UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES E TELEINFORMÁTICA

MARSHALL MOSHE MAURICIO DO NASCIMENTO

BLOCKCHAIN: UMA NOVA ABORDAGEM SOBRE VOTAÇÃO ELETRÔNICA

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

MARSHALL MOSHE MAURICIO DO NASCIMENTO

BLOCKCHAIN: UMA NOVA ABORDAGEM SOBRE VOTAÇÃO ELETRÔNICA

Monografia de Especialização, apresentada ao Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Esp. Douglas Eduardo Basso

CURITIBA
2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Redes de Computadores e Teleinformática

TERMO DE APROVAÇÃO

BLOCKCHAIN: UMA NOVA ABORDAGEM SOBRE VOTAÇÃO ELETRÔNICA

por

MARSHALL MOSHE MAURICIO DO NASCIMENTO

Esta monografia foi apresentada em 23 de Novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Esp. Douglas Eduardo Basso
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à minha família, amigos por sempre me apoiarem nos momentos de maior dificuldade, ao professor e orientador Douglas Basso, por sempre estar disponível e indicar o melhor caminho durante o desenvolvimento deste trabalho.

AGRADECIMENTOS

Agradeço ao professor Douglas Eduardo Basso, por sua compreensão, dedicação e comprometimento durante a produção deste trabalho, orientando com conselhos e dicas, sempre mostrando o caminho a ser trilhado.

Agradeço a minha família, pelo carinho, paciência, e suporte que forneceram todo o tempo, sendo imprescindível para chegar até.

Agradeço aos meus amigos por terem acreditado todo o tempo e por toda motivação fornecida, todas as broncas e cobranças, pelos conselhos e apoio em todos os momentos que de alguma forma foram importantes e contribuíram pra eu chegar até aqui.

Agradeço a todos os professores que de alguma forma contribuíram para minha formação não apenas como aluno mais como pessoa, pois durante esses meses de curso eles proporcionaram condições para evoluir em vários aspectos que julgo fundamentais para me tornar um profissional melhor.

A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê. (Arthur Schopenhauer)

RESUMO

NASCIMENTO, Marshall Moshe Mauricio do. **Blockchain: Uma nova abordagem sobre votação eletrônica**. 2018. 46 p. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

O surgimento do Bitcoin mostrou uma nova abordagem sobre velhos paradigmas, incorporando em si o Blockchain, resolveu várias questões relacionados a moeda digital, e abriu o caminho para que outras áreas usufruam de suas capacidades, seu potencial de mesclagem com outras tecnologias se mostrou capaz de resolver. Algumas linhas de pesquisa buscam através do Blockchain, aprimorar o sistema de votação convencional, mostrando soluções para questões até então sem respostas. Utilizando de sua forma descentralizada e transparente para garantir toda a lisura do processo eleitoral, todos os votos armazenados na rede Blockchain são imutáveis e os próprios nós da rede garantem que são verdadeiros, pois nada é incluído sem que os nós da rede dê seu aval para arquivamento, esse registro de voto é extremamente auditável, podem ser verificado independente do momento por qualquer pessoa. Utilizando a criptografia para cifrar os dados enviados pelo meio de comunicação, a conversa entre os nós da rede se torna mais segura, evitando que dados sejam lidos, alterados, ou que alguma informação errada chegue aos outros nós. A integração de Sistemas, fornece a autenticação necessária de cada eleitor habilitado a votar, eliminando votos duplicados. A votação eletrônica está caminhando em direção a votação remota, onde dispositivos portáteis sempre conectados à internet, possam se tornar meios para votar em qualquer lugar ou hora.

Palavras-chave: Cifras. Criptografia. Blockchain. CriptoMoeda. Internet.

ABSTRACT

NASCIMENTO, Marshall Moshe Mauricio do. **Blockchain: A new approach to e-vote**. 2018. 46 p. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The emergence of Bitcoin showed a new approach to old paradigms, incorporating the Blockchain in itself, solving several issues related to digital currency, and opened the way for other areas to enjoy their capabilities, their ability to merge with other technologies proved capable of solve the most diverse situations. Some lines of research search through the Blockchain, improve the conventional voting system, showing solutions to questions until then unanswered. Using its decentralized and transparent form to guarantee the smoothness of the electoral process, all the votes stored in the Blockchain network are immutable and the network's own nodes guarantee that they are true, since nothing is included without the network nodes giving their endorsement. archiving, this poll record is extremely auditable, can be verified to any one by anyone. Using encryption to encrypt the data sent by the communication medium, it makes the conversation between the nodes of the network secure, preventing data from being read, altered, or some erroneous information reaching the other nodes. System integration provides the required authentication of each eligible voter by eliminating duplicate votes. Electronic voting is moving toward remote voting, where portable devices that are always connected to the Internet can become a means of voting anywhere, at any time.

Keywords: Cipher. Cryptography. Blockchain. Cryptocurrency . Internet.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

BEV	*Blockchain Enabled e-Voting*
DRE	*Direct Recording Electronics*
EC	*Elections Canadá*
EUA	Estados Unidos da América
EVM	*Eletronic Voting Machine*
ID	Identidade Digital
IDBIT	*Binary Digit*, menor unidade de medida na informática
LE	Lógica e Exatidão
MAC	*Message Authentication Code*
ODIHR	*Office for Democratic Institutions and Human Rights*
OSCE	*Organization for Security and Co-operation in Europe*
RSA	*Rivest Shamir Adleman*

SUMÁRIO

1 INTRODUÇÃO

A partir da década de 80, com a evolução da criptografia, foram feitas várias tentativas de criar moedas virtuais, porém estas funcionavam de maneira centralizada, se tornando fácil de ser atacada por hackers e governos. Era necessário criar um padrão descentralizado e seguro, que fosse robusto o suficiente para garantir que alguns pontos de falha em moedas anteriores fossem corrigidos (ANTONOPOULOS, 2017).

De acordo com Ulrich (2014) o Blockchain foi criado em 2008 por Satoshi Nakamoto, para fazer a validação de transações de Bitcoin (Moeda eletrônica). Seu funcionamento é semelhante a uma base de dados pública, que armazena cada transação envolvendo Bitcoin, onde cada nova transação é verificada e armazenada por todos os nós (participantes da corrente). Dessa maneira é eliminado o gasto duplicado da moeda, porque a própria rede de participantes se torna o intermediário que garante a confiabilidade da informação e guarda o histórico de cada transação.

O Bitcoin segundo Antonopoulos (2017) é a combinação das pesquisas em Sistemas distribuídos e criptografia, gerando um Sistema altamente robusto descentralizado, evitando que algum ponto possa ser controlado ou atacado comprometendo todas as transações.O Bitcoin é baseado em três bases, são elas:

- Rede ponto a ponto (com vários nós).
- Blockchain (cadeia de blocos).
- Moeda emitida de maneira descentralizada e com base em modelos matemáticos.

Orman (2018) diz que o Blockchain são arquivos de registros sequenciais e com carimbo de tempo. Onde uma função matemática é responsável pela atualização desse registro. Para que novos dados sejam acrescentados são utilizados os valores atuais e os que devem ser inseridos como parâmetros no cálculo. Os nós participantes do Blockchain são responsáveis por resolver a função matemática, assim como a validação do resultado obtido e dessa maneira permitir que todos atualizem o registro que possuem com os novos dados. A atualização dos registros é feita de maneira individual e independente.

Fiaidhi, Mohammed, Mohammed (2018) descrevem que o Blockchain também pode ser utilizado para Sistemas médicos, onde já existem empresas trabalhando em soluções utilizando Blockchain para criar um banco de dados unificado, dessa maneira o médico despenderia menos tempo fazendo partes administrativas, e tendo mais tempo para o atendimento ao paciente, Os autores vão ainda mais longe teorizando a possibilidade de que pesquisas e novos tratamentos podem ser difundidos nessa base facilitando a disseminação do resultados obtidos.

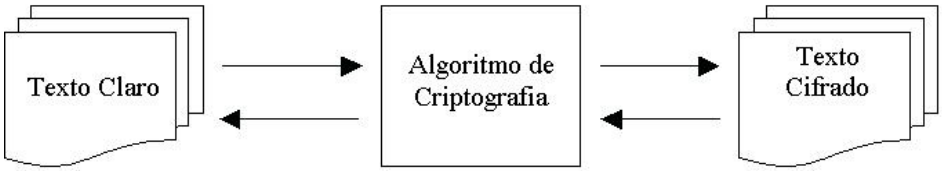
Para Yavuz et al. (2018), possuir um conceito distribuído com um alto nível de segurança, o Blockchain tem condições de abordar uma gama muito ampla de problemas e situações. Em particular a votação eletrônica é uma situação em que se pode utilizar o Blockchain. Por muito tempo, foram realizadas várias tentativas de implementar um novo modelo, porém poucas soluções se mostraram efetivamente confiáveis e continuam em uso. Há muitos métodos de pesquisa e questionários online, que de certa maneira obtiveram sucesso nesse ramo, entretanto esse tipo de metodologia não pode ser aplicado a eleições governamentais oficiais ou empresariais. Um dos principais motivos é que a eleição convencional é um elemento democrático utilizado em larga escala no mundo.

Para garantir que todo o processo de troca de informação entre os nós do Blockchain acontece de forma segura, e caso alguém intercepte algum pacote com parte da informação que não consiga decifrar será necessário o uso da criptografia.

A Criptografia desde sua criação, tem o objetivo de impedir o sucesso do interceptador ilegal dessa mensagem não tenha sucesso em decifra-la. A sua principal área de uso era a militar, protegendo informações importantes e evitando que alguém não autorizado conseguisse entender o que estava sendo transmitido. Com o seu aprimoramento novas áreas começaram a adotar os métodos criptográficos, abrangendo uma gama muito maior (MORENO; PEREIRA; CHIARAMONTE, 2005).

Para Moreno, Pereira e Chiaramonte (2005) a criptografia pode ser descrita como uma mesclagem de diversos métodos e técnicas para que de alguma forma fazer com que um texto seja muito difícil de ler, e aplicando todos os procedimentos de formar reversa tornar a mensagem legível novamente. Esse processo pode ser observado na Figura 1.

Figura 1 - Conceito básico criptografia



Fonte: Moreno, Pereira e Chiaramonte (2005).

Segundo Moreno, Pereira e Chiaramonte (2005) as cifras criptográficas substituem a informação original por combinações previamente definidas pelos algoritmos criptográficos. Dessa forma o receptor da mensagem deve possuir as combinações utilizadas para codificar a mensagem e assim desfazer todo o processo de codificação voltando à sua forma original e legível. Por cifra entende-se técnicas e métodos, que de alguma forma substituem os caracteres da mensagem original, garantindo assim que somente o destinatário correto possa decifrar todo o conteúdo e consequentemente ler o texto original.

1.1 PROBLEMA

De acordo com Bélanger e Carter (2010), o avanço da tecnologia proporciona aos governos novos meios para administrar e disponibilizar serviços a população. A eleição é um aspecto importante, e por isso é uma preocupação constante que, o processo seja sempre seguro, rápido e transparente. Em alguns países é adotado a votação pela internet, onde é possível ao eleitor votar através de dispositivos portáteis. Porém esse método, alguns pontos devem ser observados, pois além de ser seguro, transparente e veloz em suas funções, também deve possuir aceitação da população e ser acessível a todos os eleitores. É sabido que a aceitação desse tipo de sistema é variável de acordo com o nível de educação, renda, e acesso a tecnologia. Em lugares onde a população possuí um maior desenvolvimento esse tipo de sistema costuma ser mais aceito comparado a regiões com menos recursos.

No mundo moderno, um dos aspectos de maior valor em uma sociedade democrática, é um processo de votação, robusto, transparente em que ao mesmo tempo a privacidade do eleitor seja garantida. Votações são utilizados de diversas maneiras para diferentes assuntos, desde referendos de lei até em programas de televisão. Em eleições governamentais, ainda são utilizadas cédulas de papel em

alguns países. Isso gera questões sobre os custos, confiabilidade do método, assim como garantias que as cédulas entregues não serão alteradas ou ainda que novas serão incluídas para garantir vantagem na eleição (YAVUZ et al., 2018).

1.2 OBJETIVOS

O Sistema de votação, através de urnas eletrônicas ou cédulas de papel, apesar de serem os mais utilizados por vários anos, não representa o método mais eficiente, especialmente em países que possuem tecnologia avançada, e o governo possui cadastros atualizados da população votante.

Através desse contexto, a pesquisa a seguir busca mostrar uma nova vertente para o paradigma da votação eletrônica, utilizando do Blockchain para um Sistema eleitoral mais ágil, transparente e seguro.

1.2.1 Objetivo Geral

Verificar a viabilidade de uma nova metodologia de votação eletrônica utilizando Blockchain, assim como analisar seus requisitos de implantação, níveis de segurança, transparência e custo.

1.2.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

- Identificar as principais falhas e custos tanto no processo atual de votação quanto no processo proposto.
- Analisar viabilidade de mesclar tecnologias recentes e dispositivos eletrônicos no processo de votação.
- Verificar viabilidade de custos, níveis de segurança e transparência desse modelo.

1.3 JUSTIFICATIVA

Com o advento do Bitcoin, houve uma grande mudança em como observa-se o mercado financeiro assim como suas transações, seu modo descentralizado de validar transações que utilizam a moeda virtual, o grau de segurança e transparência mostrados. Como base para garantir que o Bitcoin funcione de maneira correta e segura e que as transações sejam efetivas e não possam ser alteradas, assim como eliminar um terceiro elemento para esse controle, está o Blockchain, um método automático que garante toda a integridade do funcionamento do Bitcoin.

Para Nofer et al. (2017), o mecanismo de consenso, onde maioria dos participantes da rede Blockchain votam se o livro razão será atualizado ou não, permite manter todos os fatos de maneira coerente entre os nós, utilizando uma coleção de regras e procedimentos, esse processo de consenso faz com que as transações sejam armazenadas em um bloco por um período para depois de validado ser transferido ao livro razão, onde não poderá mais ser armazenada essa informação. Todo esse processo de comunicação e validação dos nós é criptografado garantindo assim a segurança das informações transferidas pela internet.

Utilizar o Blockchain, oferece benefícios comparado aos Sistemas centralizados. Os nós da rede Blockchain não precisam verificar a confiabilidade do outro nó, visto que precisa da validação de todos, isso elimina a necessidade de uma terceira parte de confiança, consequentemente aumentando o nível de segurança, pois no modelo convencional os dados de transações assim como validações ficam armazenadas em um único local, aumentando a chance de invasão e roubo desses dados (NOFER et al., 2017).

Devido a sua flexibilidade de uso, várias áreas além da financeira podem usufruir dessa tecnologia, tais como: saúde, cartórios online, cadeia de fornecimento, etc. Este trabalho propõe o uso para votação eletrônica, não somente votações governamentais. Um Sistema de votação onde a transparência e integridade dos votos ali armazenados, possam ser auditados e consultados não somente pelos órgãos responsáveis pela eleição, e sim por todos os eleitores previamente cadastrados.

Swan (2018), sugere um modelo de eleição utilizando o Blockchain, recorrendo às amostragens para selecionar de forma aleatória os eleitores. Nesse método, os

selecionados seriam notificados, e dirigido à um site, onde os conteúdos de propaganda, com declarações, debates etc. A base dessa ideia que os eleitores tenham mais tempo para decidir sobre os temas apresentados, utilizando os recursos pessoais e tecnológicos que dispõe para a tomada de decisão. O Blockchain seria utilizado para o processo de seleção dos amostrados, podem inclusive ser utilizado em grande escala, de maneira confiável e garantindo o anonimato dos participantes.

1.4 ESTRUTURA DO TRABALHO

Esta monografia de especialização está dividida em 4 (quatro) capitulos. Neste primeiro capitulo foi introduzido o assunto tema do trabalho assim como a motivação e os objetivos geral e específicos da pesquisa, a justificativa e a estrutura geral do trabalho.

No segundo capitulo: Referencia teórica, será abordado o Blockchain, assim como conceitos de criptografia e votação eletrônica, fornecendo uma visão geral sobre os aspectos mais importantes de cada tecnologia. Mostrando seu funcionamento assim como as garantias de integridade e segurança dos dados durante todo o processo eleitoral.

No terceiro capitulo: Votação remota: é apresentada a metedologia remota eleição, onde não é mais necessário ir ao ponto pré definido para votar, utilizando dispositivos móveis e mesmo computadores conectados a internet é possível ao eleitor votar de onde estiver, mostrando os pontos necessários para sua adoção assim como vantagens de utilizá-la.

No quarto capitulo: Considerações finais, serão retomados a pergunta de pesquisa e os seus objetivos e apontado como foram solucionados, respondidos, atingidos, por meio do trabalho realizado. Além disto, serão sugeridos trabalhos futuros que poderiam ser realizados a partir do estudo realizado.

2 REFERÊNCIA TEÓRICA

Nesta seção será abordado os conceitos, modo de funcionamento e requisitos do Blockchain, criptografia e votação eletrônica, demonstrando requisitos e funcioamento individual de cada tecnologia.

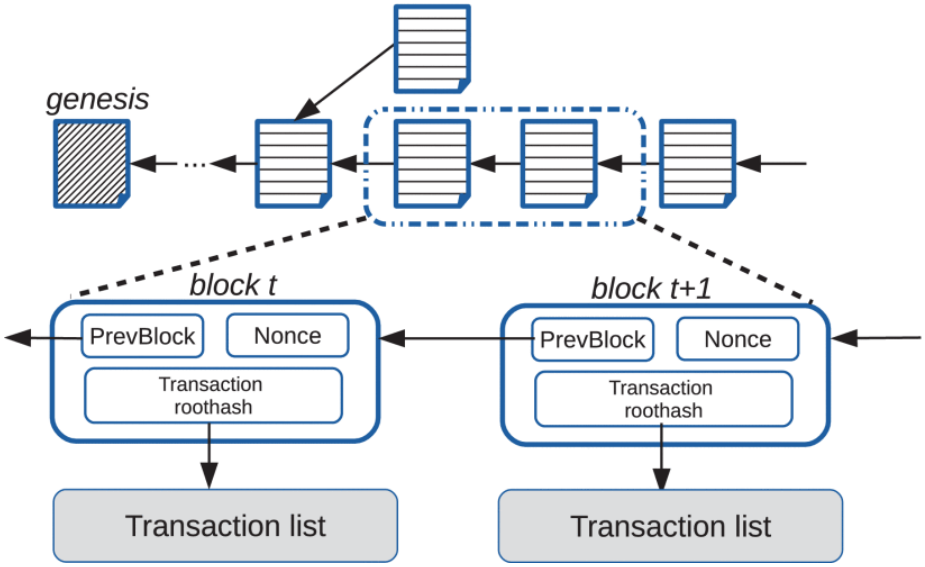
2.1 BLOCKCHAIN

Segundo Dinh et al. (2018), devido a febre do Bitcoin, as tecnologias que fazem a criptomoeda funcionar devidamente, também estão ganhando espaço, uma delas é o Blockchain. Também chamado de livro razão distribuído, devido a sua estrutura de funcionamento, que mantém todos os dados em um conjunto de nós que não possuem plena confiança um no outro. De uma forma muito simplificada o Blockchain é um log de transações organizadas e distribuídas. No cenário de banco de dados esta é uma alternativa para gerencia de operações distribuídas. Para isso funcionar todos os nós da rede Blockchain armazenam uma cópia do livro razão e por consenso adicionam novas transações nesses registros.

2.1.1 Como Funciona o Blockchain

Dinh et al. (2018) descrevem que basicamente o Blockchain consiste em vários participantes que não se confiam totalmente. Alguns desses nós se comporta de maneira bizantina (Um integrante pode mandar valores diferentes a participantes distintos, relativos a mesma informação). Em conjunto os participantes conseguem manter o Sistema distribuído e funcionando, realizando transações, onde o acordo entre a maioria dos nós da rede definem a ordem que o livro razão será atualizado com novas transações. A Figura 2, demonstra o arranjo dos dados no Blockchain, todos os blocos são ligados via ponteiro criptográfico, por este motivo é chamado de *ledger* (livro razão) distribuído.

Figura 2 - Estrutura de um bloco



Fonte: Dinh et al. (2018).

De acordo com Dinh et al. (2018) o Blockchain pode ser classificado em dois tipos, público ou privado. No caso do Blockchain ser público, não existe controle relacionado a entrada e saída dos nós (participantes, podem ser computadores, celulares inteligentes, ou qualquer outro dispositivo com capacidade de processamento) da rede Blockchain, a descentralização nesse caso é muito maior, se assemelhando muito a uma rede ponto-a-ponto (conexão direta entre os participantes, nesse tipo de rede não há um servidor central para gerenciar a comunicação, cada participante é o servidor de seu conteúdo). Na contramão o Blockchain do tipo privado possui um rigoroso controle sobre a entrada de novos nós e a saida de participantes da rede, utilizando mecanismos de verifição sobre os novos participantes, caso esse cumpra todos os requisitos exigidos é permitida sua participação na rede Blockchain, caso não cumpra sua entrada é recusada. Dessa forma todo novo participante da rede blockchain deve ser autenticado e todos os outros pares da rede devem ser informados dos novos participantes, é exigido que todos possuam conhecimento sobre todos os integrantes dessa rede.

2.1.2 Gasto Duplo

Em sua essência o Bitcoin é um passo de extrema importância na área da computação. Como resultado de anos de pesquisa em moedas digitais e criptografia,

os frutos dessas pesquisas resolve um grave problema que até a invenção do Bitcoin tornava impraticável o uso de moedas criptográficas, esse problema é o gasto duplo. Antes do Bitcoin e do Blockchain qualquer moeda poderia ser duplicada inúmeras vezes e dessa forma era muito difícil de saber se aquelas moedas já haviam sido gastas ou não anteriormente (uma analogia que pode-se usar é o anexo de um e-mail, que pode ser salvo inúmeras vezes, sendo impossível saber se o anexo já foi salvo ou não). Para resolver essa dificuldade, até então era utilizado uma terceira parte de confiança, onde validava as transações, garantindo que o dinheiro não fosse gasto em duplicidade (SWAN, 2018).

Para Swan (2018), essa questão do gasto duplo possui relação com uma situação muito mais antiga, remetendo aos Generais do império bizantino, onde esses generais não podiam confiar uns nos outros dentro do campo de batalha, porém era necessário coordenar a comunicação. Para resolver esse problema o Blockchain combina duas tecnologias e dessa forma garante que não haverá mais preocupação com esta questão, a metodologia de comunicação do BitTorrent (compartilhamento de arquivos, onde baixa-se direto do usuário fonte, uma rede ponto a ponto), que utiliza protocolos de rede ponto a ponto para compartilhar os arquivos, e a criptografia (utilizando chaves públicas e privadas), fornecem confiabilidade e segurança para a rede Blockchain. Quando uma nova Bitcoin ou outra criptomoeda é minerada, ela é adicionada a carteira do participante, e toda a rede confirma e valida essa operação, desse modo não é necessário confiança nos nós da rede, mais sim no Sistema como um todo, e cada bloco armazena transações que são guardadas de forma sequencial no livro razão do Blockchain. Uma vez armazenada, sua alteração é extremamente dificil, pois deve passar novamente pelo concenso de todos os participantes da rede, caso seja alterada em apenas um lugar, os outros integrantes serão notificados dessa alteração e a rejeitarão, decretando assim que essa nova informação é falsa.

2.1.3 Hash com Carimbo de Tempo

Conforme Ulrich (2014), diz que o Blockchain possui duas características fundamentais para serviços de certificação, a primeira é o hashing (um algoritmo matemático que transforma dados de tamanho mutável para dados de tamanho fixo), a segunda é o carimbo de tempo. Ele marca o dado com data e hora permitindo assim

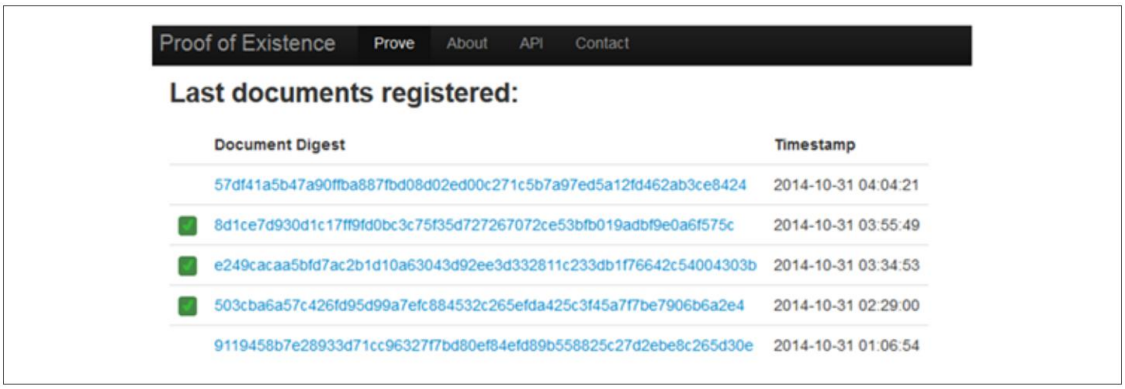
verificar quando aquele dado foi modificado ou inserido na listagem etc. O hashing pode ser usado em qualquer tipo de arquivo (imagem, áudios, pdf etc), ele retrata o conteúdo integral do arquivo, depois de aplicado o algoritmo de hashing, para desfazer essa transformação para volta-lo ao original basta reaplicar a técnica de códificação (hashing) e o arquivo voltará a ser o mesmo, desde que, o arquivo não tenha sido modificado. O tamanho do hash deve ser curto o bastante para que possa ser adicionado em forma de texto em uma transação Blockchain.

Conforme Ulrich (2014) descreve que o carimbo do tempo serve como forma de comprovar o momento especifico que uma transação ocorreu ou foi adicionado a lista, dessa forma o ledger Blockchain também pode ser utilizado como um registro. O conceito básico de utilização desse tipo de tecnologia é a utilização de hashes criptográficos para que ativos possam ser validados e atestados, dificultando assim possíveis alterações ou fraudes. Os principais serviços correlacionados ao Blockchain vão de arquivos, registros e validação de documentos. O principal destaque desse método é sua capacidade de apurar bens digitais através de um livro razão público.

2.1.4 Prova de Existência

Ulrich (2014), descreve a prova de existência como uma técnica que comprova a propriedade de dado sem expor o seu conteúdo, além de fornecer evidencias de data e hora da criação daquele documento. A Figura 3 demonstra uma captura de tela de um Sistema de ativos digitais, com a função de prova de existência.

Figura 3 - Documentos adicionados a lista de prova de existência



Fonte: Ulrich (2014).

A prova de existência funciona da seguinte maneira, ao adicionar o documento no Sistema Blockchain ele converte todo o conteúdo utilizando um hash criptográfico único, o resultado dessa transformação é um código único. Esse código é inserido em uma transação a fim de ser validado e receber o carimbo de tempo, em seguida esse hash é adicionado ao livro razão. A validação desse código pode ser feita utilizando o hash novamente, se o resultado for igual ao original este documento é validado e considerado valido, caso contrário ficará evidenciado que em algum momento foi adulterado (ULRICH, 2014).

Como mencionado anteriormente e de acordo com Ulrich (2014), o documento em si não é armazenado no Blockchain apenas o código que é gerado após a transformação do arquivo, ou seja o arquivo em si continua seguro em seu local de origem. A única forma de acessar esse código é através de uma chave privada, esta por sua vez é de conhecimento exclusivo de cada particpante, onde os demais integrantes de rede Blockchain, não conhecer essa informação. De maneira alguma o código pode ou deve ser traduzido para o documento original, hashes em sua essência são unidirecionais, ou seja, não é possível transformar o código gerado no documento original.

Conforme Ulrich (2014) descreve que devido as inúmeras aplicabilidades do Blockchain em conseguir provar a existência, assim como a integridade em dado momento dos dados ali armazenados, impressiona devido a sua alta confiabilidade e facilidade de auditoria, pois os dados ali armazenados podem ser consultados sempre que necessário. O fornecimento de um registro com data e hora junto de um estado que não foi alterado, mantendo confidencial o conteúdo que está armazenado pode ser usado para soluções civis ou governamentais dentre outras areas. Muitos profissionais da área pública assim como seus clientes poderiam usufruir de tais garantias ao poderem utilizar esses registros para provar a existências de documentos (notas promissórias, contratos, procurações etc.) que necessitem ser apresentados em algum momento como evidencia. O carimbo de tempo reforça a autenticidade do documento fornecendo a data e hora da criação daquele documento, garantindo assim a prova que o documento criado anteriormente é o mesmo do apresentado atualmente, dando celeridade à processos de autenticação de documentos, assim como validação de provas em processos que se fazem necessários apresentar evidencias ténicas.

2.2 CRIPTOGRAFIA

Ferguson, Schneier e Kohno (2010) descreve que o objetivo principal da criptografia é a encriptação ou seja a converção ou transmição dados em código. Quando duas partes querem se comunicar porém o canal utilizando para envio das informações não é seguro, faz necessário o uso de criptografia. garantindo que caso alguém consiga interceptar o que está sendo transmitido, não seja possível entender o conteúdo original o que está sendo enviado. Como padrão, deve-se assumir que os canais de comunicação não são seguros, dessa forma toda mensagem enviada pode ser escutada por todos que estiverem utilizando o mesmo canal. Partindo desse pressuposto deve-se garantir que terceiros possam capturar essa mensagem, não consigam entender o que está sendo transmitido, apenas o emissor e o receptor devem saber o que está sendo enviado, para isso é usado a criptografia.

Segundo Ferguson, Schneier e Kohno (2010) uma forma à garantir que apenas o emitente e o receptor possam entender a mensagem, é utilizando uma chave secreta (*Key*). Essa chave deve ser de conhecimento exclusivo apenas dos participantes da conversa, sendo assim nenhuma outra pessoa que está ouvindo no canal irá possuir conhecimento dessa chave. Para utilizar a chave criptografica, antes de enviar a mensagem, é utilizado uma função de de calculos matemáticos que irá embaralhar todo o conteúdo da mensagem utilizando como base um com conjunto de caracteres pré definidos (chave criptográfica), à vista disso apenas o receptor poderá descodificar essa mensagem, utilizando a mesma chave que foi definida anteriormente. Caso a mensagem seja interceptada é muito dificil de saber o seu conteúdo sem conhecimento dessa chave.

Partindo desse pressuposto, qualquer função matemática utilizada para criptografar mensagens deve ser segura e complexa o suficiente para garantir que dentre todas as possibilidades de extração de conteúdo da mensagem, as unicas informações possíveis de serem obtidas, sejam dados sobre o tamanho da mensagem assim como a hora de envio, porém é estritamente necessário que caso a mensagem seja capturada, e este terceiro não seja participante da conversa, ele não deverá conseguir entender o conteúdo (FERGUSON; SCHNEIER; KOHNO, 2010).

2.2.1 Princípio de Kerckhoffs

Para decifrar uma mensagem criptografada é necessário possuir duas informações, a primeira é o algoritmo de descriptografia, a segunda é a *Key* (chave criptográfica), como princípio de Kerckhoffs se baseia em garantir o sigilo da *Key*, na há preocupação em manter o algoritmo (grupo de regras e métodos lógicos, para à solução de um determinado problema possuindo número limitado de passos), pois caso a mensagem seja interceptada, possuindo conhecimento apenas do algoritmo é menos problemático. A principal razão para isso é devido a alta complexidade em atualizar ou customizar, que torna esse processo mais caro, dessa maneira um algoritmo pode ser utilizado por muito tempo e por muitas pessoas, o que torna todo o processo de decifrá-lo é relativamente mais fácil, pois o número de pessoas envolvidas é muito maior (FERGUSON; SCHNEIER; KOHNO, 2010).

Ferguson, Schneier e Kohno (2010) argumentam que outro ponto muito importante com relação aos algoritmos, é a necessidade de publicá-los para o maior número de comunidades de desenvolvedores. Dessa maneira, aumentam as chances de outras pessoas acharem erros de programação ou falhas de segurança, incrementando sua eficiência e segurança, tornando muito mais difíceis e complexos quaisquer tentativas de quebra dos mesmos. Por menor que seja a implementação na segurança seu impacto é muito grande, pois uma falha a menos que deixará ser explorada.

2.2.2 Autenticação

De acordo com Ferguson, Schneier e Kohno (2010), alguém que intercepte a mensagem enviada, pode não somente ouvir, mas também pode alterar ou excluir a mensagem. Para tanto é necessário que a pessoa que capture essas informações, possua muito controle sobre o canal de comunicação, contudo esse tipo de controle não é impossível. Partindo desse pressuposto alguém que consiga interceptar e apagar mensagens no meio de comunicação, pode excluir as mensagens originais, e enviar outra para o receptor, dessa forma quem recebe a mensagem não possui meios de validar o que recebeu, não é possível saber se o conteúdo enviado inicialmente foi ou não substituído no meio do caminho. Uma solução para este cenário é fazer com

que todas as mensagens enviadas possuam autenticação (método de identificação na), utilizando chaves que somente o emissor e o receptor conhecem. No entanto, as chaves utilizadas são diferentes das chaves criptográficas, tanto em seu uso quanto nos cálculos efetuados durante sua utilização.

Quando uma mensagem é enviada, um cálculo matemático utilizando a função *Message Authentication Code* (MAC) e a chave de autenticação é realizado, o receptor utiliza a chave de autenticação que possuí para fazer o cálculo inverso. Dessa maneira é possível validar a mensagem, se foi adulterada no caminho ou está intacta. Com esse processo se resolve uma parte do problema de alguém mal intencionado tentar sabotar a comunicação. Como a edição das mensagens foi garantida com a autenticação, ainda é possível excluir, alterar a ordem de entrega ou reenviar mensagens antigas. Para tratar esse tipo de situação é empregada uma técnica de numerar das mensagens em conjunto com a autenticação, dessa forma é garantido a quem recebe o ordenamento correto das mensagens o receptor não será enganado, caso a mensagem seja excluída, o receptor notifica quem envia para que seja retransmitida a mensagem (FERGUSON; SCHNEIER; KOHNO, 2010).

2.2.3 Encriptação por Chave

Segundo Ferguson, Schneier e Kohno (2010) um dos pontos mais importantes do uso da criptografia, é utilizando o compartilhamento de chaves criptográficas, quem envia a mensagem não deve enviar deliberadamente a chave pelo canal para o receptor. Dessa forma todos que utilizam o canal conseguirão obter e utilizar essa chave, fazendo com que todas as mensagens enviadas possam ser lidas e compreendidas. Como solução, foi proposto utilizar chaves públicas, onde cada indivíduo (pessoa ou equipamento) que envia mensagem no meio, possuem duas chaves, uma é enviada juntamente com a mensagem, e a outra é secreta, para exemplificar esse cenário serão utilizados dois atores: a) Ana, e b) Bob.

Como apresentado anteriormente, Bob irá gerar duas chaves que serão denominadas de chave secreta e a outra de chave pública, utilizando um algoritmo próprio pra isso, será criado às duas chaves. Após gerar as duas chaves, Bob divulga no canal a sua chave pública, para que assim todos no canal tomem conhecimento dessa chave, isso inclui Ana ou alguma outra pessoa mal-intencionada, sendo assim,

no momento que Ana quer enviar uma mensagem para Bob, ela necessita da chave pública dele, como a chave publica foi propagada no meio, ela ficará armazenada em algum repositório, ou em algum integrante do canal de comunicação, assim que ela obtém de uma fonte ou repositório confiável a chave pública de Bob, utilizando um algoritmo de criptografia e a chave pública de Bob ela criptografa e mensagem e dispara. Assim que Bob recebe essa mensagem ele deve então utilizar sua chave privada, utilizando o algoritmo de descriptografia, ele é capaz de decodificar a mensagem, independente da chave publica que foi usada, pois através de cálculos matemáticos a chave secreta é capaz de resolver e decifrar o texto enviado. Caso essa mensagem seja interceptada, sem a chave privada de Bob, não é possível decifrar o que foi enviado. Após decodificar Bob consegue ler a mensagem original (FERGUSON; SCHNEIER; KOHNO, 2010).

Ferguson, Schneier e Kohno (2010), descreve que a utilização de chave pública e privada na criptografia, trouxe a solução para o paradigma de propagar chaves pelo canal de comunicação e transformou a distribuição de chaves um problema mais simples de ser resolvido, dessa forma apenas uma chave é divulgada, enquanto a outra permanece secreta. Com isso o nível de segurança durante toda a comunicação é garantida, pois para decifrar é necessário utilizar a chave secreta que é de conhecimento apenas da pessoa que a criou.

2.3 VOTAÇÃO ELETRÔNICA

Adeshina e Ojo (2014) descrevem votação eletrônica como uma associação de vários dispositivos eletrônicos identificados como *Eletronic Voting Machines* (EVM). Nesse aspecto a gama de dispositivos é muito ampla não se mantendo apenas em urnas eletrônicas, mais abrangendo vários outros aparatos tecnológicos, como celulares, computadores etc. Além do próprio canal de comunicação (Ex: Internet, intranet, etc.). Como principal objetivo a digitalização dos vários processos de uma votação convencional utilizando cédulas de papel, etapas como, registro, verificação, contagem, todo o processo eleitoral em si. Uma vantagem em comparação aos métodos tradicionais, em termos de agilidade do processo como um todo, desde a organização, passando pelos cadastros, até a apuração dos resultados. Atualmente já é utilizado a votação digital através de urnas eletrônicas, onde estas possuem

sistemas próprios para gerenciar candidatos, computar votos, e um sistema central onde a apuração e divulgação dos resultados são muito rápidas e precisos.

Com o advento e popularização da internet e dispositivos inteligentes (celulares, tablets etc.), a votação remota se tornou uma opção viável, eliminando o deslocamento até o ponto de votação, reduzindo o tempo de votação, aumentando a comodidade e mobilidade do eleitor, pois com essa alternativa não há mais o empecilho de retornar a sua zona eleitoral para votar. Através de dispositivos moveis e com acesso à internet, é possível de votar em qualquer lugar e a qualquer hora. A automatização do processo representa uma forma de simplificar o processo eleitoral como um todo, visto que o tempo de apuração a taxa de erros são reduzidos e a (ADESHINA; OJO, 2014).

2.3.1 Direct Recording Eletronics (DRE)

Epstein (2007) descreve que há passos que devem ser seguidos para que o Sistema funcione de maneira correta, desde o desenvolvimento do software, passando pela plataforma (Sistema Operacional, hardware da urna eletrônica), até a apuração do voto. Durante o desenvolvimento do software, não há requisitos sobre como os desenvolvedores devem codificar os Sistemas DRE, porém é importante ressaltar que todos os Sistemas autorizados a serem utilizados passam por rigorosos processos de aprovação e controle, devendo seguir rígidas parametrizações do Governo federal para que sejam utilizados em eleições. Antes da utilização efetiva nas urnas é necessário que uma cópia do Sistema de votação seja validada. Garantindo assim que todas as etapas da utilização estejam de acordo com os padrões definidos pelos administradores da eleição.

Segundo Epstein (2007), outro ponto importante que passa por uma rigorosa verificação é a contagem dos votos, para isso é necessário utilizar testes de LE (Lógica e Exatidão), e seu foco não é encontrar erros ou falhas no software, ou seja, estes testes estão relacionados com a execução do sistema na urna, o objetivo principal é encontrar falhas na programação, no código fonte, falhas de lógica ou algum cálculo escrito incorretamente. Uma vez validada essa versão do software ela é distribuída para as urnas eleitorais que serão utilizadas.

No dia da votação antes da abertura das sessões é necessário realizar mais alguns passos para garantir que nenhuma urna seja configurada de forma errada ou tenha algum voto armazenado. Para isso, é necessário que um mesário instale o sistema na urna, sincronize as urnas com hora e data com o Sistema central. Além disso, é necessário imprimir a ‘fita zero’ para garantir que não há nenhum voto computado antes do início das votações. Durante o processo de votação o eleitor vai até o mesário para que seja registrada sua presença na zona eleitoral, após isso ele é liberado para votar, na urna, deve selecionar seus candidatos e após cada escolha confirmar, caso tenha digitado errado há a opção de corrigir. É permitido também digitar errado e confirmar, isso anulará o voto, ele também pode escolher votar em branco, para isso basta clicar na teclar ‘branco’ disponível no teclado da urna. Caso encontre algum erro deve submeter esses erros aos funcionários ali presente, para que as medidas necessárias sejam tomadas e assim a eleição prossiga de maneira correta. Os registros dos votos não são armazenados em um único bloco de memória na urna, eles são divididos em vários dispositivos de armazenamento, um desses é removível, e assim que a eleição é fechada esta mídia removível é enviada para apuração dos dados contidos, e comumente esses dados de registro são criptografados (EPSTEIN, 2007).

Após o fechamento do período de votação, segundo Epstein (2007), os funcionários devem mudar o status das urnas de ‘votação’ para ‘fechamento’, em seguida o mesário imprime o total de votos de cada máquina e compara com o número de eleitores, caso haja alguma diferença isso deve ser resolvido antes de enviar estes dados para a apuração oficial dos resultados. Após todos os procedimentos de fechamento, não havendo nenhum ajuste a ser feito é removido o cartão memória das urnas e enviados para a central responsável pela contagem oficial. Depois de receber os cartões, eles são inseridos de forma individual em um leitor, e um software especifico que foi desenvolvido pelo mesmo fabricante do Sistema da urna, faz a leitura dos dados ali contidos e recupera os totais, gerando assim o resultado oficial da eleição.

3 VOTAÇÃO REMOTA

De acordo com Al-ameen e Talab (2012), a votação do tipo remota, é mais flexível, permitindo que o eleitor utilize algum aparelho próprio para (celular, computador, etc.), não havendo necessidade de deslocamento até um local de votação ou supervisão de algum funcionário que trabalhe no processo eleitoral. Durante o processo de votar, é exigido o cumprimento de alguns requisitos de segurança e conectividade, para que todo o processo de eleição prossiga de maneira eficiente e sem equívocos e não sejam levantadas duvidas sobre sua validade.

3.1 CONTEXTUALIZAÇÃO SOBRE VOTAÇÃO REMOTA

Cetinkaya (2008), descreve que os requisitos de segurança embutidos em sistemas de votação eletrônico são contraditórios, usando como base conceitos de franqueza, recebimento e a não possibilidade de coibição. É possível deduzir que o sistema não deve permitir ao eleitor a comprovação sobre o conteúdo de seu voto, de certa maneira isso impossibilita que o votante venda, ou seja, coagido a votar em algum candidato. A verificação dos resultados assim como sua exatidão também são requisitos a serem observados com atenção, pois essas informações devem ser aferidas pelo órgão responsável pela eleição, assim como ficarem disponíveis para consulta do próprio eleitor, dessa maneira ele pode validar que foi computado corretamente no resultado geral da contagem dos votos.

O problema da votação surge da combinação desses requisitos. Especificamente, o problema de votação entre a liberdade de recebimento e a verificabilidade individual é descrito, pois há um *trade-off* (ato de escolher uma coisa em detrimento de outra) perceptível entre eles. Se o sistema de votação fornecer qualquer recibo que permita ao eleitor verificar seu voto na contagem final, então esse recibo também pode ser usado para compra ou venda de votos. A verificabilidade individual também contradiz a privacidade e a impossibilidade de coercividade, porque eles têm uma relação estreita com a franqueza do recebimento. Por exemplo, verificar um recibo é mais conveniente para um atacante do que comprar ou roubar chaves de acesso e lançar todos os votos. Se o recebimento de franquias não for cumprido, a não coercibilidade e privacidade não podem ser asseguradas (CETINKAYA, 2008).

Garantir a confiança não é algo fácil ou simples, pois a chance de adulteração dos votos ou resultados é existe, como forma de prevenir isso, a verificação do voto por parte do votante é extremamente necessária, pois ele pode validar manualmente que foi computado corretamente. Esse tipo de verificação auxilia que os usuários do sistema tenham a confiança que o processo todo ocorre de maneira correta e segura.

3.2 REQUISITOS DE SEGURANÇA

De acordo com Cetinkaya (2008), alguns requisitos básicos de segurança devem ser atendidos, dessa forma é gerado um grau maior de confiabilidade no processo como um todo, dentre estes pode-se destacar:

- Privacidade Eleitoral: É a não associação do voto ao eleitor, garantir a total privacidade e anonimato durante e após a eleição, para que tal façanha seja possível, é necessário desvincular e tornar-se não rastreável essa vinculação do eleitor ao voto. Existem algumas formas de atrelar o eleitor ao seu voto, pois é há algumas informações que são necessárias para validar a identidade e assim deixa um lastro do voto até o eleitor, o registro, chave pública, assim como endereço IP do eleitor são utilizados para a validação e verificação do voto, porém essas informações devem ser desvinculadas, garantindo a privacidade e anonimato do eleitor.
- Elegibilidade: Trata-se do eleitor que fez todos os processos de registros, para que possa votar remotamente, isso garante que apenas eleitores registrados estejam habilitados a votar.
- Precisão: A contagem dos votos deve ser feita corretamente, computando todos os votos validos, descartando aqueles que não seguirem as parametrizações de segurança, verificação e exclusividade, caso seja detectado qualquer alteração, inclusão ou exclusão de votos o sistema deve ser capaz de identificar esses casos e de maneira automática descarta-los.
- Exclusividade: O eleitor deve votar apenas uma vez, devendo ser proibido e bloqueado no sistema caso o eleitor tente votar novamente.
- Verificabilidade: Garantia que o processo eleitoral é exata, caso os protocolos atestem a exatidão da contagem necessariamente esses protocolos devem garantir a verificabilidade do processo como um todo, assim como

individualmente, permitindo que cada eleitor possa verificar que seu voto foi incluído corretamente.

- Equidade: Não deve haver resultado parcial, não é permitido a nenhum envolvido no processo (candidatos, eleitor ou autoridade), conhecimento parcial dos resultados, todos devem saber o resultado somente após a apuração total dos votos, sendo possível após isso a consulta dos votos.
- Não coercibilidade: Garantia que o eleitor poderá votar de maneira livre e confidencial, e o valor de seu voto deve ser protegido contra violações.

3.3 SISTEMA E-VOTAÇÃO “DEMOS”

DEMOS foi criado para ser um sistema de votação remota em que a verificação ponta a ponta é possível, dessa forma é permitido ao eleitor verificar seu voto depois de registrado, assim como sua privacidade e anonimato são mantidos. Sistema que possuem base votação por código, cada eleitor recebe uma cédula onde há todos os candidatos, cada candidato e recebe um código único, dessa forma o eleitor escolhe o código referente ao candidato na cédula e confirma seu voto. Na contagem é feito o cruzamento dessas informações, e para isso é utilizado elementos criptográficos que fazem a associação de todos os dados necessários para contagem, assim como a prova de trabalho (DELIS et al., 2014).

Em 2014 houve um caso de uso do DEMOS, utilizado em eleições europeias, Delis et al. (2014) descreve que a utilização ocorreu em duas escolas da região metropolitana de Atenas na Grécia, região extremamente populosa, no pátio dessas escolas haviam dois tablets assim como cartazes informando sobre a eleição, os eleitores puderam utilizar os tablets para votar assim como validar seu voto logo em seguida.

Delis et al. (2014) descreve a que na fase que antecede o processo eleitoral, uma autoridade precisa fornecer cédulas com números de série exclusivos e possuindo duas partes equivalentes, possuindo todos os dados para votar, em cada parte há códigos e cada código está atrelado a um candidato, esse código é criptografado e também está associado a um registro de voto, sendo assim esse modelo é chamado de cédula dupla. As cédulas são compartilhadas aos eleitores pelas autoridades, em seguida uma tabela é criada, usando como base um diagrama

de compromisso, gerando uma tabela T, todas informações são utilizadas para confirmar e vincular os candidatos, todos os candidatos são codificados primeiro, para depois serem confirmados. Todas as cédulas distribuídas possuem um número de série para cada lado, exemplo 100x, 100y, 101x, 101y e assim por diante, com base nisso a base onde essas cédulas são armazenadas possuí meios de validar e verificar os valores das cédulas ali armazenadas.

3.4 REGISTRO DO VOTO

Segundo Delis et al. (2014), assim como os demais sistemas eletrônicos de votação o DEMOS tem o pressuposto de garantir o sigilo do voto, dessa forma o método adotado é o da distribuição aleatória das cédulas, para realizar essa distribuição os números de série não possuem vínculos com os votantes, assim é entregue a cada eleitor uma cédula dupla, durante a votação em si é necessário que seja escolhido um lado, essa escolha deve ser feita de maneira aleatória, a cédula dupla possuí o objetivo de assegurar a integridade do sistema. Esse conceito de cédula dupla não é exclusivo do DEMOS, tendo sido utilizado em outros sistemas, pode-se citar como exemplo o Scantegrity (Utilizado em 2009, em Tacoma Park - EUA).O conteúdo da cédula é então verificado, por protocolos desenvolvidos especificamente para essa aplicação, caso passe nessa validação é então acrescentado ao registro, e fornece um comprovante do voto ao eleitor, dessa forma após o votante registrar seu voto, é possível conferir o que foi registrado no sistema, comparando com o comprovante emitido pelo sistema, um aspecto importante é que assim que o eleitor coloca seu voto na cédula é acrescentado 1 BIT (*Binary Digit*, menor unidade de medida na informática) de aleatoriedade.

3.5 APURAÇÃO DOS RESULTADOS E VALIDAÇÃO

Delis et al. (2014) descreve o processo de apuração em passos, seguindo uma esquematização para que cada voto computado seja verificado validado, e permitido ao eleitor consultar seu voto e caso necessário fazer o ajuste. A contagem de votos acontece após o período de votação ter sido concluído. O sistema central recebe todas as cédulas duplas (todos os dados são criptografados para garantir a segurança e

integridade das informações), abre as cédulas e valida os códigos ali contidos, dessa forma cada código validado é um voto para o respectivo candidato, conforme essa validação flui, é feita a contagem dos votos, e dessa forma o resultado é apresentado logo em seguida. Porém após a contagem dos votos as cédulas não são descartadas, elas são mantidas, assim o eleitor pode verificar novamente se o conteúdo do seu voto foi alterado ou não, permitindo uma segunda validação e verificação por parte dos eleitores. É importante ressaltar que nenhuma autoridade ou órgão oficial deve saber de antecipadamente quais cédulas serão destinadas a qual eleitor, isso garante o sigilo do voto assim como a não rastreabilidade do voto, a Figura 4 demonstra o processo de validação e verificação de cada voto mostrando os lados da cédula dupla.

Figura 4 - Esquematização para verificar votos

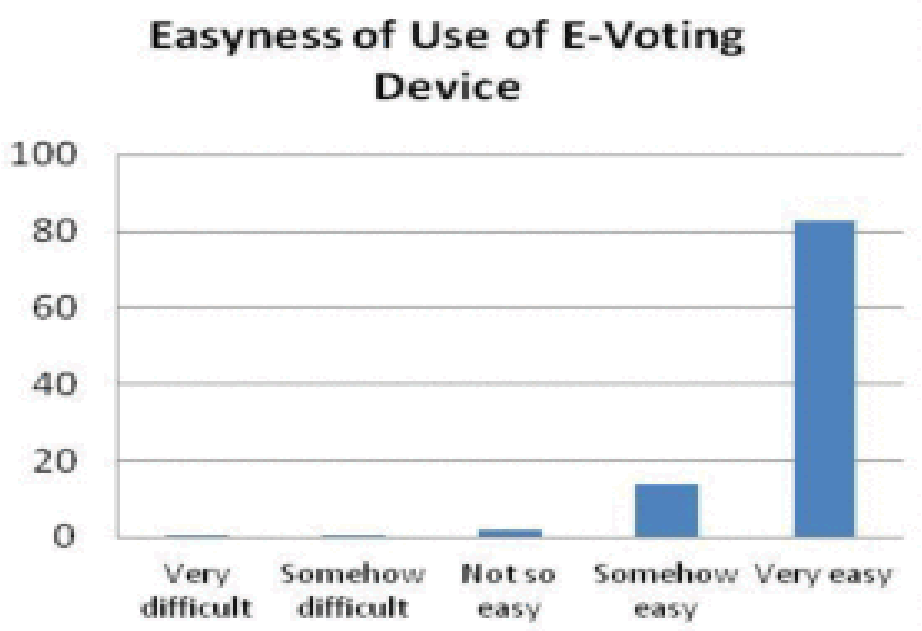
Fonte: Delis et al. (2014).

Após o processo eleitoral, segundo Delis et al. (2014), uma pesquisa de níveis de satisfação, aceitação e confiabilidade, foi efetuada. Dessa forma foi possível verificar pontos importantes com relação ao sistema e sua aprovação pelos pesquisados, os resultados dessa pesquisa são animadores, visto que em sua maioria as pessoas não somente gostaram do sistema como confiam em sua eficiência e segurança. Esse tipo de resultado é importante para que o sistema possa crescer melhorar e abranger situações maiores.

Os resultados demonstrados por Delis et al. (2014), conforme pode-se observar na Figura 5, o gráfico mostra o percentual com relação a facilidade de uso

do sistema. Um pouco mais de 80% dos eleitores, indicaram que foi muito fácil utilizar o sistema, mostrando que grande parte não tiveram dificuldades em votar. Um aspecto muito importante desse gráfico é a porcentagem dos que acharam muito difícil ou apenas difícil, ficam abaixo dos 5%, mostrando que praticamente todos conseguiram usar de forma plena o sistema. Deve ser levado em conta que a idade, nível de escolaridade e conhecimento em tecnologia são fatores muito importantes na hora de avaliar essa informação, pois pessoas idosas ou com pouco conhecimento em tecnologia terão mais dificuldades.

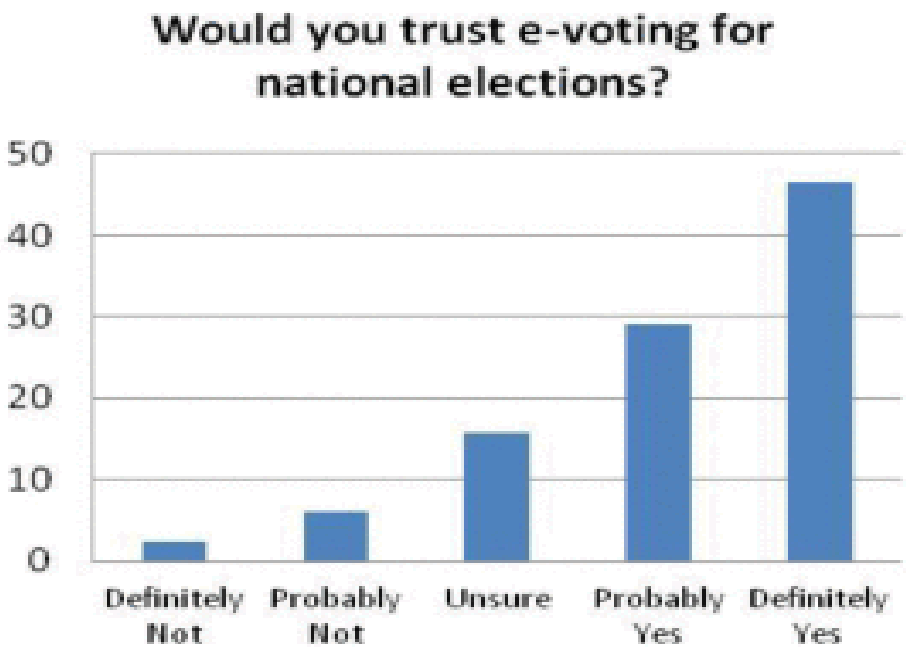
Figura 5 - Facilidade de utilização



Fonte: Delis et al. (2014).

Na Figura 6, é possível notar que o nível de confiança no sistema é extremamente alta, onde quase 50% dos eleitores disseram que possuem total confiança nesse tipo de sistema, outro ponto importante dessa questão é que a quantidade de entrevistados que de alguma forma confiam nesse tipo de sistema também é relativamente alta, com aproximadamente 30%. É possível notar que o nível de confiança, mesmo que provavelmente é muito alto chegando perto do 80%, mostrando que mesmo em eleições de grande escala, a população possui confiança em sistemas automatizados e online para gerir o processo eleitoral (DELIS et al., 2014).

Figura 6 - Nível de confiança no sistema

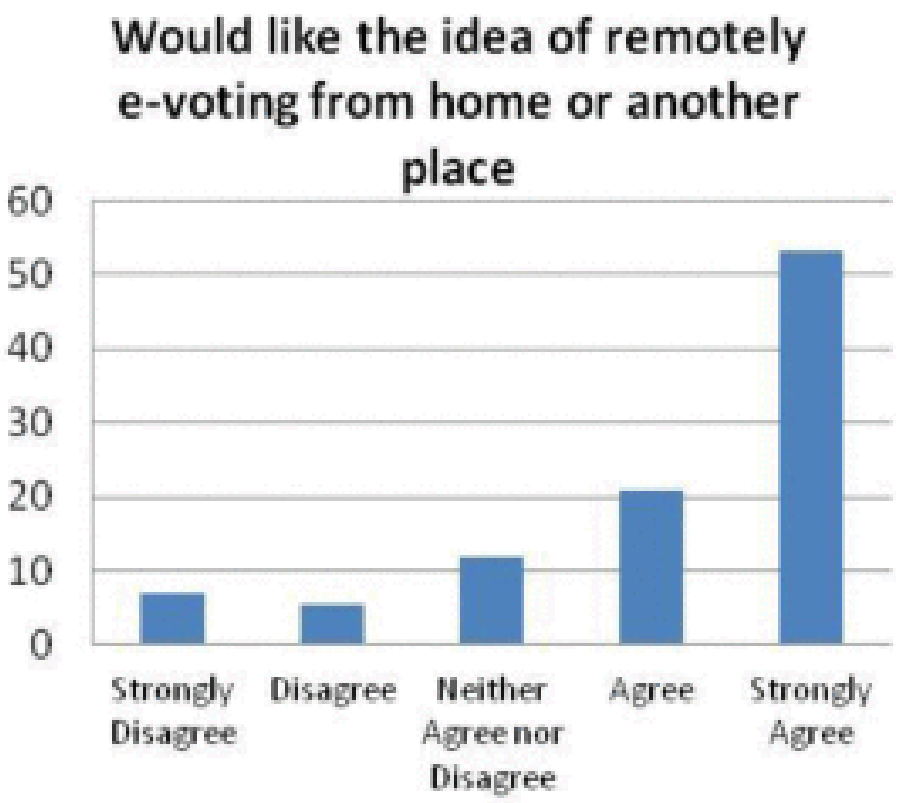


Fonte: Delis et al. (2014).

Para Delis et al. (2014), dentre os pontos pesquisados, um que deve ser mencionado é com relação a possibilidade de votar remotamente, independente do lugar, esse tipo de situação reduz a abstenção de eleitores, pois mesmo em dias de eleição. Um número muito grande de votantes não pode votar (justificam, ou simplesmente não comparecem), por não estarem em suas cidades, ou pela necessidade de se locomover até o local de votação que em muitos casos pode ser longe. A possibilidade de votar remota elimina essa situação, eliminando a necessidade de retorno à cidade do eleitor, ou que o mesmo se desloque.

Como pode-se observar na Figura 7, um pouco mais de 50% da população apoia fortemente essa ideia de votar de casa ou independente do lugar. Aproximadamente 20% dos entrevistados apoiam a ideia, somando essas duas parcelas é possível verificar que mais de 70% dos entrevistados aceitam e apoiam a ideia de votar remotamente, mostrando assim uma forte aderência nesse tipo de Sistema (DELIS et al., 2014).

Figura 7 - Aceitação da possibilidade de votar de qualquer lugar



Fonte: Delis et al. (2014).

3.6 CASOS DE USO

Neste será apresentado dois casos em que foi efetivamente utilizado sistemas de votação remota para a tomada de decisão assim como eleições gerais, demonstrando que mesmo em países desenvolvidos há uma crescente utilização de sistema digitais e online para votações. Também é apresentado de forma sucinta sua estrutura assim como resultados

3.6.1 Eleição Canadense pela Internet

De acordo Goodman e Pammett (2014), no Canadá há um órgão especifico chamado de Eleições Canadá (EC), responsável por toda eleição em âmbito federal, tendo como alguns pontos de gerencia, a fiscalização de finanças de campanha, propagandas, doações dentre outras atribuições, esse órgão está amparado pela legislação sobre eleições do Canadá, uma tentativa de atualização dessas leias foi

submetida a analise na Câmara e no Senado, o seu nome é *Fair Elections Act* (Ato de Eleições Justa). Um dos pontos da atualização é sobre a votação utilizando a internet, porém é necessário que seja aprovado pelo parlamento. O tema de votação pela internet não é recente na EC, o órgão já havia se comprometido a realizar testes desde 2008, porém o relacionamento entre o EC e o governo, tornaram esses testes mais difíceis, o que obrigou a EC a postergá-los indeterminadamente.

3.6.1.1 Eleições nos estados e municípios

Assim como a EC cuida das eleições federais há órgãos menores que são responsáveis pelos processos de votação nos municípios e possuem independência para utilização de métodos variados para votação, em alguns municípios do Canadá já é utilizado o sistema de votação pela internet, Markham com aproximadamente cem mil (100.000) eleitores foi um dos pioneiros na utilização. As autoridades da cidade argumentam que devido a capacidade e significativa aumento na acessibilidade ajudou no aumento de adesão por parte dos eleitores, fazendo com que o processo eleitoral fosse mais conveniente, aumentou o número de pessoas que votaram. Outra grande cidade que aderiu a este sistema foi à cidade de Peterborough que utiliza a internet para realização de eleições desde 2006. Outras grandes cidades estão apoiando e fazendo pesquisas junto a sua população para que o devido planejamento e implementação desse modelo possa ser adotado, em Newmarket é um caso em as autoridades locais estão apoiando essa mudança e colocando no planejamento público esse modelo, inclusive os partidos opositores nessas cidades apoiam a ideia, visto que a comodidade que a votação pela internet proporciona pode aumentar a base de votantes, diminuindo assim as abstenções durante as eleições (GOODMAN; PAMMETT, 2014).

Goodman e Pammett (2014), disserta que no estado Ontário a utilização de votação pela internet no âmbito municipal está aumento em um ritmo acelerado, doze (12) cidades em 2003 foram as primeiras a utilizar essa tecnologia, com o passar dos anos, em eleições posteriores o número de eleições que utilizavam essa metodologia aumentou de maneira significativa atingindo um quinto das eleições programas, algo em torno de 98 das 414 eleições programadas para 2014. Em cidades menores, com até vinte e cinco mil (25.000) eleitores, a votação via internet é oferecida em todas as votações e não é necessário um registro especifico ou pré-cadastro como é feito em

cidades maiores, Markham por exemplo em eleições que usaram a internet é necessário um pré-cadastro do eleitor e após todo o registro sendo autorizado é permitido ao eleitor votar pela internet. No caso de municípios menores além da votação pela internet ainda é permitido a votação por telefone, tornando nesse caso toda a votação além de eletrônica também remota.

Na província de Nova Escócia a partir de 2008 foi implantada a votação eletrônica em quatro (4) municípios, chegando a quatorze (14) em 2012, a previsão segundo autoridades locais era de que esse número aumentasse de forma gradativa tendo potencial de atingir os 54 municípios do estado, assim como na província de Ontário, os motivos que levaram a adoção deste método foram a diminuição das abstinências, se tornar líder em utilização de votação pela internet, assim como a conveniência não somente para a população mais também para o governo, pois um processo de eleição mais prático e com maior participação da população torna a base do governo mais forte. Há cidades em que a cédula de papel foi cancelada durante o dia da eleição, utilizando somente cédulas de internet e telefone, como exemplo de cidades que adotaram esse modelo estão as cidades de Digby Town, Truro e Yarmouth. Porém é importante ressaltar que como a tecnologia é relativamente nova sua utilização tende a ser adotada em cidades menores, mesmo tendo casos de grandes cidades utilizando, ainda há muitos pontos de melhoria, destacando-se o aumento da confiança da população e do governo em utilizar este método, em cidades menores nessas províncias, a votação pela internet é utilizada de forma integral, visto que algumas dessas possuem grandes populações flutuantes, ou seja, em épocas especificas do ano sua população tende a aumentar drasticamente e em outras diminuir exponencialmente (GOODMAN; PAMMETT, 2014).

3.6.1.2 Fornecedores da tecnologia

Goodman e Pammett (2014) descrevem que todas a fornecedoras da tecnologia de votação pela internet, são empresas do ramo privado, são seis (6) empresas que contratadas (CanVote, Dominion Voting, Everyone Counts, Intelivote, Scytl e Simply Voting), a partir dos testes iniciais e devido à grande adesão por parte do governo assim como da população que está comparecendo cada vez mais nas eleições, tem aumentado o número de empresas nesse nicho, trazendo serviços não somente de votação, mais também de pesquisas online, monitoramento do nível de

assiduidade dos eleitores para que os candidatos acompanhem sua base de votação. Grandes empresas desse ramo como Intelivote, Dominion, fazem pressão para que haja uma regulamentação mais firme e clara sobre o tema, visto que no Canadá apesar de utilizada a normatização de como deve ser utilizada, assim como os parâmetros de segurança a serem seguidos não são tão definidos quanto defendem essas empresas. Com relação a participação do mercado de votação algumas empresas possuem maior participação como a Intelivote, Dominion e Scytl dominam esse mercado e cada uma delas possuem cerca de um quarto de participação nas eleições, as demais empresas somadas representam cerca de vinte e cinco porcento (25%) de todos os processos de votação pela internet no Canadá.

3.6.2 Estonian Internet Voting in 2005-2014

Heiberg e Willemson (2014) relatam que no começo dos anos 2000 foi criado um esquema de votação online que foi utilizado em sete (7) votações durante os anos de 2005 até 2014, em sua essência o sistema permaneceu o mesmo. O sistema em seu conceito não é complexo, visto que utiliza conceitos de criptografia *Rivest Shamir Adleman* (RSA), são os nomes dos criados do protocolo criptográfico e utiliza o conceito de envelope duplo: O voto é Criptografado [envelope interno] utilizando uma chave pública, em seguida é assinado digitalmente [envelope externo] contendo a identidade digital do eleitor. Para que o eleitor consiga votar é necessário se autenticar no sistema, e para isso ele deve utilizar sua identidade ou seu ID Móvel (tecnologia de identificação amplamente utilizada na Estônia), após isso o sistema fornece a lista de candidatos, cada candidato está atrelado a um número, assim que o votante terminar de selecionar seus candidatos, o envelope interno contendo seus votos é criptografado utilizando uma chave pública fornecido pelo servidor, o eleitor através de sua identidade digital (a mesma que foi utilizada para a autenticação antes de votar), é a chave para assinatura digital, após esse processo o envelope é enviado ao servidor onde fica armazenado até o momento da apuração dos resultados.

O sistema segundo Heiberg e Willemson (2014), conta com várias medidas de segurança para garantir que o eleitor não seja coagido ou seu voto possa ser rastreado até ele, o método utilizado para que a coerção do eleitor seja evitada é somente computar o último voto, e nesse cenário é permitido ao eleitor votar mais de

uma vez, então caso ele seja forçado a votar em alguém, basta que depois ele acesse novamente o sistema e vote no seu candidato de preferência, esse último voto será o computado e os anteriores serão revogados, caso o eleitor prefira também há possibilidade de voto impresso, e nesse caso também invalida os votos anteriores, com essa situação a tentativa de coerção tende a ser infrutífera.

Durante todo o período de votação, todas as cédulas são armazenadas num formulário criptografado e assinado digitalmente, somente após o final da votação é que as assinaturas digitais das cédulas são dispensadas para que os valores relacionados aos Identidade Digital (ID) não sejam mais atrelados aos votos, visto que essa relação só é necessária durante o período de votação para que o eleitor possa invalidar seus votos anteriores caso necessário. Após esse processo utilizando a chave privada do servidor (armazenada em um local seguro no hardware) para descriptografar as cédulas e ter acesso aos votos (HEIBERG; WILLEMSON, 2014).

Mesmo com todos os protocolos de segurança, criptografia, métodos contra coerção, há muitas vulnerabilidades que podem ser exploradas, uma falha de segurança muito importante que ocorre é a falta de opção de verificação por parte do votante, ou seja, depois de selecionar seu candidato e confirmar, ele não consegue validar que seu voto foi mesmo computado de acordo com sua escolha, dessa forma foi possível explorar essa brecha nas eleições parlamentares de 2011 na Estônia, onde o atacante aproveitando dessa fraqueza desenvolveu diferentes versões de um vírus de computador que conseguiram não somente bloquear o voto mais também em alguns casos altera-lo. O eleitor por sua vez não possuíam ferramentas para ao final do processo de votação verificar seu voto, dessa forma o ataque passa desapercebido tanto do eleitor quanto das autoridades envolvidas no processo eleitoral. Após esse ataque em 2011 foi emitido um relatório pela *Organization for Security and Cooperation in Europe/Office for Democratic Institutions and Human Rights* (OSCE/ODIHR), apontando esse tipo de falha, e sugerindo que essa opção de verificação por parte de usuário (eleitor) seja incluída, a fim de evitar que qualquer tipo de alteração passe desapercebida no sistema.

4 CONSIDERAÇÕES FINAIS

Neste capitulo será apresentado as metodologias utilizadas, assim como os resultados da pesquisa, mostrando se os objetivos foram atingidos de alguma maneira ou não.

4.1 MODALIDADE DE PESQUISA

A pesquisa realizada visa apresentar dados e uma nova visão em relação a votação eletrônica convencional, mostrando tecnologias capazes de aperfeiçoar os métodos atuais, garantindo mais lisura no processo como um todo.

A pesquisa quanto aos objetivos caracteriza-se como explicativa, pois os conteúdos observados mostram informações concretas e apresentadas em diversos livros e artigos científicos. Em relação aos procedimentos da investigação, a pesquisa tem o caráter documental, pois os relatos apresentados foram buscados através de pesquisas em livros e artigos publicados em instituições renomados na área da tecnologia e engenharia.

4.2 INSTRUMENTO DE COLETA DE DADOS

As informações apresentadas têm como fonte livros, instituições de ensino, periódicos de grande credibilidade e circulação na área técnica, todos os autores citados de alguma forma se debruçam sobre Blockchain, criptografia ou votação eletrônica, dos autores que foi utilizado é Antonopoulos, falando de forma abragente e tecnica sobre Bitcoin e Blockchain.

4.3 CRITÉRIO PARA ANÁLISE DOS DADOS

Os dados coletados foram elaborados por autores renomados na área que cujas publicações são referência para vários trabalhos acadêmicos e livros de criptografia, Bitcoin e Blockchain e artigos de instituições renomadas no cenário acadêmico nacional e internacional.

4.4 DESCRIÇÃO DAS ETAPAS DE INVESTIGAÇÃO

Para realizar as etapas de investigação o autor procurou por material didático (livros, artigos etc.), discussão com professores da área, análise dos dados coletados. Com base em todo o material pesquisado assim como resultado da análise é possível propor novas técnicas e Sistemas que podem melhorar todo o processo de votação na inciativa privada e pública, economizando tempo, dinheiro, e com um alto nível de segurança e auditoria dos resultados.

4.5 CAMPO DE OBSERVAÇÃO

Utilizando como base o material utilizado durante todo o processo de pesquisa e investigação, é possível observar que as tecnologias apresentadas no presente trabalho, podem de forma efetiva substituir ou complementar o atual meio de votação. O fluxo de dados no canal de comunicação não será algo que a atual infraestrutura de comunicação não consiga suportar, a necessidade de dispositivos específicos também é reduzida, visto que será utilizado aparatos tecnológicos que já estão em posse dos eleitores.

Por outro lado o aspecto de segurança, validação, autenticação do eleitor é garantido pela integração dos Sistemas federais utilizados, todo o processo desde o primeiro voto pode ser acompanhado em tempo real pela população assim como entidades governamentais, em tempo real, e com total transparência dos resultados, com relação ao anonimato do voto, isso é mantido e aprimorado, pois o Sistema guardará apenas o voto, a autentica servirá apenas como garantia que não haverá voto duplicado do mesmo eleitor, ou inclusão de votos a mais, depois de concluído o voto os dados armazenados no histórico é apenas o candidato que o eleitor selecionou, garantindo que o voto continue secreto.

O Sistema é extremamente seguro por utilizar consenso e prova de existência, nada é incluído sem validação dos outros participantes da rede, e a prova de existência do voto é gerada e armazenada, podendo inclusive ser consultada. Quanto maior a rede Blockchain para votação, maior é o grau de segurança e confiabilidade do Sistema.

4.6 CONCLUSÃO

O presente trabalho possibilitou visualizar sob varios aspectos o Blockchain, e votação eletrônica, propondo uma junção das duas tecnologia para melhorar o Sistema de eleição corporativas e governamentais, agilizando todo o processo, tornando-o mais seguro, pratico, transparente e rapido. Foi demonstrado casos praticos, onde alguns paises já adotam de forma timida esse tipo de idéia, proporcionando a população maior praticidade em suas escolhas, aprimorando assim o processo democrático. O caso no ambiente corporativo da Nasdaq, foi explicitado que essa solução abrange os mais diversos tipos de eleição e niveis de companhias, mostrando seu potencial para gerenciar eleições de pequeno a grande porte, independente do graú de criticidade.

Como demonstrado neste trabalho, o nível de segurança do Blockchain, garante toda a lisura, visto que os nós da rede, que no caso são definidos pelo próprio governo, garantem que dados serão armazenados no histórico do Blockchain, e que caso alguém tente alterar algum desses registro, será necessário alterar isso em todos os nós, dificultando qualquer tipo de fraúde. Para registro e garantir que o eleitor não tente fraudar sua identificação é proposto além de biometria, a integração de contratos inteligentes e a base de dados de pessoas do governo, dessa forma uma pessoa vota uma única vez e caso necessário consegue alterar o voto uma única vez. A utilização de contrato inteligente possui um outro beneficio, já que armazena o candidato escolhido, a apuração acontece em tempo real, diminuindo o tempo e custos da apuração de resultados, visto que não há necessidade de transportar em midias portateis os votos de cada seção eleitoral.

Em comparação com o metodo atual de votação aonde é necessário transportar todas as urnas, preparar as zonas eleitorais, fazer o eleitor se deslocar até o ponto de votação, transportar o resultado para que um outro Sistema faça a leitura e validação dos resultados, a votação eletrônica remota, utilizando o Blockchain oferece muitos beneficios, além de o eleitor poder votar aonde quer que esteja, não necessitando ir justificar, visto que com acesso a internet e um dispositivo móvel ele pode ter acesso ao Sistema eleitoral. Porém há situações que podem impactar de forma grave esse processo, visto que há requisitos a serem cumpridos, caso o eleitor não possua por algum motivo conexão com a internet fica impossibilitado de realizar

seu voto. O eleitor também deve possuir o minimo de conhecimento na operação do dispositivo que usará assim como do Sistema online, caso não possua um minimo de conhecimento, também será incapaz de utilizar.

Como forma de resolver este tipo de situação o melhor cenário é mesclar os dois métodos de votação, visto que há localidades no país sem acesso a internet, onde é necessário que a urna continue sendo utilizado, pensando na parte da população que não domina equipamentos de informatica (smartphones, computadores, etc.) é necessário que não se elimine todos os pontos de votação fisica na cidade, mais os diminua, assim caso necessário ainda há outros meios de votar, porém a implicação do Sistema remoto sobre esse cenário acarreta no menor tempo em filas agilizando essa parte do processo.

O cenário votação também elenca um outro grande problema, a auditoria dos resultados, como o Blockchain é totalmente transparente, consultar seu histórico é possível, auditar esses registros é muito mais facil, visto que todos os dados estão lá, e possuem garantia que não foram adulterados, fraudadados ou exlcuídos, pois por ser descentralizado e necessitar de consenso de todos os nós, qualquer altereação em um registro já amarmazenado precisa de aceitação da maioria dos nós, então caso alguém altere um um único registro numa zona eleitoral, e tente públicar isso para os outros nós, essa modificação será rejeitada visto ela ocorreu sem o consenso de um todo, garantindo assim a lisura do processo.

REFERÊNCIAS

ADESHINA, Steve A.; OJO, Adegboyega. **Design imperatives for e-voting as a sociotechnical system**. In: 2014 11TH INTERNATIONAL CONFERENCE ON ELECTRONICS, COMPUTER AND COMPUTATION (ICECCO), Abuja, Nigéria, 01 set.-29 out. 2014. Disponível em: <https://ieeexplore.ieee.org/document/6997569>. Acesso em: 02 nov. 2018.

AL-AMEEN, Abdalla; TALAB, Samani A. **E-voting systems vulnerabilities**. In: 2012 8TH INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE AND DIGITAL CONTENT TECHNOLOGY (ICIDT2012), Jeju, Coreia do Sul, v. 1, n. 15, 26-28 jun. 2012. p.67-73. Disponível em: <https://ieeexplore.ieee.org/document/6269229>. Acesso em: 20 nov. 2018.

ANTONOPOULOS, Andreas M. **Mastering bitcoin: Programming the open blockchain**. 2. ed. Sebastopo: O'reilly Media, 2017. 537 p.

BÉLANGER, France; CARTER, Lemuria. The Digital Divide and Internet Voting Acceptance. IN: 2010 FOURTH INTERNATIONAL CONFERENCE ON DIGITAL SOCIETY, St. Maarten, Antilhas Holandesas, 10-16 fev. 2010. Disponível em: <https://ieeexplore.ieee.org/document/5432779>. Acesso em: 18 nov. 2018.

CETINKAYA, Orhan. **Analysis of security requirements for cryptographic voting protocols**. In: 2008 THIRD INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, Barcelona, Espanha, 4-7 mar. 2018, p.1451-1456. Disponível em: <https://ieeexplore.ieee.org/document/4529515>. Acesso em: 06 nov. 2018.

DELIS, Alex et al. **Pressing the button for European elections: verifiable e-voting and public attitudes toward internet voting in Greece.** In: 2014 6TH INTERNATIONAL CONFERENCE ON ELECTRONIC VOTING: VERIFYING THE VOTE (EVOTE), Lochau, Aústria, 29-31 out. 2014. Disponível em: <https://ieeexplore.ieee.org/document/7001141>. Acesso em: 06 nov. 2018.

DINH, Tien Tuan Anh et al. **Untangling Blockchain: A data processing view of blockchain systems**. In: IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, v. 30, n. 7, p.1366-1385, 1 jul. 2018. Disponível em: <https://ieeexplore.ieee.org/document/8246573>. Acesso em: 02 out. 2018.

EHMKE, Christopher; WESSLING, Florian; FRIEDRICH, Christoph M. **Proof-of-Property: A lightweight and scalable blockchain protocol**. In: 2018 IEEE/ACM 1ST INTERNATIONAL WORKSHOP ON EMERGING TRENDS IN SOFTWARE ENGINEERING FOR BLOCKCHAIN (WETSEB), Gothenburg, v. 1, n. 1, p.48-51, 27 27 mai.-3 jun. 2018. Disponível em: <https://ieeexplore.ieee.org/document/8445059/>. Acesso em: 03 out. 2018.

EPSTEIN, Jeremy. **Electronic voting**. Computer, v. 40, n. 8, ago. 2007. p.92-95. Disponível em: <https://ieeexplore.ieee.org/document/4292024>. Acesso em: 20 nov. 2018.

FERGUSON, Niels; SCHNEIER, Bruce; KOHNO, Tadayoshi. **Cryptography engineering: Design principles and practical applications**. Indianapolis: Wiley Publishing, Inc, 2010. 353 p.

FIAIDHI, Jinan; MOHAMMED, Sabah; MOHAMMED, Sami. **EDI with blockchain as an enabler for extreme automation.** IN: IEEE COMPUTER SOCIETY, v. 20, n. 4, jul./aog. 2018. p.66-72. Disponível em: <https://ieeexplore.ieee.org/document/8429272/>. Acesso em: 22 ago. 2018.

GOODMAN, Nicole; PAMMETT, Jon. **The patchwork of internet voting in Canada**. In: 2014 6TH INTERNATIONAL CONFERENCE ON ELECTRONIC VOTING: VERIFYING THE VOTE (EVOTE), Lochau, Aústria, 29-31 out. 2014. Disponível em: <https://ieeexplore.ieee.org/document/7001134#full-text-header>. Acesso em: 06 nov. 2018.

HEIBERG, Sven; WILLEMSON, Jan. **Verifiable internet voting in Estonia**. In: 2014 6TH INTERNATIONAL CONFERENCE ON ELECTRONIC VOTING: VERIFYING THE VOTE (EVOTE), 29-31 out. 2014. Disponível em: <https://ieeexplore.ieee.org/document/7001135>. Acesso em: 06 nov. 2018.

MORENO, Edward David; PEREIRA, Fabio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em software e hardware.** São Paulo: Novatec, 2005. 288 p.

NOFER, Michael et al. **Blockchain**. Business & information systems engineering (BISE), v. 59, n. 3, p.183-187, 20 mar. 2017. Disponível em: <https://aisel.aisnet.org/bise/vol59/iss3/7/>. Acesso em: 26 set. 2018.

ORMAN, Hilarie. **Blockchain: the emperors new PKI?** In: IEEE INTERNET COMPUTING, v. 22, n. 2, mar./abr. 2018. p. 23-28. Disponível em: <https://ieeexplore.ieee.org/document/8345567>. Acesso em: 20 ago. 2018.

SWAN, Melanie. **Blockchain: blueprint for a new economy**. Sebastopol: O'reilly, 2015.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. 1. ed. São Paulo: Instituto Ludwig Von Mises Brasil, 2014. 122 p.

YAVUZ, Emre et al. **Towards secure e-voting using ethereum blockchain**. In: 2018 6TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSIC AND SECURITY (ISDFS), Antalya, Turquia, 22-25 mar. 2018. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8355340>. Acesso em: 30 jul. 2018.