



RAFAEL LIMA LOPES CASTELLAN
RIAN NUNES DE FARIA

**ESTUDO SOBRE APLICAÇÃO DE BLOCKCHAIN EM SISTEMAS DE VOTAÇÃO
PELA INTERNET**

**RAFAEL LIMA LOPES CASTELLAN
RIAN NUNES DE FARIA**

**ESTUDO SOBRE APLICAÇÃO DE BLOCKCHAIN EM SISTEMAS DE VOTAÇÃO
PELA INTERNET**

Trabalho de Conclusão de Curso
apresentado ao Centro Universitário
São Lucas Ji-Paraná como requisito
parcial para obtenção do Título de
Bacharel em Sistemas de Informação.

Orientador: Prof. Esp. Wallison Storck
Coelho

Ji-Paraná

2023

Dados Internacionais de Catalogação na Publicação - CIP

C348e Castellan, Rafael Lima Lopes.

Estudo sobre aplicação de blockchain em sistemas de
votação pela internet. / Rafael Lima Lopes Castellan; Rian Nunes
de Faria. – Ji-Paraná, 2023.
28 p.; il.

Trabalho de Conclusão de Curso (Sistemas de Informação)
– Centro Universitário São Lucas Ji-Paraná, 2023.

Orientador: Prof. Esp. Wallison Storck Coelho.

1. Blockchain. 2. Criptografia. 3. Votação. 4. Internet. I.
Faria, Rian Nunes de. II. Coelho, Wallison Storck. III. Título.

CDU 342.843.5:004.422.63

AGRADECIMENTOS

Agradecemos a todos aqueles que foram fundamentais para o desenvolvimento e êxito deste projeto. Expressamos também gratidão ao nosso professor orientador, Wallison Storck Coelho, pela orientação dedicada, apoio constante e valiosas contribuições ao longo de todo o processo de elaboração deste projeto. Sua expertise, paciência e comprometimento foram fundamentais para o desenvolvimento da pesquisa, proporcionando um ambiente propício ao crescimento acadêmico e profissional.

Também gostaríamos de agradecer a todos os professores e profissionais que, de alguma forma, contribuíram para a nossa formação acadêmica. Cada ensinamento e experiência compartilhada foram de grande importância para o amadurecimento e aprimoramento das habilidades necessárias para a realização deste trabalho.

SUMÁRIO

1	INTRODUÇÃO	8
1.1	JUSTIFICATIVA	9
1.2	OBJETIVOS	10
1.2.1	OBJETIVO GERAL	10
1.2.2	OBJETIVOS ESPECÍFICOS	10
2	METODOLOGIA.....	10
3	RESULTADOS E DISCUSSÃO	11
3.1	ELEIÇÕES NO SISTEMA DEMOCRÁTICO	11
3.2	ELEIÇÕES ELETRÔNICAS	12
3.3	COMO FUNCIONA O BLOCKCHAIN	14
3.4	APLICAÇÕES DO BLOCKCHAIN	18
3.5	APLICAÇÃO DO BLOCKCHAIN EM SISTEMAS DE VOTAÇÃO PELA INTERNET	19
3.5.1	FOLLOW MY VOTE	21
3.5.2	VOATZ.....	22
3.5.3	VOTAÇÕES ELETRÔNICAS NA ESTÔNIA.....	23
4	CONCLUSÃO.....	24
5	REFERÊNCIAS BIBLIOGRÁFICAS	26

RESUMO

As eleições desempenham um papel central na democracia, sendo essenciais para a representatividade e legitimidade dos processos eleitorais. A implementação de sistemas de votação eletrônica em muitos países nas últimas décadas visou aprimorar a eficiência e acessibilidade, substituindo métodos tradicionais em papel. No entanto, tais sistemas enfrentam desafios significativos relacionados à segurança, transparência e confiabilidade. Este estudo propõe explorar a aplicabilidade do *blockchain* em sistemas de votação pela internet, buscando compreender como essa tecnologia pode oferecer uma abordagem inovadora para superar os desafios presentes nos sistemas eletrônicos convencionais. A pesquisa se concentra na relação entre o *blockchain* e os princípios democráticos, analisando benefícios, desafios e limitações de sua implementação em votações online. Para o desenvolvimento deste estudo foi realizado uma revisão integrativa da literatura, baseado em estudos acadêmicos que foram publicados nos últimos anos. Os resultados obtidos neste estudo destacam como o *blockchain* pode contribuir para o avanço do processo eleitoral, transformando-o em um sistema mais moderno, confiável e democrático. Sua natureza distribuída, imutável e segura proporciona uma abordagem transparente para o armazenamento e verificação de dados, mitigando preocupações com fraudes e manipulações. Conclui-se que a aplicação do *blockchain* nas eleições online representa uma inovação substancial para superar os desafios existentes nos sistemas eletrônicos tradicionais. No entanto, é fundamental reconhecer que a implantação de um sistema de votação eletrônica fundamentado em *blockchain* exige uma avaliação cuidadosa dos desafios técnicos, regulatórios e de aceitação.

Palavras chave: Blockchain. Criptografia. Votação. Internet.

ABSTRACT

Elections play a central role in democracy, being essential for the representativeness and legitimacy of electoral processes. The implementation of electronic voting systems in many countries in recent decades has aimed to improve efficiency and accessibility, replacing traditional paper-based methods. However, such systems face significant challenges related to security, transparency and reliability. This study proposes to explore the applicability of blockchain in internet voting systems, seeking to understand how this technology can offer an innovative approach to overcoming the challenges present in conventional electronic systems. The research focuses on the relationship between blockchain and democratic principles, analyzing benefits, challenges and limitations of its implementation in online voting. To develop this study, an integrative literature review was carried out, based on academic studies that have been published in recent years. The results obtained in this study highlight how blockchain can contribute to the advancement of the electoral process, transforming it into a more modern, reliable and democratic system. Its distributed, immutable and secure nature provides a transparent approach to data storage and verification, mitigating concerns about fraud and manipulation. It is concluded that the application of blockchain in online elections represents a substantial innovation to overcome the challenges existing in traditional electronic systems. However, it is essential to recognize that implementing a blockchain-based electronic voting system requires careful assessment of technical, regulatory and acceptance challenges.

Keywords: Blockchain. Cryptography. Voting. Internet.

1 INTRODUÇÃO

As eleições desempenham um papel fundamental na democracia, sendo um dos pilares essenciais desse sistema de governo. Elas são o mecanismo pelo qual os cidadãos têm a oportunidade de escolher seus representantes e exercer influência sobre as decisões governamentais, tornando-se um elemento importante para a estabilidade e o progresso em uma sociedade democrática. No processo eleitoral de alguns países utiliza-se sistemas de votação eletrônica. O voto por meio eletrônico traz agilidade na apuração dos resultados, logo quando a votação é encerrada, a contabilização dos votos é feita automaticamente, gerando resultados precisos em tempo reduzido. (RODRIGUES, 2023).

Com a evolução e ampla disseminação da internet, surgiu a oportunidade de adotar o voto remoto, eliminando a necessidade do deslocamento até os locais de votação. Isso não apenas agiliza o processo de votação, mas também proporciona maior comodidade aos eleitores, visto que não há a necessidade comparecer pessoalmente às zonas eleitorais. Através de dispositivos móveis com acesso à internet, os eleitores têm a capacidade de votar em qualquer local e a qualquer instante. A automação desse procedimento se apresenta como uma maneira de simplificar o processo eleitoral, reduzindo o tempo necessário para a apuração dos resultados e diminuindo a incidência de erros. (ADESHINA, 2014).

De acordo com Cetinkaya (2008) assegurar a confiança no processo eleitoral não é uma tarefa simples, devido a possibilidade de manipulação dos votos e resultados. Como medida preventiva, a verificação do voto computado pelo eleitor é de extrema importância, permitindo que ele confirme manualmente que o seu voto foi registrado de maneira correta. Essa forma de verificação ajuda os utilizadores do sistema a terem a certeza de que todo o processo ocorra de forma precisa e segura. Diante disso, a tecnologia *blockchain* surge como uma possibilidade de garantir a integridade dos resultados, a privacidade do eleitor e fornecer ainda mais confiança nas votações pela internet.

Blockchain é uma inovação tecnológica que surgiu em 2008, criado por um pseudônimo chamado Satoshi Nakamoto. Essa tecnologia teve sua primeira aparição em um artigo acadêmico relacionado à *bitcoin*. Nakamoto concebeu a criptomoeda conhecida como *bitcoin*, a qual utiliza o *blockchain* para registrar e distribuir as transações a todos os usuários da rede. Isso promove transparência e a capacidade

de auditar as operações na estrutura.

O propósito fundamental do *blockchain* é criar um registro imutável e protegido por criptografia das transações, organizadas dentro de uma lista encadeada. Essa lista é compartilhada entre todos os integrantes da rede, permitindo que qualquer pessoa tenha acesso ao seu conteúdo. A criptografia garante a privacidade de quem adiciona informações à rede, ao mesmo tempo que possibilita verificar a validade das transações. Essa tecnologia se baseia na rede *peer-to-peer* (P2P), uma arquitetura descentralizada de redes de computadores, na qual cada usuário da rede atua tanto como cliente quanto como servidor, eliminando a utilização de um servidor central (SEPÚLVIDA, 2019).

A criptografia tem um papel fundamental na tecnologia do *blockchain*, pois ela garante a integridade e segurança de dados armazenados e transmitidos pela rede. Isso é feito através de algoritmos criptográficos que protege as transações, impedindo que informações sigilosas sejam acessadas ou alteradas sem autorização. (RODRIGUES, 2023).

Este projeto propõe explorar a aplicabilidade do *blockchain* em sistemas de votação pela internet. Ao longo desta pesquisa, será analisada a relação entre *blockchain* e os princípios democráticos, buscando compreender os principais benefícios, desafios e limitações da aplicação de *blockchain* em sistemas de votação online, além de avaliar o seu potencial para transformar as eleições em um processo gradativamente mais digital.

Este estudo busca contribuir para o avanço do processo eleitoral, ao avaliar como o *blockchain* pode fornecer benefícios na busca por sistemas eleitorais mais modernos, confiáveis e democráticos. Aprofundando o conhecimento sobre a aplicação de *blockchain* em sistemas de votação pela internet.

1.1 JUSTIFICATIVA

O sistema eleitoral é um dos pilares fundamentais de qualquer democracia, e a integridade desse sistema é crucial para assegurar a representatividade e a legitimidade dos processos eleitorais. Nas últimas décadas, muitos países adotaram sistemas de votação eletrônica como uma alternativa à votação em papel, visando aprimorar a eficiência e a acessibilidade das eleições. No entanto, esses sistemas eletrônicos não estão isentos de desafios, como preocupações com segurança,

transparência e confiabilidade. (GRAAF, J. V. 2006).

Nesse contexto, a aplicação da tecnologia *blockchain* nas eleições eletrônicas tem atraído a atenção de especialistas, pesquisadores e formuladores de políticas públicas. O *blockchain*, conhecido por sua natureza distribuída e imutável, tem o potencial de abordar muitos dos problemas enfrentados pelos sistemas de votação eletrônica tradicionais. Essa tecnologia surge como uma solução inovadora que pode oferecer uma abordagem segura e transparente para o armazenamento e verificação dos dados. Sua utilização pode solucionar problemas, como falta de transparência, possíveis fraudes e manipulações, garantindo mais confiança nos resultados.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

O objetivo deste projeto é esclarecer de acordo com a literatura atualizada a aplicabilidade da solução tecnológica *blockchain* em sistemas de votação pela internet.

1.2.2 OBJETIVOS ESPECÍFICOS

- Realizar uma revisão da literatura sobre *blockchain* e eleições eletrônicas;
- Analisar as propriedades do *blockchain* e sua importância nos sistemas de votação eletrônica;
- Examinar os princípios e funcionalidades oferecidas pela tecnologia *blockchain*;
- Apresentar uma visão geral sobre os pontos positivos e negativos da aplicação do *blockchain* em eleições pela internet.

2 METODOLOGIA

Para o desenvolvimento desta pesquisa efetuou-se uma revisão integrativa da literatura, que é um método que possibilita a síntese de conhecimento e a integração da aplicabilidade de resultados de estudos relevantes na prática. As fases desta

revisão integrativa foram: definição do tema e desenho do estudo, critérios para a seleção dos estudos, pesquisa e avaliação dos dados, interpretação dos resultados e produção da revisão. O levantamento dos artigos foram realizados nos principais periódicos indexados na base de dados do Google Acadêmico utilizando-se os descritores: “*blockchain*”, “eleições”, “votação eletrônica”, “votação pela internet”, correspondentes ao idioma do banco de dados consultado. Os critérios de inclusão para a seleção do estudo foram: artigos científicos, incluindo pesquisas originais e revisões, disponíveis eletronicamente, divulgados nas línguas portuguesa, inglesa ou espanhola, em periódicos nacionais e internacionais, entre os anos de 2006 a 2023. Os critérios de exclusão foram artigos em duplicidade, dissertação, teses, resumos, e qualquer um destes que não respondiam à problemática desta pesquisa.

3 RESULTADOS E DISCUSSÃO

3.1 ELEIÇÕES NO SISTEMA DEMOCRÁTICO

Atualmente, destaca-se a relevância do voto como um elemento crucial para o bom funcionamento de sistemas democráticos. Tanto a teoria política quanto a jurídica predominantes reconhecem as eleições em geral, e a ação de votar especificamente, como aspectos essenciais para o crescimento saudável de qualquer sistema que busque ser verdadeiramente democrático. (SILVA, 2018).

Apesar das possíveis críticas em relação a essa perspectiva, é crucial reconhecer que a democracia, em sua essência, implica garantir ao cidadão que sua opinião será ouvida pelos detentores do poder político, agindo em seu nome. Diante a estrutura atual da democracia, predominantemente representativa, é incontestável que o processo eleitoral assume um papel fundamental nesse contexto de representação. (SILVA, 2018).

O Estado brasileiro evidentemente adota essa concepção de democracia, como evidenciado no artigo 1º da Constituição brasileira, que declara que a República Federativa do Brasil é um Estado Democrático de Direito. Essa afirmação é reforçada pelo parágrafo único do mesmo artigo, que estabelece que toda a autoridade se origina pela vontade do povo, sendo exercido através de representantes eleitos ou diretamente, conforme estipulado pela Constituição. Essa perspectiva constitucional é ampliada pelo artigo 14, que enfatiza a soberania popular através do sufrágio

universal e do voto direto e secreto, garantindo igualdade de peso a todos os votos. (SILVA, 2018).

3.2 ELEIÇÕES ELETRÔNICAS

Segundo Rodrigues (2023) o avanço dos procedimentos de votação através do voto eletrônico representa um momento histórico de grande relevância, prometendo uma série de vantagens, como maior transparência, eficiência e segurança, em comparação com os métodos convencionais que se baseiam em cédulas de papel. A concepção de adotar o voto eletrônico ganhou aceitação em várias nações, que implementaram e aprimoraram essa tecnologia ao longo do tempo.

A votação eletrônica abrange o uso de diversos dispositivos eletrônicos, que são conhecidos por Máquinas de Votação Eletrônica – *Electronic Voting Machines* (EVM). Essa abordagem não se limita apenas às urnas eletrônicas, mas também inclui uma variedade de aparelhos tecnológicos, como telefones celulares, computadores e outros dispositivos inteligentes. Além disso, a infraestrutura de comunicação utilizada, como a Internet ou intranet, desempenha um papel crucial nesse processo. (ADESHINA, 2014).

Segundo PIPI (2018) o conceito de *e-voting* refere-se a um processo que permite a solicitação de opiniões sobre questões políticas através da internet, além de viabilizar a tabulação eletrônica de votos em sistemas integrados. Esse processo abrange desde o cadastro dos candidatos, a contagem dos votos até a publicação do resultado final das eleições.

O objetivo central da votação eletrônica é assegurar que ela se assemelhe o máximo possível à votação tradicional, em conformidade com as leis eleitorais e os princípios democráticos. É fundamental que a votação eletrônica ofereça um nível equivalente de segurança e confiança ao processo convencional. Desta maneira, de acordo com as normas eleitorais, o voto eletrônico tem que ser uniforme e sigiloso, com acesso restrito aos registros somente por parte dos eleitores. Na visão técnica, este sistema de voto eletrônico deve ser transparente o suficiente para permitir auditorias por uma ampla gama de especialistas. Além disso, a reutilização do sistema é importante para evitar a necessidade de desenvolver um novo sistema a cada eleição. (PIPI, 2018)

Um dos benefícios desse formato de votação é a redução significativa dos

custos associados à mobilização de funcionários e também locais de votação físicos. Além disso, ele oferece a oportunidade de pessoas com deficiências ou com algum problema de mobilidade possam votar no conforto de suas casas. A infraestrutura que é necessária para conduzir uma votação eletrônica é consideravelmente menor, visto que não há a necessidade de preparar seções ou zonas eleitorais, selecionar mesários, contratar fiscais e auditores. Além disso, busca-se melhorar a confiabilidade e reduzir erros, uma vez que a interação humana, que pode ser sujeita a falhas e tendências, é minimizada. No entanto, há o desafio de desenvolver um sistema que cumpra rigorosamente os requisitos de segurança e, adicionalmente, atenda às regulamentações eleitorais vigentes no país. (PIPI, 2018).

De acordo com Rodrigues (2023), o início do voto eletrônico no Brasil foi a partir de 1996, como registrado pelo Tribunal Superior Eleitoral (TSE). Neste ano, o país iniciou a utilização das urnas eletrônicas para coleta e apuração dos votos. Desde então, o sistema de votação eletrônica tem desempenhado um papel central no cenário eleitoral brasileiro, ganhando reconhecimento como um dos mais evoluídos do mundo.

Figura 1 – Urna Eletrônica



Fonte – TSE (2021)

O procedimento de votação eletrônica no Brasil é realizado da seguinte maneira: os cidadãos se locomovem para seus locais de votação, onde são devidamente identificados através da apresentação de documentos oficiais contendo fotografia. Após essa etapa, eles são direcionados às urnas eletrônicas, onde é feita a realização de seu voto rápido e seguro. Essas urnas possuem um teclado numérico

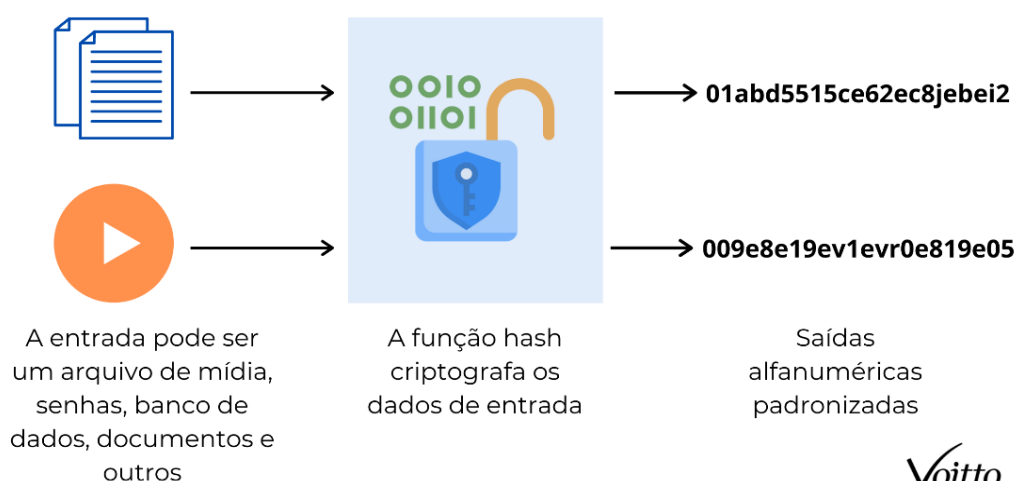
e também uma tela *touch screen*, permitindo que os eleitores façam suas escolhas entre os candidatos que são de sua preferência. Uma vez que confirmam seus votos, os dados são salvos e armazenados diretamente nas próprias urnas. (RODRIGUES, 2023).

A urna eletrônica não possui conexão com a internet ou qualquer sistema de transmissão de dados. Após o encerramento do período de votação, os dados registrados nas urnas são enviados ao TSE por meio de um canal criptografado, onde será realizada a contagem dos votos. A apuração é feita em tempo real e pode ser acompanhada pela internet, no site oficial do TSE. (ABIB, 2019).

3.3 COMO FUNCIONA O BLOCKCHAIN

O *blockchain* na sua tradução literal é denominado de cadeia em blocos, é um registro criptográfico representado em um bloco que transporta o *hash* do bloco anterior assegurando assim a autenticidade deste bloco, a inclusão dos blocos é realizada de modo linear e cronológica. Um *hash* é um conjunto de números e letras, que são produzidos por funções *hash*. A função *hash* é uma função matemática que conduz um número variável de caracteres e o converte em uma série com um número fixo de caracteres. Se for realizada uma pequena alteração em uma série, essa função cria um *hash* completamente novo. (SILVA, 2019).

Figura 2 – Funcionamento da função *hash*

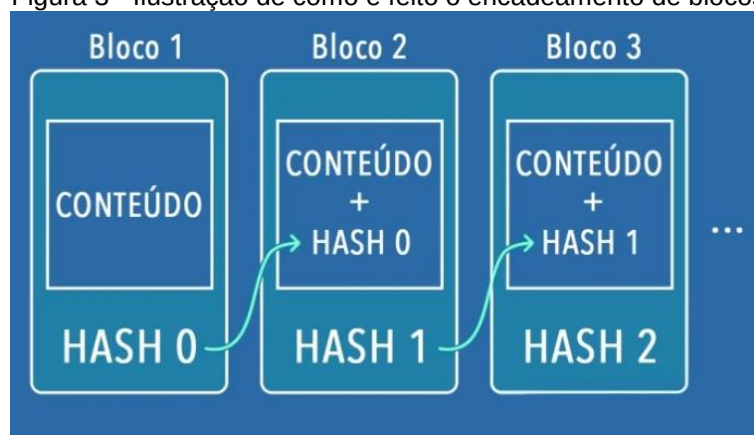


Voitto

Fonte - VALE (2020)

Devido a rede do *blockchain* ser descentralizada, toda vez que uma informação entra na rede, esta é transmitida entre todos os nós da rede, quando um nó deixa a rede, outros nós já têm armazenado uma cópia exata de toda a informação que foi compartilhada. De modo contrário, se um nó entra na rede os nós já existentes imediatamente criam cópias de suas informações para o novo membro. Assim o banco de dados é formado por uma lista de blocos que em conjunto formam uma cadeia, é deste princípio que surge o nome “cadeia em blocos” (*blockchain*). (SILVA, 2019).

Figura 3 - Ilustração de como é feito o encadeamento de blocos



Fonte - RODRIGUES (2023)

Segundo Sepúlveda (2019), dentro da arquitetura do *blockchain*, o bloco inicial é denominado "bloco gênese" por ser o ponto de partida da rede. Cada bloco que contém na rede *blockchain* possui uma estrutura contendo informações importantes sobre a sua criação:

- *Previous Hash* (*Hash Anterior*): Este elemento valida as informações recebidas do bloco anterior, garantindo a integridade da cadeia de blocos.
- *Timestamp* (Carimbo de Data/Hora): Este registro indica o momento cronológico que foi feito a inclusão do bloco à rede, permitindo a ordenação sequencial dos eventos.
- *Data* (Dados): É onde fica armazenada a informação que irá ser registrada no bloco, podendo ser qualquer dado, desde uma simples mensagem até uma transação realizada na rede.
- *Hash* (Valor de *Hash*): Esse valor representa uma identificação única gerada por um algoritmo de mapeamento de dados. Após o cálculo, o *hash* é utilizado como uma espécie de assinatura do bloco, estabelecendo uma conexão matemática com o bloco anterior, criando, assim, a estrutura encadeada e

cronológica que caracteriza o *blockchain*.

- *Nonce* (Valor arbitrário): É um número arbitrário usado apenas uma vez em um algoritmo específico, onde desempenha um papel importante na criação de novos blocos e na segurança da rede. Em um contexto de mineração, o *nonce* é um valor adicionado a um bloco em conjunto com outras informações. O minerador ajusta repetidamente o valor do *nonce* até encontrar um valor que satisfaça os requisitos específicos do algoritmo de consenso da *blockchain*.

Figura 4 - Representação de um bloco na cadeia de blocos

 Genesis Block	
 Previous Hash	0
 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
 Data	Welcome to Blockchain CLI!
 Hash	0000018035a828da0...
 Nonce	56551

Fonte - SEPÚLVIDA (2019)

Cada bloco inserido na rede é submetido a um algoritmo de consenso, onde nenhuma informação inserida pode ser apagada e todas as novas inserções devem ser creditadas por todos. Um novo bloco só pode ser criado e adicionado na rede caso atenda a regra definida no algoritmo, sendo assim, depois que atender à exigência o novo bloco é incluído no *blockchain*, tornando os dados públicos. Essa ação é realizada com o propósito de permitir que a rede opere sem o auxílio de uma autoridade reguladora, isso garante sua independência, pois garante que cada usuário da rede possa verificar a autenticidade de cada bloco e também averiguar se os dados que estão inseridos naquele bloco são autênticos. (SILVA, 2019).

Diversos algoritmos de consenso foram desenvolvidos, cada um com seu objetivo específico. O algoritmo *Proof-of-Work* (PoW), por exemplo, induz a competitividade aos nós que estão conectados na rede *blockchain*, garantindo que um nó tenha executado uma quantidade significativa de trabalho computacional, isso acaba fazendo que o algoritmo torne computacionalmente caro e inviável para um ator malicioso dominar a rede. Em contrapartida, o algoritmo *Proof-of-Stake* (PoS) adota

um método de seleção aleatória para determinar qual nó será encarregado de criar o novo bloco na rede. (SILVA, 2019).

No *blockchain*, há a possibilidade de ser aplicada diferentes técnicas de criptografia, as de destaque são a criptografia assimétrica, também denominada criptografia de chave pública, que faz o uso de pares de chaves, compostos por uma chave privada e uma chave pública. A chave privada é fornecida somente para o proprietário. Em contrapartida, a chave pública é divulgada de maneira pública. Essas chaves estão matematicamente relacionadas de tal maneira que o que é codificado com uma chave somente pode ser decodificado com a outra. (RODRIGUES, 2023).

A criptografia assimétrica desempenha um papel fundamental na garantia da autenticidade e integridade das transações. Quando um remetente assina digitalmente uma transação com sua chave privada, ele pode demonstrar que é o autor da transação, para que os outros nós possam verificar a autenticidade da transação utilizando a chave pública correspondente. (RODRIGUES, 2023).

Figura 5 – Criptografia assimétrica



Fonte - EVAL (2019)

A criptografia *hash*, como já mencionado, é uma função matemática que cria uma sequência de números e letras única e fixa para um determinado conjunto de dados, essa sequência é denominada como resumo criptográfico ou *hash* do dado original. Os *hashes* são utilizados para verificar a integridade dos blocos e dos dados neles contidos. Qualquer modificação nos dados de um bloco resulta em um *hash* completamente diferente. Ao comparar o *hash* calculado de um bloco com o *hash* armazenado no bloco anterior, os nós que estão na rede podem detectar tentativas

de manipulação ou adulteração de dados, invalidando a operação. Além disso, essa criptografia contribui para a segurança das chaves públicas na criptografia assimétrica, reforçando ainda mais a proteção dos dados. (RODRIGUES, 2023).

3.4 APLICAÇÕES DO BLOCKCHAIN

Desde que o *bitcoin* se tornou popular, o *blockchain* normalmente é associado a criptomoedas, já que sua concepção inicial foi incorporada ao projeto de Satoshi Nakamoto. No entanto, apesar do pouco conhecimento, existem adaptações dessa tecnologia para diversos campos, cada uma apresentando suas particularidades. (SEPÚLVIDA, 2019). A seguir serão apresentadas algumas aplicações que o *blockchain* pode fornecer.

Smarts Contracts: Também conhecidos como contratos inteligentes, são algoritmos autônomos que incorporam acordos e regulamentos predefinidos. Sua finalidade está na automatização, verificação e simplificação da realização de transações entre as partes, eliminando a necessidade de intermediários e fortalecendo a confiança nas operações. Esses acordos operam em uma infraestrutura *blockchain*, assegurando a integridade e segurança das operações. (RODRIGUES, 2023).

Cloud Computing: A computação em nuvem representa uma ferramenta que viabiliza o acesso a uma plataforma compartilhada de recursos computacionais configuráveis. Esses recursos podem ser facilmente acessados, transferidos e comunicados através de diversas vias, incluindo redes, servidores, armazenamento em nuvem, aplicativos entre outros meios. Em contrapartida, um banco de dados centralizado, seu custo é mais elevado e possui limitações em termos de capacidade de armazenamento e poder de processamento. (LIMA, 2022).

No contexto da tecnologia de *blockchain* distribuída, mesmo com "nós" que possuem conectividade mínima, a rede permanece segura e confiável. A computação distribuída permite a ampliação da capacidade de computação disponível para suportar bilhões de transações, independentemente da localização dos dispositivos. Considerando as vantagens oferecidas pela tecnologia *blockchain*, a integração do protocolo na computação em nuvem poderia resultar em maior confiabilidade e segurança para um banco de dados descentralizado, ao mesmo tempo em que reduz significativamente os custos envolvidos. (LIMA, 2022).

Identidades Digitais: Bovério (2018) destaca que, devido à resistência a alterações da tecnologia *blockchain*, existe a expectativa de que os identificadores pessoais, como carteira de identidade, passaporte, carteira de motorista, cartão de crédito e outros, alcancem um nível superior de segurança quando aplicadas as características de um *blockchain* a eles. Segundo Gates (2017) essa tecnologia tem potencial para solucionar muitas das atuais vulnerabilidades das identidades digitais. Ele argumenta que a utilização de um sistema de identificação fundamentado em *blockchain* implica na criação de assinaturas digitais que fazem uso de criptografia, características estas que se destacam por serem distintas, irrefutáveis, altamente seguras e praticamente invioláveis, a menos que haja autorização adequada. Portanto, devido à natureza sensível dos dados envolvidos, a tecnologia *blockchain* ofereceria um nível de segurança consideravelmente superior ao atual.

3.5 APLICAÇÃO DO BLOCKCHAIN EM SISTEMAS DE VOTAÇÃO PELA INTERNET

A aplicação do *blockchain* nas eleições eletrônicas tem emergido como um campo de pesquisa e desenvolvimento de relevância crítica, com o potencial de aprimorar substancialmente a segurança, a transparência e a confiabilidade dos processos eleitorais de acordo com os estudos de Wolf et al. (2011). Esta uma tecnologia de registro distribuído imutável e resistente a adulterações, oferece uma série de características intrinsecamente alinhadas com os desafios enfrentados nos sistemas de votação eletrônica. Este referencial teórico oferece uma análise aprofundada dos principais conceitos e implicações dessa aplicação revolucionária.

Entretanto, a implementação bem-sucedida do *blockchain* nas eleições eletrônicas requer uma abordagem cuidadosa. Questões de acessibilidade, privacidade, custos e regulamentações devem ser consideradas minuciosamente. É imperativo garantir que todos os eleitores tenham acesso às ferramentas necessárias para participar das eleições eletrônicas, enquanto simultaneamente preservam a privacidade do voto (VALIMISED, 2019). Além disso, custos significativos e complexidades associadas à infraestrutura de *blockchain* e à atualização de regulamentações eleitorais podem ser obstáculos substanciais como:

- Acesso à tecnologia: Garantir que todos os eleitores tenham acesso à tecnologia necessária para votar eletronicamente é fundamental. Isso pode

excluir pessoas que não têm acesso à internet ou a dispositivos eletrônicos.

- Custos e complexidade: A implantação de sistemas de votação baseados em *blockchain* pode ser cara e complexa. É necessário considerar o custo e a infraestrutura necessários.
- Legislação e regulamentação: As leis eleitorais e regulamentações precisam ser atualizadas para acomodar a tecnologia *blockchain*.

Em comparação com os métodos tradicionais de votação, o *e-voting* é mais amigável para o meio-ambiente, mais fácil para os eleitores, tem contagem de votos em tempo real e menos suscetível a erros. (LIU, 2017).

Com a votação eletrônica utilizando *blockchain*, uma boa parte do processo comum nos dias de hoje, não faria sentido, pois ao final de cada voto, o sistema inicia uma transação que utiliza uma *public key* para criptografar os dados. Depois, os dados referentes ao voto são encaminhados para os outros eleitores conectados a ele, de modo que todas as pessoas na rede recebem a informação do voto. Após a validação do nó, a informação é replicada para os outros nós da rede. (LIU, 2017).

Assim como Pawlak (2018) consideram a votação pela Internet como o quarto tipo de sistema eletrônico para votação, essa tecnologia distribui os dados inseridos (no caso da nossa abordagem, o voto) para milhares, dependendo da dimensão da votação, para milhões de computadores globalmente, tornando praticamente impossível que os dados sejam alterados ou excluídos uma vez que forem inseridos. Essa abordagem aumenta muito a confiança dos eleitores e do governo, garantindo a privacidade e a integridade dos dados. A grande vantagem é que não é necessário o deslocamento da população para zonas/seções eleitorais, visto que qualquer aparelho com conectividade à internet e suporte a aplicações *web* seria suficiente para realizar o seu voto.

Os resultados são processados automaticamente pelo sistema e garantem o anonimato. Cada eleitor pode conferir se seu voto foi computado, mas não é possível verificar em qual candidato foi votado para proteção do próprio eleitor, evitando assim que seja coagido a votar em algum candidato. O *blockchain* fornece esse papel em sua forma original, eliminando a necessidade de um agente intermediador para a eleição, e aumenta a confiabilidade e a integridade do voto inserido no sistema. (PAWLAK, 2018).

De acordo com Liu (2017) uma votação adotando o *blockchain* como tecnologia deve satisfazer algumas condições para que ocorra sem problemas:

- Verificação pública: Todos os envolvidos podem ver o andamento da eleição e, ao final dela, podem verificar os resultados.
- Verificação Individual: Todos os envolvidos podem verificar se seu voto foi computado.
- Privacidade: Os votos, uma vez no *blockchain*, não possuem conexão com seu eleitor.
- Transparência do processo: Todos os participantes podem consultar se outro eleitor já votou, porém sem conseguir ver em quem ele escolheu.
- Não duplicidade: Cada eleitor poderá inserir seu voto somente uma vez.
- Elegibilidade: Essa propriedade garante que apenas os votantes elegíveis devem ter a permissão de votar. Uma técnica básica para garantir isso é a autenticação.

3.5.1 FOLLOW MY VOTE

Follow My Vote é uma organização de utilidade pública dos Estados Unidos. Foi fundada em 2012 e se baseia nos valores da verdade e liberdade. Essa organização assumiu o desafio de aprimorar a integridade dos sistemas de votação utilizados em processos eleitorais pelo mundo. (FOLLOWMYVOTE, 2012).

De acordo com Rodrigues (2023) o *Follow My Vote* é um projeto dedicado à criação de uma plataforma segura de votação online, com o propósito principal de promover a transparência em processos eleitorais. Seus idealizadores acreditam que o *blockchain*, já amplamente reconhecido por garantir a segurança em transações financeiras pelo mundo, pode ser aplicada com sucesso para proteger a integridade dos votos.

Essa aplicação vai além de realizar o voto pela internet, trata-se de um programa de código aberto, o que implica que qualquer cidadão pode examinar seu código-fonte. O sistema utiliza um método de criptografia de pares de chaves para permitir que cada eleitor emita seu voto. Quando um voto é confirmado, ele é imediatamente registrado na urna através do *blockchain*. O *Follow My Vote* oferece a capacidade de verificar se o voto foi registrado através de busca em registros públicos da rede, utilizando a chave criptografada do eleitor (RODRIGUES, 2023).

Para fazer uso desse sistema, é necessário instalar um *software* em um dispositivo, podendo ser um computador ou um celular que irá fazer a função de uma

cabine de votação virtual. O sistema realiza uma verificação digital da identificação do eleitor e disponibiliza uma cédula de votação virtual. Após o preenchimento da cédula, é feita a realização voto pelo eleitor no sistema, e o *blockchain* é empregado para garantir a segurança dos dados. Adicionalmente, os utilizadores do sistema, ou seja, os eleitores, têm a opção de verificar se o voto foi corretamente cadastrado na urna, além de conduzir uma auditoria nos outros votos presentes, mantendo em sigilo as identidades dos demais eleitores (RODRIGUES, 2023).

3.5.2 VOATZ

Nas eleições de 2018 no estado da Virgínia Ocidental, foi proposto a utilização do sistema de votação eletrônica *Voatz* como uma alternativa inovadora às urnas eletrônicas. Seu objetivo era aprimorar a integridade, eficiência e transparência do processo eleitoral através da utilização de tecnologia *blockchain* para registrar os votos dos cidadãos. Contudo, para garantir a segurança do sistema, é preciso dispor de um dispositivo móvel equipado com leitura biométrica e reconhecimento facial por parte do eleitor. (ZHANG, 2018).

No entanto, essas especificações técnicas criaram um desafio substancial, uma vez que a disponibilidade desses recursos varia consideravelmente entre os dispositivos móveis disponíveis no mercado. Como resultado, a acessibilidade do aplicativo *Voatz* foi impactada, limitando seu alcance a um público mais restrito. (ZHANG, 2018).

Após o registro dos votos, as transações, que representam os votos de cada eleitor, tornam-se permanentes e são armazenadas de maneira segura na estrutura de *blockchain* do aplicativo *Voatz*. Depois da finalização do processo de votação, os eleitores recebem automaticamente um recibo digital, o qual é assinado eletronicamente e contém as escolhas de candidatos feitas por eles durante a votação. Esse recibo tem a utilidade para fins de verificação do voto, proporcionando a capacidade de realizar auditorias pós-eleitorais ao compará-lo com as informações registradas no *blockchain*. A utilização deste método garante a integridade e também a transparência do processo eleitoral de maneira efetiva. (RODRIGUES, 2023).



Fonte – VOATZ (2023)

3.5.3 VOTAÇÕES ELETRÔNICAS NA ESTÔNIA

De acordo com Rodrigues (2023), em 2005 foi implementado um sistema de voto eletrônico na Estônia, permitindo que seus habitantes votassem de maneira remota. Para garantir ainda mais a integridade e a confiança, foi realizada a aplicação da tecnologia *blockchain* nesse sistema de votação.

O serviço público de votação pela Internet na Estônia oferece aos seus eleitores a oportunidade de participar de forma totalmente digital das eleições eleitorais através de seus próprios dispositivos, utilizando a conexão à internet, dentro de um determinado período de votação estabelecido. Nesse tipo de votação, a Estônia utiliza um Cartão de Identidade (*ID-card*), que é uma espécie de carteira de identidade nacional. Esse cartão tem um chip criptográfico, o que significa que possui recursos de uma infraestrutura chamada de Infraestrutura de Chaves Públicas (ICP). Todos os residentes do país são obrigados a ter esse cartão. Basicamente, para identificar cada eleitor, é necessário usar o cartão, que está conectado a um conjunto especial de chaves criptografadas. Isso torna o processo seguro e personalizado para cada pessoa. (HEIBERG, 2014).

Segundo Rodrigues (2023), vale destacar que esse sistema de votação na Estônia não tira a possibilidade inteiramente das opções de votações tradicionais, como por exemplo, o voto em papel. Os eleitores possuem a liberdade de escolher

entre votar de forma presencial em sua seção eleitoral ou usar o sistema de votação pela internet. Diante disso, a Estônia apresenta como o *blockchain* pode fornecer benefícios substanciais ao sistema eleitoral, melhorando a segurança, a eficiência e a transparência. A aplicação dessa tecnologia tem o potencial de mudar a forma de como as eleições podem ser conduzidas, proporcionando uma nova perspectiva para assegurar a participação e a confiança do eleitor.

Nas eleições de 2019, quase metade dos eleitores (43,75%) escolheu votar de forma online. Em 2021, a votação pela internet aumentou ainda mais, atingindo 47%, enquanto a votação tradicional foi de 53%. Pela primeira vez, nas eleições parlamentares de 2023, o uso da votação online superou o uso de cédulas de papel, indicando um crescimento notável nesse sistema de votação. (LIMA, 2023).

Algumas pessoas enfrentaram dificuldades ao usar esse tipo de votação, algo parecido com o que ocorre no Brasil. Questões como condições sociais e econômicas, bem como habilidades para lidar com computadores e celulares, criaram obstáculos para os eleitores. Isso muitas vezes resultou na escolha do método tradicional de votação. (PIPI, 2018).

4 CONCLUSÃO

Este estudo teve o objetivo de explorar a aplicabilidade do *blockchain* em sistemas de votação pela internet, buscando compreender como essa tecnologia pode oferecer uma abordagem inovadora para superar os desafios presentes nos sistemas eletrônicos convencionais.

A tecnologia *blockchain*, com seus princípios de descentralização, imutabilidade e transparência, apresenta potencial para aprimorar ainda mais a integridade e a segurança das eleições eletrônicas. Ao garantir a autenticidade e a inviolabilidade dos registros, o *blockchain* pode abordar desafios como a verificação de votos, a privacidade do eleitor e a prevenção de fraudes.

No entanto, para uma implementação do *blockchain* em sistemas de votação pela Internet obter sucesso é será necessário cuidado e consideração de vários fatores, incluindo acessibilidade, privacidade, custos e regulamentações. É crucial garantir que todos os eleitores tenham acesso à tecnologia necessária, enquanto os custos e as complexidades associadas à infraestrutura de *blockchain* devem ser cuidadosamente avaliados.

Aplicações específicas do *blockchain* em sistemas de votação eletrônica, como o projeto *Follow My Vote* e o sistema *Voatz*, demonstram como a tecnologia pode ser incorporada para promover transparência, segurança e verificabilidade nos processos eleitorais. Além disso, experiências como a implementação do voto eletrônico na Estônia destacam como o *blockchain* pode ser integrado de maneira eficaz em sistemas democráticos, oferecendo aos eleitores opções flexíveis sem comprometer a segurança.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ABIB, Fellipe Ribeiro Silva. **O USO DO BLOCKCHAIN PARA ELEIÇÕES ELETRÔNICAS**. 2019.

ADESHINA, Steve A.; OJO, Adegboyega. **Design imperatives for e-voting as a sociotechnical system**. In: 2014 11th International Conference on Electronics, Computer and Computation (ICECCO). IEEE, 2014. p. 1-4.

BOVÉRIO, Maria Aparecida; DA SILVA, Victor Ayres Francisco. **Blockchain: uma tecnologia além da criptomoeda virtual**. Revista Interface Tecnológica, v. 15, n. 1, p. 109-121, 2018.

CETINKAYA, Orhan. **Analysis of security requirements for cryptographic voting protocols**. In: 2008 Third International Conference on Availability, Reliability and Security. IEEE, 2008. p. 1451-1456.

EVAL, E. **Criptografia e gerenciamento de chaves - Conceitos Importantes**. Disponível em: <<https://eval.digital/criptografia-e-gerenciamento-de-chaves-conceitos-importantes/>>. Acesso em: 21 de novembro de 2023.

FOLLOWMYVOTE. FollowMyVote. [S. l.], 2012. Disponível em: <<https://followmyvote.com>>. Acesso em 27 de outubro de 2023.

GATES, Mark. **Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money**. Breinigsville, Pensilvânia: Createspace Independent Publishing Platform. 2017. 126 p.

GRAAF, Jeroen Van. **O mito da urna: desvendando a (in)segurança da urna eletrônica**.

HEIBERG, Sven; WILLEMSON, Jan. **Verifiable internet voting in Estonia**. In: 2014 6th international conference on electronic voting: Verifying the vote (evote). IEEE, 2014. p. 1-8.

LIMA, Fábio Monteiro Santos et al. **Voto on-line: possibilidades e limites à luz dos princípios democráticos**. 2023.

LIMA, Reynaldo Dezen et al. **BLOCKCHAIN: conceito e aplicações**. 2022.CC BY-NC-ND - Belo Horizonte, 2006.

NASCIMENTO, Marshall Moshe Mauricio do. **Blockchain: uma nova abordagem sobre votação eletrônica**. 2018.

PAWLAK, Michał; GUZIUR, Jakub; PONISZEWSKA-MARAÑDA, Aneta. **Voting process with blockchain technology: auditable blockchain voting system**. In: Advances in Intelligent Networking and Collaborative Systems: The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018). Springer International Publishing, 2019. p. 233-244.

PIPI, Filippi Luigi di; YOGUI, Wellington Kazunari Zambelli. **Panorama da utilização de blockchain em votações eletrônicas e suas implicações para o Brasil**. 2020.

RODRIGUES, Luiz Guilherme Villa Verde Costa et al. **A aplicabilidade da tecnologia blockchain em sistemas de votações eletrônicas: uma revisão de literatura**. 2023.

SEPÚLVIDA, Felipe Rabelo; PAIVA, Cláudio Eduardo. **Um estudo sobre o uso da tecnologia Blockchain para votação eletrônica**. 2019.

SILVA, Matheus Passos. **A segurança da democracia e a blockchain**. *Projeção, Direito e Sociedade*, v. 9, n. 1, p. 119-138, 2018.

Tribunal Superior Eleitoral (TSE). (2021). Histórico das Eleições. Disponível em: <<http://www.tse.jus.br/eleicoes/historico-das-eleicoes>>. Acesso em: 27 de outubro de 2023.

VALIMISED. **Principles of checking an i-vote with a smart device**. Estônia, 2019.

VALE, Sávio. **Confira a definição, funcionamento e aplicações do Hash, função popular da criptografia**. Disponível em <<https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona>>. Acesso em 27 de outubro de 2023.

Voatz - Apps on Google Play. Disponível em: <https://play.google.com/store/apps/details?id=com.voatz.vma&hl=en_US>. Acesso em: 29 nov. 2023.

WOLF, Peter; NACKERDIEN, Rushdi; TUCCINARDI, Domenico. **Introducing electronic voting: essential considerations**. *International Institute for Democracy and Electoral Assistance*, 2011.

LIU, Yi; WANG, Qi. **An e-voting protocol based on blockchain**. *Cryptology ePrint Archive*, 2017.

ZHANG, Joyce; YOUNG, Andrew; VERHULST, Stefaan. **Addressing Voting Inefficiencies Resulting from Identity Challenges with Blockchain**. 2018.