UM SISTEMA DE VOTO ELETRÔNICO BASEADO EM BLOCKCHAIN

Henrique Niwa
Instituto Nacional de Pesquisas Espaciais - Laboratório Associado de Computação e Matemática Aplicada
Av. dos Astronautas, 1758 - Jardim da Granja São José dos Campos/SP - CEP 12227-010 - Brasil
henrique.niwa@inpe.br

RESUMO

Dentre os vários sistemas de votação existentes, os chamados sistemas eletrônicos de votação são considerados os mais eficientes, por permitirem maior velocidade nas apurações e por oferecerem garantias mínimas de validação dos votos efetuados pelos eleitores. Embora o sistema de voto eletrônico existente atualmente no Brasil seja muitas vezes encarado como modelo mundial de sucesso, algumas características de tal sistema ainda apresentam ineficiências que podem ser aprimoradas. Esta dissertação mostra o estudo e implementação de um sistema de voto eletrônico, utilizando-se de *blockchain*, um banco de dados descentralizado e criptografado. O sistema proposto, além de oferecer ainda mais segurança ao processo de votação, permitiria maior flexibilidade para os eleitores apresentarem e auditarem seus votos. Por ser baseado fortemente em criptografia, o sistema proposto deve ser implementado em processadores de alto desempenho, como CPUs com múltiplos núcleos.
Palavra-chave: Voto eletrônico; Blockchain; Bitcoin; Ethereum.

ABSTRACT

Among the various voting systems existing currently, those based on electronic voting are viewed as the most efficient ones, because they allow greater speed in tabulating results and offer minimal guarantees for validating the deposited votes. Although the current Brazilian voting system is viewed as a model for the rest of the world, some of its characteristics present room for improvements. This dissertation is about the study and implementation of an electronic voting system based on the blockchain, a decentralized, cryptographic database. This proposed system, in addition to offer even more security to the voting process, would enable more flexibility for voters to deposit and audit their votes. Being strongly based on cryptography, this system was implemented with high performance processors, such as multi-core CPUs. **Keywords:** Electronic voting; Blockchain; Bitcoin; Ethereum.

Como Citar:
NIWA, Henrique. Um sistema de voto eletrônico baseado em blockchain. In: SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA, 19., 2019, Rio de Janeiro, RJ. **Anais** [...]. Rio de Janeiro: Centro de Análises de Sistemas Navais, 2019.

1. INTRODUÇÃO

Existem diferentes meios de votação pelo mundo, o mais comum e simples é o que se utiliza de cédulas de votação, um processo que consiste no eleitor ir a um centro designado, criar a marcação de sua preferência sendo observado por um grupo de auditores, mas com o voto ainda secreto e depositar sua ficha de papel em uma urna. Esses votos então são agregados de todos os diferentes centros de votação e posteriormente validados e contabilizados se utilizando de métodos manuais e automáticos. Para uma pequena quantidade de votantes é um meio simples e razoavelmente rápido de votar e contar, porém para grandes populações há um grande trabalho a ser feito e portanto levam-se dias para finalizar o evento. Também existe o risco de que contagens erradas, fraude nas cédulas e urnas de votação e ausência de eleitores atrapalhe e/ou mude o resultado. No Brasil temos um sistema de voto onde se utilizam urnas eletrônicas, que fazem a contagem e contabilidade local dos votos, ainda assim é necessário que as unidades de memória de cada máquina sejam enviadas para um local central e efetuada a leitura e agregação de votos, essas unidades de memória e as máquinas em si necessitam de segurança para que os dados não sejam modificados por partes maliciosas interessadas. Desde 2005 a população da Estônia utiliza um sistema de voto eletrônico auxiliar ao tradicional, onde na última eleição 30% da população utilizou deste meio. Foi organizado de forma que o eleitor possa fazer sua escolha através de um computador pessoal e posteriormente checando seu voto através do smartphone, essa separação de dispositivos traz uma segurança na verificação individual dos votos pela população. [1][2] O sistema atual de voto eletrônico do Brasil consiste em urnas eletrônicas que realizam a gravação dos dados de forma digital, também chamadas de 1a geração ou DRE (*Direct Recording Electronic voting machine* máquina de gravação eletrônica direta do voto), podendo ser conferidas apenas com a participação do administrador do sistema e do desenvolvedor do software. Existe uma 2a geração, proposta por [3] que propõe a impressão de um comprovante do voto, possibilitando a auditoria contábil da votação, chamado *Independent Voter Verifiable Record* (Registro Independente Conferível pelo Eleitor), ou IVVR. No Brasil é comum ser chamado de "Voto Impresso Conferível pelo Eleitor", ou VICE[4]. Existe ainda uma 3a geração de sistemas eleitorais, os quais contam com RFID ou chips de identificação por rádio-frequência. Estes possibilitam a conferência do voto pelo eleitor independente de software e facilitam uma auditoria independente, sendo chamados "*End-to-End verifiability*"ou, E2E.

1.1. Motivação

O sistema eleitoral brasileiro já teve alguns incidentes de segurança, segundo [5] temos alguns exemplos:

> "O Caso Diadema, SP - 2000: A análise desses arquivos revelou que todas as urnas eletrônicas tinham sido carregadas fora da cerimônia oficial de carga e lacração, dias antes da convocação por edital público, tendo todas ficado sem lacres durante dias. A grande maioria das urnas eletrônicas utilizadas - 431 de 451 - foram inseminadas com o software de votação nos dias 22 e 23 de setembro, 2 em 24/9, 7 em 25/9, 2 em 26/9, sendo que todas elas só foram lacradas no dia 28/9. Esses dados mostravam que a totalidade das urnas eletrônicas de Diadema em 2000, estiveram carregadas com os programas mas sem lacre e sem a presença de fiscais dos partidos políticos por vários dias."[5,

24]

"O Caso Marília, SP - 2004: Em auditoria, os Arquivos de Espelhos de Boletins de Urna da 400º Zona Eleitoral indicavam que muitas seções eleitorais tiveram seus resultados recebidos para apuração antes do início da votação."[5, 26]

"O Caso Alagoas - 2006: Diversas irregularidades nos arquivos gerados pelas urnas foram detectadas por auditores externos. Frente as evidências, o administrador negou acesso aos arquivos solicitados pelos auditores e transferiu ao requerente uma cobrança antecipada no valor de 2 milhões de reais para que fosse desenvolvida uma perícia das urnas. Diante do não pagamento do valor proibitivo, o requerente foi multado e condenado por litigância de má-fé."[5, 30]

"O Caso Itajaí, SC - 2008: Nenhuma urna preparada para a votação passou pelo teste obrigatório prescrito pelo Art. 32 da Res. TSE 22.712/08. Um caso foi o da 97ª Zona Eleitoral onde a urna da seção 236 que foi sorteada para o teste obrigatório foi substituída por outra na hora do teste, preparada exclusivamente para este fim. A urna que foi utilizada para o teste foi posteriormente colocada à parte e recarregada, procedimento que destruiu eventuais provas nela gravadas."[5, 34]

Segundo [6] eram esperados 146 milhões de eleitores em 2018, porém na votação final foram contabilizados 116 milhões, havendo 11 milhões de brancos e nulos, portanto quase 20 milhões de abstenções. Em 2018 as eleições ocorreram em 7 de outubro [7], o prazo para troca de zona eleitoral em 9 de maio [8], o pedido para voto em trânsito em 23 de agosto [9], ou seja a população teve menos de 1 mês e meio para poder requisitar o direito ao voto sem estar em sua zona eleitoral de registro. Com um sistema independente da localidade dos votos, o eleitor poderá votar em qualquer dispositivo ou ainda em qualquer zona eleitoral. Essa desburocratização do voto poderia incluir uma parcela significativa de eleitores (figura 1).

1.2. Objetivos deste trabalho

O presente trabalho tem por objetivo criar um voto eletrônico seguro e eficiente, descentralizado, transparente e totalmente auditável, que possa ser usado em diferentes dispositivos e situações. Isso foi alcançado utilizando a tecnologia de *blockchain*, um banco de dados criado através de uma rede distribuída, descentralizada e com criptografia de chaves público-privada e algoritmos de hash seguros.

2. REFERENCIAL TEÓRICO

O *blockchain* é um conceito análogo a um livro-razão em que todas as transações de entrada e saída devem ser escritas em ordem histórica, com o saldo dessas transações anotado. A última informação sempre será a mais atual e levará em conta o histórico.

Figura 1: Parcela de eleitores que não votaram em 2018.

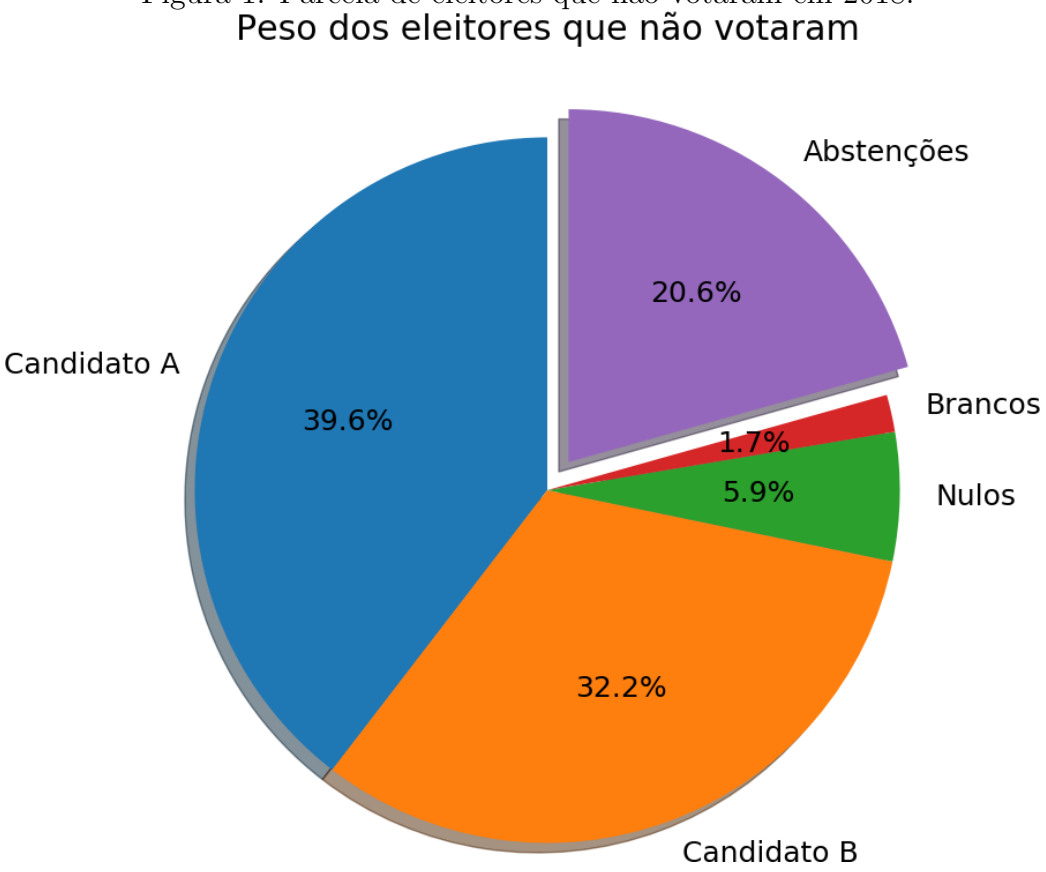


Tabela 1: Um livro razão exemplo

Índice	Remetente	Valor	Destinatário
1	Renan	10	Matheus
2	Ana	50	Matheus
3	Matheus	60	Joana

A última entrada no livro razão só foi possível pelo fato de Matheus ter tido duas entradas anteriores como destinatário.

2.1. Bitcoin

A moeda eletrônica *Bitcoin*[10] popularizou o conceito, utilizando o conceito de consenso entre os participantes, ou seja, a transação precisa ser homologada, ou aceita por um número mínimo de participantes antes de ser inclusa. Utilizando criptografia de chaves público/privada, onde a chave pública é utilizada nas comunicações do o mundo para o indivíduo e a sua chave privada é usada em conjunto com a chave pública de um terceiro para a criação de uma mensagem que só pode ser descriptografada com a chave privada do destinatário. Esse é o suporte por trás das transações que são feitas e escritas no *blockchain*. As transações são acumuladas em filas de prioridade e quando houver um consenso sobre a ordem das transações é calculada uma *hash* em cima do bloco e do bloco anterior, em conjunto com um valor que pode ser modificado, para produzir uma *hash*

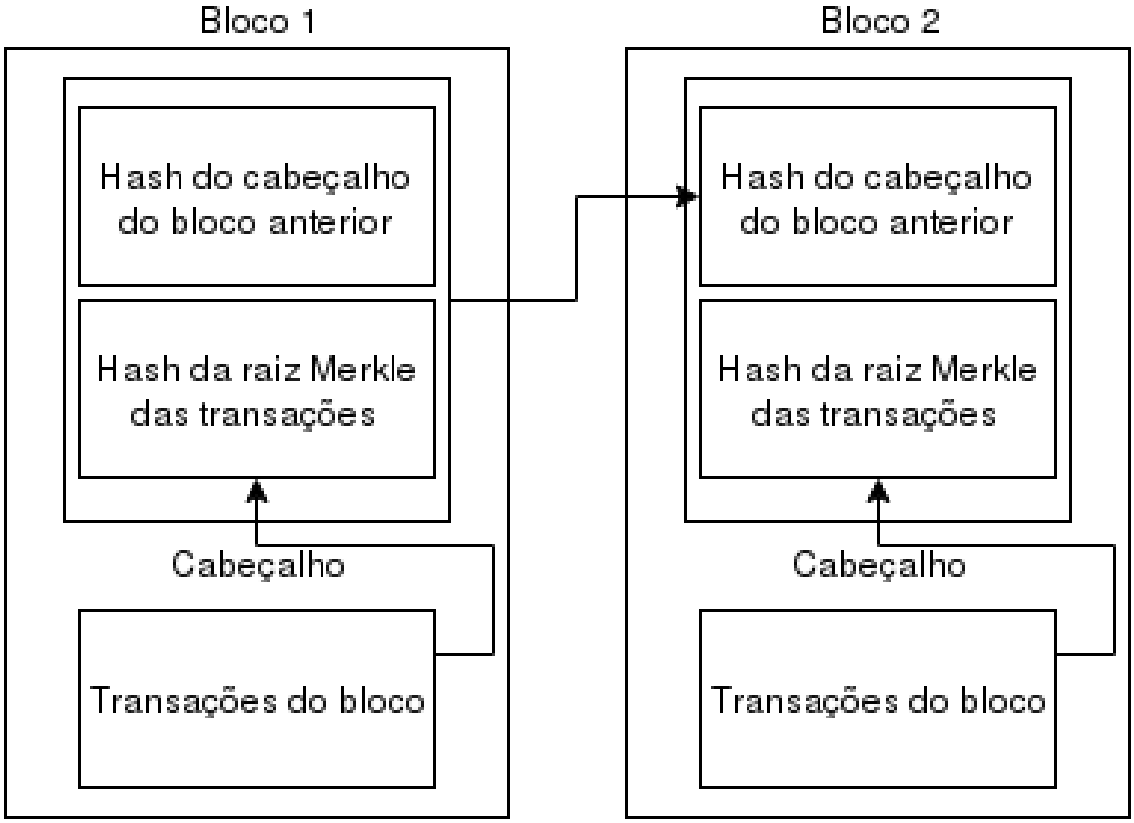
final com determinado nível de dificuldade, esse valor que pode ser alterado é chamado de nonce e o objetivo, no bitcoin, é encontrar uma *hash* final com determinado número de 0's iniciais. Esse é o principal trunfo do *bitcoin*, baseado no algoritmo Hashcalc[11], ele define que um bloco só deve ser incluso caso tenha o número mínimo de 0's a esquerda em sua *hash*, pela natureza injetora da função matemática é necessário um trabalho de força-bruta, em que todos os dados são modificados até que se atinja o resultado. Isto pode ser feito através de um campo no cabeçalho específico para isso o Nonce, como é um número de 32 bits, há

$$2^{32} = 4294967296$$

possibilidades, muitas vezes a dificuldade mínima não é atingida, pode ser modificado uma parte do campo de tempo de modo que o tempo do bloco não seja diferente do tempo atual em mais do que algumas horas, enfim a saída é mudar a ordem das transações. Vários computadores ao redor do mundo estão permanentemente conectados a internet recebendo as transações e gerando novos blocos, eles competem entre si para a maior geração de blocos possíveis, a maior cada cadeia é escolhida como a principal e replicada, todos que estavam trabalhando em uma cadeia alternativa precisam conferir quais transações foram armazenadas e iniciar uma nova busca com o restante. Essa rede distribuída garante que não haja uma autoridade principal. Neste trabalho o sistema seria gerido pelo governo e auditores, para evitar interferências externas

O encadeamento de *hash's* é caracterizado por uma árvore binária *Merkle tree*, os blocos também são encadeados como mostra a figura 2.

Figura 2: Estrutura de blocos em corrente.



Um exemplo seria um bloco com função hash h, cabeçalho do bloco como b e

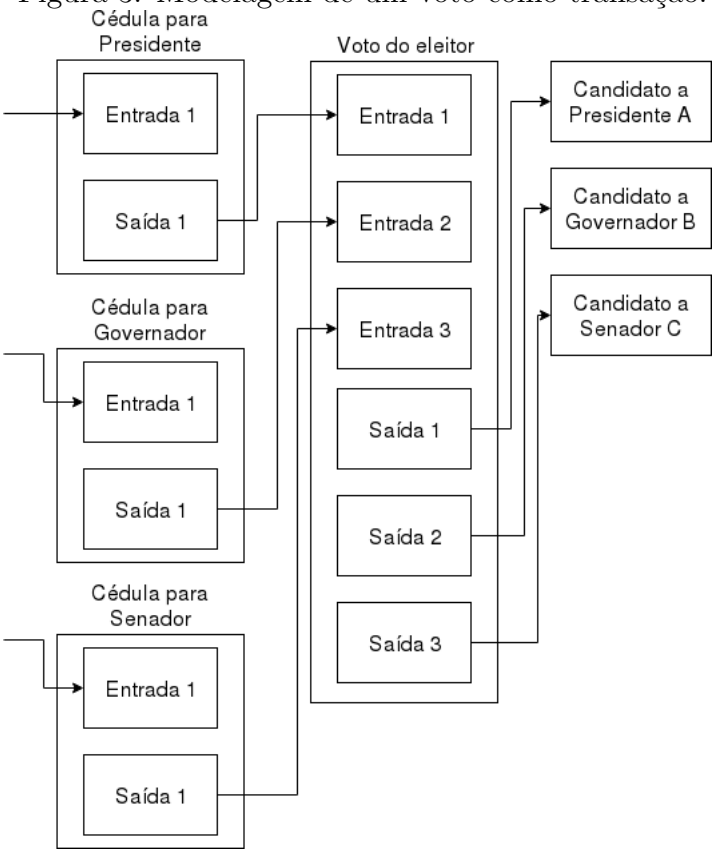
transação t, Nb é o bloco N, Nt é a hash Merkle raiz, para um bloco com 4 transações a composição dessa árvore binária seria:

$$h(b(N)) = h(b(N-1)) + h(t(Nt))$$
$$h(t(Nt)) = h(t(ab)) + h(t(cd))$$
$$h(t(ab)) = h(t(a)) + h(t(b))$$
$$h(t(cd)) = h(t(c)) + h(t(d))$$

Cada transação consiste de uma ou múltiplas entradas e uma ou múltiplas saídas. Para a finalidade de um sistema de voto, foi utilizada somente uma entrada, que é a distribuição inicial. As transações são usadas como cédulas eleitorais, cada uma representa um voto que pode ser fracionado, na distribuição cada eleitor recebe 10 unidades, podendo distribuir entre os candidatos, exemplo:
Candidato A recebe 90%
Candidato B recebe 10%

Extrapolando pra várias categorias de candidatos, podemos distribuir 100 unidades e na mesma transação efetuar a distribuição e checando na validação os diferentes pesos, numa eleição de presidente, governador, senador, deputados federais e estaduais cada categoria teria 20 unidades. Como mostra a figura 3.

Figura 3: Modelagem de um voto como transação.



Cada entrada foi uma saída anterior, como podem haver várias saídas é necessário indicar qual a numeração em que ela ocorreu. Uma transação tem o seguinte formato:

Entradas: *hash* transação de origem, número de saída dessa transação Saídas: endereço para saída, valor

Cada usuário, tanto quem receba quanto envie, possui 3 dados importantes, seu endereço que é derivado a partir da chave pública, chave pública e chave privada. A criptografia utilizada é a *Elliptic Curve Digital Signature* (ECDSA), esse sistema deriva do algoritmo *Digital Signature Algorithm* (DSA). Ao enviar os dados utiliza-se em conjunto a chave privada do remetente e a chave pública do destinatário, o qual pode verificar que os dados foram assinados pelo remetente. As chaves utilizam uma função dupla de hash SHA256, o endereço é a chave original com uma hash SHA256 e depois uma RIPEMD160.

No blockchain uma transação é criada e verificada atráves de uma linguagem de *script* baseada em *Forth* e de funcionamento análogo a uma pilha de dados. Para se enviar, cria-se um *script* utilizando uma transação de entrada que o autor seja o destinatário, uma quantidade (igual ou menor da transação original) e o endereço do novo destinatário, o destinatário irá verificar a origem como sendo do remetente através de uma assinatura feita com a chave privada do mesmo e poderá utilizar esta transação como uma entrada, se utilizando de sua chave pública que terá a mesma *hash* gravada na transação.

3. DESENVOLVIMENTO

Este trabalho se baseou no código do *bitcoin*, este projeto foi o que iniciou a revolução do *blockchain*, desde sua criação não houve nenhuma falha de segurança grave, é a criptomoeda com maior capitalização(141B USD)[1], valor individual(7200 USD)[2], maior valor mediano de transferências(509 USD)[3] e maior número de endereços ativos diários (772.000)[4]. Essa importância do *bitcoin* significa que em qualquer momento existem dezenas de milhares de desenvolvedores e usuários procurando falhas em sua rede de modo a obter acesso ou criar *bitcoins* sem efetuar os cálculos necessários. O desafio do trabalho foi escalonar a operação, a rede do *bitcoin* foi projetada desde o princípio para gerar novos blocos a cada 10 minutos[5], com cada bloco tendo em média 2000 transações, o algoritmo se adapta ao poder computacional da rede fazendo com que este intervalo se mantenha não importando o número de nodos da rede. Também conta com diversas funções, distribuição dos blocos, distribuição das transações, banco de dados otimizado para gravação e recuperação das informações, criação de uma rede independente, código criptográfico robusto. Também a cada novo desenvolvimento do código principal do *bitcoin*, as mudanças podem ser incorporadas retroativamente, não sendo necessária uma equipe de desenvolvimento própria e se utilizando do conhecimento da comunidade.

A ideia original foi trabalhar a dificuldade mínima de geração de cada bloco, permitindo uma geração mais rápida. Cada bloco gerado, ou minerado, recebe como prêmio pela participação na rede 50 *bitcoins*, cada moeda pode ser dividida em 100 milhões de unidades. Também modificando o intervalo e o tamanho dos blocos, permitindo uma geração mais rápida de blocos maiores. Os mineradores iriam distribuir frações dos *bitcoins* para cada eleitor, processo o qual também gera transações precisando de um período para criação destes novos blocos. Qualquer nodo externo poderia se conectar a rede e incluir

[1]https://bitinfocharts.com/comparison/bitcoin-marketcap.html
[2]https://bitinfocharts.com/comparison/bitcoin-price.html
[3]https://bitinfocharts.com/comparison/mediantransactionvalue-btc-eth.html
[4]https://bitinfocharts.com/comparison/activeaddresses-btc-eth.html
[5]https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html

novos blocos, gerando para si *bitcoins* e podendo distribui-los, isso seria o equivalente a forja de votos. Isto poderia ser mitigado pela criação de uma rede de computadores protegida por *firewall*. O conceito do sistema de voto com *blockchain*, são servidores funcionando como nodos completos, que gerariam blocos e receberiam transações. No período de preparação estes servidores gerariam um par de chaves e um endereço para cada eleitor, fariam a criação das cédulas distribuindo os *bitcoins* nestes endereços. Essa associação eleitor e endereço seria de responsabilidade do governo, para distribuição das chaves uma autenticação é necessária, podendo ser uma senha cadastrada previamente ou até biometria. O problema desta ideia é que os recursos computacionais exigidos seriam cada vez maiores, também há o fato de que a maioria dos cálculos seria desperdiçado, resultando em tempo e energia gastos sem utilidade.

3.1. Melhorias

O projeto final trabalhou modificando o tamanho dos blocos, o tempo de processamento entre cada bloco, a criação de transações especiais que criam *tokens* utilizando-os como cédulas, permissões de acesso, paralelização da apuração e da simulação de milhares de votos simultâneos. Estas modificações foram feitas com base no código do *bitcoin* e do *multichain*. Além disso foram criados clientes em linha de comando para as simulações e também em modo gráfico para demonstração.

3.1.1. Utilizando permissões de acesso

Um *blockchain* com permissões possui um controle de acesso, que dita quem pode administrar, conectar, enviar, receber, minerar. Algumas soluções já existem para isso como o Corda[12], *Chain Core, Credits, HydraChain, BigchainDB*. Foi escolhida a implementação do *multichain* por ser baseado e manter compatibilidade com o código do *bitcoin*, implementando este controle de acesso. Também foi escolhido pela licença do código ser aberta e qualquer trabalho derivativo também precisar ser aberto, isto concorda com os valores de pesquisa financiada com verba pública também ser aberta a todos.

O administrador possui as chaves iniciais, assim que se inicia uma blockchain, o software cria uma chave que assina os blocos e o identifica ao conectar com outros nodos. Esta chave concede permissões a qualquer outra chave. No sistema implementado as permissões padrões do sistema são:

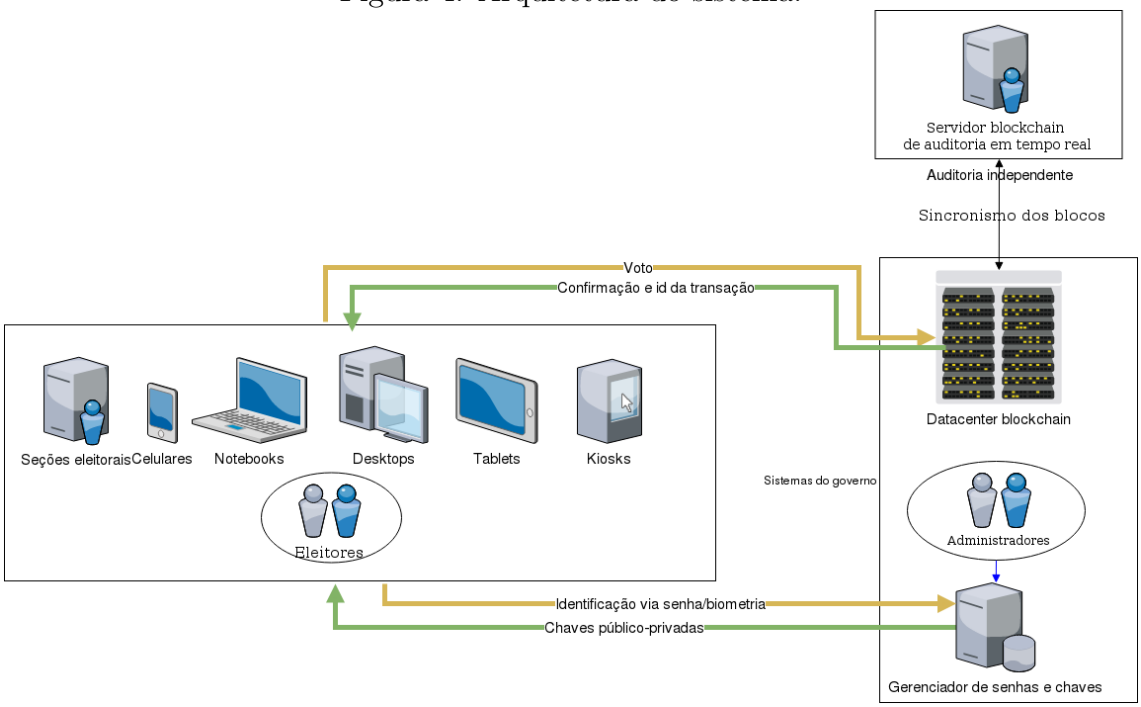
- Apenas nodos permitidos podem se conectar
- Apenas nodos permitidos podem criar blocos
- Todos os nodos podem enviar e receber transações
- Apenas transações permitidas podem ser enviadas
- Apenas nodos permitidos podem criar transações iniciais

Estas permissões são armazenadas dentro da própria *blockchain*, o nodo que tiver acesso e se conectar irá efetuar uma cópia de todos os blocos, transações e permissões.

3.2. Arquitetura

A arquitetura do sistema consiste em servidores, chamados de nodos, que fazem a criação de blocos e inclusão das transações. Estes servidores trocam blocos e transações entre si, além de receberem dos clientes as transações. Cada cliente cria e assina a transação antes de enviar (figura 4). Além disso servidores de auditoria podem ser criados e incorporados a rede, esta rede deve ser protegida por *firewall*, embora não haja formas de acesso ilegais no sistema atual, novas descobertas no protocolo podem ser feitas. Os servidores devem ser máquinas com grande capacidade de processamento e acesso a disco de alto desempenho. Os aplicativos clientes precisam apenas implementar uma forma de requisição *http* com os devidos parâmetros.

Figura 4: Arquitetura do sistema.



Fonte: Autor

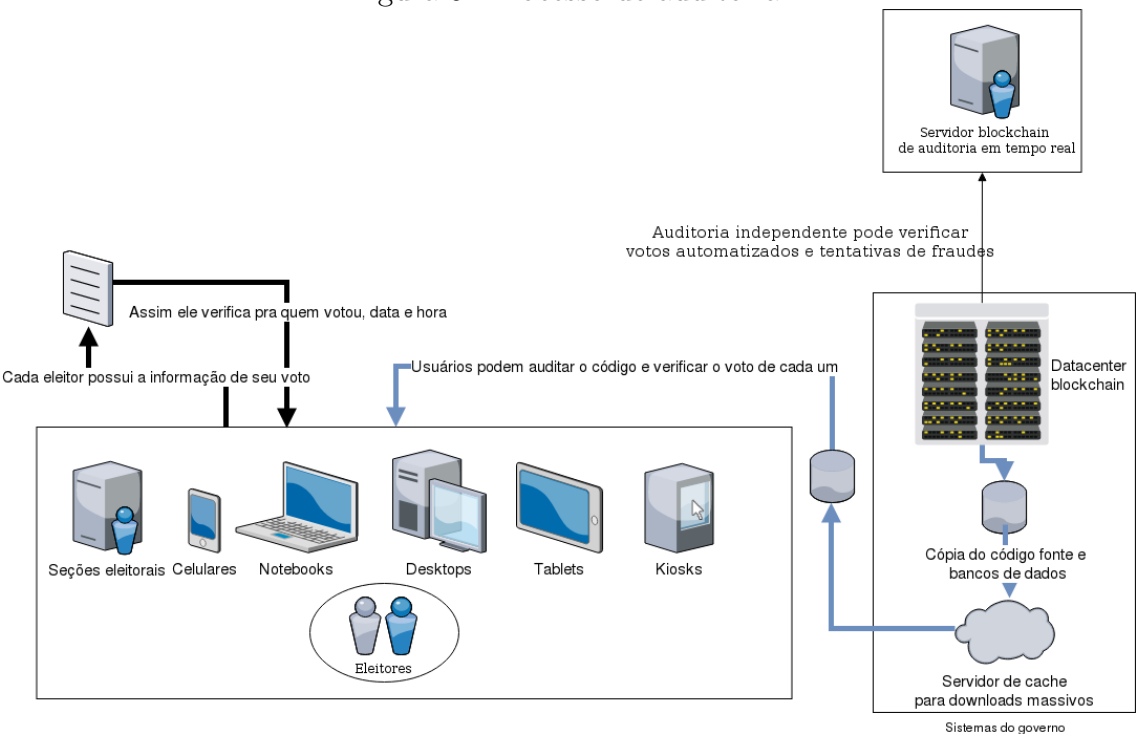
Os votos de cada cliente podem ser conferidos e contabilizados, utilizando da confirmação do voto pode-se averiguar se dentro da *blockchain* os dados foram computados corretamente. Nenhum usuário é indicado pelo seu nome ou cpf, mas sim pela sua chave pública. A auditoria pode ser feita na base de dados dos votos e também no código fonte dos programas, como mostra a figura 5.

4. FILOSOFIA DE DESENVOLVIMENTO

O sistema implementado buscou alguns objetivos:

1. Anonimato
2. Segurança
3. Imutabilidade
4. Acesso Remoto além de zonas eleitorais
5. Verificável pelo usuário

Figura 5: Processo de auditoria.



Fonte: Autor

6. Auditável
7. Código aberto

O anonimato foi garantido pelo fato dos usuários terem apenas informações das chaves públicas (através dos endereços no *blockchain*) registradas no banco de dados. A segurança se teve ao utilizar criptografia estabelecida e implementações já testadas. Imutabilidade vem da própria natureza do *blockchain*, onde cada novo bloco aumenta ainda mais a segurança dos dados. Acesso remoto se teve pelo uso de uma requisição HTTP aos serviços, qualquer cliente pode ser escrito que possua uma biblioteca de requisições web. Podem ser criados clientes para computadores desktop, aplicativos para Android e iOS, navegadores web. Esta requisição utiliza JSON e poderia ser feita utilizando HTTPS assim evitando que os dados da rede sejam interceptados e se crie uma associação da chave pública com um endereço da internet e consequentemente com uma pessoa física. Verificação através do id da transação, cada voto irá retornar um identificador que irá permitir saber o destino do voto, quantidades e data. Auditabilidade completa, no final da divulgação dos resultados, é distribuído o banco de dados com todos os votos, todos poderão ver os votos, a associação entre um eleitor e sua identidade nos registros só poderá ser feito por cada um. Ainda enquanto a votação estiver sendo realizada, um nó pode ser gerido por uma auditoria, que poderá conferir em tempo real os votos. O uso de código aberto foi primordial, pois a pesquisa utilizou de verba pública, também houve cuidado ao se escolher a licença de *copyright*, pois o código original do *bitcoin* é uma licença MIT, quer dizer que o código pode ser modificado e utilizado como quiser, sem necessitar de divulgação. A licença utilizada foi a GPLv3, ela dita que qualquer modificação deve ter seus fontes divulgados.

Foram utilizados containers docker para criação de ambientes de compilação e testes. Segundo a licença GPLv3 não se deve apenas divulgar o código fonte, mas também todo o necessário para que seja feita a compilação do mesmo, incluindo as versões das bibliotecas, compiladores e demais ferramentas. Utilizando de um container a auditoria se torna prática.

Os testes foram feitos utilizando um servidor com:

- 32GB de memória RAM
- 2x Intel(R) Xeon(R) CPU E5620[6] @ 2.40GHz (8 núcleos físicos, 16 virtuais)
- Discos em Raid0 que permitiram leitura sequencial de até 900MB/s
- Rede 100Mbit

A primeira máquina cliente:

- 12GB de memória RAM
- 2x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (8 núcleos físicos, 16 virtuais)
- Rede 100Mbit

A segunda máquina cliente:

- 4GB de memória RAM
- Intel® Core™ i7-4790 Processor @ 3.40GHz (4 núcleos físicos, 8 virtuais)
- Rede 100Mbit

4.1. Literatura correlata

Na literatura existem diversos trabalhos relacionados a voto e blockchain, foram previamente estudados os seguintes trabalhos [13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[23],[24],[25],[26],[27] A infraestrutura é assunto de alguns, outros utilizam as blockchains públicas do bitcoin e do ethereum, alguns trabalhos falam sobre o uso de biometria e voto sobre coersão. Nos trabalhos em que houve implementação não há resultados quantitativos que os tornem possíveis em eleições de grande porte. As blockchains públicas não permitem o volume de transações necessário. Seja por design do algoritmo, como é o caso do bitcoin em que os blocos são gerados a cada 10 minutos [10], ou pelo volume atual da rede, exemplo do ethereum com 750 mil diárias[7].

5. RESULTADOS

Os testes levaram em conta um número de eleitores de dezenas milhões de usuários e também o tempo de votação com as urnas eletrônicas atuais do Brasil, onde a apuração é feita no mesmo dia. Nos testes não foi possível passar da barreira de 45 milhões de

[6]https://ark.intel.com/content/www/us/en/ark/products/47925/intel-xeon-processor-e5620-12m-cache-2-40-ghz-5-86-gt-s-intel-qpi.html

[7]https://bitinfocharts.com/comparison/transactions-btc-eth.html

transações por dia no hardware utilizado, melhores resultados são esperados com maior capacidade de processamento e velocidade de armazenamento. Por permitir o voto em qualquer dispositivo, além das zonas eleitorais, o processo de eleição pode se estender por vários dias que não encareceria os custos com infraestrutura. Também não há possibilidade de que a contagem seja divulgada pois cada eleitor tem acesso somente ao seu voto. Ainda há outra forma de remediar esta limitação utilizando de vários nodos, que trocariam entre si blocos e transações, havendo uma distribuição de carga. Também há a possibilidade de que se crie vários *blockchains* delimitados por região física, o eleitor que vá votar para governador não precisaria ter acesso ao *blockchain* de outros estados, para categorias mais abrangentes como presidente também é possível que os votos sejam feitos em separados e na apuração de cada região seja contabilizada no geral. O processo de cada cliente se inicia ao conectar a um dos nodos principais através de uma chamada *HTTP-RPC*, autenticando com seu CPF e uma senha previamente estabelecida, em contra-partida recebe uma id de transação, indicando qual sua cédula e a localização da transferência para seu endereço dentro dessa transação, pois uma transação pode ter várias saídas pra destinatários diferentes, além disso receberá suas chaves público-privadas e o endereço. No cliente do eleitor há uma listagem de todos os candidatos e seus endereços associados.

5.1. Simulando processo eleitoral

Os testes utilizaram os dados de 50 milhões de execuções simulando eleitores com destino a dois candidatos. Essas execuções foram divididas em 500 instâncias simultâneas, a mediana do tempo de execução foi de 0,799763s.

5.1.1. Distribuição

A distribuição dos votos consiste primeiramente da criação de uma transação especial com a quantidade total de votos a serem utilizados. Nenhum voto fora dessa transação pode ser computado pelos nodos. A partir de uma transação de origem, a próxima deve usar a quantidade exata de votos ou incluir uma saída extra com os votos restantes e um endereço. Há limitações no tamanho máximo do número de saídas da transação, nos testes o limite padrão de 4000 saídas foi utilizado. O processo de distribuição tem uma natureza obrigatoriamente sequencial, as primeiras 3999 cédulas são distribuídas entre os eleitores e a última saída para o endereço do administrador com o total de votos menos esses 3999. Essa transação gera um identificador que é usado na próxima iteração. Isso se repete até que todos os eleitores tenham recebido e o endereço do administrador ficaria com o resto das cédulas não utilizadas.

Tabela 2: Tempo para simulação da distribuição dos votos

Votos	Tempo	Número de transações
1 milhão	44,865s	251
10 milhões	509,859s	2501
100 milhões	5619,241s	25007

5.1.2. Simulando os votos

Tabela 3: Tempo para simulação da execução dos votos

Votos	Tempo de execução
50 milhões	29h37m

Na execução dos votos temos que inicialmente o número de transações por hora era de 2 milhões, mas ao término de 24 horas haviam sido executados 43 milhões de votos, aproximadamente 10% a menos em relação ao esperado inicialmente. Também temos que o consumo de memória se manteve constante (¡ 1600MB.

5.1.3. Apuração

O processo de apuração é um problema massivamente paralelo, são milhões de operações independentes umas das outras, para tanto foram criadas funções otimizadas para processadores de vários núcleos. As informações das transações contém individualmente um volume de dados muito pequeno, são milhões de operações de curtíssimo tempo. O processo é paralelizado utilizando *OpenMP*, onde cada *thread* recebe um bloco com várias transações, cada bloco pode conter um número variado de transações e cada transação tem um número variável de saídas, pra cada uma dessas saídas teve de ser feita a contabilidade. O escalonamento do trabalho e do número das *threads* é dinâmico por conta dessa variação.

Tabela 4: Tempo para apuração de 50 milhões de votos

Número de threads	Tempo de execução
1	1531,356s
2	770,941s
4	389,177s
8	205,703s
16	176,852s
32	177,400s

5.2. Auditoria

Segundo Rivest[31], um dos autores da chave de criptografia RSA e autor do Princípio da Independência de Software em Sistemas Eleitorais: “Um sistema eleitoral é independente do software se uma modificação ou erro não-detectado no seu software não pode causar uma modificação ou erro indetectável no resultado da apuração.” De acordo com este princípio, o presente trabalho atende, pois sua implementação pode ser feita em outra linguagem ou arquitetura desde que respeitando as regras do *blockchain*, usando as mesmas funções matemáticas, regras do protocolo e com as mesmas regras de transação.

O código fonte compactado fica abaixo de 10MB, isto inclui os fontes originais do *bitcoin* e *multichain* mais modificações e melhorias implementadas pelo autor. A imagem docker do ambiente de compilação com todas as bibliotecas instaladas ocupa 600MB instalado. O banco de dados com o histórico de 100 milhões de votos contabilizados tem 55GB, 50 milhões 35GB e 10 milhões 5GB.

Cada voto ou transação, gera um identificador.

$$7d2572c5426faca62f37e6ab275fafd792869e9ee2f5d32b5aaa767e1e375f82$$

Ele pode ser usado para recuperar os dados de voto e assim validar se a escolha do eleitor foi mantida ou manipulada. Esse identificador pode ser convertido para um *QR code* para facilidade de uso. O eleitor interessado em auditar seu próprio voto pode fazer o download do código, a base de dados, compilar ele mesmo e validar as informações, nessa transação haverá a transação origem da cédula dele, pra quais endereços de candidatos ele enviou e a quantidade de votos. Existem[8] interfaces[9] gráficas[10] e web para explorar o *blockchain*, elas podem ser usadas neste sistema.

6. CONCLUSÕES

O objetivo deste trabalho foi implementar e testar um sistema de votação eletrônico, baseado em *blockchain*, com código livre e uma licença que obriga qualquer trabalho derivativo que disponibilize as modificações (GPLv3). Isso faz com que tanto o código como a base de votos possam ser auditados por qualquer um.

Em comparação com o sistema de urna eletrônica no Brasil as seguintes diferenças, melhorias são apresentadas:

1. Votos são gravados eletronicamente localmente dentro da urna. Na presente proposta, os votos são transmitidos por rede, podendo inclusive utilizar uma rede não segura como a internet.

2. Votos podem ser corrompidos em hardware [32]. Nesta implementação, os votos são transmitidos no mesmo instante em que são realizados, e após inclusão na *blockchain* não há chance alguma de modificação.

3. Necessidade de comparecimento a uma zona eleitoral. Na presente proposta podemos ter softwares de voto funcionando em celulares e computadores pessoais, cada eleitor será responsável exclusivamente por seu voto, não sendo possível que manipule os votos de outra pessoa.

4. Atualmente, a auditoria é feita por grupos convidados pelos órgãos competentes, sendo feita exclusivamente no software e apenas no processo de voto não na contabilização; uma auditoria em tempo real em época de eleição não é possível. Nesta proposta, qualquer pessoa que tenha acesso a *blockchain* pode conferir em tempo real a inclusão dos votos, embora a divulgação desses dados alterasse o resultado.

5. Um eleitor não pode verificar se seu voto foi computado corretamente. Mesmo que haja a impressão de um comprovante da escolha feita, o eleitor não tem como verificar que seu voto foi incluso no total. Na nossa proposta, o voto fica exposto e pode ser verificado pelo usuário de forma anônima.

6. No processo de voto atual, a privacidade do eleitor é garantida apenas pela câmara de votação. Na nossa proposta, o eleitor poderia votar de qualquer lugar e sua

[8]https://btc.com
[9]https://blockchair.com
[10]https://blockchair.com

privacidade de voto na auditoria é garantida pelo uso de chave pública identificando seu voto. Apenas quem distribuiu o voto sabe a relação entre chave pública e identidade.

Os resultados foram animadores, levando em conta que a *blockchain* utilizada pelo *bitcoin* teve uma média diária de 380 mil transações e a *blockchain* do *ethereum* 900 mil, o sistema desenvolvido obteve 43 milhões utilizando a mesma estrutura de segurança, redundância e flexibilidade do *bitcoin*, utilizando de um processador lançado em 2010. Os resultados serão melhores utilizando melhor hardware.

Também deve-se levar em conta que este sistema proposto é de código aberto, utilizando hardware convencional e sem custos para utilização, nas blockchains do bitcoin e ethereum há taxas para cada transação, as médias são bitcoin: 2,9 USD e ethereum 0,14 USD.

Há limitações no algoritmo que precisam ser verificadas, a geração e inclusão de milhões de transações precisa evitar conflitos de hash e há várias travas para o acesso às estruturas de dados, para evitar condições de corridas nas *threads* concorrentes. O acesso a disco também requer milhares de operações não sequenciais por segundo, que poderiam ser beneficiadas utilizando de armazenamento flash.

7. REFERÊNCIAS BIBLIOGRÁFICAS

[1] LEETARU, K. *How Estonia's E-Voting System Could Be The Future*. 2017. Disponível em: <https://www.forbes.com/sites/kalevleetaru/2017/06/07/how-estonias-e-voting-system-could-be-the-future>. Acesso em: 24 mar. 2019. 2

[2] SOLVAK, K. V. M. *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015)*. 2016. Disponível em: <http://skytte.ut.ee/sites/default/files/skytte/e$_v oting_i n_e stonia_v assil_s olvak_a 5_w eb.pdf$¿.$Acessoem$: $24mar.2019.2$

[3] MERCURI, R. T. *Electronic vote tabulation checks and balances*. Tese (PhD) — University of Pennsylvania, Philadelphia, 2001. AAI3003665. Disponível em: <https://repository.upenn.edu/dissertations/AAI3003665>. 2

[4] FILHO, A. B. *Modelos e Gerações dos Equipamentos de Votação Eletrônica*. 2014. Disponível em: <http://www.brunazo.eng.br/voto-e/textos/modelosUE.htm>. Acesso em: 24 mar. 2019. 2

[5] CUNHA, S. S. d. et al. *Relatório sobre o Sistema Brasileiro de Votação Eletrônica*. COMITÊ MULTIDISCIPLINAR INDEPENDENTE, 2014. Disponível em: <http://www.brunazo.eng.br/voto-e/textos/CMind-1-Brasil-2010.pdf>. 2, 3

[6] ARRIAL, T. *Estudo Técnicos - junho de 2018*. Confederação Nacional de Municípios, 2018. Disponível em: <https://www.cnm.org.br/cms/biblioteca/Eleitorado-2018.pdf>. 3

[7] TSE. *Eleições 2018: confira as datas do calendário eleitoral*. 2018. Disponível em: <https://g1.globo.com/politica/eleicoes/2018/noticia/eleicoes-2018-datas.ghtml>. 3

[8] CALEGARI, L. *Prazo para agendar pedido ou transferência de título eleitoral acaba sexta*. 2018. Disponível em: <https://exame.abril.com.br/brasil/prazo-para-pedir-ou-transferir-titulo-eleitoral-termina-nesta-sexta/>. 3

[9] RAMALHO, R. *Prazo para eleitor pedir voto em trânsito termina nesta quinta*. 2018. Disponível em: <https://g1.globo.com/politica/eleicoes/2018/noticia/2018/08/22/termina-nesta-quinta-feira-prazo-para-eleitor-pedir-voto-em-transito.ghtml>. 3

[10] NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 24 mar. 2019. 4, 11

[11] BACK, A. *Hashcash - a denial of service counter-measure*. 2002. Disponível em: <http://www.hashcash.org/papers/hashcash.pdf>. Acesso em: 24 mar. 2019. 5

[12] G. CARLYLE J., G. I. H. M. B. R. *Corda: An Introduction*. 2016. Disponível em: <https://docs.corda.net/$_s$*tatic/corda* − *introductory* − *whitepaper.pdf*¿.*Acessoem* : 24*mar*.2019. 8

[13] BISTARELLI, S. et al. An end-to-end voting-system based on bitcoin. In: *Proceedings of the Symposium on Applied Computing*. New York, NY, USA: ACM, 2017. (SAC '17), p. 1836–1841. ISBN 978-1-4503-4486-9. Disponível em: <http://doi.acm.org/10.1145/3019612.3019841>. 11

[14] Cooley, R.; Wolf, S.; Borowczak, M. Blockchain-based election infrastructures. In: *2018 IEEE International Smart Cities Conference (ISC2)*. [S.l.: s.n.], 2018. p. 1–4. 11

[15] ADIPUTRA, C. K.; HJORT, R.; SATO, H. A Proposal of Blockchain-Based Electronic Voting System. In: *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. [S.l.: s.n.], 2018. p. 22–27. 11

[16] SINGH, A.; CHATTERJEE, K. SecEVS : Secure Electronic Voting System Using Blockchain Technology. In: *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*. [S.l.: s.n.], 2018. p. 863–867. 11

[17] Shahzad, B.; Crowcroft, J. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, v. 7, p. 24477–24488, 2019. ISSN 2169-3536. 11

[18] WU, H.; YANG, C. A Blockchain-Based Network Security Mechanism for Voting Systems. In: *2018 1st International Cognitive Cities Conference (IC3)*. [S.l.: s.n.], 2018. p. 227–230. 11

[19] ZHANG, W. et al. A Privacy-Preserving Voting Protocol on Blockchain. In: *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. [S.l.: s.n.], 2018. p. 401–408. 11

[20] KHOURY, D. et al. Decentralized Voting Platform Based on Ethereum Blockchain. In: *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*. [S.l.: s.n.], 2018. p. 1–6. 11

[21] Yavuz, E. et al. Towards secure e-voting using ethereum blockchain. In: *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. [S.l.: s.n.], 2018. p. 1–7. 11

[22] ALENCAR M. F; SIMÕES, M. C. *Ethervoltz: um sistema de votação auditável baseado no blockchain ethereum*. Tese (Graduação em Engenharia da Computação) — ETEP Faculdades/Faculdade de tecnologia de São José Dos Campos, 2017. Disponível em: <http://www.inicepg.univap.br/cd/INIC$_2$017/*anais*/*arquivos*/$RE_0475_1017_03.pdf$¿. 11

[23] ANANDARAJ, S.; ANISH, R.; DEVAKUMAR, P. Secured electronic voting machine using biometric. In: *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. [s.n.], 2015. p. 1–5. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7192976&isnumber=7192777>. 11

[24] Grewal, G. S. et al. Du-vote: Remote electronic voting with untrusted computers. In: *2015 IEEE 28th Computer Security Foundations Symposium*. [s.n.], 2015. p. 155–169. ISSN 2377-5459. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7243731&isnumber=7243713>. 11

[25] BENALOH, J. Simple verifiable elections. In: *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*. Berkeley, CA, USA: USENIX Association, 2006. (EVT'06), p. 5–5. Disponível em: <http://dl.acm.org/citation.cfm?id=1251003.1251008>. 11

[26] Clarkson, M. R.; Chong, S.; Myers, A. C. Civitas: Toward a secure voting system. In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. [S.l.: s.n.], 2008. p. 354–368. ISSN 1081-6011. 11

[27] ADIDA, B. Helios: web-based open-audit voting. In: *In Proceedings of the 17th conference on Security symposium (SS'08). USENIX Association*. Berkeley, CA, USA: [s.n.], 2008. p. 335–348. 11

[28] GRAAF, J. V. d. O mito da urna. p. 86, 2017. Disponível em: <https://inscrypt.dcc.ufmg.br/wp-content/uploads/2017/11/o-mito-da-urna.pdf>. 11

[29] BARTOLUCCI, S.; BERNAT, P.; JOSEPH, D. SHARVOT: Secret SHARe-Based VOTing on the Blockchain. In: *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. [S.l.: s.n.], 2018. p. 30–34. 11

[30] ARAUJO, R.; FOULLE, S.; TRAORé, J. A practical and secure coercion-resistant scheme for remote elections. In: CHAUM, D. et al. (Ed.). *Frontiers of Electronic Voting*. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2008. (Dagstuhl Seminar Proceedings). Disponível em: <http://drops.dagstuhl.de/opus/volltexte/2008/1295>. 11

[31] RIVEST R.L; WACK, J. On the notion of "software independence" in voting systems. MIT, 2006. Disponível em: <https://people.csail.mit.edu/rivest/pubs/RW06.pdf>. 13

[32] FERNANDES, C. *Estudo e Avaliação Tecnológica dos Dados Oficiais da Eleição de Alagoas 2006 1o Turno*. 2006. 18,38-43 p. Disponível em: <http://www.brunazo.eng.br/voto-e/arquivos/AL06-laudoFerITA.zip>. Acesso em: 24 mar. 2019. 14