Fundação Universidade Federal do ABC
Pró reitoria de pesquisa
Av. dos Estados, 5001, Santa Terezinha, Santo André/SP, CEP 09210-580
Bloco L, 3ºAndar, Fone (11) 3356-7617
iniciacao@ufabc.edu.br

Relatório Final de Iniciação Científica
referente ao Edital: 2024.1

Nome do aluno: Gustavo Jun Miyamoto Hassegawa

Assinatura do aluno:

Nome do orientador: Mario Alexandre Gazziro

Assinatura do orientador:

Título do projeto: Revisão de sistemas eleitorais utilizando tecnologia blockchain: Comparação entre sistemas

Palavras-chave do projeto: Sistemas Eleitorais, Máquinas eleitorais, Blockchain

Área do conhecimento do projeto: Ciência da Computação

Bolsista: Sim.

Santo André

Setembro 2025

Sumário

1. Resumo

Este relatório final de iniciação científica com o tema **Revisão de sistemas eleitorais utilizando tecnologia blockchain: Comparação entre sistemas**, tem como objetivo documentar a pesquisa de iniciação científica feita. Por sua vez, o trabalho de revisão, como um todo, busca comparação de características entre diferentes projetos em que a tecnologia blockchain tenha sido aplicada de forma a aprimorar a segurança e performance de uma máquina eleitoral. Elencando, seus pontos fortes, deficiências e implementações, assim, realizando um panorama geral do atual estado da arte e auxiliando a pesquisa em futuros artigos.

2. Introdução

A democracia surgiu na Grécia antiga, por mais que ela não seja a mesma desde o seu surgimento ainda pode ser descrita como a forma de governo em que o povo escolhe seus governantes por meio de eleições. Atualmente, o Brasil é uma república democrática e desde 1996 realiza eleições utilizando urnas eletrônicas, assim a contabilização de votos é rápida e reduz os gastos públicos com as eleições, entretanto, nas eleições recentes as urnas foram alvos de críticas de políticos que diziam que elas não eram seguras e poderiam ser facilmente fraudadas, gerando uma grande desconfiança em grande parte da população.

Assim, a implementação de diversas camadas de segurança, que permitam assegurar o resultado das eleições se tornou de extrema importância, um dos métodos mais populares em desenvolvimento, atualmente, é o uso da tecnologia blockchain, que traria vantagens como a imutabilidade, auditabilidade e descentralização que são inerentes do blockchain.

Diante desse contexto, o presente trabalho teve como objetivo realizar uma pesquisa de revisão sobre sistemas eleitorais que utilizam blockchain, comparando as diferentes abordagens quanto à escalabilidade, segurança, protocolos de consenso e algoritmos criptográficos. A análise busca identificar tendências, desafios e oportunidades na aplicação dessa tecnologia em processos eleitorais, fornecendo uma visão para futuras pesquisas e desenvolvimento de sistemas mais seguros e confiáveis.

3. Fundamentação teórica

3.1. Tecnologias Abordadas

3.1.1. Blockchain

A tecnologia blockchain é um registro distribuído e descentralizado, no qual cada transação é adicionada como um bloco ao final da cadeia. Cada novo bloco contém as informações da transação e o hash criptográfico do bloco anterior, garantindo a integridade dos dados. Assim, qualquer alteração em um bloco invalida os hashes dos blocos subsequentes, comprometendo toda a cadeia. A figura 1 descreve o funcionamento criptográfico de uma blockchain, onde o hash do bloco depende da informação armazenada nele e do hash do bloco anterior, onde a única exceção a essa regra é o Bloco Gênesis que não possui um hash anterior.

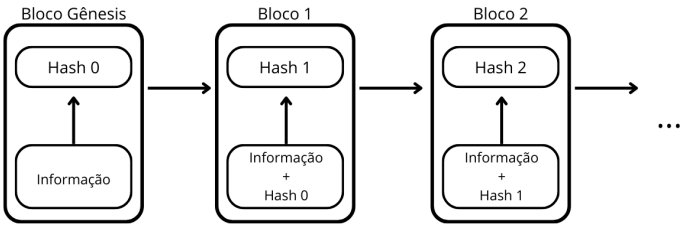

Figura 1: Estrutura encadeada de blocos em uma blockchain. Fonte: elaborado pelo autor

Todos os nós (computadores) da rede possuem uma cópia idêntica da blockchain e participam de um protocolo de consenso para determinar qual versão da cadeia é considerada válida. Portanto, quanto maior o número de nós na rede, mais difícil se torna alterar a blockchain de forma maliciosa.

Um dos maiores desafios para aplicações que utilizam blockchain atualmente é em relação à escalabilidade da blockchain, uma vez que a cada bloco adicionado, se torna mais complexo calcular o bloco subsequente. Essa estrutura foi inicialmente proposta por Satoshi Nakamoto no whitepaper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (Nakamoto, 2008), onde são descritas as bases da blockchain como um sistema resistente a modificações e descentralizado.

3.1.2. Máquinas Eleitorais

As primeiras eleições realizadas no Brasil, em que se contabilizou o voto de maneira totalmente eletrônica, ocorreram no ano de 1994. Sua introdução tinha por objetivo agilizar o processo eleitoral e diminuir as fraudes nos votos impressos.

Segundo o Tribunal Regional Eleitoral de São Paulo (TRE-SP), por meio da notícia “Saiba mais sobre a segurança da urna eletrônica”, publicada em 02/10/2024, a cada eleição o código-fonte da urna é disponibilizado ao público e passa por auditorias de testes de integridade e autenticidade, garantindo assim o pleno funcionamento das urnas no dia da eleição.

O Brasil foi um dos primeiros países a implementar o uso das urnas eletrônicas no mundo, nos dias atuais alguns países utilizam as máquinas de votação eletrônica em algumas regiões, como é o caso dos Estados Unidos, Índia, Bélgica, Canadá, França, entre outros.

3.1.3. Independência de software

Segundo Ronald Rivest, no artigo "*On the notion of "software independence*" in voting systems" (R. Rivest, 2008), um sistema eleitoral com independência de software é aquele que quando ocorre uma alteração ou erro no seu software, não causará uma mudança não detectável ao final de uma eleição. Para além desta definição, Rivest distingue a independência de software em fraca e forte, onde um sistema com fraca independência atende à definição anterior — ou seja, qualquer erro ou manipulação no software será detectável. Já um sistema com com forte independência de software é aquele em que não apenas permite a detecção de erros, mas também possibilita a correção desses problemas sem a necessidade de repetir a eleição, garantindo ainda mais robustez e confiabilidade ao processo eleitoral.

4. Estado da arte

ElectionBlock:

O sistema ElectionBlock é dividido em dois componentes principais: a estação de voto e a estação central. Na estação de voto, são coletados o voto e a digital do eleitor. Inicialmente, verifica-se se o eleitor possui biometria cadastrada e, em seguida, se ele já realizou o voto. Caso ambas as verificações sejam bem-sucedidas, o registro do voto é efetuado.

Na estação central, todas as transações da blockchain são transmitidas da estação de voto para um servidor Flask, hospedado no servidor central. Os dados recebidos são inseridos em uma fila de votos, que é processada e esvaziada após atingir um determinado número de registros.

Cada voto registrado contém a identidade do eleitor, o candidato escolhido, o número da campanha e o horário da votação. Essas informações são combinadas para gerar um código hash, que é posteriormente processado em uma árvore de Merkle. O hash da raiz da árvore é utilizado como identificador do novo bloco adicionado à blockchain.

As atualizações da blockchain são propagadas para as estações de voto utilizando a arquitetura *publish-subscribe* (pub-sub) implementada com Redis, garantindo que todos os nós mantenham cópias locais atualizadas da cadeia de blocos.

Para aumentar a escalabilidade do sistema, foi implementada a divisão da blockchain (*blockchain sharding*). Embora essa abordagem aumente a capacidade de processamento, ela introduz riscos à integridade das informações, visto que cada fragmento opera como uma blockchain independente. Para mitigar esse problema, os autores propõem a implementação de um mecanismo de comunicação entre os diferentes fragmentos da cadeia.

DVTChain:

A arquitetura proposta pela DVTChain envolve três entidades externas: a comissão eleitoral, os eleitores e o *Crypto Server*. A comissão eleitoral é responsável por supervisionar o processo eleitoral, iniciar e encerrar as eleições, publicar os resultados e criar a lista de eleitores antes do início do pleito. Os eleitores, por sua vez, são as pessoas registradas pela comissão que votarão em seus respectivos distritos eleitorais. Já o *Crypto Server* é um nó dedicado exclusivamente ao armazenamento das

chaves pública e privada, sendo utilizado para manter os votos encriptados antes do envio à blockchain.

Na arquitetura proposta, a comissão eleitoral cria e administra a eleição por meio de contratos inteligentes (*smart contracts*), que identificam as diferentes responsabilidades e transações durante o processo eleitoral. Foram implementados três contratos inteligentes: o contrato de eleitor, o contrato de candidato e o contrato de votação.

O contrato de eleitor armazena o hash das informações do eleitor durante o registro, assegurando tanto a proteção dos dados quanto o anonimato dos votantes. Esse hash também é utilizado posteriormente para autenticação dos votos. O contrato de candidato registra na blockchain as informações dos concorrentes, permitindo que, durante o processo de votação, os eleitores escolham entre os candidatos listados. Após a escolha, o voto é encriptado com a chave pública gerada pela comissão eleitoral e enviado ao contrato de eleição, que o adiciona à blockchain. No sistema proposto, cada voto corresponde a um bloco da cadeia, o que pode representar um desafio para eleições de grande escala, devido ao crescimento acelerado da blockchain.

Após o encerramento da votação, a comissão eleitoral descriptografa os votos utilizando a chave privada e os envia ao contrato de votação. Este, por sua vez, associa os votos aos candidatos correspondentes, por meio do contrato de candidato, realizando a contagem e publicando os resultados.

A DVTChain assegura o anonimato dos eleitores, uma vez que suas identidades são convertidas em hashes e representadas apenas por chaves públicas. Como os votos são encriptados antes de serem adicionados à blockchain, torna-se inviável associá-los a eleitores específicos. Além disso, durante a contagem, os contratos inteligentes associam os votos aos candidatos sem revelar as identidades dos votantes. A integridade do sistema é garantida pelo uso da Árvore de Merkle (*Merkle Tree*), na qual um hash raiz é calculado a partir dos hashes de votos agrupados (neste caso, a cada 8 votos). Dessa forma, qualquer alteração mínima em um dos votos modificaria o hash raiz, permitindo a detecção de inconsistências.

Por fim, a imparcialidade é assegurada pela separação entre as fases de votação e contagem, além da encriptação dos votos na blockchain, evitando que resultados parciais influenciem a decisão dos eleitores que ainda não votaram.

AMVChain:

AMVChain utiliza assinatura em anel ligada para garantir uma melhor anonimidade entre eleitores, a assinatura em anel ligada permite que o participante apresente uma assinatura válida a partir de um conjunto de chaves sem revelar qual chave foi utilizada. Quanto mais pessoas participam da assinatura mais anônima se torna o voto.

A arquitetura da implementação foi dividida em 4 camadas, aplicação, contrato inteligente, consenso e armazenamento. A camada de aplicação tem como objetivo fornecer uma interface gráfica para os diferentes usuários, além disso, nesta camada os eleitores e candidatos podem se cadastrar fornecendo suas informações pessoais e recebem um id para votantes e candidatos. Para a comissão eleitoral existem outras funções como a visualização da rede blockchain e as informações da eleição, assim como criar eventos eleitorais e iniciar eleições.

Na camada de contratos inteligentes ocorrem diversos processos por meio de contratos inteligentes, como a validação de usuários e a distribuição de chaves públicas

pelos votantes que serão utilizadas para a geração de uma assinatura em anel, gerenciamento de autoridade. Os contratos propostos pelos autores são os seguintes: *VoteManage,* verifica a identidade automaticamente, *VoteAuthority*, atribui diferentes permissões e cargos , *VoteVerify*, verifica a assinatura dos votos, *VoteCount*, calcula os votos e anuncia os resultados.

A camada de consenso utiliza o algoritmo de consenso PBFT (*Pratical Bizantine Fault Tolerance*), entretanto, à medida que se adicionam nós de verificação, o tempo de cálculo cresce exponencialmente (n^2), para evitar isso os autores decidiram transformar locais de votação em nós proxy. Os locais de votação recebem os votos e transmitem para os outros nós, que irão verificar se o voto é válido e enviarão o bloco à blockchain. Na camada de armazenamento Hyperledger Fabric é adotado como modelo de conservação de informações, dados como os votos e os contratos inteligentes são armazenados na blockchain, cada instituição, local de votação, possui uma cópia da blockchain.

Durante todo o processo eleitoral os contratos inteligentes desempenham um papel fundamental, como, verificação de identidade e contabilização de votos.Além disso, os contratos inteligentes garantem que apenas eleitores qualificados consigam acessar à blockchain e informações dos candidatos. AMVChain conseguiu prover anonimidade e privacidade do eleitor por meio da assinatura em anel ligada, e conseguiu garantir certa escalabilidade do sistema para eleições de grande porte.

Abuidris et al. 2020:

Os autores propuseram um mecanismo de votação eletrônica baseado em um protocolo de consenso híbrido denominado PSC-Bchain, que combina os protocolos Proof of Credibility (PoC) e Proof of Stake (PoS). Além da fusão dos métodos de consenso, o sistema incorpora um mecanismo de fragmentação (*sharding*), visando não apenas aumentar a segurança, mas também melhorar a escalabilidade e a performance do sistema.

O sistema é composto por diversos componentes, entre eles os *Manage Servers* (MS), que armazenam informações dos nós em blockchains de camada baixa e publicam dados na blockchain de camada alta. Os MS também são responsáveis pela autenticação e verificação dos usuários.

A arquitetura de rede proposta consiste em múltiplas blockchains operando em paralelo, o que contribui para o aumento da escalabilidade e da eficiência do sistema. As blockchains de camada baixa são blockchains privadas que armazenam informações sobre os nós e os eleitores, e nelas é aplicado o protocolo de consenso PoC. Por outro lado, a blockchain de camada alta, que é pública (como, por exemplo, a rede Ethereum), é responsável por armazenar os votos e adota o protocolo de consenso PoS.

Os testes realizados pelos autores demonstraram que a blockchain híbrida proposta é mais segura contra ataques em comparação às blockchains convencionais. Além disso, o protocolo de consenso híbrido PSC-Bchain apresentou desempenho superior em termos de eficiência quando comparado a protocolos tradicionais, como Proof of Work (PoW) e o próprio PoS.

Provotum:

Provotum é uma aplicação de máquina eleitoral com blockchain que utiliza o protocolo de consenso PoA (*Proof-of-Authority*), no qual um grupo de validadores é confiado com a criação de blocos, validação de transações e segurança da blockchain. Assim, foi possível selecionar um grupo de validadores confiáveis para realizar esse papel e aumentar a confiança na blockchain.

Os autores dividiram as partes envolvidas em quatro tipos: Validadores (*Sealers*), Autoridade Eleitoral (*Voting Authority*), Eleitores (*Voters*) e Provedor de Identidade e Acesso (*Identity and Access Provider*). Os validadores ou seladores são autoridades autorizadas a assinar blocos, participar do protocolo de consenso e do processo de desencriptação. A Autoridade Eleitoral é a administradora da eleição e atua como coordenadora da fase de votação. Entre suas competências estão a coordenação da fase inicial da eleição com os validadores, a publicação do contrato inteligente e a abertura e o encerramento da eleição. Os eleitores são cidadãos elegíveis para votar. Estes devem autenticar sua identidade com o Provedor de Identidade e Acesso, que permitirá ao votante cadastrar o voto. Por fim, o Provedor de Identidade e Acesso pode ser dividido em dois serviços: o Provedor de Identidade (IdP), que verifica a elegibilidade e identidade do eleitor, devolvendo a ele um token de acesso único; e o Provedor de Acesso (AP), serviço disponibilizado pela Autoridade Eleitoral, que valida o token. Caso seja bem-sucedida, a validação permite que o Provedor de Acesso disponibilize na conta blockchain do eleitor os tokens de voto que ele poderá usar para participar da eleição.

O protocolo de votação do Provotum é dividido em três fases: pré-eleição (*Pre-Voting Phase*), votação (*Voting Phase*) e pós-eleição (*Post-Voting Phase)*. Entretanto, antes das etapas descritas anteriormente, ocorre o processo de Provisionamento de Identidade (*Identity Provisioning)*, no qual a elegibilidade do eleitor é verificada pelo Provedor de Identidade e Acesso, permitindo sua participação na eleição.

Na fase pré-eleição, ocorrem os ajustes finais para o início da eleição. Esta fase é dividida em três passos: **Registro (*Registration*)**, onde todos os validadores geram chaves públicas e privadas para as contas da blockchain e registram a chave pública junto à Autoridade Eleitoral, o que permite a validação de blocos na blockchain; **Pareamento (*Pairing*)**, onde a Autoridade Eleitoral funciona como um nó de inicialização, ajudando todos os validadores a se conectarem. Após isso, a Autoridade Eleitoral implanta o contrato inteligente do voto na blockchain, que irá lidar com toda a informação específica de votos; **Geração de chaves (*Key Generation*)**, quando o contrato inteligente já está na blockchain, inicia-se o processo de Geração Distribuída de Chaves (*Distributed Key Generation*), um protocolo criptográfico em que se cria uma chave privada compartilhada entre múltiplas partes, sem que nenhuma delas conheça a chave completa. Todos os validadores geram um par de chaves privada e pública ElGamal e um Schnorr proof of knowledge, que são enviados ao contrato inteligente na blockchain. Esse processo consegue diminuir as chances de uma falha de ponto único (Single Point-of-Failure) em um dos validadores. Após a verificação das provas enviadas, a Autoridade Eleitoral cria uma chave pública combinando todas as chaves enviadas, que será utilizada por todos os eleitores para a encriptação do voto.

A fase de votação possui três passos, todos realizados pelo eleitor no cliente de votação. Primeiramente, o eleitor pode cadastrar seu voto e encriptá-lo, processo realizado pela aplicação quando ele faz sua escolha. Em adição ao voto encriptado, o sistema gera um Non-Interactive Zero-Knowledge Proof (NIZKP), provando que o voto

possui uma escolha sem revelar o real conteúdo. Após isso, o voto encriptado e a prova NIZKP são enviados para o contrato inteligente, e o voto é registrado assim que a prova é verificada pelo contrato. Ao final, o eleitor recebe uma confirmação do voto, que pode ser usada depois para checar se o voto foi cadastrado como esperado.

Finalmente, na fase pós-eleição, a eleição é encerrada em um tempo pré-determinado e comunicado a todos. Assim, o contrato inteligente encerra a eleição, não aceitando mais votos para registro na blockchain, e os validadores podem decriptar os votos e publicar o resultado final. Inicialmente, os votos são recuperados da blockchain, somados homomorficamente e parcialmente decriptados utilizando a chave privada combinada com a chave pública de todos os validadores.

Zaghloul et al. d-Bame:

O sistema d-Bame proposto por Zaghloul et al. utiliza a participação de duas partes conflitantes para assegurar a integridade e transparência do processo eleitoral, a aplicação pode ser implementada em dispositivos IoT (*Internet of things*) como em aparelhos celulares o que pode aumentar a participação dos eleitores na eleição. A blockchain executa um contrato inteligente como um quadro de avisos publicamente acessível e resistente a alterações para o armazenamento permanente de votos.

O sistema proposto possui seis entidades que participam do processo eleitoral como: eleitores (*Voters*): usuários cadastrados com direito a voto; Candidatos (*Election Candidates*): os usuários registrados como candidatos elegíveis. Registrador (*Registrar*): primeira entidade organizadora da eleição, responsável por gerar uma cédula de voto digital, a qual é única e aleatória, no sentido de que não é possível associá-la ao respectivo eleitor. Essa cédula é compartilhada com os eleitores de forma anônima. Moderador (*Moderator*): entidade também envolvida na organização da eleição, com a função de ocultar a identidade dos eleitores e entregar as cédulas de forma anônima. O moderador, por sua vez, não sabe quem é o eleitor que receberá a cédula, sendo, portanto, incapaz de associar a cédula ao seu respectivo eleitor. Rede Blockchain (*Blockchain Network*): responsável por armazenar os votos da eleição, além disso, roda um contrato inteligente (*smart-contracts*) da eleição. A Blockchain não consegue ligar cédulas a seus respectivos votantes e também não diferencia votos válidos de inválidos.

No que tange a segurança o esquema satisfaz pontos essenciais à um sistema eleitoral como: resistência a votos duplos; anonimidade; resistência a coerção - mesmo sob coerção, o eleitor pode votar conforme instruído, mas ainda preservar seu voto verdadeiro; auditabilidade, verificação universal - qualquer pessoa pode verificar se os votos legítimos foram cadastrados; resistência à ataques pela rede. Além disso, o modelo garante confiança distribuída (*Distributed Trust*): os autores assumem que a eleição será organizada por um registrador e um moderador com interesses conflitantes. Assim, é improvável que colaborem de forma maliciosa. Esse modelo se diferencia por não exigir confiança em uma única entidade, já que a desconfiança mútua funciona como um mecanismo de verificação e equilíbrio.

A arquitetura proposta pelos autores segue as seguintes etapas:

Preparação (*Setup*): O registrador e o moderador geram, cada um, um par de chaves. As chaves privadas são escolhidas aleatoriamente, e as chaves públicas correspondentes são calculadas usando o protocolo de Diffie-Hellman.

Registro de eleitor (*Voter Registration*) : Nesta etapa ocorre a validação, os eleitores provam ao registrador que são aptos a cadastrarem seus votos por meio de documentos, após a validação os eleitores são adicionados a lista eleitoral.

Primeiramente, cada eleitor seleciona uma das chaves privadas e sua chave pública é então calculada, essas chaves públicas são compartilhadas com o registrador durante o registro. O registrador verifica a elegibilidade dos eleitores, assina as chaves públicas e gera uma assinatura aleatória para o eleitor, em seguida, adiciona a assinatura e a chave pública do eleitor na lista eleitoral que é fechada quando a fase de registro termina.

Aquisição da Cédula (*Acquiring Ballot*) : No processo de aquisição da cédula de voto digital, o registrador cria cédulas únicas e as assina digitalmente com o esquema ElGamal, embaralhando-os em seguida. O eleitor solicita a cédula por meio do moderador, que verifica sua identidade, aplica um fator de cegamento para ocultar sua chave pública e encaminha a requisição ao registrador. Este então atribui uma cédula cifrada ao eleitor, garantindo que nem ele nem o moderador saibam a identidade completa do votante ou o conteúdo do boletim. O eleitor, ao final, decifra a cédula com segurança, preservando o anonimato e a integridade do processo.

Registro de Votos (*Casting Votes*) : Após o eleitor selecionar os candidatos desejados, a cédula passa por um processo de dupla encriptação, utilizando as chaves públicas do registrador e do moderador. Em seguida, o voto encriptado é enviado para o contrato inteligente da eleição, que o adiciona permanentemente à blockchain. O eleitor, então, recebe uma confirmação de que o voto foi registrado, juntamente com o hash da transação, que pode ser utilizado posteriormente para verificar se o voto foi corretamente armazenado.

Apuração (*Tabulation*) : Após o término da fase de registro dos votos, os votos armazenados na blockchain são coletados para validação e contagem. O moderador e o registrador revelam publicamente suas chaves secretas, permitindo que a autoridade responsável pela apuração desencripte as cédulas. Caso a cédula esteja entre as válidas, os votos são interpretados e os contadores dos candidatos são atualizados. A eleição pode estabelecer regras próprias para desqualificar votos inválidos, como a seleção simultânea de candidatos mutuamente exclusivos.

A implementação foi capaz de oferecer requisitos de segurança como proteção contra votos duplicados, anonimato do eleitor, resistência à coerção e proteção contra a manipulação de resultados. Além disso, é capaz de realizar eleições em larga escala. Os autores demonstram que a aplicação pode funcionar em desktops e smartphones; no entanto, ela não apresenta escalabilidade.

5.Metodologia

5.1. Métodos

A seleção de artigos, para esta pesquisa de revisão bibliográfica, foi realizada por meio de bases de dados conhecidas, como o Google Scholar, IEEE Xplore e Scopus, seguindo os parâmetros descritos:

1. Postagem nos últimos 5 anos (2020-2025);
2. Número relevante de citações;
3. Atendam os requisitos de um sistema de votação eletrônica.

A coleta de dados foi realizada a partir da leitura dos artigos, foram elencados características como, frameworks de blockchain, protocolos de consenso utilizados,

algoritmos de hash e de criptografia e tipos de blockchain. Assim, os dados extraídos foram organizados em tabelas comparativas, permitindo identificar padrões de uso entre os artigos coletados.

6.Análise de Resultados

Com base nos dados obtidos ao longo da pesquisa, foi possível elaborar tabelas comparativas que sintetizam as principais características das diferentes implementações analisadas. A construção dessas tabelas teve como objetivo evidenciar elementos técnicos e funcionais considerados fundamentais para a avaliação da viabilidade e da robustez das soluções estudadas.

Nesse sentido, foram atribuídos critérios de relevância às características que exercem influência direta sobre aspectos críticos da aplicação das tecnologias analisadas, especialmente no que diz respeito à segurança dos sistemas eleitorais, à escalabilidade das arquiteturas baseadas em blockchain, e à natureza dos frameworks utilizados no processo de desenvolvimento.

A análise dessas variáveis permite não apenas compreender o grau de maturidade tecnológica das soluções existentes, mas também identificar vantagens e limitações específicas de cada abordagem. Tal compreensão é essencial para orientar futuras pesquisas, bem como para subsidiar decisões técnicas e estratégicas em contextos de aplicação real

6.1. Framework

Em diversas implementações analisadas, os autores optaram por desenvolver suas aplicações a partir de frameworks de blockchain já consolidados no ecossistema global, com destaque para o Ethereum. A Tabela 1 apresenta um panorama dessas escolhas, evidenciando uma predominância crescente da utilização do Ethereum como base tecnológica em sistemas de votação eletrônica baseados em blockchain.

Essa preferência se justifica, principalmente, pela capacidade do Ethereum de suportar contratos inteligentes (smart contracts), escritos em linguagens como Solidity. Esses contratos permitem a automatização segura de processos fundamentais no contexto eleitoral, como o cadastro de eleitores, a verificação de elegibilidade, a emissão de votos e a apuração dos resultados. Além disso, os contratos inteligentes operam de forma transparente e imutável na blockchain, o que contribui para o aumento da confiança e da auditabilidade do sistema.

Tabela Framework Utilizados		
Artigo	**Autor**	**Framework**
DVTChain	Alvi et al. 2021	Ethereum
AMVChain	Li et al. 2021	Hyperledger Fabric
A Secure Decentralized E-Voting with Blockchain & Smart Contract	Kumar et al. 2023	Ethereum

Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System	Killer et al. 2020	Ethereum
d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting	Zaghloul et al. 2021	Ethereum
Electronic Voting System Using an Enterprise Blockchain	Gonzalés et. al. 2022	Hyperledger Fabric
A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT	Li et al. 2021	Ethereum
Decentralized E-voting system based on Smart Contract by using Blockchain Technology	Al-madani et. al. 2020	Ethereum

6.2. Protocolo de Consenso:

O protocolo de consenso é um algoritmo que permite que um grupo de processos ou nós descentralizados cheguem a um acordo, consenso, sobre um único valor comum. Em sistemas descentralizados, como os analisados, o protocolo de consenso é extremamente relevante, uma vez que, a falta de uma entidade central de controle faz com que seja necessário que todos os participantes do sistema concordem qual é o estado válido atual do sistema.

A Tabela 2, revela uma predominância de três tipos de protocolos de consenso, Proof-of-Work(PoW), Proof-of-Stake(PoS) e Proof-of-Authority(PoA). O Proof-of-Work, utilizado pelo bitcoin, assegura a integridade da informação da rede por meio da resolução de problemas criptográficos de alta complexidade. É extremamente seguro contra ataques, já que um invasor precisa controlar mais de 50% dos nós da blockchain, o que é inviável para grandes blockchains públicas. Entretanto, sua desvantagem é a baixa escalabilidade, pois o elevado consumo energético e tempo necessário para validar blocos limitam o número de transações processadas por segundo.

Proof-of-Stake, modelo utilizado pelo Ethereum, surge como uma alternativa mais eficiente, é utilizada a posse de tokens como critério para selecionar validadores. Esse modelo reduz drasticamente o consumo energético e aumenta a escalabilidade, já que a validação de blocos é mais rápida e exige menos recursos.

Por fim, o Proof-of-Authority, realiza a verificação dos dados por meio de um conjunto restrito de validadores previamente autorizados, Esse modelo proporciona alta escalabilidade uma vez que menos nós são envolvidos. Entretanto, do ponto de vista de segurança da informação o PoA é menos robusto, uma vez que depende da confiança

dos validadores autorizados, ele se torna mais adequado para redes privadas onde a identidade dos validadores servem como garantia de confiabilidade.

Em geral, se observou que o PoW foi mais utilizado em contextos que os autores se preocuparam mais com a segurança do sistema eleitoral. Já os que utilizaram PoA foram mais utilizados em sistemas que focaram mais em desempenho do sistema eleitoral para um grande número de eleitores. PoS foi mais presente em sistemas que utilizam o framework do Ethereum, uma vez que o PoS é o protocolo de consenso nativo do Ethereum e garante uma boa consistência dos dados e escalabilidade.

Tabela 2: Protocolo de Consenso e Escalabilidade

Artigo	Autor	Framework	Escalável
ElectionBlock	Ibrahim et al. 2021	PoW	Sim
DVTChain	Alvi et al. 2021	PoS	Não
AMVChain	Li et al. 2021	PBFT	Possui, para um número relativamente grande de eleitores
A Secure Decentralized E-Voting with Blockchain & Smart Contract	Kumar et al. 2023	PoS PoW	Não
Secure large-scale E-voting system based on blockchain contractusing a hybrid consensus model combined with sharding	Abuidris et al. 2020	Híbrido PSC-Bchain	Sim
Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System	Killer et al. 2020	PoA	Sim
d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting	Zaghloul et al. 2021	PoS	Sim
Blockchain and Aadhaar based Electronic Voting System	Tyagi et. al. 2020	Pos e PoW	Não
Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities	Yang et. al. 2020	PoW	Não

Electronic Voting System Using an Enterprise Blockchain	Gonzalés et. al. 2022	PoC	Sim
A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT	Li et al. 2021	PBFT	Sim
Decentralized E-voting system based on Smart Contract by using Blockchain Technology	Al-madani et. al. 2020	PoW	Não

6.3. Algoritmo de Hashing e Criptografia:

Para assegurar a segurança e anonimato do eleitorado e consistência dos dados são utilizados algoritmos de hashing e criptografia para as mais diferentes finalidades dentro do sistema eleitoral.

6.3.1. Algoritmo de Hashing:

As funções criptográficas de hash são funções unidirecionais, ou seja, não é possível obter a informação original a partir de um hash já calculado. Isso faz com que sejam úteis para alguns usos em cibersegurança como o armazenamento de senhas e integridade de arquivos.

No caso das blockchains, a função mais comum para os algoritmos de hash é a verificação da integridade dos dados armazenados nos blocos da blockchain. Como exemplificado na Figura 1, o hash de cada bloco é calculado a partir das informações armazenadas pelo bloco e pelo hash do bloco anterior, então uma alteração nos dados de um bloco alteraria o seu respectivo hash assim como todos os hash subsequentes, o que possibilita a detecção imediata de falhas no sistema.

Tabela 3: Algoritmo de Hashing

Artigo	Autor	Algoritmo de Hashing
ElectionBlock	Ibrahim et al. 2021	SHA-256
DVTChain	Alvi et al. 2021	SHA-256
A Secure Decentralized E-Voting with Blockchain & Smart Contract	Kumar et al. 2023	SHA-256

Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System	Killer et al. 2020	Keccak-256
d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting	Zaghloul et al. 2021	Keccak-256
A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT	Li et al. 2021	Keccak-256
Decentralized E-voting system based on Smart Contract by using Blockchain Technology	Al-madani et. al. 2020	Keccak-256

A Tabela 3: Algoritmos de Hashing apresenta os algoritmos utilizados nos trabalhos analisados. Em geral, os autores recorreram principalmente a dois tipos: SHA-256 e Keccak-256. Ambos são considerados robustos contra colisões, mas diferenciam-se quanto à eficiência e à classificação: o SHA-256 integra a família SHA-2, enquanto o Keccak-256 é a base do padrão SHA-3, desenvolvido como sucessor do SHA-2 para prevenir possíveis vulnerabilidades futuras. Nesse sentido, os algoritmos da família SHA-3, como o Keccak-256, são considerados mais robustos que os de SHA-2.

O Keccak-256 apresenta desempenho superior, com maior velocidade de hashing, menor número de ciclos por byte e maior volume de dados processados por segundo em comparação ao SHA-256.

Dessa forma, a análise evidencia uma tendência de adoção crescente do Keccak-256 em relação ao SHA-256, devido à sua maior velocidade e robustez, ainda que produza saídas de tamanho superior.

6.3.2. Algoritmo de Criptografia:

Os algoritmos de criptografia citados nos artigos analisados em geral servem para proteger a informação, como o algoritmo ElGamal, ou proteger a identidade do eleitor, como a encriptação em grupo.

O algoritmo ElGamal de encriptação tem como base a resolução de um problema de escala logarítmica que é considerado complexo de resolver, isso faz com que o algoritmo seja eficiente contra ataques. Outro algoritmo de

encriptação utilizado, com menos frequência, foi o RSA que tem como base a fatoração de grandes números primos, é considerado bem seguro contra possíveis ataques.

O algoritmo RSA é mais antigo que o ElGamal e seu uso está mais consolidado em aplicações, entretanto, o ElGamal é um algoritmo probabilístico, ou seja, o mesmo voto pode ser cifrado de maneiras diferentes, isso garante maior anonimato e sigilo do eleitor, em comparação com o RSA o ElGamal possui maior escalabilidade. Além disso, ElGamal é utilizado em esquemas de encriptação homomórfica em que é possível que os votos sejam somados sem descriptografá-los.

A encriptação baseada em grupo (*Group-Based Encryption*) é um esquema criptográfico baseado em compartilhamento secreto, no qual um conjunto de usuários constrói coletivamente as chaves usadas na encriptação. Cada participante escolhe um valor secreto e publica uma parte correspondente. A partir dessas partes públicas, são gerados valores que dependem de todos os demais membros do grupo. A segurança do sistema se baseia na dificuldade do problema da hipótese decisória de Diffie-Hellman (*Diffie-Hellman*), garantindo que nenhum usuário isolado consiga descriptografar ou manipular os dados. Assim, a decriptação ou a agregação correta das mensagens (como a contagem de votos) só pode ser realizada de forma colaborativa, preservando o sigilo individual e assegurando que o resultado final dependa do grupo como um todo.

A Assinatura em anel é um esquema de assinatura digital que permite a um usuário assinar uma mensagem em nome de um grupo, sem revelar qual dos membros efetivamente a assinou. Para verificar a assinatura, basta a chave pública de todos os integrantes do grupo, mas o verificador não consegue distinguir quem foi o autor. Esse mecanismo garante anonimato e autenticidade ao mesmo tempo: sabe-se que a assinatura veio de alguém do grupo, mas não de quem. Em sistemas de votação, por exemplo, isso protege a identidade do eleitor ao mesmo tempo em que confirma que o voto foi emitido por um participante legítimo.

Os algoritmos ElGamal e RSA são utilizados para encriptar a informação, ou seja, em sistemas de blockchain eleitorais são responsáveis pela proteção dos dados da eleição. A partir da análise da Tabela 4: Algoritmo de Criptografia é possível perceber que a encriptação ElGamal foi utilizada mais vezes que a RSA uma vez o ElGamal garante um maior anonimato e sigilo do eleitor, permite a utilização de encriptação homomórfica, assim não é preciso descriptografar o código, além disso, é um algoritmo de escala logarítmica que é mais difícil de resolver quando em comparação com o RSA, assim está mais protegido a possíveis ataques.

A encriptação baseada em grupo e a assinatura em anel, ambas tem o objetivo de preservar a identidade de quem assina determinada informação, assinando em “grupo”, entretanto se diferenciam em como são aplicadas, enquanto a encriptação baseada em grupo precisa de uma autoridade central inicial a assinatura em anel não, portanto, a autoridade central pode rastrear a quem pertence o voto criptografado. Assim, para assegurar maior confiabilidade ao processo eleitoral é mais recomendado o uso da assinatura em anel.

Tabela 4: Algoritmo de Criptografia		
Artigo	**Autor**	**Algoritmo de Criptografia**
AMVChain	Li et al. 2021	Assinatura em anel linkada RSA
Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System	Killer et al. 2020	ElGamal
d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting	Zaghloul et al. 2021	ElGamal
Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities	Yang et. al. 2020	ElGamal e Encriptação baseada em grupo
A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT	Li et al. 2021	ElGamal Zero-Knowledge Proofs

6.4. Tipo de Blockchain:

Existem diferentes tipos de Blockchain que se especificam por suas características e funcionamentos. É importante sempre levar em consideração o tipo de blockchain utilizado pela aplicação, uma vez que pode definir pontos importantes, como permissões que os usuários possuem e centralização do sistema.

A blockchain pública, permite a participação de qualquer parte interessada, ou seja, podem participar, validar e visualizar as transações, e é descentralizada, isso faz com que seja um modelo de alta transparência. Entretanto, a sua velocidade é reduzida à medida que o número de transações e usuários aumenta, e por ser aberta a qualquer usuário o risco à privacidade dos participantes é maior, então é necessário que seja feita uma proteção adicional dos dados.

Blockchains privadas, são restritas e permissionadas, ou seja, para a participação efetiva na blockchain, é necessário que o usuário seja aprovado, isso melhora o controle de acesso a rede e à manutenção da confidencialidade, além disso, como menos nós

participam do protocolo de consenso sua velocidade e consumo de energia são menores, assim se apresentando uma grande escalabilidade. Diferentemente das públicas, blockchains permissionadas são centralizadas em alguns nós que definem regras, estabelecem regras e supervisionam os processos. Apesar disto, a confiança se baseia na entidade controladora da blockchain uma vez que ela realiza todas as ações na rede, isto também pode diminuir a transparência visto que a blockchain pode ser acessível a apenas um grupo seleto de usuários.

Já blockchains híbridas combinam elementos das públicas e privadas, assim é possível reduzir desvantagens de ambos os tipos equilibrando segurança, transparência e eficiência. Neste tipo de blockchain parte da rede é pública, permitindo auditoria, transparência e validação das informações por qualquer participante, e parte é privada, restrita a entidades que são previamente selecionadas. A combinação desses fatores permite que informações dos usuários sejam protegidas e resultados e provas criptográficas sejam tornados públicos, assegurando confiança no processo.

Tabela 5: Tipo de Blockchain

Projeto	Autor	Tipo de Blockchain
ElectionBlock	Ibrahim et al. 2021	Permissionada (Privada)
DVTChain	Alvi et al. 2021	Sem permissão (Pública)
AMVChain	Li et al. 2021	Permissionada (Privada)
Secure large-scale E-voting system based on blockchain contractusing a hybrid consensus model combined with sharding	Abuidris et al. 2020	Híbrida
Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System	Killer et al. 2020	Permissionada (Privada)
Blockchain and Aadhaar based Electronic Voting System	Tyagi et. al. 2020	Permissionada (Privada)

Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities	Yang et. al. 2020	Permissionada (Privada)
Electronic Voting System Using an Enterprise Blockchain	Gonzalés et. al. 2022	Permissionada (Privada)
A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT	Li et al. 2021	Permissionada (Privada)
Decentralized E-voting system based on Smart Contract by using Blockchain Technology	Al-madani et. al. 2020	Permissionada (Privada)

A partir da análise da Tabela 5: Tipo de Blockchain é possível perceber que o tipo de blockchain mais utilizada é a privada uma vez que é utilizado para realizar a filtragem de quais nós serão utilizados para o protocolo de consenso e verificação dos votos, assim a segurança é aumentada uma vez que nós maliciosos não terão acesso à rede, além disso a escalabilidade também é maior quando em comparação às blockchain públicas não permissionadas. A auditabilidade é feita por meio dos nós participantes da blockchain, neste sentido, o ideal seria o uso de blockchains híbridas que permitem que apenas aos nós autorizados, no caso podem ser órgãos ou instituições reguladoras que fazem parte do processo eleitoral, e permite que os eleitores acessem diretamente os dados armazenados na blockchain e verifiquem por meio do hash de seu voto se está de fato armazenado.

7.Conclusão

Esta pesquisa teve por objetivo compreender o estado atual da utilização da blockchain em sistemas eleitorais e comparar suas diferentes aplicações. Os resultados mostram que as pesquisas mais recentes têm priorizado a escalabilidade dos sistemas, aspecto constantemente enfatizado nos artigos analisados. Destaca-se, nesse contexto, o crescente uso do framework Ethereum, principalmente devido aos *smart contracts*, que permitem automatizar tarefas como a verificação da elegibilidade do eleitor e a contagem de votos, tornando o processo mais ágil. Além disso, o protocolo nativo de consenso do Ethereum, o Proof-of-Stake (PoS), oferece maior escalabilidade em comparação ao Proof-of-Work (PoW) utilizado pelo Bitcoin.

No que compete à segurança e criptografia do sistema, o uso dos algoritmos de hash ficou balanceado, uma vez que, o SHA-256 e Keccak-256 são ambos algoritmos robustos, mesmo que o último seja mais avançado e seguro. Já o uso dos algoritmos de

criptografia, foram especificados apenas em alguns dos artigos abordados, para a proteção dos dados armazenados na blockchain se notou um grande uso do algoritmo de criptografia ElGamal, que por ser de escala logarítmica e probabilístico é extremamente robusto à ataques, além de permitir a encriptação homomórfica que permite que os votos sejam contados sem que sejam descriptografados.

Em relação ao anonimato do eleitor, proteção à identidade, os protocolos foram a encriptação baseada em grupo e a assinatura em anel, no caso a assinatura em anel se mostra como a escolha mais ideal para garantir o anonimidade uma vez que na encriptação baseada em grupo é possível rastrear a chave que assinou o voto e assim descobrir a identidade do eleitor.

Este trabalho conseguiu observar as tendências atuais em sistemas eleitorais baseados em blockchain, como o uso de frameworks e protocolos de consenso mais eficientes, algoritmos criptográficos robustos e mecanismos de anonimato que assegurem não apenas a confiabilidade do processo eleitoral, mas também a proteção integral da identidade do eleitor.

Referências

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 16 abr. 2025.

RIVEST, R. et al. On the notion of “software independence” in voting systems. The Royal Society , 3759, 2008.

TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO. *Saiba mais sobre a segurança da urna eletrônica*. 2024. Disponível em: https://www.tre-sp.jus.br/comunicacao/noticias/2024/Outubro/saiba-mais-sobre-a-seguranca-da-urna-eletronica. Acesso em: 1 nov. 2024.

Paul, P et. al., Blockchain Technology and Its Types—A Short Review. In: International Journal of Applied Science and Engineering (IJASE), 2021. pp. 189-200.

Ibrahim, M. et al. ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication. In: 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C), 2021, pp. 123-129, doi: 10.1109/ICSA-C52384.2021.00033.

Alvi, S. et al. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. Journal of King Saud University - Computer and Information Sciences, 6855-6871, 2022.

Li, C. et al. AMVchain: authority management mechanism on blockchain-based voting systems. Peer-to-Peer Networking and Applications, 2801–2812, 2021 doi:10.1007/s12083-021-01100-x.

Abuidris, Y. et al. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding, ETRI Journal, 357 - 370, 2020.

Killer, C. et al. Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System, 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, NSW, Australia, 2020, pp. 172-183, doi: 10.1109/LCN48667.2020.9314815.

Zaghloul, E. et al. d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting, in IEEE Internet of Things Journal, vol. 8, no. 22, pp. 16585-16597, 15 Nov.15, 2021, doi: 10.1109/JIOT.2021.3074877.

Kumar, R. et al. A Secure Decentralized E-Voting with Blockchain & Smart Contracts, 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 419-424, doi: 10.1109/Confluence56041.2023.10048871.

Tyagi, A. K. et al. Blockchain and Aadhaar based Electronic Voting System, 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2020, pp. 498-504, doi: 10.1109/ICECA49313.2020.9297655.

Yang, X. Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities, Future Generation Computer Systems, vol. 112, 2020, pp 859-874, doi: 10.1016/j.future.2020.06.051.

González, D. et al. Electronic Voting System Using an Enterprise Blockchain, Applied Sciences. vol. 12. pp 531. doi: 10.3390/app12020531.

Y. Li et al. A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT, in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 119-130, 2022, doi: 10.1109/TDSC.2020.2979856.

Al-madani, A. M. et al. Decentralized E-voting system based on Smart Contract by using Blockchain Technology, 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 2020, pp. 176-180, doi: 10.1109/ICSIDEMPC49020.2020.9299581.

Pun, K. Y. et al. Comparative Study on Hash Function Algorithms for Blockchain Technology. *Applied Information Technology And Computer Science*, 2024, *5*(1), pp 16-33.

Kuznetsov, O. et al. Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain, International Journal of Computer Network and Information Security. 2021. 13. 1-15. 10.5815/ijcnis.2021.02.01.

Maetouq, A. et al. Comparison of Hash Function Algorithms Against Attacks: A Review. International Journal of Advanced Computer Science and Applications (IJACSA) vol 9. pp 98-103 (2018). http://dx.doi.org/10.14569/IJACSA.2018.090813

Perera, N. et al. A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity, Cryptography, 2022, vol 6, 10.3390/cryptography6010003.

Paul, P. K. et al. Blockchain Technology and its Types-A Short Review, International Journal of Applied Science and Engineering, 2021, vol. 9, pp 189-200.

Mallouli, F. et al. A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms, 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 2019, pp. 173-176, doi: 10.1109/CSCloud/EdgeCom.2019.00022.