UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

LUIS FERNANDO MACHADO POZZOBON

SISTEMA DE VOTAÇÃO REMOTO BASEADO EM BLOCKCHAIN

DOIS VIZINHOS

2022

LUIS FERNANDO MACHADO POZZOBON

SISTEMA DE VOTAÇÃO REMOTO BASEADO EM BLOCKCHAIN

BLOCKCHAIN-BASED REMOTE VOTING SYSTEM

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia de Software do Curso de Bacharelado em Engenharia de Software da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Newton Carlos Will

DOIS VIZINHOS

2022

LUIS FERNANDO MACHADO POZZOBON

SISTEMA DE VOTAÇÃO REMOTO BASEADO EM BLOCKCHAIN

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia de Software do Curso de Bacharelado em Engenharia de Software da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 23/junho/2022

Newton Carlos Will
doutorado
Universidade Tecnológica Federal do Paraná

Marco Antonio Simões Teixeira
doutorado
Universidade Tecnológica Federal do Paraná

Marisangela Pacheco Brittes
doutorado
Universidade Tecnológica Federal do Paraná

DOIS VIZINHOS
2022

Dedico este trabalho especialmente à minha avó, por tudo que fez por mim, pois sem ela, eu nunca teria chegado até aqui.

AGRADECIMENTOS

Agradeço a minha família, mãe, pai e especialmente a minha avó Zenilda, que me deram condições, força e esperança para chegar até esta etapa da minha vida sem vocês nada disso seria possível. Agradeço ao Prof. Me. Rodrigo Tomaz Pagno e Prof. Dr. Newton Carlos Will pela orientação, confiança e compreensão na elaboração deste trabalho. Agradeço a coordenação do curso de Bacharelado em Engenharia de Software e a todos os professores que participaram da minha formação, que me guiou até aqui. Agradeço a todos os meus amigos e colegas que me auxiliaram e estiveram ao meu lado durante essa jornada, e a todos os que influenciaram direta ou indiretamente na minha formação, a todos vocês, meu sincero agradecimento.

RESUMO

Juntamente com a evolução dos sistemas computacionais utilizados por usuários e organizações, cresce também a quantidade de dados confidenciais a serem armazenados e o número de ameaças sobre eles. Nesse cenário, a Intel lançou no final de 2015, juntamente com sua linha de processadores de 6a geração (Skylake), a tecnologia Software Guard Extensions (Intel SGX), a qual fornece mecanismos de segurança para a execução de códigos dentro de uma área protegida no software, chamada de enclave, permitindo aos desenvolvedores que realizem a integração da mesma com seus sistemas. Dentre os mecanismos fornecidos, a tecnologia provê o recurso para selagem dos dados que estão no enclave, permitindo que sejam armazenados de forma segura, utilizando-se de uma chave de criptografia única, gerada e mantida pelo processador a partir das informações deste e do enclave. No entanto, garantir a segurança sobre os dados de todos os sistemas computacionais é um processo complexo. O presente trabalho faz uso do recurso de selagem de dados provido pela tecnologia Intel SGX para a criptografia de arquivos, criando assim um sistema de arquivos virtual onde aplicações possam armazenar seus dados e os mesmos possuam as garantias de segurança fornecidas pela tecnologia Intel SGX, de modo que, se a mídia de armazenamento for comprometida, os dados estarão seguros. Para validação da proposta, é feita a integração do software Cryptomator com um enclave para a selagem de dados. Os resultados demonstram que a solução é factível, tanto no quesito de desempenho quanto em segurança, podendo ser expandida e refinada para uso prático.

Palavras-chave: selagem de dados; criptografia de arquivos; confidencialidade; integridade; secure storage.

ABSTRACT

As computer systems used by individuals and organizations evolve, the amount of confidential data to be stored and the number of threats against them also increase. In this scenario, Intel launched in late 2015, along with its 6th generation processor line (Skylake), the Software Guard Extensions (Intel SGX) technology, which provides security mechanisms for executing code within a protected area in the software, called an enclave, allowing developers to integrate it with their systems. Among the provided mechanisms, the technology offers the feature of sealing data within the enclave, allowing them to be securely stored using a unique encryption key generated and maintained by the processor based on its information and that of the enclave. However, ensuring the security of data across all computer systems is a complex process. This paper utilizes the data sealing feature provided by Intel SGX technology for file encryption, thus creating a virtual file system where applications can store their data, with the security guarantees provided by Intel SGX technology, so that if the storage media is compromised, the data remains secure. To validate the proposal, the Cryptomator software is integrated with an enclave for data sealing. The results demonstrate that the solution is feasible, both in terms of performance and security, and can be expanded and refined for practical use.

Keywords: data sealing; file encryption; confidentiality; integrity; milk.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O processo de eleição de cargos políticos onde os candidatos se elegem segundo o voto da maioria, é um dos sistemas mais antigos de votação na história. Todo esse processo é denominado Sistema de Votação, e é formado de acordo com as leis e regras de cada país que o utiliza, como diz Costa (2008).

Com o passar do tempo as formas de executar essas votações foram se aprimorando e nos dias atuais os Sistemas de Votação são divididos em duas classes, a primeira delas, o modo tradicional, conhecido por não ser automatizado e ter seus votos registrados em cédulas de papel, onde após a votação é realizado a contagem dessas cédulas.

Apesar desse sistema ter sido amplamente utilizado por diversos países segundo Democracy e Assistance (2015), possui diversos problemas como o tempo para a apuração dos votos, que pode levar até dias para ser finalizada, erros de preenchimento na cédula do voto, falta de segurança devido às urnas trazerem margem para fraudes e manipulação desses votos, entre outros.

Com a evolução da tecnologia, os Sistemas de Votação evoluíram para a segunda classe, o meio eletrônico, com o objetivo de corrigir as falhas originárias do sistema de votação tradicional (com uso de cédulas) (COSTA, 2008), tais como: reduzir o tempo de apuração dos votos drasticamente; eliminar a chance de erros de preenchimento no voto em cédulas de papel; facilitar a usabilidade e a inclusão de pessoas idosas e/ou com dificuldades em realizar o voto da forma tradicional.

Esses sistemas eletrônicos entraram em operação em diversos países, segundo Democracy e Assistance (2015) 23 utilizam sistemas eletrônicos para eleições a nível nacional, e 18 utilizam para eleições regionais, dentre esses países estão o Brasil, Canadá, França, Estados Unidos, Austrália e Argentina.

No Brasil os sistemas de voto eletrônico são considerados os mais eficientes em questão de velocidade de apuração e contagem dos votos segundo SENSUS (2010), sendo aprovado por 94,4% dos brasileiros, onde 97,1% dos participantes avaliaram como positiva a agilidade na apuração dos resultados do pleito, entre os quais, 57,4% classificaram como ótima e 39,7% como boa.

Apesar do sistema atual de votação brasileiro ser visto como de sucesso, há muitos elementos que podem ser melhorados, preservando os elementos positivos da urna eletrônica, como a segurança, rapidez, facilidade e anonimidade.

A migração do sistema de votação atual presencial para um sistema remoto traria benefícios como o de permitir que os votos sejam realizados pela internet, não sendo necessário o deslocamento até os locais de votação, opção de realizar auditorias e apuração dos votos automática, eliminando a necessidade de um terceiro envolvido fazer a contagem dos votos.

Com a evolução das tecnologias de segurança da informação, no decorrer dos anos, surgiram soluções interessantes sendo aplicadas em diversas áreas relacionadas, a blockchain

é uma dessas. Devido às tendências das criptomoedas nos últimos anos, o Bitcoin, na maioria das vezes, é o que as pessoas pensam quando se fala em blockchain. Apesar de ser uma moeda virtual já muito disseminada, e que foi um dos pontos iniciais da utilização de redes blockchain como afirma ULRICH (2014), é necessário que o foco seja distribuído entre os caminhos e aplicações que essa tecnologia tem a oferecer.

Segundo Niwa (2019), 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 armazenado, onde a última informação sempre será a mais atual e levará em conta todo o histórico armazenado.

Este projeto traz como uma proposta, um sistema de votação totalmente remoto baseado nessa tecnologia, que utiliza de uma rede P2P descentralizada, onde, segundo Campos (2020), cada nó (computador) da rede tem o papel de cliente e servidor, armazenando os dados da rede em formato de um livro-razão público. Dessa maneira, são formados por blocos de informação conectados entre si através de hashes gerados a partir de vários critérios, como o próprio conteúdo do bloco, com o intuito de manter a integridade e solidez das informações.

Esses hashes servem para manter uma ligação válida entre os blocos, como uma certa forma de autenticação, pois quando algum bloco é alterado, seu hash muda e se torna diferente do que foi gravado nos blocos vizinhos onde estava sendo referenciado, se tornando assim inválido (CAMPOS, 2020). Este é um dos principais pontos positivos que essa tecnologia oferece, o que a torna muito útil em diversas aplicações relacionadas a transações e transferências seguras que necessitam disso para preservar a integridade das informações.

1.1 Justificativa

O sistema atual brasileiro de votação é considerado bem sucedido, afinal fazemos uso dele nos dias atuais, porém há muitos aspectos que podem ser melhorados utilizando blockchain a fim de criar um processo de eleição mais seguro, confiável e prático, seja ele qual for.

Atualmente os dados das eleições são criptografados e armazenados em mídias de resultados (Pendrives) que são encaminhados ao local próprio para transmissão à zona eleitoral ou ao Tribunal Regional Eleitoral (TRE) para a contagem dos votos (TSE, 2020d), com exceção algumas localidades de difícil acesso, como aldeias indígenas e certas comunidades ribeirinhas, onde a transmissão é feita via satélite para o respectivo Tribunal ou zona (TSE, 2020c).

Um ponto importante a ser considerado nesse processo é a segurança e a confiabilidade do resultado de uma eleição. Por normalmente terem seus dados armazenados em uma base de dados centralizada, ou seja, toda a informação coletada nas eleições fica armazenada nessas mídias de resultado.

Utilizando de exemplo as eleições brasileiras, que têm seus dados divididos entre as zonas eleitorais, ficando vulneráveis a ataques físicos e/ou digitais, independente da estrutura de segurança da urna eletrônica ou do local de armazenamento, lembrando que não é possível

encontrar o voto de uma zona eleitoral armazenado nos dados de outra (TSE, 2020d), e isso pode fazer com que caso ocorra algum tipo de violação e/ou adulteração, seja improvável recuperar os dados reais, pois há somente um local onde estas informações estão armazenadas, e nestes casos, este local não é mais de confiança.

Utilizando um banco de dados distribuídos, estas informações se encontrariam em vários locais distintos em forma de cópia de segurança, onde poderiam ser realizadas auditorias, comparando o resultado principal, com as cópias de segurança armazenadas nestes bancos de dados, vale ressaltar que o local onde estes bancos de dados se encontram não necessita ser de conhecimento dos envolvidos.

Porém, apenas utilizando uma base de dados descentralizada, não resolveria outros problemas de segurança como ataques diretos às informações armazenadas. Não há importância em armazenar os dados de forma distribuída como cópias de segurança, se este dado pode ser adulterado nestas bases de dados através de algum tipo de ataque, é então que entra a oportunidade de utilizar uma forma de votação como transações na rede blockchain para assegurar que os dados trafegando sejam imutáveis e transparentes.

Qualquer nó da rede consegue ter acesso aos dados e transações realizadas, que no caso desta proposta, seria o voto, e esta informação por estar interligada através de referências as informações anteriores (blocos, como são chamados na rede blockchain), isto os torna imutáveis, pois os próprios nós na rede impossibilitam que qualquer bloco seja alterado sem que todos os outros nós validem e autorizem esta alteração.

Por se tratar de um algoritmo, a possibilidade de erro na contagem dos votos também pode ser descartada, sendo esta causada pela perda de informações no processo, ou por erro humano ao interagir com o sistema, pois após a eleição, o próprio sistema realizaria a contagem automaticamente e disponibilizaria o resultado total ao término do horário de votação, para qualquer um visualizar.

Outro questionamentos ao sugerir uma votação remota é como será feita a identificação/autenticação do eleitor na hora do voto para evitar fraudes que possam ser realizadas sem esta etapa. Uma forma poderia ser utilizar o processo que o TSE (2020d) utiliza atualmente nas eleições do Brasil através da identificação biométrica (digital), reconhecimento facial e por voz, com auxílio de uma senha escolhida pelo eleitor na hora de seu cadastro.

Ao analisar os dados informados pelo TSE (2020b), onde nas eleições de 2018, estavam aptos a votar 87.363.098 eleitores por meio da identificação biométrica, (59,31% do eleitorado total de 147.306.275) em 2.793 municípios (48,65% do total, de 5.570), vemos que é possível aplicar estas formas de autenticação.

Outro ponto importante que pode ser discutido é a diminuição de custos que uma possível votação eletrônica remota pode ocasionar. Para comparação, somente em uma licitação de 180.000 urnas eletrônicas feita para “substituir parte de seu parque tecnológico, que atualmente é de 470 mil unidades em todo o país, excluídas as de 2006 e 2008. Os modelos 2006 e 2008, que somam 83 mil equipamentos, fazem parte dos que serão substituídos pelo modelo

UE 2020"(TSE, 2020a), foram gastos cerca de R$ 800.000.000, esse valor aumenta muito se aplicado a todas as unidades já adquiridas, excluindo outros custos envolvidos nesse processo da votação, podemos comparar com os custos previstos com a implementação desse sistema de voto remoto.

Esses são alguns motivos que reforçam a importância da criação desta proposta, para que votações totalmente remotas possam se tornar realidade, trazendo esses diversos benefícios e servindo como exemplo para o desenvolvimento de outros projetos em outras áreas utilizando *blockchain*.

1.2 Objetivo Geral

Propor um sistema de votação eletrônico remoto baseado em *Blockchain* para, possivelmente, ser utilizado em qualquer processo de votação que exige confiabilidade na apuração dos votos, e assegure a autenticidade e privacidade do eleitor e a integridade da votação.

1.3 Objetivos Específicos

- Melhorar a confiabilidade, segurança dos resultados e informações no processo de votação remoto utilizando a rede blockchain Ethereum como peça principal;
- Assegurar a anonimidade do eleitor através da utilização das chaves pública/privadas da própria rede Ethereum;
- Minimizar o impacto da coerção e compra de votos no processo eleitoral permitindo que o eleitor altere seu voto;
- Propor soluções para diminuir o impacto da transparência dos votos antes da eleição ser encerrada, causada também pela possibilidade do eleitor alterar seu voto;
- Propor funcionalidades de gerenciamento e auditorias de maneira transparente e que se encaixem nos critérios anteriormente elencados;
- Disponibilizar uma opção de sistema de votação eletrônico baseado em blockchain que poderá ser utilizado em qualquer processo de votação;
- Trazer mais facilidade, economia de tempo e comodidade para o eleitor, eliminando a necessidade de deslocamento até o local para realizar a votação;
- Documentar o processo de concepção da proposta e do projeto, registrando as vantagens, problemas e desafios a fim de disponibilizar esse conteúdo para futuras implementações nessa ou em diversas outras áreas que utilizem a tecnologia blockchain.

2 ASPECTOS CONCEITUAIS

2.1 BLOCKCHAIN

2.1.1 Origem

Após o surgimento do *Bitcoin* em 2008, criado segundo ULRICH (2014), por um programador conhecido como Satoshi Nakamoto, realizar transações pela internet se tornou possível sem o intermédio de empresas terceiras como o PayPal, pois havia um problema que até então não fora resolvido, o "gasto duplo" que poderia ocorrer em transações de criptomoedas sem o intermédio de terceiros.

Este "gasto duplo" acontece quando uma transação é realizada e os outros usuários desse sistema não são informados que esta moeda ou unidade monetária já foi utilizada, podendo assim ser gasta novamente em uma nova transação para outro usuário sem nenhum tipo de restrição.

A única forma de resolver este problema até então, era um membro terceiro armazenar registros de todo o histórico de transações dos usuários, podendo assim validar essas transações através destes registros e realizar o intermédio recebendo as transações de uma pessoa, e enviando à outra.

O *Bitcoin* conseguiu solucionar esse problema eliminando o terceiro membro envolvido utilizando uma espécie de Livro Razão público e distribuído formado por blocos, hoje conhecido como *blockchain*, que ocupa este lugar automaticamente ao deixar todas as transações registradas em todos os nós conectados na rede P2P, tornando praticamente impossível para um possível hacker tomar controle da parte majoritária dos nós, impedindo assim que ataques fraudulentos aconteçam (SATOSHI, 2008).

Desde então essa tecnologia vem sendo utilizada e disseminada em diversas outras criptomoedas como Ethereum, Tether, XRP e Litecoin, que segundo a cotação das criptomoedas (BITCOIN, 2020) hoje estão entre as 10 com o maior valor de mercado. Porém várias outras utilidades estão sendo descobertas, discutidas e implementadas utilizando redes em formato blockchain, uma delas, a votação eletrônica.

2.1.2 Arquitetura

Segundo Greve *et al.* (2018) o funcionamento do blockchain é fundamentado por sete propriedades, que contribuem para o desenvolvimento de novas aplicações. São elas:

1. Descentralização: A aplicação é executada de forma distribuída através do estabelecimento de confiança entre as partes, sem a necessidade de uma entidade intermediária confiável. Ambas as partes trabalham como clientes e servidores, transformando essa

comunicação e replicação de estado em uma rede peer to peer (P2P). Esse é o principal motivador para o crescente interesse na blockchain e suas aplicações.

2. Disponibilidade e Integridade: Todo o conjunto de dados e transações são replicados em diferentes nós de maneira segura, criando uma espécie de livro razão distribuído, de forma a manter o sistema e os dados sempre disponíveis e consistentes.

3. Transparência e Auditabilidade: Todas as transações registradas no livro razão são públicas, podendo ser verificadas e auditadas por qualquer nó da rede. Além disso, os códigos da tecnologia costumam ser abertos e passíveis de verificação.

4. Imutabilidade e Irrefutabilidade: As transações registradas no livro razão são imutáveis. Uma vez registradas não podem ser refutadas nem alteradas. Atualizações são possíveis a partir da geração de novas transações e realização de um novo consenso.

5. Privacidade: É possível oferecer privacidade aos usuários sem que os terceiros envolvidos tenham acesso e controle dos seus dados. Na tecnologia, cada usuário gerencia suas próprias chaves e cada nó servidor armazena apenas fragmentos criptografados de dados do usuário. Transações são até certo ponto anônimas, com base no endereço dos envolvidos na *blockchain*.

6. Desintermediação: A blockchain possibilita a integração entre diversos sistemas de forma direta e eficiente. Assim, é considerada um conector de sistemas complexos (sistemas de sistemas), permitindo a eliminação de intermediários de maneira a simplificar o projeto dos sistemas e processos.

7. Cooperação e Incentivos: Oferta de modelo denegócios à base de incentivos, à luz da teoria dos jogos. O consenso sob demanda passa a ser oferecido como serviço em diversos níveis e escopos.

Para atingir estas propriedades, uma rede em blockchain precisa ser fortemente baseada em 3 elementos essenciais, a Criptografia, o Consenso e o Livro Razão, cada um destes elementos tem um papel muito importante para o funcionamento como um todo da rede, a seguir veremos como cada um deles funciona.

2.1.2.1 Criptografia

Por se tratar de uma tecnologia de segurança de informações, redes em blockchain são fortemente baseadas em criptografia. Dentre as tecnologias criptográficas mais utilizadas estão o resumo criptográfico(funções hash) e as assinaturas digitais.

Segundo Schmitt (2001) a criptografia tem como principais objetivos a confidencialidade e autenticação através da transformação de uma informação em algo cifrado e ininteligível. Ainda diz que a criptografia é separada em dois tipos, simétrica e assimétrica.

Na criptografia simétrica segundo Schmitt (2001) a mesma chave criptografa e descriptografa a informação, acarretando no problema de compartilhamento de chaves, onde apenas a própria pessoa poderá ter realizar essas operações sem que a segurança e anonimidade dos dados sejam violadas.

Já na criptografia assimétrica, Schmitt (2001) diz que é formada por duas chaves, a chave pública e a privada, onde é possível gerar a chave pública através da privada, mas não é possível gerar a privada a partir da pública, onde a informação criptografada por uma é descriptografada pela outra, resolvendo assim o problema da criptografia assimétrica, e permitindo que a chave pública seja compartilhada sem que a chave privada e a segurança/privacidade do seu dono seja exposta.

- **Função hash:**

Segundo Greve *et al.* (2018) as funções hash são unidirecionais, ou seja, raramente permitem a recuperação da informação original a partir de um hash gerado a partir dela. E que para estas funções sejam eficientes, devem satisfazer os seguintes requisitos: (1) resistência à colisão, onde seja praticamente impossível encontrar dois valores x e y, dado que x <> y e hash(x) = hash(y).

Em outras palavras uma função hash é resistente a colisão quando dois valores diferentes quase nunca darão resultado ao mesmo hash passando pela mesma função criptográfica, e (2) ocultação, onde dado um valor x que possui um universo de possibilidades muito pequeno, esta função hash se torna responsável de utilizar um valor bem aleatório n, e gerar o hash(n || x), que implica na concatenação (||) do valor aleatório n com o valor de x, tornando assim inviável descobrir o valor de x mesmo fazendo parte de um conjunto pequeno de possibilidades.

Ao satisfazer essas duas propriedades então é possível hashes representarem um resumo confiável de informações quaisquer, ocupando um espaço fixo em memória muito menor que uma cópia na íntegra dessas informações.

- **Chaves:**

Além da segurança, uma rede blockchain também oferece a anonimidade através da utilização de chaves público/privadas criptografadas, onde segundo Bashir (2017) a chave pública pode ser revelada e utilizada por qualquer um que queira enviar ou receber transações na blockchain e a chave privada é utilizada para autenticar e validar essas transações, sendo assim de suma importância ser de conhecimento apenas de seu proprietário.

Uma rede em *blockchain* costuma usar essas chaves para validar as transações de forma inteligente, onde a chave pública é utilizada como uma espécie de endereço, e a chave privada é tratada como uma senha. Supomos que uma pessoa A utilizando a rede do *Bitcoin*, decide transferir 10 unidades monetárias para a pessoa B, ela precisará da chave pública da pessoa B, e da sua própria chave privada para "assinar" a transação, garantindo assim a autenticidade da mesma já que a chave privada é de conhecimento apenas de seu proprietário.

O mesmo vale para que uma transação tenha identificação da pessoa que a emitiu, pois a chave pública desse usuário é gravada para que sirva como uma forma de verificação e localização das transações feitas por ele. Após um remetente realizar uma transferência, a transação é armazenada como um bloco na rede *blockchain*, com a data e hora da transação, além das informações transferidas, ficando assim disponível para ser consultada por qualquer pessoa sem que sua identidade seja exposta.

- **Assinaturas digitais:**

Assinaturas digitais devem servir ao mesmo propósito de uma assinatura manual, como as feitas nos documentos e registradas em cartórios, dessa forma somente você pode assinar algo, mas qualquer um pode verificar a sua autenticidade.

Como diz Greve *et al.* (2018) e Schmitt (2001) as assinaturas digitais são implementadas através de criptografia de chave assimétrica, formada por um par de chaves, a pública *(pk)*, e a privada/secreta *(sk)*, que como dito anteriormente é usada para assinar as transações. Este par de chaves é implementado através de 3 algoritmos:

1. *generateKeys(keysize)* que recebe um key size e retorna um par de chaves pública/privada (pk,sk);

2. *sign(sk,msg)* que recebe uma chave secreta (sk) e uma mensagem (msg) e retorna a assinatura (sig) da mensagem;

3. *verify(pk,msg,sig)* que recebe uma chave pública pk, uma mensagem msg e uma assinatura sig, e retorna um valor booleano true se sig for válida, e false caso a assinatura seja inválida.

Para uma assinatura digital ser válida, ela deve possuir 2 propriedades:

1. Autenticidade: Dado o método verify (pk,msg,sign(sk,msg))comum apk e sk válidas,o retorno deve ser igual a true, caso contrário false;

2. Ser Infalsificável: A assinatura não pode ser forjada.

A autenticidade garante a autoria de uma mensagem através da assinatura, que poderá ser verificada posteriormente. E como essa assinatura é infalsificável, qualquer alteração no documento a torna inválida, preservando assim a integridade do mesmo. Além disso garante o não repúdio, onde o emissor não pode negar a assinatura depois de feita.

Como apresentado na função hash, utilizar a mensagem na íntegra não é uma opção prática quando se trata da autenticação e validação da mesma, pois a mensagem pode ser muito grande de acordo com seu conteúdo, tornando assim uma boa prática utilizar o resumo criptográfico hash(msg) de uma mensagem para identificá-la e realizar a verificação através da função sign(sk,hash(msg)), já que o retorno de hash(msg) sempre retorna um valor fixo de bits, essas

funções criptográficas são resistentes a colisão. O resumo criptográfico da chave pública (pk) também é utilizado como endereço na blockchain, a fim de identificar as transações.

2.1.2.2 Livro Razão

Como diz Greve *et al.* (2018) o livro razão (*ledger*) da *blockchain* é a estrutura que armazena todas as transações realizadas de forma distribuída e imutável, onde todas as novas transações são registradas e replicadas para todos os outros nós da rede P2P.

Essas transações são separadas e armazenadas em espécies de blocos de informação, encadeados através de um apontador criptografado, ou *hash pointer*, que serve como um ponteiro para os outros blocos encadeados.

Este *hash pointer* serve como um ponteiro para onde está armazenado um certo dado d e seu resumo criptográfico H(d). Assim além de permitir a recuperação desse dado d, um *hash pointer* permite sua verificação através da função H(d) vista anteriormente. Esses hashes podem ser usados para criar qualquer tipo de estrutura de dados com encadeamento, como listas, árvores e grafos. Essas transações precisam obedecer aos princípios ACID dos banco de dados.

Segundo Date (2004), as propriedades ACID (Atomicidade, Consistência, Isolamento e Durabilidade) são definidas da seguinte forma:

1. Atomicidade (*Atomicity*): Refere-se às transações aplicadas da forma "tudo ou nada", ou seja, que se qualquer parte de uma transação falhar, toda a transação é considerada como uma falha e o banco de dados é retornado ao estado em que estava antes do início da transação. Esse retorno ao estado original é conhecido como *rollback* (reversão). Por outro lado, se a transação concluída com êxito, o banco de dados é permanentemente atualizado - um processo conhecido como *commit*(persistência da informação).

2. Consistência/Correção (*Consistency*): Significa que os dados gravados devem ser válidos de acordo com as regras definidas. Caso não sejam, acontece um *rollback* da transação.

3. Isolamento (*Isolation*): Garante que as transações sendo executadas em paralelo resultem em um estado final idêntico ao que seria alcançado se as transações fossem executadas em série. Importante em sistemas que realizam transações concorrentes.

4. Durabilidade (*Durability*): Garante que uma transação, uma vez persistida (*committed*), permanecerá neste estado mesmo que haja um problema grave no sistema.

- **Transação:**

Segundo Greve *et al.* (2018) uma transação é basicamente uma sequência de operações sobre estados, e incorpora uma transferência de ativos,ou um contrato inteligente. Normalmente

um ativo representa uma unidade monetária qualquer, mas pode ser qualquer coisa possível de representar digitalmente, como um voto, um livro, um filme, etc.

Em um caso básico, uma transferência de ativos envolve a assinatura digital do remetente, o endereço do destinatário, e as entradas/saídas do ativo representado. Para validar uma transação, é necessário 4 passos básicos:

1. Verificar se a assinatura digital do remetente é válida;
2. Verificar se o endereço do destinatário é válido;
3. Verificar a existência do ativo sendo transacionado, ou seja verificar se é algo que o remetente obteve nas transações anteriores;
4. Verificar se o ativo em transação não foi gasto anteriormente pelo remetente.

Outras medidas de verificação e validação podem ser tomadas, dependendo do objetivo e estrutura de cada aplicação. Como as transações são validadas individualmente por cada nó da *blockchain*, o processo se torna mais simples e descentralizado. Quando se trata de um contrato inteligente, há diversas possibilidades, já que o mesmo pode ser responsável por n funcionalidades além da transferência de um ativo.

- **Bloco:**

Como dito anteriormente, um bloco é onde as informações necessárias de cada transação são armazenadas, e é composto por um cabeçalho (*header*) e o corpo (*body*). Há diversos modelos e estruturas recomendadas para esses blocos, nesta seção será apresentado um modelo básico, com intuito de ilustrar o funcionamento e relacionamento dos blocos na rede *blockchain*.

No cabeçalho do bloco, normalmente são armazenadas as informações do relacionadas ao próprio bloco, como o seu hash, índice (*index*), hash do bloco anterior (*previousHash*), data e hora de sua criação (*timestamp*) e o número aleatório de dificuldade (*nounce*). Já no corpo do bloco, são armazenadas as transações realizadas naquele bloco. A Figura 1 ilustra a estrutura básica de um bloco.

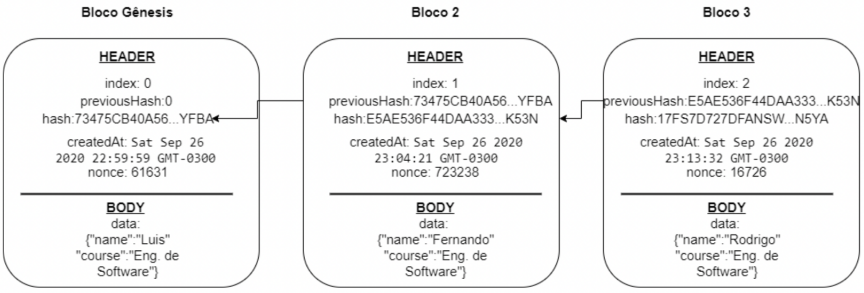
O conjunto de blocos forma o livro-razão ou blockchain conforme a Figura 2 ilustra, que fica armazenada em um nó que deseja fazer a validação das transações armazenadas nesses blocos através dos protocolos de consenso.

A Figura 2 ilustra como os blocos estão interligados através de seus *hashes*, cada bloco possui a propriedade previousHash que faz referência a propriedade hash do bloco anterior, formando assim uma cadeia de blocos interligados, que como citado anteriormente, utilizam resumos criptográficos para formar seus identificadores, fazendo com que caso um bloco, como o segundo da Figura 2 seja alterado, sofra um ataque ou algo do gênero, tenha sua propriedade hash alterada, perdendo a ligação com todos os outros blocos na sequência, e assim se tornando inválido perante os mesmos.

Figura 1 – Estrutura básica de um bloco

Fonte: Autoria própria.

Figura 2 – Estrutura básica de um bloccckchain



Fonte: Autoria própria.

2.1.2.3 Consenso

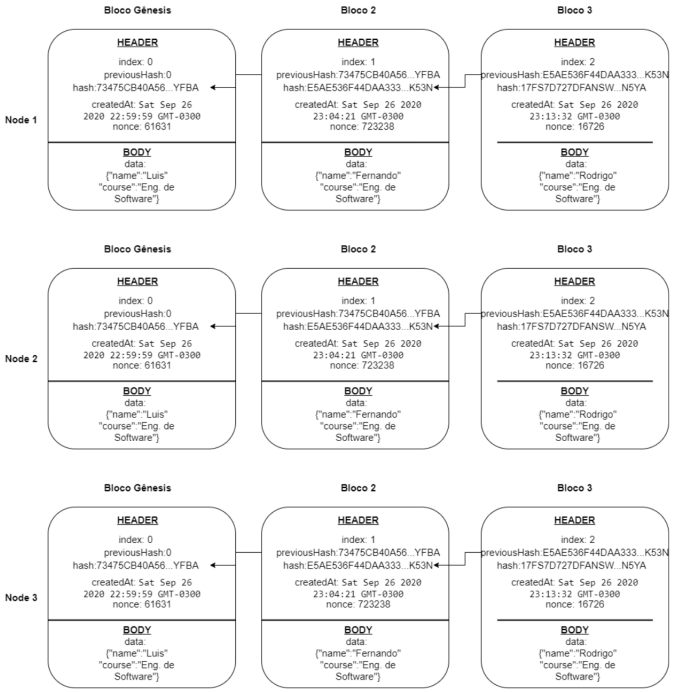
O Consenso é uma solução confiável quando se trata de aplicações distribuídas, pois mesmo em um sistema passível de falhas, os participantes utilizam de um consenso para escolher decisões em comum com o intuito de preservar a consistência e progresso do estado da aplicação. Protocolos de consenso são utilizados na blockchain para entrar em acordo sobre qual o próximo bloco a ser adicionado na estrutura (CARVALHO; ÁVILA, 2019).

Antes de conhecer esses protocolos de consenso e suas características, é importante saber que segundo Carvalho e Ávila (2019) existem tipos diferentes de estrutura de uma rede blockchain, as duas principais são a pública e a privada.

- **Blockchain Pública (sem permissão):**

Em uma rede *blockchain* pública, como ilustra a Figura 3, os nós P2P são desconhecidos e podem entrar e sair da rede a qualquer momento, normalmente não necessitam de identificação, sendo assim anônimos, podendo englobar usuários do mundo inteiro sem controle dos participantes (GREVE *et al.*, 2018).

Figura 3 – Estrutura básica de uma rede distribuída de blockchains



Fonte: Autoria própria.

Unindo com todas as características de uma *blockchain*, podemos criar uma rede distribuída armazenando cópias de cada um desses livros-razão em cada um desses nós participantes, fazendo com que em casos de ataques onde mesmo com as propriedades de segurança já citados, consigam alterar a propriedade dos blocos de um nó, (representado como os Nodes 1, 2 e 3 na Figura 3) haverá vários outros nós com a informação original dessa blockchain que sofreu o ataque e foi adulterada, e utilizando os protocolos de consenso, somente as blockchains que são aceitas pela maioria dos outros nós são propagadas para os outros nós.

Uma rede blockchain sofreria um ataque real somente se 50% + 1 de seus nós fossem adulterados, fazendo assim com que a maioria dos nós possuíssem a mesma informação, que a partir desse momento seriam considerados os nós, blockchains e blocos válidos.

Segundo (CARVALHO; ÁVILA, 2019) esse tipo de blockchain costuma utilizar protocolos de consenso como *Proof of Work* (Prova de Trabalho) para validar as transações, por mais que atualmente outros protocolos venham tomando força como *Proof of Stake* (Prova de Participação).

Como diz seu próprios criadores Satoshi (2008) e Greve *et al.* (2018), o consenso do Bitcoin baseado em *Proof of Work* ordena as requisições de transações enviadas por todos os nós da rede distribuída e agrupa as transações em blocos com o objetivo de eleger uma espécie de líder ou responsável através de um oráculo randômico (gerador de números randômicos), responsável por gerenciar o consenso daquelas requisições de transação agrupadas.

Para se eleger um nó precisa realizar uma prova de trabalho (*Proof of Work*), ao resolver um enigma criptográfico muito complexo que exige muito poder computacional. Todo esse processo é conhecido como mineração e os nós (computadores) que a realizam mineradores.

O nó que ganhará o direito de gerenciar o consenso será o que conseguir resolver o enigma criptográfico primeiro, propagando o seu bloco para a rede. Esse bloco somente será aceito pelos outros nós da rede caso seja válido.

Como todo esse processo custa um processamento e poder computacional alto, o próprio Satoshi (2008) propôs o incentivo, recompensando os nós que vencem o processo e propaga o seu bloco pela rede neste caso, com uma certa quantidade de *Bitcoins*.

- **Blockchain Privada (com permissão):**

Em uma blockchain privada, Carvalho e Ávila (2019) dizem que por se tratar de redes controladas, não há necessidade de um protocolo de consenso, já que as operações serão validadas pelos próprios administradores.

Porém Greve *et al.* (2018) diz que protocolos podem ser adaptados e utilizados em uma rede blockchain, e os incentivos podem ou não serem utilizados de acordo com as necessidades dos administradores, afinal a própria organização poderá desenvolver seu programa de incentivo.

O ponto forte de redes blockchain permissionadas que utilizam protocolos adaptados, é o tempo de latência da validação dos blocos, que se dá quase em tempo real, propriedade que as redes públicas não podem utilizar por não ter conhecimento e/ou controle dos envolvidos.

3 TRABALHOS RELACIONADOS

Para melhor compreensão e entendimento do problema, uma pesquisa foi realizada para encontrar trabalhos relacionados em busca da experiência repassada, problemas e possíveis soluções, para então a partir destes aprimorar esta proposta utilizando os resultados obtidos.

A pesquisa foi feita utilizando 2 das plataformas de busca de artigos e livros disponíveis na internet, sendo eles: *Google Scholar* e *IEEE Xplore*. O Quadro 1, mostra de forma analítica as principais informações dos trabalhos encontrados.

Quadro 1 – Principais informações dos trabalhos relacionados encontrados

Título	Local de publicação	Autor(a)(es)	Ano
blockchain e a Revolução do Consenso sob Demanda	Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)	Fabíola Greve, Leobino Sampaio, Jauberth Abijaude, Antonio Coutinho, Ítalo Valcy, Sílvio Queiroz	2018
Um sistema de voto eletrônico baseado em *blockchain*	XIX Simpósio de Pesquisa Operacional & Logística da Marinh	Henrique Niwa	2019
Uma nova abordagem sobre votação eletrônica	Monografia de Especialização em Redes de Computadores e Teleinformática - UTFPR	Marshall Moshe Mauricio do Nascimento	2018
A segurança da democracia e a *blockchain*a	Revista Estudos Eleitorais, Brasília	Matheus Passos Silva	2019

Fonte: Autoria própria.

O estudo de Greve *et al.* (2018) aborda de forma abrangida a estrutura, funcionamento e utilização da tecnologia *blockchain*, apresenta os pontos positivos e negativos da tecnologia, além de possíveis utilizações para a mesma.

Já o trabalho de Niwa (2019) contempla a proposta e o desenvolvimento de um sistema de voto eletrônico baseado no algoritmo do Bitcoin para criar um sistema descentralizado que possua a funcionalidade de suportar eleições e votações utilizando do mesmo método de geração de Bitcoins e recompensas que o algoritmo original possui, alegando que desde sua criação o algoritmo nunca passou por problemas graves de segurança. Niwa (2019) cita a criptografia de chave pública/privada para assegurar a anonimidade dos eleitores, onde privacidade de voto na auditoria é garantida pelo uso de chave pública identificando seu voto, assegurando que apenas quem distribuiu o voto sabe a relação entre chave pública e identidade.

Partindo desta premissa, nem mesmo o eleitor pode ter conhecimento de seu par de chaves pública/privada, caso tenha, abre margem para o problema já abordado anteriormente de coerção por parte dos candidatos e/ou interessados. Porém esse problema ainda persiste caso o eleitor não possa de alguma forma alterar seu voto, caso seja persuadido por outras pessoas.

Ainda neste mesmo trabalho, Niwa (2019) corrobora com o problema citado anteriormente da divulgação em tempo real dos votos alterar o resultado da eleição, porém não propõe ou implementa uma solução. Essa abordagem satisfaz o modelo proposto para o projeto de Niwa (2019) porém, não é totalmente aplicável levando em consideração os aspectos de anonimidade e de interesse público abordados anteriormente.

O artigo de Nascimento (2018) assim como o de Greve *et al.* (2018) aborda de forma geral o funcionamento de um rede em *blockchain*, porém se aprofunda na questão da votação eletrônica, levantando pontos e justificativas para sua futura utilização. Greve *et al.* (2018) cita além do voto eletrônico, muitas outras aplicações da *blockchain*, se aprofunda na tecnologia e estrutura da rede descentralizada e suas diversas formas de representações, mas não se aprofunda no tema abordado neste presente trabalho.

Nascimento (2018) também conclui que a partir de seus estudos, um sistema com esse intuito poderia substituir de forma efetiva ou complementar o sistema atual de votação, ressaltando os aspectos de segurança e os benefícios que o sistema poderia disponibilizar aos eleitores. Apresenta como base, pontos congruentes com o trabalho de Niwa (2019), ressaltando os pontos positivos de se utilizar uma rede *blockchain* para voto eletrônico e sua possível solução para a Integridade, Solidez e Completude de uma eleição.

O trabalho de Nascimento (2018) levanta um problema interessante em relação a população que não possuiria condições financeiras de adquirir um aparelho celular ou computador para realizar a votação ou não ter uma conexão a internet além das pessoas que não possuem conhecimento suficiente para votar através desses aparelhos. Como solução, o autor propõe mesclar a votação presencial com a votação remota, que é uma ótima solução para essas pessoas que por algum motivo não consigam votar de forma remota. Por fim, Nascimento (2018) não explica de forma detalhada como esse processo seria feito, mas partindo da premissa de que as urnas eletrônicas consigam de alguma forma validar junto a rede *blockchain* os usuários que já votaram via outra urna eletrônica ou o sistema online, é possível mesclar as duas tecnologias com o intuito de facilitar o acesso para as pessoas que tenham as dificuldades citadas anteriormente.

O estudo de Silva (2019), aborda de forma mais analítica a questão da utilização de *blockchain* nos processos eleitorais, mais especificamente a questão da democracia brasileira, apontando os pontos negativos do sistema atual.O autor propõe a utilização de um sistema baseado em *blockchain* para resolver alguns dos problemas apresentados e trazer outros benefícios através do voto remoto.

Os trabalhos citados acima possuem relação com este devido a natureza de suas pesquisas e objetivos, auxiliaram a elencar os pontos positivos e negativos de se utilizar *blockchain* em um processo eleitoral, além de ressaltar dificuldades que impedem que um sistema de votação remoto seja aplicado respeitando os critérios necessários para assegurar a lisura de um processo eleitoral.

É importante destacar alguns dos exemplos de eleições eletrônicas que já utilizaram a tecnologia *blockchain* em seus processos eleitorais. Em março de 2018 Serra Leoa realizou aquela que é considerada como a primeira eleição no mundo totalmente baseada em *blockchain* (BIGGS, 2018). Já em em maio de 2018 ocorreram nos Estados Unidos as primeiras eleições registradas em *blockchain* do país (JS, 2020).

Estas eleições são parecidas nos aspectos que foram implementadas, utilizando redes *blockchain* privadas com o objetivo principal de suportar a eleição e contabilizar os votos, ajudando a entender o funcionamento e impulsionando pesquisas e melhorias nessa área da tecnologia.

O presente trabalho propõe e implementa um sistema de votação remoto na rede *blockchain Ethereum*, conhecida pela criptomoeda com o mesmo nome. A rede *Ethereum* suporta a implementação de contratos inteligentes através da linguagem *Solidity*, que tornam possível a criação de regras pré estabelecidas através de um código que é executado automaticamente.

Tem como objetivo principal trazer mais facilidade na hora de realizar eleições e uma redução de custos juntamente do tempo necessário para a implementação. Busca também solucionar os problemas que votações online possuem através da natureza da tecnologia *blockchain*, e propor soluções que sanem os outros problemas gerados por um sistema de votação em ambiente não monitorado, como a anonimidade, coerção e influência dos resultados, utilizando como forma de auxílio, uma entidade moderadora que ficará responsável pela garantia desses pontos através do gerenciamento dos eleitores e candidatos.

4 DESENVOLVIMENTO E ARQUITETURA

Este capítulo apresenta a proposta de um sistema de votação remota baseado em blockchain considerando os aspectos do processo eleitoral brasileiro como base por seu reconhecimento e aceitação nacional, porém com intuito de ser utilizado para qualquer forma de votação. A seção 4.0.1 descreve a metodologia utilizada para escolher as ferramentas e softwares para o desenvolvimento. Já a seção 4.0.2 foca na concepção da proposta baseando-se em premissas do processo eleitoral brasileiro como citado anteriormente. A seção 4.0.3 descreve como foram as atividades passo a passo durante o desenvolvimento do presente trabalho, com um cronograma mensal.

4.0.1 Tecnologias

As tecnologias escolhidas para a concepção do sistema de votação, a priori se basearam nos seguintes critérios:

- **Baixa curva de aprendizado:** Como o objetivo do projeto é se tornar de código aberto, quanto mais simples e intuitivo a tecnologia seja, mais pessoas terão a capacidade de implementar suas ideias e melhorias ao projeto, sem tornar a complexidade um fator impeditivo para que isso aconteça.
- **Agilidade no desenvolvimento:** É desejável que as ferramentas e tecnologias utilizadas no processo sejam muito produtivas na questão de desenvolvimento das funcionalidades do projeto.
- **Baixo custo:** É necessário que não haja custos desnecessários para o desenvolvimento do projeto, afinal todos os recursos utilizados virão de origem própria.
- **Desempenho:** É importante que o software desenvolvido seja planejado e estruturado para ter o melhor desempenho possível, tanto do lado do cliente quanto do servidor.
- **Suporte** É desejável que as ferramentas, técnicas e tecnologias utilizadas no projeto tenham uma comunidade e/ou uma empresa comprometida com o suporte para os usuários.
- **Conteúdo:** É muito importante que haja uma grande disponibilidade de conteúdo na internet das ferramentas e tecnologias utilizadas para que soluções para possíveis problemas sejam fáceis de encontrar, e que tenha a disposição, padrões e métodos de desenvolvimento cada vez mais refinados pelos seus usuários.

A aplicação será dividida em 4 etapas, o backend, frontend, banco de dados e a rede blockchain, cada etapa será desenvolvida utilizando diferentes linguagens, bibliotecas, frameworks e ambientes citados abaixo:

4.0.1.1 *Blockchain*

Dentre as redes em blockchain pesquisadas, a Ethereum acaba satisfazendo a maioria dos critérios citados anteriormente, por se tratar de um conjunto entre a rede distribuída em blockchain, e um ambiente de desenvolvimento próprio chamado EVM (*Ethereum Virtual Machine*), acaba se tornando uma ótima opção para o desenvolvimento do contrato inteligente.

- ***Solidity***: Linguagem orientada a objetos, utilizada para desenvolver contratos inteligentes, podendo ser usada em qualquer rede blockchain, porém em sua grande maioria é utilizada para criar esses contratos inteligentes na Ethereum.
- ***Truffle***: Framework utilizado principalmente para testes e deploys dos contratos inteligentes.
- ***Ganache***: Uma rede blockchain pessoal para desenvolvimento baseado na rede Ethereum. Utilizado para implantar contratos, desenvolver aplicativos e executar testes.

4.0.1.2 Backend

O *backend* é comumente responsável pela comunicação e validação das informações da aplicação entre o usuário e o banco de dados, nesse caso será utilizado também para servir de ponte para a rede blockchain, será construído utilizando as seguintes tecnologias:

- ***TypeScript***: TypeScript é uma extensão do JavaScript, conhecida por adicionar a possibilidade de tipagem à linguagem e detectar erros durante o processo de desenvolvimento, não somente na execução da aplicação, para que o código escrito possa ser executado, o Typescript é compilado e gera um build em JavaScript, que pode ser interpretado por qualquer SO ou ferramenta que utilize JavaScript, como os navegadores (TYPESCRIPT, 2020).
- ***Node.js***: Também será utilizado Node.js, um framework JavaScript de desenvolvimento voltado para o lado servidor das aplicações(server-side), pode ser escrito em TypeScript e compilado para JavaScript, costuma ser utilizado pelo desempenho, alta disponibilidade de conteúdo como bibliotecas e frameworks JavaScript, e por unir o backend e o frontend em uma única linguagem, tornando-se uma ótima opção para o projeto (JS, 2020).
- ***Web3.js:*** Uma biblioteca também desenvolvida e disponibilizada em Javascript, utilizada para interagir diretamente com a rede blockchain da Ethereum e seu ecossistema baseado em contratos inteligentes (ETHERS, 2020).

4.0.1.3 Frontend

Junto do *backend* a escolha da linguagem para o frontend também será Typescript e JavaScript, agilizando o processo de desenvolvimento e facilitando a curva de aprendizado das bibliotecas e ferramentas que serão utilizadas, citadas a seguir:

- ***React Native:*** Um framework utilizado para desenvolver o aplicativos mobile, mantido pelo Facebook (REACT, 2020) e utilizado para desenvolvimento nativo entre Android e IOS, conta com alta disponibilidade de conteúdo na internet, apoio da comunidade e vários facilitadores para o desenvolvimento, além de ser disponível em JavaScript.

4.0.1.4 Banco de Dados

O banco de dados utilizado será o MongoDB Community Server, um banco de dados noSQL orientado a documentos, que possui versão gratuita para a comunidade (MONGODB, 2020), e um sistema de armazenamento em nuvem gratuito até 500MB, que acelera o desenvolvimento pois é rapidamente criado e disponibilizado pelo próprio sistema, e pode ser acessado de qualquer lugar através da URL de conexão.

4.0.1.5 Hardware

Um computador foi utilizado como servidor para o backend, frontend e o banco de dados, provindo de meios próprios e não contratado por terceiros, com as seguintes especificações:

- Processador: AMD Ryzen 5 3600, 12 Threads, 6 Cores;
- Placa de video: NVIDIA GeForce GTX 1660 SUPER ,6 GB VRam;
- Ram: Team Group T-Force Vulcan 8GB (2x8), DDR4, 2666MHz;
- Disco: HD TOSHIBA HDWD110, 1TB, SSD Sandisk, 256GB;
- Fonte: 500W

4.0.2 CONCEPÇÃO DA PROPOSTA

Com base no processo eleitoral brasileiro, é possível elencar 4 principais problemas que apenas considerando a natureza da tecnologia, faz com que se utilize uma rede blockchain e dos contratos inteligentes para realizar um processo de votação e contabilização dos votos, trate esses problemas que tornam o voto remoto hoje inviável. São eles:

1. Completude: Garantir que todos os votos válidos sejam contabilizados corretamente; Ao ser implementado com base em um código pré-estruturado que tem como objetivo o de realizar a contabilização de apenas votos válidos, utilizando como prerrogativa alguma condição específica, como um identificador do usuário e o seu tipo de voto (branco/nulo), a contagem sempre será válida.

2. Solidez: Votos inválidos devem ser fáceis de detectar e se descartar; Considerando que os eleitores teriam suas formas de autenticação (login e senha/biometria) feitas de forma controlada e monitorada pelo agente empregador da eleição, votos inválidos seriam contabilizados e desconsiderados pelo próprio algoritmo e outros usuários que não teriam direito ao voto, não conseguiriam influenciar no resultado da votação.

3. Elegibilidade: Apenas eleitores legítimos poderão participar na eleição; Considerando o mesmo aspecto citado anteriormente, esse ponto também seria garantido.

4. Integridade: O resultado da votação não deve sofrer nenhum tipo de violação e/ou adulteração, os candidatos e votos já salvos não podem ser alterados; Com base na natureza da rede blockchain, seus protocolos criptográficos, sua estrutura encadeada e a descentralização da base de dados, assegura que os dados uma vez computados se tornem imutáveis, podendo ser alterados somente através de novas transações autorizadas pelo próprio contrato inteligente.

Estes problemas são sanados com o desenvolvimento de dois contratos inteligentes na rede *Ethereum* utilizando a linguagem *Solidity*, um contrato que armazenará as informações da eleição e será chamado de *Election*, de forma geral e outro que armazenará e terá toda a regra de negócio para a realização das votações, que serão chamadas de *Ballots*.

O contrato *Election* terá a responsabilidade de fazer a implantação de diversas instâncias do contrato Ballot, uma para cada Distrito, de forma que separe os eleitores de cada um e armazenar os endereços destas Ballots para que seja possível acessar através do aplicativo.

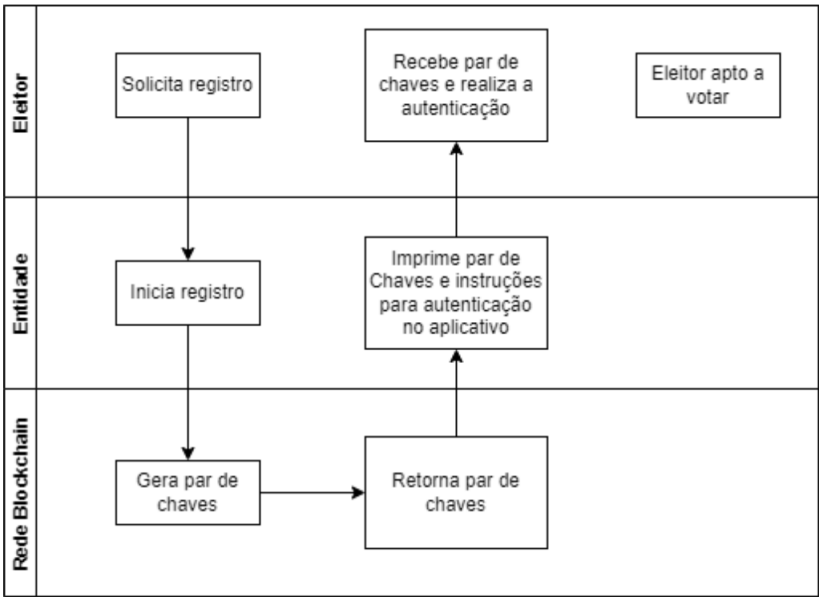
O contrato *Ballot* terá como principal objetivo armazenar as informações dos candidatos e fazer a armazenagem dos votos com base em uma variável que guarda os endereços dos eleitores válidos aptos a votar. Este contrato terá uma data inicial e data final, utilizada para validar o período da votação, e impedir que votos sejam contabilizados após o término.

Mesmo as propriedades de segurança, um dos principais aspectos ainda ficaria sem uma solução concreta, a Anonimidade do eleitor, ou seja, impedir que sua identidade seja relacionada ao seu voto, a fim de evitar diversos problemas sociais que isso poderia causar, como alterar a integridade da eleição, visto que por não ser em um ambiente monitorado como nas urnas eletrônicas, possíveis candidatos poderiam utilizar de coerção com os eleitores para benefício próprio, além da integridade física e mental do votante para com membros da sociedade que discordam da sua escolha.

Como a forma de autenticação utilizada em redes blockchain como da Ethereum seja formada por um par de chaves pública/privada (melhor abordada na seção Chaves), a identidade do eleitor ainda poderia ser descoberta ao ter acesso aos dados cadastrais dos eleitores que ficam em posse da entidade que gerencia as votações, sendo assim, não sendo possível a armazenagem dessas chaves de forma alguma em nenhum local, como para a finalidade de verificação ou comprovação do voto para com o eleitor.

Para este problema, o presente estudo propõe utilizar um método de distribuição das chaves através do próprio algoritmo de criptografia da rede Ethereum em conjunto com a Metamask, que gera o par de chaves pública/privada assim que a entidade responsável pela votação faça o cadastro do eleitor. Essas chaves serão utilizadas para a autenticação do usuário na rede Ethereum através do aplicativo de carteira digital Metamask, que faça conexão com a rede *Ethereum*, Este processo pode ser melhor visualizado na Figura 4.

Figura 4 – Processo de autenticação da rede *Ethereum*



Fonte: Autoria própria.

Vale ressaltar que nem o algoritmo nem a entidade deverá ter acesso ou armazenar essas chaves, uma vez que o usuário seja cadastrado o algoritmo gera um papel com as instruções para fazer a autenticação no aplicativo, e de manter a chave privada em sigilo.

O cadastro realizado pela entidade responsável pela votação contemplaria as informações pessoais do usuário (Nome, Idade, Endereço, etc.), o distrito, localidade ou grupo que este se encontra para que seja possível realizar uma busca das votações em aberto que são incluídas neste grupo sempre que ele faça a autenticação e por fim a sua identidade biométrica (digital), utilizada para realizar a autenticação no sistema em conjunto com a chave privada.

O comprovante da votação deve ser gerado a partir da conclusão da mesma, e salvo em um banco de dados fora da rede blockchain apenas com as informações do eleitor e da votação que este participou, para disponibilizar meios de auditoria caso necessário.

Esse problema poderia ser minimizado ocultando as chaves pública/privada do usuário, porém a chave privada é necessária para realizar o login na rede e a chave pública de assinar as transações, para ocultar do eleitor, sendo assim necessário terceirizar o serviço de autenticação na rede salvando essas chaves em outra base de dados e relacionar com algum outro meio de autenticação de conhecimento do usuário.

Isto quebra completamente o princípio da anonimidade e ainda mais o da confiabilidade da eleição, uma vez que as chaves estão armazenadas, estão extremamente vulneráveis a ataques, podendo afetar diretamente na confiabilidade das eleições, isto para tentar solucionar um problema que não depende do sistema, e sim do eleitor.

Uma das principais características das redes blockchain é a transparência, que torna todas as transações e informações passadas na rede visíveis para todo o mundo fora da blockchain, independente do escopo da variável ou função declarada para armazenar algum dado ou executar alguma operação, isso é citado na documentação da linguagem (SOLIDITY, 2022).

Outro problema acarretado pela transparência da rede é a manipulação da opinião pública devido à divulgação dos votos em tempo real, assim que são computados pela rede, ficam disponíveis para visualização utilizando ferramentas de busca especializada para redes blockchain, como a Ethers (2022).

Isso pode afetar diretamente no resultado final de uma eleição devido a possibilidade de mudar a opinião dos eleitores que ainda não votaram, com base nos votos já computados dos candidatos. Em uma possível eleição com milhões de eleitores, se torna humanamente impossível fazer essa busca voto a voto, porém com a ajuda de algoritmos isso poderia se tornar um problema.

Este problema é minimizado utilizando a lógica de escopo de variáveis e funções dos contratos inteligentes, que utilizando o modo private, só permite a interação com essas variáveis ou funções dentro do próprio contrato, nem mesmo contratos parentes podem realizar as ações de get ou set. Vale ressaltar que ainda é possível visualizar os dados de voto a voto utilizando qualquer ferramenta de busca especializada como citado anteriormente, mas essa funcionalidade minimiza esse fator.

O aplicativo mobile foi desenvolvido utilizando o framework React Native, e possui uma Tela de Autenticação, Tela Inicial que lista todas as votações, uma tela de Detalhes da Votação, que mostra os candidatos e a que cargos estão disputando, e uma Tela de Votação, que solicita para que o usuário confirme seu voto ao clicar em um candidato, utilizando seu CPF e Senha passados pela entidade responsável pela votação. O backend desenvolvido utilizando Node.js é o responsável por simular a base de dados da entidade, e disponibilizar as informações do eleitor para que ele possa realizar a conexão com a base e a autenticação por CPF e Senha. Os resultados com imagens dos contratos, frontend e backend estão disponíveis no Capítulo 6.

4.0.3 Sequência de Passos

1. Estudo bibliográfico: Realização de uma pesquisa bibliográfica sobre outros trabalhos feitos anteriormente sobre esse assunto, a rede blockchain, suas características e aplicações, com o intuito de entender como a tecnologia é estruturada, como funciona e quais são seus paradigmas;

2. Análise sobre a aplicação de blockchain à um sistema de votação: Com um conhecimento geral sobre a tecnologia, um estudo mais focado na aplicação de uma rede blockchain à um sistema de votação foi feito;

3. Coleta de informação: Aplicação de um formulário aos alunos de Engenharia de Software, com intuito de coletar opiniões e sugestões sobre os sistemas conhecidos de votação, e um sistema remoto baseado em blockchain.

4. Análise das informações coletadas: Após a coleta dos dados através do formulário, uma análise foi feita, elencando as principais vantagens e desvantagens dos sistemas abordados, segundo os participantes.

5. Análise técnica para elencar possíveis tecnologias que auxiliem o desenvolvimento de um projeto de votação remota baseado em blockchain: Após estudar e entender melhor sobre blockchain, e as informações passadas pelos participantes do questionário, foram escolhidas algumas tecnologias, linguagens, ferramentas e técnicas que foram úteis na concepção da ideia do projeto, baseando-se nos critérios explicados;

6. Desenvolvimento do TCC 1: Trabalho de Conclusão de Curso n° 1 foi escrito com base nas informações obtidas e estudos realizados.

7. Entrega TCC 1: O documento de TCC 1 foi entregue pronto para avaliação dos responsáveis.

8. Defesa do TCC 1: Apresentação feita para a banca sobre o trabalho e pesquisas realizadas até o momento.

9. Concepção dos contratos inteligentes: Após a escolha das tecnologias, técnicas e ferramentas, o desenvolvimento se iniciou primeiramente pelos dois contratos inteligentes responsáveis pelo gerenciamento das votações. Estes contratos inteligentes irão implementar todas as funcionalidades necessárias para o funcionamento de uma votação na blockchain. Mas não asseguram que a lisura do processo eleitoral seja feita na sua totalidade, não considerando a anonimidade, coerção e os votos em tempo real.

10. Criação do banco de dados: Desenvolvimento de um banco de dados de armazenamento tradicional para obter e persistir informações que auxilia no processo de autenticação e gerenciamento dos usuários.

11. Desenvolvimento do backend: O backend foi responsável pela comunicação entre o banco de dados e o frontend com o objetivo de implementar uma camada adicional de autenticação baseada em CPF e senha, de uma base de dados com usuários de teste pré estabelecidos;

12. Desenvolvimento do frontend: Terminado o desenvolvimento dessas três etapas, o desenvolvimento do frontend foi iniciado, é responsável pela parte interativa com o usuário, utilizada para a autenticação e voto do eleitor;

13. Publicação dos contratos inteligentes: Após o término do desenvolvimento do frontend, o contrato inteligente foi publicado na rede Ropsten Testnet da Ethereum, e no servidor próprio o backend, frontend e o banco de dados da aplicação.

14. Votação simulada: Completada a fase de testes, uma votação simulada foi realizado para testar as funcionalidades do contrato inteligente através da rede Ropsten Testnet da Ethereum e visualizar as interações através da ferramenta Etherscan.

15. Visualização dos resultados: Terminado o período de votação, os resultados foram analisados para assegurar a veracidade dos mesmos e a forma que foram registrados.

16. Desenvolver uma conclusão: Com base nas informações coletadas, uma análise foi feita e a partir dos resultados obtidos para criar uma conclusão, abordando todos os aspectos positivos e negativos do projeto e as suas dificuldades e impedimentos.

17. Desenvolvimento da Monografia de TCC 2: Monografia de TCC 2 feita, com base nas informações obtidas através do desenvolvimento, teste e uso dos contratos inteligentes e do aplicativo mobile.

18. Defesa do TCC 2: Apresentar trabalho realizado para a banca de professores.

Abaixo serão abordadas as principais atividades a serem desenvolvidas, porém essas atividades poderão ser alteradas, removidas e adicionadas conforme as necessidades identificadas durante o processo de desenvolvimento, são elas:

- Cadastrar usuários: Deverá ser possível o cadastro de novos usuários.

- Autenticar usuários: Ao entrar no aplicativo o usuário deverá comprovar sua identidade através de biometria em conjunto de uma senha.

- Criar uma votação: Um usuário poderá criar uma votação com data de início e data de fim;

- Adicionar opções de voto: O usuário que criou a votação poderá adicionar as opções para votação, com um nome, descrição e foto;

- Votar: Qualquer usuário autenticado poderá votar nas opções disponíveis;
- Ver os resultados: Qualquer usuário poderá ver os resultados através do aplicativo após o término do período de votação.

5 METODOLOGIA

Nesta seção, o projeto será classificado segundo Gil (1991), que descreve várias formas de classificar as pesquisas. São elas:

5.0.1 Natureza

O projeto é de natureza aplicada, com o objetivo de gerar conhecimentos para aplicação prática dirigidos à proposta de solução dos problemas envolvendo os processos eleitorais e/ou de votação empregados nos dias de hoje no Brasil.

5.0.2 Abordagem do Problema

Na abordagem para o processamento e análise dos dados, será utilizado o método qualitativo, pois será necessário avaliar a opinião dos votantes em relação ao sistema, abordando seus diversos aspectos, como a segurança, anonimidade, confiabilidade e praticidade.

5.0.3 Objetivos

O projeto é composto por uma abordagem exploratória, visando proporcionar maior familiaridade com o problema e coletar informações úteis para a concepção e a solução dos problemas enfrentados.

5.0.4 Procedimentos Técnicos

A técnica utilizada para a coleta das informações será feita através de Pesquisa Bibliográfica, para obter as informações utilizando material já publicado, constituído basicamente de livros e artigos disponibilizados na Internet, e pesquisa experimental, que vai envolver um questionário pré-determinado, que será distribuído ao fim de uma votação de teste, para que os participantes possam avaliar o método e dar sugestões através de perguntas com classificação de concordância e campos de digitação, mais especificamente utilizando a ferramenta Formulários Google. Os resultados da pesquisa se encontram no Capítulo 6.

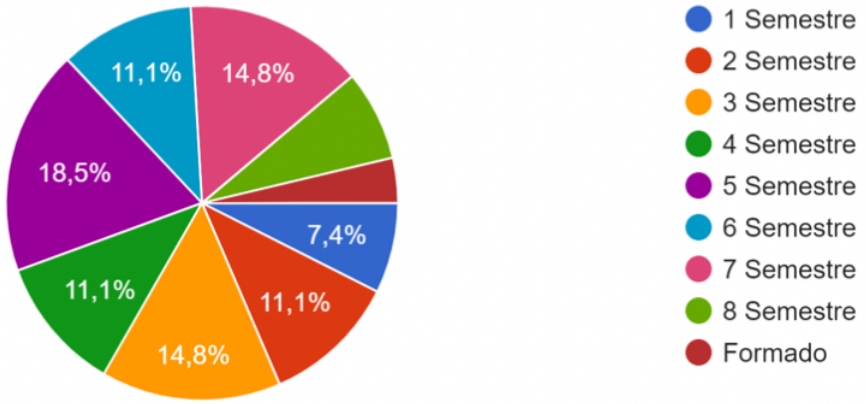
6 RESULTADOS

6.0.1 PESQUISA : SISTEMAS DE VOTAÇÃO PRESENCIAL E REMOTO

Um questionário com 14 perguntas, optativas e obrigatórias foi aplicado e distribuído entre os alunos de Engenharia de Software entre o período de 13/11/2020 e 16/11/2020, utilizando a ferramenta Google Forms, com objetivo de coletar as opiniões dos participantes sobre sistemas de votação presenciais e remotos.

A pesquisa teve um total 27 participantes, entre o 1° semestre e os já formados pelo curso, como mostra a Figura 5, que responderam utilizando como base, qualquer tipo de votação presencial ou remota que tenham participado.

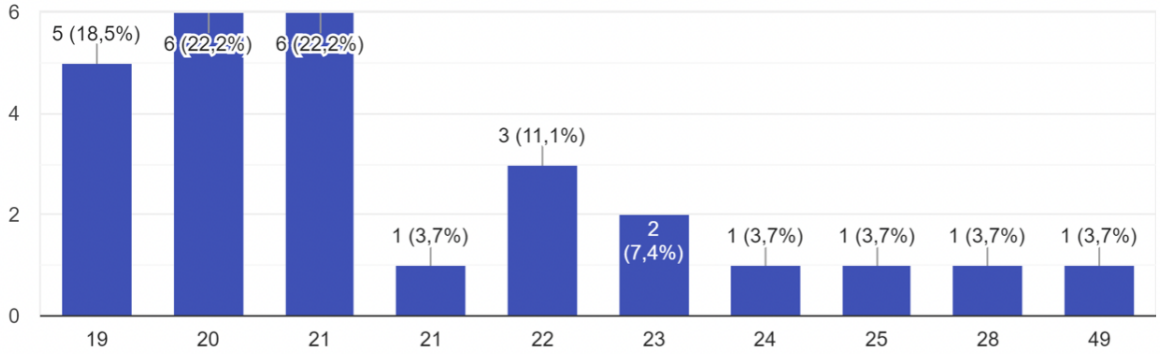
Figura 5 – Semestre dos participantes da pesquisa



Fonte: Autoria própria.

Como a Figura 6 apresenta, 62,9% dos participantes possuem entre 19 e 21 anos, concentrando a maioria das pessoas nesta faixa etária.

Figura 6 – Idade dos participantes da pesquisa



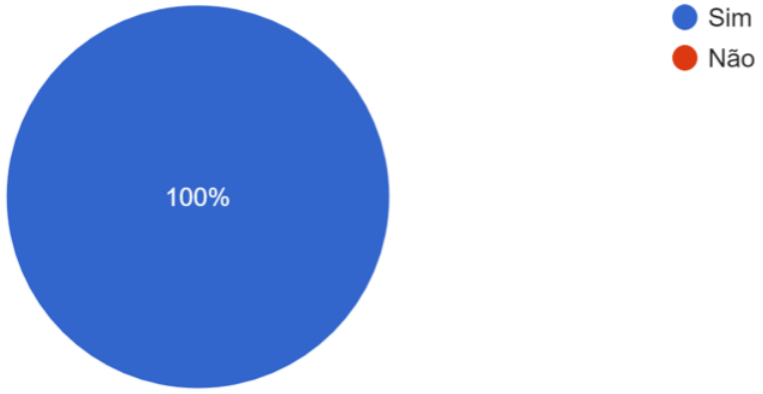
Fonte: Autoria própria.

6.0.2 Resultados

Utilizando a própria ferramenta *Google Forms*, é possível extrair as respostas em forma de gráficos de análise nas perguntas baseadas em opções e numéricas, além de disponibilizar as respostas na íntegra para as perguntas em formato descritivo.

Abaixo estão os gráficos baseados nas respostas dos participantes, mostrando o total de respostas e a porcentagem (%) de pessoas que escolheram a opção. A Figura 7 mostra que 100% dos participantes já estiveram em uma votação presencial, qualquer que seja, eletrônica ou não, tornando assim as opiniões mais assertivas e de acordo com a realidade devido a essas experiências passadas.

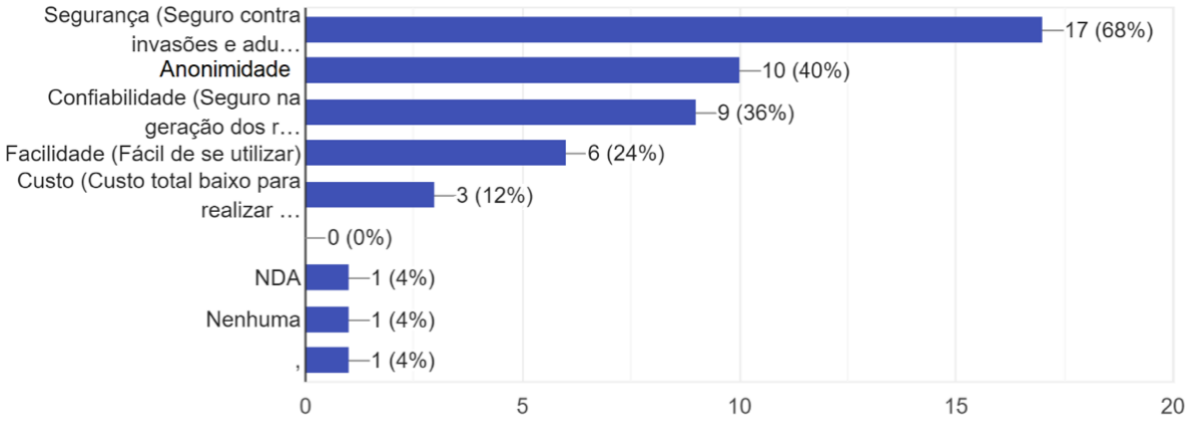
Figura 7 – Participação em votações presenciais



Fonte: Autoria própria.

A Figura 8 apresenta os pontos positivos definidos pelos participantes da pesquisa, podendo ter vários escolhidos por pessoa, sendo eles o mais votado a Segurança, com 68% das escolhas, logo após a Anonimidade com 40%, depois a Confiabilidade com 36%, Facilidade com 24% e o Custo da votação presencial com 12%.

Figura 8 – Pontos positivos em votações presenciais

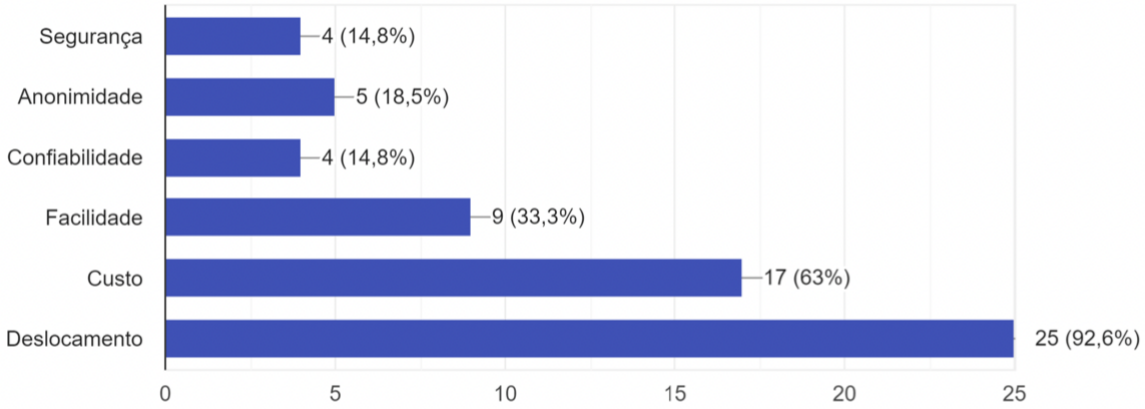


Fonte: Autoria própria.

Percebe-se que para os participantes, os pontos positivos de uma votação presencial estão concentrados principalmente na área de segurança, tanto da votação quanto do votante, sendo divididas entre a segurança contra invasões e adulterações, a anonimidade do votante, e a confiabilidade dos resultados gerados pelo sistema.

Inversamente proporcional, os pontos negativos em uma votação presencial, como ilustra a Figura 9 ficam concentrados no votante e na suas necessidades, como a necessidade de deslocamento e o custo para se implementar uma votação deste tipo.

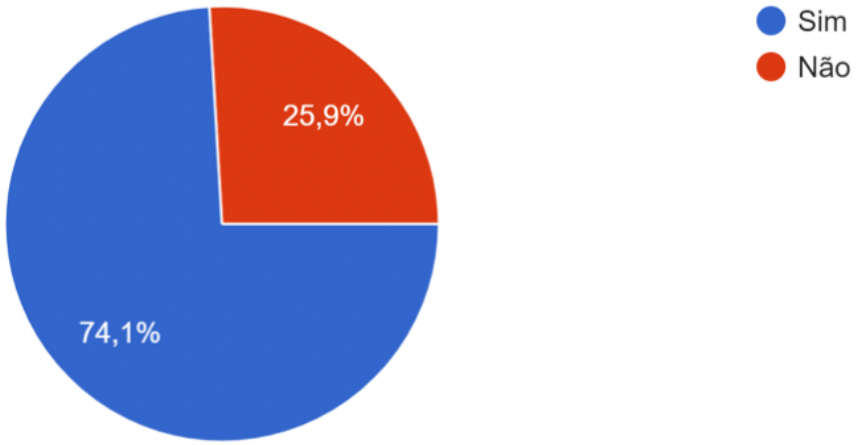
Figura 9 – Pontos negativos em votações presenciais



Fonte: Autoria própria.

Ao questionar aos participantes sobre sua participação em votações online/remotas, a situação muda, como mostra a Figura 10, 74,1% já participou de votações online/remotas, e 25,9% nunca participou, o que torna uma expressão significativa de 1⁄4 dos participantes, que mesmo assim foram questionados sobre os pontos positivos e negativos de votações online/remotas como é mostrado logo à frente.

Figura 10 – Participação dos participantes em votações online/remotas

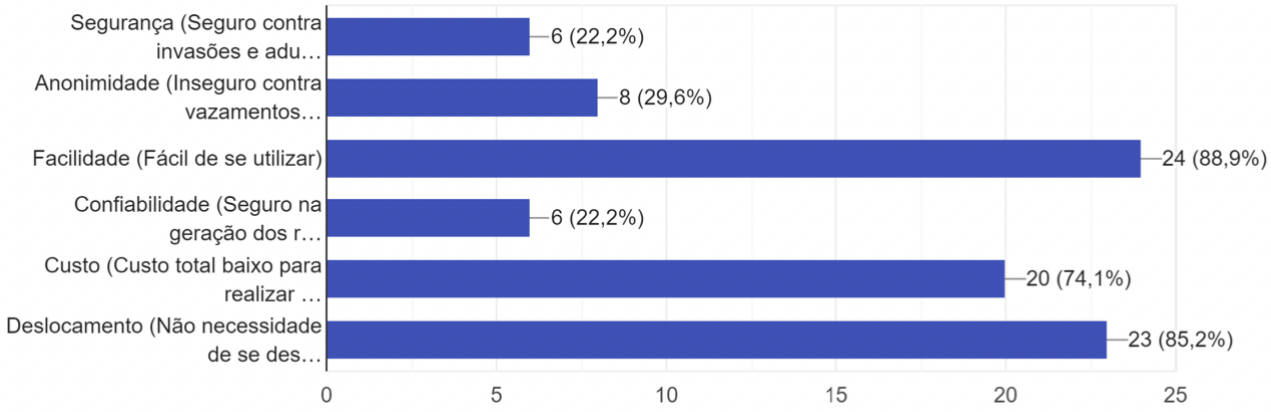


Fonte: Autoria própria.

Seguindo de forma lógica, é possível observar na Figura 11 que as respostas para os pontos positivos de uma votação online/remota foram basicamente os tratados como pontos

negativos nas votações presenciais, são eles: Facilidade, com 88.9% dos votos; Custo, com 74.1%, e Deslocamento com 85.2% das escolhas.

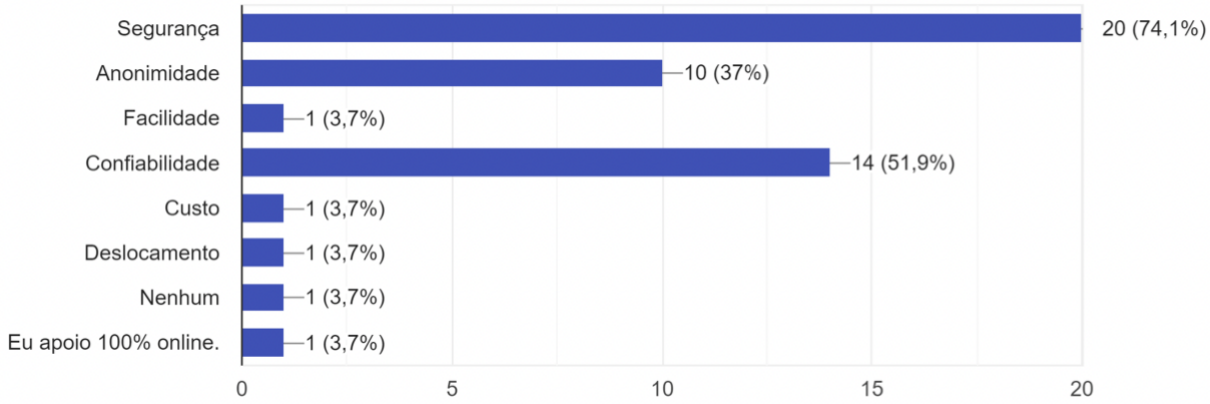
Figura 11 – Pontos positivos de votações online/remotas



Fonte: Autoria própria.

Como ilustra a Figura 12, os participantes julgam ser pontos negativos em votações online/remotas a Segurança com 74,1% de escolha, a Anonimidade com 37% e a Confiabilidade com 51,9% dos votos, nascendo assim uma oportunidade para juntar os aspectos ligados à segurança que uma votação presencial proporciona, com os aspectos ligados à facilidade, custo e comodidade que uma votação online/remota ocasiona.

Figura 12 – Pontos negativos de votações online/remotas

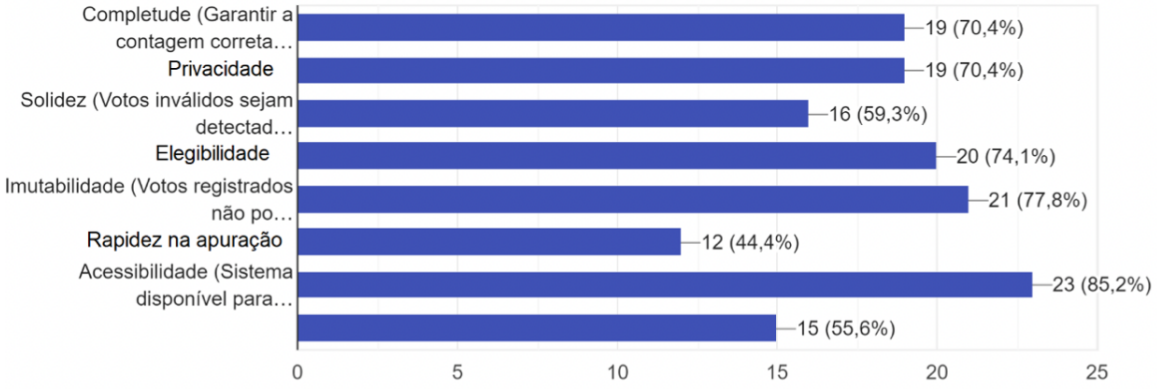


Fonte: Autoria própria.

Ao questionar sobre os principais pontos para que seja possível implementar um sistema de votação totalmente online/remoto, as respostas se tornaram mais homogêneas, como podemos observar na Figura 13.

Os aspectos ligados à segurança e confiabilidade foram os mais escolhidos, afinal é necessário para que o sistema possa ser utilizado. Já os aspectos como a rapidez na apuração

Figura 13 – Pontos mais necessários para a implementação de votações online/remotas

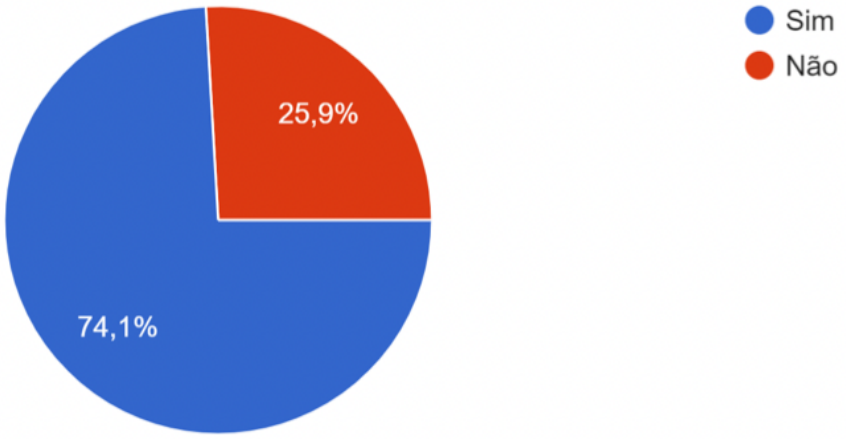


Fonte: Autoria própria.

e diminuição de coação eleitoral foram os pontos julgados não tão importantes no primeiro momento.

A Figura 14 mostra a porcentagem dos participantes que possuem conhecimento sobre blockchain, a tecnologia abordada no projeto, mostrando que a grande maioria conhece, 74,1%.

Figura 14 – Conhecimento dos participantes sobre blockchain



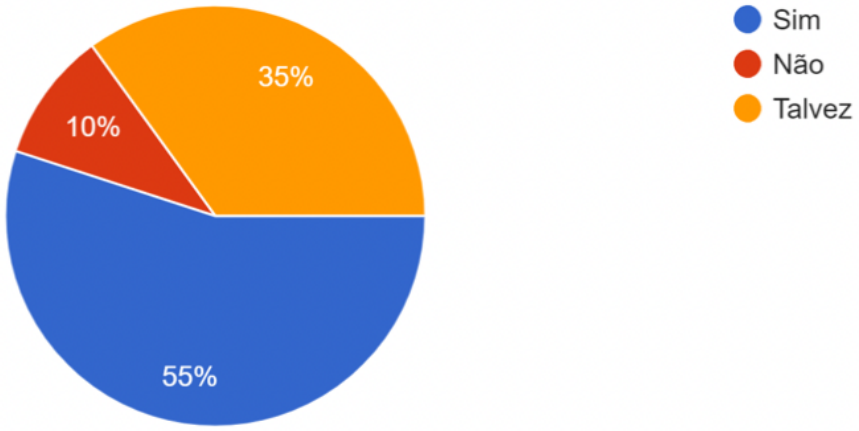
Fonte: Autoria própria.

Os participantes que já possuíam conhecimento sobre blockchain responderam a pergunta final, julgando se um sistema baseado nessa tecnologia, supriria os principais aspectos necessários abordados anteriormente para a criação de um sistema de votação totalmente online/remoto. Na Figura 15 podemos ver o resultado, que ficou dividido entre 55% de pessoas que acham que sim, 35% que julgam talvez ser possível e 10% não acham que seria o suficiente.

Os participantes que responderam Não e Talvez, disseram do porquê não ser possível, e o que mais seria necessário para que um sistema baseado em blockchain pudesse suprir as necessidades que os sistemas remotos possuem hoje.

Dentre as justificativas para não ser possível, a principal foi que não há garantia de que somente pessoas realizassem uma votação, e não inteligências artificiais e bots programados para essa função.

Figura 15 – Opinião dos participantes sobre blockchain aplicado a votações online/remotas



Fonte: Autoria própria.

Porém vale lembrar da proposta de autenticação, onde a princípio seria feito via biometria juntamente de uma senha escolhida pelo votante. Além de que apenas um voto por pessoa seria contabilizado, tornando assim ataques com esses bots algo muito improvável.

6.0.3 Análise dos resultados

Ao analisar os dados coletados, é possível perceber que as desvantagens e pontos negativos de um meio de votação, são o inverso das vantagens e pontos positivos do outro meio, tornando-se assim uma boa oportunidade para unir as vantagens dos dois meios de votação, presencial e remoto, tornando o processo de uma eleição muito mais simples, seguro, confiável e acessível.

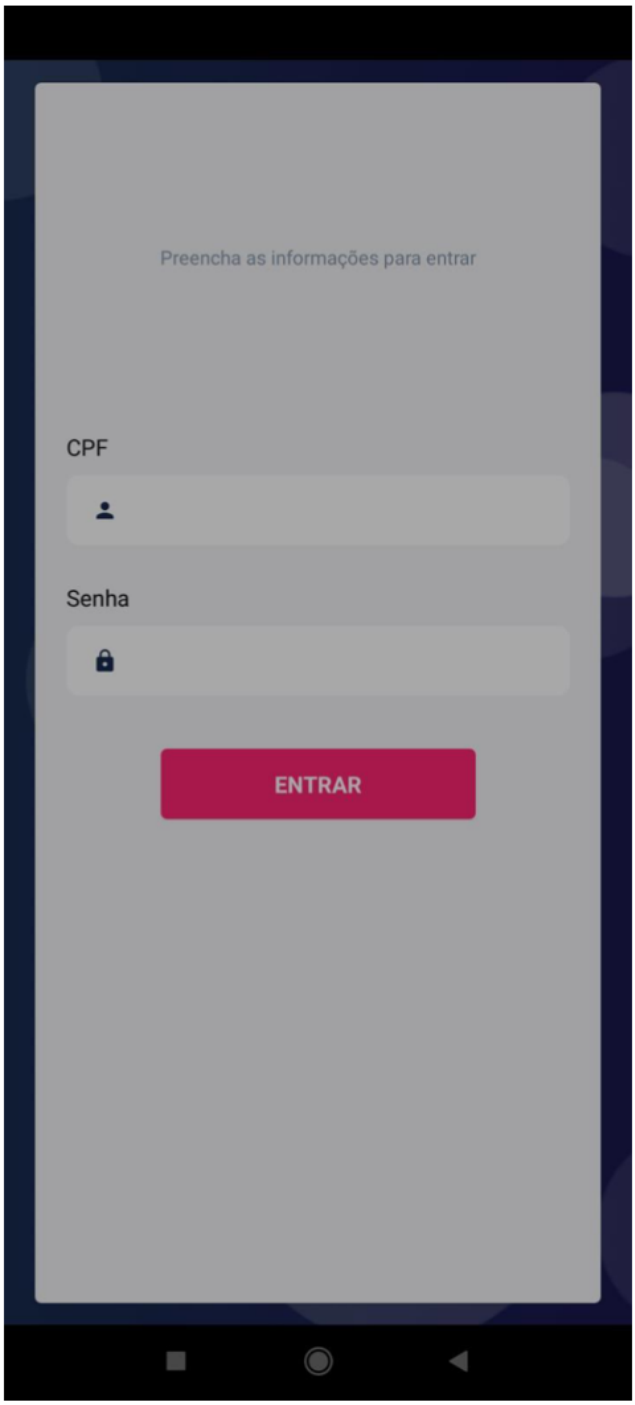
Utilizando *blockchain* isso se torna possível, afinal a tecnologia possui como seus principais benefícios as fraquezas e pontos negativos levantados pela pesquisa.

6.0.4 Desenvolvimento

Esta seção trata dos resultados obtidos após o desenvolvimento das três etapas citadas anteriormente, os contratos, o backend e o frontend.

Na Figura 16 é apresentada a tela de login do aplicativo que utiliza o CPF como identificador único do usuário e a senha para primeira fase de autenticação.

Figura 16 – Login do aplicativo



Fonte: Autoria própria.

A Figura 17 apresenta a tela de confirmação pelo usuário, para conectar com o aplicativo.

Figura 17 – Tela de conexão com o Metamask

Fonte: Autoria própria.

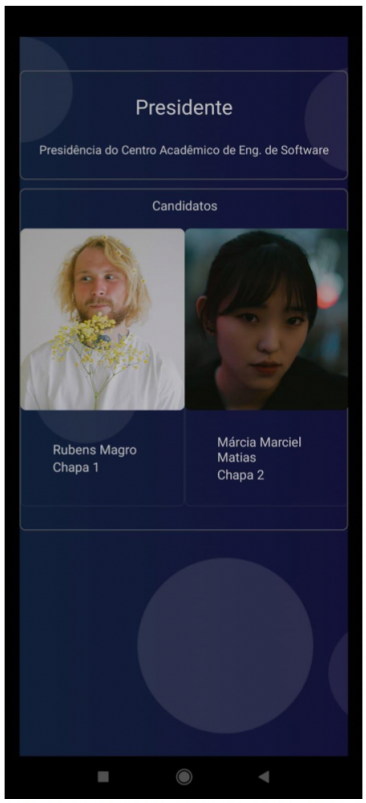
A Figura 18 apresenta a tela que lista todas as votações disponíveis e as datas que chegam ao fim.

Figura 18 – Tela de listagem de votação disponíveis

Fonte: Autoria própria.

Ao clicar em votar, o eleitor é direcionado para para a tela que mostra os candidatos ao cargo selecionado, conforme apresentados nas Figuras 19 e 20.

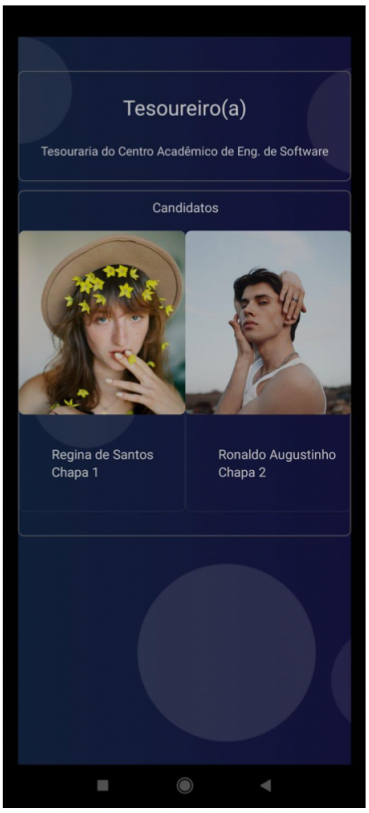
Figura 19 – Tela que mostra os candidatos a Presidente



Fonte: Autoria própria.

Pressionando o candidato que deseja votar, a tela apresentada na Figura 21 é aberta, solicitando para o usuário confirmar seu voto, e mostra todas as informações do candidato e ao cargo que está concorrendo, além de solicitar novamente o CPF e Senha como forma de autenticação antes de redirecionar para a Metamask.

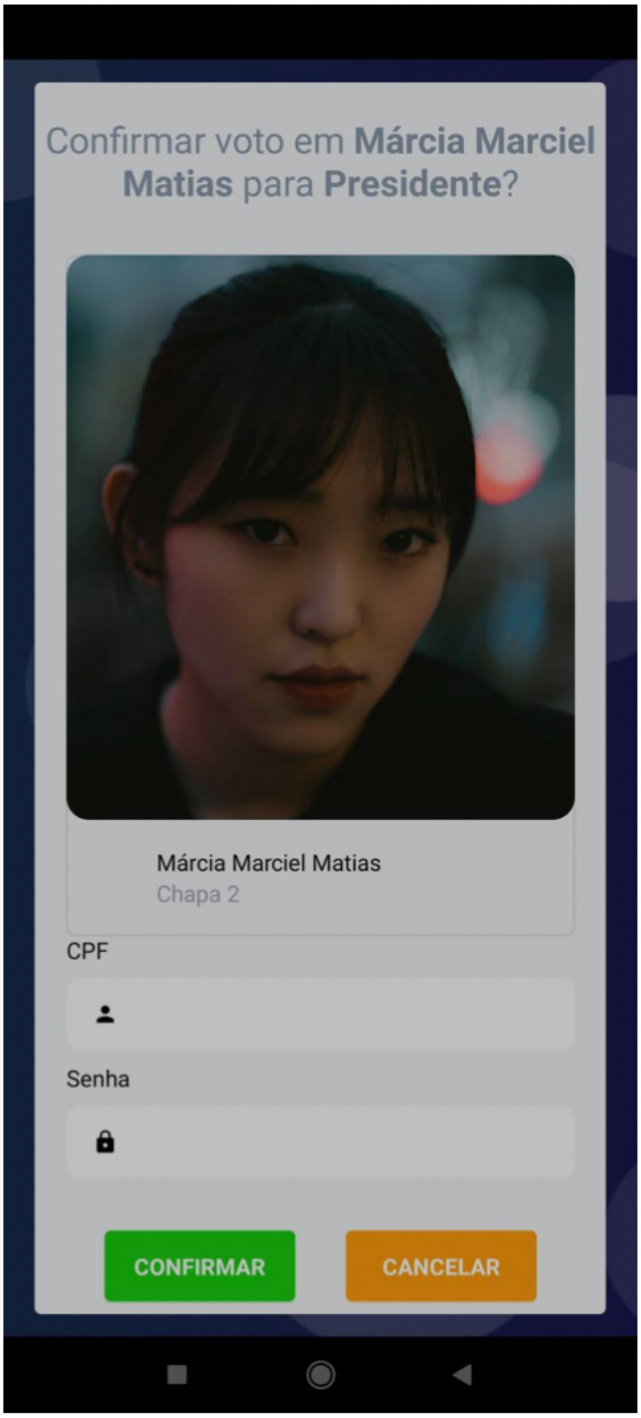
Figura 20 – Tela que mostra os candidatos a Tesoureiro(a)



Fonte: Autoria própria.

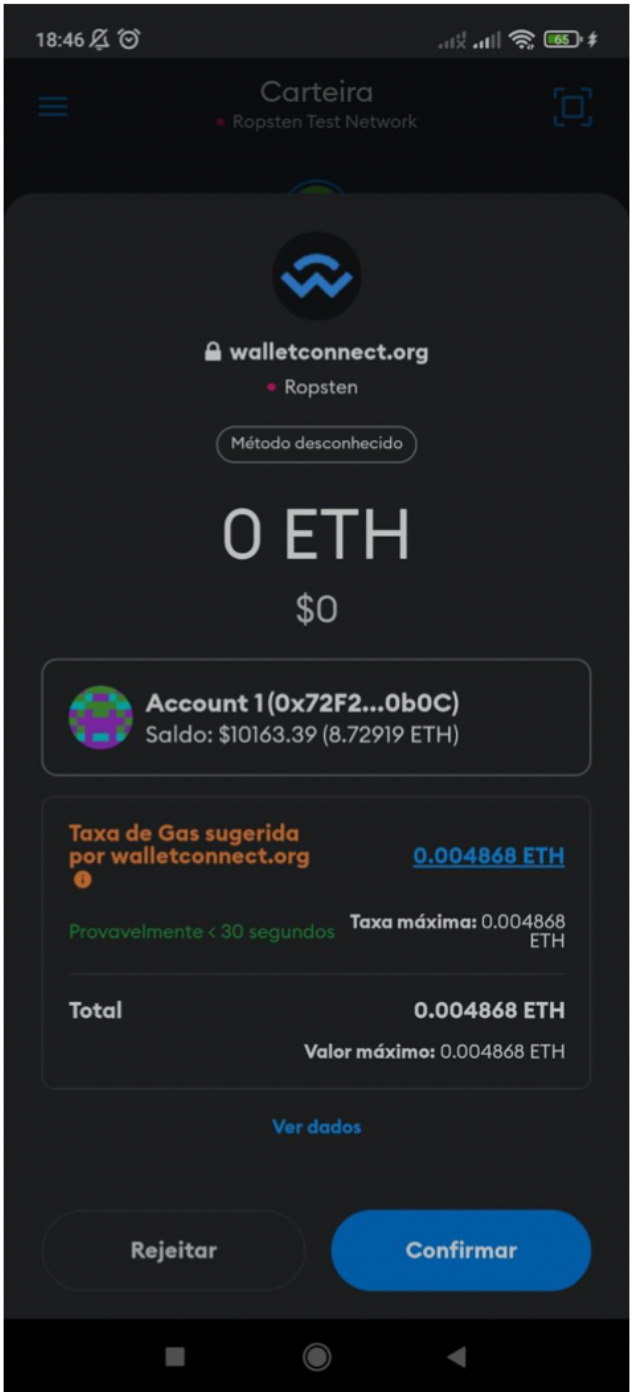
Após a votação é apresentada a tela de confirmação do voto (Figura 22) quando o usuário se autenticar e confirmar seu voto, sendo direcionado para o aplicativo da Metamask onde confirma a transação e realiza seu voto.

Figura 21 – Tela de voto do aplicativo



Fonte: Autoria própria.

Figura 22 – Tela de confirmação do voto pela Metamask



Fonte: Autoria própria.

7 CONCLUSÃO

De forma geral, ao analisar as pesquisas e os projetos já realizados na área, percebe-se que blockchain é uma tecnologia que pode ser utilizada amplamente para diversas finalidades, mas principalmente em segurança de informações, afinal suas principais características são de ser uma rede distribuída, imutável e anônima, proporcionando diversos benefícios a quem a empregar em alguma solução.

De diversas dessas soluções, a votação remota mostrou-se uma boa oportunidade, aproveitando da situação das votações de 2020 para levantar essa possibilidade de evolução do meio de votação empregado nos dias de hoje.

Ao realizar uma pesquisa bibliográfica, juntamente de uma pesquisa opinativa, e propor utilizar dos benefícios de uma rede blockchain a um sistema de votação online/remoto, percebe-se que é possível juntar as melhores qualidades e benefícios das votações eletrônicas presenciais, às melhores de um sistema totalmente remoto, removendo a necessidade de deslocamento, diminuindo os custos de implementação e manutenção de votações, além de assegurar a anonimidade, confiabilidade e segurança de forma geral do sistema, utilizando blockchain.

Durante o processo de desenvolvimento da ferramenta, é possível perceber que há uma enorme quantidade de conteúdo separadamente de cada ferramenta e tecnologia utilizada para aplicativos mobile, porém há pouquíssimo conteúdo que relacione essas ferramentas e tecnologias, de forma que dificulta e influencia no resultado final do aplicativo. Praticamente não há conteúdo em português que auxilie no desenvolvimento utilizando blockchain e aplicativos mobile.

O aplicativo tem muitos pontos a serem melhorados ainda, que ficam como trabalhos futuros para que se torne cada vez mais possível a existência de um aplicativo remoto utilizando recursos seguros como uma rede blockchain para melhorar nosso processo eleitoral e facilitar a vida do eleitor.

REFERÊNCIAS

BASHIR, I. **Mastering Blockchain**. [*S.l.*]: Packt Publishing, 2017. ISBN 9781787129290.

BIGGS, J. **Sierra Leone just ran the first blockchain-based election**. 2018. Disponível em: https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/?guccounter=1. Acesso em: 22 jul. 2021.

BITCOIN. **Portal Cotação das Criptomoedas**. 2020. Disponível em: https://portaldobitcoin.uol.com.br/cotacoes/. Acesso em: 22 set. 2020.

CAMPOS, E. M. **Engenharia de Software - 7.ed.** Rio de janeiro: Lumen Juris, 2020. 120 p. ISBN 978-65-5510-033-4.

CARVALHO, C. A. d.; ÁVILA, L. V. A tecnologia blockchain aplicada aos contratos inteligentes. **Revista Em Tempo**, Scielo, v. 18, n. 01, p. 156–156, 2019. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3210. Acesso em: 29 set. 2020.

COSTA, R. G. **Sistema Seguro de Votação Multi-Cédulas**. 2008. 110 p. Dissertação (Monografia) — Pontifícia Universidade Católica do Paraná, Curitiba, 2008.

DATE, C. J. **Introdução a sistemas de bancos de dados**. [*S.l.*]: Elsevier Brasil, 2004. 896 p.

DEMOCRACY, I. I. for; ASSISTANCE, E. **Use of E-Voting Around the World**. 2015. Disponível em: https://www.idea.int/news-media/media/use-e-voting-around-world. Acesso em: 2 nov. 2020.

ETHERS. **Documentation**. 2020. Disponível em: https://docs.ethers.io/v5/. Acesso em: 22 out. 2020.

ETHERS. **The Ethereum Blockchain Explorer**. 2022. Disponível em: https://etherscan.io/. Acesso em: 13 jun. 2022.

GIL, A. C. **Como elaborar projetos de pesquisa**. 3rd. ed. São Paulo: Atlas, 1991. 158 p.

GREVE, F. *et al.* Blockchain e a revolução do consenso sob demanda. **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Minicursos**, p. 1–52, 2018. Disponível em: http://143.54.25.88/index.php/sbrcminicursos/article/view/1770.

JS, N. **About Node.js**. 2020. Disponível em: https://nodejs.org/en/about/. Acesso em: 22 out. 2020.

MONGODB. **The database for modern applications**. 2020. Disponível em: https://www.mongodb.com. Acesso em: 23 out. 2020.

NASCIMENTO, M. M. M. d. **Uma nova abordagem sobre votação eletrônica**. 2018. 46 p. Dissertação (Monografia de Especialização em Redes de Computadores e Teleinformática) — Universidade Tecnológica Federal do Paraná, Curitiba, 2018.

NIWA, H. Um sistema de voto eletrônico baseado em blockchain. *In*: **XIX Simpósio de Pesquisa Operacional Logística da Marinha**. [*S.l.*: *s.n.*], 2019. p. 2877–2893.

REACT, N. **A framework for building native apps using React**. 2020. Disponível em: https://reactnative.dev/. Acesso em: 23 out. 2020.

SATOSHI, N. **Bitcoin: A peer-to-peer electronic cash system**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 21 set. 2020.

SCHMITT, M. A. R. **Criptografia de chaves públicas**. 2001. Disponível em: https://memoria.rnp.br/wrnp2/2001/palestras_middleware/pal_middl_02.pdf. Acesso em: 3 nov. 2020.

SILVA, M. P. A segurança da democracia e a blockchaina. **Estudos Eleitorais, Brasília,**, v. 13, n. 3, p. 71–105, 2019.

SOLIDITY. **Contracts — Solidity 0.8.14 documentation - State Variable Visibility**. 2022. Disponível em: https://docs.soliditylang.org/en/v0.8.14/contracts.html#state-variable-visibility. Acesso em: 4 jun. 2022.

TSE. **Custos e quantidades de urnas**. 2020. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2020/Fevereiro/tse-abre-propostas-de-precos-de-concorrentes-na-licitacao-para-aquisicao-de-urnas-eletronicas. Acesso em: 14 jun. 2020.

TSE. **Estatísticas Eleitorais**. 2020. Disponível em: https://www.tse.jus.br/eleicoes/estatisticas/estatisticas-eleitorais. Acesso em: 13 jun. 2020.

TSE. **Totalização dos resultados das eleições**. 2020. Disponível em: http://www.tse.jus.br/eleicoes/processo-eleitoral-brasileiro/totalizacao/totalizacao-dos-resultados-das-eleicoes. Acesso em: 6 ago. 2020.

TSE. **Urna Eletrônica**. 2020. Disponível em: http://www.tse.jus.br/eleicoes/urna-eletronica/urna-eletronica. Acesso em: 23 mar. 2020.

TYPESCRIPT. **TypeScript: Typed JavaScript**. 2020. Disponível em: https://www.typescriptlang.org/pt/. Acesso em: 22 out. 2020.

ULRICH, F. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 120 p. ISBN 8581190766.