UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE SOBRAL

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E COMPUTAÇÃO

MESTRADO ACADÊMICO EM ENGENHARIA ELÉTRICA E COMPUTAÇÃO

CARLOS JEFFERSON SOARES ARAÚJO

PREVENÇÃO DE COERÇÃO EM SISTEMAS DE VOTAÇÃO ELETRÔNICA BASEADOS EM BLOCKCHAIN: UMA REVISÃO SISTEMÁTICA

SOBRAL

2024

CARLOS JEFFERSON SOARES ARAÚJO

PREVENÇÃO DE COERÇÃO EM SISTEMAS DE VOTAÇÃO ELETRÔNICA BASEADOS EM BLOCKCHAIN: UMA REVISÃO SISTEMÁTICA

Dissertação apresentada ao Curso de Mestrado Acadêmico em Engenharia Elétrica e Computação do Programa de Pós-Graduação em Engenharia Elétrica e Computação da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia de Computação. Área de Concentração: Engenharia de Computação

Orientador: Prof. Dr. Antonio Emerson Barros Tomaz

SOBRAL

2024

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A688p Araújo, Carlos Jefferson Soares.
Prevenção de coerção em sistemas de votação eletrônica baseados em Blockchain: Uma revisão sistemática / Carlos Jefferson Soares Araújo. – 2024.
47 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Campus de Sobral, Programa de Pós-Graduação em Engenharia Elétrica e de Computação, Sobral, 2024.
Orientação: Prof. Dr. Antonio Emerson Barros Tomaz.

1. Blockchain. 2. Votação Eletrônica. 3. Coerção. 4. Processo Eleitoral. I. Título.

CDD 621.3

CARLOS JEFFERSON SOARES ARAÚJO

PREVENÇÃO DE COERÇÃO EM SISTEMAS DE VOTAÇÃO ELETRÔNICA BASEADOS EM BLOCKCHAIN: UMA REVISÃO SISTEMÁTICA

Dissertação apresentada ao Curso de Mestrado Acadêmico em Engenharia Elétrica e Computação do Programa de Pós-Graduação em Engenharia Elétrica e Computação da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia de Computação. Área de Concentração: Engenharia de Computação

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Antonio Emerson Barros Tomaz (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Iális Cavalcante de Paula Júnior
Universidade Federal do Ceará (UFC)

Prof. Dr. Fischer Jônatas Ferreira
Universidade Federal de Itajubá (UNIFEI)

Prof. Dr. Allysson Allex de Paula Araújo
Universidade Federal do Cariri (UFCA)

À minha esposa, minha família e meus amigos que sempre estiveram comigo nessa vida. Obrigado!

AGRADECIMENTOS

À Deus, que por sua tamanha graça me salvou e me deu a eternidade nos olhos. Tudo por Ele e para Ele.

Aos meus pais, irmãos e amigos que deixaram a suas marcas neste ser vivente. Amo cada um de vocês e desejo sempre ter perto de mim.

À minha linda esposa. Seu amor e seu cuidado sempre me fizeram ir cada vez mais longe. Seu perdão e seu amor sempre me deram combustível para perseguir o melhor e prover da melhor forma possível ao nosso doce lar.

Ao Prof. Dr. Antonio Emerson Barros Tomaz por me orientar em minha dissertação de mestrado e sempre apontar o melhor caminho com muita atenção.

Ao Doutorando em Engenharia Elétrica, Ednardo Moreira Rodrigues, e seu assistente, Alan Batista de Oliveira, aluno de graduação em Engenharia Elétrica, pela adequação do *template* utilizado neste trabalho para que o mesmo ficasse de acordo com as normas da biblioteca da Universidade Federal do Ceará (UFC).

“Well, whatever happens...happens.”

(Spike Spiegel)

RESUMO

A Blockchain é uma tecnologia que está sendo largamente utilizada em diversos contextos para resolução de numerosos problemas. Um exemplo disso é que a Blockchain está presente em sistemas eleitorais eletrônicos. Qualquer processo eleitoral possui diversas propriedades que devem ser satisfeitas. Desde a etapa de credenciamento e identificação, passando pelo momento de votar até o período de pós-eleição, muitas ameaças à integridade do processo eleitoral são possíveis de ocorrer. Com isso, sistemas eleitorais informatizados podem tomar vantagem das propriedades da Blockchain. Uma das ameaças a um determinado sistema eleitoral se dá através da coerção, que ocorre quando um indivíduo induz ou pressiona alguém a fazer algo pela força, intimidação ou através da ameaça. O propósito principal deste trabalho é identificar que métodos são utilizados para inibir a coerção em sistemas de votação eletrônica que utilizam a Blockchain. Para atingir esse objetivo, uma revisão sistemática da literatura foi realizada, seguindo as premissas do protocolo PRISMA. A literatura foi acessada e selecionada a partir das seguintes bases de dados: SCOPUS, IEEE Xplore e Springer Link. 25 foram escolhidos para compor o grupo dos estudos primários. O cenário atual da literatura indica que as características da Blockchain se encaixam como soluções para muitos desafios de sistemas eleitorais, pricipalmente quanto a robustez e confiança do sistema. O futuro das eleições terá como uma das protagonistas a Blockchain e os sistemas atenderão as principais demandas de um sistema de votação eletrônica.

Palavras-chave: Blockchain; Votação Eletrônica; Coerção; Processo Eleitoral.

ABSTRACT

Blockchain is a technology that is being widely used in various contexts to solve numerous problems. In this sense, Blockchain is present in electronic voting systems. Any electoral process has several properties that must be satisfied. From the accreditation and identification stage, through the voting phase, to the post-election period, many threats to the integrity of the electoral process can occur. Consequently, computerized electoral systems can leverage the properties of the Blockchain. One of the threats to a specific electoral system arises through coercion, which occurs when an individual induces or pressures someone to do something through force, intimidation, or threats. The main purpose of this study is to identify methods used to inhibit coercion in electronic voting systems that utilize Blockchain. To achieve this goal, a systematic literature review was conducted according to the principles of the PRISMA protocol. The literature was accessed and selected from the following databases: SCOPUS, IEEE Xplore, and Springer Link. 25 articles were chosen for analysis. The analyses of this literature indicate that the characteristics of Blockchain align as solutions to many challenges of electoral systems, especially regarding the robustness and reliability of the system. The future of elections will have Blockchain as one of the protagonists, and the systems will meet the key demands of an electronic voting system.

Keywords: Blockchain; E-voting; Coercion; Electoral Process.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

PoW	*Proof of Work*
PoS	*Proof of Stake*
PBFT	*Pratical Byzantine Fault Tolerance*
DKG	Distributed Key Generation
zkSNARKs	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
DoS	*Denial of Service*
SPF	*Single Point of Failure*

SUMÁRIO

1 INTRODUÇÃO

Em qualquer sociedade democrática, votar é um estimado símbolo de liberdade e um meio de mostrar a vontade da população de forma clara e decisiva. De forma geral, o processo de votação pode ser resumido em poucos passos para sua realização: indicação de candidatos disponíveis, registro da intenção de voto dos eleitores, contagem dos votos e finalização do processo eleitoral (Chaeikar *et al.*, 2021). À primeira vista, o processo anteriormente descrito pode parecer simples porém, para que um sistema eleitoral seja efetivamente implementado, é necessário satisfazer uma lista de requisitos por se tratar de algo tão crítico para a preservação de uma sociedade justa.

O avanço da tecnologia da informação e, mais recentemente, da tecnologia Blockchain têm impulsionado o desenvolvimento de sistemas de votação eletrônica. A Blockchain é um livro-razão distribuído mantido por um conjunto de nós de uma rede *peer-to-peer (P2P)*, que, por meio de um mecanismo de consenso, garantem a validade e integridade das transações. O livro-razão construído pela rede Blockchain é, geralmente, público e utiliza primitivas criptográficas para garantir que as transações já registradas não podem ser alteradas ou deletadas. Portanto, a Blockchain pode ser vista como um base de dados distribuídos em que apenas novas transações podem ser adicionadas. Essa ideia foi introduzida em 2008 pelo pseudônimo Satoshi Nakamoto, em que este criou o Bitcoin para criação de um sistema monetário decentralizado no contexto financeiro (Nakamoto, 2008).

Os blocos na rede Blockchain carregam informações que foram mutuamente validadas entre os nós da Blockchain, inserindo estas informações no *ledger*, isto é, determinando quem possui aquela informação na rede (Christidis e Devetsikiotis, 2016). O forte interesse dos pesquisadores e indústria pela Blockchain é justificado pelas diversas vantagens que essa tecnologia oferece, tais como segurança, transparência, imutabilidade, entre outras.

Embora a tecnologia Blockchain tenha sido inicialmente aplicada a criptomoedas e se tornado famosa por isso, as aplicações que estão sendo investigadas e implementadas usando essa tecnologia são inúmeras e nos mais diversos campos (Casino *et al.*, 2019). O principal motivo para este fenômeno decorre da utilização de características da Blockchain que são úteis para implementação, como por exemplo, a característica de ser decentralizada, imutável, entre outras. De modo relativamente recente, os estudos sobre a aplicação da Blockchain em sistemas de votação eletrônica têm ganhado força e envolvido diversos tópicos de estudos, tanto que já existem alguns países, como por exemplo Estônia, Coreia do Sul e outros que se utilizam de um

sistema eleitoral onde a Blockchain é empregada (Vladucu *et al.*, 2023).

A crescente demanda por mecanismos mais robustos que assegurem a transparência e a proteção do processo eleitoral é um tema crítico que as autoridades eleitorais precisam enfrentar de forma contínua. Nesse contexto, pesquisas e avanços constantes em criptografia e verificação de integridade utilizando a tecnologia Blockchain surgem como soluções que atendem de forma eficaz essa demanda no que se refere aos processos eleitorais.

Os sistemas de votação eletrônica enfrentam diversos desafios, tais como a garantia de privacidade, a resistência à fraude, a obtenção de evidências, a facilidade de uso, a escalabilidade, a velocidade e a contenção de custos (Garg *et al.*, 2019). Muitos desses desafios podem ser superados por meio da implementação da Blockchain, visto que algumas de suas propriedades, como a integridade, a disponibilidade, a transparência e a acessibilidade, são inerentes a essa tecnologia (Chaeikar *et al.*, 2021). Portanto, a Blockchain tem o potencial de se tornar uma solução conveniente para os sistemas de votação.

Diante do apresentado, uma revisão sistemática se torna útil para analisar a fundo as lacunas e limitações presentes em uma determinada área de estudo. Para obter um trabalho de revisão sistemática rigoroso e aplicar ao tema de pesquisa deste trabalho, faz-se necessária uma metodologia igualmente rigorosa. Isto posto, este trabalho seguiu o protocolo PRISMA. O protocolo PRISMA auxilia os pesquisadores para uma melhor apresentação de revisões sistemáticas ou meta-análises, dado que é fundamentado em uma pergunta objetiva, empregando métodos detalhados e claros, e possibilitando a identificação, seleção e avaliação crítica das pesquisas mais relevantes sobre determinado tema a ser estudado (Shamseer *et al.*, 2015).

1.1 Declaração do problema e questões de pesquisa

Um dos problemas enfrentados nos processos eleitorais é o da coerção. Coerção ocorre quando um eleitor é coagido, isto é, induzido ou pressionado por alguém a fazer algo pela força, intimidação ou através da ameaça, que neste caso é impelir o votante a escolher uma opção que não é o seu intento (Juels *et al.*, 2005). Neste contexto, um sistema de votação eletrônico é tido como resistente à coerção quando o agente da coerção não pode determinar nem influenciar o voto de um eleitor e, adicionalmente, é incapaz de forçar a abstenção de voto de um eleitor. A coerção é particularmente complexa de abordar em sistemas eleitorais eletrônicos, incluindo aqueles que empregam tecnologia Blockchain. Sua devida mitigação é fundamental para conferir a credibilidade e robustez necessárias a tais sistemas.

Dado que este tópico é relativamente recente na literatura, a quantidade de pesquisas que exploram a aplicação da tecnologia Blockchain em sistemas de votação eletrônica, com foco na prevenção da coerção, ainda é limitada. Observando este cenário, uma revisão sistemática se faz útil para buscar lacunas e limitações nestes estudos e, assim, trazer luz a possíveis soluções para estas deficiências da área. Este trabalho propôs-se a abordar as seguintes questões de pesquisa (QP) derivadas do problema enunciado:

- **QP1.** Quais mecanismos são usados para prevenir a coerção em sistemas de votação eletrônica baseados em Blockchain?
- **QP2.** Qual é a eficácia dos mecanismos de prevenção de coerção em sistemas de votação eletrônica baseados em Blockchain?

1.2 Objetivo geral

Identificar e analisar os métodos mais recentes para prevenir a coerção em sistemas de votação eletrônica baseados em Blockchain.

1.3 Objetivos específicos

- Apresentar uma revisão bibliográfica dos métodos mais recentes para prevenir a coerção em sistemas de votação eletrônica baseados em Blockchain.
- Identificar os diferentes tipos de coerção que podem ocorrer em sistemas de votação eletrônica baseados em Blockchain.
- Identificar as limitações dos métodos existentes na literatura.
- Analisar como a Blockchain é empregada na solução do problema de coerção.

1.4 Organização do trabalho

O Capítulo 2 apresenta uma base teórica que explora os conceitos relacionados a Blockchain, votação eletrônica e coerção. O Capítulo 3 descreve os procedimentos metodológicos adotados para atingir os objetivos estabelecidos neste estudo. No Capítulo 4 mostra uma análise das publicações sobre o tema, apresentando os resultados da pesquisa e a discussão em torno desses resultados. Por fim, o Capítulo 5 apresenta as conclusões deste trabalho e suas considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são abordados os conceitos de Blockchain, votação eletrônica e coerção, os quais serviram como fundamentos para alcançar os objetivos deste trabalho.

2.1 Blockchain

A Blockchain é um sistema de registros distribuído que opera por meio de uma rede *peer-to-peer* (P2P) composta por diversos nós, os quais, por meio de um processo de consenso, asseguram a autenticidade e integridade das transações (Nakamoto, 2008) . Dessa forma, a Blockchain pode ser entendida como um banco de dados distribuído no qual apenas novas transações podem ser acrescentadas. O registro mantido pela rede Blockchain é, em maior parte, de acesso público e emprega técnicas criptográficas para garantir a imutabilidade das transações previamente registradas.

A Blockchain pode ser classificada em três categorias baseado no modo como é administrada, a saber: Blockchain pública, privada ou híbrida. Na Blockchain pública, qualquer um pode se juntar à rede, isto é, o participante pode ler, escrever dados na rede ou participar dela. A rede Blockchain pública é decentralizada, ninguém tem controle total sobre a rede e os participantes possuem a garantia de que os dados não podem ser mudados uma vez que foram validados. No caso da Blockchain privada, há restrições sobre quem pode participar da rede e que tipo de transações podem ser feitas por uma entidade. Por último, a Blockchain híbrida somente possui restrições sobre os participantes da rede (Al-Maaitah *et al.*, 2021).

Muitos autores costumam categorizar a Blockchain em versões. No livro de Swan (2015), tem-se:

- *Blockchain 1.0*. Abordagem de soluções focadas em transações monetárias decentralizadas, contexto em que foi desenvolvido o *Bitcoin*.
- *Blockchain 2.0*. Se destina à descentralização dos mercados de forma mais geral e contempla a transferência de muitos outros tipos de ativos além da moeda, como por exemplo ações, títulos, contratos inteligentes e outros.
- *Blockchain 3.0*. Para além do contexto monetário e de valores, a Blockchain possui aplicações na área de serviços governamentais, computação, sistemas de autenticação, entre outras.

O interesse do uso da tecnologia Blockchain em outras áreas de estudo se deu por

suas características que podem ser bem aproveitadas em outros campos de aplicações. Segundo Le e Hsu (2021), as principais características da Blockchain são:

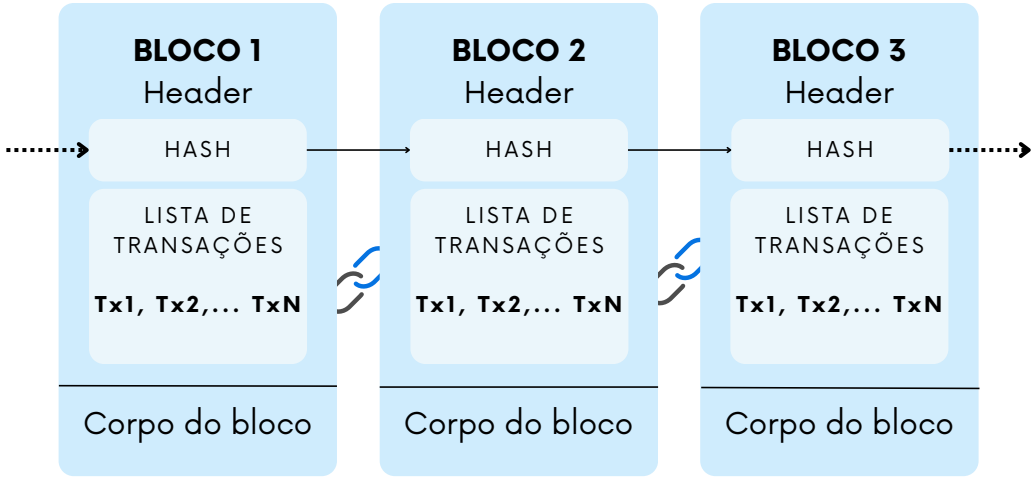
- *Decentralização*. Quaisquer sistemas e aplicações que são desenvolvidos utilizando Blockchain têm a característica de serem executados de maneira distribuída, isto é, não possuem a necessidade de entidades intermediando o processo. Por conta disso, a confiança entre as partes é estabelecida através de métodos de consenso na rede.
- *Disponibilidade e Integridade*. A Blockchain é formada por vários nós e as transações bem como o apurado de dados na rede são replicados em diferentes nós de forma segura, garantindo que o sistema se mantenha disponível e consistente.
- *Transparência e Auditabilidade*. Cada transação feita na *ledger* é pública, fazendo com que seja possível cada informação ser verificada e auditada. Ademais, muitas das implementações da Blockchain são de código aberto, fazendo com que a comunidade possa analisar como são operados os processos na rede.
- *Privacidade e Anonimidade*. Um sistema baseado em Blockchain preserva a anonimidade quando: (a) não há nenhuma ligação entre as identidades criptográficas e as identidades das partes no mundo real; (b) não há ligação estabelecida entre o remetente e destinatário de uma transação; (c) não há ligação entre as transações de um mesmo usuário. Neste caso, na realidade, só é possível oferecer um certo nível de anonimidade. Quanto à privacidade, ela é preservada em um sistema de Blockchain quando o conteúdo da transação só é acessado unicamente pelas partes envolvidas no processo.
- *Imutabilidade e Irrefutabilidade*. Cada transação efetuada na *ledger* é imutável e as informações que foram inseridas na rede não podem ser repudiadas. Só é possível a operação de inserção de dados na Blockchain após a realização de um novo consenso.

Os conceitos apresentados até agora possuem a finalidade de mostrar uma perspectiva geral do entendimento da Blockchain. Aliado a isso, as próximas seções deste capítulo tratam de aspectos mais detalhados acerca da tecnologia, isto é, sua estrutura, aplicações e perspectivas.

2.1.1 Estrutura da Blockchain

A Blockchain é estruturada de forma a se caracterizar como um sistema distribuído e decentralizado. Esta, por sua vez, é formada por blocos onde está contido o registro completo das transações efetuadas na rede. Estes registros são imutáveis, permanentes e transparentes. Nestes blocos também está contido o *header*, isto é, o cabeçalho do bloco e nele estão o *timestamp* (informações acerca do horário da transação), contém também o *hash* daquele bloco e de seu anterior e um *nonce*, que é um valor aleatório utilizado para verificar o *hash* (Aggarwal e Kumar, 2021b). Por fim, a estrutura básica da Blockchain é apresentada na figura 1. Cada transação é representada na figura como "*Tx1*"(transação 1) e assim por diante (com *TxN* sendo a *n-ésima* transação na rede).

Figura 1 – Estrutura básica da Blockchain



Fonte: Adaptado de (Zheng *et al.*, 2017)

2.1.2 Algoritmos de Consenso

Para que cada nó da rede possa identificar que somente informações válidas estão na Blockchain e que os dados sejam íntegros é necessário que haja consenso entre os seus participantes.

Consenso em uma Blockchain pode ser entendido como regras seguidas na rede de forma a se obter um acordo entre os nós que a compõem para que sejam adicionadas novas informações na Blockchain. Cada nó na rede contém uma cópia da Blockchain e adotam as

mesmas regras de consenso para validação e geração de novos blocos. É um conceito vital para que a Blockchain mantenha características como decentralização, integridade e uniformidade, mantendo cada mudança na *ledger* verificável e validada pelos seus integrantes (Raj, 2021).

Em vista disso, alguns algoritmos foram desenvolvidos ao longo dos anos para implementar este conceito entre os blocos da Blockchain. Entre eles estão *Proof of Work (PoW)*, *Proof of Stake (PoS)* e *Pratical Byzantine Fault Tolerance (PBFT)*.

2.1.2.1 Proof of work

O algoritmo *Proof of Work* (*PoW*) demanda que sejam dados incentivos apropriados na rede àqueles que resolverem um problema matemático complexo, o que é normalmente chamado de mineração. Após a solução do problema, transações podem ser verificadas na Blockchain como recompensa. Este modelo desencoraja indivíduos maliciosos pois faz com que seja necessário investir um grande poder computacional e uma quantidade de tempo considerável no processo de mineração, fazendo com que as ações de atacantes sejam restritas por conta do grande investimento em equipamento para ameaçarem a rede (Raj, 2021).

O problema que os mineradores precisam resolver é determinar a saída correta dada uma entrada composta pelo *hash* do bloco anterior variando o *nonce*. O primeiro minerador que encontrar a solução e ter o processo validado pela rede pode efetuar a transação na rede. Este tipo de algoritmo de consenso é largamente empregado na Blockchan pública e um exemplo que se destaca é a cripto-moeda *Bitcoin*.

2.1.2.2 Proof of Stake

Proof of stake (*PoS*) é um algoritmo de consenso que traz mais eficiência para as redes Blockchain pois elimina o procedimento de mineração utilizado no algoritmo *PoW*. Para o caso do algoritmo *PoS*, têm-se dois termos que compõem este método, que são os validadores (similar aos mineradores no algoritmo *PoW*) e a validação (similar ao processo de mineração). Estes validadores empregam uma parte do que possuem como *stakes*. Com isso, este *stake* é usado para selecionar a próximo validador na rede. Isto significa que quanto mais investimento por parte dos validadores, mais comprometimento com a rede este participante possui. A partir disso, é possível selecionar os validadores de acordo com seu empreendimento. O protocolo *PoS* dispõe de dois métodos de seleção dos próximos validadores: *coin-age selection* (seleção por antiguidade) e *randomized block selection* (seleção aleatória de bloco) (Vladucu *et al.*, 2023).

2.1.2.3 Pratical Byzantine Fault Tolerance

O algoritmo de consenso conhecido como *Practical Byzantine Fault Tolerance* (*PBFT*) opera com um nó principal e diversos nós secundários. Esses nós colaboram na implementação de um algoritmo de consenso destinado a solucionar o dilema dos Generais Bizantinos. Esse problema, oriundo da teoria dos jogos, descreve a complexidade que entidades descentralizadas enfrentam ao tentar chegar a um acordo sem depender de uma autoridade central confiável. O *PBFT* foi desenvolvido com eficiência para funcionar em sistemas assíncronos, minimizando a sobrecarga de tempo associada à resolução de desafios presentes em soluções de Tolerância a Falhas Bizantinas já existentes.

O processo de consenso se divide em cinco etapas: solicitação, pré-preparação, preparação, compromisso e resposta. Durante a fase de solicitação, o cliente envia seu pedido ao nó principal, que atua como líder. Na fase de pré-preparação, o nó principal comunica a solicitação aos demais nós do sistema, conhecidos como nós secundários. Nas etapas de preparação e compromisso, tanto o nó principal quanto os nós secundários executam o serviço solicitado. Por fim, na fase de resposta, todos os nós enviam uma resposta ao cliente. Nós defeituosos são representados por nós maliciosos. O protocolo é considerado bem-sucedido quando o cliente recebe $n = 3f + 1$ respostas idênticas de diferentes nós na rede. Nesse contexto, n representa o número total de nós, e f representa o número de nós defeituosos (Vladucu *et al.*, 2023).

2.1.3 Smart Contracts

Smart Contracts (Contratos Inteligentes) são pequenas funções ou programas que auxiliam na execução de contratos no ambiente da Blockchain (Agrawal *et al.*, 2022). Os *Smart Contracts* são desenvolvidos na linguagem de programação Solidity e entram em execução quando determinadas condições são atendidas. Eles representam programas que tem como finalidade automatizar a execução de acordos, sendo igualmente empregados na automatização de fluxos de trabalho.

Um contrato inteligente consiste em uma classe que abrange variáveis de estado, funções, modificadores de função, eventos e estruturas, desempenhando e regulando eventos e ações pertinentes conforme os termos estabelecidos no contrato. Além disso, ele tem a capacidade de chamar outros contratos inteligentes (Buterin, 2015). Segundo Aggarwal e Kumar

(2021a), algumas propriedades dos *smart contracts* são:

- Registro de dados: Todos os contratos são guardados na Blockchain em ordem cronológica.
- Sem intermediários: Não há a participação ou envolvimento de validadores intermediários, permitindo transparência e reacionamento direto entre as partes envolvidas na transação.
- Confiança: Devido às características intrínsecas da Blockchain de ser imutável e não-repudiável, existe suporte a confiança entre as partes envolvidas nos contratos.

Além disso, os contratos inteligentes desempenham um papel fundamental no processo de leitura e gravação de informações nas redes Blockchain, bem como na definição dos critérios que governam as transações na rede (Kumar *et al.*, 2023).

2.2 Votação eletrônica com Blockchain

Votação eletrônica é um método de votação que utiliza dispositivos eletrônicos para guardar e/ou contar votos (Tas e Tanriover, 2020). A votação eletrônica normalmente está vinculada a utilização de equipamentos eletrônicos e/ou software para que um processo eleitoral ocorra. É indispensável que sistemas desta natureza sejam capazes de efetuar e processar tarefas ligadas às fases de um processo de votação (Jafar *et al.*, 2022).

Um sistema de votação eletrônica necessita incluir principalmente as fases de registro, autenticação, votação e contagem de voto (Tas e Tanriover, 2020). Na fase de registro acontece o credenciamento dos eleitores aptos para participar do processo eleitoral. Em seguida, na fase de autenticação, as autoridades responsáveis pelo processo eleitoral verificam as credenciais de cada eleitor para permitir que somente votantes válidos possam participar do processo. Na etapa de votação ocorre o registro das intenções de voto do eleitorado. Cada voto é cifrado e verificado. Por fim, os votos são contados e os resultados exibidos.

Um sistema de votação eletrônica precisa satisfazer uma série de critérios para ser considerado apto de prover uma eleição não enviesada e acurada bem como ser transparente e possível de ser implementado (Vladucu *et al.*, 2023). Estes critérios são definidos a seguir.

– *Acurácia*. Esta propriedade garante que todos os votos válidos são contados corretamente e que os resultados da eleição são fidedignos a contagem. Esta caraterística assegura que ninguém é capaz de alterar o voto de outros eleitores

e que os resultados incluem somente os votos efetuados por eleitores válidos únicos e autênticos (Sadia *et al.*, 2020).

- *Anonimidade*. Para que um sistema de votação seja implementado, é vital que ele ofereça suporte a anonimidade do eleitor. Este sistema garante a anonimidade quando o eleitor vota de forma a não ser possível identificar a relação entre o voto e o eleitor que efetuou aquele voto durante todo o processo de eleição (Huang *et al.*, 2021).
- *Auditabilidade*. O processo de votação deve ser capaz de ser avaliado, verificado e auditado por agentes autônomos. Neste caso, a Blockchain possui esta característica por dispor de um *timestamp* e este elemento é utilizado para validação das transações na rede. Além disso, os nós na Blockchain podem ser utilizados para verificar as transações validadas através do conteúdo dos arquivos de *hash* armazenados nos blocos, isto é, dados imutáveis acerca dos outros nós participantes da rede. Esta propriedade da Blockchain confere a ela a possibilidade de rastrear todas as transações efetuadas na *ledger*(Awalu *et al.*, 2019).
- *Elegibilidade*. Esta propriedade é garantida quando somente eleitores aptos permitidos a votar participam do processo eleitoral (Benabdallah *et al.*, 2022).
- *Integridade*. Esta característica é conferida ao sistema de votação eletrônica quando se torna impossível mudar (contra a vontade do eleitor) ou eliminar votos depois destes terem sido efetuados (Adeshina e Ojo, 2019).
- *Privacidade*. Uma característica altamente requisitada em um sistema de votação é a garantia de privacidade. É entendida como a impossibilidade de associar o voto com o eleitor que o efetuou. Neste caso, a privacidade do eleitor deve ser assegurada durante todo o processo eleitoral e após ele ser finalizado (Cetinkaya e Cetinkaya, 2007).
- *Confiabilidade*. Um determinado processo eleitoral é confiável quando é implementado e executado seguramente de forma que não haja nenhuma perda dos votos (Tas e Tanriover, 2020). Por possuir cópias das transações em cada bloco, a Blockchain garante confiabilidade a um sistema eleitoral que a utilize.
- *Segurança*. Um sistema de votação é dito seguro quando este elimina potenciais ameaças e vulnerabilidades que possam torná-lo indisponível ou violar sua integridade durante todo o processo eleitoral (Kho *et al.*, 2022).

- *Transparência*. Este critério é definido como a capacidade do sistema de votação exibir informações acerca do processo eleitoral de forma clara aos usuários da rede, dado que a Blockchain mantém todo o histórico das transações contidas no sistema (Vladucu *et al.*, 2023).
- *Verificabilidade*. Este critério está relacionado com a capacidade do sistema fornecer meios de verificar se os resultados da eleição não foram falsificados. Deste modo, seja a nível de usuário ou da unidade verificadora, o sistema de votação eletrônica deve permitir avaliar se houve ou não fraude nos votos inseridos nele (Kho *et al.*, 2022).
- *Resistência a coerção*. Um sistema de votos deve ser resistente a coerção, prevenindo que algum agente malicioso não seja capaz de instruir eleitores a votarem contra sua vontade (Dimitriou, 2020).

3 PROCEDIMENTO METODOLÓGICO

Neste capítulo, apresentaremos os passos e técnicas usados para alcançar o propósito deste estudo. O presente trabalho consiste em uma revisão sistemática da literatura que adota uma abordagem qualitativa. A revisão sistemática da literatura tem como objetivo responder às perguntas de pesquisa e alcançar os objetivos estabelecidos. Para isso, foram utilizadas as publicações listadas nas bases de dados Scopus, IEEE Xplore e Springer. Estas bases foram escolhidas por indexarem um volume substancial de trabalhos de pesquisa e serem grandemente reconhecidas no meio acadêmico. As pesquisas foram atualizadas até 20 de julho de 2023, que é o ano de produção e finalização desta dissertação, e os anos de publicação dos trabalhos selecionados foram limitados ao período entre 2018 e 2023, dado que 2023 foi o ano de conclusão da pesquisa. Foram consideradas publicações relevantes na área e selecionadas de acordo com os critérios de busca, os quais serão detalhados posteriormente. Ademais, foram buscados textos acadêmicos em língua inglesa e portuguesa, sendo estes publicações de jornais ou revistas de cunho científico, de qualquer tamanho.

Quanto aos procedimentos utilizados neste trabalho, foram feitas uma revisão bibliométrica seguida de uma análise do conteúdos das publicações de forma sistemática. A bibliometria é entendida como uma técnica estatística e quantitativa que mede sistematicamente índices de produções acadêmicas com relação a suas contribuições a determinado tópico de pesquisa, influência, tendências e pesquisadores (Araujo, 2006). A revisão sistemática foi efetuada usando os procedimentos do protocolo PRISMA: formulação das questões de pesquisa, definir os critérios de exclusão, elaboração das *strings* de busca, análise, síntese e divulgação dos resultados. O protocolo PRISMA ajuda pesquisadores a melhorarem a apresentação de revisões sistemáticas ou meta-análises, pois é baseado em uma pergunta objetiva, utiliza métodos detalhados e claros, e permite identificar, selecionar e avaliar criticamente as pesquisas mais relevantes sobre o assunto estudado (Shamseer *et al.*, 2015).

Para a elaboração das *strings* de busca foi levado em consideração a sintaxe utilizada em cada base de dados e o refinamento da *string*. As *strings* de busca que melhor retornaram resultados em cada plataforma são as que se seguem:

1. SCOPUS:*((ALL (blockchain)) OR (ALL (distributed AND ledger))) AND ((ALL (electronic-voting)) OR (ALL (e-voting)) OR (ALL (e-vote))) AND ((ALL (coercion)) OR (ALL (coercion-free)) OR (ALL (coercion-resistant)))*

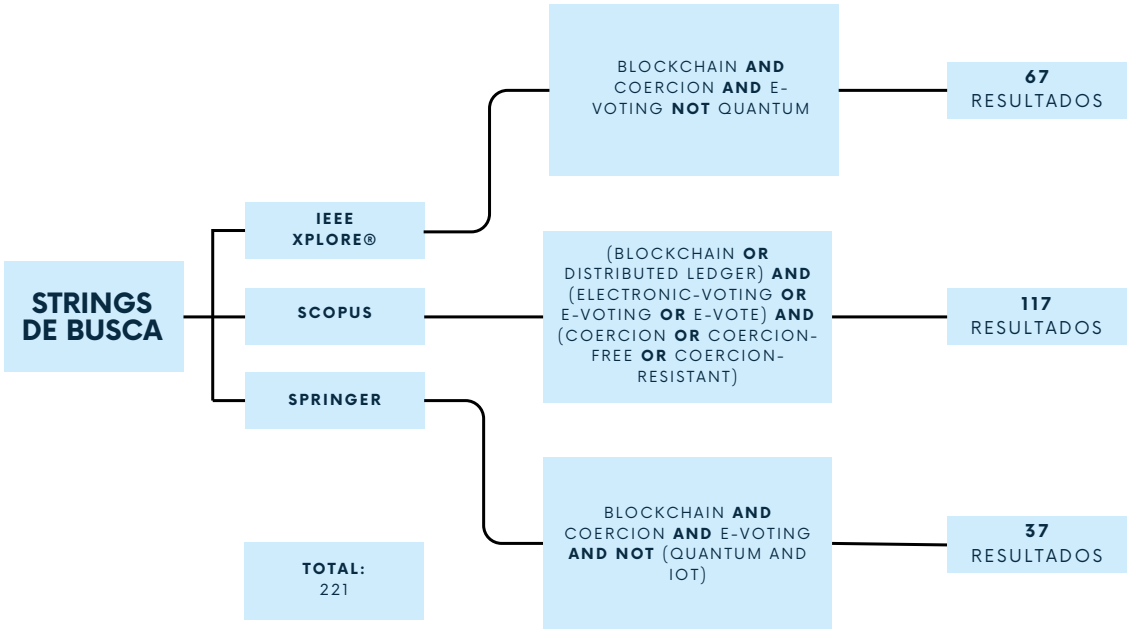
SRCTYPE (p OR j)

2. IEEE: *("Full Text & Metadata":blockchain) AND ("Full Text & Metadata":coercion) AND ("Full Text & Metadata":e-voting) NOT ("All Metadata":quantum)*

3. SPRINGER: *blockchain AND coercion AND e-voting AND NOT (quantum AND iot)*

Foram utilizadas *strings* de buscas diferentes em cada plataforma pois os resultados obtidos foram mais satisfatórios desse modo pois as publicações que foram exibidas eram mais contundentes em relação ao assunto desta revisão sistemática. Por inúmeras vezes, ao se utilizar strings de busca mais simples e semelhantes, cada base de dados retornava resultados nada contundentes em relação ao tema abordado ou trabalhos em que as palavras chaves apenas se encontravam nas seção das referências do artigo. Os resultados se deram de acordo com a Figura 2. De forma geral, as palavras-chaves da pesquisa foram buscadas em todo o corpo do texto e metadados dos trabalhos acadêmicos. De forma específica, os tipos de textos acadêmicos buscados eram artigos de revistas ou publicações de conferências.

Figura 2 – Quantitativo de publicações de cada string de busca



Fonte: Autor

De acordo com os resultado descritos acima, a pesquisa continuou para a etapa de seleção sistemática das publicações para então serem revisadas e cumprir o objetivo desta

produção acadêmica como mostrado na Figura 3. Os critérios de exclusão de artigos para uso neste trabalho se deu da seguinte forma:

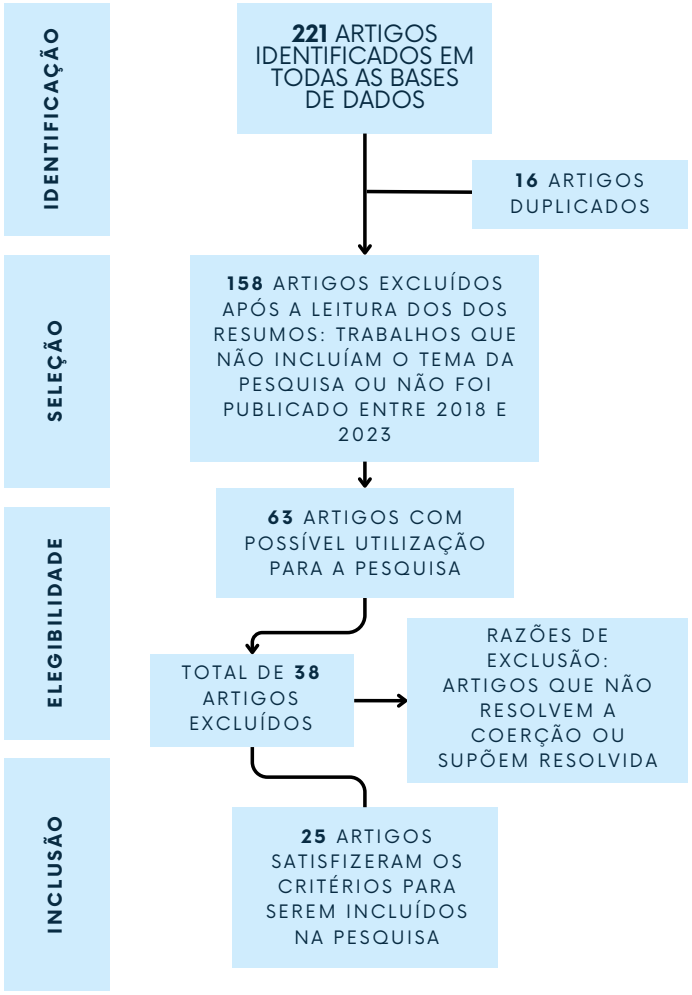
(i) Trabalhos que não incluíam o tema da pesquisa ou não foi publicado entre 2018 e 2023.
(ii) Artigos que não resolvem a coerção ou supõem resolvida.

De forma análoga, aqueles trabalhos que não foram excluídos deste estudo na etapa de exclusão passaram então a compor o grupo de trabalhos primários para serem analisados nesta revisão sistemática.

Na Figura 3 é mostrado que de 221 publicações buscadas, 25 trabalhos primários foram incluídos nesta revisão por satisfazerem os critérios necessários. De todo modo, mesmo os artigos não incluídos neste trabalho expandiram os conhecimentos sobre o tópico bem como apresentaram novas perspectivas sobre os usos da Blockchain e mostraram formas mais claras de expor o assunto desta pesquisa sistemática.

O próximo passo deu-se de modo a produzir a análise bibliométrica dos resultados da pesquisa de uma perspectiva geral, mostrando informações como frequência de artigos através dos anos, áreas de publicação e países de origem dos estudos que mais produziram acerca do tema. Por fim, a análise e discussão acerca do tema deste trabalho foram desenvolvidas a partir da leitura completa dos 25 artigos, onde foi visto com profundidade os métodos ali propostos fazendo uma análise qualitativa e detalhada destas publicações, avaliando os modelos produzidos observando as possíveis soluções do problema da coerção.

Figura 3 – Seleção sistemática



Fonte: Autor

4 ANÁLISE DA LITERATURA

Quanto à busca por resultados referentes à prevenção da coerção em sistemas de votação eletrônica que empregam a tecnologia Blockchain, as análises conduzidas neste estudo sistemático da literatura estão descritas nas seções a seguir.

4.1 Análise bibliométrica

Os resultados bibliométricos estão descritos em diferentes parâmetros, como evolução cronológica, áreas de publicação e países. A quantidade de publicações resultantes da *string* de busca e que foram utilizadas nesta revisão são mostradas na Tabela 1.

Tabela 1 – Quantidades de publicações por ano em cada base de dados

Scopus		**IEEE Xplore**		**Springer**	
Ano	Qtd.	Ano	Qtd.	Ano	Qtd.
2018	0	2018	2	2018	0
2019	0	2019	3	2019	0
2020	0	2020	5	2020	0
2021	6	2021	2	2021	2
2022	4	2022	0	2022	0
2023	0	2023	0	2023	1
Total	10	Total	12	Total	3

Fonte: Autor

Observando as publicações sobre sistemas de votação eletrônica que utilizam Blockchain e que tangem o tópico da coerção, ainda não era substancial a quantidade de trabalhos que tratavam deste tema nos anos anteriores ao de 2018. No entanto, a partir de 2018(ano contido no intervalo das buscas desta revisão), encontram-se avanços substanciais nesse tema, bem como a implementação de um sistema mais robusto observando as características essenciais de um sistema eleitoral, visto o trabalho de Braghin *et al.* (2019). Um fato que corrobora para esta afirmação se dá pelo fato de que especificamente na base de dados do IEEE não há trabalhos publicados antes de 2018 com os dados de busca utilizados, o mesmo ocorre com a base de publicações do Scopus. Algo semelhante acontece com os resultados na base da Springer, onde os trabalhos datam de 2019.

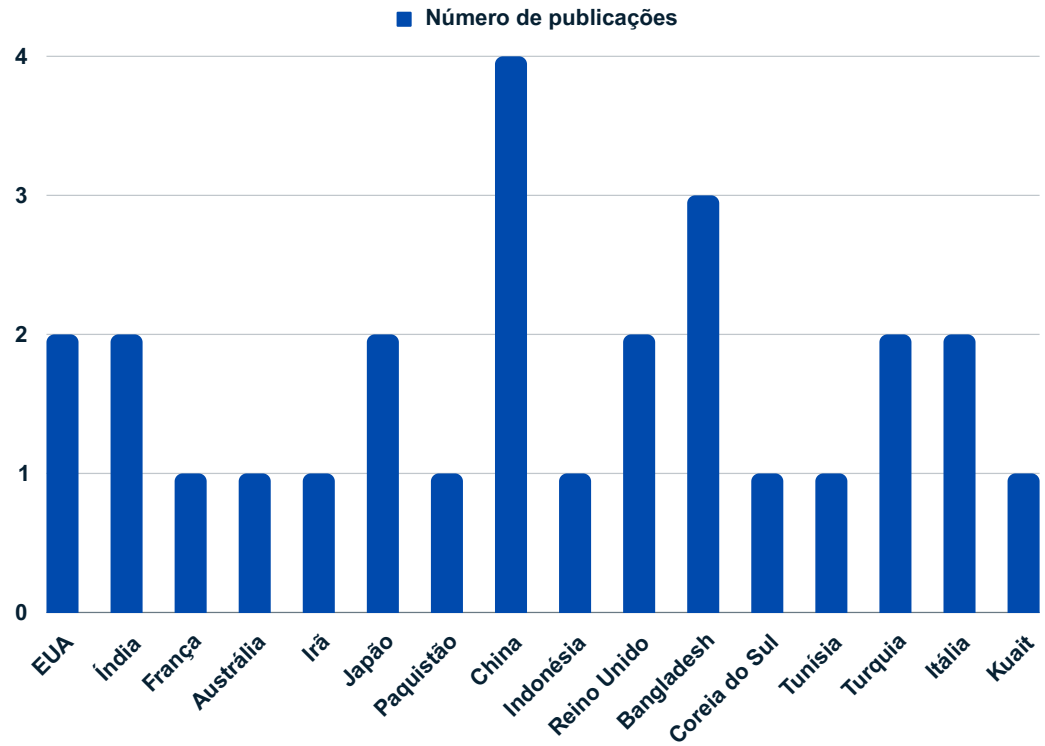
Considerando que se trata de um tópico atual e delicado, é compreensível que as publicações relacionadas à votação eletrônica que utilizam a tecnologia Blockchain como forma de combater a coerção ainda estejam nos seus estágios iniciais de desenvolvimento. No entanto,

a comunidade acadêmica reconhece o significativo potencial dessa questão. De acordo com a Tabela 1, é possível ver o aumento de publicações na base de dados Scopus no ano de 2021, e existe a perspectiva de que novas publicações possam surgir ao longo de 2023 em todas as bases visitadas nesta revisão.

As áreas de publicação naturalmente sobre Blockchain estão ligadas à computação pois sistemas de votação eletrônica obviamente possuem temas que profissionais e pesquisadores da área lidam diretamente.

Ao analisar a quantidade de publicações por países de origem dos trabalhos acadêmicos, observa-se que a China lidera em termos de produção científica relacionada aos resultados das pesquisas, seguida pela Índia e pelos Estados Unidos. Na Figura 4 temos um quantitativo de produções relacionado ao país de origem da pesquisa. Cabe ressaltar também que, dentre as três bases de dados, somente na Scopus há uma publicação brasileira, porém está distante do escopo desta revisão sistemática.

Figura 4 – Países de origem das publicações utilizadas neste review



Fonte: Autor

4.2 Revisão sistemática qualitativa

A Blockchain tem sido uma ferramenta de grande valia na expansão de horizontes de diversas áreas do conhecimento desde quando foi idealizada. Redes de criptomoedas, por exemplo, utilizam o que é chamado de Blockchain 1.0 e compõem uma considerável parcela das redes disponíveis. De modo semelhante, as versões 2.0 e 3.0 costumam englobar aplicações em *smart contracts*, economia, mercado, criptografia, votação eletrônica, entre outras (Benabdallah *et al.*, 2022).

Com a Blockchain, muitas possibilidades de melhorias em tecnologias diversas se tornaram realidade. No contexto de votação eletrônica, o potencial de sistemas baseados em Blockchain tem se mostrado vasto. As técnicas utilizadas nestes tipos de processos vêm se tornando cada vez mais robustas e processos eleitorais eletrônicos podem se beneficiar das características desta tecnologia.

No entanto, votação eletrônica que utiliza a Blockchain ainda possui desafios e um deles é a implementação de um processo eleitoral livre de coerção. Para contornar esta dificuldade, algumas propostas foram feitas. Dentre as possibilidades de solução para este desafio, mecanismos diversos foram aplicados para contornar o problema, que são: a utilização de cédula de voto falsa ou cifrada, emprego de protocolos de segurança propostos pelos autores, a possibilidade de atualização de voto no decorrer do processo eleitoral, emprego de métodos criptográficos, dentre outros mecanismos menos recorrentes.

4.2.1 Cédula de voto falsa ou cifrada

De forma geral, este método traz a possibilidade aos eleitores de induzir os atacantes ao erro, mostrando informações falsas acerca das informações de intenções de voto ou exibindo uma cédula de voto falsa. Em segundo lugar, a possibilidade de cifrar a cédula de voto faz com que o atacante seja desencorajado a continuar a coagir determinado eleitor durante o processo eleitoral, pois não seria possível decifrar as informações contidas na cédula de voto.

Neste assunto, Zaghloul *et al.* (2020) propuseram a possibilidade de o votante utilizar um boletim de votação falso cifrado com uma chave alternativa para compartilhar com aquele que pratica a coerção. Isto significa que a cédula de voto exibe informações falsas quando decifrada utilizando a chave alternativa e, desse modo, é possível desencorajar e eliminar a coerção.

No artigo de Kumar *et al.* (2020), os autores fornecem um meio de evitar a coerção

por meio da atribuição de um número aleatório ao comprovante de votação em que somente a Autarquia Eleitoral conhece, fazendo com que a resolução da cifra do voto seja possível somente se um indivíduo consiga presumir corretamente o número aleatório secreto que foi atribuído ao comprovante de voto, que é o equivalente a resolver o problema de logaritmo discreto de curvas elípticas (*ECDLP - Elliptic Curve Discrete Logarithm Problem*).

4.2.2 Protocolos de segurança

Para tentar contornar o problema da coerção, alguns autores optaram por adaptar ou criar novos protocolos de segurança para que, assim, determinadas informações no sistema de votação sejam anônimas ou protegidas para inibir a ação do atacante.

Por exemplo, no trabalho de Dehez-Clementi *et al.* (2021), os autores propõem um sistema de votação utilizando uma infraestrutura baseada em Blockchain de forma a utilizar um protocolo de geração de chaves distibuídas (*Distributed Key Generation (DKG)*). Neste método proposto, o sistema provê comunicação anônima entre o eleitor e o sistema de votação de forma que o atacante não possa identificar o eleitor e assim usar a imutabilidade dos dados na rede Blockchain para asseverar a integridade da contagem de votos e não haver interferência na tomada de decisão do eleitor. A comunicação é anônima no sistema pois uma das características do protocolo *DKG* é de indistinguibilidade de transações e desvinculação de contas da Blockchain.

Avaliando um caso real onde a Blockchain é utilizada em um sistema de votação, temos o trabalho de Sertkaya *et al.* (2022), em que os autores oferecem uma nova abordagem sobre o sistema de votação via internet da Estônia. Na publicação, a preocupação se dá na distribuição segura de credenciais onde empregam-se credenciais de identidades auto-soberanas como autenticação externa à unidade certificadora. Estas credenciais anônimas impedem terceiros de atribuir determinado voto a seu respectivo eleitor, dessa forma desencorajando a coerção. A maior limitação do manuscrito é a necessidade de uma nova solução de fornecimento de registros de identidade que suporte as credenciais anônimas apresentadas no trabalho. Outra limitação é o uso concomitante do voto impresso, isto é, não é um sistema que utiliza unicamente meios eletrônicos.

4.2.3 Atualização de voto

Uma das soluções mais utilizadas pela literatura contida nesta revisão é a possibilidade de atualização de voto. Nesse caso, o eleitor tem a possibilidade de alterar sua intenção

de voto caso a integridade do votante no processo eleitoral esteja comprometida por conta da coerção.

Em Golnarian *et al.* (2022) e Adiputra *et al.* (2018), a solução proposta diminui a efetividade de coagir um determinado eleitor permitindo que este seja capaz de atualizar o seu voto. No primeiro artigo, é permitido sair do processo eleitoral, de modo que os votos seriam invalidados pelo próprio eleitor e este abandonaria a sua participação na eleição. Já no segundo texto, somente o último voto do eleitor será de fato contabilizado. Esta solução por um lado é promissora pois desencoraja a coerção pois teria possibilidade de o eleitor sair do processo e se livrar da influência do atacante, fazendo com que o atacante não tenha mais a vantagem desejada. Por outro lado, isto pode gerar efeitos maléficos sobre o processo no geral bem como deteriorar a autonomia dos indivíduos que são aptos a votar.

Widayanti *et al.* (2021) sugerem a possibilidade de o eleitor mudar sua intenção de voto quando for conveniente se valendo de uma chave privada de acesso à rede onde a escolha do eleitor está guardada e em conexão com os outros nós da rede. Neste caso, uma barreira aparente está no fato de alguns países não permitirem alteração de intenção de voto de um eleitor.

Por se tratar de um trabalho que propõe um modelo de votação remota, Hardwick *et al.* (2018) indicam que é difícil resolver o problema da coerção por meios tecnológicos nesse caso. Com isso, é proposta a possibilidade de um sistema onde o eleitor possa mudar a intenção de voto até a finalização do processo. Um dos problemas apontados reside no fato de processos de larga escala, onde algumas soluções em Blockchain possuem elevados custos computacionais por conta do grande volume de transações que seriam efetuadas.

Em Suwito e Dutta (2019), os autores propõem um sistema de votação onde há seções de votação e o problema da coerção é tratado de forma a possibilitar o eleitor de votar novamente outras vezes e contar apenas a última escolha feita no prazo da eleição. O votante pode também usar suas credenciais para ir até a sua zona eleitoral para verificar o a descrição do seu voto. Admite-se que o sistema é implementado contendo a função de processo eleitoral sem comprovante de votação. Ainda não foi implementado e os elevados custos de utilização em larga escala é ainda impeditivo.

Por fim, no trabalho de Chaieb e Yousfi (2020), o sistema proposto utiliza credenciais para os eleitores serem possibilitados de votar. Essas credenciais são compostas de elementos baseados em assinatura de grupo *BBS* e são compostos por números atribuídos a cada participante do processo eleitoral. Com estas credenciais, o eleitor fica autorizado a exercer sua cidadania na

eleição. Caso o votante esteja sob influência externa, este pode utilizar credenciais falsas para que a integridade da sua verdadeira intenção de voto permaneça intacta, sendo possível votar novamente utilizando as suas credenciais verdadeiras posteriormente.

4.2.4 Métodos criptográficos

Uma quantidade expressiva de autores optaram por implementar primitivas criptográficas ou algoritmos específicos para auxiliar na resolução do problema da coerção. Primitivas criptográficas são blocos de construção fundamentais para desenvolvimento de protocolos de segurança que visam obter confidencialidade, autenticação, integridade e não-repúdio em sistemas (Shim, 2016).

No trabalho de Murtaza *et al.* (2019), o autores utilizam como base a primitiva criptográfica *Zero knowledge proof* para verificar a validade de uma afirmação revelando apenas informações necessárias sobre os dados da afirmação. Neste contexto, os autores utilizam uma primitiva criptográfica desenvolvida por eles chamada de *Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARKs)*, onde esta técnica permite o convencimento de uma entidade verificadora acerca da validade da afirmativa proposta sem revelar a própria afirmativa, garantindo a inibição da coerção. Isto é, a coerção se dá pela impossibilidade de revelar a escolha do voto para terceiros, neste caso, um atacante que tente coagir um eleitor no processo mas ainda preservando a verificabilidade do voto na rede.

No artigo de Islam *et al.* (2022), os autores propõem um sistema de votação em que cada eleitor atribui diferentes pontuações para cada candidato ao invés de um único voto. Cada voto é protegido por uma chave privada. O candidato com maior pontuação vence a disputa. Após a submissão dos votos, cada voto é protegido com um método de cifração e o trabalho proposto garante o processo eleitoral livre de coerção através da primitiva criptográfica *Zero knowledge proof*. Dessa forma, um atacante que tente influenciar o voto do eleitor será incapaz de efetivamente concretizar sua investida, uma vez que, após a votação, é impossível relacionar uma determinada intenção de voto com seu respectivo eleitor sem o envolvimento da unidade organizadora do processo eleitoral. Um dos problemas vistos nesse tipo de sistema de votação se dá pela dificuldade de implementação deste método em sistemas de votação de grande escala dado o tempo de execução elevado e altos custos envolvidos no processamento das informações. Para tal finalidade, os autores recomendam a *Hyperledger Fabric*, uma infraestrutura Blockchain modular que se adéqua às necessidades mais específicas de uma determinada aplicação, fazendo

com que o tempo de resolução das transações sejam viáveis em larga escala.

Neste artigo de Abegunde *et al.* (2021), os autores propõem uma aplicação baseada em Blockchain onde um sistema de votação eletrônica descentralizada é sugerido. Esta aplicação funciona na rede Ethereum para proteger a aplicação de alguns ataques como *Denial of Service* (*DoS*), *Single Point of Failure* (*SPF*), e *Fraudulent Record Modification*. Adicionado a isso, o trabalho propõe um novo algoritmo de consenso chamado *Proof of Smart Vote*, em que este é uma alternativa ao algoritmo de consenso *Proof of Work*. Para tratar do problema da coerção, os autores configuraram o sistema de forma que a identificação do eleitor não está associada com o voto em si. A verificação de voto do eleitor acontece ao final do processo e, neste caso, só é mostrado que o voto não foi alterado, desencorajando assim a coerção. A limitação do estudo proposto reside no fato de ainda não ter sido implementado de forma a combinar a possibilidade dos eleitores verificarem seu voto após votarem com uma votação sem comprovante.

A proposta de Li *et al.* (2021) é a de utilizar o que os autores chamaram de autenticação anônima baseada em atributos publicamente rastreáveis. Este método se baseia em um técnica de autenticação por atributos, onde é possível manter o anonimato no processo de autenticação dado que informações sobre identidade não são compartilhados, mas sim atributos. Para o caso de um sistema de votação eletrônica utilizando Blockchain, a análise do modelo de segurança resultou em um sistema com as seguintes características: Confidencialidade, Anonimato, impossibilidade de falsificação, verificabilidade, contagem(*accountability*). Com isto, é possível considerar que o trabalho consegue propor um sistema em que não seja possível um indivíduo coagir eleitores dado o anonimato no processo de votação, no entanto, ainda falta testar escalabilidade do sistema.

O trabalho de Spadafora *et al.* (2023) busca mitigar a coerção se utilizando de *tokens*. Quando um eleitor votar, um *token* falso e outro válido são gerados e enviados para os candidatos. O *token* válido é enviado para o candidato escolhido e o *token* falso é enviado para o outro candidato. No processo de votação, apenas o eleitor conhece o *token* válido e, pela característica do sistema utilizado no trabalho de haver uma unidade central no processo, é impossível que terceiros possam reconhecer o *token* válido e não é possível exibir informações sobre ele sem que haja adulteração no processo eleitoral. Este trabalho é uma produção ligada a matemática teórica e ainda não foi implementada.

Dimitriou (2020) também propôs um modelo de votação baseado em Blockchain, que reduz uma grande quantidade de sobrecarga de computação e comunicação. No modelo, a

resistência à coerção e a impossibilidade de comprovação do voto são garantidas por meio de um token aleatório - um elemento resistente a adulterações que atua como uma caixa-preta na construção da cédula de voto para o usuário. No entanto, isso requer um administrador confiável para registrar os eleitores. Neste artigo, o autor supõe que o indivíduo que pratica a coerção e o eleitor não estão lado a lado. Tudo o que o atacante pode fazer é emitir instruções e pedir uma prova por parte do votante.

Em Braghin *et al.* (2019), foi proposto um esquema de votação eletrônica remota, onde os eleitores podem votar a partir de um navegador onde há o plugin desenvolvido na publicação. O artigo propõe um ambiente onde se alcançam diversas características de um processo eleitoral robusto. Para mitigar a coerção, é utilizado uma técnica de *hash* conhecida como *Chameleon Hash*, onde esta é entendida como uma função *hash* resistente à colisão e está associada ao uso de um par de chaves públicas e privadas de modo que o funcionamento desta função se baseia na ideia de que o destinatário da mensagem só pode replicar a mensagem no caso da autorização do remetente. Este princípio é utilizado na votação eletrônica na etapa de votação, onde o eleitor pode enganar o indivíduo que pratica a coerção. No entanto, o trabalho possui dois grandes problemas. O primeiro é que não é admitido que aquele que pratica a coerção está presente no momento em que o eleitor está votando, tornando assim o processo menos robusto e inválido quanto à coerção (mesmo que em escala menor). O segundo problema é que os autores não descrevem os requisitos para implementação do sistema ou os aspectos de validação e verificação.

4.2.5 Mecanismos menos recorrentes

Existem trabalhos que implementaram outros tipos de métodos para combater a coerção. Nesta seção, encontram-se métodos contra a coerção como a adoção de votos sem comprovantes para que não haja como comprovar informações de voto para determinado atacante, reconhecimento facial para voto remoto e averiguar as redondezas do eleitor, uso de *token* de acesso fornecido a cada eleitor, entre outros.

Neste artigo de Sadia *et al.* (2020), os eleitores são divididos em grupos e para cada um destes é atribuído um horário de votação específico. A organizadora do processo eleitoral faz uma lista com os dados de cada eleitor apto para votar. Esta lista contém os nomes, números de identificação eleitoral, impressão digital, entre outras informações que sejam necessárias. A organizadora então configura o bloco de Gênese que possui como entradas os eleitores aptos, suas

impressões digitais (e seus valores convertidos em binários), janela de tempo para votação (com tempo do início e fim). Estes eleitores são então divididos aleatoriamente em grupos. Com isso, cada grupo deve votar no período de tempo especificado pela organização do processo eleitoral para que a votação seja concluída. As informações dos horários de voto são enviados para o e-mail ou celular do eleitor e assim este pode prosseguir com a validação de sua identidade e efetuar seu voto. Para que a coerção seja combatida, este tempo é desconhecido pelos próprios eleitores, fazendo com que a influência externa seja desencorajada. Um dos problemas desta abordagem é que os aparelhos utilizados pelos eleitores necessitam ter meios de captar a impressão digital do eleitor e na persistência de um atacante sobre o eleitor em acompanhar os horários de votação, mesmo que esta tarefa seja difícil de se executar.

O sistema proposto por Tas e Tanriover (2021) tem na etapa inicial a autenticação do eleitor pela autoridade organizadora e então se seguem até o eleitor finalizar o voto. Para cada eleitor, um *token* é distribuído e então a escolha do candidato é feita. Os dados do voto são cifrados, enviados para a rede Blockchain e então o processo é finalizado. Para cifrar as informações dos votos é utilizado o método de cifração homomórfica e isto garante confidencialidade e anonimato. Após a cifração, ao invés dos dados serem enviados para os nós da rede, eles são divididos em partes e enviados aos nós. Isso ocorre para que não haja intenção maliciosa de realizar contagem dos nós antes da fase de contagem ou obter informações que trariam vantagens para um candidato específico. Estas partes seriam unidas novamente na fase de contagem. Diante disso, a coerção é evitada pois não é possível vincular as informações de voto a um determinado eleitor, dado que o *token* é distribuído aleatoriamente e as informações dos votos são divididas até o fim do processo eleitoral. Um dos avanços significativos desta publicação é que o sistema foi implementado.

No caso de Hao *et al.* (2021), cada eleitor possui uma chave de sessão e então o processo de votação se inicia. Utilizando as chaves de sessão dos eleitores, o sistema de votação utiliza uma função *hash* para operar estas chaves e então estas são salvas em uma lista. Ao votar, é criado um polinômio onde a lista de chaves e as intenções de votos estão relacionadas. Para inibir a coerção, cada parte do polinômio que relaciona a intenção de voto do eleitor é verificado e atribuído a ele um coeficiente conhecido apenas pela organizadora do processo. Cada parte do polinômio fica relacionada a um candidato e, com isso, mesmo que haja a tentativa de recuperar estes coeficientes não será possível pois necessitaria cooperação entre todos os candidatos ao pleito na eleição.

No trabalho de Alvi *et al.* (2022), os autores propuseram um sistema de votação onde o processo é realizado por uma comissão de eleição. Neste sistema, cada eleitor é representado por um *hash* para proteger sua identidade, impossibilitando o evento de um determinado eleitor ser identificado por terceiros. Neste processo, não há o compartilhamento de nenhum tipo de comprovante de votação e também não há forma de exibir qual a intenção de voto do votante no processo, garantindo ao processo a inibição da coerção.

No artigo de Zaghloul *et al.* (2021) , o processo de voto funciona de forma a garantir que os votos são cifrados e não há a possibilidade de estabelecer nenhuma ligação entre o eleitor e seu voto a menos que duas das entidades envolvidas no processo eleitoral, registrador e moderador, hajam em unidade. No entanto, é estabelecido que estas duas entidades possuem interesses conflitantes, fazendo com que essa coparticipação não aconteça. Com isto posto, o cenário é de escolha entre duas propriedades: verificação universal ou resistência a coerção. Para o caso da verificação universal, a escolha é feita quando o sistema de votação necessite obter a possibilidade dos eleitores verificarem seus votos foram contados da forma devida, tornando viável a avaliação se houve alguma tentativa de adulteração dos votos por parte do registrador. Para este caso, após a eleição, os agentes maliciosos que praticaram coerção poderão observar se os eleitores que sofreram o ataque foram contados para determinado candidato. Para o caso de optar por uma forte resistência a coerção, o sistema é implementado de forma a garantir uma votação sem comprovantes, fazendo com que não seja possível traçar qualquer ligação entre o eleitor e seu voto em nenhuma fase da eleição.

Outro sistema foi proposto por Li e Xiong (2021), os autores propõem um esquema de re-cifração onde duas chaves públicas e duas chaves privadas são usadas para identificação real e identificação do sistema de votação, respectivamente. Como os dados dos votos dos eleitores são cifrados em duas etapas e de forma separada, não é possível atribuir nenhuma ligação entre os dados do voto e a identidade do eleitor. No sistema também não é possível provar em quem o eleitor votou pois não há comprovantes de voto de nenhuma natureza. No entanto, os autores apontam para o fato que a etapa de contagem de votos seja feita apenas ao final do processo eleitoral para que não se tenham pistas sobre as escolhas dos eleitores. Vale ressaltar que este sistema foi implementado.

Na publicação de Pooja *et al.* (2021), os autores produziram um sistema de votação onde se utilizam de detecção de rostos para inibir a coerção. Na etapa após a autenticação, o módulo de captura pré-voto é acionado e este confere se o eleitor é o único participante da

votação no momento, isto é, se há somente um único rosto sendo reconhecido. Após isso, o sistema prossegue com a etapa de votação. Neste caso, o sistema ainda é fraco para combater a coerção dado que é possível um indivíduo pressionar o eleitor sem necessariamente estar diante do dispositivo de reconhecimento facial. Entretanto, uma propriedade promissora foi elencada pelos autores como trabalho futuro que é a possibilidade do módulo de reconhecimento facial também identificar emoções, onde será possível identificar a possibilidade de o eleitor estar sobre pressão. Ainda assim, não é uma publicação que obtém um sucesso considerável no combate a coerção.

Os autores Agate *et al.* (2021) propuseram um processo eleitoral onde há a existência de funcionários que supervisionam o procedimento e cabines de votação que garantem a privacidade dos usuários, isto é, há uma entidade centralizadora do processo envolvida. Para garantir que o processo eleitoral seja livre de coerção, os autores optaram por um sistema sem comprovantes de voto e a votação ocorrendo em uma seção eleitoral onde os eleitores possuem privacidade ao votar. Outra característica que vale a pena salientar sobre o trabalho é que o processo é *open source*, ou seja, profissionais de segurança podem analisar o código fonte e utilizar para testes e expansão.

Na Figura 5 é mostrada como as publicações estão distribuídas de acordo com o tipo de solução proposta para inibir a coerção em sistemas de votação eletrônica com base em Blockchain.

4.3 Discussão

Avaliando a natureza dos trabalhos bem como o conteúdo de suas publicações, é natural que as publicações sobre sistemas de votação eletrônica que utilizam Blockchain esteajam concentradas na área de computação e afins. Isto se justifica pelo fato de sistemas informatizados possuírem uma natureza intrínsicamente ligada a software e hardware, partes estas que necessitam ser desenvolvidas para que, de fato, o sistema de votação eletrônica seja plenamente implementado. Para tal feito, desenvolvedores e engenheiros de sistemas são necessários para produzirem estes sistemas eleitorais de modo que as demandas sejam satisfeitas.

De acordo com a análise bibliométrica das publicações, o país que mais se destacou na área desta pesquisa foi a China. Já do ponto de vista qualitativo, foi inferido que sempre há um *trade-off* entre as propriedades da votação eletrônica pois, para prevenir a coerção, normalmente os sistemas propostos estavam configurados de modo a não ser possível que o eleitor pudesse

Figura 5 – Mecanismos utilizados nos trabalhos selecionados

Mecanismo	Publicações	Descrição
Cédula de voto falsa ou cifrada	Zaghloul et al.(2020), Kumar et al.(2020),	Nestes trabalhos a coerção foi combatida utilizando cifração da cédula de voto ou exibindo cédulas de voto falsas para o atacante.
Protocolos de segurança	Dehez-Clementi et al. (2021), Sertkaya et al. (2022)	Nestes trabalhos a coerção foi combatida através da utilização de protocolos de segurança propostas pelos autores.
Atualização de voto	Golnarian et al. (2022), Adiputra et al. (2018), Widayanti et al. (2021), , Hardwick et al. (2018), Suwito e Dutta (2019), Chaieb e Yousfi (2020),	Nestes trabalhos a coerção foi combatida através da possibilidade de alteração da intenção de voto por parte do eleitor.
Métodos criptográficos	Murtaza et al. (2019), Islam et al. (2022), Abegunde et al. (2021), Spadafora et al. (2023), Dimitriou (2020), Li et al. (2021), Braghin et al. (2019)	Nestes trabalhos a coerção foi combatida com o emprego de técnicas criptográficas variadas, como por exemplo: zKSNARK, tokens de voto, métodos de autenticação, entre outros.
Outros	Sadia et al. (2020), Tas e Tanriöver (2021), Hao et al. (2021), Alvi et al. (2022), Zaghloul et al. (2021), Li e Xiong (2021), Pooja et al. (2021), Agate et al. (2021),	Nestes trabalhos a coerção foi combatida por métodos não muito utilizados na literatura, como por exemplo votos sem comprovante, reconhecimento facial, entre outros.

Fonte: Autor

verificar seu voto posteriormente, ou a impossibilidade de o processo eleitoral ser remoto, pois tornava-se difícil garantir que o eleitor não passaria por coerção durante a votação, por exemplo.

A descentralização do sistema eleitoral apresenta desafios significativos, como a possibilidade de participação de pessoas não autorizadas nos processos eleitorais. Além disso, existe uma lacuna decorrente da ausência de um sistema que permita a verificação autônoma das credenciais dos indivíduos, sem depender exclusivamente de uma entidade certificadora ligada aos processos eleitorais de cada país. É fundamental garantir a soberania dos dados de cada pessoa, assegurando a autenticidade e a não-repudiação de suas credenciais e atributos (Vladucu *et al.*, 2023).

É importante destacar também que dentre os artigos utilizados nesta revisão não há uma implementação utilizada em maior escala e que seja avançada o suficiente para possuir todas as características essenciais de um sistema eleitoral eletrônico com Blockchain, sendo possível então a exploração dessa limitação. Ainda há certas lacunas abertas que os autores apontam na

conclusão de seus trabalhos e, por mais que já existam países que adotaram a Blockchain em seus processos eleitorais (veja Sertkaya *et al.* (2022)), ainda são necessários avanços substanciais na área para que eleições sejam seguras, principalmente quanto a permitir uma eleição sem uma unidade mediadora, e o processo seja imbuído de robustez e completude com relação aos requerimentos de sistema.

Com relação a preocupações de trabalhos futuros, alguns assuntos podem ser melhor desenvolvidos. Ao apresentar os testes desenvolvidos, os trabalhos poderiam possuir testes mais contundentes com relação a latência (tempo para processamento de informações), recursos (gasto de poder de processamento e energia), entre outras preocupações. No entanto, a realidade é que os sistemas propostos ainda não foram plenamente implementados e, por consequência, assumem que outras características importantes de um sistema eleitoral confiável já tenham sido implementadas.

Por fim, a Blockchain é uma tecnologia que traz muitos benefícios para sistemas de votação eletrônica e, principalmente com relação a coerção, ainda há possibilidades de avanços, dado que é necessário unir esta característica a outras propriedades importantes de um processo eleitoral. É importante também investigar a possibilidade de se utilizar de técnicas de credenciamento auto-soberanas no processo eleitoral, para que haja ainda menos interferências indesejadas e diminuir as possibilidades da coerção ocorrer.

5 CONSIDERAÇÕES FINAIS

A tendência de pesquisar sobre o uso da Blockchain em sistemas de votação ganhou força nos últimos anos. Como visto anteriormente, as primeiras publicações a aparecerem nas bases de dados incluídas nesta revisão datam do ano de 2018 e o tema experimentou certa visibilidade, principalmente entre 2021 e 2022. No entanto, desde a sua criação em 2008 por Nakamoto, um tempo considerável de dez anos se passou até que os primeiros trabalhos sobre a aplicação em sistemas eleitorais eletrônicos vieram a ser publicados. Além disso, dada a complexidade e sensibilidade deste assunto, os sistemas implementados ainda estão sendo desenvolvidos ou são aplicados em pequena escala. Alguns países já adotaram a Blockchain em seus pleitos, no entanto, ainda há muito o que se aprimorar nestes sistemas.

Diante do que foi analisado, respondendo a **QP1**, a possibilidade de alteração de voto pode ser apontada como principal solução para a coerção, sendo este recurso o mais utilizado pelos autores, como visto na Figura 5. Em grande parte dos trabalhos este foi o modo mais utilizado para resolução do problema da coerção, seja com a participação de uma entidade central ou não. Outro meio efetivo para lidar com o problema da coerção foi o de cifrar as cédulas de votos na Blockchain com chaves secundárias e assim mascarar a real intenção de voto do eleitor caso este seja coagido por terceiros.

Quanto a **QP2**, de acordo com a análise da literatura feita nesta revisão sistemática, foi visto que as soluções propostas por alguns autores são efetivas na solução do problema da coerção, a exemplo de Zaghloul *et al.* (2020), Tas e Tanriover (2021), entre outros. Contudo, até nestes trabalhos há ainda a possibilidade de haver coerção. Em alguns casos, entretanto, os autores assumiam contextos impraticáveis, como no exemplo de Dimitriou (2020), em que o autor supôs que o atacante não estaria no mesmo ambiente do eleitor no momento do voto. Ocorre também que os trabalhos vistos nesta revisão apresentam certa incompletude nos sistemas de votação pois algumas características de um sistema robusto não são plenamente incorporadas às soluções desenvolvidas nas publicações. Acontece que em alguns momentos é inevitável abrir mão de uma característica em detrimento de outra. Por exemplo, no trabalho de Li *et al.* (2021), por mais que outras propriedades sejam satisfeitas, a escalabilidade do sistema não foi descrita ou testada, ou o trabalho de Agate *et al.* (2021), onde o sistema é mediado por uma entidade centralizadora.

Apresenta-se, portanto, como oportunidade de dar sequência à este trabalho, a publicação dos resultados da revisão sistemática com o intuito de a comunidade acadêmica

visualize esta lacuna na tecnologia de votação eletrônica e tenham um ponto de partida claro e confiável a partir das análises produzidas neste trabalho corrente.

Concluindo, a tecnologia Blockchain possui uma versatilidade ímpar e seu potencial tem sido explorado com sucesso na aplicação em sistemas de votação eletrônica, trazendo numerosas possibilidades para combater a coerção neste contexto. É possível, então, utilizar mais de um método que combatem a coerção, aliando com métodos de autenticação mistos para por um fim na coerção. Ainda há muito o que desenvolver no campo do combate a coerção, entretanto já há uma gênese encorpada e caminhos que começaram a ser pavimentados com uma base sólida de conhecimento no tema.

REFERÊNCIAS

ABEGUNDE, J.; SPRING, J.; XIAO, H. Seva: A smart electronic voting application using blockchain technology. In: **2021 IEEE International Conference on Blockchain (Blockchain)**. [*S. l.*: *s. n.*], 2021. p. 353–360.

ADESHINA, S. A.; OJO, A. Maintaining voting integrity using blockchain. In: **2019 15th International Conference on Electronics, Computer and Computation (ICECCO)**. [*S. l.*: *s. n.*], 2019. p. 1–5.

ADIPUTRA, C. K.; HJORT, R.; SATO, H. A proposal of blockchain-based electronic voting system. In: **2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)**. [*S. l.*: *s. n.*], 2018. p. 22–27.

AGATE, V.; De Paola, A.; FERRARO, P.; Lo Re, G.; MORANA, M. Secureballot: A secure open source e-voting system. **Journal of Network and Computer Applications**, v. 191, p. 103165, 2021. ISSN 1084-8045. Disponível em: https://www.sciencedirect.com/science/article/pii/S1084804521001776.

AGGARWAL, S.; KUMAR, N. Chapter fifteen - blockchain 2.0: Smart contracts working model. In: AGGARWAL, S.; KUMAR, N.; RAJ, P. (Ed.). **The Blockchain Technology for Secure and Smart Applications across Industry Verticals**. Elsevier, 2021, (Advances in Computers, v. 121). p. 301–322. Disponível em: https://www.sciencedirect.com/science/article/pii/S006524582030070X.

AGGARWAL, S.; KUMAR, N. Chapter nine - architecture of blockchain: Introduction to blockchain. In: AGGARWAL, S.; KUMAR, N.; RAJ, P. (Ed.). **The Blockchain Technology for Secure and Smart Applications across Industry Verticals**. Elsevier, 2021, (Advances in Computers, v. 121). p. 171–192. Disponível em: https://www.sciencedirect.com/science/article/pii/S0065245820300644.

AGRAWAL, K.; AGGARWAL, M.; TANWAR, S.; SHARMA, G.; BOKORO, P. N.; SHARMA, R. An extensive blockchain based applications survey: Tools, frameworks, opportunities, challenges and solutions. **IEEE Access**, v. 10, p. 116858–116906, 2022.

AL-MAAITAH, S.; QATAWNEH, M.; QUZMAR, A. E-voting system based on blockchain technology: A survey. In: **2021 International Conference on Information Technology (ICIT)**. [*S. l.*: *s. n.*], 2021. p. 200–205.

ALVI, S. T.; UDDIN, M. N.; ISLAM, L.; AHAMED, S. 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**, v. 34, n. 9, p. 6855–6871, 2022. ISSN 1319-1578. Disponível em: https://www.sciencedirect.com/science/article/pii/S1319157822002221.

ARAUJO, C. A. A. Bibliometria: evolução histórica e questões atuais. **Em Questão**, v. 12, n. 1, p. 11–32, dez. 2006. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/16.

AWALU, I. L.; KOOK, P. H.; LIM, J. S. Development of a distributed blockchain evoting system. In: . New York, NY, USA: Association for Computing Machinery, 2019. (ICEME 2019), p. 207–216. ISBN 9781450372190. Disponível em: https://doi.org/10.1145/3345035.3345080.

BENABDALLAH, A.; AUDRAS, A.; COUDERT, L.; MADHOUN, N. E.; BADRA, M. Analysis of blockchain solutions for e-voting: A systematic literature review. **IEEE Access**, v. 10, p. 70746–70759, 2022.

BRAGHIN, C.; CIMATO, S.; COMINESI, S. R.; DAMIANI, E.; MAURI, L. Towards blockchain-based e-voting systems. In: ABRAMOWICZ, W.; CORCHUELO, R. (Ed.). **Business Information Systems Workshops**. Cham: Springer International Publishing, 2019. p. 274–286. ISBN 978-3-030-36691-9.

BUTERIN, V. A next generation smart contract & decentralized application platform. In: . [*S. n.*], 2015. Disponível em: https://api.semanticscholar.org/CorpusID:19568665.

CASINO, F.; DASAKLIS, T. K.; PATSAKIS, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. **Telematics and Informatics**, v. 36, p. 55–81, 2019. ISSN 0736-5853. Disponível em: https://www.sciencedirect.com/science/article/pii/S0736585318306324.

CETINKAYA, O.; CETINKAYA, D. Verification and validation issues in electronic voting. v. 5, 01 2007.

CHAEIKAR, S. S.; JOLFAEI, A.; MOHAMMAD, N.; OSTOVARI, P. Security principles and challenges in electronic voting. In: **2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)**. [*S. l.*: *s. n.*], 2021. p. 38–45.

CHAIEB, M.; YOUSFI, S. Loki vote: A blockchain-based coercion resistant e-voting protocol. In: THEMISTOCLEOUS, M.; PAPADAKI, M.; KAMAL, M. M. (Ed.). **Information Systems**. Cham: Springer International Publishing, 2020. p. 151–168. ISBN 978-3-030-63396-7.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, v. 4, p. 2292–2303, 2016.

DEHEZ-CLEMENTI, M.; LACAN, J.; DENEUVILLE, J.-C.; ASGHAR, H.; KAAFAR, D. **A Blockchain-enabled Anonymous-yet- Traceable Distributed Key Generation**. p. 257–265, 2021.

DIMITRIOU, T. Efficient, coercion-free and universally verifiable blockchain-based voting. **Computer Networks**, v. 174, p. 107234, 2020. ISSN 1389-1286. Disponível em: https://www.sciencedirect.com/science/article/pii/S1389128619317414.

GARG, K.; SARASWAT, P.; BISHT, S.; AGGARWAL, S. K.; KOTHURI, S. K.; GUPTA, S. A comparitive analysis on e-voting system using blockchain. In: **2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)**. [*S. l.*: *s. n.*], 2019. p. 1–4.

GOLNARIAN, D.; SAEDI, K.; BAHRAK, B. A decentralized and trustless e-voting system based on blockchain technology. In: **2022 27th International Computer Conference, Computer Society of Iran (CSICC)**. [*S. l.*: *s. n.*], 2022. p. 1–7.

HAO, Y.; ZENG, Z.; CHANG, L. An improved coercion-resistant e-voting scheme. **Security and Communication Networks**, v. 2021, 2021. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118580135&doi=10.1155%2f2021%2f5448370&partnerID=40&md5=18d98da3aff24c10f082b30d3c37c52f.

HARDWICK, F. S.; GIOULIS, A.; AKRAM, R. N.; MARKANTONAKIS, K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)**. [*S. l.*: *s. n.*], 2018. p. 1561–1567.

HUANG, J.; HE, D.; OBAIDAT, M. S.; VIJAYAKUMAR, P.; LUO, M.; CHOO, K.-K. R. The application of the blockchain technology in voting systems: A review. **ACM Comput. Surv.**, Association for Computing Machinery, New York, NY, USA, v. 54, n. 3, apr 2021. ISSN 0360-0300. Disponível em: https://doi.org/10.1145/3439725.

ISLAM, K. S.; ISLAM, M. B.; AVORNU, C.; LOU, J.; SHUKLA, P. K. Blockchain based new e-voting protocol system without trusted tallying authorities. In: **2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)**. [*S. l.*: *s. n.*], 2022. p. 311–317.

JAFAR, U.; AZIZ, M. J. A.; SHUKUR, Z.; HUSSAIN, H. A. A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems. **Sensors**, v. 22, n. 19, 2022. ISSN 1424-8220. Disponível em: https://www.mdpi.com/1424-8220/22/19/7585.

JUELS, A.; CATALANO, D.; JAKOBSSON, M. Coercion-resistant electronic elections. In: **Proceedings of the 2005 ACM workshop on Privacy in the electronic society**. [*S. l.*: *s. n.*], 2005. p. 61–70.

KHO, Y.-X.; HENG, S.-H.; CHIN, J.-J. A review of cryptographic electronic voting. **Symmetry**, v. 14, n. 5, 2022. ISSN 2073-8994. Disponível em: https://www.mdpi.com/2073-8994/14/5/858.

KUMAR, M.; CHAND, S.; KATTI, C. P. A secure end-to-end verifiable internet-voting system using identity-based blind signature. **IEEE Systems Journal**, v. 14, n. 2, p. 2032–2041, 2020.

KUMAR, R.; BADWAL, L.; AVASTHI, S.; PRAKASH, A. A secure decentralized e-voting with blockchain smart contracts. In: **2023 13th International Conference on Cloud Computing, Data Science Engineering (Confluence)**. [*S. l.*: *s. n.*], 2023. p. 419–424.

LE, T.-V.; HSU, C.-L. A systematic literature review of blockchain technology: Security properties, applications and challenges. **Journal of Internet Technology**, v. 22, p. 789–801, 07 2021.

LI, P.; LAI, J.; WU, Y.; SCIANCALEPORE, S. Publicly traceable attribute-based anonymous authentication and its application to voting. **Sec. and Commun. Netw.**, John Wiley Sons, Inc., USA, v. 2021, jan 2021. ISSN 1939-0114. Disponível em: https://doi.org/10.1155/2021/6611518.

LI, W.; XIONG, H. Efficient proxy re-encryption scheme for e-voting system. **KSII Transactions on Internet and Information Systems**, v. 15, n. 5, p. 1847 – 1870, 2021. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85107418362&doi=10.3837%2ftiis.2021.05.015&partnerID=40&md5=c2c8c91fc878f7caf967a2e6001cab5f.

MURTAZA, M. H.; ALIZAI, Z. A.; IQBAL, Z. Blockchain based anonymous voting system using zksnarks. In: **2019 International Conference on Applied and Engineering Mathematics (ICAEM)**. [*S. l.*: *s. n.*], 2019. p. 209–214.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Decentralized business review**, 2008.

POOJA, S.; RAJU, L. K.; CHHAPEKAR, U.; CH, C.; C.B, r. C. Face detection using deep learning to ensure a coercion resistant blockchain-based electronic voting. **Engineered Science**, v. 16, p. 341–353, 2021. ISSN 2576-9898. Disponível em: http://dx.doi.org/10.30919/es8d585.

RAJ, P. Chapter one - demystifying the blockchain technology. In: AGGARWAL, S.; KUMAR, N.; RAJ, P. (Ed.). **The Blockchain Technology for Secure and Smart Applications across Industry Verticals**. Elsevier, 2021, (Advances in Computers, v. 121). p. 1–42. Disponível em: https://www.sciencedirect.com/science/article/pii/S0065245820300565.

SADIA, K.; MASUDUZZAMAN, M.; PAUL, R. K.; ISLAM, A. Blockchain-based secure e-voting with the assistance of smart contract. In: PATEL, D.; NANDI, S.; MISHRA, B.; SHAH, D.; MODI, C. N.; SHAH, K.; BANSODE, R. S. (Ed.). **IC-BCT 2019**. Singapore: Springer Singapore, 2020. p. 161–176.

SERTKAYA, I.; ROENNE, P.; RYAN, P. Y. Estonian internet voting with anonymous credentials. **Turkish Journal of Electrical Engineering and Computer Sciences**, v. 30, p. 420 – 435, 2022. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85125950900&doi=10.3906%2felk-2105-197&partnerID=40&md5=415c5e6c6e3dda671ecc7d44234bc605.

SHAMSEER, L.; MOHER, D.; CLARKE, M.; GHERSI, D.; LIBERATI, A.; PETTICREW, M.; SHEKELLE, P.; STEWART, L. A. Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015: elaboration and explanation. **BMJ**, BMJ Publishing Group Ltd, v. 349, 2015. Disponível em: https://www.bmj.com/content/349/bmj.g7647.

SHIM, K.-A. A survey of public-key cryptographic primitives in wireless sensor networks. **IEEE Communications Surveys Tutorials**, v. 18, n. 1, p. 577–601, 2016.

SPADAFORA, C.; LONGO, R.; SALA, M. **A coercion-resistant blockchain-based E-voting protocol with receipts**. 2023. 500-521 p. Disponível em: /article/id/95027388-43f9-4586-8db5-120145b15708.

SUWITO, M. H.; DUTTA, S. Verifiable e-voting with resistance against physical forced abstention attack. In: **2019 International Workshop on Big Data and Information Security (IWBIS)**. [*S. l.*: *s. n.*], 2019. p. 85–90.

SWAN, M. **Blockchain: Blueprint for a New Economy**. 1st. ed. [*S. l.*]: O'Reilly Media, Inc., 2015. ISBN 1491920491.

TAS, R.; TANRIOVER, O. O. A systematic review of challenges and opportunities of blockchain for e-voting. **Symmetry**, v. 12, n. 8, 2020. ISSN 2073-8994. Disponível em: https://www.mdpi.com/2073-8994/12/8/1328.

TAS, R.; TANRIOVER, O. O. A manipulation prevention model for blockchain-based e-voting systems. **Security and Communication Networks**, v. 2021, 2021. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105757733&doi=10.1155%2f2021%2f6673691&partnerID=40&md5=4a55a7bc7a90da23683b2727eb51504d.

VLADUCU, M.-V.; DONG, Z.; MEDINA, J.; ROJAS-CESSA, R. E-voting meets blockchain: A survey. **IEEE Access**, v. 11, p. 23293–23308, 2023.

WIDAYANTI, R.; AINI, Q.; HARYANI, H.; LUTFIANI, N.; APRILIASARI, D. Decentralized electronic vote based on blockchain p2p. In: **2021 9th International Conference on Cyber and IT Service Management (CITSM)**. [*S. l.*: *s. n.*], 2021. p. 1–7.

ZAGHLOUL, E.; LI, T.; REN, J. Anonymous and coercion-resistant distributed electronic voting. In: **2020 International Conference on Computing, Networking and Communications (ICNC)**. [*S. l.*: *s. n.*], 2020. p. 389–393.

ZAGHLOUL, E.; LI, T.; REN, J. d-bame: Distributed blockchain-based anonymous mobile electronic voting. **IEEE Internet of Things Journal**, v. 8, n. 22, p. 16585–16597, 2021.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. In: **2017 IEEE International Congress on Big Data (BigData Congress)**. [*S. l.*: *s. n.*], 2017. p. 557–564.