Sistema de Votação Eletrônica baseado em Assinatura Cega e BigchainDB

Leonardo Pinto Guilherme, Luis Claudio Batista da Silva, Nilson Mori Lazarin

[1]Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ)
Rio de Janeiro, RJ – Brazil

leonardo.guilherme@aluno.cefet-rj.br

{luis.silva,nilson.lazarin}@cefet-rj.br

Abstract. *The electronic voting machine contributed to a more agile voting process and eliminated many known frauds. On the other hand, it also increased the electorate's distrust of the process, as voters can no longer observe what happens to their vote. The public auditing of the vote is a much-debated subject because the means available to audit the vote compromise the anonymity of the voter's choice, considered a mandatory requirement in Brazilian democracy. This work presents an electronic voting system model that implements Blockchain and Blind Signatures to allow auditing and anonymity of the voter's choice during the process.*

Resumo. *A urna eletrônica contribuiu para sufrágios mais ágeis e eliminou muitas das fraudes conhecidas. Por outro lado, também fez crescer a desconfiança do eleitorado com o processo, uma vez que o eleitor não é mais capaz de observar o que acontece com o seu voto. A auditoria pública do voto é um assunto muito debatido, pois os meios disponíveis para auditá-lo comprometem o anonimato da escolha do eleitor, considerado um requisito obrigatório na democracia brasileira. Este trabalho apresenta um modelo de sistema eletrônico de votação baseado em Blockchain e Assinaturas Cegas para permitir a auditagem e garantir o anonimato da escolha do eleitor durante o processo.*

1. Introdução

Com um processo eleitoral desenvolvido para a realidade brasileira, a digitalização do sufrágio teve como objetivo não apenas aumentar a segurança das votações, mas também reduzir tempo, recursos e custos do processo. Através da urna eletrônica, foi possível garantir o sigilo da escolha do eleitor, implementar múltiplos mecanismos de segurança para impedir adulterações do voto e agilizar a sua apuração [TSE 2016].

Enquanto a tecnologia da informação cumpre com o seu papel de apoiar em atividades que, antes, eram manualmente custosas de serem executadas, por outro lado, obscurece, ao ser humano, o funcionamento de diversas etapas do processo eleitoral. Especialmente em relação a auditagem do voto, levantam-se muitos questionamentos na sociedade em função do processo atual não oferecer meios para o eleitor confirmar a autenticidade do seu próprio voto após depositado [Oliveira 2021].

Entretanto, a rastreabilidade do voto para confirmar sua autenticidade não pode comprometer o anonimato. Anteriormente, [Marcacini and Barreto Junior 2019] con-

cluíram não haver meio de conduzir uma eleição que seja, ao mesmo tempo, (a) 100% digital, (b) publicamente auditável e (c) com votos anônimos.

Visando possibilitar um meio de auditagem do voto digital, este trabalho apresenta um modelo de sistema eletrônico de votação que implementa, dentre outras tecnologias, a blockchain e as assinaturas cegas em um processo similar ao pleito eleitoral em funcionamento no Brasil. O modelo garante o voto exclusivamente digital, o anonimato da escolha do eleitor e se limita em garantir a segurança da informação de toda a infraestrutura utilizada na proposta. Como contribuição, o trabalho oferece uma perspectiva digital para a auditagem do voto, sem a necessidade de gerá-lo fisicamente, em caso de dúvidas sobre a lisura de uma eleição.

Este artigo está organizado da seguinte forma: na Seção 2 são apresentados os trabalhos relacionados; a Seção 3 apresenta o atual modelo do processo eleitoral brasileiro; na Seção 4 é apresentado o modelo de sistema eletrônico; na Seção 5 é apresentada uma prova de conceito, utilizando o pacote OpenSSL; por fim, na Seção 6 é apresentada a conclusão.

2. Trabalhos Relacionados

O trabalho apresentado por [Marcacini and Barreto Junior 2019] apresenta uma análise sobre as problemáticas envolvidas em um processo eleitoral eletrônico. Os autores discutem sobre os meios de conduzir um sufrágio que seja, ao mesmo tempo, (a) 100% digital, (b) publicamente auditável e (c) anônimo em relação ao voto, em que concluem que apenas dois quaisquer entre os três requisitos podem ser atendidos. Sobre o sigilo, os autores mencionam o artigo 14 da Constituição Federal, que garante ao eleitor o voto secreto, em que de nenhuma maneira deve ser possível identificar quem votou em quem. Logo, mais que um voto secreto, exige-se um voto anônimo.

Em [Adiputra et al. 2018] é proposto um processo eleitoral online com o uso da blockchain. Um par de chaves pública e privada é criado para a comissão eleitoral cifrar e decifrar os votos, enquanto cada eleitor também deve criar o seu próprio par de chaves pública e privada, de modo a conferir a autenticidade do documento que identifica o eleitor - a chave privada do eleitor deve ser guardada secretamente. O voto, já cifrado, é enviado para uma rede blockchain, que se registra como um novo bloco na rede. Desta maneira, qualquer eleitor pode conferir que um voto foi, de fato, enviado. Entretanto, o sistema proposto se conecta à internet, permitindo tentativas de ataques remotos.

Segundo [Osgood 2016], o uso da blockchain se apresenta como uma tecnologia capaz de oferecer sigilo absoluto ao eleitor enquanto previne fraudes digitais no sufrágio. No trabalho, propõe-se um sistema híbrido de votação, com uma urna eletrônica e outra com cédula de papel. As cédulas de papel devem conter um QR Code e devem ser escaneadas pela urna eletrônica. Ao fim das votações, os votos são gravados em um DVD, que, com as cédulas de papel, devem ser guardadas em local seguro. Então, realiza-se a contagem dos votos registrados em cada máquina. Caso todos os votos sejam considerados válidos, os dados entram em uma nova rede de blockchain com outras máquinas. A proposta, porém, não atende ao requisito de uma eleição 100% digital, como mencionado por [Marcacini and Barreto Junior 2019].

Baseando-se no conceito de assinaturas digitais, [Barros and Pimenta 2018]

propõem um sistema de votação eletrônico com a garantia do anonimato. Para isso, durante o processo de votação, usam assinaturas digitais duplamente cegas e atribuem ao voto um identificador anônimo. O esquema impede que o eleitor gere evidências da sua escolha depositada na urna, além de garantir a autenticidade do eleitor e do seu voto. Por outro lado, o sistema exige que o eleitor instale uma aplicação em seu dispositivo móvel pessoal para realizar o processo, o que pode levar a dificuldade em garantir a segurança física e digital desses dispositivos.

Como diferencial aos trabalhos relacionados, o modelo proposto não exige conexão de redes que, se aplicado, tende a aumentar os riscos em relação à segurança da informação. Como resultado, a proposta em questão possibilita um mecanismo de validação do voto pelo próprio eleitor e um novo meio de se auditar as votações, tal como discutido por [Marcacini and Barreto Junior 2019]. Dessa forma, o trabalho contribui apresentando uma possível alternativa à proposta do voto fisicamente impresso como caminho para a realização de auditoria.

3. Processo Eleitoral Brasileiro

Elaborado pelo Tribunal Superior Eleitoral (TSE), o processo eleitoral brasileiro é composto por diversas etapas, entre as quais estão o cadastro eleitoral, a votação e a totalização dos votos, sendo estas as mais relevantes para este estudo.

3.1. Etapa de Cadastro Eleitoral

O brasileiro que atingiu a maioridade eleitoral e está obrigado a votar, deve, em até seis meses antes da data do pleito, alistar-se no cartório eleitoral mais próximo da sua casa. Para efetuar o cadastro, o eleitor deve apresentar um documento oficial com foto e comprovante de residência. Nesta etapa, realiza-se também a coleta biométrica dos dedos do cidadão. Estas informações são armazenadas sigilosamente no cadastro do eleitor.

Uma vez confirmados os dados, o eleitor é inscrito na Justiça Eleitoral e recebe um novo documento: o título de eleitor, que serve para provar que o cidadão está inscrito em uma determinada zona eleitoral. Desde abril de 2020 o TSE possibilita a emissão do título de maneira online, por meio do sistema Título Net.

3.2. Etapa de Votação

Nesta etapa, além do eleitor, na seção eleitoral também participam os membros da Mesa Receptora dos Votos, composto pelo Presidente, Secretário, 1º e 2º Mesários [TRE 2020]:

- **Presidente**: responsável por iniciar e encerrar as votações, autorizar o eleitor a votar e zelar pela preservação da urna eletrônica.
- **Secretário**: responsável pelo preenchimento da ata da mesa receptora de votos e pelo controle da movimentação de pessoas na seção.
- **Mesários**: o 1º e o 2º mesários substituem o presidente na sua ausência, além de localizar o nome do eleitor no caderno de votação e colher sua assinatura.

Quando aberta a etapa de votações, o eleitor devidamente inscrito na Justiça Eleitoral deve se dirigir para a seção eleitoral indicada em seu título. Em sua seção, o eleitor deve apresentar o título junto a um documento oficial com foto. O mesário deve localizar o nome do eleitor no caderno de votação para, logo, colher sua assinatura e realizar a

leitura biométrica dos dedos do eleitor. Em seguida, o Presidente da mesa libera o terminal do eleitor para o depósito do voto. O eleitor deve se dirigir até a cabine de votação, onde está a urna eletrônica, para digitar o número do seu candidato para o(s) cargo(s) indicado(s) e confirmar o seu voto. Quando finalizado, o eleitor deve se retirar da seção.

3.3. Etapa de Apuração

Esta etapa ocorre após a finalização das votações nas seções eleitorais. Os dados registrados na urna são assinados digitalmente, criptografados e armazenados em uma mídia de resultado. Logo, gera-se um boletim de urna, isto é, a divulgação do resultado das votações da urna em questão.

A totalização dos votos inicia, de fato, quando a mídia de resultado é encaminhada para um local de transmissão dos dados, que devem ser recebidos pelo Tribunal Regional Eleitoral, responsável por fazer a soma dos votos de todos os boletins de urna. Logo, os resultados das eleições são divulgados pelo próprio Tribunal.

4. Modelo Proposto

Assinatura Cega é uma assinatura digital, porém com a diferença de que as partes assinam um documento com o conteúdo oculto, ou seja, não são capazes de ler as informações contidas no documento. Por outro lado, as partes que o assinam podem ser conhecidas normalmente, pois o objetivo é apenas preservar o sigilo do teor do documento. Este tipo de assinatura é útil quando o documento em questão contém informações confidenciais ou que não podem ser acessadas por outras pessoas. O conceito da assinatura cega foi apresentado por [Chaum 1983] e já foi utilizado em outros estudos relacionados à segurança da informação em eleições, tal como [Barros and Pimenta 2018].

O BigchainDB é um sistema gerenciador de banco de dados (SGBD) não-relacional, baseado em MongoDB, que implementa a blockchain, permitindo o registro descentralizado de transações imutáveis e anônimas. Com este SGBD, pode-se realizar *queries* de inserção e leitura dos dados registrados, entretanto, não é possível alterar ou apagar um registro, uma vez que os dados estão registrados na blockchain [GmbH 2018].

Este trabalho, baseado no processo eleitoral brasileiro, apresenta uma etapa de validação do voto pelo próprio eleitor, antes do seu depósito na urna. Além disso, fornece instrumentos para uma possível auditoria pública das eleições, a qualquer tempo. Para adoção do método proposto, algumas modificações ao processo atual seriam necessárias, principalmente na etapa de cadastro do eleitor e na etapa de votação. Tais modificações são apresentadas a seguir.

4.1. Cadastro Eleitoral

Durante a emissão do título eleitoral é necessário gerar um par de chaves assimétricas. A *chave privada* deve ser cifrada, por um algoritmo simétrico de bloco, e protegida por uma senha pessoal cadastrada pelo próprio eleitor. O eleitor deve receber um *cartão*[1] contendo sua chave para usá-lo no dia das eleições. Dessa forma, a chave fica em posse apenas do eleitor. Por outro lado, a *chave pública* fica armazenada no banco de dados do sistema central, junto às demais informações do eleitor.

[1]Um *smart device* que garanta a persistência e a segurança das informações armazenadas.

4.2. Pleito Eleitoral

Nesta subseção são apresentadas as modificações mais abrangentes, propostas por este trabalho. Cada passo desta etapa pode envolver atores e dispositivos diferentes, em contextos diferentes. Abaixo são descritos os processos de abertura, funcionamento e fechamento da Seção de Votação.

4.2.1. Abertura da Seção de Votação

Esta etapa é responsável por sincronizar os *terminais* da seção eleitoral. O processo deve ser realizado no dia da eleição, presencialmente, pelos mesários designados para aquela seção. São gerados um par de chaves assimétricas em cada terminal, em função da *chave pública da eleição*. As *chaves públicas* dos mesários da seção e a *chave pública* da zona eleitoral são previamente armazenadas no *cartão da seção eleitoral* pela autoridade.

A *chave pública* de cada terminal é armazenada no *cartão da seção* eleitoral e todas as chaves são distribuídas entre os *terminais*. O processo, apresentado na Figura 1, se dá da seguinte forma:

Geração da chave do terminal de escolha: O Presidente da seção deve inserir o *cartão da seção* no terminal de escolha e iniciar o processo de sincronização. O terminal gera aleatoriamente uma *chave privada*, em função da *chave pública da eleição*. A *chave privada* do terminal é armazenada localmente. Posteriormente o terminal gera uma *chave pública* derivada da chave privada e a armazena no *cartão da seção*. O presidente remove o cartão e o entrega ao 1º mesário.

Geração da chave do terminal do mesário: O primeiro mesário insere o *cartão da seção* no *terminal do mesário* e inicia o processo de sincronização. O terminal gera aleatoriamente uma *chave privada*, baseada na *chave pública da eleição*, e a armazena localmente. Posteriormente, o terminal gera uma *chave pública* derivada de sua chave privada aleatória e a armazena no *cartão da seção*. O 1º mesário remove o cartão e o entrega para o 2º mesário.

Geração da chave do terminal de depósito e importação de chaves públicas: O segundo mesário insere o cartão no *terminal de depósito* e inicia o processo de sincronização. O terminal gera aleatoriamente uma *chave privada*, baseada na *chave pública da eleição*, e a armazena localmente. Posteriormente, o terminal gera uma *chave pública* derivada de sua *chave privada* aleatória e a armazena no *cartão da seção*. Além disso, o terminal copia as *chaves públicas* do cartão e as armazena localmente. O 2º mesário encerra o processo de sincronização, remove o cartão e o devolve para o 1º mesário.

Importação de chaves públicas no terminal do mesário: O primeiro mesário insere o cartão no *terminal de mesário* e continua o processo de sincronização. O terminal copia as *chaves públicas* do cartão e as armazena localmente. O 1º mesário encerra o processo de sincronização, remove o cartão e o entrega para o presidente.

Importação de chaves públicas no terminal de escolha: O presidente insere o cartão

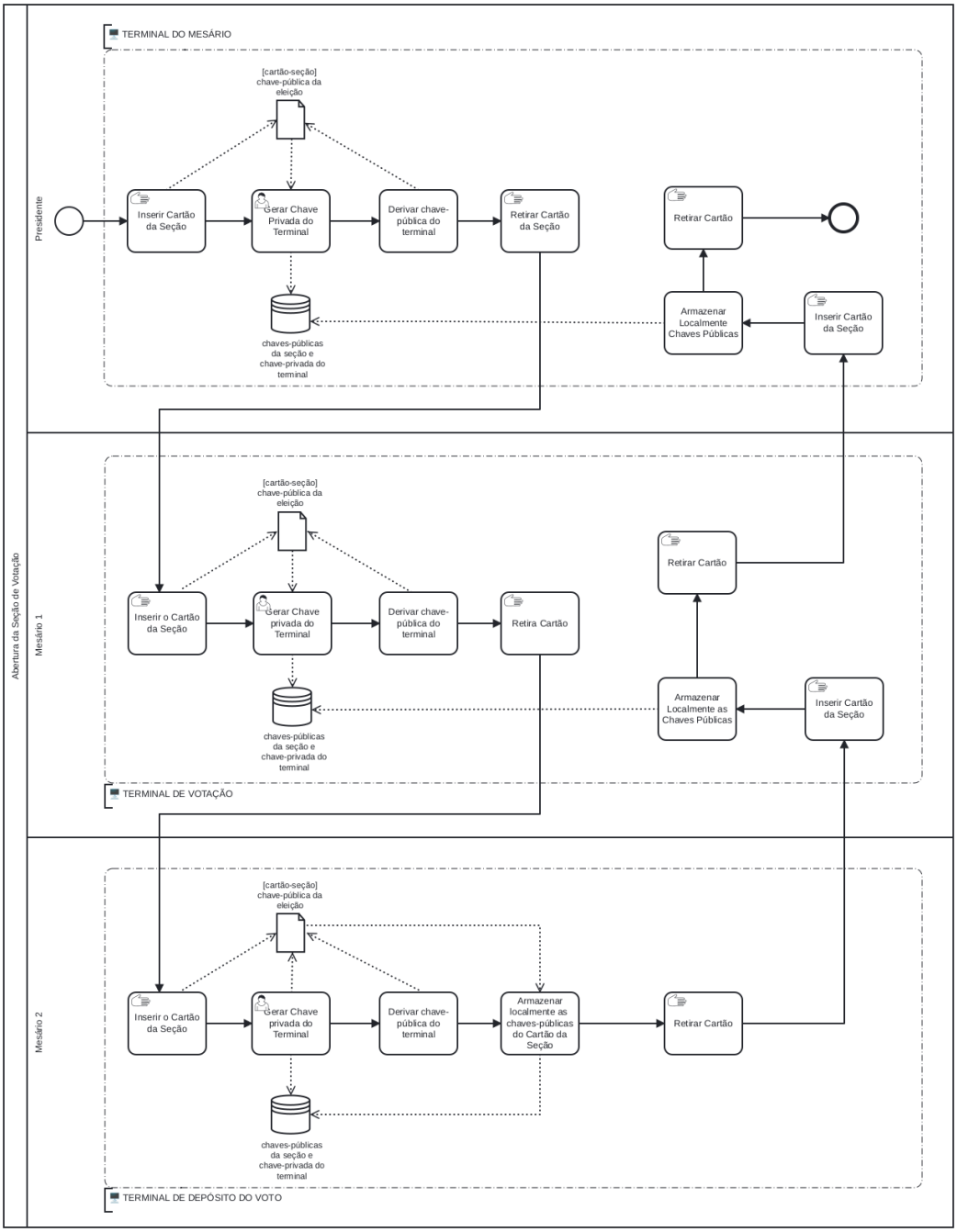

Figura 1. Abertura da Seção Eleitoral

no *terminal de escolha* e continua o processo de sincronização. O terminal copia as *chaves públicas* do cartão e as armazena localmente. O presidente encerra o processo de sincronização e remove o *cartão da seção*.

4.2.2. Votação

O fluxo da etapa de votação foi dividido em três partes. Todas as atividades desta etapa ocorrem em um único ambiente: na seção eleitoral do eleitor, presencialmente, no dia da

votação. Essas etapas, apresentadas na Figura 2, são descritas abaixo:

Emissão da cédula: O eleitor se dirige ao terminal do mesário para gerar a *cédula eleitoral*. O mesário deverá verificar a identidade do eleitor. O eleitor insere seu *cartão eleitoral* no terminal. O mesário inicia o processo de emissão da *cédula eleitoral*, inserindo seu cartão e senha pessoal. O terminal gera e grava no *cartão do eleitor* a *cédula eleitoral*. O eleitor retira seu cartão.

Escolha do candidato: O eleitor se dirige ao *terminal de votação* da seção eleitoral, conforme previamente indicado em seu título de eleitor, para selecionar os candidatos. O terminal valida a assinatura do mesário e libera a escolha de candidatos. Uma vez confirmada a escolha do eleitor, o voto é cifrado com uma chave derivada da *chave privada* do *terminal de votação* com a *chave pública* do *terminal de depósito*; e com um vetor de inicialização aleatório, para que cada voto seja único. Além disso, um *digest* do voto cifrado é gerado. O voto cifrado e o *digest* são armazenados no *cartão do eleitor*. Em seguida, o eleitor deve retirar o cartão do terminal.

Assinatura Cega: Ainda na seção eleitoral, o eleitor deve se dirigir novamente ao mesário com seu *cartão eleitoral* e o inserir no terminal. O mesário, por sua vez, deverá assinar o arquivo *digest* do voto cifrado. Cabe ressaltar que a assinatura cega é, justamente, o passo que garante ao eleitor o anonimato da sua escolha neste ato, uma vez que o mesário assina apenas o *digest* do voto cifrado. Caso nenhuma inconsistência seja encontrada com os dados ou a assinatura do eleitor, o mesário pode autorizar que o eleitor prossiga ao passo de depósito do voto.

Depósito do Voto: Por fim, o eleitor deve seguir ao *terminal de depósito do voto*, onde o seu *cartão eleitoral* deve ser inserido, mais uma vez, e é confirmada a assinatura do mesário. Se nenhuma mensagem de erro for indicada na tela (falha na validação da assinatura), o voto será depositado na urna. O banco de dados do terminal de depósito é o BigChainDB, o qual manterá registrado os votos dos demais eleitores que depositaram o voto nesta mesma urna.

Cabe ressaltar que a senha pessoal utilizada no processo se deu por motivos de implementação para o ambiente de validação da proposta. Considera-se a identificação biométrica, já presente no sistema eleitoral brasileiro, como uma solução mais adequada.

4.2.3. Fechamento da Seção de Votação

O depósito do voto na urna representa o seu registro no BigChainDB. Neste banco de dados apenas será registrado o candidato votado por cada eleitor. Nenhuma informação do eleitor é registrada no banco de dados. O encerramento da seção de votação é realizado pelo presidente, inserindo o *cartão da seção* no *terminal de votação* que gera e emite o boletim de urna. Este boletim é cifrado usando a *chave privada* do terminal e a *chave pública* da zona eleitoral. Além de ser armazenado no *cartão da seção eleitoral*. Por fim, a *chave privada* do terminal é destruída, impedindo que qualquer outra informação possa ser assinada ou qualquer outro voto possa ser decifrado. O *cartão da seção* é enviado para a zona eleitoral para totalização dos votos.

Cabe ressaltar que a totalização dos votos não é objeto deste estudo, visto que a prova de conceito foi realizada utilizando uma única seção eleitoral.

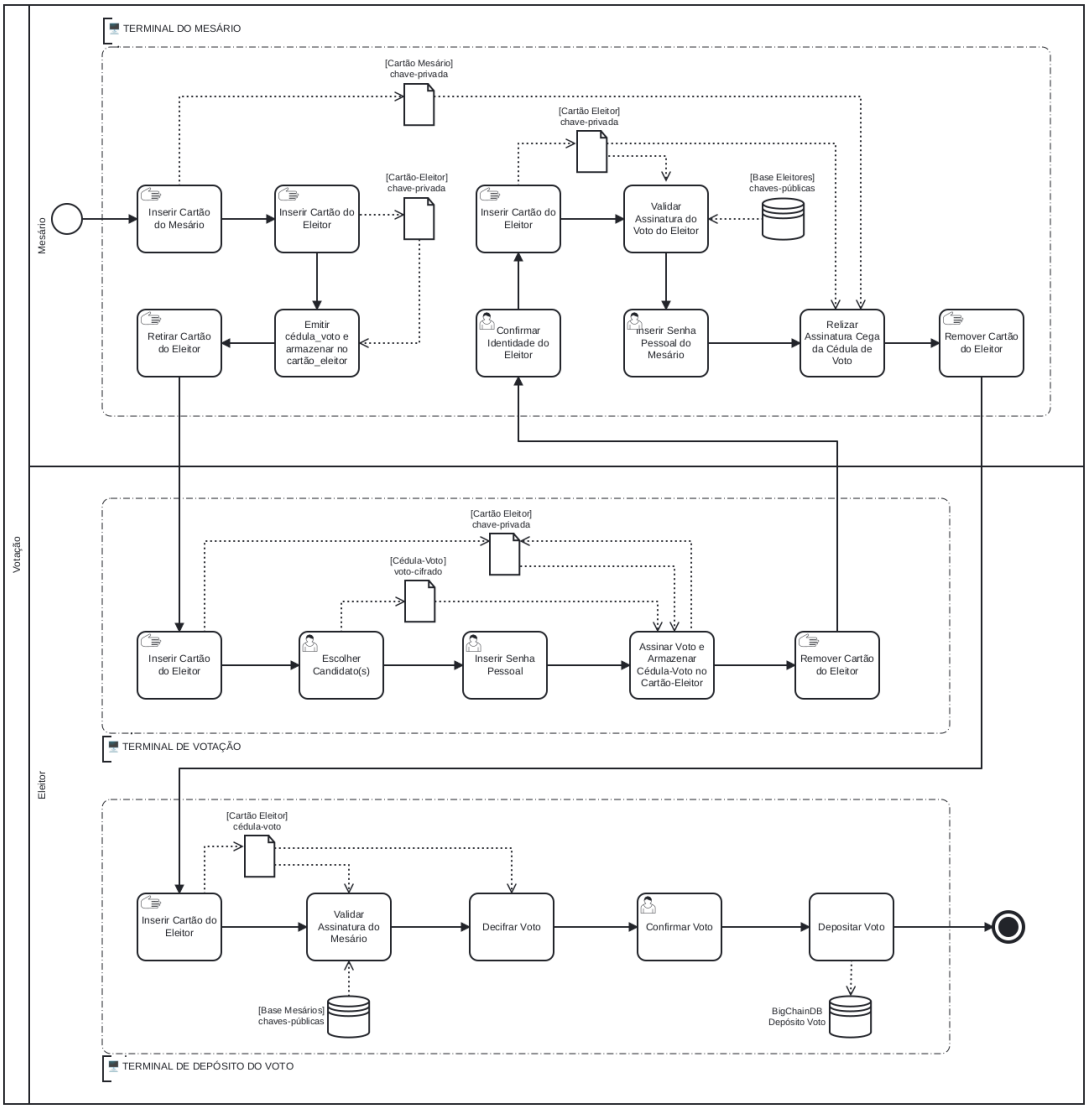

Figura 2. Processo de Votação

5. Prova de Conceito

A implementação utiliza comandos que fazem parte do pacote OpenSSL, um ferramental de administração de bibliotecas relacionadas com a criptografia. A sequência de comandos do processo é viável de ser executada manualmente, mas para desenvolver a implementação com maior produtividade, agilidade e organização, optou-se por automatizá-los usando Python. Abaixo são apresentados os comandos realizados, em cada um dos sistemas envolvidos no processo eleitoral, para viabilizar o modelo proposto.

5.1. Servidor Central da Instituição

Neste terminal são registrados os dados do eleitor. Os dados de interesse para esta proposta são o número de inscrição do eleitor associado à sua *chave pública*. Os comandos necessários para esta etapa estão descritos na *Lista de Comandos 1*.

O *comando 1* gera uma *chave privada* de 4096 bits, cifrada pelo AES com uma senha inserida pelo eleitor no momento da criação da chave. O *comando 2* exporta a *chave*

pública do eleitor. A *chave pública* é armazenada em um diretório público, enquanto a *chave privada* é armazenada no *cartão eleitoral*. Os *comandos 1 e 2* são repetidos para cada eleitor na etapa de cadastro eleitoral e *XXX* é o número de inscrição do eleitor.

Após finalizada a etapa de cadastro de todos os eleitores, o *comando 3* executa o algoritmo Diffie-Hellman que resultará em uma *chave pública* global da eleição. Ela servirá para sincronizar todas as zonas eleitorais e urnas envolvidas na etapa da votação, de modo a manter uma troca de informações segura entre elas.

Por fim, o *comando 4* gera uma *chave privada*, baseada na *chave pública* da eleição, e o *comando 5* gera uma *chave pública*, onde *XYZ* é a identificação da zona eleitoral. Estes comandos devem ser gerados para cada zona eleitoral.

Lista de Comandos 1 Comandos OpenSSL necessários no servidor central

1: openssl genrsa -aes-256-cbc -out [ECard]/XXX_private.pem 4096
2: openssl rsa -in [ECard]/XXX_private.pem -pubout –out [repositório]/XXX_public.pem
3: openssl genpkey -genparam -algorithm DH -out chave-publica-eleicao.pem
4: openssl genpkey -param file chave-publica-eleicao.pem -out privZONA_XYZ.pem
5: openssl pkey -in privZONA_XYZ.pem -pubout -out pubZONA_XYZ.pem

5.2. Terminal do mesário

Como configuração inicial, antes do início das votações, cada seção eleitoral recebe um dispositivo de armazenamento removível *(SeCard)* para sincronização e armazenamento das chaves de cada terminal da seção. Além disso, antes da fase de votação a autoridade eleitoral deve inserir todas as *chaves públicas* dos eleitores da respectiva seção no *terminal do mesário*.

O *terminal do mesário* também deve realizar o passo de sincronização para habilitação da seção eleitoral. Neste caso, a geração da *chave privada* e a exportação de sua respectiva *chave pública* é executada pelos *comandos 1 e 2* da *Lista de Comandos 2*.

A geração de cédula eleitoral é realizada pelos *comandos 3 e 4*. O *comando 3* gera aleatoriamente uma cédula. No *comando 4* a cédula é assinada, com a *chave privada* do mesário e sua senha pessoal. Por fim, a cédula é armazenada de forma criptografada no cartão do eleitor, através do *comando 6*. A chave criptográfica entre os terminais de mesário e de escolha foi obtida através do *comando 5*.

Lista de Comandos 2 Execução do OpenSSL no terminal do mesário

1: openssl genpkey -param file [SeCard]/chave-publica-eleicao.pem -out privTM.pem
2: openssl pkey -in privTM.pem -pubout -out [SeCard]/pubTM.pem
3: openssl rand -base64 4096 > cedula.bin
4: openssl dgst -sha512 -sign [ECardMesário]/ZZ_private.pem -out [ECard]/cedula.sign cedula.bin
5: openssl pkeyutl -derive -inkey privTM.pem -peerkey pubTE.pem -out kTM-TE.bin
6: openssl aes-256-cbc -e -kfile kTM-TE.bin -out [ECard]/cedula-cifrada.bin cedula.bin
7: openssl dgst -sha512 -verify XXX_public.pem -signature [ECard]/voto.sign [ECard]/voto.hash
8: openssl dgst -sha512 -sign [ECardMesário]/ZZ_private.pem -out [ECard]/voto.sign [ECard]/voto.hash

Neste terminal é realizada a validação da assinatura digital do eleitor gerada a partir do *message digest* do voto. O *comando 7* é responsável por este processo. Para isso, é necessário que a *chave pública* do eleitor esteja previamente armazenada no terminal. Neste momento o mesário deve verificar a documentação do eleitor e comprovar que a *chave pública* refere-se a pessoa que apresenta o *cartão eleitoral*.

Por fim, o mesário deve assinar cegamente o voto, através da assinatura do *message digest* do voto. Nesta etapa, o mesário utiliza de seu próprio *cartão eleitoral*, contendo sua *chave privada*. Para efetivar a assinatura, o mesário deve inserir sua senha privada, cadastrada durante a etapa de cadastro eleitoral. O *comando 8* executa esta função e sobrescreve o arquivo de assinatura do voto.

5.3. Terminal de Votação

Este é o terminal onde o eleitor realiza a escolha dos seus candidatos para os respectivos cargos em disputa.

O primeiro passo para habilitação da seção eleitoral é a geração de uma *chave privada* e sua respectiva *chave pública* em cada um dos terminais. No caso do *terminal de votação*, a geração da *chave privada* e exportação de sua respectiva *chave pública* é executada pelos *comandos 1 e 2* da *Lista de Comandos 3*. A *chave púbica global* gerada no servidor central e distribuída para cada seção eleitoral é utilizada como parâmetro para geração da *chave privada*.

A validação da cédula eleitoral é realizada pelos comandos 4 e 5. O comando 4 decifra a cédula eleitoral, obtendo o arquivo original gerado no terminal do mesário. Para isso é necessário derivar a chave criptográfica utilizada para cifrar a cédula, através da chave privada do terminal de escolha com a chave pública do terminal do mesário, conforme o comando 3. Por fim, pelo comando 5 valida a assinatura do mesário com base na cédula eleitoral.

Uma vez iniciada a votação, o eleitor realiza sua escolha. O *comando 7* executa a cifragem do voto do eleitor. Neste comando, Y representa o número do candidato escolhido. Utiliza-se como parâmetro o arquivo binário, criado na derivação apresentada no *comando 6*, para cifrar o voto. A saída do *comando 7* é um arquivo binário com a informação do voto do eleitor que é armazenado no *cartão eleitoral*. É importante destacar que o voto foi cifrado utilizando o AES em modo de operação CBC, recebendo um vetor de inicialização aleatório, assim dois votos iguais possuem um arquivo de saída totalmente diferente.

Em seguida, para possibilitar a assinatura cega do voto por parte do mesário, os *comandos 8 e 9* são executados. O *comando 8* calcula o *message digest* do arquivo binário do voto, a saída é uma cadeia de 512 caracteres armazenado no *cartão eleitoral*. Finalmente, no *comando 9*, o arquivo referente ao *message digest* do voto é assinado pelo eleitor. Para a assinatura, utiliza-se a *chave privada* do eleitor e a senha registrada na etapa de cadastro eleitoral. A saída gera um arquivo que também é armazenado no *cartão eleitoral*.

5.4. Terminal de Depósito do Voto

Especialmente neste terminal, é necessária a configuração do banco de dados BigChainDB, para o registro dos votos. Este terminal também possuirá o seu próprio par

Lista de Comandos 3 Execução do OpenSSL no terminal de escolha

```
1: openssl genpkey -param file [SeCard]/chave-publica-eleicao.pem -out privTE.pem
2: openssl pkey -in privTE.pem -pubout -out [SeCard]/pubTE.pem
3: openssl pkeyutl -derive -inkey privTE.pem -peerkey pubTM.pem -out kTE-TM.bin
4: openssl aes-256-cbc -pbkdf2 -d -kfile kTE-TM.bin -in [ECard]/cedula-cifrada.bin cedula.bin
5: openssl dgst -sha512 -verify ZZ_public.pem -signature [ECard]/cedula.sign cedula.bin
6: openssl pkeyutl -derive -inkey privTE.pem -peerkey pubTD.pem -out kTE-TD.bin
7: openssl aes-256-cbc -e -kfile kTE-TD.bin -out [ECard]/voto-secreto.bin <<< Y
8: openssl sha512 [ECard]/voto-secreto.bin > [ECard]/voto.hash
9: openssl dgst -sha512 -sign [ECard]/XXX_private.pem -out [ECard]/voto.sign [ECard]/voto.hash
```

de *chaves pública* e *privada*, geradas em um processo idêntico ao que ocorreu nos terminais da seção. Os *comandos 1 e 2* da *Lista de Comandos 4* realizam o processo neste terminal.

Neste terminal ocorre novamente o processo de derivação das *chaves privadas* do terminal de votação com a *chave pública* do terminal de depósito do voto. Para isso, antes da execução do comando abaixo, a *chave pública* do terminal de depósito é utilizada. O produto deste comando é um arquivo binário. O processo de derivação é realizado através do *comando 3* da *Lista de Comandos 4*.

Posteriormente é realizada uma verificação da assinatura do mesário, para tal, todas as *chaves públicas* dos mesários que irão atuar na seção devem estar previamente armazenadas. O *comando 4* calcula um novo *message digest*, tendo como saída o arquivo de validação *(validacao.hash)*. Isso impede que o voto seja alterado durante o processo.

Lista de Comandos 4 Execução do OpenSSL no terminal de depósito do voto

```
1: openssl genpkey -param file [SeCard]/chave-publica-eleicao.pem -out privTD.pem
2: openssl pkey -in privTD.pem -pubout -out [SeCard]/pubTD.pem
3: openssl pkeyutl -derive -inkey privTD.pem -peerkey pubTE.pem -out kTD-TE.bin
4: openssl sha512 [ECard]/voto-secreto.bin > validacao.hash
5: openssl dgst -sha512 -verify ZZ_public.pem -signature [ECard]/voto.sign validacao.hash
6: PythonScript << openssl aes-256-cbc -pbkdf2 -d -kfile kTD-TE.bin -in [ECard]/voto-secreto.bin
```

O próximo passo é verificar a correspondência com o arquivo recebido pelo mesário e confirmar a sua assinatura. Qualquer inconsistência nesta etapa, o comando indica um erro na tela do terminal. O *comando 5* executa a confirmação de que o voto do eleitor através de seu *message digest* (validacao.hash) foi assinado cegamente pelo mesário. Por fim, o *comando 6*, a partir do arquivo gerado na derivação entre os terminais de votação e depósito, é possível decifrar o voto do eleitor. A saída deste comando deve enviar o voto a um *script* responsável por guardar o voto do eleitor no BigChainDB.

6. Conclusão

Com o BigchainDB, as assinaturas cegas e outras tecnologias, este trabalho apresentou um modelo de sistema de votação integralmente digital e sem qualquer tipo de conexão com redes. Adaptado do processo eleitoral brasileiro, a proposta permite que a auditagem

dos votos seja realizada a qualquer tempo, uma vez que as informações criptografadas do voto se mantêm armazenadas no *cartão eleitoral*, em posse do eleitor.

Anteriormente considerado inviável, o modelo de sistema proposto possibilita a auditagem de uma eleição sem comprometer o anonimato do voto, que se mantém exclusivamente em versão digital. Logo, descarta o voto físico como um requisito obrigatório para a auditagem pública. Deve-se considerar, no entanto, que o escopo do trabalho está limitado somente a segurança da informação do processo de votação. Para além da tecnologia da informação, o sufrágio também abrange atores da esfera jurídica, social, entre outros que não são tratados neste trabalho. Por isso, embora o sistema apresentado oportunize a auditagem do voto, cabe avaliar se a solução é conveniente nas demais esferas. Entretanto, abre caminho para que futuros trabalhos sigam contribuindo para um processo eleitoral com votos exclusivamente digitais.

Referências

Adiputra, C. K., Hjort, R., and Sato, H. (2018). A proposal of blockchain-based electronic voting system. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pages 22–27.

Barros, C. F. d. and Pimenta, D. F. (2018). A Receipt-Free i-Voting System Based on Blind Signatures and Anonymous IDs. In *Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 113–120. SBC.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. In Chaum, D., Rivest, R. L., and Sherman, A. T., editors, *Advances in Cryptology*, pages 199–203. Springer, Boston, MA. https://doi.org/10.1007/978-1-4757-0602-4_18.

GmbH, B. (2018). BigchainDB 2.0, The Blockchain Database.

Marcacini, A. T. R. and Barreto Junior, I. F. (2019). Aspectos jurídicos, políticos e técnicos sobre sistemas eletrônicos de votação e a urna eletrônica brasileira. *Revista Brasileira de Estudos Políticos*, v.118. https://doi.org/10.9732/rbep.v118i0.696.

Oliveira, F. M. d. (2021). *A transparência e a auditoria da urna eletrônica: a soberania popular materializada na legitimidade do voto*. Monografia (Graduação em Direito), Faculdade de Direito, Universidade Federal do Ceará, Fortaleza. http://www.repositorio.ufc.br/handle/riufc/57982.

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

TRE (2020). Atribuições – Tribunal Regional Eleitoral do Rio Grande do Norte. https://www.tre-rn.jus.br/eleitor/mesario/atribuicoes.

TSE (2016). *Urna eletrônica: 20 anos a favor da democracia*. Tribunal Superior Eleitoral, Brasília. https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/1935.