta *EasyCrypt* para validar um novo protocolo de *i-voting* que suporta a verificação pós-eleitoral usando um recibo gerado em conjunto por aplicativos e servidores de votação. É inspirado no protocolo *IVXV-ÜK-1.0* da Estônia (2017).

j. *Voatz* (https://voatz.com/): é uma plataforma *HyperLedger permissioned blockchain* para o processo de *e-election* com o uso de *smatphones.* Não há informações técnicas sobre a plataforma *mobile*; e

k. *VoteWatcher* (http://votewatcher.com/): a plataforma norte-americana é baseada em protocolo específico - *Florincoin blockchain*. O sistema armazena o voto digitalizado em cédula de papel na plataforma *off-line Florincoin* para que, posteriormente, o *hash code* seja encaminhado à plataforma *Bitcoin public blockchain* para ser utilizado como um *bulletin board*.

2.2.5 Verificação E2E Estoniana

A aplicação de verificabilidade *E2E* estoniana não existia até as eleições de 2013 porque o governo estoniano acredita que o sistema de *i-voting* está seguro com base na infraestrutura de identidade eletrônica - *ID Card*[24].

---

[23] *In 2014, Smartmatic and Cybernetica founded a multidisciplinary center of research and development, aiming to advance online voting on a global scale - TIVI is the result of this successful partnership. Today, out of the eight countries pioneering election automation Smartmatic provides technology and services to six of them: Belgium, Brazil, Estonia, the Philippines, US and Venezuela.*

[24] Cf. Capítulos 4 e 5.

No entanto, o Comitê Eleitoral Nacional da Estônia ou *National Election Committee (NEC)* adota a verificação *E2E* porque nas eleições parlamentares do ano de 2011 são encontradas falhas gravíssimas da aplicação no sistema de *i-voting* no país.

Segundo os especialistas da empresa *Smartmatic-Cybernetica:*

> Embora seja bastante simples, o sistema tem vários pontos fracos, alguns dos quais foram explorados durante as eleições parlamentares de 2011. O ataque mais severo e amplamente publicado foi proposto por um estudante que fez uso do fato de que, em sua forma original, o sistema de votação não dava nenhum *feedback* confiável sobre como o voto foi efetivamente recebido pelo servidor. O aluno desenvolveu várias versões do *malware* que foram capazes de bloquear e até mesmo alterar o voto. Devido à natureza simples do protocolo básico, tais manipulações permaneceriam despercebidas pelo eleitor (HEIBERG e WILLEMSON, 2014, p. 24).

A partir desse fato, a *OSCE/ODIHR* (2011) recomenda ao *NEC* a criação de um grupo de trabalho para implementar uma aplicação de verificabilidade *E2E* no sistema de *i-voting.*

Consequentente, o *NEC* testa dois projetos pilotos para aplicação verificabilidade individual de ponta a ponta nas eleições municipais de 2013 e do parlamento europeu no ano de 2014, sendo que o primeiro teste não apresenta falha, mas o segundo teste de 2014 apresenta dois problemas no aplicativo de verificação individual *E2E* (HEIBERG e WILLEMSON, 2014, pp. 27-28).

No ano de 2013, os especialistas da Universidade de *Michigan* (EUA) e do *Open Rights Group* do Reino Unido também observam o sistema *i-voting* estoniano e relatam que o sistema não possui características suficientes para ser um sistema auditável por um aplicativo de verificação *E2E* pelo eleitor, pois o sistema usa um *design* conceitual simples ao custo de ter que confiar implicitamente na integridade dos computadores de eleitores, nos componentes de segurança instalados nos servidores de dados e nas pessoas que trabalham para as entidades organizadoras do pleito (SPRINGALL, DURUMERIC, HALDERMAN *et al.*, 2014, p. 01).

Em contraparte, os especialistas Heiberg, Martens, Vinkel e Willemson (2016, pp. 213-214-2015) propuseram no ano de 2016 uma segunda atualização do sistema de *i-voting* – denominado de *IVXV-ÜK-1.0,* com o objetivo de redesenhar o sistema de votação pela Internet da Estônia para se tornar menos dependente do fator humano, permitir uma verificabilidade *E2E* mais independente e aprimorar a separação de tarefas entre diferentes organizações.

A atualização do sistema de *i-voting* foi publicada em junho de 2017 no documento intitulado *General Framework of Electronic Voting and Implementation thereof at National*

Elections in Estonia, State Electoral Office of Estonia[25], que reporta uma visão generalista dos processos de votação pela Internet[26].

Em que pese os esforços do *NEC* e especialistas responsáveis pelo sistema de *i-voting,* a pesquisa observa que a aplicação de verificação de ponta a ponta não atende uma apuração completa da coleta das cédulas eletrônicas até a totalização e publicação dos resultados[27].

Corrobora com o posicionamento da pesquisa a *OSCE/ODIHR* que, no ano de 2019, aconselha novamente a revisão do processo de verificabilidade *E2E* da cédula eletrônica para as eleições pela Internet na Estônia.

> O comitê estadual de votação estoniano pode fortalecer o seu processo de auditoria desenvolvendo uma estratégia completa e exigindo que os auditores implementassem ferramentas de auditoria crítica de forma independente e do "zero". As especificações tecnológicas que acompanham a estrutura legal podem definir sistemas de votação aceitáveis em termos mais gerais, mas incluem requisitos adicionais relacionados à força criptográfica, garantia de qualidade, desenvolvimento e implantação de *software*, além de responsabilidade *(accountability)* e verificabilidade *(verifiability end-to-end)* (OSCE/ODIHR, 2019, p. 12).

No mesmo ano, a *Minister for Foreign Trade and Information Technology*, Kert Kingo, do governo estoniano cria o grupo de trabalho e publica o primeiro esboço, *E-election Security Working Party Report* (ESTONIA, 2019, pp. 30-31; 46-47; 57-58), para analisar todos os aspectos relacionados a votação pela Internet, inclusive, a verificação de ponta a ponta.

A postura da Ministra estoniana é acertada porque a Estônia vem de um problema grave com o documento de identificação digital - *ID Card*, ocorrido no ano de 2017. Segundo o relatório governamental da *Information System Authority - ROCA Vulnerability and eID: Lessons Learned*:

> Na noite de 30 de agosto de 2017, um pesquisador do Centro de Pesquisa em Criptografia e Segurança da Universidade *Masaryk* notificou a Estônia da vulnerabilidade de segurança nos *chips* usados no cartão de identificação. De acordo com a análise do grupo de pesquisa, a vulnerabilidade, conhecida como *ROCA (Return of the Coppersmith Attack)*, afeta a geração de pares de chaves criptográficas *RSA* em *chips* produzidos por um dos principais fabricantes – *Infineon.*

---

[25] *Document: IVXV-ÜK-1.0 (20 June 2017)* - Quadro Geral de Votação Eletrônica e sua Implementação nas Eleições Nacionais da Estônia, Escritório Eleitoral Estadual da Estônia.

[26] Cf. Capítulo 5.

[27] Cf. Introdução - seção 1.3.

> Ao todo são aproximadamente 800 mil cartões com *chips* vulneráveis desde 2014 no país (ESTONIA, 2018, p. 01).

Como se pode notar, a investigação entende que a infraestrutura de identificação digital estoniana não é absolutamente segura. Isto nos faz refletir sobre os impactos negativos que podem ter ocorrido no sistema de votação pela Internet entre 2014 e 2017.

Da mesma forma como o governo estoniano não tinha conhecimento da vulnerabilidade dos *chips*, os riscos de segurança do *ID Card* ainda podem ser eminentes e causar danos no processo de votação pela Internet.

Diante da exposição desses estudos anteriores, pode-se afimar que a verificabilidade de ponta a ponta em eleições eletrônicas é um campo de estudo ainda emergente com o objetivo de tornar qualquer processo de votação eletrônica mais transparente para a sociedade.

Notadamente há dois pontos críticos que a maioria dos trabalhos em verificabilidade *E2E* não abordam que são os riscos de segurança das informações em eleições eletrônicas e o comprovante do voto na posse do eleitor.

É importante dizer que a segurança de dados é composta por processos, pessoas e tecnologias. Por mais que a questão da segurança eletrônica em *e-election* seja um tema que coloca à prova o sistema político e democrático de um país é essencial que isto seja enriquecido com mais pesquisas científicas, pois os protocolos de autenticação e criptografia computacional não fornecem "garantias eternas" para qualquer sistema de votação eletrônica.

Em matéria de auditoria, o recibo de contra-prova do voto em poder do eleitor é um dilema no processo democrático, pois o comprovante é a forma do eleitor auditar o seu voto, mas também é um meio de provar para o corruptor que a cédula eletrônica ou cédula em papel está com voto acordado ou coercitivo entre as partes.

O modelo de verificação *E2E* estoniano aduz que não fornece recibo do voto para o eleitor com base na recomendação de n° 51 do *Committee of Ministers of the Council of Europe* (2005). Todavia, o eleitor pode simplesmente fazer uma captura da tela *(screen shot)* do telefone celular para guardá-lo como comprovante do voto ou ter inconscientemente um *malware* no seu *laptop* ou celular visualizando todas as informações do voto.

Por isso, em que pese as diversas abordagens com tecnologias próprias ou com a *blockchain*, é possível notar o ineditismo que a tese traz para a comunidade científica ao abordar

uma forma de incluir a tecnologia *blockchain* para potencializar a confiança no modelo estoniano de *i-voting.*

2.2.6 Tecnologia Blockchain e Distributed Ledger Technology (DLT)

A tecnologia *blockchain* é formada por conceitos já existentes na criptografia computacional como, por exemplo, a função *hash* criptográfica ou *cryptographic hash function* e o *smart contract* ou contrato inteligente – também conhecido como *chaincode*, que são estudados desde os anos noventa por Bayer, Haber e Stornetta (1993) e Szabo (1996;1997).

Em 2008, o estudioso Satoshi Nakamoto[28] introduz uma visão moderna de implementar uma espécie de dinheiro ou moeda eletrônica chamada de *Bitcoin (token)* em um tipo denominado de *public permissionless blockchain,* que funciona através de um protocolo de consenso – *Proof of Work (PoW)* ou Prova de Trabalho, entre todos os participantes ou "nós de rede" *(nodes* ou *miners)* para validar cada transação. Isto faz com que um usuário não transacione o mesmo valor monetário em moeda eletrônica por mais de uma vez para garantir a integridade, a transparência e evitar o termo intitulado de "gasto duplo".

O renomado especialista em criptografia computacional, Bruce Schneier aduz que:

> Ao analisar o tipo público, pode-se observar que são três elementos essenciais que compõem a estrutura de dados e os protocolos. O primeiro elemento é o *ledger*, que realiza a mesma cópia para todos os *nodes* como uma forma de registrar o fato e a ordem dos acontecimentos, mas que na verdade é também uma rede centralizada dentro das suas próprias regras. A não permissão pública *(public permissionless)* do *ledger* faz com que qualquer usuário possa lê-lo, mas também o torna imutável – o maior atrativo da tecnologia. O segundo recurso é o algoritmo de consenso que contribui para garantir que as cópias do *ledger* sejam idênticas para todos. Para isso ocorrer, há o processo de mineração que, além de requer um poder computacional acima do comum para mantê-lo (armazenamento de dados e energia elétrica), é um ponto crítico do processo pela "não permissão pública". E, por fim, o terceiro elemento é o *token*. Um tipo de *token* tem valor e pode ser comercializado publicamente entre os usuários, atuando como um tipo de "moeda" para alinhar as regras de incentivo para o processamento da rede. Todas as transações envolvendo esses *tokens* são armazenadas no *ledger* (SCHNEIER, 2019, p. 01).

No decorrer dos anos a tecnologia *blockchain* é impulsionada para outros setores de atuação no comércio e administração pública, pois se torna bastante atrativo um sistema ou aplicação que forneça a integridade, a transparência e a imutabilidade de dados em rede distribuída pela Internet – *Distributed Ledger Technology (DLT)*, com o objetivo de inibir

[28] Pseudônimo.

fraudes em produtos ou serviços. Consequentemente, a *blockchain* e *DLT* culminam-se em um tipo de panaceia para sistemas de registros de dados para a Internet.

A autora Melaine Swan retrata esse cenário ao afirmar que a tecnologia passa por dois momentos importantes. O primeiro é a "*blockchain* 1.0" que diz respeito a descentralização do sistema monetário. A segunda parte ela chama de "*blockchain* 2.0", pois está relacionada com a descentralização dos demais produtos e serviços.

> A tecnologia contempla a transferência de muitos outros tipos de ativos que vão além da moeda, por exemplo, a) no âmbito geral: transações judiciais, contratos aduaneiros, arbitragem de terceiros, operações de assinatura multipartidárias; b) transações financeiras: mercado financeiro, crowdfunding, fundos mútuos, derivados, anuidades e pensões; c) registros públicos: propriedades móveis em geral, veículos, licenças de negócios, certidões de casamentos e atestados de óbito; d) identificação: carteira de motorista, carteira de identificação, passaportes e registros de eleitor; e) registros privados: cargas, contratos, apostas e assinaturas; f) atestados: seguros, prova depropriedade, documentos com firma reconhecida; g) chaves de ativos físicos: casas, quartos de hotel, aluguel de carros e acesso ao automóvel; h) intangíveis: patentes, marcas, direitos autorais e reservas (SWAN, 2015, pp. 12 e 43).

Independente do *buzzword* que a *blockchain* e *DLT* exercem até os dias atuais, a pesquisa aborda os aspectos gerais das tecnologias com base nos trabalhos de (NAKAMOTO, 2008); (XU, WEBER, STAPLE, ZHU, BOSCH, BASS e PAUTASSO, 2017); (PAUTASSO, ZHU, GRAMOLI, PONOMAREV, TRAN e CHEN, 2016); (YAGA, MELL, ROBY e SCARFONE, 2018); (ZHENG, XIE, DAI, CHEN e WANG, 2018); (YLI-HUUMO, KO, CHOI, PARK e SMOLANDER, 2016); PILKINGTON (2016); (NOWIŃSKI e KOZMA, 2017); (GATTESCHI, LAMBERTI e DEMARTINI, 2018); (BUTERIN, 2013); (ETHEREUM, 2019); (SOLIDITY, 2017); (MONERO, 2019); (SOVRIN NETWORK, 2020); (BERÉS, SERES, BENCZÚR e QUINTYNE-COLLINS, 2020); (ANDOLA, GAHLOT, GOGOL e VENKATEASEN, 2019) para discutir e entender o seu processo de transformação em relação à: a) Infraestrutura de rede; b) Componentes da *blockchain*; c) Camadas da arquitetura; d) Diferenças entre protocolos de consenso; e) Tipos de tecnologias da *blockchain*; f) Vantagens entre as tipologias; g) Desvantagens entre as tipologias; h) Plataformas *blockchain*; e i) Algoritmos em tecnologia *blockchain*.

Na Tabela 1 são apresentadas as diferenças entre sistema centralizado, descentralizado e distribuído. Conclui-se que a infraestrutura de rede da tecnologia *blockchain* é distribuída, *peer-to-peer (P2P),* com descentralização do *ledger* entre os participantes da plataforma.

Tabela 1: Infraestrutura de rede da tecnologia blockchain

INFRAESTRUTURA DE REDE BLOCKCHAIN	
Centralized system	• Sistema é controlado por uma organização ou usuário. • Servidor, *ledger* e etc., estão no mesmo local físico.
Descentralized system	• Controle do sistema é compartilhado entre entidades independentes. • Servidor, *ledger* e etc., não estão no mesmo local físico.
Centralized ledger	• Não há regra de consenso. • Sem restrição para operações no banco de dados. • Amazenamento de dados centralizado. • Autoridade central. • *Backup* e outros meios de proteção de dados.
Distributed ledger	• Há protocolo de consenso. • Há restrições para operações no banco de dados - *ledger*. • É uma rede distribuída – *peer-to-peer (P2P).* • Autoridade descentralizada e resiliente. • Autenticação com autorização criptográfica computacional. • Imutabilidade dos dados adicionados em cada bloco do *ledger*. • Interação direta dos *nodes* com ativos digitais através do *smart contract.*

Fonte: Elaborado pelo autor

Na Tabela 2 são apresentadas as tecnologias que compõem o funcionamento da tecnologia *blockchain*.

Tabela 2: Componentes da tecnologia blockchain

COMPONENTES DA BLOCKCHAIN	
Ledger	• É um banco de dados distribuído que registra as transações de forma imutável. Como é um tipo de *DLT*, a *blockchain* garante a imutabilidade do histórico de transações – inclusive códigos-fonte, do início (bloco gênese) ao final (bloco atual).
Peer-to-peer network (P2P), node e miner	• É uma rede de computadores formada por "nós de rede" *(nodes)* que compartilham o "processamento de borda" ou *edge computing* na Internet para manter ativo o *ledger*. *Miners* são *nodes* que também operam (ou competem entre si) para descobrir o *hash* criptográfico correto e validar um *block* na cadeia de blocos.
Smart contract ou chaincode	• São códigos imutáveis que são executados na camada de aplicação em rede *blockchain.*
Consensus protocol	• O protocolo de consenso é um algoritmo que governa o núcleo de existência da plataforma *blockchain* para validar e ordenar todos os blocos no *ledger*. Existem cinco tipos: *Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Elapse Time (PoET), Practical Bizantyne Fault Tolerance (PBFT).* Todos são discutidos na Tabela 4.
Membership service	• É uma função que dispõe de autenticação e autorização (identidade e segurança) para garantir a participação dos usuários em rede *blockchain.*
Event	• É uma função sistêmica importante na geração de eventos na *blockchain* ou *DLT,* pois permite que aplicativos ou sistemas interajam com a plataforma.

Fonte: Elaborado pelo autor

Na Tabela 3 são apresentadas as camadas lógicas *(software)* e físicas *(hardware)* que compõem a estrutura de uma plataforma em *blockchain*. Os mecanismos de consenso são explicados na Tabela 4.

Tabela 3: Camadas da arquitetura blockchain

CAMADAS DA ARQUITETURA BLOCKCHAIN	
Application* e *presentation layer	• *Smart contract, chaincode, decentralized applications (DApps) e user interface*
Consensus Layer	• *Pow, PoS, DPoS, PoET* e *PBFT*
Network layer	• *P2P*
Data structure layer	• *Digital signature, hash, merkel tree e transaction*
Infrastructure layer	• *Virtual machine, containers, services e messaging*

Fonte: Elaborado pelo autor

Na Tabela 4 são apresentados os protocolos de consenso. Nota-se que os mecanismos de consenso *PoW, PoS* e *DPoS* são tecnicamente mais próximos do conceito do protocolo de consenso da *blockchain* de Satoshi Nakamoto, enquanto os demais são derivações criadas para atender determinados tipos de produtos ou serviços.

Tabela 4: Diferença entre PoW, PoS, DPoS, PoET e PBFT

DIFERENÇAS ENTRE PROTOCOLOS DE CONSENSO	
Proof of Work (PoW)	• *PoW* é o protocolo de consenso original da *blockchain* de Satoshi Nakamoto (2008) que executa a governança do registro de dados e, em especial, evitar o "gasto duplo" da criptomoeda ou *criptocurrency*. • Os mineradores competem entre si para validar o código *hash*. Ato contínuo, o *miner* "vencedor" distribui para os *nodes* que, posteriormente, é adicionado ao *ledger*. O primeiro *miner* que encontrar o *hash* recebe a recompensa pela "mineração" dos dados – criptomoeda ou *"token" (Biticoin)*. • A dificuldade do "quebra-cabeça" para validar a função *hash* é dinâmica, ou seja, torna-se mais difícil durante o dimensionamento do *ledger*. • É necessário poder computacional para vencer a "batalha" entre os *miners*. Com isso, o processamento é oneroso (energia elétrica), pois um *miner* pode construir um laboratório de computadores com Circuitos Integrados de Aplicação Específica ou *Application Specific Integrated Circuits (ASICs)* para "minerar" um volume de funções *hash* bastante significativo em face dos demais *miners* que atuam apenas com um microcomputador. • A escalabilidade é baixa em vista do consumo de energia computacional e a distribuição do *ledger* para cada *node*. • Possui dificuldade alta contra os ataques de *Denial of Service (DoS)*. • Um *node* ou grupo de *nodes* com maior número de blocos vinculados ao *ledger* se tornam "mais confiáveis" do que outros usuários da rede *blockchain*. Isto pode ser uma desvantagem para a plataforma *blockchain* porque, segundo Satoshi Nakamoto, há a possibilidade de um cenário em que 51% dos *nodes* ou *miners* podem validar funções *hash* para alterar o conteúdo de um ou mais blocos já validados pela rede *blockchain*. O que pode ocasionar em fraude e a mutabilidade do sistema.

Proof of Stake (PoS)	• O *PoS* ou Prova de Participação é uma alternativa ao protocolo *PoW* que foi criado pela plataforma de criptomoeda *Peercoin* (2011). • A probabilidade de "mineração" depende do número de *tokens* ou moedas eletrônicas que um *node* ou *miner* possui que dita a influência dele na rede, por exemplo, um usuário com 15% da participação na rede *blockchain* tem 15% de probabilidade de "minerar" o próximo bloco para validar a função *hash* do que os seus concorrentes. • A vantagem é o baixo consumo de poder computacional e a defesa em relação à *DoS*. • A desvantagem é a hipótese dos 51% que podem concentrar o poder de consenso da rede *blockchain.*
Delegated Proof of Stake (DPoS)	• É um algoritmo *PoS* usado na rede *blockchain* para alcançar um consenso distribuído, que com base na quantidade de suas moedas eletrônicas, tem poder de voto (influência) para delegar *nodes* ou grupos para alcançar consenso na validação de blocos. É uma maneira de "forjar" blocos em vez de minerá-los.
Proof of Elapsed Time (PoET)	• É um algoritmo de mecanismo de consenso com baixa utilização de recursos e consumo de energia. • Mantém o consenso mais eficiente, seguindo um sistema de "loteria justo" com base no menor tempo de espera aleatório para cada usuário. • Criado pela *Intel* em 2016 para se adequar à *permissoned blockchain*. • O *PoET* é econômico e oferece oportunidades iguais para todos os participantes. No entanto, não é adequado para redes *blockchain* públicas sem permissão. • A desvantagem é a vulnerabilidade encontrada capaz de comprometer a confiabilidade de uma fração significativa de *nodes* (CHEN, XU, GAO e SHI, 2017).
Practical Byzantine Fault Tolerance (BFT)	• Na criptografia computacional, o termo vem do "problema dos generais bizantinos" que é desenvolvido para descrever uma circunstância em que os atores devem concordar na estratégia de ter vários "nós de consenso" para evitar a catastrófica falha do sistema por *nodes* influenciadores e maliciosos (menos de um terço do total). • A plataforma *Hyperledger Fabric* uso o *BFT* como protocolo de consenso.

Fonte: Elaborado pelo autor

Na tabela 5 são apresentados os tipos de tecnologias em *blockchain* que configuram modalidades específicas para produtos ou serviços.

É importante mencionar que a *public permissionless blockchain* é a tipologia original do conceito da *blockhain* de Satoshi Nakamoto, enquanto que os demais tipos são derivações da tecnologia para fins específicos e comerciais.

Tabela 5: Tipos de tecnologias blockchain

TIPOS DE TECNOLOGIAS BLOCKCHAIN	
Public Permissionless Blockchain	• A *blockchain* sem permissão pública é quando um usuário anônimo tem permissão para ler *(read),* escrever *(write)* e validar *(commit)* as transações realizadas no *ledger* para torná-las visíveis na rede *blockchain*. Uma cópia do *ledger* é compartilhada entre os *nodes* ou *miners* da rede distribuída –

	distributed ledger technology (dlt). Isto faz com que todos tenham acesso ao "livro-razão" na "cadeia de blocos". • Acesso público e descentralizado. • Utiliza o protocolo de consenso *PoW*. • O banco de dados é imutável, isto é, a transação vinculada ao *ledger* não pode ser alterada. Isto quer dizer que o mesmo *node* terá blocos anexados à rede *blockchain* sobre o mesmo assunto para caracterizar a imutabilidade dos dados. No caso de alteração, o consenso entre os *nodes* garante a integridade da informação nova em outro bloco que será anexado ao *ledger*. • Baixa escalabilidade para o número de participantes.
Public Permissioned Blockchain	• A *blockchain* com permissão pública é quando um usuário anônimo tem permissão para ler *(read)* as transações na *blockchain*, mas somente participantes autorizados tem permissão para escrever *(write)* e validar *(commit)* as transações realizadas para torná-las visíveis no *ledger*. • É possível que essa condição de permissão pública seja realizada de maneira oposta, por exemplo, os *nodes* autorizados apenas tem permissão para ler cada transação, enquanto que qualquer *node* pode escrever e validar cada transação na rede *blockchain*. • Acesso público e descentralização controlada. • Utiliza o protocolo de consenso *PoS* que permite a escalabilidade de alta performance em relação ao *PoW*. • A validação pode ser escalonada individualmente ou em grupo de *nodes* ou *miners* autorizados. • É mais vantajodo que o tipo *public permissionless*.
Private Permissionless Blockchain	• A *blockchain* sem permissão privada é realiza dentro de uma infraestrutura de *P2P,* mas todas as permissões são centralizadas. Logo, a descentralização não é o fator preponderante neste tipo de *blockchain*. • Todos os usuários podem ler *(read)*, mas somente os *nodes* escolhidos podem escrever *(write)* e validar *(commit)* transações. • Acesso restrito. • Utiliza o protocolo *PBFT*. • São adotados principalmente por empresas que desejam explorar o termo *blockchain* dentro da empresa.
Private Permissioned Blockchain	• A *blockchain* com permissão privada é uma alternativa para o setor empresarial que opta em rede *blockchain* com maior desempenho. Para isso, as empresas preferem um *node* execute apenas cálculos necessários para determinadas aplicações. • Os usuários deve ser identificáveis, e não apenas "confiáveis" com o anonimato, para que as permissões sejam concedidas – grupo de consórcio. • Acesso privado e restrito. • Utiliza o protocolo *PBFT*. • A escalabilidade é bastante alta. • Custo abaixo em relação aos demais tipos de *blockchain*.

Fonte: Elaborado pelo autor

Na Tabela 6 são listadas as vantagens em utilizar cada tipo de *blockchain.*

Tabela 6: Vantagens das tipologias blockchain

VANTAGENS DAS TIPOLOGIAS BLOCKCHAIN	
Public Permissionless	• Execução de aplicativos descentralizados – *dApps.* • Não há necessidade de intermediário. • A rede é pública e transparente. • Oferece o anonimato. • A rede é imutável.
Public Permissioned	• Execução de aplicativos descentralizados – *dApps.* • Não há necessidade de intermediário. • Escalável. • Processamento rápido. • A rede é imutável. • Custo baixo da infraestrutura para a transação.
Private Permissionless	• Identidade do *node* é privada e conhecida entre os participantes. • Centralização de dados. • Simplificação de documentos. • Redundância menor de dados. • Rede finita de dados. • Bastante escalável. • Permite a mutabilidade. • *Compliance* interno. • Redução de custos das transações.
Private Permissioned	• Participantes dos *nodes* são pré-definidos em "consórcio". • Identidade do *node* é privada e conhecida entre os participantes. • Privacidade de dados é alta. • Segurança das informações é alta. • Centralização de dados. • Documentação simplificada. • Redundância menor de dados. • Rede finita de dados. • Altamente escalável. • Permite a mutabilidade. • *Compliance* interno. • Redução de custos das transações.

Fonte: Elaborado pelo autor

Na Tabela 7 são listadas as desvantagens em utilizar cada tipo de *blockchain.*

Tabela 7: Desvantagens das tipologias blockchain

DESVANTAGENS DAS TIPOLOGIAS BLOCKCHAIN	
Public Permissionless	• Escalabilidade: há limitação no número de transações que podem ser realizadas (NAKAMOTO, 2008). • Performance baixa e custo alto: a) é necessário alto poder de processamento, tornando a rede lenta e muito onerosa por causa do armazenamento de dados, energia elétrica e *edge computing,* para o consenso ser alcançado pelos *nodes* ou *miners* quando executam o *smart contract* ou validam as transações no

	ledger,; b) o número de transações na rede é proporcional ao números de *nodes* ou *miners.* • Identidade anônima: risco favorável para agentes maliciosos. • Desafio da imutabilidade: muito embora a imutabilidade de transações e blocos sejam a principal característica do *blockchain* público, a imutabilidade do código (contrato inteligente) é um desafio para a rede *blockchain*. A *blockchain* considera a implantação de contrato inteligente como uma transação e, como são transações, são imutáveis. Portanto, qualquer *bug* ou problema ou um *loop* de código não pode ser alterado ou corrigido. Isso significa que, contratos inteligentes precisam ser meticulosamente construídos e testados antes de serem implantados e devem ter operações de comando *KILL* (encerramento de um processo - *shutdown*). • Concentração de poder e vulnerabilidade na segurança de dados: para obter os benefícios de *tokens* (moedas eletrônicas) da *blockchain* pública, os *nodes* operam como "nós de rede" completos. Um "nó de rede" completo significa que os *nodes* carregam uma cópia completa do *ledger*. A medida que a rede *blockchain* cresce em volume de dados, torna-se caro para usuários menores e *nodes* individuais operar como "nós de rede" completos. Apenas usuário com maior poder de processamento pode operar como "nós de rede" completo. O cenário pode levar à centralização da rede e, consequentemente, influenciar a rede *blockchain* para ocorrer a hipótese dos 51% de ataque à rede.
Public Permissioned	• Identidade anônima: risco favorável para agentes maliciosos. • Desafio da imutabilidade: idem ao *public permissionless.* • Concentração de poder e vulnerabilidade da segurança: idem ao *public permissionless.*
Private Permissionless	• Não é descentralizada. • Pode ser distribuída – *P2P.* • Identidade é transparente.
Private Permissioned	• Não é descentralizada. • Não é distribuída – *P2P.* • Identidade é transparente. • A formação de um "consórcio" é um desafio porque as empresas necessitam ter negócios semelhantes com problemas idênticos, por exemplo, as instituições financeiras.

Fonte: Elaborado pelo autor

Na Tabela 8 são apresentadas as diferenças entre as plataformas *Ethereum, Hyperledger Fabric* e *Sovrin Network* que adotam tipologias específicas para atender algum produto ou serviço em rede *blockchain.*

Tabela 8: Plataformas blockchain

PLATAFORMAS BLOCKCHAIN	
Ethereum	• É uma extensão do conceito da *blockchain* de Satoshi Nakamoto. • Plataforma de código aberto. • É uma *blockchain* pública. • Participantes podem acessar o *ledger.* • É baseada em contratos inteligentes.

	• Os desenvolvedores podem elaborar aplicativos descentralizados por meio de contratos inteligentes e organizações autônomas descentralizadas ou *Descentralized Autonomous Organzation (DAO)*. • É uma plataforma genérica e as transações são validadas pelo consenso de *PoW*. • É usado para aplicativos *business-to-consumer (B2C)*. • Desenvolvido na linguagem de programação *Solidity*. • Possui moeda eletrônica chamada de *Ether*. • Privacidade e a escalabilidade possuem desempenhos insatisfatórios. • A vulnerabilidade e falha na plataforma são discutidas em (BERÉS, SERES, BENCZÚR e QUINTYNE-COLLINS, 2020).
Hyperledger Fabric	• É uma plataforma *blockchain* privada para aplicativos corporativos. • Plataforma é de código aberto. • Utiliza protocolo de consenso *PBFT*. • Não possui um mecanismo de consenso *blockchain*. • *Ledger* não é público. • É usado para aplicativos *Business to Business (B2B)*. • *Chaincode* (contrato inteligente) pode ser escrito em linguagens de programação *Java Script, Go* e *Node.js*. • Não possui moeda eletrônica. • Privacidade e a escalabilidade possuem performance altas. • A vulnerabilidade e falha na plataforma são discutidas em (ANDOLA, GAHLOT, GOGOL e VENKATEASEN, 2019).
Sovrin Network	• É uma plataforma *public* e *private permissioned blockchain* para *Decentralized Identifiers (DiDs)*. • Plataforma é de código aberto. • A base do código-fonte é *Hyperledger Fabric.* • Utiliza protocolo de consenso *PBFT*. • Utiliza um tipo próprio de "*Sovrin" ledger (on-ledger* e *off-ledger).* • Não possui um mecanismo de consenso *blockchain*.

Fonte: Elaborado pelo autor

Na Tabela 9 são apresentados os algoritmos em criptomoedas e suas respectivas plataformas em *blockchain.*

Tabela 9: Algoritmos blockchain e DLT

ALGORITMOS BLOCKCHAIN E DLT	
Bitcoin	• É utilizado na *public permissionless* ou *permissioned blockchain.* • Utiliza linguagem de progração C++ ou *Python.* • É utilizado nas plataformas *Ethereum* e *Litecoin.*
Solidity	• É utilizado na *private permissionless* ou *permissioned blockchain.* • É uma linguagem de programação orientada a objetos para escrever contratos inteligentes *(smart contract* ou *chaincode)*. • Utiliza linguagem de progração *C++, Java Script, Go* e *Node.js*. • É projetada para operar com *Ethereum Virtual Machine (EVM).* • É utilizado nas plataformas *Hyperledger Fabric, R3* e *Corda.*
Monero	• É utilizado na *public permissionless* ou *permissioned blockchain.* • É uma criptomeda com base conceitual na *Bitcoin,* porém com diferenças singulares.

	• A tecnologia *Monero* utiliza diferentes tecnologias de privacidade para ofuscar as informações e proteger o anonimato dos usuários: a) assinaturas em anel (ocultar o remetente da transação); b) endereços *stealth* (ocultar o destinatário); c) *Ring Confidential Transactions (RingCT)* (ocultar o conteúdo do *ledger*); e d) rede de anonimato em *Invisible Internet Project* (*I2P)* ou *The Onio Router (Tor*). • O tamanho do bloco no protocolo *Monero* é dinâmico, ou seja, adapta-se de forma automática de acordo com o número de transações na rede, sendo que o tempo médio de mineração gira em torno de dois minutos para validar o protocolo de consenso na cadeia de blocos. • O algoritmo de mineração é denominado de *Random X* que possui o mesmo conceito do *PoW* de Satoshi Nakamoto (2008), mas é desenhado para evitar as "fazendas de minerações" ou *farms* que utilizam de computação customizada em Circuitos Integrados de Aplicação Específica e obter um melhor desempenho durante as transações. • Utiliza a linguagem de programação *C++*. • É utilizado na plataforma *Monero (XMR)*.

Fonte: Elaborado pelo autor

2.2.7 Por que a Pesquisa opta pela Tecnologia Blockchain?

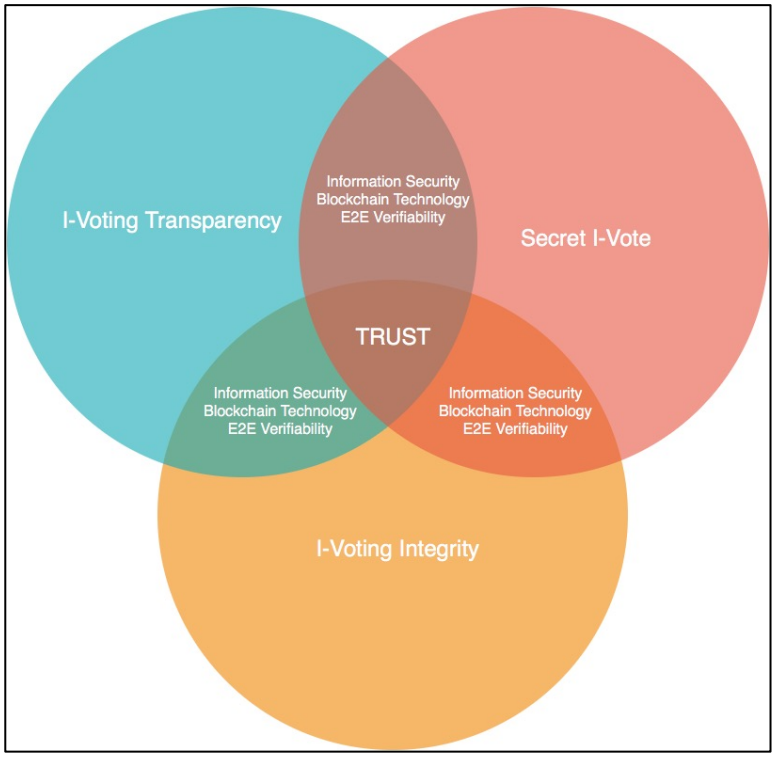
Segundo os estudos anteriores, a maioria das tecnologias para sistemas de votação envolvem algoritmos de criptografia de chave privada, chave pública ou função *hash* para garantir o sigilo e a integridade da cédula eletrônica, sendo comum o uso de protocolos de criptografia em diversas camadas de segurança para sistemas com *softwares* embarcados para dificultar o acesso de agentes não autorizados.

Consequentemente, a transparência em eleições eletrônicas é ofuscada pela dificuldade das pessoas de compreender a linguagem computacional utilizadas para garantir o sigilo e a integridade na votação pela Internet. Por exemplo, após o resultado oficial das eleições eletrônicas o órgão responsável torna público uma lista com *hash code* ou arquivos de *log* ou parte do código fonte do sistema de votação que, na maioria dos casos, é disponibilizado em plataforma *web* - *open source.*

Por outro lado, a pesquisa observa que não há argumentos científicos que comprovem a adoção de único algoritmo criptográfico que seja altamente eficiente em eleições.

Deste ponto em diante a transparência se torna o ponto central do dilema em sistemas de *i-voting* para consubstanciar o sigilo e a integridade do voto nas eleições. A transparência ajuda a fortalecer, gradativamente, os laços de confiança na instituição, na tecnologia e nas pessoas em processos eleitorais. Neste caso, a aplicação da verificabilidade *E2E* é o principal instrumento para a realização desse processo para a votação pela Internet na Estônia.

Figura 1: Dilema da confiança em i-voting



Fonte: Elaborado pelo autor

A resposta da pesquisa é corroborada por Bruce Schneier (2019), especialista em segurança da informação e crítico da tecnologia *blockchain*, que entende que a tecnologia pode ser parte da confiança que a tese busca com a aplicação de verificação de ponta a ponta para o sistema de votação pela Internet da Estônia.

De acordo com o especialista:

> Ao analisar a confiança e segurança, no meu livro *Liars and Outliers,* eu listei quatro sistemas generalistas de incentivos da confiabilidade para o comportamento humano. Os dois primeiros são a moral e a reputação, sendo que são mais eficientes para determinadas escalas populacionais. O terceiro são as instituições que com base nas regras (direitos, deveres e sanções) ditam o comportamento humano no seu convívio. E o quarto são os sistemas de segurança que, enumerados, são desde fechaduras, alarmes e sistemas de auditoria *forense* e etc. Todos os quatro elementos trabalham juntos para construir a confiança, por exemplo, sistema financeiro, comercial e até o próprio indivíduo, que inclui sistema de segurança para Internet e etc. Já Kevin Werbach descreve quatro "arquiteturas de confiança" diferentes. A primeira é a confiança de ponto a ponto, o que remete ao aspecto da reputação. A segunda é a confiança leviatã vinculada a confiança institucional. A terceira é confiança intermediária, ou seja, uma forma técnica que proteje o elo de confiança entre as partes. E a quarta arquitetura é a confiança distribuída, que podemos associá-la ao emergente sistema de segurança em *blockchain.* O que o *blockchain* faz é transferir parte da confiança das pessoas e das instituições para confiar na tecnologia. A partir daqui é desenvolvido um cenário de credibilidade na confiança,

> pois quando a tecnologia aplicada é falha, as vezes não há recurso. Assim, confiar na tecnologia é mais difícil do que confiar nas pessoas. O *blockchain* não elimina a necessidade de confiar em instituições e seres humanos, pois sempre haverá uma grande lacuna que não pode ser resolvida apenas pela tecnologia. Qualquer sistema *blockchain* terá que coexistir com outros sistemas mais convencionais (SCHNEIER, 2019, pp. 02-03).

É importante entender que a corrupção – fato gerador da fraude eleitoral, é uma questão social. Neste sentido, o desafio é empreender qualquer tecnologia computacional para impedir a ação do ser humano de acometer infrações contra o processo democrático, especialmente, em eleições eletrônicas pela Internet.

Assim, a pesquisa entende que há óbices e dubiedades com o sistema de votação pela Internet na Estônia. Contudo, a pesquisa acredita que com a tecnologia *blockhain* pode propor uma aplicação independente ao sistema de *i-voting* para resolver, particularmente, as hipóteses apresentadas na Introdução (seção 1.3).

3. METODOLOGIA

"Os métodos são regras precisas e fáceis, a partir da obervação exata da qual se terá certeza de nunca tomar um erro por uma verdade e sem desperdiçar inutilmente as forças de sua mente, mas ampliando seu saber por meio de um contínuo progresso para chegar ao conhecimento verdadeiro de tudo do que se é capaz"
René Descartes

A metodologia proposta consiste na pesquisa ampla e dirigida sobre *e-voting* e, consequentemente, *i-voting* e a tecnologia *blockchain* no campo experimental, teórico e prático, do cenário internacional para encontrar uma evidência factível para a hipótese do trabalho.

Deste modo, não é possível realizar a investigação sem um paradigma que corrobore com as arguições da pesquisa. Logo, a escolha de um cenário propício se fez mais do que necessário para conduzir e fornecer informações suficientes para o resultado final da tese.

O requisito para escolher o paradigma é o grau de experiência no sistema de votação pela Internet dentro do contexto da democracia eletrônica no processo eleitoral. E, com isso, mensurar a existência de prognósticos efetivos de pleitos eleitorais no âmbito tecnológico, sócio-político, regulatório e cultural.

Segundo Vinkel e Krimmer (2016, p. 186) a implementação de um sistema de *i-voting* nos últimos anos tem sido bastante ativa no cenário internacional, constatando-se por volta de vinte países ou mais que adotaram o sistema de votação pela Internet em determinada etapa do seu pleito eleitoral, sendo que há outras nações que ainda analizam a possibilidade de implementá-lo.

3.1 DELIMITAÇÃO DA PESQUISA

A delimitação do paradigma é construída a partir da análise de três países, a Confederação Suíça, a República da Estônia e o Reino da Noruega.

As experiências da Estônia, Suiça e Noruega tem maior destaque por serem os casos mais consolidados e evidentes dentre todas as nações que já tentaram em algum momento o *modus operandi* da Internet para o processo eleitoral, independentemente da particularidade cultural, econômica, geográfica e sociopolítica.

> **Estônia.** Na Estônia, desde a sua implementação em 2002 até a primeira eleição na cidade de Talín no ano de 2005, houve um aumento constante no uso do sistema de *i-voting* até as eleições gerais de 2011 - ano em que o modelo pela Internet se tornou mais popular do que o tradicional voto em papel. A Estônia é a única nação que

> realizou eleições locais em 2005, 2009 e 2013; eleições nacionais nos anos de 2007, 2011 e 2015; e eleições para o Conselho do Parlamento Europeu em 2009, 2011 e 2014. Além disso, as características sociodemográficas na determinação do uso do sistema de *i-voting* têm desaparecido desde que o desafio de atingir 100.000 eleitores foi conquistado em 2009. Há dois pontos importantes que devem ser ressaltados, a confiança no sistema pela sociedade estoniana e a neutralidade política do sistema que não produz resultados tendenciosos nas eleições.
>
> **Suiça.** A Suíça é uma Confederação[29] que utiliza eleições *on-line* nos cantões. Com o voto postal sendo um favorito de longa data em um país onde as eleições e os referendos são realizados frequentemente, logo, o passo seguinte para soluções *on-line* não foi uma surpresa. Diferentes cantões tiveram pilotos e testes desde o início dos anos 2000. Atualmente, duas diferentes tecnologias de sistemas de votação estão em uso, e menos de dez cantões suíços usam *i-voting system* em algum nível de atividade eleitoral (até 2015 costumava haver três soluções diferentes com mais da metade dos cantões participando do *i-voting*). A identificação do eleitor no sistema de *i-voting* é baseada em senhas exclusivas através do sistema postal e é oferecida também uma verificação individual do voto. Desde 2008, a votação *on-line* pela Internet também é oferecida para expatriados suíços. Semelhante à Estônia, os suíços alcançaram uma experiência de usuário estável no início da década de 2010, e hoje buscam possibilidades de aprimorar seus (diferentes) sistemas para torná-los mais transparentes, observáveis (pelas agências internacionais) e auditáveis[30].
>
> **Noruega.** A Noruega iniciou o seu projeto de *i-voting* com dois pilotos, o primeiro nas eleições locais de 2011 e o segundo nas eleições gerais de 2013. Ambos os pilotos foram realizados em um pequeno número de unidades do governo local. A Noruega implementou o sistema após rigorosa análise constitucional e uma minuciosa pesquisa internacional. Desde o início, a verificabilidade de conversão foi implementada e um esforço grande foi implantado para garantir a confiança do público com as soluções de segurança mais recentes para o sistema. Tanto tecnicamente, quanto da perspectiva pública, ambos os pilotos foram percebidos como bem-sucedidos. No entanto, após alguma avaliação, o governo norueguês decidiu descontinuar os pilotos de *i-voting system* devido aos possíveis riscos na segurança do sistema, as subjacentes mudanças na liderança política e a falta de confiança que os políticos depositam no sistema[31] (VINKEL e KRIMMER, 2016, pp. 186-187 com grifo nosso).

A análise dos estudiosos trouxe com clareza que a Estônia é o paradigma mais apropriado e conveniente para a proposta da investigação científica em razão da escalabilidade e experiência adquirida no decorrer dos quinze anos do processo eleitoral com votação pela Internet[32].

---

[29] Composta por vinte e seis cantões ou estados.

[30] Após a definição de um regulamento novo em 2014, o Conselho Federal suíço estabeleceu um grupo de especialistas em *i-voting system* no mês de agosto de 2017 (PUIGGALÍ e RODRÍGUEZ-PÉREZ, 2018, pp. 94 e 95).

[31] A Noruega realizou testes em larga escala de votação *on-line* pela Internet durante as eleições locais de 2011 e as eleições parlamentares de 2013. Em 2016 e 2018, vários municípios e um condado usaram *i-voting system* para referendos locais. No entanto, houveram várias falhas: cartões de votação com impressão incorreta, geradores pseudo-aleatórios defeituosos, e certificados digitais mal configurados (BULL, GJØSTEEN e NORE, 2018, p. 166).

[32] Id. cit. 24

3.2 DELIMITAÇÃO DO PROBLEMA

O problema da pesquisa é dividido em dois estágios:

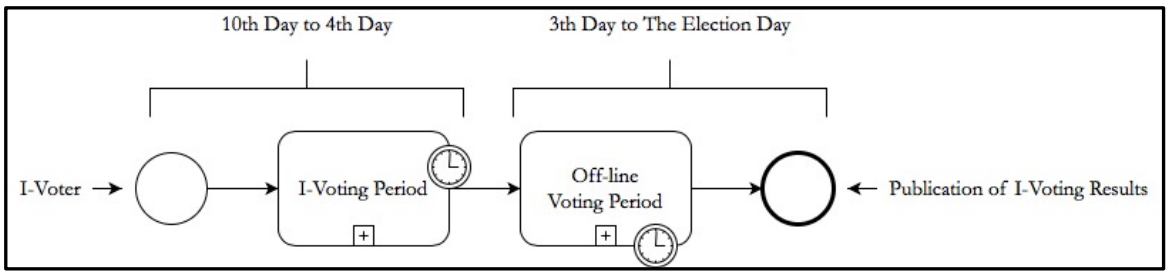
a) Parte das operações no processo de votação pela Internet são realizados em ambiente *off-line;*

b) Aplicação da verificação de ponta a ponta é individual com limitação à consulta no ambiente *on-line.*

3.2.1 Ambiente Off-line de Votação pela Internet

O ambiente *off-line* do sistema de *i-voting* estoniano tem início após o período de votação pela Internet designado por lei (do 10° dia ao 4° dia), que corresponde aos três dias subsequentes "sem eleição" ou *"dark days"* até o dia oficial da eleição (do 3° dia ao dia oficial da eleição)[33].

Figura 2: Ambiente on-line e off-line no sistema de i-voting



Fonte: Elaborado pelo autor

No cenário *off-line* ocorrem os seguintes processos: a) checagem da integridade dos votos eletrônicos correspondentes à assinatura digital e o *time-mark;* b) anonimização das cédulas eletrônicas; c) uso da chave privada nas cédulas eletrônicas; d) gravação dos dados em mídia digital; e) (re)embaralhamento das cédulas eletrônicas; f) contagem; e g) publicação do resultado.

O eleitor não tem mais acesso a sua cédula eletrônica nos processos que são realizados durante as operações em *off-line*. Para a pesquisa, o ambiente *off-line* traz dubiedade ao sistema de *i-voting* porque não atende o princípio da transparência - disciplinado e recomendado pela *OSCE/ODIHR* (2013, pp. 9-12), para os processos de votação pela Internet.

---

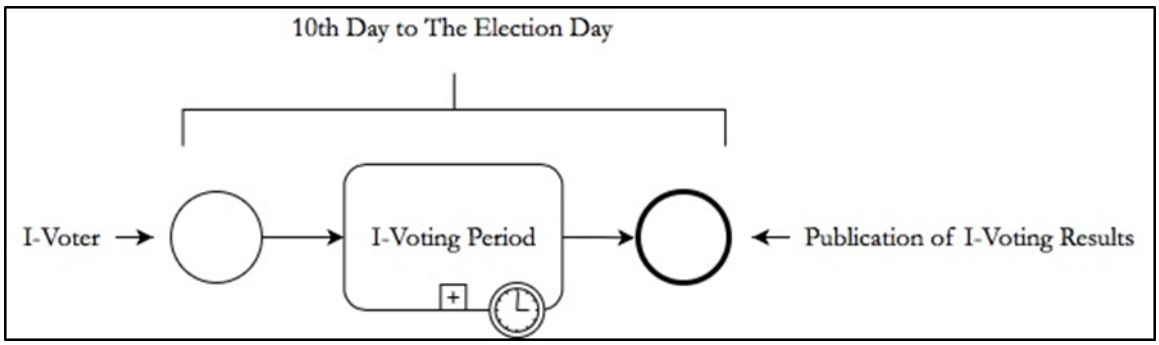
[33] Id. cit. 26.

3.2.2 Solução: Prolongação do Período de Votação

A resolubilidade é eliminar o processo *off-line* do sistema de *i-voting* da Estônia e substituí-lo para um ambiente *on-line*, prologando-se o período de votação, sendo necessário, inclusive, a alteração da lei especial.

É importante enfatizar na pesquisa que a expansão do tempo de votação pela Internet influencia para o maior tempo de processamento para a verificação *E2E*. Neste caso, a investigação entende que, por razões da infraestrutura atual de segurança do sistema de *i-voting*, o eleitor pode ter acesso à sua cédula eletrônica para verificação *E2E* antes do processo de anonimização, criptografia com chave privada e contagem das cédulas eletrônicas.

Figura 3: Extensão do período de votação no sistema de i-voting



Fonte: Elaborado pelo autor

3.2.3 Verificação E2E da Cédula Eletrônica na Base de Dados

Segundo Rabin e Rivest (2014, p. 61), os sistemas de votação com verificação de ponta a ponta fornecem alta confiabilidade para que os erros e as fraudes possam ser detectados e, também, contribuindo para que o resultado da eleição seja anunciado corretamente.

Desde o ano de 2004, protocolos como *visuais cryptography system, Punchscan system, Prêt à Voter system, Helios, Scratch, and Vote System, Three Ballot voting protocol, Scantegrity I e II systems* e *STAR-Vote system* são voltados para verificabilidade de eleições *on-line* (SILVA, 2018, p. 351). Entretanto, até os dias atuais não há um protocolo de criptografia computacional que seja consolidado e específico para sistemas de *i-voting*, salvo a adoção óbvia da base conceitual e técnica a todos eles[34].

[34] *RSA, AES* e etc.

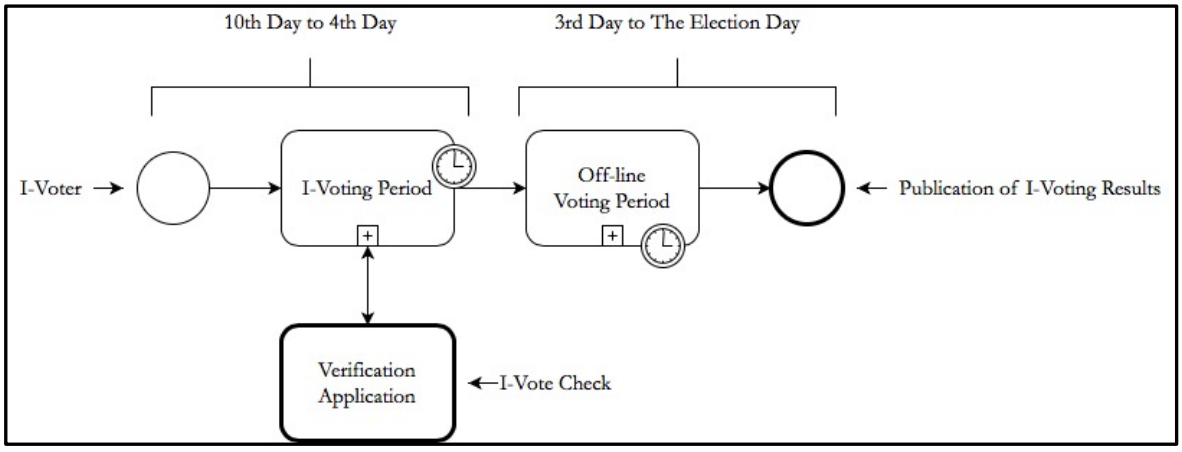
Notadamente, para a pesquisa isso tem um motivo elementar. Segundo o estudioso e empreendedor tecnológico sobre segurança em sistemas digitais de votação, Andreu Riera[35], a criptografia de dados é um dos pilares da segurança no processo eleitoral pela Internet, e não o fator preponderante de todo o sistema.

> *I-Voting system* é uma aplicação distribuída constituída por um conjunto de protocolos e mecanismos criptográficos que juntos permitem que uma votação aconteça inteiramente sobre redes de computadores, de maneira segura, mesmo assumindo que seus legítimos participantes possam ter comportamentos maliciosos (RIERA, 1999, p. 23).

Logo, é um sinal positivo para ampliar a relação de confiança a adoção de tecnologias novas que incluam criptografia computacional como um garantidor em parte do sistema de votação pela Internet estoniano.

No sistema de *i-voting* estoniano, o aplicativo de verificação do armazenamento da cédula eletrônica na base central de dados é explicado no documento *IVXV – ÜK.* Contudo, para a pesquisa o procedimento não é aceitável como uma aplicação de verificação *E2E,* pois ele é de ponta a ponta até certo ponto no ambiente *on-line* - período que corresponde à coleta das cédulas eletrônicas pela Internet.

Figura 4: Período de verificação da cédula eletrônica no sistema de i-voting



Fonte: Elaborado pelo autor

[35] Fundador da *Scytl*, ele foi pioneiro na pesquisa sobre segurança de voto eletrônico, primeiro como pesquisador acadêmico e depois como presidente da empresa de 2001 a 2006. Ele faleceu em 11/03/2016 devido a um acidente de carro na cidade de Manresa, em Barcelona.

Para a investigação acadêmica, a solução para o problema em questão está na tecnologia *blockchain* para potencializar os dilemas do anonimato, integridade e transparência no processo de votação pela Internet na Estônia.

3.2.4 Solução: Tecnologia Blockchain

Apesar da pesquisa já avaliar a possibilidade de utilizar a tecnologia *blockchain* para sistemas de votação pela Internet desde o seu início no ano de 2015, em 2017, Priit Vinkel, *Chancellery of Riigikogu, Secretariat of National Electoral Committee*[36], participou da conferência *re: publica 2017* e confirmou que existe a possibilidade de analisar o uso da tecnologia *blockchain* como parte do sistema de *i-voting* na Estônia, mas durante a sua resposta na conferência, ele não especificou como utilizar a arquitetura *blockchain* no sistema de votação pela Internet (SILVA 2018, p. 352)[37].

Em vista disso, no ano seguinte, os especialistas estonianos Heiberg, Siim, Willemson e Kubjas apresentaram o estudo que, a partir de outras pesquisas, reflete sobre a possibilidade da tecnologia *public permissionless blockchain* em eleições eletrônicas.

> Mesmo sendo muito atraente a perspectiva da integridade eleitoral, o *blockchain* têm inúmeras desvantagens técnicas, econômicas e até políticas que precisam ser levadas em conta. Selecionar um bom *trade-off* entre propriedades desejáveis e restrições impostas por diferentes implementações *blockchain* é uma tarefa altamente não trivial (HEIBERG, SIIM, WILLEMSON e KUBJAS, 2018, p. 259).

Na opinião dos especialistas, a tecnologia *public permissionless blockchain* não é ideial para os sistemas de *e-voting* e *i-voitng* em razão das características tecnológicas do tipo "sem permissão pública".

A pesquisa concorda com os especialistas, mas entende que o importante é que a proposta em torno do tema não careça apenas de encontrar a tecnologia computacional condinzente, mas também buscar criatividade para inovar ou aprimorar modelos teorizados ou experimentais em face dos desafios que a própria tecnologia *blockchain* impõe para o sistema de votação pela Internet.

---

[36] Chancelaria do *Riigikogu*, Secretaria do Comitê Nacional Eleitoral - *Lossi plats 1a, Tallinn, Estonia.*

[37] *re:publica 2017 - Digital Democracy: E-Voting for everyone?* Disponível nos 52 minutos e 28 segundos do vídeo.

Logo, pode-se concluir que a investigação traz determinado ineditismo à proposta para o cenário estoniano de votação pela Internet.

3.3 APLICAÇÃO DA PROPOSTA COM A TECNOLOGIA BLOCKCHAIN

A pesquisa expõe de forma sucinta a maneira como a solução é abordada com a utilização da tecnologia *blockchain* para a verificabilidade de ponta a ponta em parte do sistema de *i-voting* da Estônia.

3.3.1 Tecnologia Blockchain: Arquitetura e Algoritmo

A abordagem da tese manifesta preferência pelas seguintes tecnologias com base na análise de estudos do Capítulo 2:

- *Public permissioned blockchain;*
- Algortimo *Monero.*

Para a pesquisa as duas tecnologias são compatíveis com as hipóteses apresentadas porque as demais arquiteturas em *blockchain* não atendem a proposta pelos seguintes motivos:

- *Public permissionless blockchain*: baixa performance de desempenho por causa do tempo excessivo de distribuição do *ledger* completo para todos os *nodes*; a escalabilidade é bastante limitada; e o acesso ao *ledger* público para qualquer usuário possibilita o *tracking* de conteúdo do bloco, infringindo as regras eleitorais pela antecipação do resultado durante o pleito eleitoral;

- *Private permissionless* e *Private permissioned:* ambas as tipologias não podem ser consideradas *blockchain* porque não atendem os três elementos que caracterizam a *blockchain* de Satoshi Nakamoto (2008): *ledger* distribuído, algoritmo de consenso e *token* (SCHENEIER, 2019, p. 01).

- Plataforma *Ethereum:* é uma extensão da *public permissionless blockchain* que utiliza o protocolo de consenso *PoW (Bitcoin)*, logo, a performance e a escalabidade tem desempenhos insatisfatórios; a moeda *Ether* e a aplicação *DAO* possuem falhas já constatadas na carteira de usuários da criptomoeda.

- Plataforma *Hyperledger Fabric:* é direcionada para ambientes privados e corporativos; não atendem os três elementos da *blockchain* de Satoshi Nakamoto; em alguns casos, um *Enterprise Resource Planning (ERP)* é mais vantajoso do que aderir a um projeto apenas pela terminologia *blockchain.*

- Plataforma *Sovrin Network*: é uma plataforma de identificação digital de identidade única *open-source* baseda em arquitetura semelhante ao *Hyperledger Fabric;* não atendem os três elementos da *blockchain* de Satoshi Nakamoto.

3.3.2 Processamento, Contagem e Verificação E2E

Para o processamento e contagem das cédulas eletrônicas que são realizados em ambiente *off-line*, a investigação propõe a verificabilidade de ponta a ponta em tecnologia *public permissioned blockchain,* adaptada e customizada com o algoritmo *Monero:*

- Apenas o criptograma *random number* e o *session code*[38] são registrados na cadeia de blocos, permanecendo cada registro imutável no *ledger* distribuído*;*

- A ausência da prova de eliminação da última cédula eletrônica registrada durante o processo de votação múltipla é resolvido com a quantidade de registros na cadeia de blocos pelo eleitor e a imutabilidade do *ledger*; e

- Para a operação de votação paralela (cédula eletrônica e papel), o sigilo e integridade das cédulas eletrônicas são asseguradas com o registro na cadeia de blocos e a imutabilidade do *ledger;*

- No processo de anonimização*,* a verificação *E2E* fornece o duplo grau de segurança no *ledger* até o último processamento das cédulas eletrônicas antes da aplicação da criptografia de chave privada pelo *HSM*.

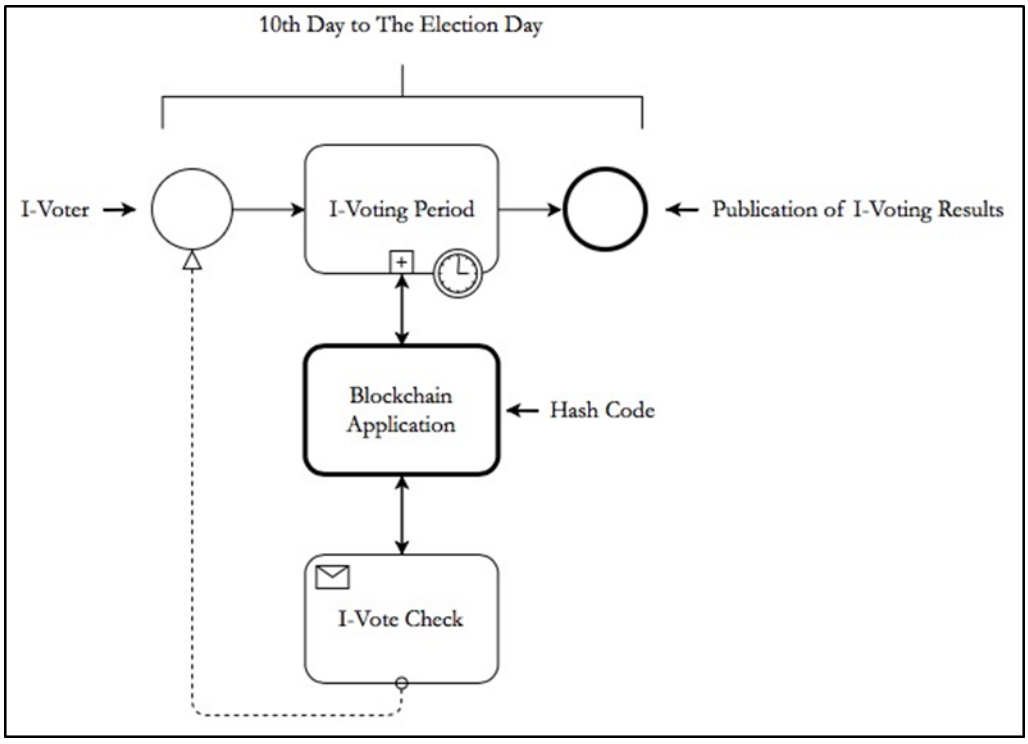
[38] Id. cit. 26.

Para a aplicação da verificação de ponta a ponta no ambiente *on-line*, a proposta com a tecnologia *public permissioned blockchain,* adaptada e customizada, com o algoritmo *Monero* aborda a seguinte solução:

- Com o *ledger* distribuído a verificação *E2E* é individual, universal e permanente.

Vale ressaltar que o período de votação pela Internet estendido é importante para a pesquisa porque o eleitor tem mais tempo para registrar e verificar o seu voto no cronograma do sistema eleitoral estoniano.

Figura 5: Verificação E2E da cédula eletrônica com aplicação em blockchain



Fonte: Elaborado pelo autor

3.3.3 Atores no Processo E2E Blockchain I-Voting

A plataforma *E2E Blockchain I-Voting* é composta pelos eleitores na categoria de nós de rede ou *nodes* e os demais atores indispensáveis do pleito eleitoral estão na categoria de nós mineradores ou *miners*, são eles[39]: a) Eleitor: *node* ou nó de rede*;* b) *National Electoral Committee (NEC)* ou Comitê Nacional Eleitoral: *miner* ou minerador; c) *State Electoral Office*

[39] Id. cit. 26.

(SEO) ou Sede Eleitoral Estadual: *miner*; d) *Information System Authority (RIA)* ou Autoridade do Sistema de Informação: *miner*; e) *Electronic Voting Committee (EVC)* ou Comitê de Voto Eletrônico: *miner*; f) *Rural Municipality ou City Secretaries (RMCS)* ou Secretarias Municipais e Rurais: *miners*; e g) Partidos politicos: *miners.*

O papel do *node* é armazenar o dado do sistema de *i-voting* estoniano no *ledger* distribuído*,* enquanto que os *miners* realizam a prova de consenso para validar e gravar definitivamente o dado na cadeia de blocos do *node* e manter a cópia do banco de dados – *ledger,* intacta para todos os atores envolvidos no processo de verificação ponta a ponta denominado de *E2E Blockchain I-Voting*[40].

O papel dos *miners* são importantes para aumentar o grau de transparência na regra de consenso do processo de votação.

3.3.4. Visão Geral do Processo E2E Blockchain I-Voting

Para a pesquisa, o sistema de verificação *E2E* no sistema de *i-voting* da Estônia deve ser um sistema independente que irá armazenar apenas identificadores da cédula eletrônica que, com o auxílio do aplicativo denominado de *Block Chain Verification Application*[41] na rede *E2E Blockchain I-Voting*, o eleitor verifica o voto eletrônico no processo de votação pela Internet.

Com base na infraestrutura do sistema de *i-voting,* a investigação entende que para a verificação *E2E* obter sucesso é necessário que o *random number* e o *session code* sejam processados pelo módulo chamado de *Processor*, e não pelo *Collector*.

Isto porque no *Processor* a cédula eletrônica consegue alcançar as hipóteses de solução proposta, haja vista que, é a última etapa em que a cédula eletrônica ainda não está no estágio de anonimização. Isto é, cédula eletrônica ainda está assinada digitalmente no sistema.

De acordo com a figura abaixo, a aplicação *E2E Blockchain I-Voting* deve operar da seguinte maneira:

a) Quando o eleitor faz *upload* da cédula eletrônica, o *random number* é gerado pelo *Voter Application* e a aplicação *Processor* utiliza o *digital signed*

[40] Nome dado pela pesquisa.
[41] Id. cit. 52.

cryptogram para gerar o arquivo *session code.* Ambos são registrados no bloco correspondente do *node* pela aplicação *E2E Blockchain I-Voting*;

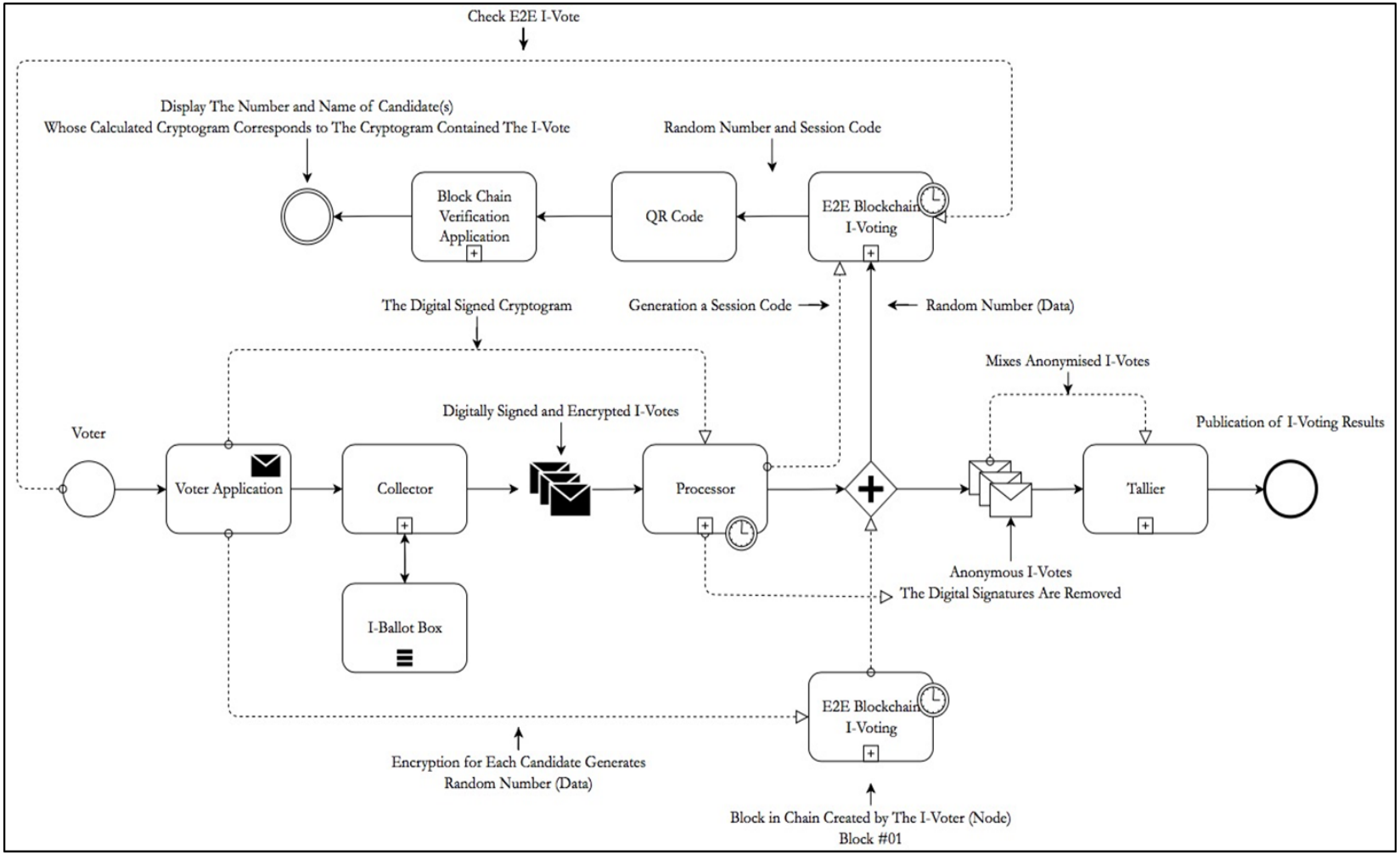
b) Após a transação do arquivo que contém o *random number* e o *session code* validado por um *miner* na rede distribuída de *nodes,* a aplicação *E2E Blockchain I-Voting* gera um arquivo *QR Code* que pode ser verificado com outra aplicação via *smart device* pelo *Block Chain Verification Application;*

c) Os *miners* pré-autorizados validam as transações dos *nodes* sem recompensas digitais *(token digital)* para manter a cópia do *ledger* independente e intacta para cada *node,* tornando a cadeia do registro de blocos pela aplicação *E2E Blockchain I-Voting* permanente e inalterável.

Para a pesquisa o número de computadores para o processamento da mineração deve ser analisado e discutido para ser disciplinado em lei especial e adotado na infraestrutura do sistema de *i-voting*.

No Capítulo 5 são apresentados com maiores detalhes o ambiente operacional e seus respectivos processos inerentes ao sistema de votação pela Internet.

Figura 6: Operação simplificada da Aplicação E2E Blockchain I-Voting



Fonte: Elaborado pelo autor

3.3.5 Intrumentos de Prototipagem e Design de Interação

A prototipagem na interação humano-computador é um método amplamente utilizado no processo de desenho centrado no usuário. É o processo que auxilia no desenvolvimento do *software* que atenda às expectativas e necessidades do usuário (eleitor), neste caso, a proposta da tese.

No campo do design de interação, o desenvolvimento da pesquisa é a partir da aplicação de conceitos construídos com base na observação das experiências e testes com usuários, com o intuito de melhorar a relação humano-computador.

Com efeito, o desenvolvimento da proposta utiliza a ferramenta de análise de processos denominada Modelo e Notação de Processos de Negócio ou *Business Process Model and Notation (BPMN),* com a finalidade de acompanhar sistematicamente como os recursos tecnológicos, físicos, humanos e etc., são alocados e convertidos em ações operacionais na busca das metas organizacionais.

> O *BPMN* define uma série de etapas: a) determinação da cúpula diretiva e equipe interna do projeto; b) prioridade de processos; c) desenvolvimento do *business case;* c) determinar o patrocinador do projeto; d) implementar e automatizar o projeto; e) identificar melhorias no processo; f) excução do protótipo; e g) implementar a mudança necessária no projeto ou sistema (MOLINARI e RAMOS, 2011, p. 29 com adaptações).

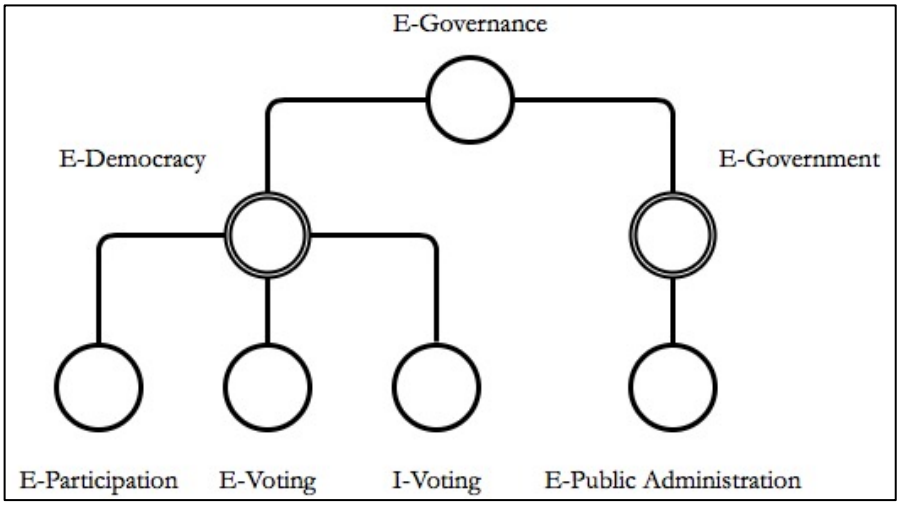
A pesquisa faz uso da ferramenta *open-source draw.io* para explicar e desenhar o modelo atual com diagramas para o sistema de *i-voting* estoniano e a proposta da tese.

4. GOVERNANÇA ELETRÔNICA ESTONIANA

"Bureaucracy is not an obstacle to democracy, but an inevitable complement to it."
Joseph A. Schumpeter

Segundo a *UNESCO* (2011), *e-governance* é a utilização das Tecnologias de Informação e Comunicação (TIC) pelo setor público com o objetivo de melhorar a informação e a prestação da atividade burocrática que engloba, por exemplo, *e-democracy*, *electronic participation (e-participation)* ou participação eletrônica, *e-voting*, *i-voting*, *e-government* e *electronic public administration (e-public administration)* ou administração pública eletrônica, para cidadãos, agentes públicos *in loco*, empresas, organizações não-governamentais, comunidade acadêmica e outros governos[42 e 43].

Figura 7: Estrutura de governança eletrônica européia



Fonte: Elaborado pelo autor

No contexto da era digital, um governo deve possuir habilidade e resiliência para redesenhar os seus processos de negócios com o uso de técnicas de melhoria ou inovação e, assim, providenciar a evolução contínua dos serviços digitais.

Diante desta reflexão, qual é o futuro do *e-governance* nos dias atuais?

---

[42] Reprodução da aula de *e-Governance and e-Democracy in Ragnar Nurkse Department of Innovation and Governance at TalTech University* ministrada pelo Prof. Dr. Robert Krimmer no dia 19/10/2018.

[43] O modelo europeu possui características diferentes do modelo norte-americano. De acordo com *The United Nations Department of Economic and Social Affairs (UNDESA),* por ter sido caracterizado na década de noventa pelo governo norte-americano – início do governo *on-line*, na estrutura norte-america, o *e-government* vem antes de *e-governance.*

A melhoria, inovação ou modernização tecnológica no ambiente governamental não estão apenas baseada no modelo ocidental preconizado na década de noventa, mas nos avanços rápidos da TIC que moldam a aldeia global[44] e, em consonância com o apelo constante da sociedade por instrumentos confiáveis, eficazes e eficientes em processos democráticos.

Com base no exposto acima, a demanda por serviços públicos de qualidade reflete a necessidade do governo de agir e pensar como uma plataforma digital inovadora e resiliente - *Goverment as a Platform (GaaP)*.

Neste sentido, a pesquisa entende que a partir das acepções de Tim O'Reilly (2010, p. 33), uma plataforma de governo no ambiente digital deve adotar padrões abertos para estimular a inovação e o desenvolvimento tecnológico - *open by design*; projetar e construir sistemas que outros possam ajudar, ou seja, a infraestrutura deve ser simples, confiável e acessível em que as informações subjacentes sejam claras e compreensíveis – *digital by default*; o ecossistema digital governamental é centrado para o cidadão e os serviços são testados e determinados por eles – *citizen centric society;* adotar a mineração de dados ou *data mining* para aproveitar a participação implícita dos cidadãos, isto é, as informações que os usuários produzem através da sua interação com os serviços *on-line* ajuda a melhorar a formulação de políticas e a prestação dos serviços, pois é fato que os usuários deixam rastros digitais que podem ser usados para entender o seu comportamento a fim de melhorar os serviços existentes ou projetar um novo; adotar uma postura pró-ativa no desenvolvimento tecnológico mediante o uso de técnicas de inovação, ou seja, um governo deve arriscar no cenário digital porque uma das vantagens dos modelos de negócios baseados na *web* é a facilidade de experimentação positiva ou negativa; e, por fim, adotar o pioneirismo no mundo digital ou *leading by example,* que remete ao perfil de inovação tecnológica no governo – seja ela uma mudança incremental ou revolucionária, demostrando aos cidadãos o potencial de aplicação da própria plataforma.

Neste cenário, a Estônia desenvolve a cultura de transformação digital a longo prazo, com ênfase na necessidade de serviços digitais inovadores e o melhor custo-benefício para o próprio poder estatal e seus contribuintes. Isto pode ser corroborado por Helen Margaretts e

[44] Termo cunhado pelo sociólogo Herbert Marshall McLuhan na obra "A Galáxia de Gutenberg", de 1962.

Andre Naumann (2017, p. 02) enfatizando que o governo estoniano foi o que mais se aproxima de colocar em prática o modelo de *GaaP* do que qualquer outro país com o uso das tecnologias.

Importante ressaltar que não é a ideia central da investigação científica comentar a história da sociedade digital estoniana. Porém, é interessante fazer um breve resumo para entender o seu pioneirismo como nação digital e o compromisso com a inovação tecnológica de forma híbrida entre governo e empresas que proporciona, por exemplo, o sistema de votação pela Internet.

4.1. E-ESTONIA: DIGITAL NATION

A República da Estônia é um país com população de aproximadamente 1.300.000 (um milhão e trezentos mil) habitantes alocados em 45.227 km^2 de territorialidade. É também um dos três países do Mar Báltico[45] que compõem o leste europeu (ESTONIA, 2018).

Após recuperar a sua independência geográfica e política no ano de 1991, o país se tornou membro de pleno direito da União Europeia (UE) e da *North Atlantic Treaty Organization (NATO)* ou Organização do Tratado do Atlântico Norte (OTAN) em 2004, da *Organisation for Economic Co-operation and Development (OECD)* ou Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 2010 e da zona do Euro em 2011. Na política, a Estônia é uma democracia parlamentarista com um primeiro-ministro como chefe do governo e um presidente como chefe de estado (SOLVAK e VASSIL, 2016, p. 02).

Segundo o Dr. Embaixador Roberto Colin (BRASIL, 2018), a economia estoniana possui recursos limitados, pois é a característica do país[46 e 47]. Para reverter esse quadro no final da década de noventa - pós era da dominação soviética, o ex-presidente da Estônia, Thomas Hendrik Ilves, e ex-diretor de tecnologia da informação do governo estoniano, Taavi Kotka, foram os protagonistas de maior destaque, pois apostaram na transformação digital do país com

[45] Ao lado da Letônia e Lituania.

[46] Agronegócio em pequena escala. Desde 2000, o país apostou no investimento estrangeiro em produtos e serviços de TIC e telecomunicações.

[47] Em 02/08/2018, o doutorando se encontrou com o Embaixador Dr. Roberto Colin, na sede da Embaixada do Brasil em *Tallinn*, Estônia. Durante a reunião, ele recebeu a informação de que a economia do país atua mais fortemente como um *hub* logístico de entrada e saída de produtos para a região e países vizinhos da europa oriental, principalmente, a Rússia.

recursos tecnológicos do legado soviético[48] em sintonia com o advento da globalização no cenário mundial.

A partir deste marco, o desenvolvimento tecnológico é construído com base na expertise e empreendedorismo de seus governantes, tornando-se estratégico para o governo estimular o desenvolvimento de produtos e serviços em tecnologias para a Internet, especialmente para o setor privado e público, até os dias atuais.

No mesmo sentido, Siim Sikkut[49], *Estonian Government Chief Information Officer (CIO) in Ministry of Economic Affairs and Communications* ou Diretor de Tecnologia da Informação do governo estoniano no Ministério de Assuntos Econômicos e Comunicação explica que:

> A Estônia começou a implementar a tecnologia digital na prestação de serviços governamentais a partir do final dos anos 90 e com foco na eficiência das operações em *back office*[50] que, ao longo do tempo, tornou-se o fator principal da economia e estratégia nacional. Este fator é composto por quatro pontos importantes: a) gerir o risco cibernético[51] de forma organizada e resiliente; b) adotar técnicas de usabilidade com *design* computacional centrado no cidadão para garantir a ampla aceitação do uso dos sistemas governamentais; c) implementação da identidade digital como ferramenta estratégica dos serviços governamentais; e d) trocas seguras de dados em vários setores e aplicações do governo. Com isso, a inovação foi o passo seguinte do governo até os dias de hoje com o propósito de criar sistemas com interações simples, inclusive com a ajuda de empreendedores privados. A evolução desse cenário foi um governo como plataforma de serviços, que com a análise de dados consegue aperfeiçoá-lo e, também, prever o comportamento do usuário na busca da qualidade dos serviços. Isto tudo é feito com o compartilhamento seguro de dados. O exemplo de sucesso formado pela identidade digital que foi construída mediante a parceria entre o setor público e privado e o sistema *X-Road* que faz a "ponte" entre os sistemas públicos e privados para os cidadãos estonianos e residentes no país – com exceção do programa *e-Residency* que permite o acesso a plataforma *web* de estrangeiros não residentes. O governo adota um modelo de governança muito híbrido, aonde cada ministério tem seu Diretor de TI focado no desenvolvimento digital. Além disso, o escritório do *CIO* foi estabelecido para trabalhar com todos os ministérios no estabelecimento de regras e na experimentação de tecnologias novas, trabalhando em estreita colaboração com o escritório do Primeiro-Ministro para alinhar à agenda digital do país. Por fim, a Estônia pôs à prova como o governo eletrônico é um caminho disponível e replicável para qualquer país, especialmente nações pequenas e

---

[48] Em contato com Embaixador brasileiro Dr. Robert Colin em *Tallinn*, Estônia, no dia 02 de agosto de 2018, a Estônia "herdou" o quartel general de defesa cibernética dos soviéticos na capital *Tallinn*. Hoje o *Cooperative Cyber Defence Centre of Excellence (CCD COE)* e se tornou um parceiro militar estratégico da OTAN na Organização das Nações Unidas (ONU). Isto ajudou a impulsionar o país para que o seu *core business* seja baseado em tecnologias para a Internet e, provavelmente, o marketing estatal.

[49] A transcrição do texto é resultado do encontro com Siim Sikku sobre o *e-Estonia* em três momentos. O primeiro foi no dia 29/05/2018 - *Tallinn e-Governance Conference 2018*, o segundo no dia 25/06/2018 - *Summer School on Secure e-Governance* e o terceiro em 20/12/2018 – *Meeting in Ragnar Nurkse Department (TalTech).*

[50] Atividades internas.

[51] Termo cunhado por Norbert Wiener em 1948.

> não apenas as mais ricas. Esta inovação importante e segura foi alcançada a um custo comparativamente baixo e com determinação para ter sucesso.

Na mesma linha de raciocínio, Daniel Vaarik (2015, p. 06) argumenta que o *e-government* da Estônia é formado por quatro valores fundamentais: a) descentralização; b) interoperabilidade; c) plataforma aberta; e d) *open-ended process* ou processo aberto. Assim, entende-se que que o conceito e a infraestrutura de governo eletrônico estão dispostos para o desenvolvimento contínuo e inovação.

Na prática, o governo estoniano se utiliza de um método híbrido e recursos tecnológicos na implementação do seu *e-governance* em parceria com o setor privado, o *X-Road*[52].

A plataforma de interoperabilidade opera com Interfaces para Programação de Aplicações ou *Application Programming Interface (API)* entres os setores público e privado, tornando-se o *backbone*[53] do país e operando como um *middleware*[54] desde o ano de 2001.

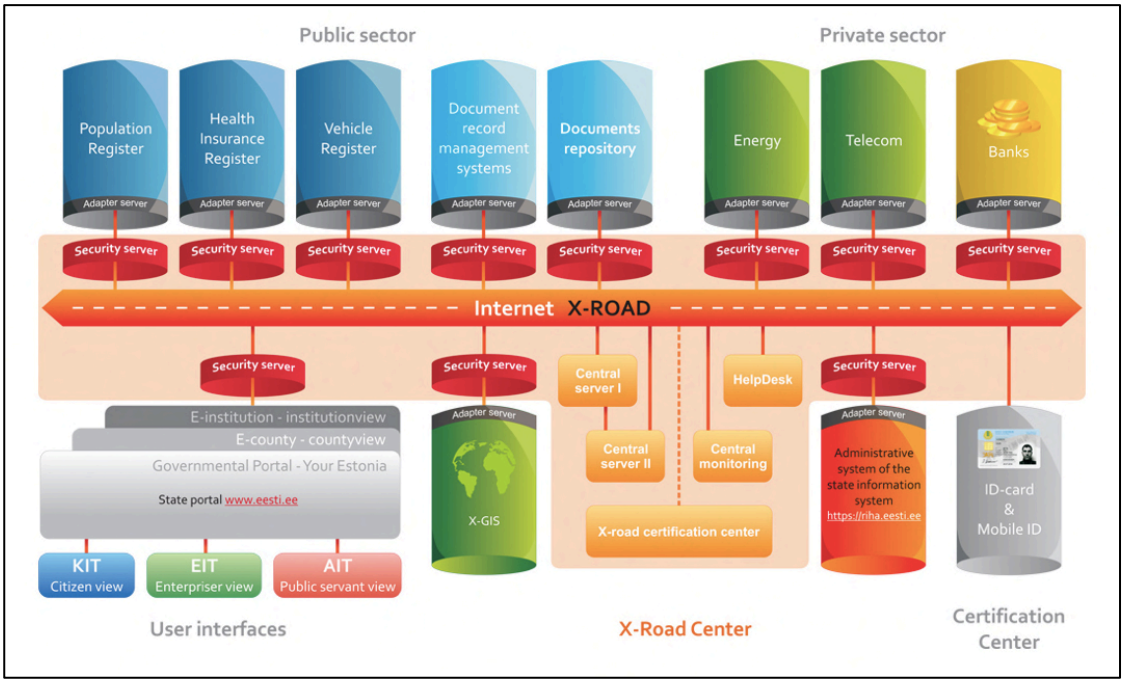
---

[52] *X-Road Versions: • Version 1.0 – 2001. XML-RPC; • Version 2.0 – 2002. SOAP RPC/encoded; • Version 3.0 – 2004 Asynchronous services; • Version 4.0 – 2006.Security update; • Version 5.0 – 2010 SOAP document/literal wrapped; • Version 6.0 – 2014 Federation, External trust service providers.*

[53] O sistema de "estrada de transporte de dados digitais" no país é importante porque a maioria ds registros e bancos de dados mantidos pelo governo está disponibilizado via *X-Road*. Sem a plataforma, o governo para armazenar e trocar dados teria que construir um *data center* ou contratar uma ou mais empresas para transmitir os dispositivos de armazenamento de dados entre municípios e agências em toda a Estônia.

[54] Programa ou Sistema computacional que atua como uma ponte entre um sistema operacional ou banco de dados e aplicativos em uma rede.

Figura 8: Representação gráfica da plataforma X-Road



Fonte: Estonia (2016)

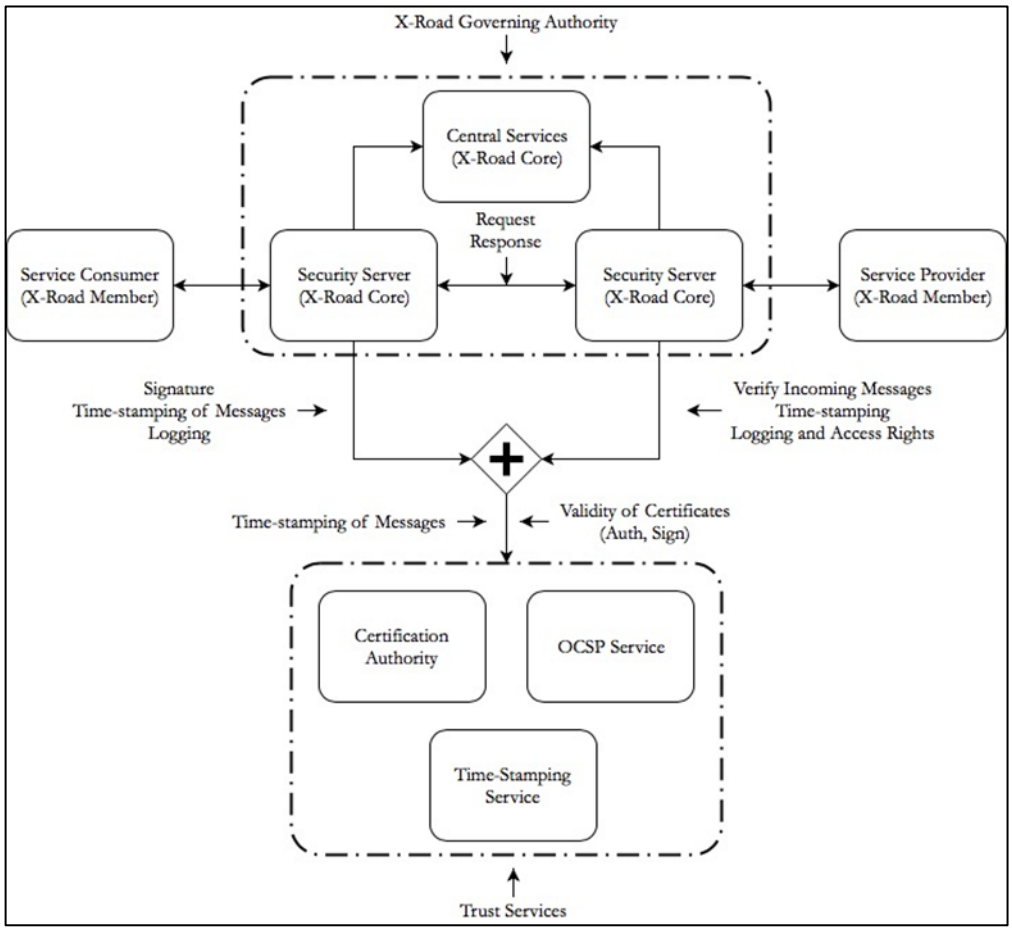
Segundo o *National Information System Authority* ou Autoridade Nacional do Sistema de Informação ou *Riigi Infosüsteemi Amet (RIA)* [55], agência pública responsável por todo o ambiente de tecnologia da informação do governo estoniano, a plataforma *X-Road* é:

> Baseada no ecossistema interoperável com a capacidade tecnológica para trocar dados. Todavia, para realizar esta operação, um membro deve descrever os dados compartilhados para que os demais membros possam utilizá-los com base em um acordo ou contrato. Isto facilita o engajamento mútuo e colaborativo para melhorar o próprio processo de negócio, podendo ser uma entidade pública ou privada (ESTONIA, 2018).

Com relação à proteção de segurança das informações na plataforma, o *X-Road* atua com uma camada de servidores de segurança entre o sistema de interoperabilidade e os demais servidores de sistemas interconectados, conforme é mostrado nas Figuras 8 e 9.

[55] Na língua estoniana.

Figura 9: Infraestrutura segura de troca de dados do X-Road



Fonte: Elaborado pelo autor

É importante mencionar que o nome *X-Road* é utilizado para referenciar a plataforma na língua inglesa, enquanto *X-tee* é a nomenclatura original na língua estoniana[56]. Desde 2018, o *X-Road* se tornou um nome relacionado à tecnologia desenvolvida pelos governos da Estônia e a Finlândia[57] *(X-Road member)* através do *Nordic Institute for Interoperability Solutions (NIIS)*[58].

---

[56] A marca de patente do *X-tee* está disponível em: <https://www2.epa.ee/Patent/mark.nsf/vwSearchEst/A84B46325F5E0E4FC2257FE3004D1131?OpenDocument&Eesti>. A marca de patente do *X-Road* pod está disponível em: <https://www2.epa.ee/Patent/mark.nsf/vwSearchEst/C55C2745DB922D82C2257FE3004D113C?OpenDocument&Eesti>.

[57] Os dois países possuem acordos multilaterais por razões culturais. A língua finlandesa é a mais próxima da língua estoniana, tornando mais prático qualquer vínculo sociocultural ou político. Em 2018, a Finlândia implementou o *Suomi.fi Data Exchange Layer,* uma plataforma de serviços no modelo ao *X-Road/X-tee* realizado pelo *NIIS*. Disponível em: <https://www.suomi.fi/frontpage/>.

[58] As seguintes atividades são realizadas pelo *NIIS* com relação ao *X-Road/X-tee* e outros componentes principais da infraestrutura de governo eletrônico, conforme decidido pelos membros do *NIIS* (Anna-Maija Karjalainen*, Director General, Public Sector ICT, Ministry of Finance, Finland;* e Siim Sikkut*, Deputy Secretary General for Communications and State Information Systems, Ministry of Economic Affairs and Communications,*

A pesquisa *in loco* buscou mais informações sobre a plataforma em dois primeiros momentos. O primeiro ocorreu no *e-Estonia ShowRoom*[59], ambiente preparado para receber cidadãos, empreendedores e autoridades governamentais nacionais ou estrangeiras. E, na sequencia, durante o curso *Secure E-Governance*[60] realizado pela *TalTech*[61].

Não obstante, a investigação recorreu à literatura técnica da *RIA* para concatenar as ideias colhidas *in loco* em razão das diferentes percepções sobre a plataforma.

> A arquitetura da plataforma *X-Road* é formada por uma pilha de protocolos e tecnologias: a) *WDSL* e *UDDI*[62] para serviços através do portal do governo (www.eesti.com), aonde o cidadão através da sua interface envia solicitações *on-line* e não tem a obrigação de fornecer dados porque já estão disponíveis nos determinados bancos de dados e sistemas de informações. Para o servidor público, segue o mesmo raciocínio porque não há necessidade de verificar os dados em diferentes bancos de dados e não há necessidade de revisar documentos; b) *SOAP (XML* e *RPC)* e *LDAP*[63] utilizados para o tráfego de dados no *X-Road* com conexão aos servidores de segurança, servidores centrais, portal do governo e o *Mini Information System Portal (MISP)*[64]; c) *Java, .NET, PHP, Python* e *SAP* são ferramentas utilizadas nos sistemas de informações para o regstro de tráfego, por exemplo, registro populacional e passaportes. A segurança do *X-Road* é garantida por sua arquitetura, juntamente com outras medidas normativas, organizacionais e técnicas. Os dados criptografados são transferidos diretamente através de servidores seguros de um sistema de informação para outro, sendo que os dados não passam pelo servidor central do *X-Road* (I e II)[65] e não podem ser visualizados. O servidor central possui apenas informações estatísticas sobre transferência de dados. O servidor central do *X-Road* também emite certificados para proteger os servidores e fornecer uma lista de certificados confiáveis para sistemas conectados ao *X-Road.* Além disso, o servidor central aceita *hashes* de *log* de servidores seguros para que, se necessário, uma cadeia de uso de serviços possa ser construída no futuro. Neste caso, o *log* do provedor de serviços, o *log* do usuário do serviço e o *hash* do servidor central são comparados. Esse método permite verificar a integridade dos *logs* de servidores seguros, pois é impossível alterar um *log* sem que seja detectável depois. Já os grupos de usuários dos serviços são descritos no servidor central. Na prática, para implementar serviços já criados, você deve se tornar um membro do *X-tee*, instalar um servidor de segurança *X-Road*, fazer um acordo com um provedor de serviços *X-tee* adequado, elaborar uma lógica para criar os dados internos para o serviço escolhido e processar a resposta. O *X-Road* foi desenvolvido há mais de dez anos e uma grande quantidade de código está disponível, o que simplifica significativamente a criação de novas soluções, sendo possível a

---

Estonia): gerenciamento, desenvolvimento, verificação e auditoria do código fonte; gestão da documentação; administração de requisitos comerciais e técnicos; desenvolvimento: desenvolver e implementar princípios de licenciamento e distribuição; fornecer suporte para membros e cooperação internacional.

[59] O doutorando visitou o local no dia 31 de maio de 2018 e no dia 25 de fevereiro de 2019.

[60] A tradução mais contextual é Segurança Digital em Governança Eletrônica.

[61] Participação na *Summer School Secure E-Governance* entre 25/06 a 07/07 de 2018.

[62] É um a descrição em formato *XML* de um *Web Service* que utilizará *SOAP* ou *RPC* como protocolo. E *UDDI* é um *framework* de plataforma independente - desenvolvido na plataforma *.NET*, para descrever e integrar os serviços de negócios usando a Internet, possibilitando uma exposição controlada dos serviços.

[63] *SOAP* é uma especificação para requisitar métodos de negócio, como documentos *XML*, e suporta outros protocolos como *HTTP* e *SMTP*. Já o *RPC* é um protocolo de chamada de processos remoto. *LDAP* é um protocolo de aplicação aberto para acessar e manter serviços de informação de diretório distribuído sobre a Internet.

[64] Destina-se ao uso dos serviços disponíveis na plataforma *X-Road.*

[65] Cf. Figura 7.

> reutilização do código[66]. Se ainda não houver um serviço *X-tee* adequado, ele poderá ser criado em cooperação entre as partes. Com relação aos dados mais específicos e sensíveis, eles também podem ser trafegados, desde que o proprietário tenha ciência que é o controlador dos dados[67] durante todo o processo e que a tecnologia *X-Road* oferece apenas uma troca segura de dados (ESTONIA, 2018).

Em terceiro momento, durante o *X-Road Community Event 2018*[68], realizado pelo *NIIS,* a investigação tomou conhecimento de um conjunto de recursos padronizados para apoiar e facilitar o intercâmbio de dados com base nos seguintes recursos tecnológicos.

> São eles: a) gerenciamento de endereços, b) roteamento de mensagens, c) gerenciamento de direitos de acesso, d) autenticação no nível da organização, e) autenticação no nível da máquina, f) criptografia na camada de transporte, g) marcação de tempo (data e hora) ou *time-stampig,* h) assinatura digital de mensagens, i) *logging*[69] e j) tratamento de erro ou *error handling.* A identidade de cada organização e o risco de acesso são gerenciados pelos *security server* ou servidores de segurança mediante a verificação dos certificados emitidos por uma *Certification Center* ou Autoridade de Certificação Central quando um "ator" qualquer ingressa no ecossistema *X-Road*. As identidades são mantidas centralmente, mas todos os dados são trocados diretamente entre um cliente e um provedor. O roteamento de mensagens é baseado na organização de identificadores a nível de serviço que são mapeados para locais de rede física dos serviços providos pelo *X-Road*. Todas as evidências relacionadas à troca de dados são armazenadas localmente pelas partes envolvidas e nenhuma terceira parte tem acesso aos dados. O *time-stamping* e a assinatura digital garantem o princípio do não repúdio[70] dos dados enviados via *X-Road/X-tee*. No mesmo sentido, a agência enfatiza ainda que a arquitetura do sistema *X-Road* é composta por um sistema distribuído sem ponto singular à falha ou *single point of faliure;* os ativos digitais adotam propriedades de segurança (integridade, autenticidade, criptografia digital, confiabilidade, verificabilidade, escalabilidade e disponibilidade); o uso da plataforma não altera o padrão *FURPS*[71]*;* utiliza o modelo de autorização em dois níveis; os modelos de dados são transparentes com tecnologias de gerenciamento de banco de dados e o uso de padrões para facilitar o acesso de serviços acoplados; e a arquiterura é baseada em linguagem *XML* para compartilhamento de informações via Internet[72]. No tocante à conectividade e ao desenvolvimento da plataforma, ela utiliza protocolos abertos a partir de *freeware*[73] ou programa gratuito. A transmissão dos dados é realizada pela Internet com certificado *Secure Sockets Layer (SSL)*[74], sem a necessidade de uma *Virtual Private Network (VPN)*, sendo que a segurança da informação adota autenticação, autorização

---

[66] Disponível em: <https://github.com/nordic-institute/X-Road-code-samples/blob/master/COMPONENTS.md>.

[67] *General Data Protection Regulation (GDPR).*

[68] No dia 12/09/2018, a participação *in loco* no grupo de trabalho *"X-Road Track Developer"* proporcinou a aquisição de conhecimento e experiência de analistas, engenheiros e programadores da plataforma.

[69] O registro de dados é o processo de coleta e armazenamento de dados durante um período de tempo para analisar tendências específicas ou registrar os eventos ou ações baseadas em dados de um sistema, rede ou ambiente de TIC. Isto permite que o rastreamento das interações pelas quais dados, arquivos ou aplicativos são armazenados, acessados ou modificados em um dispositivo ou aplicativo de armazenamento.

[70] Princípio presente na área de Segurança da Informação que serve para prevenir que, as partes integrantes de uma transação, venham a contestar ou negar uma transação após sua realização. Ou seja, os fatos são argumentados com base nas evidências técnicas.

[71] *Functionality, Usability, Realiability, Performance e Supportability.*

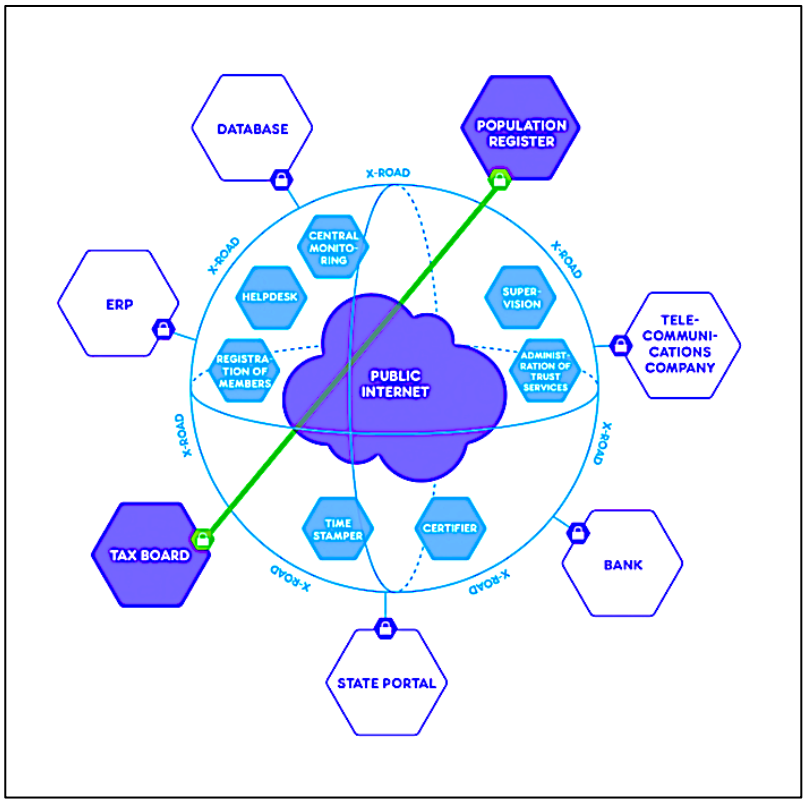
[72] O desenvolvimento da plataforma é por meio de *Application Programming Interface (API).*

[73] *Softwares* que não necessitam de licenças ou *royalties.*

[74] Tipo de segurança digital que permite a comunicação criptografada entre um *website* e um *browser*.

multinível, sistema de processamento de *log*, tráfego de dados criptografados e registro de data e hora. No ambiente de segurança em *lato sensu*, os processos são divididos em três partes: 1) para a autenticação e autorização das partes por meio da interface de usuário simples pelo programa *Mini Information System Portal (MISP)*, os servidores de segurança autenticam as partes com base em certificados localizados no servidor central. Os certificados são criados pelo centro de certificação garantindo a autenticidade do proprietário do certificado. Depois que as partes são autenticadas com base nas informações disponíveis no servidor central, a autorização é realizada no servidor de segurança. Os proprietários dos dados mantêm controle sobre quem pode acessar seus dados, por exemplo, cada organização pode determinar quais serviços estão "abertos" à outra parte para acessá-los. A interface administrativa do servidor de segurança permite total liberdade na especificação de diferentes acessos para diferentes partes, por exemplo, quando uma consulta é feita ao servidor de segurança, a disponibilidade do serviço descrito na consulta para a organização é verificada para permissão ou não; 2) a proteção de dados no ambiente *X-Road* é por dados criptografados que são transferidos diretamente através de servidores de segurança entre sistemas de informações, sendo que os dados não trafegam pelo *X-Road* e, também, não podem ser visualizados por meio dele; 3) o monitoramento é feito pelos servidores de segurança que registram o tráfego de dados entre si e enviam apenas um *hash* de *log* para o servidor central que, posteriormente, compara os *logs* dos servidores de segurança e o *hash* do servidor central para provar o acesso e uso de determinado dado; d) as transações de dados e informações individuais não dependem de um servidor central, pois a arquitetura é distribuída e sem pontos de falhas (NIIS, 2018).

Figura 10: Representação gráfica da plataforma X-Road



Fonte: NIIS (2018)

É possível entender que o projeto foi elaborado de maneira distribuída para evitar os riscos inerentes com uma central de dados robusta e o alto custo de investimento em TIC,

principalmente na década de noventa. Hoje, a plataforma conta com a colaboração de atores estatais, empresas e programadores "fãs" do *X-Road*.

Não obstante, há um processo de transparência das informações na plataforma por meio de uma ferramenta de monitoramento. Isto é, os dados do *X-Road* são coletados dos servidores de segurança dos membros da plataforma na Estônia e disponibilizados pelo *X-Road Center* da *RIA* e pelo *"RIA X-Road v6 OpenData Module EE*[75]*",* sendo publicados em dados abertos com um atraso de dez dias a partir do tempo real de execução da transação[76]. Também é possível o monitoramento de todos os "atores" presentes na plataforma mediante o sistema *"X-Road v6 usage statistics: members networking visualization instance EE*[77]*"*.

É importante enfatizar a observação dos estudiosos Solvak e Vassil (2016, pp. 14-15) sobre o ambiente de *e-governance* estoniano. Para eles, o componente crítico de qualquer sistema funcional de *e-governance* é a identificação digital de cidadãos e residentes. E, com base nos critérios supracitados, ela requer várias pré-condições institucionais, legais e sociais para ser implementada. O modelo estoniano utiliza um único identificador numérico que é usado para toda a população, em vez de inúmeros identificadores pessoais para diferentes serviços públicos e privados. O ambiente normativo disciplina o processo pelo qual instituições, indivíduos e empresas podem solicitar e receber acesso a qualquer informação armazenada em bancos de dados do governo. Com base na identificação única e no *middleware* implementado pelo governo, a camada de aplicação se torna também um ambiente para agências governamentais e corporações privadas criarem aplicações de sistemas para terem acessos ao ambiente de *e-governance*, com base nos padrões e procedimentos exigidos pela plataforma.

> Destacam-se três pontos e seus componentes essenciais. a) Identidade digital: sistema nacional de identificação, identificador exclusivo para todos os residentes, base nacional de registro populacional digital, quadro regulatório, cartão de identificação digital, documento de indentificação via aprelho de telefonia celular ou *mobile identity document (ID)* e outras formas de identificação digital; b) Camada de troca dados: *middleware* unificado e descentralizado para troca de dados, autenticação de cliente, serviços de registro, visualização de *design* para consultas *(query design* e *design view)*, entrada de dados, tranferência segura de dados, registro de *log*, rastreamento de consulta[78], visualização e monitoramento; c) Camada de aplicação: aplicativos integrados desenvolvidos de forma independente pelas instituições

[75] Disponível em:<https://logs.x-tee.ee/EE/gui/>.

[76] Os dados são renovados todas as noites entre 0:00-6:00 (EET UTC+2h/EEST UTC+3h). Os registros de data e hora são arredondados e apresentados na forma de registro de data e hora do *Unix*.

[77] Disponível em: <https://logs.x-tee.ee/visualizer/EE/>.

[78] Diz respeito a técnica de *query tracking*. No processo de consultas do usuário ao sistema, é a maneira de cruzar os dados identificados para prever tendências e/ou buscar melhorias no sistema.

> estatais, seguindo um conjunto unificado de procedimentos; registro de comércio eletrônico ou *e-business register*, polícia eletrônica ou *e-police*, votação pela Internet ou *Internet voting*, prescrição eletrônica ou *e-prescription*, escola eletrônica ou *e-school*, saúde eletrônica ou *e-health*, impostos eletrônicos ou *e-tax*, serviços de assistência social ou *social welfare services* e etc (SOLVAK e VASSIL, 2016, p. 15).

Pode-se concluir que parte do sucesso do *e-Estonia* são: a) a combinação da iniciativa privada com o setor público; b) o papel ativo do governo no desenvolvimento baseado em projetos com resultados; c) a infraestrutura de identificação digital e a camada de segurança para a troca de dados pelo *X-Road;* d) o acesso seguro da interface do cidadão no portal munido da transferência segura de documentos; e) segurança jurídica e, por fim, f) o ineditismo da plataforma *X-Road* no ambiente de *e-governance.*

4.1.1 Documento Eletrônico de Identidade ou ID Card

Não é finalidade da pesquisa só discorrer sobre o documento de identificação eletrônica estoniano, mas expôr a sua importância estratégica no ambiente de governança eletrônica e, principalmente, para o sistema de votação pela Internet do país.

> Segundo a Autoridade Nacional do Sistema de Informação da Estônia, o cartão de identificação digital deve ser universal e suas funções devem ser usadas em qualquer forma de comunicação comercial, governamental ou privada (ESTONIA, 2018).

Durante o período de investigação científica na Estônia, a pesquisa observou que o documento eletrônico de identidade ou *electronic identity document (e-ID)* ou *ID Card* é o tema de suma importância da transformação digital no país. Nas palavras do *Chief Information Officer (CIO)* do governo estoniano, Siim Sikkut[79]:

> Na Estônia, é direito do nascituro o recebimento de um número de identidade digital autenticada e segura por meio de uma certidão de nascimento digital emitida pelo hospital, para que o recém-nascido ao chegar em casa esteja com o seu seguro de saúde válido automaticamente. Todos os residentes da Estônia a partir dos 15 anos de idade possuem cartões de identificação digital ou *ID Card*, que são usados em serviços de saúde, bancários e no comércio em geral. Com a identidade digital nacional estoniana, os indivíduos podem assinar contratos, criptografar *e-mails* ou documentos, comprar bilhetes de trem e **até mesmo votar**. O *ID Card* da Estônia não foi meramente uma inovação em si, mas anunciou a chegada de um dos mais sofisticados governos digitais do mundo. Os impostos podem ser depositados em menos de uma hora e o pagamento dos reembolsos ocorrem dentro de 48 horas. São três fatores que contribuíram para o sucesso da identidade digital da Estônia, o primeiro é a obrigatoriedade imposta que foi fator crucial, pois o cidadão não podia simplesmente recusar para continuar com o documento de papel e outros processos materiais. Em segundo lugar, as assinaturas digitais representaram uma maneira legal e segura de assinar qualquer documento, criando uma infinidade de conveniências e oportunidades para o cidadão. Finalmente, o sistema foi desenvolvido por meio de

[79] Id. cit. 51.

> uma série de parcerias público-privadas e a um preço satisfatório. Não se pode deixar de mencionar que a identidade digital veio com desafios, o governo teve que organizar treinamentos para os cidadãos, especialmente, nas áreas rurais e para ajudar os idosos a se adaptarem à nova prestação de serviços públicos. De outra parte, cerca de 10% da população estoniana ainda não está *on-line* para determinados serviços. Todavia, há outros avanços que irão ocorrer, por exemplo, a aposentadoria automática aos 63 anos e o Mercado Único Digital ou *Digital Single Market* em toda a União Européia, significando o reconhecimento nesse segmento (grifo nosso).

Desde a sua implementação em 1° de janeiro de 2002, o *ID Card* é utilizado como passaporte para cidadãos estonianos que viajam pela União Européia, cartão nacional de seguro de saúde, prova de identificação no acesso em contas bancárias, assinaturas digitais, votação pela Internet (desde 2005), verificação de registros médicos, solicitações ou reivindicações fiscais, prescrições eletrônicas e etc.

A autoridade emissora é a Polícia de Migração da Estônia ou *Migration Border*. Tecnicamente, a estrutura física do cartão de identidade nacional é baseada em *chip*[80], ou seja, é semelhante a um cartão de instituição bancária com um circuito integrado ou *chip* acoplado no material plástico. O *chip* é composto de 16 *Kbytes* de criptografia computacional baseado no modelo RSA[81] com 02 (duas) chaves privadas, chave pública com criptografia de 256 *bytes*, certificado de autenticação, certificado de assinatura digital e um arquivo com dados pessoais. A parte frontal do cartão contém a assinatura e a foto do titular do cartão, e também os seguintes dados impressos: a) nome do titular do cartão, b) sexo do titular do cartão, c) cidadania do titular do cartão, d) código pessoal do titular do cartão (código de identificação nacional), e) data de nascimento do titular do cartão, f) número do cartão e g) validade do cartão. Já na parte posterior do cartão estão impressos: h) o local de nascimento do titular do cartão, i) data da emissão do cartão e j) todos os dados do cartão no formato legível por máquina - adota a diretiva *ICAO Doc. 9303 part* 3[82], para a emissão do formato digital de todos os dados para leitura de máquina, sendo que a empresa que personaliza o cartão é a *Gemalto*[83]. O *ID Card* contém dois certificados e suas chaves privadas estão associadas e protegidas com códigos *Personal Indentification Nunmber (PIN)*. Os certificados contêm apenas o nome do titular e o código

---

[80] É uma pequena lâmina miniaturizada (silício) usada na construção de transistores, díodos ou outros semicondutores, capaz de realizar diversas funções mais ou menos complexas no ambiente eletrônico.

[81] É um modelo de criptografia computacional patenteado na década de 70 por Ronald Rivest, Adi Shamir e Leonard Adleman. É o modelo mais utilizado no mundo em criptografia computacional.

[82] É baseado na norma internacional da aviação civil para identificação digital. Por exemplo, é a faixa alfa-numérica e com signos para leitura em equipamentos infra-vermelho.

[83] A *Gemalto* opera pela a *TRÜB Baltic AS* na Estônia, subsidiária da empresa Suíça *TRÜB AG* desde 2015.

pessoal de identificação nacional, sendo que o certificado de autenticação contém o endereço de *e-mail* exclusivo do titular. É possível o cartão trazer informações detalhadas da autorização de permanência no país para estrangeiros ou qualquer outra informação pertinente ao caso (TALTECH, 2018).

> O certificado de autenticação em cada cartão de identificação estoniano contém o endereço de *e-mail* atribuído pelo governo do titular do cartão no formato de ID-code@eesti.ee, por exemplo, 47302200234@eesti.ee, este endereço é entendido como um canal oficial de comunicação entre o governo e a pessoa, enquanto o governo pode usá-lo para fornecer ao cidadão avisos oficiais e informações pessoais relacionadas à ela. No entanto, outras pessoas também podem enviar mensagens para esse endereço eletrônico. O endereço @eesti.ee envolve um servidor de redirecionamento de *e-mail* que redireciona todas as mensagens enviadas do endereço @eesti.ee para o e-mail real, como @gmail.com, @hotmail.com e etc. ou para o *e-mail* institucional relacionado a atividade laboral da pessoa. O usuário pode redirecionar suas mensagens para até cinco endereços por vez. Importante dizer que há medidas *anti-spam* que são implementadas no servidor de encaminhamento do endereço @eesti.ee. Por fim, o *spam* é ilegal na Estônia e os *spammers* podem ser processados de acordo com a lei (ESTONIA, 2012).

É importante ressaltar que o ambiente digital de suporte ao cidadão estoniano para a identidade digital é o portal *ID (www.id.ee),* gerenciado pela *RIA* em parceria com a empresa *SK ID Solutions,* que possibilita ao usuário o acesso às atualizações dos *softwares,* certificados digitais, aplicativos e demais informações úteis.

Segundo a *SK ID Solutions* (2019) estão ativos 1.323.566 *ID cards*, 224.280 *Mobiil-ID* e 2.486.916 *Smart-ID* (incluídos programas externos), sendo que 451.730 *Smart-ID* são na Estônia. O total de transações no dia 20/09/2019 é de 1.218.812 e no mês de agosto foi de 32.293.905.

Na Estônia, há mais dois outros meios de obter acesso ao sistema de governança eletrônica sem a utilização do *ID Card*: *Digi-ID* e *Mobiil-ID.*

4.1.2 Digi-ID

O *Digi-ID* é um *ID-card* semelhante a um *smart card* ou cartão inteligente. Ele possui todos os atributos do *ID-card*, com exceção de não trazer impresso a foto do proprietário do cartão, impossibilitando, assim, a utilização como documento de identidade digital.

O *Digi-ID* é utilizado no processo de votação pela Internet.

4.1.3 Mobile ID

Segundo as informações no portal *ID*, a partir dos quinze anos de idade, o cidadão estoniano pode consultar a sua operadora de telefonia celular[84] e assinar um contrato *Mobiil-ID* para receber um cartão *Subscriber Identity Module (SIM)* ou Módulo de Identificação do Assinante através de portabilidade. A ativação do cartão *SIM* é no *website* da Polícia e Guarda de Fronteiras ou nas lojas das operadoras de telefonia[85] (ESTONIA, 2019).

É importante ressaltar que de acordo com a empresa *Cybernetica* (2018, p. 12), a tecnologia *Mobile ID* é apenas um *chip* de identificação que é utilizado desde as eleições locais no ano de 2011. Apesar da possibilidade de votar pela Internet, o *chip* não é acessível a todos os serviços de *e-gov* ou serviços privados disponibilizados na plataforma *X-Road*.

4.1.4 Estonian ID Card: ROCA Vulnerability

No ano de 2018, a *RIA* (ESTONIA, 2018) emite um comunicado oficial para explicar que na noite de 30 de agosto de 2017, um grupo de pesquisadores do Centro de Pesquisa em Criptografia e Segurança da Universidade *Masaryk* notificou o Centro de Respostas a Emergências Computacionais da Estônia, em razão da vulnerabilidade de segurança em aproximadamente oitocentos mil *chips* do *the Estonian ID Card* utilizados desde 2014 no país[86].

De acordo com a análise dos pesquisadores, a vulnerabilidade denominada *Return of the Coppersmith Attack (ROCA)* é uma falha algortima na construção de números primos para a geração de chaves criptográficas *RSA*. A falha permite que todas as chaves suscetíveis forneçam uma impressão digital verificável em microssegundos de qualquer *laptop* comum. Isto significa que todas as chaves vulneráveis podem ser rapidamente identificadas, mesmo em conjuntos de dados de grandes proporções (NEMEC, SYS, SVENDA, KLINEC e MATYAS, 2017).

---

[84] Empresas *Telia*, *Elisa* e *Tele2*.

[85] Códigos *PIN* do *Mobiil-ID* do cartão *SIM*: código *PIN1 Mobiil-ID* - para identificação; código *PIN2 Mobiil-ID* - para assinaturas digitais; e código *PUK do Mobiil-ID* - para desbloquear os códigos *PIN* de um *Mobiil-ID* bloqueado.

[86] Os *chips* com falhas são produzidos pela empresa *Infineon*, que também é uma fornecedora dos cartões de identificação da empresa *Gemalto* que opera no país como *TRÜB Baltic*.

Segundo Heiberg e Willemson (2016, p. 03), a votação na Internet da Estônia está "fortemente concentrada" na infraestrutura do *ID Card* existente que, essencialmente, fornece um pré-canal seguro entre o governo e o eleitor na forma de par de chaves público-privadas.

Para a pesquisa, o caso *ROCA* é prova da insegurança das informações no ambiente de votação pela Internet da Estônia porque, provavelmente, sem a descoberta dos analistas checos em 2017, o governo estoniano continuaria com o mesmo *chip* em operação até os dias atuais.

Vale ressaltar ainda que, os pleitos eleitorais de 2014 *(the European Parliament election),* 2015 *(the Riigikogu election)* e 2017 *(the local government councils)* podem ser classificados como processos de votação pela Internet suspeitos de fraudes, em razão da vulnerabilidade nos *chips* do *ID Card* presentes desde o ano de 2014.

Conclui-se na pesquisa que ainda é um desafio para o governo da Estônia a documentação eletrônica de identificação no processo de votação pela Internet. Muito embora estudiosos considerem a baixa participação dos eleitores no sistema de *i-voting* um hábito em evolução (SOLVAK e VASSIL, 2016, p. 121), a pesquisa entende que a insegurança ou falta de confiança no processo de *i-voting* é uma das causas de ausência dos eleitores nos pleitos eleitorais[87].

4.1.5 Base Regulatória

Não é o objetivo discutir as leis estonianas, mas é importante apenas citar a segurança jurídica necessária para o uso da identidade digital e as tecnologias interrelacionadas no *e-governance* do país*,* pois a regulação é o mecanismo importante para complementar a garantia da confiança na instituição governamental.

Deste modo, o governo estoniano elaborou um rol de leis ou decretos que oferecem suporte para a implementação e continuidade da tecnologia desde o início da transformação no

[87] Id cit 26.

país[88], são elas: *Personal Data Protection Act (1996)*[89 e 90], *Public Information Act (2000)*[91], *Population Register Act (2000)*[92], *Digital Signatures Act (2000)*[93], *Identity Documents Act (1999), Electronic Identification and Trust Services for Electronic Transactions Act (2016), Competition Act (2001), Electronic Communications Act (2004)*[94] e *Interoperability Framework Regulation (EU/2017).*

4.1.6 Digital ID e I-Voting

Com base no exposto, a investigação conclui nesse capítulo que o projeto de votação pela Internet somente é possível em razão da infraestrutura tecnológica de identidade eletrônica, pois ela desempenha um papel importante na estratégia de *e-governance* da Estônia.

É importante esclarecer que a proposta da tese não é analisar a tecnologia por detrás da identidade eletrônica estoniana no processo eleitoral pela Internet, mas abordar um modelo de aplicação para verificar a cédula eletrônica durante o processo de votação pela Internet.

---

[88] É importante mencionar que agumas leis são concomitantes com as normas institucionalizadas pela União Européia.

[89] *The aim of this Act is to protect the fundamental rights and freedoms of people regarding the processing of their personal data, above all the inviolable right to a private life. This Act provides: 1) the conditions and procedures for the processing of personal data; 2) the procedure for the exercise of state supervision upon the processing of personal data; 3) liability for the violation of the requirements for the processing of personal data* (SOLVAK e VASSIL, 2016, p. 19).

[90] Revisado em 2008 e 2018.

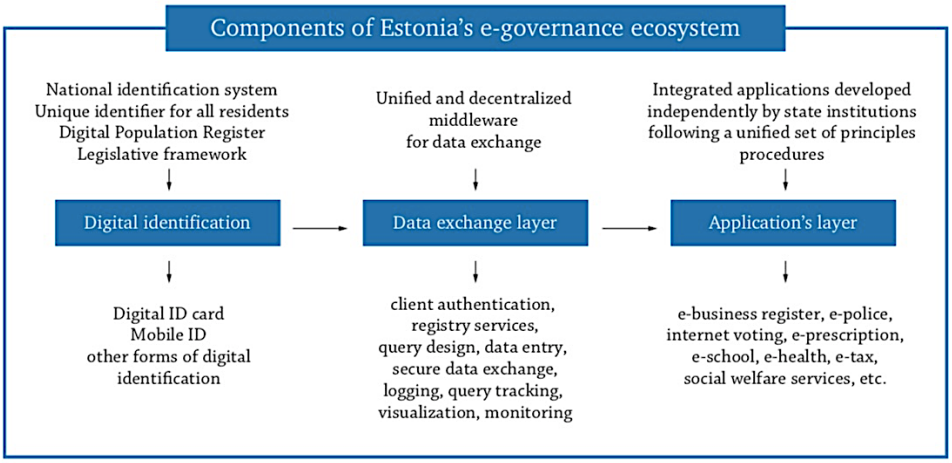
[91] *The purpose of this Act is to ensure that every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public services* (SOLVAK e VASSIL, 2016, p. 19).

[92] *This Act provides for the composition of data in the population register and the procedure for the introduction and maintenance of the population register, the processing of data and access to data in the population register, the entry of data on residence in the population register and exercise of supervision over the maintenance of the population register* (SOLVAK e VASSIL, 2016, p. 20).

[93] *This Act provides the conditions necessary for using digital signatures and digital seals, and the procedure for exercising supervision over the provision of certification services and time-stamping services* (SOLVAK e VASSIL, 2016, p. 20). Foi revogado em 2016.

[94] *The purpose of this Act is to create the necessary conditions for the development and promotion of electronic communications networks and electronic communications services without giving preference to specific technologies and to ensure the protection of the interests of users of electronic communications services by promoting free competition and the purposeful and just planning, allocation and use of radio frequencies and numbering* (SOLVAK E VASSIL, 2016, p. 20).

Figura 11: Integração de sistemas via X-Road



Fonte: Solvak e Vassil (2016, p. 15)

4.1.7 E-Estonia: Marketing Play

A pesquisa observa que o país adotou o título *e-Estonia* como *slogan* ou marca para se autodenominar uma nação digital ou sociedade digital da União Europeia (UE)[95]. Contudo, a investigação *in loco* percebe uma "jogada" de marketing bastante peculiar.

O governo estoniano apresenta um dos modelos de *e-govenance* mais perceptíveis na transformação das nações na era digital. Não é comum um governo fazer marketing dos próprios serviços de *e-government* e *e-democracy* para o mundo. No entanto, a Estônia cria projetos para que o país seja pioneiro em iniciativas tecnológicas para a Internet.

Por exemplo, o projeto de desenvolvimento digital da Estônia fez do país um "vale do silício" europeu, concentrando atualmente 1.029 *start-ups* para a área de tecnologia da Internet. Dentre elas, pode-se destacar a *TransferWise, Bolt, Pipedrive OÜ, Veriff, Paxful, Starship Technologies, Monese, Coolbet, Milrem Robotics* e *Ridango* (STARTUP ESTONIA, 2020). Dentre eles, o país tem orgulho de intitular quatro casos de sucesso em tecnologia para a Internet como "unicórnios", as empresas *Skype*, *Transferwise*, *Pipedrive* e *Taxify*.

Um outro exemplo é o programa *E-Residency,* criado por Taavi Kotka, que oferece aos estrangeiros a oportunidade ter acesso a plataforma *X-Road* com um *ID Card* e utilizar alguns serviços eletrônicos, como a autenticação e a assinatura digital. Qualquer pessoa física ou empresa estrangeira pode ter acesso ao programa a um custo de aproximadamente cem euros

[95] *e-nation, e-state, e-country ou e-society*.

(ESTONIA, 2019). É importante dizer que o *E-Residency* não é considerado um visto de permanência no país porque para adquirí-lo é suficiente apenas aderir ao programa como um "migrante digital", seja um indivíduo "fã" do programa ou se cadastrar como empresa interessada em fazer negócio na Estônia[96].

Um dos exemplos mais importante da pesquisa é a votação pela Internet, que é divulgada pelo governo estoniano como um produto eficaz e seguro para eleições eletrônicas. No entanto, a pesquisa observa que há muita discordância com o modelo estoniano de *i-voting*, especialmente, em relação à confiança do processo eleitoral do ambiente *on-line* e *off-line* de votação[97].

Apesar do país informar que 99% do sistema público é realizado pela Internet, o governo da Estônia é "conservador" em relação ao casamento, o divórcio e a compra ou venda de imóvel[98].

No mesmo sentido, a experiência *in loco* da pesquisa mostra que o *ID Card* não é para todos os estrangeiros com permanência na Estônia, pois há falsa percepção da sociedade estoniana de que qualquer estrangeiro tem direito a identidade eletrônica na nação digital[99]. A solicitação do Visa depende da circunstância e do motivo de permanência no país. Neste caso, o modelo permitido é o *Long-stay (D) visa*[100] que não dá direito ao *ID Card*. No caso *in loco*, a operação para adquirir o Visto de permanência é realizada manualmente e em papel, sendo que o solicitante deixa em posse da polícia estoniana o seu passaporte com *chip* e recebe uma foha de papel manuscrita e datada para transitar pelo país até a conclusão do processo de permanência.

---

[96] No *ID Card E-Residency* é impresso apenas o número de identificação da pessoa física. Para abrir uma conta corrente no país é necessário provar o vínculo *Business-to-Business (B2B)* para evitar fraudes e "lavagem de dinheiro".

[97] Cf. Capítulos 2, 3 e 5.

[98] Segundo informações do apresentador no *E-Estonia Show Room,* o comportamento das pessoas influencia na decisão do governo em dispor do serviço de matrimônia pela Internet. Já a operação imobiliária é uma forma de garantir os verdadeiros proprietários.

[99] No primeiro dia na *TALTECH*, o Prof. Dr. Robert Krimmer informou que eu receberia um *ID Card*. Em visita ao Parlamento da Estônia, a convite de Siret Kotka-Repinski, membro do Parlamento estoniano, a parlamentar ficou surpresa com a ausência do cartão eletrônico para o doutorando. Em fevereiro de 2018, ao visitar o *E-Estonia ShowRoom* pela segunda vez, o apresentador ficou surpreso com a ausência da identidade eletrônica do doutorando após dez meses de permanência no país.

[100] Informado apenas no *website Ministry of Foreign Affairs* e não no portal da Polícia de Migração.

O governo da Estônia é um modelo singular de promover os próprios serviços eletrônicos. No entanto, a experiência estoniana tem mostrado que o caminho para se posicionar como nação digital requer muito mais do que propaganda.

Em contato com Embaixador brasileiro Dr. Robert Colin em *Tallinn*, Estônia, no dia 02 de agosto de 2018, a Estônia "herdou" o quartel general de defesa cibernética dos soviéticos na capital Tallinn. Hoje o *Cooperative Cyber Defence Centre of Excellence (CCD COE)* se tornou um parceiro militar estratégico da Organização do Tratado do Atlântico Norte (OTAN) na Organização das Nações Unidas (ONU). Isto ajudou a impulsionar o país para que o seu *core business* seja baseado em tecnologias para a Internet e, também, o marketing estatal.

Apesar de ter o centro das operações em cibersegurança da UE no país, dois casos põem dúvidas sobre o modelo de segurança da Internet na Estônia. O primeiro são os ataques de *hackers* que desconectaram o país da Internet entre 27 de abril à 18 de maio no ano de 2007 (CCD COE, 2007) e, segundo é a descoberta da vulnerabilidade no *chip* do *ID card* estoniano em 2017 (ESTONIA, 2018).

5. SISTEMA ESTONIANO DE VOTAÇÃO PELA INTERNET

"Anything that gives us new knowledge gives us an opportunity to be more rational"

Herbert A. Simon

A Estônia é o único país que utiliza a votação pela Internet de forma contínua e oficial no processo eleitoral da nação. De 2005 até 2019 são doze pleitos eleitorais: a) eleições municipais ou *the local government councils* (2005, 2009, 2013 e 2017); b) eleições parlamentares ou *the Riigikogu elections* (2007, 2011, 2015 e 2019); e c) eleições do Parlamento Europeu ou *the European Parliament elections* (2009, 2014 e 2019). Em março de 2019, o relatório final da missão de avaliação eleitoral da *OSCE/ODIHR* reportou a maturidade do processo de *i-voting* no pleito eleitoral estoniano.

> Todos os interlocutores da equipe de especialistas em eleições concordaram que a confiança na votação pela Internet na Estônia está aumentando, citando a conveniência e a ausência de ciberataques como os principais motivos. A equipe de especialistas em eleições avaliou que a votação pela Internet não é mais considerada um experimento pelas autoridades, mas parte de uma estrutura regular (OSCE/ODIHR, 2019, p. 09).

Durante a pesquisa *in loco* como observador das eleições pela *TALTECH* entre os dias 21/02/2019 a 27/02/2019, foi possível analisar o processo eleitoral desde o período de campanha dos candidatos, o ambiente de votação em cédula de papel e pela Internet. Todo o processo pré-eleitoral da Estônia ocorre em dez dias antes do dia da eleição. Há dois tipos de formas de votação: em cédula de papel e em cédula eletrônica pela Internet.

O processo de votação antecipada ou *advance voting,* é realizado de três maneiras:

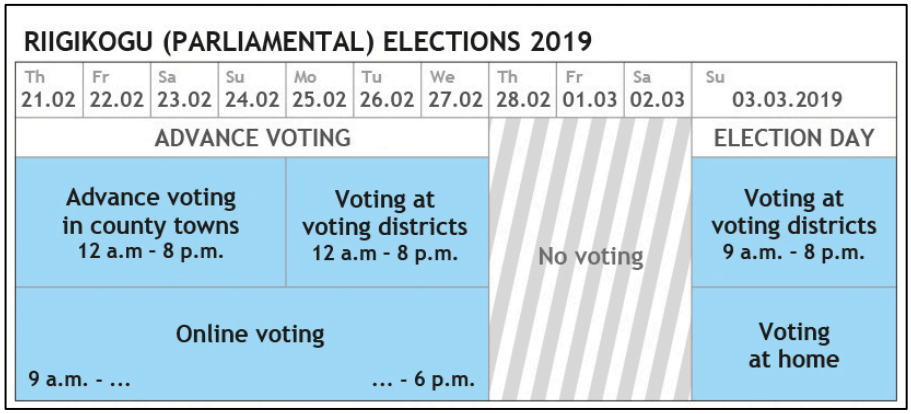
a) *advance voting in county towns* que ocorre do 10° ao 7° dia *(early voting)*;
b) *voting at voting districts* que ocorre do 6° ao 4° dia *(advance voting)*; e
c) *online voting* ou *i-voting* que ocorre do 10° ao 4° dia *(advance voting)*.

Na sequencia, do 3° ao 1° dia não há sufrágio, pois é utilizado para anular automaticamente no ambiente *off-line* as cédulas registradas na votação múltipla e votação paralela; corrigir e eliminar imperfeições oriundas de inelegibilidades ou quaisquer ações inadequadas à probidade do processo eleitoral pela autoridade responsável.

No "último dia" (*zero day),* é o *election day* ou dia da eleição para votar somente via *voting at voting districts* e *voting at home*.

> Na Estônia, a votação pela Internet é aberta dez dias antes do dia da eleição. Na quinta-feira às 9 horas e encerrada quatro dias antes do dia da eleição às 18 horas. É possível votar 24 horas pelo *website* www.valimised.ee. De acordo com os dados recebidos do servidor de Registro da População ou *Population Register*, as possíveis alterações na lista de eleitores são inseridas no sistema de votação pela Internet pelo menos uma vez a cada 24 horas (ESTONIA, 2017, p. 08).

Figura 12: Cronograma das Eleições de 2019



Fonte: Estonia (2019)

Como as regras e os princípios norteadores do processo eleitoral são disciplinados em lei, a visão geral do processo eleitoral estoniano começa com a base regulatória que é composta pela *Constitution of Estonia* ou Constituição da Estônia, *Riigikogu Election Act* ou Lei Eleitoral do Parlamento, *Municipal Council Election Act* ou Lei Eleitoral do Conselho Municipal e *European Parliament Election Act* ou Lei Eleitoral do Parlamento Europeu.

De acordo com a legislação eleitoral do parlamento estoniano de 2019, há diversos tipos de canais de votação: a) *foreign voting by post* ou votação no estrangeiro pelo correio que deve ser realizado 30 dias antes do dia oficial da eleição via cédula de papel; b) *foreign voting at the foreign mission* ou votação em embaixada diplomática ou consular que ocorre entre 15° e 10° dias antes do dia oficial da eleição via cédula de papel; c) *early voting (at the polling station)*[101] ou votação antecipada (primeira fase) em zona eleitoral via cédula de papel; d) *advance voting (at the polling station) (voting in the location of the voter)*[102 e 103] ou votação antecipada

[101] Os eleitores estonianos podem votar fora de seu distrito de residência apenas durante esta fase eleitoral.
[102] Segundo a lei, é em *supermarket voting, custodial institutions, hospitals and twenty-four-hour social welfare institutions.*
[103] Também ocorre o processo de votação em navios de bandeira estoniana em águas internacionais.

(segunda fase) no local do eleitor via cédula de papel; e) *i-voting* ou votação pela Internet[104]; e f) *election day voting* ou votação no dia oficial da eleição[105].

A gestão do processo eleitoral é realizada pelos seguintes órgãos *National Electoral Committee (NEC)* ou Comitê Eleitoral Nacional, *State Electoral Office (SEO)* ou Escritório Eleitoral Estadual, *Information System Authority (RIA)*, *Electronic Voting Committee* ou Comitê de Votação Eletrônica, *Estonian Computer Emergency Response Center* ou Centro de Resposta a Emergências Computacionais da Estônia, *Rural Municipality or City Secretaries* ou Secretarias Rurais ou Secretarias Municipais, *Voting District Committee (VDC)* ou Comitê Distrital de Voto, *Vote Counting Committee (VCC)* ou Comitê de Contagem de Votos, *Ministry of Interior* ou Ministro do Interior e outros órgãos governamentais de apoio e comunidade acadêmica. Com base na legislação, o *NEC* estabelece alguns princípios para o processo eleitoral e em especial para o sistema de *i-voting*:

> a) *Time framework of i-voting* ou Prazo estrutural da votação pela Internet: os votos *on-line* pela Internet podem ser registrados entre o 10° ao 4° dia antes do dia oficial da eleição; b) *Possibility to recast an i-vote* ou Possibilidade de registrar ilimitadamente um voto *on-line*: durante o período de votação *on-line*, o eleitor pode votar quantas vezes quiser, mas apenas o último voto é contabilizado; c) *Primacy of ballot paper voting* ou Primazia da cédula de papel: se um eleitor que já votou pela Internet se dirigir para a zona eleitoral do seu distrito e votar em cédula de papel durante a "votação antecipada", o voto pela Internet será cancelado. Depois disso, o eleitor não pode votar novamente pela Internet ou cédula de papel. A pesquisa entende que este princípio é um meio de coibir o voto de "cabresto"; d) *Similarity of e-voting to regular voting* ou Similaridade do voto pela Internet aos votos regulares (por lei): o voto *on-line* pela Internet adota a lei, os costumes e princípios gerais do processo eleitoral do país. Assim, é uniforme e secreto, apenas os eleitores elegíveis podem votar, aonde cada pessoa pode dar apenas um voto e deve ser impossível que os eleitores saibam de que maneira alguém votou na eleição. A coleta de votos pelo sistema físico ou virtual deve ser segura, confiável e verificável; e) *An e-voter shall vote themself* ou voto personalíssimo, significa que é proibido o uso do *ID-card, Mobiil-ID* ou *Digi-ID* de outra pessoa para votar ou transferir os códigos *PIN* para outro eleitor (SOLVAK e VASSIL, 2016, pp. 09-10 com adaptações).

Não é objeto da pesquisa se aprofundar em cada detalhe das atividades burocráticas do pleito eleitoral da Estônia, pois durante o tempo de investigação na *TALTECH,* o grupo de pesquisa *Cost of Democratic Elections (CoDe)* ou Custo das Eleições Democráticas formado por professores, mestrandos e doutorandos – inclusive estudantes de intercâmbio, já estuda o custo operacional das eleições no país.

---

[104] Somente no distrito do eleitor, salvo em casos, como hospital e etc., podendo ser em outro local.
[105] *Voting at home* ou voto na residência só ocorre nesse dia a pedido do eleitor para casos excepcionais.

Consequentemente, um dos resultados de pesquisa do *CoDe* é o recente estudo de caso das eleições parlamentares de 2019 na Estônia que não aborda os aspectos tecnológicos *(hardware* e *software)*, mas apenas os custos das atividades individuais e operacionais (os valores dos custos não apresentam qualquer referência de fonte) e as regras de negócios baseadas na legislação estoniana em conjunto com os procedimentos administrativos relacionados com as atividades dos organizadores - *NEC, SEO, RIA* e demais membros responsáveis pela *e-election*.

O papel do *CoDe* é provar que o custo da votação pela Internet é mais vantajoso do que outros canais de votação na Estônia:

> Em relação à análise de custos, podemos levantar algumas declarações gerais sobre as Eleições Locais da Estônia (2017): 1) *E-voting* é o canal de votação mais barato proposto no contexto eleitoral analisado devido à aceitação da ferramenta pelos cidadãos e à redução de custos envolvidos na implantação. O custo por voto eletrônico é metade do custo da segunda opção mais barata – *voting by paper ballot in election day* (KRIMMER, DUENAS-CID, KRIVONOSOVA, VINKEL e KOITMAE, 2018, pp. 20).

Por outro lado, a pesquisa entende que o projeto *CoDe* é parte da estratégia de marketing do governo estoniano para comunicar que o sistema de *i-voting* é o melhor custo-benfício em processos de eleição eletrônica.

O artigo científico faz uma afirmação equivocada ao dizer que o custo do sistema de votação pela Internet é mais barato em razão da aceitação da ferramenta pelos estonianos.

De acordo com os dados de Solvak e Vassil (2016, p. 106), a participação dos eleitores estonianos pela Internet é inferior ao número de votos em papel. Por exemplo, os dados mais recentes do governo estoniano (ESTONIA, 2019) comprovam que o número de eleitores pela Internet na eleição *Riigikogu (parliamentary) elections 2019* é de 247.232 (27,86%) em face do total de 887.420 eleitores. Isto demonstra que a curva de aceitação pelos eleitores ainda é pequena nesses quinze anos de votação pela Internet.

O trabalho acima também não traz os custos de *software* e *hardware* para todos os aspectos do ambiente de *e-election,* em especial, a segurança da informação, fator crucial para qualquer processo de votação eletrônica ou votação pela Internet.

Para a pesquisa, o processo estoniano de *i-voting* não deve ser calculado apenas pelo custo operacional da mão-de-obra durante o período eleitoral, pois não transmite a realidade dos custos totais de um processo de votação pela Internet para defender o seu espaço remoto.

5.1. SISTEMA DE I-VOTING DA ESTÔNIA

Em primeira análise, a pesquisa parte do pressuposto de que há confiança implícita no sistema de *i-voting (*pessoas, processos e tecnologias), e que os microcomputadores, *laptops* e aparelhos celulares dos eleitores não estão infectados com programas maliciosos como *malwares* e etc.

A partir disto, a estrutura geral dos processos de *i-voting* da Estônia são baseados pela observação analítica *in loco* e com base no documento *IVXV - ÜK - 1.0, General Framework of Electronic Voting and Implementaton thereof at National Elections in Estonia* e no repositório *GitHub.*

É importante dizer que o documento *IVXV - ÜK - 1.0* traz uma visão dos processos do sistema de votação pela Internet, porém, bastante segmentado e com informações parciais, dificultando a análise das conexões tecnológicas por detrás dos atores, processos, sub-processos, funções e tarefas de *softwares* e *hardwares* no ambiente de votação pela Internet.

Além disso, o documento também não traz elementos sobre todos os aspectos relacionados à segurança da informação no sistema de *i-voting* estoniano.

> Este documento não tem como objetivo definir o nível de segurança específico dos componentes do sistema, estruturas de dados, plataformas de *software* e *hardware* utilizadas ou a estrutura tecnológica detalhada. No caso de um ataque em larga escala ou erro no sistema de *i-voting*, o organizador da eleição poderá anular total ou parcialmente os votos digitais. Neste caso, o eleitor poderá votar de novo através da cédula de papel (ESTONIA, 2017, p. 04).

A lacuna de informações sobre a gestão de segurança das informações do sistema de votação pela Internet da Estônia é um obstáculo da pesquisa, pois nem todas as informações são fornecidas pela *RIA, NEC, SEO* e demais membros da comissão eleitoral, por exemplo, a empresa *Cybernetica-Smartmatic* que atua de forma conjunta com o governo estoniano no centro de pesquisas voltado para *i-voting*[106].

Torna-se bastante delicado falar sobre segurança da informação no processo de votação pela Internet da Estônia na condição de cidadão estrangeiro. Neste caso, a pesquisa presume

---

[106] Disponível em: <https://www.ivotingcentre.ee>.

que o *X-Road* seja parte do perímetro de segurança da informação do processo eleitoral, pois o sistema de *i-voting* é uma camada de aplicação que interage com a plataforma *X-Road.*

Todavia, o objeto da investigação não é expor o documento *IVXV - ÜK - 1.0,* mas apresentar partes do sistema de votação pela Internet para entender a funcionalidade do processo de *i-voting* por meio de diagramas elaborados pela pesquisa.

5.1.1 Atribuições e Responsabilidades

Durante a observação da investigação, os procedimentos para a votação pela Internet na Estônia estão sob a responsabilidade do *NEC* que, em primeiro ato, torna público a abertura do processo de eleição, pois é o órgão de maior autoridade no pleito eleitoral.

O *NEC* atua para gerir, acompanhar e validar os processos da eleição pela Internet, sendo que os demais atores responsáveis pela operação e funcionamento do sistema de *i-voting*, *SEO, RIA* e outros, seguem as orientações do *NEC* para também gerir e conduzir o pleito pela Internet.

No que diz respeito à tecnologia do sistema de *i-voting*, a *RIA* em parceria com as empresas privadas *Smartmatic-Cybernetica* são responsáveis pelas aplicações de *softwares* (disponibilizados dias antes do período da pré-eleição)*, hardware,* criação do par de chaves criptográficas (pública e privada) e demais infraestruturas condizentes com o sistema de votação pela Internet.

O eleitor é responsável pela sua identidade digital (regularização) e configuração do seu computador pessoal (instalação do programa *Voter Application, firewall* e anti-vírus) e dispositivo inteligente - aparelho de telefonia celular ou *tablet*, (instalação do programa *Verification Application*) para verificação do armazenamento da cédula eletrônica no servidor central de dados, que pode ser visualizado por um *QR Code* na tela do computador com uma câmera de celular ou *tablet.*

5.1.2 Organização do Processo de I-Voting

O sistema *i-voting* estoniano é formado por quatro estágios (ESTONIA, 2017, p. 08):

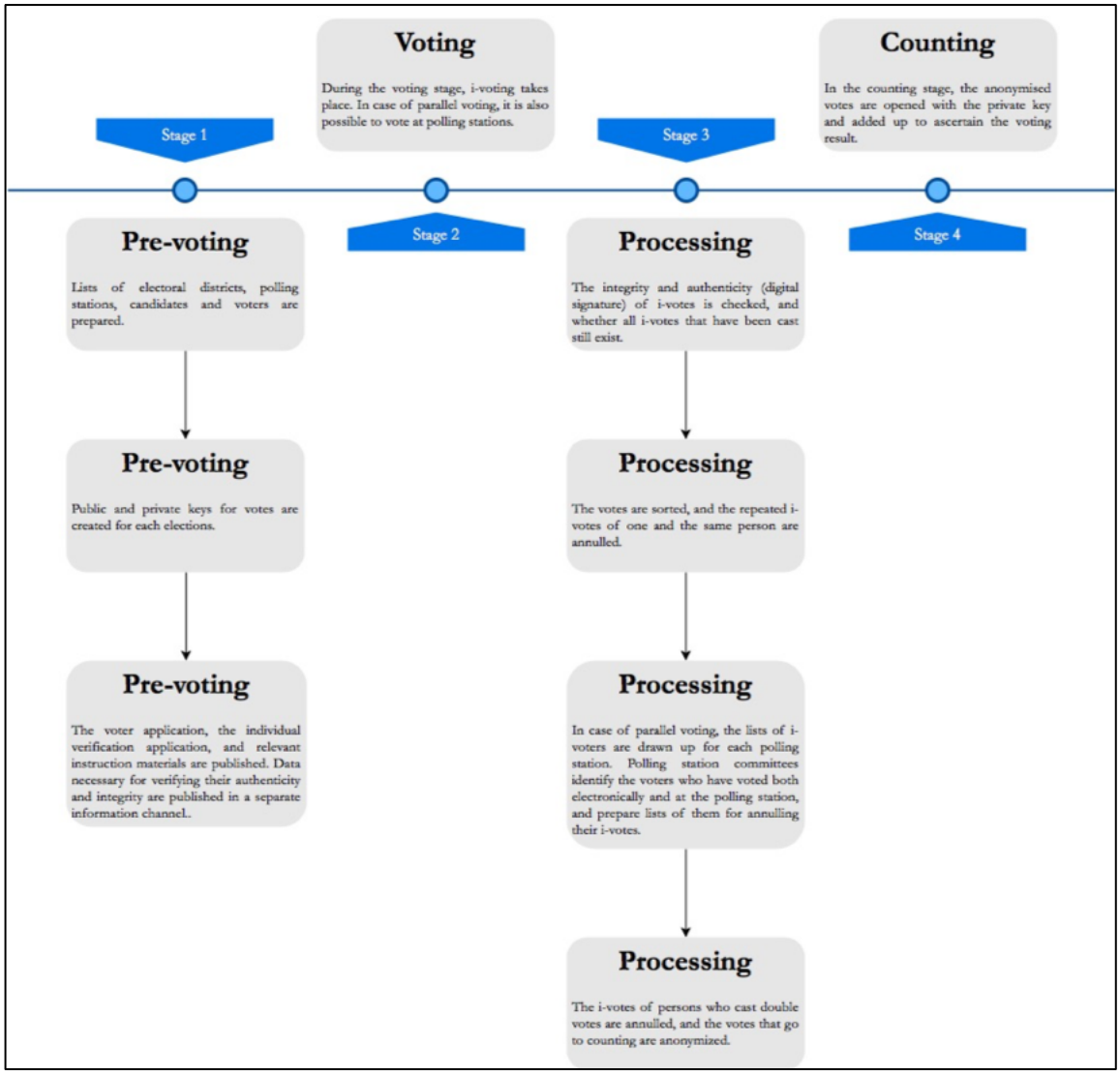
1) *Pre-voting* ou pré-votação;
2) *Voting* ou votação;
3) *Processing* ou processamento; e
4) *Counting* ou contagem.

Para a pesquisa é importante dizer que a votação pela Internet apenas ocorre no estágio de número 2 *(Stage 2)*. Isto significa que o procedimento de *i-voting* é configurado durante a coleta da cédula eletrônica no ambiente *on-line*.

É possível notar que a aplicação para verificabilidade de ponta a ponta não faz parte das etapas que compõem a organização do processo de *i-voting* da Estônia.

Com base na proposta da investigação, a aplicação de verificação *E2E* deveria estar inter-relacionada nos estágios de números 2 e 3 para configurar que o sistema de *i-voting* atende os princípios da *OSCE/ODIHR* – dilemas do anonimato, integridade e transparência, para processos de votação pela Internet.

Figura 13: Etapas do i-voting estoniano



Fonte: Elaborado pelo autor

5.1.3 Escopo Inicial do I-voting

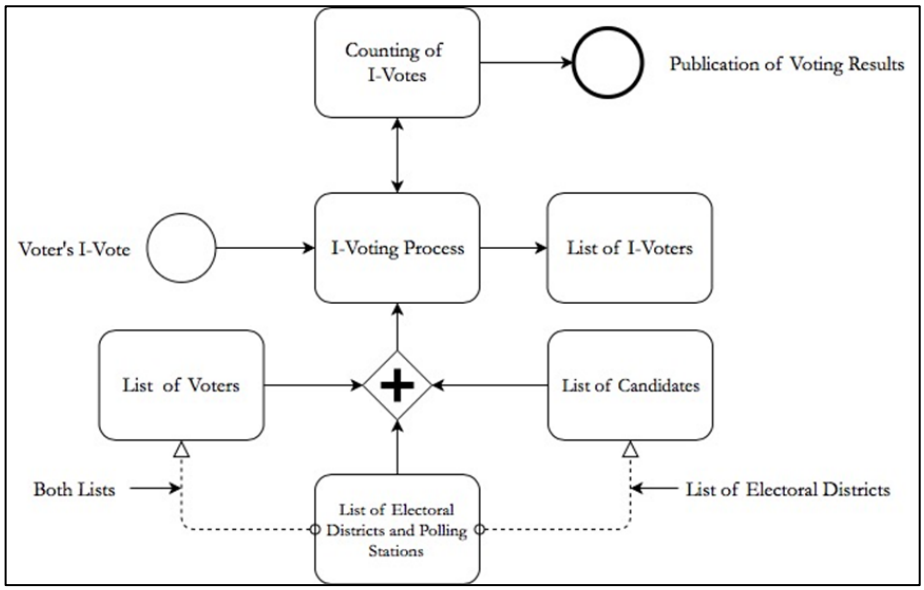
As principais etapas em qualquer processo democrático são (ESTONIA, 2017, p. 05):

a) Declaração da eleição;
b) Registro de candidato;
c) Preparação da lista de eleitores;
d) Votação;
e) Contagem dos votos; e
f) Publicação do resultado da eleição.

No processo eleitoral da Estônia, o pleito é realizado por distritos eleitorais, ou seja, o voto do eleitor é associado ao candidato e partido político correspondente ao distrito eleitoral.

Deste modo, parte inicial do processo de *i-voting* é composto pela correlação das listas de eleitores e candidatos com a lista do distrito eleitoral correspondente, como mostrado na figura abaixo.

Figura 14: Escopo inicial do sistema de i-voting



Fonte: Elaborado pelo autor

5.1.4 Processos e Sub-processos

A pesquisa fez a transcrição dos processos, sub-processos e serviços externos independentes que fazem parte do sistema de votação pela Internet estoniano na Tabela 10.

Cada entidade tem um papel específico de entrada e saída de dados no sistema de *i-voting* que pode ser observado na tabela abaixo (ESTONIA, 2017, pp. 09-12).

Tabela 10: Processos, sub-processos e serviços externos do sistema de i-voting

PROCESSOS E SUB-PROCESSOS	
Voter	Realiza o voto através do *Voter Application.*
Voter Application	Aplicação do sitema de *i-voting* que é executada no computador do eleitor para realizar a escolha do candidato e partido político através da cédula eletrônica para depois criptografá-lo e assiná-lo digitalmente. Após a assinatura digital, o aplicativo exibe um *QR Code* no computador para ser decodificado pelo *Verification Application.*
Verification Application	Aplicação do sitema de *i-voting* executada no *smart device* do eleitor para confirmar o registro do voto na urna digital pela aplicação do servidor *Collector.*
Collector	Servidor de sistema que armazena as cédulas eletrônicas na urna digital e as envia juntamente com os arquivos de registro para o *Processor.*
Collection Application	Aplicação do *Collector* para registro e gravação na urna digital. Utiliza serviços de servidores externos.
Processor	Aplicação do sitema de *i-voting* que: a) verifica as assinaturas digitais e a integridade das cédulas eletrônicas recebidas do *Collector*; b) anula os votos digitais repetidos; Atualiza a lista de eleitores; c) classifica as cédulas por distritos eleitorais; d) remove as assinaturas digitais; e e) (re)embaralha os votos eletrônicos anonimizados pela criptografia de chave privada para enviá-los para o servidor de totalização.
Processing Application	Aplicação do *Processor* na realização das tarefas e pode ser auditado pela aplicação *Auditor.*
Mixer	É o *Hardware Security Module (HSM)* que utiliza a chave privada para criptografia de chave privada e misturar as cédulas eletrônicas anonimizadas que são enviadas pela aplicação *Processor.*
Mixing Application	Ferramenta do *Mixer* para a realização das tarefas e o cálculo para checar se o número de votos no *input* e *output* são correspondentes.
Tallier	É o servidor de contagem das cédulas eletrônicas que está conectado com o *HSM* no ambiente *off-line.*
Auditor	Realiza a auditoria das operações do *Tallier* e *Mixer.*
Audit Application	Sistema do *Auditor* que faz a verificação matemática das operações através do *Processor.*
Client Desk	É um ator no sitema de *i-voting* que auxilia o eleitor com problemas de autenticação no sistema de *i-voting.*
Identification Service	Sistema externo utilizado para identificar o eleitor.
Signature Service	Sistema externo para confirmar e validar a assinatura do eleitor.
Registration Service	Auxilia o *Collector* no registro dos votos recebidos na urna eletrônica ou *i-ballot box.* Após o final do período de votação, o *Registration Service* encaminha os registros para o *Processor.*

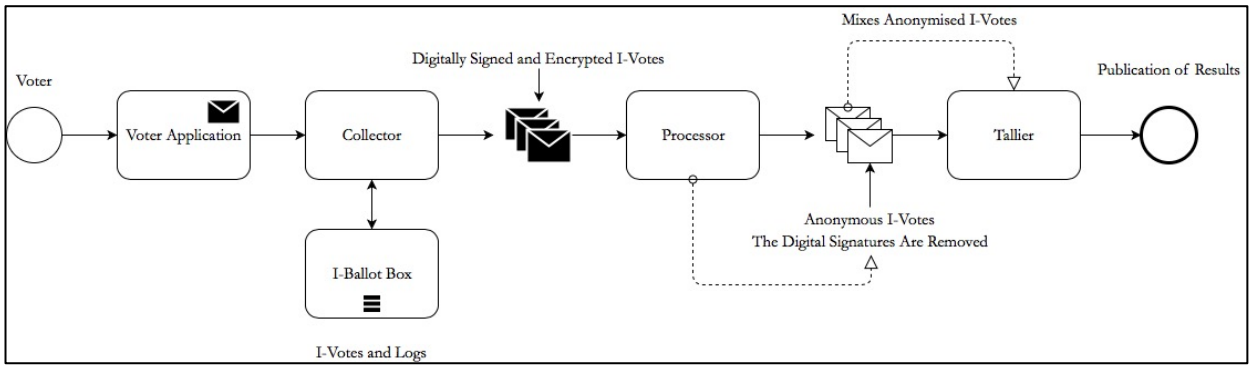
Fonte: Elaborado pelo autor

5.1.5 Partes Principais do Sistema de I-voting

Segundo o documento *IVXV - ÜK - 1.0* (ESTONIA, 2017, p. 09), o sistema de votação pela Internet é composto por quatro elementos principais:

a) Eleitor ou voter - *Voter Application*;
b) Servidor de sistema denominado *Collector*;
c) Processamento de dados chamada *Processor*; e
d) Criptografia com chave privada e totalização *Tallier* - (re)embaralhamento das cédulas eletrônicas anonimizadas pelo *Mixer*.

Figura 15: Partes principais do sistema de i-voting



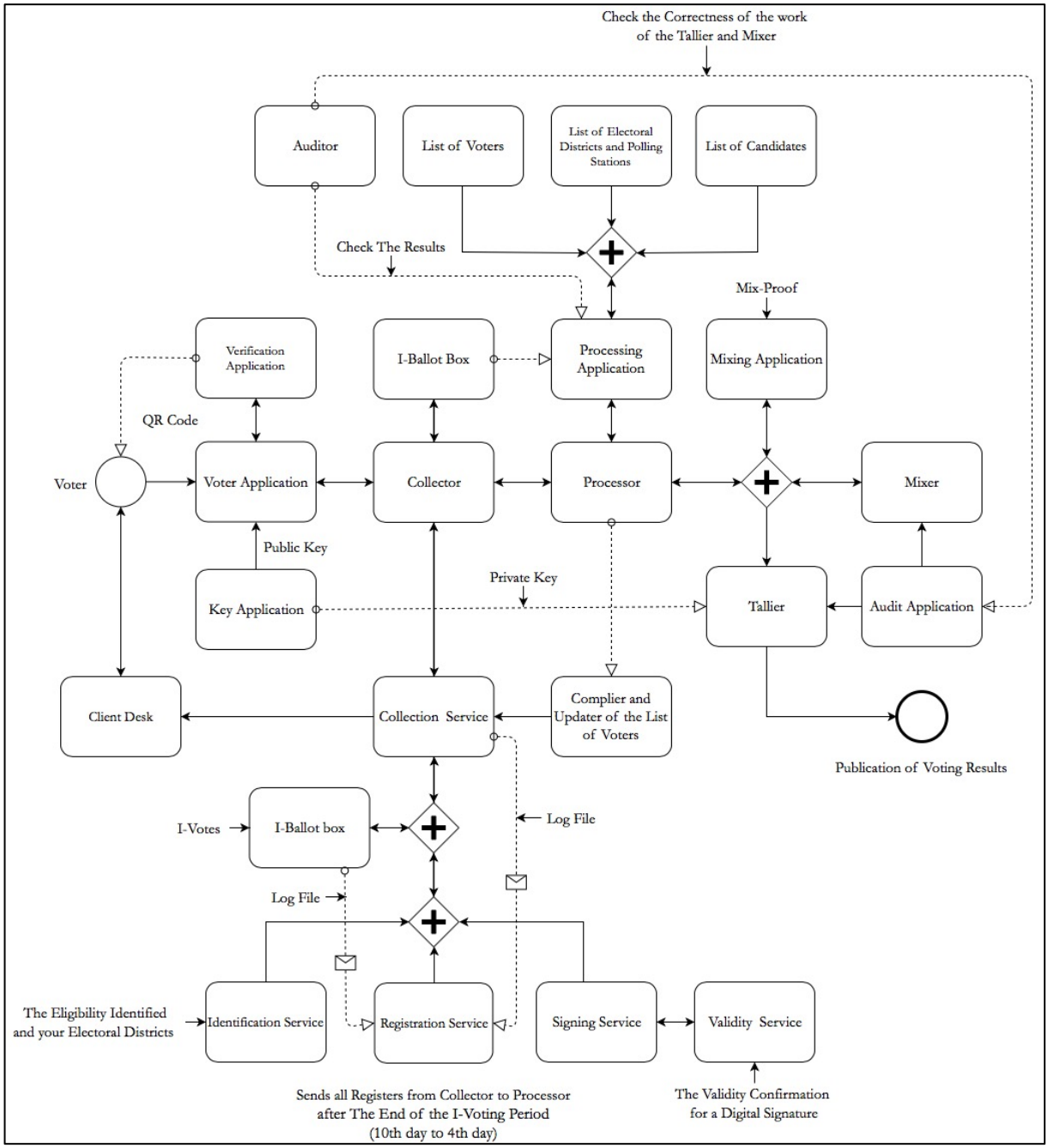
Fonte: Elaborado pelo autor

5.1.6 Visão Geral do Sistema de I-voting

Os diagramas correspondentes da Tabela 10 estão na visão macro do sistema de *i-voting* estoniano diagramado na Figura 16. No decorrer do trabalho, a pesquisa detalha as partes e o fluxo das informações no processo de *i-voting*:

a) Identificação do eleitor, votação (envio das cédulas eletrônicas);
b) Envio da cédula eletrônica para a urna digital durante o processo de votação (registro do voto eletrônico na base central de dados);
c) Verificação da integridade da cédula eletrônica;
d) Controle e preservação de apenas uma cédula eletrônica do eleitor na votação múltipla;
e) Controle dos eleitores na votação paralela;
f) Processo de anonimização das cédulas eletrônicas (remoção da assinatura digital e do *time-mark* ou *time stamp*);
g) Embaralhamento das cédulas anonimizadas;
h) Contagem das cédulas eletrônicas anonimizadas; e
i) Infraestrutura de servidores de dados.

Figura 16: Sistema de i-voting da Estônia



Fonte: Elaborado pelo autor

5.1.7 Identificação do Eleitor

De acordo com o governo estoniano (2017, pp. 13-18) a identificação do eleitor estoniano é realizada pela certificação de autenticação *(PIN1)* que corresponde ao programa *Voter Application* e a certificação de assinatura digital *(PIN2)* vinculada ao programa *Digital Signature – ID,* ambos para o processo de criptografia com chave pública.

Logo, a pesquisa conclui que o processo de identificação do eleitor estoniano não é autenticação de dois fatores ou verificação em duas etapas.

Em breve análise *in loco*, o eleitor escolhe um tipo de autenticação, por exemplo, *ID card, Digi-ID* ou *Mobile ID* e, após a identificação no sistema, o *Voter Application* exibe do lado esquerdo da tela as opções de votação que são agrupadas por distrito eleitoral, candidato e partido político. A lista exibida é enviada pelo sistema denominado *Collection*.

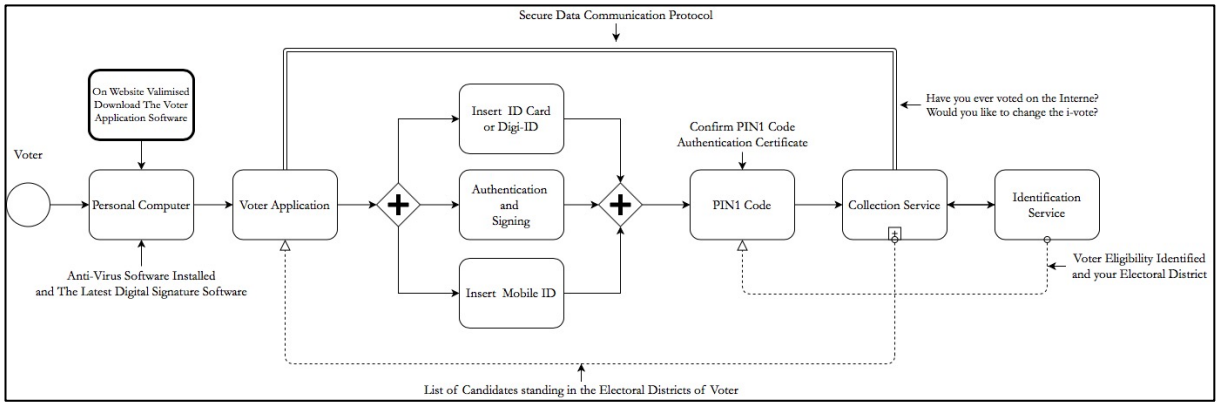
O *Collection Service* verifica se o eleitor já realizou o voto pela Internet, e em caso positivo, o eleitor é notificado para, opcionalmente, continuar a lançar um voto novo ou realizar a verificabilidade de registro do voto anterior pelo programa *Verification Application.*

A pesquisa observa que a cédula eletrônica que pode ser registrada por inúmeras vezes no sistema de votação pela Internet no período *on-line*, mas não produz contra-prova ou recibo de que a cédula anterior é eliminada automaticamente pelo sistema de *i-voting* durante o período *off-line* de processamento das cédulas eletrônicas.

É percebido também pela investigação que o uso de serviços externos ao sistema de votação pela Internet pode aumentar o risco de vulnerabilidades mesmo que as autoridades do processo de votação afirmem que a aplicação *Voter Application* estabelece conexão segura através do protocolo de comunicação de dados com o sistema *Collection Service* e confirmar a autenticação do eleitor pelo serviço externo *Identification Service*.

Neste caso, o eleitor confia no sistema de que não haverá falhas no *software* e má conduta nas pessoas que estão por detrás da arquitetura do sistema de *i-voting*.

Figura 17: Etapa de identificação do eleitor no sistema de i-voting



Fonte: Elaborado pelo autor

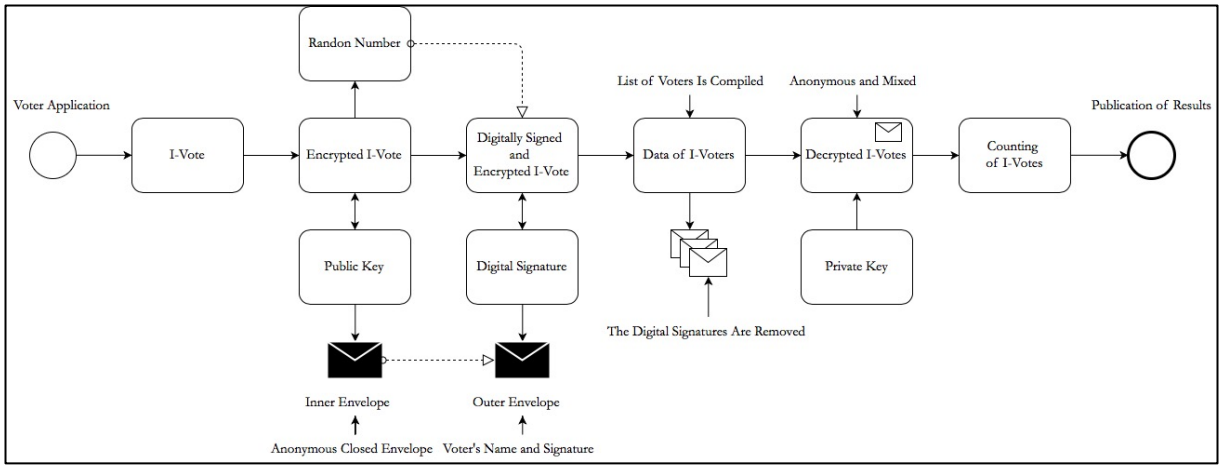
5.1.8 Par de Chaves Criptográficas: Pública e Privada

O par de chaves criptográficas estão sob responsabilidade do *NEC, SEO* e membros, sendo que a construção algorítmica e tecnológica está a cargo do *RIA* e as empresas *Smartmatic-Cybernetica.*

A chave pública é utilizada para criptografia da cédula eletrônica no "esquema de envelope" e a criptografia com a chave privada somente é ativada para abertura das cédulas eletrônicas após o processo de retirada dos dados pessoais – anonimização, e durante a contagem de cédulas eletrônicas no ambiente *off-line*. Após trinta dias do resultado da eleição, a chave privada torna-se sem efeito permanente.

Em breve síntese, a figura abaixo mostra como funciona o par de chaves pública e privada no sistema de votação pela Internet.

Figura 18: Chaves criptográficas do sistema de i-voting



Fonte: Elaborado pelo autor

5.1.9 Integridade da Cédula Eletrônica

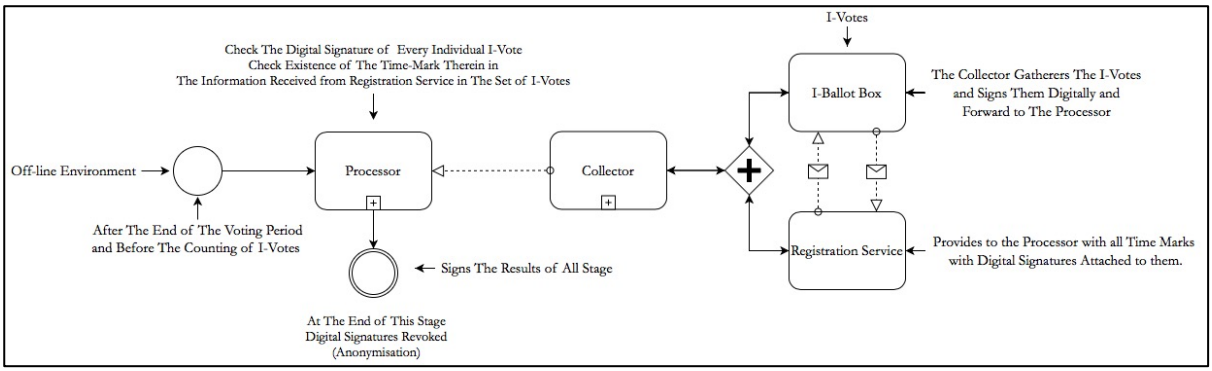
A análise de integridade de cada cédula eletrônica é realizada após o término do período de votação pela Internet.

Neste caso, o *Processor* recebe do serviço externo *Registration Service* os *time-marks* com as assinaturas digitais que correspondem aos votos de cada eleitor. Na sequencia, o *Processor* compara se a quantidade de cédulas eletrônicas registradas na *i-ballot box* são correspondentes aos *time-mark* do *Registration Service.*

É importante mencionar que a análise de integridade das cédulas eletrônicas ocorre antes da anonimização, pois é procedimento necessário para desvincular a conexão da chave criptográfica pública com o voto pela Internet.

Basicamente é a análise de *logs* que o *Collector* e *i-ballot box* enviam para o *Registration Service* validar a integridade dos votos no sistema de *i-voting*[107].

Figura 19: Integridade da cédula eletrônica no sistema de i-voting



Fonte: Elaborado pelo autor

5.1.10 Anulação, Anonimização e Mixer

O sistema de *i-voting* opera de duas formas: semi-automático e automático. Parte do processo semi-automatizado está relacionado com o processo de *annulment of repeated or double i-votes*, que ocorre durante a votação paralela.

A votação paralela é quando o eleitor registra dois votos dentro do período eleitoral: um voto em cédula de papel e outro voto cédula eletrônica.

Durante *dark days* que é do 3° ao 1° dia da eleição antes do dia oficial, a autoridade responsável pela eleição produz um arquivo de extensão *portal document format (pdf)* que contém os eleitores classificados por zonas eleitorais que registram votos pela Internet, mas sem infringir o sigilo do voto.

---

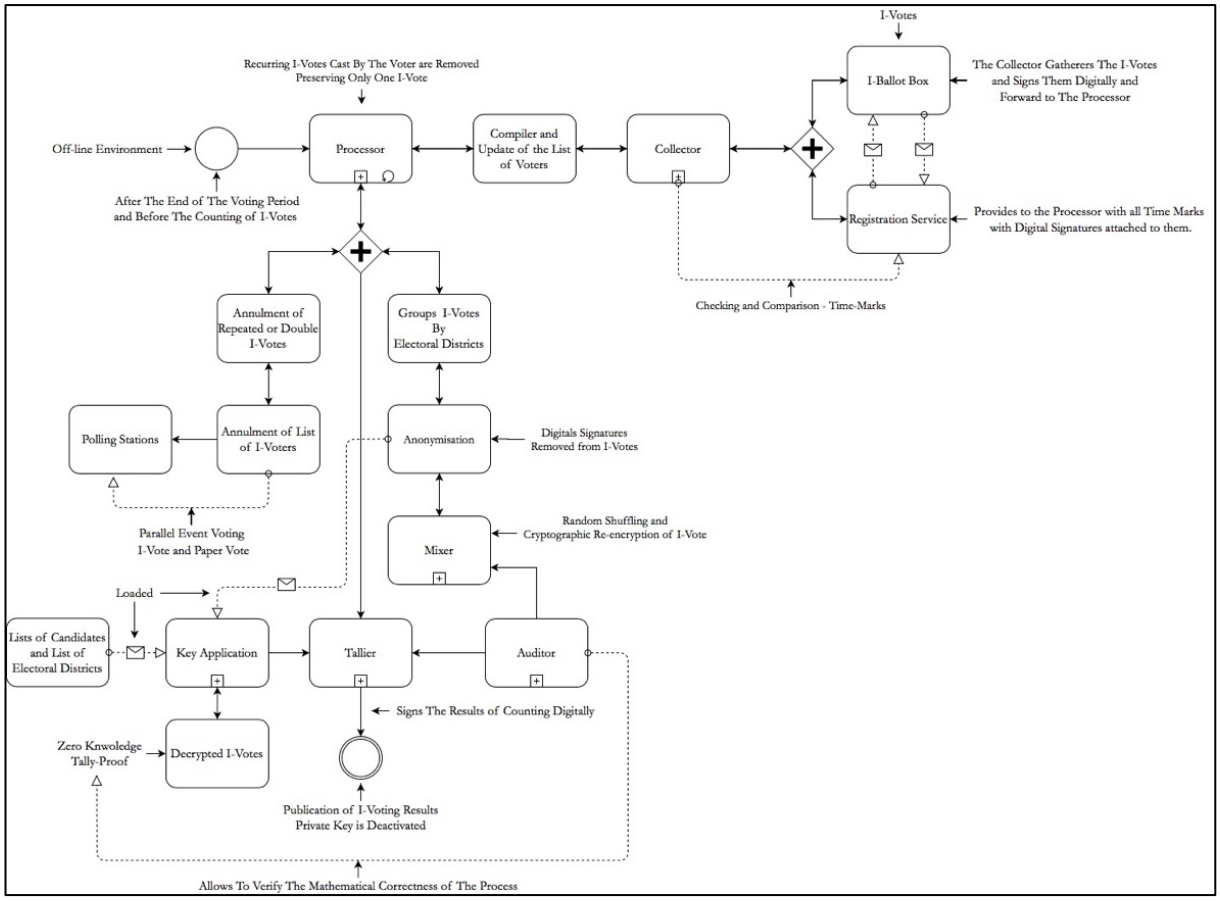
[107] Cf. Figura 16.

Na sequencia o arquivo é encaminhado para as respectivas *polling stations* ou zonas eleitorais para que cada voto duplicado seja identificado para ulterior exclusão da cédula eletrônica em razão do princípio da primazia da cédula em papel.

Para a pesquisa o procedimento de verificação da votação pararela é suscetível de falhas e vulnerabilidades internas, pois a eleição está sob a responsabilidade de agentes que podem agir maliciosamente com as informações disponibilizadas no arquivo com extensão *pdf*.

Além disso, o fator exógeno é altamente arriscado porque o arquivo com extensão *pdf* é enviado para as zonas eleitorais por correio eletrônico ou sistema proprietário do governo podendo ser interceptado por um agente contrário aos preceitos éticos em processos eleitorais.

Figura 20: Anulação, anonimização e mixer das cédulas eletrônicas



Fonte: Elaborado pelo autor

5.1.11 Envio e Verificação E2E da Cédula Eletrônica

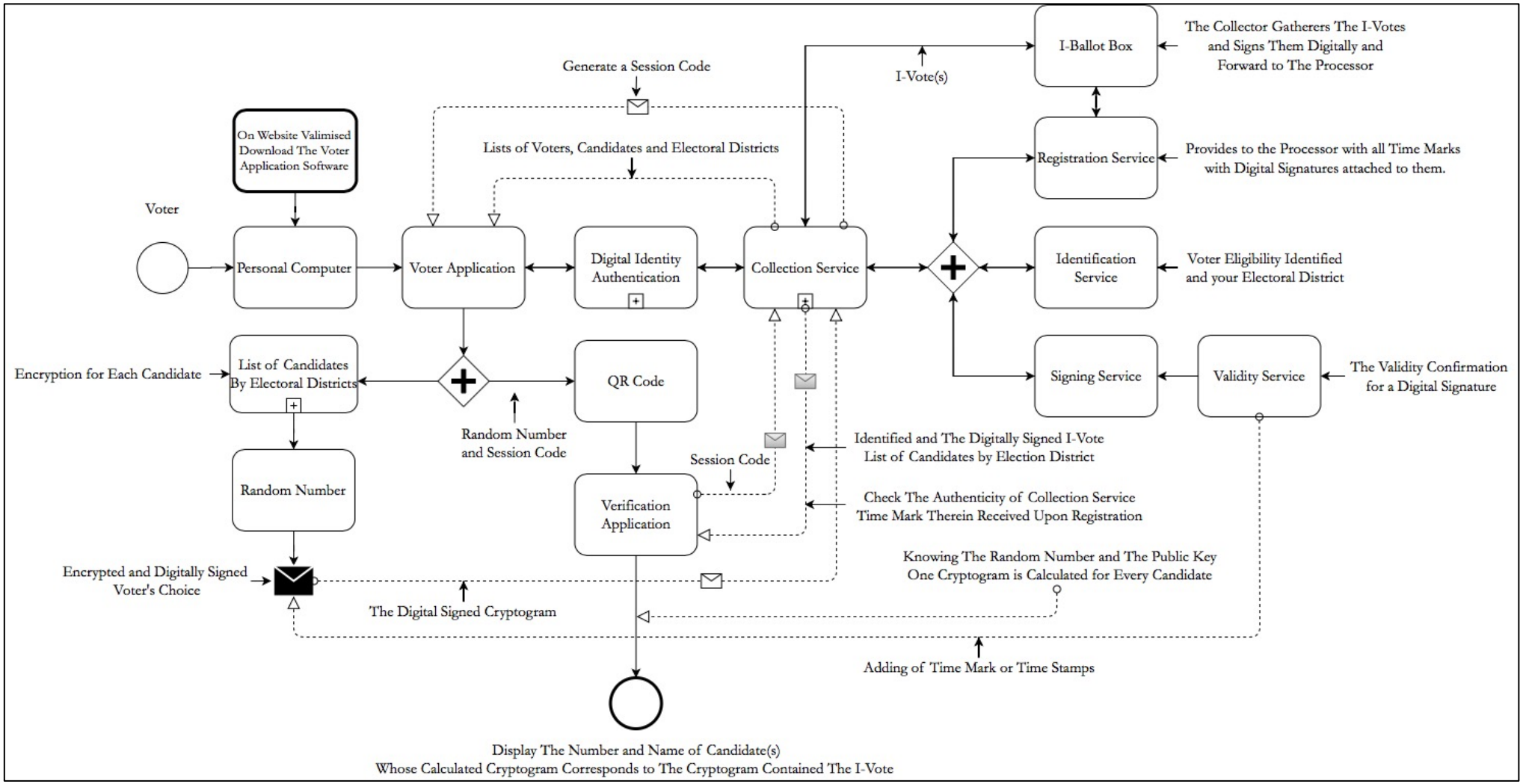
Para a pesquisa a Figura 21 é uma das mais importante da tese porque retrata o modelo de verificabilidade de ponta a ponta atual no sistema de votação pela Internet.

De acordo com o *NEC* (ESTONIA, 2017, pp. 15):

a) O envio da da cédula eletrônica é realizado pelo eleitor que faz a sua escolha entre os candidatos exibidos na tela do computador pelo *Voter Application*.
b) O Voter Application criptografa cada escolha do eleitor na cédula eletrônica – *digital signed cryptogram*, sendo gerado um número randômico que corresponde à chave pública – *random number*. Na sequencia, o eleitor assina digitalmente a cédula eletrônica criptografada e a envia ao *Collection Service* para gerar o *session code.*
c) O *Collection Service* verifica a existência do eleitor na lista de eleitores e anexa a cédula eletrônica com a confirmação temporal de validade - *time-mark*.
d) O *Collection Service* faz a requisição ao sistema externo *Registration Service* para (re)utilizar o *time-mark* e registrar a cédula eletrônica na urna digital ou *Internet ballot box (i-ballot box)*.
e) No estágio de verificação, o *Collection Service* notifica o eleitor que o registro da cédula eletrônica está confirmado *(random number)* e *(session code)* por meio do *QR Code* visualizado por um *smart device*.
f) Durante a leitura pelo *smart device*, o criptograma de cada candidato e partido político exibido no formato de *QR Code* é recalculado pela aplicação *Verification Application* para retornar com o conteúdo do voto eletrônico para o eleitor.

A verificação *E2E* é limitada e ocorre três vezes a cada trinta minutos. A pesquisa observa que qualquer modificação na cédula eletrônica a partir do *Processor* que está no ambiente *off-line,* não é verificada pelo eleitor.

Figura 21: Etapas de envio e verificação do registro da cédula eletrônica no sistema de i-voting



Fonte: Elaborado pelo autor

5.1.12 Infraestrutura dos Servidores de Dados

Em concordância com a observação da pesquisa *in loco* e as observções de Springall, Finken, Durumeric *et al.* (2014, pp. 02-03) durante as eleições de 2013 na Estônia, a arquitetura e a infraestrutura de servidores são semelhantes*,* inclusive os procedimentos da administração pública para os pleitos eleitorais que é abordado no capítulo.

A investigação observa que o processo de votação pela Internet é configurado de duas formas, a etapa *on-line* de coleta dos votos digitais e a etapa do processamento e contagem das cédulas eletrônicas no ambiente *off-line*, isto é, o eleitor não tem acesso e conhecimento do tratamento da cédula eletrônica após o período de votação pela Internet.

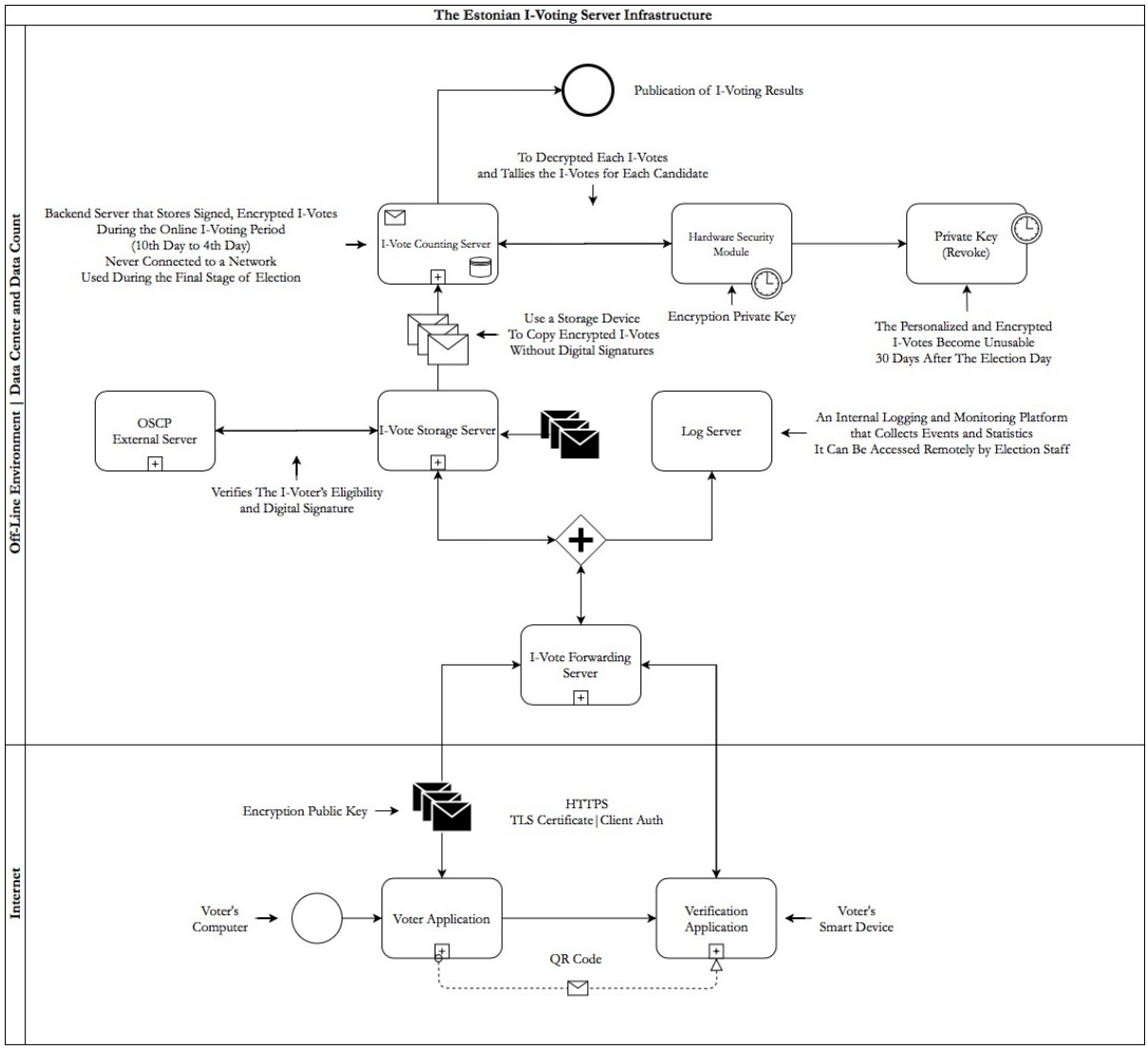
No sistema estoniano de votação pela Internet, o sigilo da votação é também garantido com um algoritmo de criptografia assimétrica que é usado para que as cédulas criptografadas com a chave pública possam através do *Tallier* serem criptografadas pela chave privada e, consequentemente, anonimizadas.

Por isso, o sistema de *i-voting* adiciona um *random number* durante o processo de votação, tornando-se necessário para garantir que os criptogramas de cada cédula sejam diferentes para o mesmo candidato e partido político.

O único aspecto manual no ambiente *off-line* é a gravação das cédulas eletrônicas em dispositivo de mídia digital ou *flash memory card* para que os votos eletrônicos sejam inseridos no *Hardware Security Module (HSM)* que corresponde a chave privada. O *HSM* somente é ativado com a presença das autoridades *NEC, SEO, RIA* e demais membros e observadores eleitorais.

A Figura 22 mostra a infraestrutura de servidores do sistema de votação pela Internet.

Figura 22: Infraestrutura de servidores de dados do sistema de i-voting



Fonte: Elaborado pelo autor

5.1.13 Como Votar pela Internet?

O *modus operandi* para o eleitor votar pela Internet é simples. Primeiro, só eleitores regulares podem votar. Para que isto seja obedecido, a infraestrutura do *ID Card* estoniano é o elemento essencial para garantir que o eleitor é autêntico e único no processo eleitoral.

Na Estônia é o *ID Card* ou um aparelho celular com cartão *SIM* para os certificados de autenticação e assinatura digital com o *software Mobile-ID,* que fornece a tecnologia como parte do processo de *i-voting - knowledge-based key shares* (nome de usuário, senha e *PIN*). Os certificados de autenticação *(PIN1)* e assinatura digital *(PIN2)* são executados internamente por chaves criptográficas públicas do tipo *RSA* no *chip* do cartão em concordância com o aplicativo *Voter Application* (CYBERNETICA, 2018, pp. 11-16).

O eleitor também pode verificar a cédula eletrônica no servidor central de dados pelo aplicativo instalado no seu *smart device* com o auxílio da câmera para ler o *QR Code.* No *QR Code* há um criptograma assinado digitalmente que contém o *random number* e o *session code*, que correspondem às escolhas do eleitor (número, candidato e partido político).

A quantidade de verificação do voto digital via *QR Code* na base de dados é limitada pelo *NEC* – três vezes a cada trinta minutos, e não abrange os processos após o período de votação *on-line*, ou seja, a interação entre o sistema de *i-voting* e o eleitor é durante a coleta das cédulas eletrônicas, operando à parte o processamento, a contagem e a publicação do resultado da votação no ambiente *off-line.*

É importante mencionar que as cédulas eletrônicas são contadas separadamente das cédulas em papel.

Após o encerramento do período no dia oficial da eleição é realizada a contagem e totalização das cédulas eletrônicas e cédulas em papel para a publicação do resultado.

Os processos administrativos, *Prepare Software*[108] e *Activities Just Prior I-Voting Period*[109] são comentados com mais detalhes no trabalho de Iova (2019, pp. 34-80), como também, as atribuições dos atores da administração pública e privada responsáveis pelo pleito eleitoral.

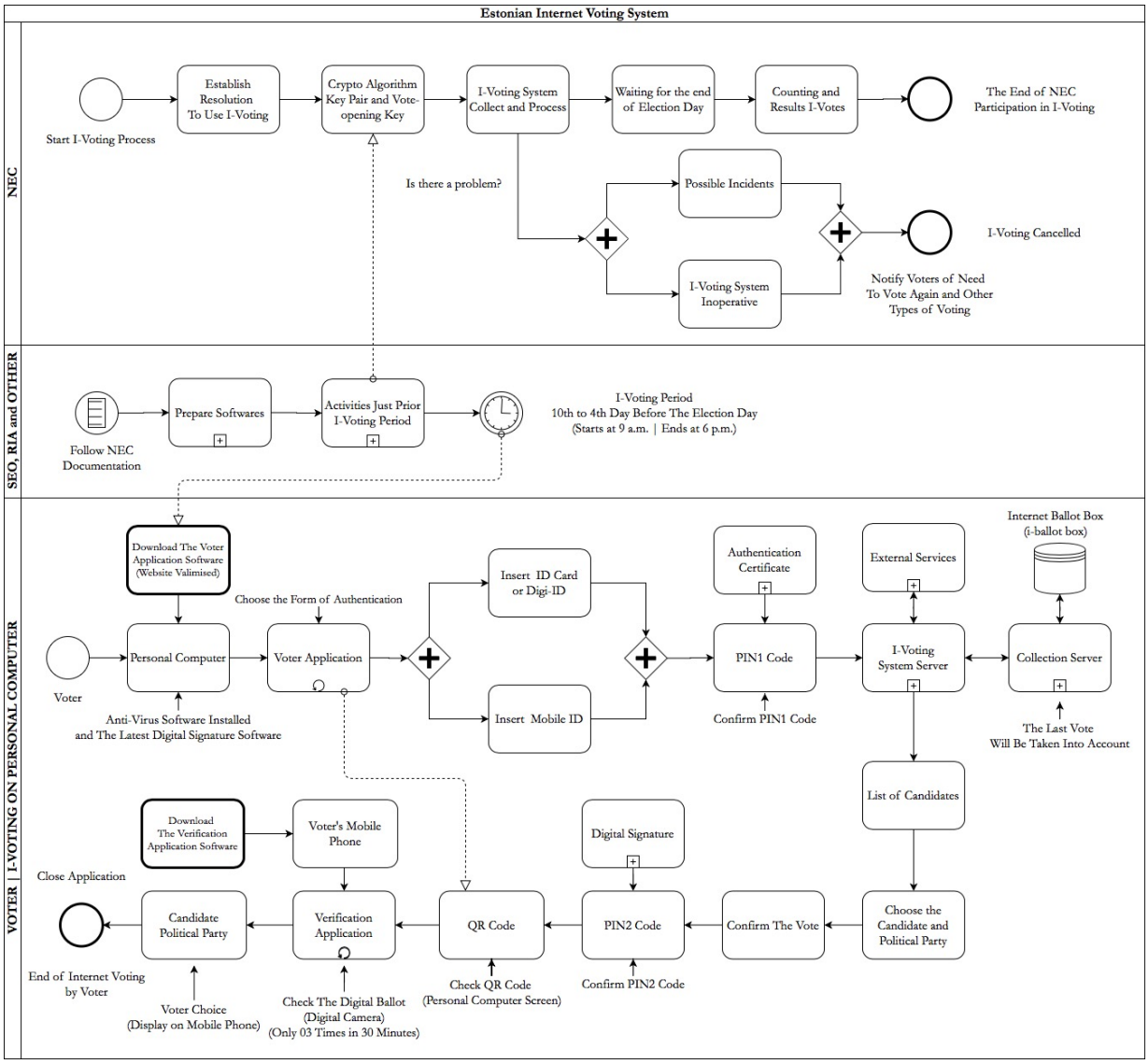
É importante ratificar novamente que a pesquisa presume que o ambiente está livre de agentes e programas maliciosos no sistema de votação pela Internet.

---

[108] *Decide and Approve Information Security Policy; Decide and Approve Electronic Voting Protocol Suite; Decide and Approve Technical Guidelines; Decide and Approve Applicable OS for the voting app; Create and Update and Develop the voting app; Create and Update and Develop the vote-check app; Organise resolution of incidents hindering i-vote; Decide and Approve Testing; Organise audit; Audit; Publish Report on the Testing Results.*

[109] *Create Encryption Key and Vote-Opening Key; Distribute 2.1 Keys (NEC); Distribute 2.1 Keys (SEO); Publish apps and Publish authenticity information.*

Figura 23: Modus operandi do processo de votação no sistema de i-voting



Fonte: Elaborado pelo autor[110]

[110] A figura é inspirada no rascunho elaborado pela pesquisa com o doutorando Marlon Freire da Universidade do Porto na Biblioteca Nacional da Estônia em 2019.

6. BLOCKCHAIN TECHNOLOGY FOR END-TO-END VERIFIABLE ELECTIONS ON PART OF ESTONIAN INTERNET VOTING SYSTEM

"Those who can imagine anything, can create the impossible"

Alan Turing

Durante a investigação *in loco* na Estônia, a pesquisa empreende que os primeiros passos para conjecturar o cenário inicial para a propositura da tese é analisar a infraestrutura de interoperabilidade do *X-Road* com a camada de aplicação do sistema de *i-voting* para, na sequencia, expor a abordagem da verificação *E2E* com a tecnologia *blockchain.*

6.1 AMBIENTE X-ROAD

Como já foi explicado no Capítulo 5, o ambiente de votação pela Internet na Estônia é dividido em duas partes: a) *on-line* (acesso, criptografia com chave pública, coleta e verificação das cédulas eletrônicas); e b) *off-line* (anonimização, criptografia com chave privada, contagem, totalização e publicação das cédulas digitais). Além disso, o sistema de *i-voting* funciona somente na camada de aplicação da plataforma *X-Road.*

Neste sentido, a pesquisa opta por analisar primeiro a arquitetura *X-Road* porque ela pode oferecer a infraestrutura para implementação de uma aplicação com tecnologia *blockchain.*

> O *X-Road* é uma solução de camada de troca de dados com código aberto que permite que as organizações troquem informações pela Internet. É uma camada de troca de dados distribuída gerenciada centralmente entre sistemas de informação e fornece uma maneira padronizada e segura de produzir e consumir serviços. O *X-Road* garante a confidencialidade, a integridade e a interoperabilidade entre os envolvidos no processo de troca de dados na plataforma (ESTONIA, 2018)[111].

No entanto, a investigação observa que a infraestrutura do ambiente de *e-governance* entre o setor público e privado, baseada em sistemas de dados distribuídos e protegida por

[111] Informações colhidas durante o *Nordic Institute for Interoperability Solutions (NIIS) 2018. X-Road implements a set of common features to support and facilitate data exchange. X-Road provides the following features out of the box: a) address management; b) message routing; c) access rights management; d) organization level authentication; e) machine level authentication; f) transportation layer encryption; g) time-stamping; h) digital signature of messages; i) logging; and j) error handling.*

servidores de segurança do *X-Road* – conforme a figura 7, não é a arquitetura ideial para propor na tese:

> O único meio viável para implementar a tecnologia *blockchain* na plataforma *X-Road* é na camada de segurança para manter a sua estrutura descentralizada de dados. Consequentemente, o desafio aqui não está concentrado totalmente na criptografia computacional, mas na engenharia para criar um serviço confiável, escalável e sem interrupções (SILVA, 2018, p. 352).

Muito embora o governo estoniano tenha afirmado que a partir de 2012 alguns serviços utilizem a tecnologia *blockchain,* tal afirmação é duvidosa por razões técnicas e informativas, pois a dubiedade e a análise *in loco* reforçam que a utilização da tecnologia *blockchain* na plataforma *X-Road* é tecnicamente impraticável, seja ela baseada nas acepções de Satoshi Nakamoto (2008) ou nas derivações existentes nos dias de hoje.

Durante o contato com especialistas que atuam direta e indiretamente com a plataforma *X-Road*, há divergências de opiniões sobre o uso real ou uma implementação possível na arquitetura. Para a pesquisa a tecnologia *blockchain* tem seus desafios, principalmente, com a performance e escalabilidade, pois são fatores que influenciam bastante na sua implementação em sistemas como o *X-Road*.

Por fim, abordar esse cenário inviabiliza a contribuição da tese para o sistema de *i-voting* da Estônia. A pesquisa se concentra na abordagem do modelo independente de sistema de verificação de ponta a ponta com a tecnologia *blockchain.*

6.2. BLOCKCHAIN E VERIFICAÇÃO E2E

Antes de iniciar a construção da abordagem sobre a verificação *E2E* com a tecnologia *blockchain*, é necessário para a pesquisa discorrer sobre alguns pontos relevantes nesse processo de investigação para esclarescer o que é contemplado na tese e, consequentemente, os desafios que a própria tecnologia *blockchain* impõe para o resultado da pesquisa.

6.2.1 Identidade Eletrônica

No ínicio dos anos 2000, a confiança nos sistemas de votação era baseada no conceito da certificação (VINKEL e KRIMMER, 2016, p. 21). Contudo, a partir de 2002, o governo estoniano aposta na identidade eletrônica como fator preponderante para construção da confiança do seu ambiente digital na plataforma *X-Road* que, consequentemente, torna-se o pilar para o sistema de *i-voting.*

Com os passar dos anos, a literatura do gênero demonstra que, na maioria dos trabalhos, a certificação é substituída pelo conceito da verificabilidade como o fator principal para garantir e potencializar a confiança nos sistemas de votação, especialmente, os processos democráticos com o uso da Internet (SILVA, 2018, p. 351).

Não é o objetivo da pesquisa tratar da autenticação e certificação da identidade eletrônica dos eleitores no processo de votação pela Internet, pois o objetivo não é certificar de que o eleitor é ele próprio durante o processo de *i-voting.*

Para a pesquisa o problema com o *ID Card* no ano de 2017 traz dubiedade para eleições futuras em relação a arquitetura e a infraestrutura da identidade eletrônica estoniana.

Nos estudos anteriores do Capítulo 2, a pesquisa observa trabalhos em que a tecnologia *blockchain* é utilizada para ampliar a transparência e a verificabilidade pública nos sistemas de votação a partir da autenticação do eleitor no *ledger*. Todavia, a elegibilidade e a privacidade dos eleitores no *ledger* é uma superação a ser considerada na abordagem da proposta do sistema de *i-voting* com a tecnologia *blockchain* porque são necessárias muitas transações para atribuir a elegibilidade de todos os *nodes*, ocasionando um aumento de volume de dados e baixa performance na escalabilidade da rede.

6.2.2 Privacy by Desing

Para a pesquisa é importante que o projeto esteja de acordo com o fundamento da privacidade do eleitor, pois é necessário evitar qualquer meio de rastreamento do eleitor na cadeia de blocos para ocultar qualquer tipo de associação à sua identidade e conteúdo do voto eletrônico durante o processo de votação pela Internet.

Conjecturando tecnologias *blockchain* durante a investigação científica no Capítulo 2 e, conforme a metodologia acertada no Capítulo 3, a opção pelo sistema algoritmo *Monero* se torna a mais adequada para se construir uma cadeia de blocos *public permissioned* porque além de possuir consenso distribuído, o algoritmo oferece técnicas tecnologia anônima e irrastreável.

Para atingir o anonimato ou a privacidade, o *Monero* utiliza a técnica da criptografia de assinatura em anel ou *ring signatures* - um esquema de assinatura criptográfica anônima para assinar transações, que ofusca o remetente, o destinatário e o conteúdo do bloco na cadeia, tornando impraticável o rastreamento entre as partes envolvidas e suas respectivas transações na rede *blockchain.*

Por fim, no *Monero* ainda há a compatibilidade com sistemas operacionais para *laptops* e *smart devices* presentes no mercado, ampliando, assim, a margem de utilização destes dispositivos no processo de votação pela Internet.

6.2.3 Performance e Security by Desing

Também não é o propósito da investigação científica enviar as cédulas eletrônicas para a cadeia de blocos por razões técnicas que envolvem o armazenamento, a escalabilidade e o desempenho do sistema, conforme analisado no Capítulo 2. Isto porque o envio de uma cédula eletrônica para cada bloco pode também afetar a *performance* do sistema.

A limitação de tamanho e frequência dos blocos na cadeia é um problema comum da tecnologia *public permissionless blockchain* porque torna a quantidade de transações por segundo processadas no *ledger* muito baixa.

> Segundo Satoshi Nakamoto, o armazenamento na cadeia de blocos pode ultrapassar aproximadamente cento e cinquenta *gigabytes*, tornando inviável armazená-lo em todos os nós da rede *blockchain,* prejudicando a escalabilidade e desempenho de qualquer sistema (NAKAMOTO, 2008, p. 05).

A pesquisa, neste sentido, opta em armazenar dois registros da cédula eletrônica no bloco do eleitor na aquitetura *E2E Blockchain I-Voting* que opera segundo o algoritmo *Monero* de forma customizada, pois a média de mineração no algoritmo do *Monero* são de dois minutos para cada transação válida.

Segundo Solvak e Vassil (2016, p. 115), o eleitor estoniano leva em média noventa segundos para votar pela Internet. Neste caso, a pesquisa pode calcular a média de três minutos e quarenta segundos de processamento para cada eleitor.

O desenho da arquitetura *E2E Blockchain I-Voting* fortalece o grau de segurança das informações em parte do sistema de *i-voting.* Não obstante, a tecnologia *blockchain* por detrás da abordagem da pesquisa traz um conjunto de ferramentas computacionais de design para a segurança da informação.

6.2.4 Poder de Mineração da Blockchain

O desafio da mineração em *blockchain* são as *farms* ou fazendas de mineração existentes, como por exemplo, os centros computacionais na República da China para as criptomoedas de *bitcoin* que podem influenciar de forma negativa a cadeia de blocos da rede (NAKAMOTO, 2008, p. 06). Não obstante, é elementar dizer que existe a possibilidade desse

fato também ocorrer para pleitos eleitorais realizados pela Internet, pois com base em provas sólidas, um fato desse tipo incide em uma agressão diplomática, ensejando, assim, em possível conflito cibernético entre os dois países. Na linha do direito internacional, o interesse em manipular eleições tradicionais em outros países não é algo novo, tornando a prática pela Internet real e iminente.

De outra parte, com o uso da tecnologia do *Monero,* as chances de um fato desse ocorrer são bastante inferiores ao modelo tradicional que utiliza tecnologia *blockchain*, pois no *Monero* (2019)*,* o algoritmo de mineração - *Random X,* é atualizado para evitar as *farms* de utilizar da computação customizada *ASICs* para manipular a regra de consenso do *ledger*.

6.2.5 Abordagem de Verificação E2E com Monero

Já foi mencionado na pesquisa o consenso de que sistemas de votação pela Internet precisam fornecer algum tipo de verificabilidade de ponta a ponta para consolidar a confiança no processo eleitoral, seja ele individual, universal ou múltiplo.

A pesquisa entende que a verificabilidade individual é confiável desde que o eleitor consiga acompanhar o processo de ponta a ponta. O aspecto da verificabilidade individual deve proporcionar uma prova de confiança ao eleitor, isto é, evidenciar que a cédula eletrônica está armazenada e processada corretamente pelo servidor de dados correspondente ao pleito eleitoral. Por exemplo, o servidor de dados armazena a cédula e gera um tipo de recibo digital que contém identificadores do local de armazenamento e processamento no sistema de votação.

No caso do modelo estoniano de verificação pela Internet, é possível apenas evidenciar pela aplicação *Verification Application* que a cédula eletrônica está registrada no servidor central de dados, tornando o processo parcialmente verificável durante e após o período de votação pela Internet, conforme é mencionado na Figura 3.

Apesar do governo estoniano seguir as recomendações da *OSCE/ODIHR* (2013, p. 68), o eleitor não consegue visualizar o estado do seu voto pela Internet até o estágio final de verificação da segurança das informações contidas na cédula eletrônica porque está no ambiente *off-line,* conforme Figuras 1 e 3, e isto enfraquece o elo de confiança no sistema de *i-voting* da Estônia.

6.3. VALIDAÇÃO DA PROPOSTA

A pesquisa traça o cenário dentro do *E2E Blockchain I-Voting* para explicar como a arquitetura funciona de forma independente com o sistema de *i-voting* da Estônia. É importante enfatizar que somente parte do sistema de *i-voting* estoniano é abordado pela pesquisa com relação a verificação ponta a ponta do voto eletrônico.

A abordagem proposta pela investigação acadêmica consegue resolver o dilema do anonimato, integridade e transparência no processo de votação pela Internet estoniano, contribuindo visivelmente para fortalecer os laços de confiança entre o eleitor e demais atores do pleito eleitoral pela Internet.

6.3.1 Anonimato

No sistema de *i-voting* estoniano, apesar do descobrimento de problemas no *chip* de autenticação do *ID Card* no ano de 2017*,* não é objeto da pesquisa controlar o acesso aos eleitores no processo de votação.

Neste caso, a tecnologia do algoritmo *Monero* oferece a vantagem de não produzir rastros da identidade do eleitor e do seu conteúdo, mesmo que a arquitetura seja implementada como uma tipologia *public permissioned.*

Assim, o dilema do anonimato é garantido ao eleitor estoniano pelos dois sistemas interdependentes que autenticam e validam o acesso público com permissão ao sistema de votação pela Internet.

6.3.2 Integridade

O ambiente de segurança das informações do sistema de *i-voting* também é favorecido porque a segurança da cédula eletrônica é reforçada duplamente.

A primeira etapa deste perímetro de segurança no sistema de votação pela Internet é o registro do *random number* e do *session code* na aplicação *E2E Blockchain I-Voting* que, ulteriormente, é codificado pela aplicação *Block Chain Verification Application* para mostrar via *QR Code* os nomes e números dos candidatos e seus respectivos partidos políticos. É importante ressaltar aqui que, o conteúdo do bloco do *node* também pode ser ocultado para o próprio eleitor com o intuito de evitar qualquer tipo de “voto de cabresto” no processo eleitoral.

A segunda etapa é o arquivo *hash code* gerado pela integração de cada bloco na cadeia distribuída do *ledger*.

Em ambas as etapas, a integridade da cédula eletrônica no sistema de *i-voting* estoniano é garantida e possibilita inclusive um duplo grau de auditoria com as informações disponibilizadas pelo próprio sistema de *i-voting* na aplicação *Auditor* - que faz a verificação das tarefas realizadas pelo *Processor, HSM (zero knwonoledge* e *tally-proof)* e *Mixer,* para checar os resultados providos pelo sistema, conforme exibido pela Figura 16.

6.3.3 Transparência

A pesquisa entende que a transparência no processo de votação pela Internet é a etapa mais desafiadora da proposta porque é nela que a confiança no sistema de votação é abordada com a tecnologia *blockchain* para potencializar o sigilo e a integridade do voto.

No Capítulo 3, a votação paralela, a votação múltipla *(double* e *repeated i-voting)* e o processo de anonimização da cédula eletrônica são analisados em razão da ausência de transparência no processo de *i-voting* porque:

a) Votação múltipla: o eleitor pode votar diversas vezes *on-line* durante o período permitido para inibir a prática da coerção ou voto de cabresto, sendo que apenas o último voto eletrônico é armazenado no servidor de dados pela Internet; e

b) Votação paralela: o eleitor pode registrar o seu voto em cédula de papel ou cédula eletrônica, sendo que o processo de votação permite que o eleitor realize as duas operações. Durante o processamento de anulação no ambiente *off-line*, a cédula em papel tem supremacia em relação ao voto eletrônico como uma forma de evitar a coerção ou voto de cabresto; e

c) Processo de anonimização: as cédulas eletrônicas são transportadas manualmente via *memory flash card* para o dispositivo de criptografia de chave privada *HSM*.

Em vista disso, a pesquisa ratifica que na letra *a)* há ausência da prova de eliminação da última cédula eletrônica registrada para o eleitor; na letra *b)* a operação manual possibilita a

infração do sigilo do voto eletrônico; e na letra *c)* a operação manual possibilita a fraude ou manipulação de agentes maliciosos durante a apuração do resultado da eleição.

A abordagem do modelo novo de aplicação para verificação *E2E* com a tecnologia *blockchain* dá oportunidade de aperfeiçoar a transparência durante o processo eleitoral pela Internet porque fornece a possibilidade:

- Duplo grau de segurança com a rede de *ledger* distribuído; e
- Verificação *E2E* individual, universal e permanente.

O processamento de anonimização das cédulas eletrônicas é o ambiente mais crítico da da pesquisa para a organização do pleito estoniano, pois é uma mudança de cultura tecnológica interna.

Por outro lado, é a recomendação da tese a alteração do ambiente *off-line* (Figura 22) para o ambiente *on-line* para atingir o grau máximo de transparência no sistema de *i-voting.*

Para a pesquisa, neste caso, o dilema da transparência é atendido para a proposta da tese.

6.4. E2E BLOCKCHAIN I-VOTING E BLOCK CHAIN VERIFICATION APPLICATION

A arquiterura *E2E Blockchain I-Voting* e a aplicação *Block Chain Verification Application* são referenciadas na pesquisa em três fases: a) visão geral; b) funcional; e c) aplicação.

No entanto, a investigação não aborda as fases de implantação (iniciação prática) e implementação (execução) por causa do aspecto temporal e limitante da pesquisa e, principalmente, o acesso direto com a infraestrutura física e lógica do sistema de *i-voting* do governo da Estônia.

6.4.1 Visão Funcional e Geral da Arquitetura

Para entender a lógica por detrás da abordagem da pesquisa, adota-se que a plataforma *E2E Blockchain I-Voting - E2E Blockchain API, smart contract, Random X, E2E Block Chain API,* já está em execução com o sistema de votação pela Internet da Estônia.

Com efeito, é apresentada pela pequisa a interação do eleitor com a arquitetura *E2E Blockchain I-Voting* que, consequentemente, também se comunica com a *Public Permissioned*

Ledger para fornecimento e verificação das informações contidas na cédula eletrônica do eleitor que correspondem ao seu voto pela Internet através *Block Chain Verification Application*.

As regras que envolvem a arquitetura são explicadas pela investigação no contexto do período eleitoral, acesso e escopo da aplicação *E2E Blockchain I-Voting.*

Período eleitoral. O período eleitoral no processo de votação pela Internet estoniano é reformulado para se estender até o dial oficial da eleição ou *Election Day*, conforme a figura 4. Desta forma, o eleitor tem acesso às informações da sua cédula eletrônica e tempo maior para votar ou votar novamente pela Internet.

Acesso com permissão pública no *ledger*. A tipologia adotada na arquitetura *E2E Blockchain I-Voting* é *public permissioned ledger* porque o número de *nodes* e *miners* são conhecidos dentro do sistema de votação pela Internet, ou seja, identificados por chaves públicas pela aplicação *Voter Application*.

Bloco "*genesis*" no *ledger*. O bloco "*genesis"* ou o primeiro bloco na cadeia para cada eleitor é criado automaticamente pela arquitetura *E2E Blockchain I-Voting*, sendo que as informações no *ledger* são o *upload* dos arquivos *random number* e *session code* no bloco de cada eleitor.

Controle da dificuldade de mineração. O conjunto de regras de governança do protocolo de consenso da rede distribuída ajusta a dificuldade de mineração de forma descentralizada. A quantidade de zeros na identificação do bloco define o grau de dificuldade.

Eleitores *(Nodes).* Os eleitores são os "nós da rede distribuída" na arquitetura *E2E Blockchain I-Voting.* O *nodes* podem ler e submeter transações na respectiva *blockchain,* mas não são autorizados a validar as transações como *miners.*

NEC, SEO, RIA, EVC, RMCS, Political Parties (Miners). Os agentes públicos e demais membros responsáveis pelo sistema de *i-voting* são os "mineradores da rede distribuída" na arquitetura *E2E Blockchain I-Voting* para consolidar a transparência no processo de votação, ou seja, a confiança no sistema. Cada *miner* apenas tem autorização para ler e, principalmente, validar cada transação no registro de cada bloco. O objetivo é manter a consistência do *ledger* (banco de dados) das transações oriundas de parte do sistema de *i-voting*. Assim, os *miners* "competem computacionalmente" para manter a integridade do *ledger* fazendo com que todos os *miners* da *public permissioned ledger* verifiquem o mesmo *ledger*.

No caso da tese, não há *token digital* como "pagamento ou prêmio" na busca do "enigma" do *hash code* (impressão digital de determinado dado) para atender determinados critérios que são parte das regras de negócio da arquitetura escritos no protocolo de consenso e contrato inteligente.

Resumidamente, as funções dos *miners* são:

a) Validar cada transação de cada eleitor para garantir que a regra *"one person, one vote"* seja obedecida;

b) Encontrar o código especial (numero randômico) para validar e vincular as cadeias de blocos transacionadas na rede e manter cópia da *blockchain* intacta – o *ledger,* para todos os *nodes*.

Voter Application, E2E Blockchain I-Voting **e** ***Block Chain Verification Application.*** O eleitor deve fazer o *download* do *Voter Application* e *E2E Blockchain I-Voting* no seu computador pessoal e do *Block Chain Verification Application* no seu *smart device.*

6.4.2 Aplicações Blockchain

A arquitetura *E2E Blockchain I-Voting* utiliza o algoritmo *Monero blockchain* adaptado e customizado para o contexto do sistema de votação pela Internet estoniano. A aplicação em tecnologia *blockchain* possui um *input* de dados já mencionados na Figura 6.

A pesquisa enfatiza que a recomendação para modificar a origem das informações para a verificação de ponta a ponta dos votos eletrônicos pelo eleitor é acertada porque a aplicação *Processor* é o último estágio de verificação da autenticidade e integridade da cédula eletrônica antes da anonimização e contagem dos votos no ambiente *off-line* do sistema de *i-voting,* conforme mostra a Figura 24.

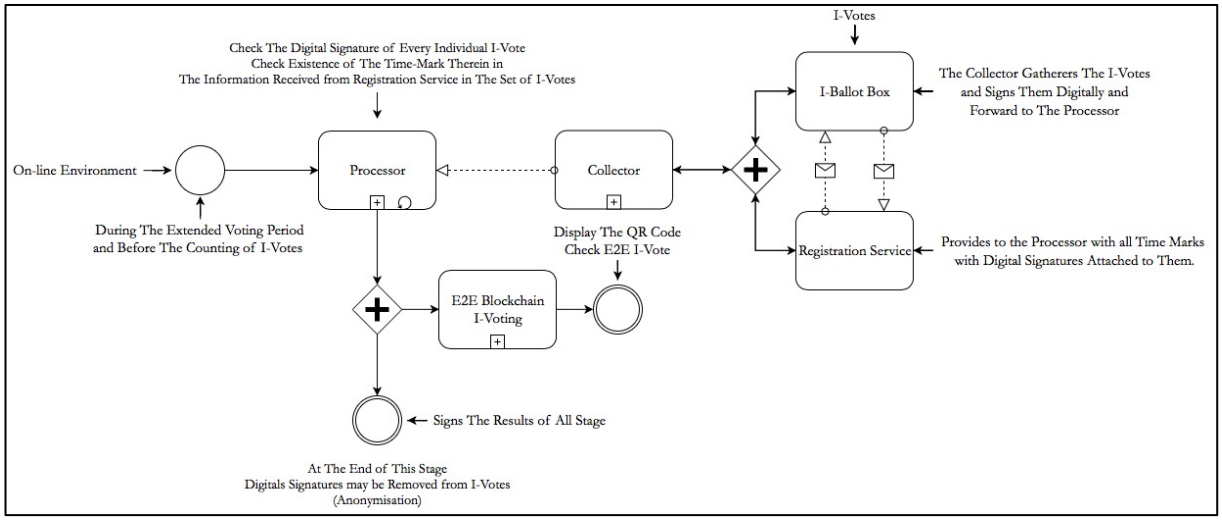
De outra parte, é a recomendação da pesquisa que o ambiente *off-line* de processamento dos votos eletrônicos seja incorporado ao ambiente *on-line* para potencializar a transparência durante o processo de votação com período estendido para o eleitor – Figuras 03 e 22.

O processo na plataforma *E2E Blockchain I-Voting* é realizado dentro da tipologia *public permissioned blockchain*. Neste caso, a funcionalidade da *blockchain* é iniciada a partir do *input* originário do sistema de *i-voting* que gera o arquivo que contém o *random number*

criado após o voto do eleitor pelo *Voter Application,* e o arquivo *Session Code* criado depois do processamento através do *Processor Application.* As estapas de operação na *blockchain* são simplificadas abaixo:

a) Requisição de transação na *blockchain* após o registro do voto eletrônico;
b) O bloco #01 do eleitor *(node)* é criado a partir do criptograma de assinatura digital gerado pelo *Processor Application* no sistema de *i-voting;*
c) O bloco #01 é compartilhado entre os *nodes* na rede distribuída da *blockchain*;
d) A transação realizada pelo bloco #01 é validada pela rede distribuída dos *miners;*
e) O *Hash Code* é criado após o bloco #01 ser validado por um dos *miners;*
f) O bloco #01 é anexado na cadeia de blocos criando a *blockchain/ledger*;
g) Cada *node* na *blockchain* possui uma cópia do *ledger* para torná-lo imutável;
h) A aplicação de verificação ponta a ponta é acionada para exibir o número do candidato e o partido político após o voto do eleitor ou a confirmação ofuscada do conteúdo.
i) A cada voto novo pelo eleitor, o processo na cadeia de blocos se repete para validar a transação atualizada;
j) O eleitor pode verificar o voto digital na *blockchain* durante e após o período eleitoral.

Figura 24: Arquitetura E2E Blockchain I-Voting e Processor



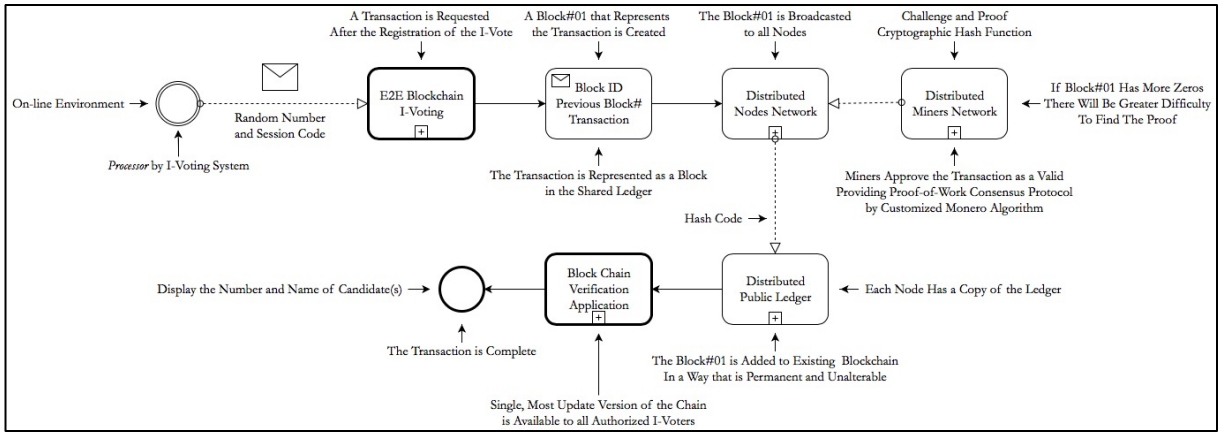
Fonte: Elaborado pelo autor

Os processos de integração da *E2E Blockchain I-Voting* com o sistema de *i-voting* da Estônia, a *Block Chain Verification Application,* os *nodes* e os *miners* também são importantes

para o entendimento da abordagem da pesquisa que é exequível para a proposta de verificação ponta a ponta para o pleito eleitoral pela Internet.

A figura 25 exibe a operação da aplicação *E2E Blockchain I-Voting* na abordagem nova do sistema de *i-voting* para a verificação *E2E* do processo eleitoral estoniano.

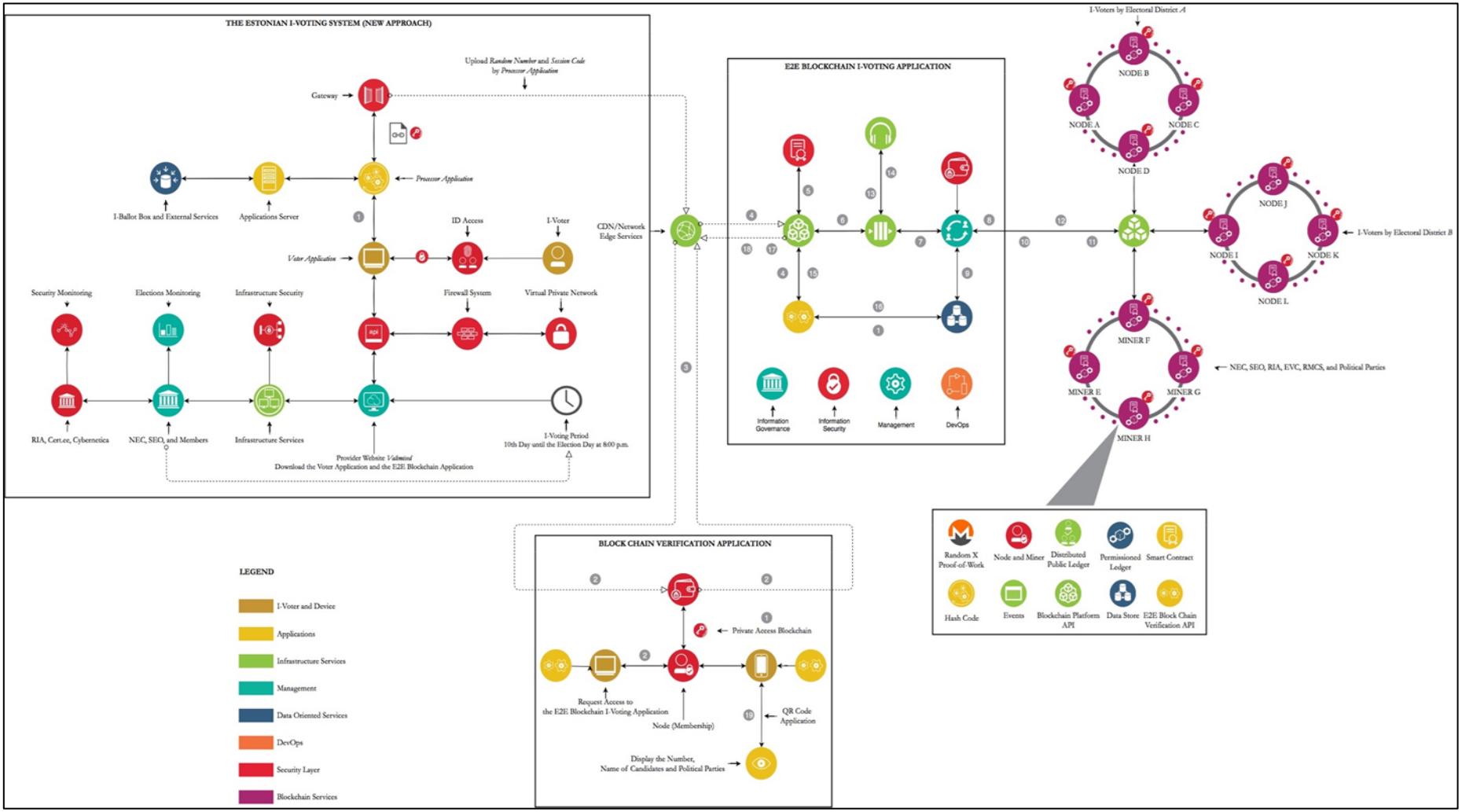
Figura 25: Operação da aplicação E2E Blockchain I-Voting



Fonte: Elaborado pelo autor

Por fim, a figura 26 é a integração entre o sistema de *i-voting* da Estônia e as aplicações *E2E Blockchain I-Voting* e *Block Chain Verification Application.*

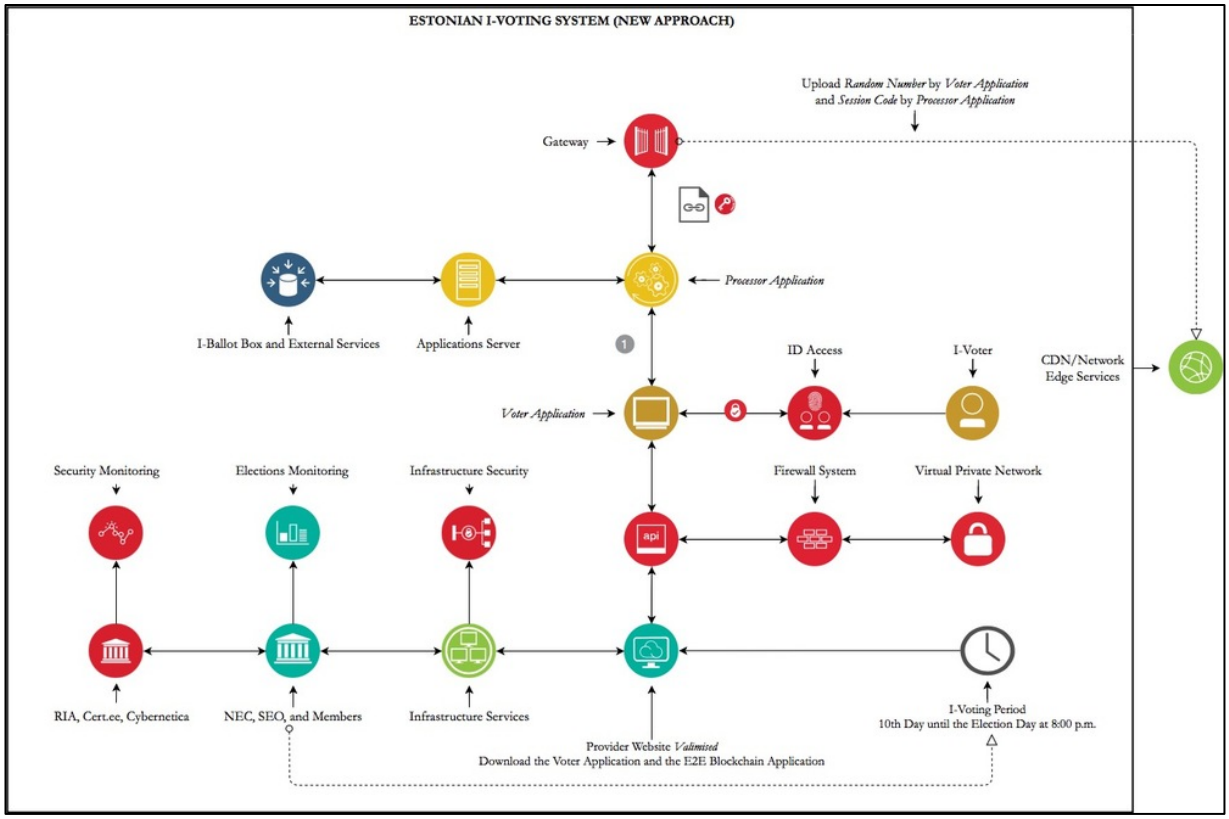
Figura 26: The I-Voting System, E2E Blockchain I-Voting e Block Chain Verification Application



Fonte: Elaborado pelo autor

A estapas enumeradas na cor cinza da figura 26 são explicadas abaixo para entender o fluxo das informações entre cada plataforma interrelacionada com o processo de votação correspondente - *I-Voting System, E2E Blockchain I-Voting* e *Block Chain Verification Application.*

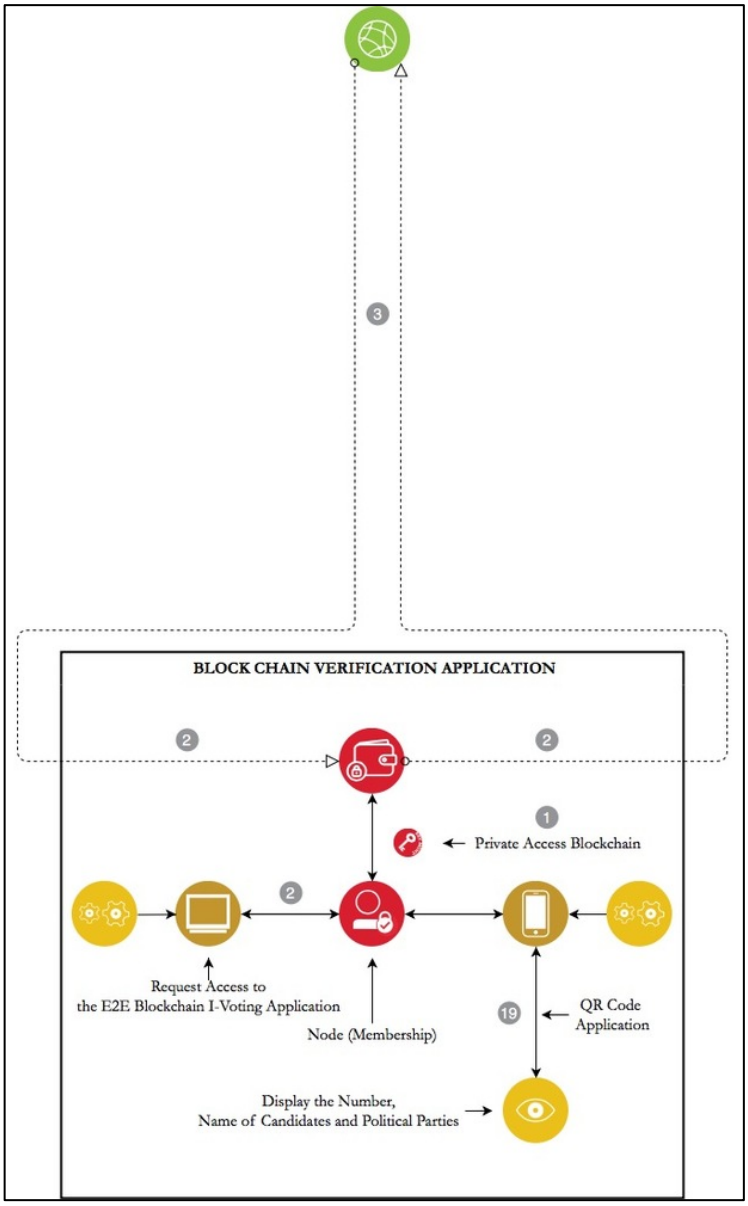
Figura 27: New approach of the i-voting system



Fonte: Elaborado pelo autor

- No sistema de *i-voting* é realizado o *upload* do arquivo que contém os identificadores de conteúdo da cédula eletrônica do eleitor - *random number* e *session code,* para a aplicação *E2E Blockchain I-Voting.* A aplicação *E2E Blockchain I-Voting* gerencia o registro de *upload* do arquivo no sistema de votação pela Internet para o *ledger* da rede distribuída de *nodes.*

Figura 28: Block Chain Verification Application



Fonte: Elaborado pelo autor

- O eleitor tem acesso permitido na aplicação *Block Chain Verification Application* através da sua "carteira privada" ou *wallet* que armazena as suas credenciais via *ID Card* e a sua chave privada.

2

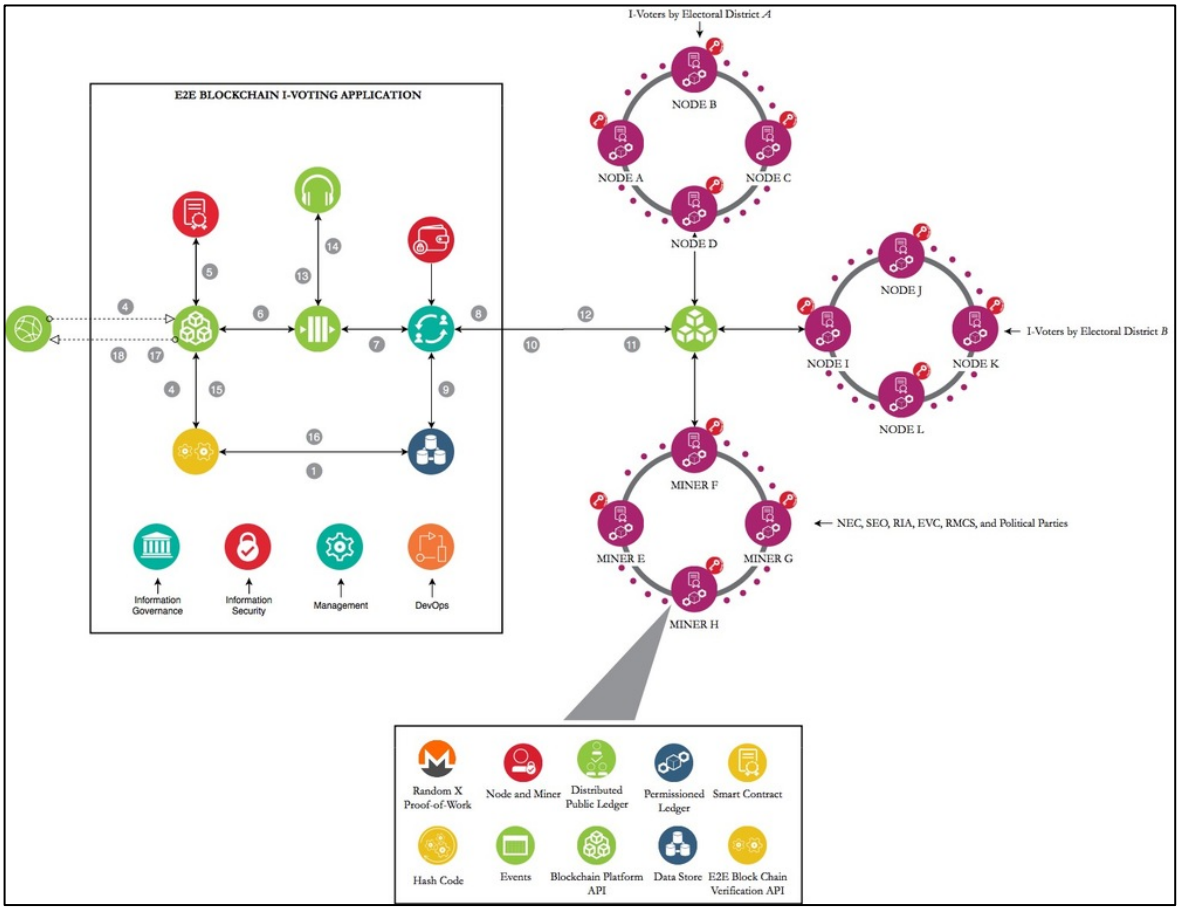
- A requisição do eleitor é recebida pela rede *Edge Service* para o roteador encaminhá-la para o servidor da aplicação *E2E Blockchain I-Voting* que corresponde ao domínio https://e2eblockchain.ee[112].

3

- O arquivo com o *random number* e *session code* do *block#* é enviado no formato *QR Code* para ser codificado e visualizado pelo eleitor através do *Block Chain Verification Application.*

19

Figura 29: E2E Blockchain I-Voting



Fonte: Elaborado pelo autor

[112] O endereço na Internet é hipotético para a proposta da tese.

- A aplicação *E2E Blockchain I-Voting* utiliza a estrutura de gerenciamento de acesso e identidade da plataforma que foi customizada *(Monero)* para autenticar e autorizar o eleitor através do certificado digital.

4 5

- Por meio do barramento de mensagens, a aplicação *E2E Blockchain I-Voting* gerencia as rotas de transações dos *smart contracts* ou contratos inteligentes.

6 7

- O gerenciador de rotas das transações pode transmitir uma mensagem para a rede *blockchain* usando credenciais que identificam a *Block Chain Verification Application* que chama o *smart contract*. O gerenciador de transações acessa o conteúdo registrado pelo *E2E Blockchain I-Voting* no *wallet* (que geralmente contém informações de identificação sobre o eleitor), para assinar digitalmente a solicitação do *smart contract* para identificar a *Block Chain Verification Application* que está construindo a chamada do *smart contract*. De forma mais simples, o gerenciador de transações também pode transmitir uma mensagem assinada pelo eleitor diretamente para a *Block Chain Verification Application*.

8

- O gerente de transações da *E2E Blockchain I-Voting* requisita os *smart contracts* de um ou mais nós do *ledger* distribuído. Quando há dados originados de fora do *ledger*, o gerenciador de transações grava e lê os dados em coordenação com a requisição dos *smart contracts* da *blockchain*.

9

- A aplicação *E2E Blockchain I-Voting* utiliza o protocolo *Random X* para executar o contrato inteligente entre o grupo de *nodes* de um determinado distrito eleitoral para que, posteriormente, os *miners* confirmem as transações para o *ledger*. Na abordagem da tese, o *smart contract* não tem necessidade de acessar dados externos porque o *upload* do arquivo já foi realizado para a aplicação *E2E Blockchain I-Voting*.

10 11 12

- Os *events* ou eventos são realizados à medida que a aplicação *E2E Blockchain I-Voting* solicita transações e adiciona no *ledger*. Neles trafegam as informações via barramento de mensagens para acionar as interações da rede *blockchain* e as mensagens para o eleitor.

13 14

- Quando o eleitor faz a verificação de ponta a ponta na *Block Chain Verification Application,* a aplicação *E2E Blockchain I-Voting* comprova se o *block#* validado pelo *miner* no *ledger* é correspondente ao *upload* realizado do sistema de *i-voting* – Figura 28.

15 16 17 18

6.5. TRABALHOS FUTUROS

Em razão do aspecto temporal limitante da pesquisa e pela inviabilidade de testar as aplicações de verificabilidade *E2E* com a tecnologia *blockchain* no sistema de *i-voting* estoniano, a pesquisa pretende no futuro:

a) Escrever as linhas de códigos na linguagem C++ do algoritmo *Monero* para customizar o modelo proposto;
b) Elaborar o relatório técnico com base na proposta da tese;
c) Entrar em contato com o governo estoniano para discutir a viabilidade da proposta, em especial, com o Grupo de Trabalho *E-election Security Working Party* criado em 2019; e
d) Enviar para a biblioteca da *TALTECH* uma cópia da tese no formato *pdf.*

6.6. LIÇÕES APRENDIDAS

A pesquisa entende que as lições aprendidas com o tema na Estônia são bastante importantes para que outras nações democráticas entendam que o processo de votação pela Internet ainda é um longo caminho de aperfeiçoamento cultural e tecnológico.

6.6.1 Realidade Estoniana

I. Sistema de votação pela Internet não é seguro totalmente, pois além dos problemas encontrados na pesquisa há dois deles que não são solucionados na tese, a centralização do servidor de dados e a autenticação eletrônica do eleitor. Ambos são propensos às ações de agentes maliciosos exógenos e internos;

II. O problema de 2017 com o *ID Card* estoniano ainda transmite dúvida e insegurança na arquitetura e infraestrutura do sistema de *i-voting*;

III. A ausência de transparência em partes do processo de *i-voting* prova que o modelo estoniano não difere de outros sistemas de votação com problemas semelhantes;

IV. Na eleição de 2019, a participação do eleitorado corresponde apenas trinta por cento dos eleitores. Isto é um indicador negativo para o modelo estoniano que existe há quinze anos. Em comparação com as evidências dos dados de especialistas estonianos, a curva de aceitação do sistema de *i-voting* ainda é bastante baixa e lenta. Não obstante, é também possível conjecturar um outro indicador negativo, pois a Estônia é a única nação que insiste com o *i-voting* dentre os vinte e seis estados-membros da União Européia e, também, em relação aos demais países democráticos. Portanto, conclui-se que o sistema de votação pela Internet não é confiável plenamente; e

V. Marketing estatal excessivo em relação ao sistema de *i-voting*.

6.6.2 Por que I-voting Não é Recomendável?

I. Sistemas políticos são corruptíveis por natureza, pois nenhum sistema é perfeito nas sociedades democráticas. É muita presunção acreditar que um governo seja honesto plenamente. Com isso, a primeira recomendação é aceitar os problemas sociais de corrupção e desonestidade eleitoral;

II. Em vista disso, não é suficiente afirmar que o processo de *i-voting* é seguro, pois a questão social é o maior desafio das eleições eletrônicas;

III. Sendo a fraude eleitoral uma questão social, é impossível acreditar que somente a tecnologia seja capaz de resolver o problema da votação eletrônica ou votação pela Internet na sua plenitude;

IV. Logo, não é suficiente apenas empreender com protocolos de chaves criptográficas, pois o sistema como um todo pode apresentar alguma vulnerabilidade em algum ponto do seu ambiente humano e tecnológico;

V. Em relação ao sistema de *i-voting* estoniano, é nítida a transferência da confiança no sistema político para a tecnologia. Neste sentido, é inocente acreditar que o eleitor em casa é a pessoa que está votando no sistema, sendo que na verdade é a tecnologia como, por exemplo, o *ID Card* estoniano; e

VI. A experiência estoniana ensina que se deve ter cuidado com o marketing excessivo do sistema de *i-voting* para outros países, por exemplo, a propaganda de que o sistema é confiável, participação "satisfatória" dos eleitores, segurança "inabalável" das informações, transparência total do processo de votação e etc.

6.6.3 Qual é a Esperança para o I-voting no Futuro?

I. O sistema *i-voting* ainda é um modelo de votação eletrônica em processo de amadurecimento cultural e tecnológico, como é o caso estoniano.

II. Um sistema de *i-voting* não pode ser utilizado para otimizar um processo eleitoral completo, pois a tecnologia adotada deve ser compreendida como um instrumento complementar no processo de votação, mas desde que projete a confiança no sistema para todos;

III. A solução é empreender um sistema de *i-voting* com tecnologias para potencializar a confiança no sistema de votação mesmo com o eleitor consciente de que o governo é corrupto;

IV. Um país com dimensões territoriais e populacionais maiores do que a Estônia como, por exemplo, a República Federativa do Brasil ou a República da Índia, torna-se inviável a prática de um sistema de votação pela Internet; e

V. A esperança para o futuro das eleições eletrônicas com *i-voting* é o desenvolvimento de pesquisas que retratam a realidade do sistema e buscam a melhor forma de resolver os desafios tecnológicos e o fator humano, e não apenas o marketing estatal e comercial das empresas.

6.6.4 Qual é o Mérito da Experiência Estoniana?

I. A pesquisa afirma que o modelo de interoperabilidade do sistema *X-Road* é a parte mais significativa da experiência estoniana porque remete para um conceito novo de *e-governance* que pode ser recomendada para outras nações;

II. É salutar aprender com o modelo de *e-governance* da Estônia para entender que dados e informações podem ser operados de forma eficaz, eficiente, otimizada e privada;

III. A questão da segurança das informações é um tema *Ad infinitum*[113], inclusive na plataforma *X-Road;* e

IV. A experiência estoniana mostra para as nações democráticas que a adoção de um sistema de *i-voting* no processo eleitoral ainda é bastante prematuro na era atual.

---

[113] Do latim "Até o infinito" ou "Sem fim".

7. CONCLUSÃO

"Vamos tentar fazer algo útil"
***Demi Getschko*[114]**

"Por falta de um prego, perdeu-se a ferradura; por falta de uma ferradura, perdeu-se o cavalo; por falta do cavaleiro, perdeu-se a batalha; E assim, um reino foi perdido. Tudo por falta de um prego"
James Gleick

A interrelação de circunstâncias da pesquisa é sobre a observação de tecnologias novas para votação na escolha de candidatos e partidos políticos. Neste contexto, a investigação acadêmica observa que o sistema de *i-voting* da República da Estônia é o paradigma mais consolidado no cenário internacional.

O sistema de votação pela Internet estoniano é um conjunto de tecnologias computacionais que fornecem a arquitetura e a infraestrutura tecnológicas para cada pleito eleitoral. A pesquisa pode afirmar que parte do sucesso do sistema de *i-voting* para os eleitores estonianos está relacionada com a interoperabilidade do ambiente de *e-governance* e a identidade digital.

De outra parte o modelo estoniano é suscetível à fraudes e vulnerabilidades semelhantes a outros países democráticos.

A pesquisa observa que o sistema de *i-voting* possui falhas e vulnerabilidades apresentadas na seção 1.2 da Introdução – Figuras 17, 20, 21 e 22, que comprometem bastante a confiança no modelo estoniano de eleição eletrônica. Inclusive, a aplicação de verificabilidade de ponta a ponta do modelo atual é ineficaz em transmitir a confiança para os eleitores.

Com base na observação, a solução encontrada pela pesquisa é abordar um modelo de aplicação para verificação de ponta a ponta com o uso da tecnologia *public permissioned blockchain* para que a transparência amplie a confiança dos eleitores, partidos políticos e organizadores do pleito eleitoral - Figuras 24, 25, 26, 27, 28 e 29.

---

[114] Orientação acadêmica realizada em 24/08/2016 após o término do primeiro dia do VII Seminário de Proteção de Dados Pessoais em São Paulo, Brasil.

Para auxiliar na proposta, a investigação busca na literatura modelos sobre o tema. Contudo, depara-se com um acervo limitado, tanto para as pesquisas realizadas pela comunidade acadêmica, como por empresas do setor privado que, em alguns casos, tem parceiria com o poder público – como no caso da Estônia.

A discussão realizada no Capítulo 2 demonstra que a abordagem da tese é inédita, pois a maioria dos trabalhos, com ou sem a tecnologia *blockchain,* apresentam modelos de eleições eletrônicas completas. No entanto, as pesquisas não findam as suas experiências.

Um ponto crítico da pesquisa documental é que a maioria da literatura tem foco no registro da cédula eletrônica no *ledger* como, por exemplo, as reflexões de Heiberg *et al.* (2018) em sugerir a utilização da tipologia *public permissionless blockchain* como *bulletin board* para o processo de votação pela Internet através da integração de uma *blockchain API* direta com a aplicação externa *Registration Service* presente no sistema de votação pela Internet estoniano.

Para a pesquisa, a sugestão não é factível porque a aplicação de verificabilidade *E2E* ainda utiliza informações somente do ambiente *on-line.* Vale ressaltar que na maioria dos trabalhos analisados, também é percebida a falta de aprimoramento científico para utilizar a tecnologia *blockchain* ao contexto do paradigma abordado.

É importante ratificar que a pesquisa pressupõe que o cenário estoniano está livre de situações tóxicas como, por exemplo, pessoas e programas maliciosos no ambiente de processamento dos votos eletrônicos, no sistema de *i-voting* e nos dispositivos eletrônicos dos eleitores.

A metodologia na tese aposta no aperfeiçoamento científico com a tecnologia *blockchain,* porém dentro dos limites que a própria tecnologia impõe na atualidade – discutido no Capítulo 2.

Como já foi mencionado, a tipologia *public permissioned blockchain* é a mais adequada ao cenário estoniano de verificação *E2E* para votação pela Internet.

A plataforma *blockchain* para construção do modelo é a original – que pode ser encontrada em repositórios *open-source*. Entretanto, deve-se assumir a ação customizada com o algoritmo do sistema *Monero* para abordar a tipologia *public permissioned blockchain* em razão do ambiente peculiar de votação *on-line* (votar, ler e validar) que somente pode ter a

participação de eleitores, partidos políticos, agentes públicos e terceiros autorizados por lei, promovendo, assim, a individualidade e universalidade da verificação de ponta a ponta.

O algoritmo *Monero* é a forma mais recomendada pela tese porque o algoritmo traz meios de impossibilitar o rastreamento da identidade do bloco, a exposição do conteúdo do *ledger* e restringir o poder de "mineração" para evitar as aplicações *ASICs* de agentes maliciosos contra a rede distribuída do *ledger.*

Para a solução ser aplicada, é recomendado a alteração do período de votação no ambiente *on-line* - Figuras 5 e 6, para as arquitetutas *E2E Blockchain I-Voting* e *Block Chain Verification Application* – Figura 26.

É importante ressaltar que a alteração do período eleitoral *on-line* causa impacto na legislação estoniana.

O ponto focal da estratégia de fazer o *upload* de dois arquivos de tamanho inferior no *ledger* em vez da cédula eletrônica, deve-se à escalabilidade e o tempo de resposta do processamento de validação da cadeia de blocos e, como resultado, a cópia do *ledger* para a rede distribuída de *nodes* na aplicação *E2E Blockchain I-Voting.*

Na aplicação *E2E Blockchain I-Voting* não há registro do voto eletrônico no *ledger*, mas apenas o *upload* do *random number* e *session code* que correspondem à confidencialidade e integridade do processamento da cédula eletrônica antes das etapas de anonimização das cédulas eletrônicas.

Para a pesquisa, a abordagem é mais transparente porque as assinaturas digitais do criptograma garantem que a cédula eletrônica não seja alvo de manipulação indesejada antes e após a contagem dos votos eletrônicos.

A finalidade da proposta é potencializar a confiança no sistema de *i-voting* com a tecnologia *E2E Blockchain I-Voting* pelo "duplo grau de segurança da cédula eletrônica" – a imutabilidade dos arquivos *random number* e *session code* no *ledger* e a validação do *hash code* no mesmo *ledger*, pois se o *ledger* for alterado, o *hash code* também é alterado e toda a cadeia precisa ser validada pelos *miners* novamente.

Os argumentos da tese são factíveis e harmônicos porque no estágio final da pesquisa surgem dois documentos importantes que ratificam a abordagem proposta como válida.

O primeiro é o relatório final publicado pela *OSCE/ODIHR* (2019, p. 12) da *Riigikogu Election 2019* na Estônia. O segundo é o relatório interno do governo estoniano, *E-election Security Working Party Report*[115] (ESTONIA, 2019, pp. 30-31; 46-47; 57-58)[116], sobre o mesmo pleito eleitoral, aonde ambos são claros em enfatizar que parte do sistema de votação pela Internet estoniano é vulnerável e dúbio – ou seja, não consolida plenamente a confiança individual e universal, especialmente, a respeito do procedimento de verificação ponta a ponta do sistema de *i-voting*.

Neste sentido, a tese contribui para o fortalecimento da confiança com a adoção da tecnologia *blockchain* para a verificação de ponta a ponta em parte do sistema de *i-voting* estoniano para consubstanciar o aperfeiçoamento no campo político, social, regulatório e tecnológico.

---

[115] Grupo de trabalho criado pela *Minister for Foreign Trade and Information Technology*, Kert Kingo, e publicado em dezembro de 2019.

[116] *"I will set up an e-election working group to evaluate the electronic voting system and the compliance of electronic voting information system processes and security measures existing cybersecurity and election management regulations"*, Kert Kingo (ESTONIA; 2019, p. 04).

8. REFERÊNCIAS

ADIDA B. *Helios: Web-based open-audit voting*. In USENIX Security Symposium, 2008.

_____; *et al*. *Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios*. In: USENIX EVT/WOTE, 2009.

ANDOLA, N.; GAHLOT, R.; GOGOL, M.; VENKATEASEN, S. *Vulnerabilities on Hyperledger Fabric*. ResearchGate, 2019.

ALVAREZ, Michael R.; HALL, Thad E. *Point, Click, and Vote*. The Brookings Institution Press, 2004.

BAYER, Dave; HABER, Stuart; STORNETTA, W Scott. *Improving the eficiency and reliability of digital time-stamping*. In Sequences II, Springer, 1993.

BEITANE, A. *Casting Votes Digitally: Examining the Latvian National Position on Internet Voting.* Tartu University, 2016.

BELL, S.; BENALOH, J.; BYRNE, M. D.; DEBEAUVOIR, D.; EAKIN, B.; FISHER, G.; KORTUM, P.; MCBURNETT, N.; MONTOYA, J.; PARKER, M.; PEREIRA, O.; WALLACH, D. S.; WIN, M. *STAR-vote: A secure, transparent, auditable, and reliable voting system.* USENIX Journal of Election Technology and Systems (JETS) 1(1), 2013.

BENALOH, J.; LAZARUS, E. *The trash attack: An attack on verifiable voting systems and a simple mitigation*. Technical report, 2011.

BISTARELLI, S.; MANTILACCI, M.; SANTANCINI, P.; SANTINI, F. *An End-to-end Voting-system Based on Bitcoin*. In Proceedings of the Symposium on Applied Computing, SAC ’17, 2017.

BISMARK, D.; *et al*. *Experiences Gained from the first Prêt à Voter Implementation*. In: First International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE). IEEE, 2009, pp. 19–28.

BOGUCKI, B. *Buying Votes in the 21st Century*: *The Potential Use of Bitcoins and Blockchain Technology in Electronic Voting Reform*. Asper Review of International Business and Trade Law, 2017.

BRAZIL. Cetic.br. *Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação.* Disponível em: <https://www.cetic.br>, 2019.

_____. Cert.br. Cartilha de Segurança para Internet, 2012.

_____. *The Embassy of Brazil in Estonia.* 2018.

BERÉS, F., SERES, I. A.; BENCZÚR, A.; QUINTYNE-COLLINS, *M. Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users*. ResearchGate, 2020.

BULENS, P.; GIRY, D.; PEREIRA, O. *Running mixnet-based elections with Helios*. In: USENIX EVT/WOTE, 2011.

BURTON, C.; *et al*. *Using Prêt à Voter in Victorian State elections*. In: USENIX EVT/WOTE, 2012.

BUTERIN, V. *A next-generation smart contract and decentralized application platform*, 2014.

_____. *Ethereum white paper*, 2013.

CALTECH-MIT. Voting Technology Project. *Voting: What is, what could be*. Technical report, Caltech/MIT, 2001.

CARBACK, R.; *et al*. *Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy*. In: USENIX Security. 2010.

CHAUM, D. *Surevote: Technical overview*. In Proceedings of the Workshop on Trustworthy Elections, ser. WOTE, Aug. 2001.

_____; *et al*. *Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes*. In: USENIX EVT. 2008.

_____; *et al*. *Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes*. In: IEEE Transactions on Information Forensics and Security 4.4, 2009, pp. 611– 627.

CHAUM, D.; ESSEX, A.; CARBACK, R.; CLARK, J.; S. POPOVENIUC; A. SHERMAN; VORA, P. *Scantegrity: End-to-end voter-verifiable optical-scan voting*. IEEE Security & Privacy, 2008.

CHAUM, D.; RYAN, P. Y. A.; SCHNEIDER, Steve. *A Practical Voter-Verifiable Election Scheme*. English. In: Computer Security – ESORICS 2005. Ed. by Sabrinade Capitani di Vimercati, Paul Syverson, and Dieter Gollmann. Vol. 3679. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, pp. 118– 139.

CHONDROS, N.; ZHANG, B.; ZACHARIAS, T.; DIAMANTOPOULOS, P.; MANEAS, S.; PATSONAKIS, C.; DELIS, A.; KIAYIAS, A.; ROUSSOPOULOS, M. *Distributed, End-to-end Verifiable, and Privacy-Preserving Internet Voting Systems*. Cornell University. eprint arXiv:1608.00849, 2016.

CHRISTIAN, B.; GJØSTEEN, K.; NORE, H. *Faults in Norwegian Internet voting*. In *Proceedings*: Third International Joint Conference on Electronic Voting, E-Vote-ID 2018, 2–5 October 2018, Lochau/Bregenz, Austria, 2018.

CLARK, J.; ESSEX, A. *CommitCoin: carbon dating commitments with Bitcoin*. In: Financial Cryptography and Data Security. Springer, 2012, pp. 390–398.

CLARKSON M. R; CHONG S; MYERS A. C. *Civitas: Toward a secure voting system*. In IEEE Symposium on Security and Privacy, 2008.

COLEMAN, S.; FREELON, D. *Handbook of Digital Politics*. Elgar, 2015.

CRAMER R.; GENNARO R.; SCHOENMAKERS B. *A secure and optimally efficient multi-authority election scheme.* EUROCRYPT, 1997.

CRESWELL, J. W.; CRESWELL, J. D. *Research design: qualitative, quantitative, and mixed methods approaches*. 5th ed. Thousand Oaks: CA, Sage, 2018.

CULNANE, C.; SCHNEIDER, S. A. *A peered bulletin board for robust use in verifiable voting systems*. In *IEEE CSF 2014*, pages 169–183. IEEE Computer Society, 2014.

CYBERNETICA. *Cryptographic algorithms lifecycle report 2017*. Estonian Information System Authority (RIA), 2018.

DELIS, A.; *et al*. *Pressing the Button for European Elections 2014: Public attitudes towards Verifiable E-Voting in Greece*. 2014. Disponível em: <https://drive.google.com/file/d/0B-mtbRwyPn_SdnpMRzBKcEZWUm8/ view?usp=sharing>.

ESSEX, A.; *et al*. *Punchscan in practice: an E2E election case study*. In: Proceedings of Workshop on Trustworthy Elections, 2007.

ESTONIA. *E-election Security Working Party Report*, 2019.

_____. INFORMATION SYSTEM AUTHORITY (RIA). *ROCA Vulnerability and eID: Lessons Learned*. Disponível em: < https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf>, 2018.

FAOUR, N. *Transparent Voting Platform Based on Permissioned Blockchain*. Master's thesis, Higher School of Economics, National Research University, Russia. Disponível em: <https://arxiv.org/abs/1802.10134>, 2018.

FISCHER, E.; COLEMAN, K. *The direct recording electronic voting machine (DRE)*. Whashington, DC: The Library of Congress, 2006.

Fisher, K.; Carback, R.; Sherman, A.T. *Punchscan: Introduction and System Definition of a High-integrity Election System*. In: Preproceedings of the 2006 IAVoSS Workshop on Trustworthy Elections, Robinson College (Cambridge, United Kingdom), International Association for Voting System Sciences, 2006.

FULLER, R. B. *No More Secondhand God (late Night, April 9, 1940)*. In No More Secondhand God and other Writings. Carbondale: Southern Illinois University Press, 3-36, 1963.

GALINDO, D.; GUASCH, S.; PUIGGALÍ, J. *Neuchâtel's Cast-as-Intended Verification Mechanism.* In: Haenni, Rolf; Koenig, Reto and Wikström, Douglas (eds): E- Voting and

Identity. VoteID 2015. Lecture Notes in Computer Science, vol 9269. Springer, Cham, pp. 3-18, 2015.

GATTESCHI, V.; LAMBERTI, F.; DEMARTINI, C. *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?* Disponível em: < https://www.researchgate.net/publication/323298791_Blockchain_and_Smart_Contracts_for_Insurance_Is_the_Technology_Mature_Enough>, 2018.

GERMANNA, M. *Internet voting and turnout: Evidence from Switzerland*. Author links open the author workspace. Electoral Studies, Volume 47. Elsevier, 2017.

GERTLER, P. J.; MARTÍNEZ, S.; PREMAND, P.; RAWLINGS, L. B.; VERMEERSCH, C. M. J. *Avaliação de Impacto na Prática*. BID. the Inter-American Development Bank. Segunda Edição, 2018.

GIL, A. C. 2017. *Como elaborar projetos de pesquisa*. 6. ed. São Paulo: Atlas.

GLEICK, J. *Caos: A Criação de Uma Nova Ciência*. Editora Elsevier: São Paulo, 1989.

HAO, F., RYAN, P. Y.; ZIELÍNSKI, P. *Anonymous voting by two-round public discussion*. IET Information Security. IET Digital Library, 2010.

GJØSTEEN K. *The norwegian internet voting protocol*. IACR Cryptology ePrint Archive, vol. 2013, p. 473, 2012.

GONGGRIJP, R.; *et al*. *RIES - Rijnland Internet Election System: A Cursory Study of Published Source Code*. English. In: E-Voting and Identity. Ed. by Peter Y.A. Ryan and Berry Schoenmakers. Vol. 5767. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009, pp. 157–171.

HAENNI, R.; DUBUIS, E.; RETO, E. K.; LOCHER, P. *Process Models for Universally Verifiable Elections.* In Proceedings: Third International Joint Conference on Electronic Voting, E-Vote-ID 2018, 2–5 October 2018, Lochau/Bregenz, Austria, 2018.

HEIBERG, S.; MARTENS, T.; VINKEL, P.; WILLEMSON, J. *Improving the Verifiability of the Estonian Internet Voting Scheme. Improving the Verifiability of the Estonian Internet Voting Scheme*. In Robert Krimmer, Melanie Volkamer, Jordi Barrat, Josh Benaloh, Nicole Goodman, Peter Y. A. Ryan, and Vanessa Teague, editors, E-Vote-ID 2016: Electronic Voting, volume 10141 of LNCS, 2016.

_____.; KUBJAS, I.; SIIM, J.; WILLEMSON, J. *On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards*. In *Proceedings*: Third International Joint Conference on Electronic Voting, E-Vote-ID 2018, 2–5 October 2018, Lochau/Bregenz, Austria, 2018.

_____.; WILLEMSON, J. *Verifiable Internet Voting in Estonia*. In Proceedings: 6th International Conference on Electronic Voting, EVote2014, 28–31 October 2014, Lochau/Bregenz, Austria, 2014.

_____.; PARSOVS, A.; WILLEMSON, J. *Log analysis of Estonian Internet voting 2013-2014*. In: *International Conference on E-Voting and Identity*. Springer, 2015.

HOLZER, M.; SCHWESTER, R. W. *Public Administration*: *An Introduction*. 1st Edition. Routledge, 2011.

HUBBERS, E.; JACOBS, B.; PIETERS, W. *RIES - Internet Voting in Action*. In: 29th International Computer Software and Applications Conference (COMPSAC 2005). IEEE. 2005, pp. 417–424.

IOVA, R. S. *I-Voting Costs: A Case Study of the 2019 Estonian Parliamentary Elections.* Master Thesis at the Ragnar Nurkse Department of Innovation and Governance (Tallinn University of Technology - Tallinn, Estonia), 2019.

JOAQUIM, R.; RIBEIRO, C.; FERREIRA, P. *Veryvote: A voter verifiable code voting system*. In International Conference on E-Voting and Identity, 2009.

JONES, B. *A Report on the Feasibility of Internet Voting*. The California Internet Voting Task Force. Secretary of States – Elections, 2000.

JORBA, A. R. *Design of implementable solutions for large scale electronic voting schemes*. Tese de Doutorado. Universitat Autonoma de Barcelona, 1999.

KIAYIAS, A.; KULDMAA, A.; LIPMAA, H.; SIIM, J.; ZACHARIAS, T. *On the security properties of e-voting bulletin boards.* In Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5 - September 7, 2018, Proceedings. To appear, 2018.

KIRBY, K.; MASI, A.; MAYMI, F. *Votebook. A proposal for a blockchain-based electronic voting system.* Disponível em: <http://www.economist.com/sites/default/files/nyu.pdf>, 2016.

KIZHAKKEDATHIL, N. *A Study into The Prospects of Implementing End-to-End Verifiability in Estonian I-voting.* TALTECH, 2016.

KHAN, K. M.; ARSHAD, J.; MUBASHIR, M. *Secure Digital Voting System Based on Blockchain Technology*. Published in IJEGR, 2018.

KLOTZ, R. J. *The Politics of Internet Communication*. Rowman & Littlefield Publishers, 2003.

KRIESI, H.; TRECHSEL, A. H. *The politics of Switzerland*. Cambridge University Press, 2008.

KRIMMER, R. *The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy*. Ph.D. Dissertation, Institute for Public Administration, Tallinn University of Technology, 2012.

_____. *Internet Voting in Austria: History, Development, and Building Blocks for the Future.* Doctoral thesis, WU Vienna University of Economics and Business, 2017.

_____. FISCHER, D.H. *The E-Voting Mirabilis: A Conceptual Framework for the Analysis of ICT in Elections*. Revista Expert Electoral, 16 (3), 2017.

_____; DUENAS.CID, D.; KRIVONOSOVA, I. *How much does an e-vote cost? Cost Comparison per Vote in Multichannel Elections in Estonia.* In Proceedings: Third International Joint Conference on Electronic Voting, E-Vote-ID 2018, 2–5 October 2018, Lochau/Bregenz, Austria, 2018.

LA GRONE, C.C. *Engaging Youth Voter Participation with Internet Voting in Estonia.* TALTECH, 2016.

LEE, K.; JAMES, J. I.; EJETA, T. G.; KIM, H. J. *Electronic voting service using blockchain*. *The Journal of Digital Forensics*, *Security and Law*: JDFSL, 11(2). Disponível em: <https://commons.erau.edu/jdfsl/ vol11/iss2/8/>, 2016.

LEPPIK, Ü. *Casting Votes Digitally: Examining the Latvian National Position on Internet Voting.* Tartu University, 2015.

LIU, Y.; WANG, Q. *A Secure End-to-End Verifiable E-voting System*. Using Zero Knowledge Based Blockchain. Published in IACR Cryptology ePrint Archive, 2017.

MACEDO, S. *Why Public Reason? Citizens' Reasons and the Constitution of the Public Sphere.* Working Paper, Princeton University, 2010.

MARCONI, M.; LAKATOS, E. *Fundamentos de Metodologia Científica*. 7° ed. São Paulo: Atlas, 2010.

MARGARETTS, H.; NAUMANN, A. *Government as a platform: what can estonia show the world?* Oxford Internet Institute. University of Oxford, 2017.

MEDEIROS, M. *Mecanismo de consenso em uma rede ponto a ponto distribuída para validação e registros de diplomas universitários*. Dissertação de Mestrado. PUC-SP, 2019.

METER, C. *Design of Distributed Voting Systems*. Master's thesis, Heinrich-Heine-Universität Düsseldorf. Disponível em: <https://arxiv.org/pdf/1702.02566.pdf>, 2015.

MERKLE, R. C. *Secrecy, Authentication, and Public Key Systems*. Thesis from Stanford Universisty – Department of Electrical Enginnering. Disponível em: <http://www.merkle.com/papers/Thesis1979.pdf>, 1979.

MOLINARO, L. F. R.; RAMOS, K. H. Carneiro. *Gestão de Tecnologia da Informação*. Governança de TI. Arquitetura e Alinhamento entre Sistemas de Informação e o Negócio. Rio de Janeiro: LTC, 2011.

MONERO. *Cryptonote. Disponível em: <https://cryptonote.org/whitepaper.pdf>, 2019.*

MCLUHAN, H. M. *The Gutenberg Galaxy: The Making of Typographic Man*. University of Toronto Press, 1962.

NAKAMOTO, S. *Bitcoin: A peer-to-peer electronic cash system*. Disponível em: <https: //bitcoin.org/bitcoin.pdf>, 2008.

NEMEC M.; SYS M.; SVENDA P.; KLINEC D.; MATYAS V. *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*. 24th ACM Conference on Computer and Communications Security (CCS'2017), ACM, 2017, 1631–1648.

NOIZAT, P. *Chapter 22 – blockchain electronic vote*. In David Lee Kuo Chuen, editor, Handbook of Digital Currency, pages 453 – 461. Academic Press, San Diego, 2015.

NORDEN, L. D.; FAMIGHETTI, C. *America's Voting Machines at Risk*. Brennan Center for Justice at New York University School of Law, 2015.

NOWIŃSKI, W.; KOZMA, M. *How Can Blockchain Technology Disrupt the Existing Business Models?* Disponível em: < https://www.researchgate.net/publication/319911238_How_Can_Blockchain_Technology_Disrupt_the_Existing_Business_Models>, 2017.

O'REILLY, T. *Government as a Platform*. In: D. Lathrop eds., Open Government: Collaboration, Transparency, and Participation in Practice, Sebastopol, Calif.: O'Reilly Media. Disponível em: <https://www.mitpressjournals.org/doi/pdf/10.1162/INOV_a_00056>, 2010.

PANJA, S.; ROY, B. K. *Bronco Vote: Secure Voting System using Ethereum's Blockchain*. Published in IACR Cryptology ePrint Archive. Gaby G. Dagher, Praneeth Babu Marella, author Jordan Mohler Published 2018 in ICISSP, 2018.

PILKINGTON, M. *Blockchain Technology: Principles and Applications.* Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016.

POPOVENIUC, S.; HOSP, B. *An introduction to Punchscan*. In: IAVoSS Workshop On Trustworthy Elections (WOTE 2006). Robinson College United Kingdom. 2006, pp. 28–30.

_____. *An Introduction to PunchScan*. English. In: Towards Trustworthy Elections. Ed. by David Chaum et al. Vol. 6000. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, pp. 242–259.

PUIGGALI, J.; CUCURULL, J.; GUASCH, S.; KRIMMER, R. *Verifiability Experiences in Government Online Voting Systems*. In: Krimmer, Robert; Volkamer, Melanie; Braun Binder, Nadja; Kersting, Norbert; Pereira, Oliver and Schürmann, Carsten (eds): Electronic Voting: Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017.

_____; RODRÍGUEZ-PÉREZ, A. *Defining a national framework for online voting and meeting its requirements: the Swiss experience*. In Proceedings: Third International Joint Conference on Electronic Voting, E-Vote-ID 2018, 2–5 October 2018, Lochau/Bregenz, Austria, 2018.

RABIN, M.; RIVEST, R. *Practical Provably Correct Voter Privacy Protecting End-to-End Voting Employing Multiparty Computations and Split Value Representations of Votes.* In Proceedings: Third International Joint Conference on Electronic Voting, E-Vote-ID 2014, 28–31 October 2014, Lochau/Bregenz, Austria, 2014.
RAMACHANDRAN, A.; KANTARCIOGLU, M. *Using Blockchain and smart contracts for secure data provenance management.* Disponível em: <https://arxiv.org/abs/1709.10000>, 2017.

RIEMANN, R.; GRUMBACH, S. *Distributed Protocols at the Rescue for Trustworthy Online Voting.* Cornell University, 2017.

RISVIK, C. *End-To-End Verifiability in Electronic Elections*. An E-voting Protocol Based on Blockchain, 2016.

RIVERO, F. G. *Tecnologia e Política: O voto e seu suporte*. PUCSP, 2012.

RIVEST, R.L.; SHAMIR, A.; ADLEMAN, L. M. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Vol. 21. Communications of the ACM, 1978.

RIVEST, R. L.; WACK, J. P. *On the notion of software independence in voting systems*. Prepared for the TGDC, and posted by NIST at the given URL, 2006.

ROGERS, E. M. *Diffusion of innovations* (1st ed.). New York: Free Press of Glencoe, 1962.

RYAN, P. Y.A. *et al*. *Prêt à Voter: Voter-Verifiable Voting System*. In: Information Forensics and Security, IEEE Transactions on 4.4, 2009, pp. 662–673.

_____; WALLACH, D. S. *Casting Votes in the Auditorium*. In USENIX/ACCURATE Electronic Voting Technology Workshop, 2007.

SANDLER, D.; DERR, K.; WALLACH, Dan S. *VoteBox: A Tamper-evident, Verifiable Electronic Voting System*. In 17th USENIX Security Symposium, 2008.

SERDÜL, U. *Internet voting and turnout*: Evidence from Switzerland. M Germann. Electoral Studies, 2017.

SCHRYEN, G. *Security Aspects of Internet Voting*. Proceedings of the Hawaii International Conference on System Sciences, 2004.

SCHNEIER, B. *Applied Cryptography, Second Edition*: Protocols, Algorthms, and Source Code in C. Publisher: John Wiley & Sons, 1996.

_____. *Blockchain and Trust.* Disponível em: <https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html>, 2019.

SILVA, R. *Blockchain Technology for End-To-End Verifiable Elections on Internet Voting Systems.The Estonia Case-study*. In Proceedings: Third International Joint Conference on Electronic Voting, E-Vote-ID 2018, 2–5 October 2018, Lochau/Bregenz, Austria, 2018.

_____.; GETSCHKO, Demi. *Internet Voting in Brazil*: Is It Possible? CeDEM17 Conference for E-Democracy and Open Government, v. 1., 2017.

_____. *Governo Eletrônico*. Vlex Brasil, 2013.

SOLVAK, M.; VASSIL, K. *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)*. Johan Skytte Institute of Political Studies, 2016.

SPRINGALL, D.; FINKENAUER, T.; DURUMERIC, Z.; KITCAT, J.; HURSTI H.; MACALPINE, M.; HALDERMAN, J. A. *Security Analysis of the Estonian Internet Voting System.* Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 703-715, ACM, 2014.

STALLINGS, W. *Criptografia e Segurança de Redes: Princípios e Práticas* – 6ª edição. São Paulo: Pearson, 2015.

SWAN, M. *Blockchain: Blueprint for a New Economy*. O'Reilly, US, 2015.

SZABO, N. *Smart contracts: building blocks for digital markets*. EXTROPY: The Journal of Transhumanist Thought, (16), 1996.

TANENBAUM, A. S.; Wetherall, D. *Redes de Computadores*. 5a Edição. São Paulo: Pearson, 2011.

TAKABATAKE, Y.; KOTANI, D.; OKABE, Y. *An anonymous distributed electronic voting system using Zerocoin*. IEICE Technical Report, 116(282). Disponível em: <http://hdl.handle.net/2433/217329>, 2016.

TORN, T. *Security* A*nalysis of Estonian I-voting System Using Attack Tree Methodologies.* TALTECH, 2014.

TSOUKALAS, G.; *et al*. *From Helios to Zeus*. In: USENIX Journal of Election Technology and Systems 1.1, 2013,

TURING, A. *Computing Machinery and Intelligence*, 1950.

VAARIK, D. *Where Stuff Happens First*. White Paper on Estonia's Digital Ideology. BDA Think tank of the President of Estonia. Disponível em: <https://www.mkm.ee/sites/default/files/digitalideology_final.pdf>, 2015.

VINKEL, P. *Remote Electronic Voting in Estonia: Legality, Impact and Conference*. TUT PRESS, 2015.

_____.; KRIMMER, Robert. *The How and Why to Internet Voting an Attempt to Explain E-Stonia*. In Robert Krimmer, Melanie Volkamer, Jordi Barrat, Josh Benaloh, Nicole Goodman, Peter Y. A. Ryan, and Vanessa Teague, editors, E-Vote-ID 2016: Electronic Voting, volume 10141 of LNCS, 2016.

WASEDA. *Waseda IAC Digital Government Rankings*. Disponível em: <http://business.gmu.edu/blog/tech/2018/11/28/2018-waseda-iac-digital-government-rankings-released/>, 2018.

WAZLAWICK, R. S. *Metodologia de Pesquisa para Ciência da Computação*. 6ª Tiragem. Elsevier Editora Ltda. São Paulo, 2009.

WIENER, N. *Cyberneetics: or Control and Communication in the Animal and the Machine*. Fourth Printing. Disponível em: <https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf>, 1985.

WOLCHOK, S.; WUSTROW, E.; ISABEL, D.; HALDERMAN, J. A. *Attacking the Washington, D.C. Internet Voting System.* In Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012. Disponível em: <https://jhalderm.com/pub/papers/dcvoting-fc12.pdf>, 2012.

WOOD, G. *Ethereum: A secure decentralised generalised transaction ledger.* EIP-150 REVISION, 2017.

WONG, C.W.; WU, M. *Counterfeit detection using paper puf and mobile cameras.* In: *Information Forensics and Security* (WIFS). IEEE International Workshop, 2015.

WU, Y. *An E-voting System based on Blockchain and Ring Signature*. Master's thesis, University of Birmingham. https://www.dgalindo.es/mscprojects/yifan.pdf>, 2017.

XU, X.; WEBER, I.; STAPLE, M.; ZHU, L.; BOSCH, J.; BASS, L.; PAUTASSO, C. *A Taxonomy of Blockchain-Based Systems for Architecture Design*. IEEE International Conference on Software Architecture (ICSA), Gothenburg, 2017.

_____.; PAUTASSO, C.; ZHU, L.; GRAMOLI, V.; PONOMAREV, A.; TRAN, A. B.; CHEN, S. *The blockchain as a software connector*. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. Disponível em: <http://10.1109/WICSA.2016.21>, 2016.

YAGA, D.; MELL, P.; ROBY N.; SCARFONE K. *Blockchain Technology Overview*. Disponível em: < https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>, 2018.

YAVUZ, E.; KOÇ, A. K.; CABUK, U. C.; DALKILIÇ, G. *Towards Secure E-Voting Using Ethereum Blockchain*. 6th International International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey. Disponível em: <https: //www.researchgate.net/publication/323318041>, 2018.

YIN, R. K. *Case study research: design and methods*. 6th ed. Thousand Oaks, CA: Sage, 2017.

YLI-HUUMO, J.; KO, D.; CHOI, S.; PARK, S.; SMOLANDER, K. *Where Is Current Research on Blockchain Technology? A Systematic Review*. Disponível em: < https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477>, 2016.

ZAGÓRSKI, F.; CARBACK, R. T.; CHAUM, D., CLARK, J., ESSEX, A.; VORA, P. L. *Remotegrity: Design and use of an end-to-end verifiable remote voting system*. In *International Conference on Applied Cryptography and Network Security. Springer*, 2013.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H. *Blockchain challenges and opportunities: a survey.* Disponível em: < https://www.semanticscholar.org/paper/Blockchain-challenges-and-opportunities%3A-a-survey-Zheng-Xie/305edd92f237f8e0c583a809504dcec7e204d632>, 2018.

ZHANG, W.; HU, Y.; YUAN, Y.; HUANG, S. *A Privacy-Preserving Voting Protocol on Blockchain.* IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018.

ZHAO, Z.; CHAN, T. H. H. *How to Vote Privately Using Bitcoin*. In Sihan Qing, Eiji Okamoto, Kwangjo Kim, and Dongmei Liu, editors, Information and Communications Security: 17th International Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers, volume 9543 of LNCS. Springer, 2016.

9. SITES ACESSADOS

AGORA. Disponível em: <https://agora.vote>; <https://medium.com/agorablockchain/agora-official-statement-regarding-sierra-leone-election-7730d2d9de4e>, 2018.

BERLINER BPM-OFFENSIVE. Disponível em: <http://bpmb.de/index.php/BPMNPoster>, 2015.

BOULÉ. Disponível em: <https://www.newswire.com/news/introducing-boul-blockchain-based-online-voting-technology-19975015>, 2018.

CALIFORNIA INTERNET VOTING TASK FORCE. Disponível em: < https://elections.cdn.sos.ca.gov/ivote/final_report.pdf>, 2000.

CARTER CENTER. *Internet Voting Pilot: Norway's 2013 Parliamentary Elections*. 2014. Disponível em: >http://www.cartercenter.org/resources/pdfs/peace/democracy/Carter-Center-Norway-2013-study-mission-report2.pdf>.

COALICHAIN. Disponível em: <https://www.coalichain.io/>, 2017.

COUNCIL OF EUROPE. Disponível em: < https://www.coe.int/en/web/electoral-assistance/e-voting>, 2017.

DEF CON 2017. Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure. Disponível em: <https://www.defcon.org/>, 2019.

DEMOCRACY.EARTH. Disponível em: <https://www.democracy.earth/>, 2017.

DRAW.IO. Disponível em: < https://app.diagrams.net>, 2018.

ESTONIA. *Centre of Excellence for Internet Voting*. Smartmatic. Cybernetica. Disponível em: < https://www.ivotingcentre.ee>, 2014-2016.

_____. *e-Estonia*, 2018.

_____. *ID*, 2018.

_____. *General Framework of Electronic Voting and Implementation of National Elections in Estonia - IVXV Scheme*. Estonian Information System Authority (RIA), 2017.

_____. *Riigikogu Election Act*. Disponível em: <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504122017004/consolide>, 2018.

_____. *Municipal Council Election Act*. Disponível em: <https://www.riigiteataja.ee/en/tolge/pdf/502012019005>, 2018.

_____. *Digital Signatures Act*. Disponível em: <https://www.riigiteataja.ee/en/eli/530102013080/consolide>, 2014.

_____. *Information System Authority (RIA)*. Disponível em: <https://www.ria.ee/en.html>, 2018.

_____. *IVXV online voting system*. GitHub. Disponível em: <https://github.com/vvk-ehk/ivxv>, 2017.

_____. *E-valimiste Turvalisuse Töörühma Koondaruanne. (E-election Security Working Party Summary Report)*. Disponível em: < https://www.mkm.ee/sites/default/files/e-alimiste_tooruhma_koondaruanne_12.12.2019.pdf>, 2019.

ETHEREUM. Disponível em: <https://ethereum.org/pt-br/>, 2015.

EUROPEAN COMMISSION. *Desi. The Digital Economy and Society Index*. Disponível em: <https://ec.europa.eu/digital-single-market/en/desi>, 2018.

_____. *eGovernment infographics brochure*: European Union. Disponível em: <https://joinup.ec.europa.eu/sites/default/files/inline-files/SC502_D08_eGovInfographicBrochure_v2.00_2.pdf>, 2018.

_____. *European Parliament Election Act.* Disponível em: <https://www.riigiteataja.ee/en/eli/504122017001/consolide>, 2018.

_____. *European eGovernment Benchmark.* Disponível em: <https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2018-digital-efforts-european-countries-are-visibly-paying>, 2018.

E-VOTING.CC. *Map of E-Voting Usage in the World*. Disponível em: <http://www.e-voting.cc/en/it-elections/world-map/>, 2018.

E-VOX. *Open e-Democracy Platform*. <http://e-vox.org/>, 2017.

FOLLOW MY VOTE. Disponível em: <https://followmyvote.com/>, 2016.

ITU COPENHAGEN. USA: *Virginia ditches DRE voting machines after ITU researcher's hack*. Disponível em: <https://en.itu.dk/about-itu/press/news-from-itu/2017/virginia-uk#>, 2017.

MONERO. *The Moneto Project*. Disponível em: <https://github.com/monero-project>, 2019.

NISS. *Nordic Institute for Interoperability Solutions*. Disponível em: <https://github.com/nordic-institute/X-Road-code-amples/blob/master/COMPONENTS.md>.
NOIZAT, Pierre. Chapter 22 – blockchain electronic vote. In David Lee Kuo Chuen, editor, Handbook of Digital Currency. Academic Press, San Diego, 2015.

OAS. *Organization of American States*. Department of Electoral Cooperation and Observation. Disponível em: <http://www.oas.org/en/spa/deco/>, 2019.

OECD. *The Organisation for Economic Co-operation and Development*. Disponível em: <http://www.oecd.org/gov/>, 2018.

ONLINE VOTING. *Successfully Solving the Challenges*. TIVI Whitepaper. Disponível em: <http://www.smartmatic.com/fileadmin/user_upload/Whitepaper_Online_Voting_Challenge_Considerations_TIVI.pdf>, 2018.

OSCE/ODIHR. *ESTONIA PARLIAMENTARY ELECTIONS 6 March 2011.* Disponível em: <https://www.osce.org/files/f/documents/a/9/77557.pdf>, 2011.

_____. *Handbook for Observation of new voting technologies*. Disponível em: <https://www.osce.org/odihr/elections/104939?download=true>, 2013.

_____. *ESTONIA PARLIAMENTARY ELECTIONS 3 March 2019 ODIHR Election Expert Team Final Report 2019*. Disponível em: < https://www.osce.org/odihr/elections/estonia/424229?download=true>, 2019.

POLYS. Disponível em: <https://polys.me/admin/create-vote/1591467678528>, 2018.

RE:PUBLICA. *Digital Democracy*: E-Voting for everyone? Disponível em: <https://re-publica.com/en/session/digital-democracy-e-voting-everyone>, 2017.

SCYTL. *Company Overiew*. About the Founder. Disponível em: <https://www.scytl.com/en/company-overview/>, 2016.

SECUREVOTE. Disponível em: <https://secure.vote/>, 2016.

SOLIDITY. Disponível em: <https://solidity-portuguese.readthedocs.io/pt/latest/#>, 2017.

SOVRIN NETWORK. Disponível em: <https://sovrin.org>, 2020.

STARTUP ESTONIA, 2020. Disponível em: <https://startupestonia.ee/startup-database>, 2020.

THE SOCIAL SMART CONTRACT. Disponível em: <http://paper.democracy.earth/>, 2018.

TIVI. Disponível em: <https://tivi.io/>, 2015.

UNIVERSITY OF WASHINGTON COMPUTER SECURITY. *Security Review: Helios Online Voting*. 2009. Disponível em: <ttps://cubist.cs.washington.edu/Security /2009/03/13/security-review-helios-online-voting/>, 2019.

UNPAN. *United Nation Public Administration Network*. Disponível em: <http://www.unpan.org>, 2018.

WOMBAT VOTING SYSTEM. 2011. How to Vote: Wombat Voting System. Disponível em: <http://www.wombat-voting.com/how-to-vote>, 2019.

VOATZ. Disponível em: <https://voatz.com/>, 2016.

VOTEWATCHER. Disponível em: <http://votewatcher.com/>, 2017.

10. GLOSSÁRIO

Accountability - termo na língua inglesa que significa responsabilização com ética.

Algoritmo - sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas.

Anonimato - sigilo da informação que relaciona uma determinada pessoa.

Anonimização - técnica de criptografia computacional para ocultar um dado.

Aplicativo - programa de computador concebido para processar dados eletronicamente, facilitando e reduzindo o tempo de execução de uma tarefa pelo usuário.

Application Programming Interface (API) - interface para programação de aplicação.

Assinatura eletrônica - qualquer dispositivo eletrônico para identificar uma pessoa.

Assinaturas em anel - técnica de criptografia para ocultar o remetente.

Autenticação de dois fatores – requer a verificação de acesso em outro canal eletrônico de acesso (código de acesso e etc.), ou seja, *two-factor authentication* é a maneira de ter mais uma forma de acessar a sua conta pessoal de qualquer plataforma na Internet.

Backbone - rede de transporte que designa o esquema de ligações centrais de um sistema de redes mais amplo, tipicamente de elevado desempenho e com dimensões continentais.

Banco de dados - conjunto de dados inter-relacionados sobre determinado assunto, armazenados em sistemas de processamento de dados segundo critérios preestabelecidos; base de dados.

Bitcoin - criptomoeda ou moeda eletrônica.

Botnets – rede formada por centenas ou milhares de computadores "zumbis" e que permite potencializar as ações danosas executadas pelos *bots.*

Bot – programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.

Bug - falha em dispositivo ou programa de computador.

Business-to-business (B2B) - relacionamento restrito entre empresas.

Blockchain - tecnologia de registro distribuído com o objetivo de descentralizar a tomada de decisão através de um protocolo de consenso como medida de segurança.

Bloco *genesis* - primeiro bloco da cadeia *blockchain.*

Código malicioso *(Malware)* – são programas de computador específicos para executar ações que causem danos ou atividades maliciosas em nome do usuário.

Core business – negócio principal de uma empresa.

Chave criptográfica - técnica de comunicação segura na presença de terceiros que utiliza algoritmos de operações matemáticas. Há dois modelos: chave criptográfica privada (private key) para ocultar a mensagem e a chave criptográfica pública (public key) para ler a mensagem.

Chip - circuito integrado utilizado para operações matemáticas.

Criptograma - lógica algoritma pré-determinada para decifrar uma mensagem.

Criptomoeda - tecnologia da *blockchain* para assegurar a validade das transações.

Distributed Denial of Service (DDoS) - técnica pela um atacante utiliza um conjunto de computadores distribuídos para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

E-Democracy - participação dos cidadãos em assuntos governamentais pela Internet.

E-Governance - tecnologias da informação na prestação de serviços eletrônicos.

E-*Government* - prestação de serviços eletrônicos pela Internet.

End-to-End verifiability (E2E) - técnica de verificação de ponta a ponta utilizada para auditar processos de votação em eleições.

E-Participation - participação dos cidadãos no governo pela Internet.

E-Public administration - conjunto de políticas públicas para a Internet.

Error handling - processo de resposta à ocorrência de exceções ou condições anômalas ou excepcionais que requerem processamento especial durante a execução de um programa de computador.

E-Voting – dispositivo mecânico ou eletrônico para votação em eleições.

Government to Citizen (G2C) - relacionamento entre o governo e o cidadão.

Hardware Security Module (HSM) - dispositivo de computação que protege e gerencia chaves eletrônicas e executa funções de criptografia. Esses módulos são uma placa de *plug-in* ou um dispositivo externo que se conecta diretamente a um computador ou servidor de rede.

Hash function - algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo.

Insider threat - ameaça interna para uma organização proveniente de pessoas da organização, como funcionários, ex-funcionários, terceirizados ou parceiros de negócios, que possuem informações privilegiadas sobre as práticas de segurança, dados e sistemas de computadores da organização.

ID Card - cartão eletrônico de identificação pessoal que pode ser também via celular.

Internet das coisas - conceito de que todos os dispositivos eletrônicos estão interconectados pela Internet.

Internet voting - processo de votação eletrônica pela Internet.

I2P - projeto de Internet invisível é uma rede sobreposta e *darknet* que permite que as aplicações de *software* enviem e recebam mensagens para outros na rede e de forma segura, sob pseudônimos.

Java - linguagem de programação para computadores.

Ledger - registro da cadeia de blocos de uma rede *blockchain.*

Liquid democracy - forma de democracia delegativa em que o poder de votar de uma pessoa é transferido para um representante indicado por ela.

Man-in-the-middle - forma de ataque em que os dados trocados entre duas partes são interceptados, registrados e alterados pelo atacante sem o conhecimento da vitima.

Middleware - *software* de computador que fornece serviços para *softwares* aplicativos além daqueles disponíveis pelo sistema operacional.

Miner - *node* que competem entre si para validar um *hash function* e alocar um bloco na cadeia do *ledger* de uma rede *blockchain.*

Modus operandi – termo em latim que significa modo de operação.

Node - nó de rede ou usuário com um computador que participa de uma rede *blockchain.*

Off-line – sistema com acesso à Internet.

On-line – sistema sem acesso à Internet.

Once-only - conceito de *e-government* para garantir que cidadãos, instituições e empresas tenham apenas que fornecer certas informações às autoridades apenas uma vez.

Personal Indentification Nunmber (PIN) - código de segurança que pode ou não divergir da senha de acesso de um determinado sistema com no máximo dez dígitos.

Phishing – ocorre por meio de mensagens eletrônicas aonde o atacante tenta obter dados da vítima por meio técnico e engenharia social.

Privacy by desing - conceito de que todo projeto em sistemas deve ser construído respeitando a privacidade dos dados pessoais.

Protocolo de consenso – serve para alcançar a confiabilidade geral de um sistema pelo consenso entre todos os participantes, por exemplo, o protocolo de prova de trabalho do *blockchain*.

Integridade de dados - manutenção e a garantia da precisão e consistência de dados durante todo o ciclo de vida da informação.

Proxy - é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.

QR Code - código de barras bidimensional que pode ser facilmente escaneado usando a maioria dos telefones celulares equipados com câmera.

Random number - número aleatório ou randômico é um número que pertence a uma série numérica e não pode ser previsto a partir dos processos anteriores da série.

Remote voting – conceito de votar pela Internet.

Ring Confidential Transactions (RingCT) - recurso de privacidade que foi implementado no protocolo *Monero*. Com transações confidenciais, a privacidade transacional dos usuários é aprimorada porque o valor dos dados transferidos é ofuscado.

Secure Sockets Layer (SSL) - tipo de segurança digital que permite a comunicação criptografada entre um website e um *browser*, sem a necessidade de uma *Virtual Private Network (VPN)*.

Segurança da informação - conjunto de padrões técnicos para proteger e preservar dados e informações no ambiente físico ou remoto. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e a legalidade.

Smart contract - programa de computador ou um protocolo de transação que se destina a executar, controlar ou documentar ações e eventos de acordo com os termos de um contrato ou protocolo de consenso.

Smart device - dispositivo "inteligentes" com acesso à internet.

Spoofing – técnica que o atacante pode se passar por um usuário ou um dispositivo eletrônico para roubar dados e informações.

Servidor de dados - computador conectado a uma rede interna ou pela Internet que tem o objetivo proporcionar um local para o armazenamento de arquivos.

Session code - código de sessão para vincular um determinado dado à um registro localizado em servidor de dados.

Sistema distribuído - sistema que interliga vários nós de rede pela Internet.

Startup - uma empresa emergente que tem como objetivo principal desenvolver ou aprimorar um modelo de negócio.

Stealth (address) - técnica de criptografia para ocultar o destinatário.

Sybil attack – técnica computacional para criar em um sistema psedo-usuários para influenciar e manipular o sistema.

Sufrágio – processo de votação para eleição política.

Time-stampig - marcação de tempo (data e hora) de um registro computacional.

Token - na rede *blockchain* é um ativo eletrônico que pode ser uma criptomoeda.

Tor - *software* livre e de código aberto que proporciona a comunicação anônima e privada pela Internet.

Unicórnio - é uma *startup* que possui avaliação de preço de mercado no valor de mais de um bilhão de dólares.

Upload - utilizado para referenciar a transmissão de dados de um dispositivo para outro através de um canal de comunicação previamente estabelecido em redes de computadores.

Virtual Private Network (VPN) - rede de comunicações privada construída sobre uma rede de comunicações pública como a Internet.

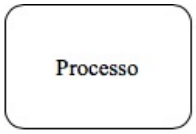
Voto de cabresto - é um mecanismo de acesso aos cargos eletivos por meio da compra de votos com a utilização da máquina pública ou o abuso de poder econômico.

X-Road – plataforma *middleware* do *e-governance* da Estônia.

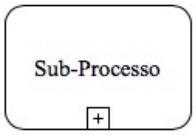
Zero knwonoledge proof - na criptografia uma prova de conhecimento-zero ou protocolo de conhecimento-nulo é um método interativo que possibilita uma parte provar para outra que uma declaração é verdadeira sem revelar qualquer coisa além da veracidade da declaração.

11. APÊNDICE

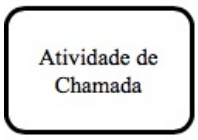
Segue abaixo a simbologia do *BPMN 2.0 - Business Process Model and Notation* utilizada na pesquisa acadêmica (BERLINER BPM-OFFENSIVE, 2015, com adaptações).



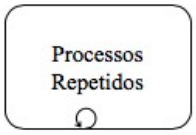
Processo é um entidade que representa um *software* dentro de um sistema computacional.



Sub-Processo indica(m) outro(s) processo(s) com **Marcador de Sub-Processo** ⊞. Dependendo do **Evento**, ele pode interromper o fluxo de um processo ou executá-lo em paralelo sem interrompê-lo.



Atividade de Chamada é uma referência a um (sub)processo definido globalmente e que pode ser (re)utilizado dentro do tempo permitido.



Processo com Marcador de Repetição ↻ significa que a atividade realizada dentro de um processo é cíclica e temporal.

Evento de Início padrão que indica um ponto de partida de um processo.

Evento Intermediário indica um ponto de partida entre um ou mais processos.

Evento Final padrão que indica o final de um processo.

Evento Temporal signifca tempo de um processo (instante, intervalo ou limite de tempo) que podem ser evento único ou cíclico.

Condicional significa uma condição na regra de negócio institucional.

Desvio é um ponto de ramificação em que os fluxos de saída são ativados simultaneamente. No caso de convergência de fluxos, espera-se que todos os caminhos de entrada estejam conclusos antes de disparar o fluxo de saída.

Fluxo de Sequencia define a ordem de execução de tarefa e o fluxo de dado.

Fluxo de Mensagem simboliza fluxo de informação que transpõe fronteira interna e externa de um sistema ou regra de negócio institucional.

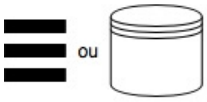
Fluxo de Mensagem com Dados significa que a informação é transmitida e/ou processada entre um ou mais (sub)processos.

Link de Dados representa um canal de transmissão de dados de um sistema computacional.

Mensagem *(black)* é usada para representar o conteúdo de uma comunicação entre processos. Neste caso, o *software* de criptografia com a chave pública.

Mensagem *(gray)* é usada para representar um dado tratado entre um ou mais processsos que será (re)utilizado pelo mesmo ou outro processo de um sistema.

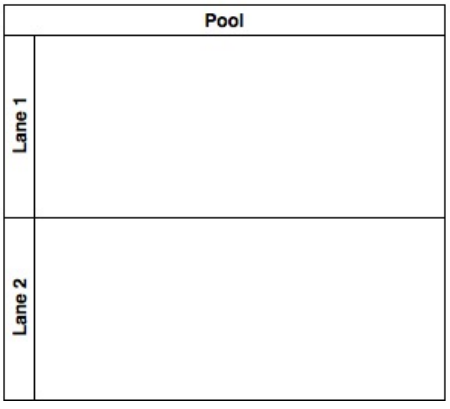
Mensagem *(white)* é usada para representar o conteúdo de uma comunicação entre dois processos. Neste caso, o *software* de descriptografia com a chave privada.



Repositório de Dados é um local onde um (sub)processo pode ler e escrever na base de dados ou um sistema de arquivos.

Anotação é usada para expor qualquer informação no (sub)processo.

Evento de Perímetro é para relacionar no mesmo perímetro um ou mais (sub)processos de um sistema e a interoperabilidade entre eles e demais sistemas de fora do perímetro.



Agrupamento de Atores indica a divisão e o grau de responsabilidade pelas atividades realizadas dentro de um sistema computacional ou regra institucional.