Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

DANILO PEREIRA DE LIMA

SISTEMA ELEITORAL BRASILEIRO UTILIZANDO BLOCKCHAIN

Brasília
2021

DANILO PEREIRA DE LIMA

SISTEMA ELEITORAL BRASILEIRO UTILIZANDO BLOCKCHAIN

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. MSc. Rafael Sarres

Brasília
2021

DANILO PEREIRA DE LIMA

SISTEMA ELEITORAL BRASILEIRO UTILIZANDO BLOCKCHAIN

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu em* Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. MSc. Rafael Sarres

Brasília, ___ de _____ de 2021.

Banca Examinadora

_____

Prof. Dra. Tânia Cristina da Silva Cruz

_____

Prof. Sylas Rodrigues Mendes

AGRADECIMENTO(S)

Aos meus pais, de quem herdei o incessante desejo de encontrar respostas para os vários fenômenos que compõe e afetam as nossas vidas. Em especial, minha mãe, empregada doméstica, que me ensinou que a maior riqueza que existe na vida é o conhecimento. Faço menção honrosa a minha avó Maria das Dores (in memorian) cujos traços de caráter e compaixão me foram transmitidos.

A minha companheira, Cristiane Alves de Lima pelo apoio, incentivo, compreensão, auxílio, carinho incomensuráveis. Pelos conselhos, direcionamentos e confiança. Pelo exemplo de conduta pessoal e profissional que continuamente me inspiram.

Ao Prof. Rafael Sarres, meu orientador, pelo seu exemplo de profissionalismo e dedicação acadêmica. Pela experiência compartilhando o seu vasto conhecimento em sala de aula. Pela influência na minha formação enquanto pesquisador. Pela confiança depositada em mim quando assumiu este projeto. Por me direcionar trazendo contribuições importantíssimas e, sobretudo, pela compreensão e paciência na condução do desenvolvimento deste trabalho.

Aos professores do curso de Rede de Computadores com Ênfase em Segurança do UniCEUB pelo comprometimento com o curso no momento de pandemia. Aos colegas de classe que fizeram parte dessa jornada nos momentos de aprendizado e descontração.

Ao amigo Ricardo Alexandre, companheiro de profissão, pelo incentivo dentro e fora da academia, pelas discussões técnicas que sempre contribuíram para o enriquecimento do conhecimento, e por sempre lutar ao meu lado nos momentos difíceis. A amiga Cristiany Souza, companheira de profissão, pela inspiração profissional, pelas contribuições que sempre enriquecem meu profissionalismo, pelos incentivos acadêmico e profissional. Ao amigo Diego Rocha, companheiro de profissão, pelo incentivo dentro e fora da academia, pelas discussões acadêmicas que foram muito importantes para minha evolução, pelos desafios propostos e vencidos e por sempre acreditar no meu potencial.

A todas as pessoas que contribuíram direta ou indiretamente e que deixei de mencionar, estendo os meus agradecimentos.

“Cometer injustiça é pior do que sofrê-la.”

Platão

RESUMO

O Brasil possui um dos melhores o sistema eletrônico de votação do mundo. Nenhum sistema eleitoral no mundo possui capacidade de apuração semelhante ao brasileiro. Contudo, verifica-se alguns problemas, como a falta de transparência uma vez que a verificação do processo eleitoral é centralizada no Tribunal Superior Eleitoral (TSE) e a alguns consultores convidados, não havendo possibilidade de uma auditoria completa. Este estudo de caso se propõe a compreender como ocorre o processo eletrônico de votação brasileiro e a viabilidade de utilização de tecnologia blockchain no processo, além demonstrar a inviabilidade do eleitor executar seu voto on-line. Assim, objetiva-se demonstrar como a auditoria proposta pela tecnologia blockchain pode ser utilizada em contra ponto a validação do eleitor pela impressão do voto.

Palavras-chave: Segurança da informação. Blockchain. Processo eleitoral brasileiro. Sufrágio universal. Urna Eletrônica.

ABSTRACT

Brazil has one of the best electronic voting systems in the world. No electoral system in the world has a counting capacity similar to that of Brazil. However, there are some problems, such as the lack of transparency since the verification of the electoral process is centralized at the Superior Electoral Court (TSE) and some invited consultants, with no possibility of a complete audit. This case study aims to understand how the Brazilian electronic voting process occurs and the feasibility of using blockchain technology in the process, in addition to demonstrating the impracticability of the voter to perform his vote online. Thus, the objective is to demonstrate how the audit proposed by blockchain technology can be used in counterpoint the validation of the voter by the impression of the vote.

Key words: Information security. Blockchain. Brazilian electoral process. Universal suffrage. Electronic Urn.

SUMÁRIO

INTRODUÇÃO

O nível de informatização do sistema eleitoral foi alcançado gradualmente, sempre passando pelo crivo da segurança e da garantia do sigilo do voto, acompanhando as evoluções tecnológicas. Entretanto, a criação de um aparelho mecanizado para coletar votos é um desejo antigo no país. O primeiro Código Eleitoral, de 1932, previa em seu artigo 57 o “uso das máquinas de votar, regulado oportunamente pelo Tribunal Superior Eleitoral”, devendo ser assegurado o sigilo do voto. Na década de 1990, a urna eletrônica tornou-se uma realidade.

Em setembro de 2020, O Tribunal Superior Eleitoral publicou um edital de chamamento público a empresas de tecnologia para que apresentem propostas de soluções de evolução do sistema eletrônico de votação que é adotado no Brasil desde 1996. A iniciativa faz parte do Projeto Eleições do Futuro, que tem como objetivo usar a tecnologia em favor do cidadão.

O Sumário Executivo Levantamento da Tecnologia Blockchain do Tribunal de Contas da União (2020) afirma que, a blockchain se enquadrada como uma tecnologia de propósito geral, ou seja, uma tecnologia com características únicas e capazes de impactar drasticamente as relações econômicas e sociais preexistentes, bem como prover significativas melhorias e facilitar a criação de inovações em diversos setores governamentais.

O presente estudo se propõe a compreender como se dá o processo eletrônico de votação utilizado pelo Tribunal Superior Eleitoral e a viabilidade de utilização de tecnologia blockchain para realização de um pleito eleitoral.

Os objetivos do presente trabalho são: Compreender a segurança e a auditoria do sistema eleitoral brasileiro analisando os seus limites para implementação de uma rede blockchain de acordo com a legislação brasileira. Observando a possibilidade de realização da votação on-line e a possibilidade da auditoria do eleitor na cédula de votação utilizada para registro do voto.

Para alcançar esses objetivos, procedeu-se de pesquisa metodológica e um estudo de caso para resoluções dos problemas apresentados.

Espera-se demonstrar com a presente pesquisa a possibilidade de utilização da tecnológica blockchain no processo eleitoral e uma reflexão sobre o

poder de auditoria e transparência que a tecnologia pode proporcionar. Sob a ótica acadêmica, a presente pesquisa pretende trazer soluções para os estudos de casos publicados sobre sistemas eleitorais utilizando tecnologia blockchain. Além disso, contribuirá para a reflexão de conceitos existentes para tais sistemas, a impossibilidade de realização de um pleito totalmente on-line e a auditoria do eleitor na cédula de votação utilizada pelo mesmo.

O presente trabalho foi então estruturado em 3 capítulos. No primeiro capítulo tem como objetivo demostrar como funciona o Sistema Eletrônico de Votação e de Totalização dos Votos, observando alguns processos que são importantes no aspecto da segurança da informação para garantir a lisura e auditoria das eleições brasileiras de acordo com a legislação; no segundo capítulo proporciona uma análise a partir de publicações técnicas e estudos acadêmicos sobre Distributed Ledger Technology (DLT) e Blockchain, além de abordar as principais características da tecnologia que podem contribuir com o processo de transformação digital do Sistema Eletrônico de Votação e de Totalização dos Votos; no terceiro capítulo, apresenta-se como estudo de caso a possibilidade de implementação da tecnologia blockchain para ser utilizada no Sistema Eletrônico de Votação e de Totalização dos Votos.

1 DIREITO ELEITORAL

Os processos que ocorrem em todas as etapas de eleição são regidos por um conjunto de leis e normas, o Direito Eleitoral tem como base jurídica a Constituição Federal, o Código Eleitoral (Lei 4.737/1965), a Lei das Eleições (Lei 9.504/1997), a Lei dos Partidos Políticos, (Lei 9.096/1995), a Lei da Inelegibilidade (LC 64/1990), a Lei da Ficha Limpa (LC 135/2010), sem prejuízo de outras normas jurídicas, como as derivadas de atos normativos dos tribunais eleitorais, sem prejuízo da jurisprudência e doutrina acerca da matéria (TEIXEIRA; ESTANCIONE, 2016).

1.1 Voto Secreto

A Democracia significa participação do povo nas decisões mais importantes do país. Essa participação pode ocorrer de forma direta, indireta, plebiscito, referendo ou iniciativa legislativa popular. O voto é o instrumento que viabiliza a democracia, ou seja, quando falta ética no voto, conspurca-se a estética da democracia (GOMES, 2021).

Canotilho (2003) indica a liberdade do voto e o voto secreto como princípios materiais do sufrágio. A liberdade de voto significa garantir ao eleitor o exercício do direito de voto sem qualquer coação física ou psicológica de entidades públicas ou de entidades privadas. O princípio do voto secreto significa que o cidadão eleitor guarda para si a sua decisão, o que pressupõe não só a pessoalidade do voto, como a proibição de sinalização do voto, bem como deve impossibilitar uma reconstrução posterior do sentido da imputabilidade subjetiva do voto (RORIZ, 2013 apud CANOTILHO, 2003).

Segundo Toledo (2016), o artigo 1º, parágrafo único da Constituição, permite verificar a forma ativa em que o povo exerce o seu direito ao voto e a forma passiva do direito político de ser votado.

> Art. 1º Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição (Brasil, 1988).

Toledo (2006) menciona que os termos “cidadania” e “direitos fundamentais” popularizaram-se em nosso país com o final da ditadura militar e com a promulgação da Constituição Federal de 1988.

> Decorre do art. 14 e parágrafos da Constituição Federal de 1988 e tem o seguinte conteúdo normativo que resulta da letra do preceito: (a) o sufrágio é universal e o alistamento obrigatório, (b) o voto é direto, secreto, obrigatório e igual para todos. Por outro lado, implicitamente, denota-se que o voto é, também, pessoal (TOLEDO, 2006 apud MENDES, 1994).

> Art. 14. A soberania popular será exercida pelo sufrágio universal e pelo voto direto e secreto, com valor igual para todos, e, nos termos da lei, mediante: I – plebiscito; II – referendo; III – iniciativa popular (Brasil, 1988).

> O voto é exercido de forma direta, e, na lição no Professor Alexandre de Moraes, apresenta diversas características constitucionais, quais sejam, personalidade, obrigatoriedade, liberdade, sigilosidade, igualdade e periodicidade (TOLEDO, 2006 apud MORAES, 2003).

Toledo (2006) reforça que o artigo 60, § 4º da Constituição Federal prevê como cláusula pétrea o voto direto, secreto, universal e periódico. Acolhe-se, portanto, a afirmação de Pinto Ferreira “A essência da República está no voto direto, secreto, universal e periódico” (TOLEDO, 2006 apud FERREIRA, 1992).

> Art. 60 § 4º Não será objeto de deliberação a proposta de emenda tendente a abolir: I - a forma federativa de Estado; II - o voto direto, secreto, universal e periódico; III - a separação dos Poderes; IV - os direitos e garantias individuais (Brasil, 1988).

1.2 Sistema Eletrônico de Votação

O sistema eleitoral brasileiro informatizado no que diz respeito a votação e totalização de votos é regido dos artigos 59 a 62 da Lei nº 9.504/97, abaixo a descrição do artigo 59 que garante que as eleições ocorram utilizando sistema eletrônico (TEIXEIRA; ESTANCIONE, 2016).

> Art. 59. A votação e a totalização dos votos serão feitas por sistema eletrônico, podendo o Tribunal Superior Eleitoral autorizar, em caráter excepcional, a aplicação das regras fixadas nos artigos 83 a 89 (BRASIL, 1997).

Em casos excepcionais o Direito Eleitoral utiliza dos artigos 83 a 89, para poder garantir as eleições utilizando cédulas manuais confeccionadas para Justiça Eleitoral (BRASIL, 1997).

1.2.1 Urnas Eletrônica

A Procomp Indústria Eletro eletrônico, atual Diebold, líder de automação bancária no Brasil, contratou a Fundação Centros de Referência em Tecnologias Inovadoras – CERTI, como parceira tecnológica para o concorrer o edital do TSE para o projeto de criação da urna eletrônica (FUNDAÇÃO CENTROS DE REFERÊNCIA EM TECNOLOGIAS INOVADORAS, 2021).

> A CERTI, ampliando seu processo de desenvolvimento rápido de produtos, executou o projeto mecânico da urna eletrônica, além de contribuir no desenvolvimento do hardware (HD) eletrônico, do software (SW) de apoio e nos testes do produto (HW, SW e embalagem). A solução da urna Diebold apresentou as características de pouco mais de 8kg de peso, teclado numérico, pequeno monitor de cristal líquido e autonomia de 12 horas de funcionamento sem energia externa. Em 2000, as urnas receberam ainda um dispositivo de áudio através do qual, usando fones de ouvido, deficientes visuais passaram a ter condições de ouvir a confirmação dos números digitados no teclado, que também contava com identificação em braile (FUNDAÇÃO CENTROS DE REFERÊNCIA EM TECNOLOGIAS INOVADORAS, 2021).

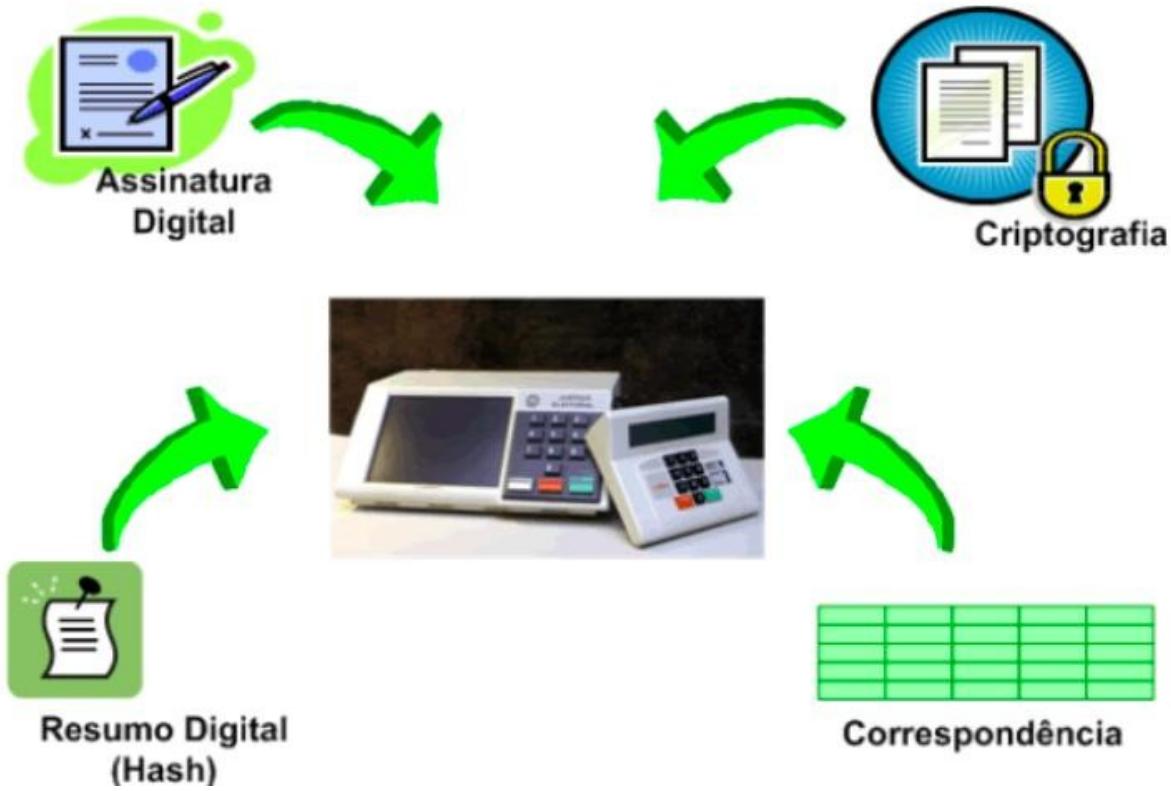
A urna eletrônica é composta por dois componentes, o terminal do mesário e o terminal do eleitor. O terminal do mesário possibilita a identificação do eleitor, em alguns modelos e verificado através da biometria, após a verificação é habilitado o terminal do eleitor para votação. Os componentes são de uso específico para eleições, com as seguintes características: resistente, de pequenas dimensões, leve, com autonomia de energia e com recursos de segurança (TRIBUNAL SUPERIOR ELEITORAL, 2021a).

Figura 1: Urna Eletrônica

Fonte: Tribunal Superior Eleitoral

A urna eletrônica possui os seguintes mecanismos de segurança: assinatura digital, criptografia, resumo digital e a tabela de correspondência de todas as urnas utilizadas (TRIBUNAL SUPERIOR ELEITORAL, 2021a).

Figura 2: Mecanismo de segurança



Fonte: Tribunal Superior Eleitoral

A criptografia é um mecanismo de segurança que tem o objetivo de embaralhar os dados tornando inacessíveis a pessoas não autorizadas, usando na técnica de assinatura digital. A urna eletrônica utiliza a assinatura digital nos seguintes casos, para garantir a integridade do conteúdo dos arquivos digitais, isto é, visa garantir que os softwares não sejam modificados intencionalmente ou não perca as características originais por possíveis falhas, é também para assegurar a autenticidade dos softwares, confirmando que o software assinado tenha origem oficial, ou seja, que foi gerado pelo TSE (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

O resumo digital também utiliza o mecanismo de criptografia para geração de hash, utilizando um arquivo digital, pode-se calcular o resumo digital deste arquivo com algoritmo público (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

> No caso dos sistemas de urna, são calculados os hashes de todos os arquivos e esses resumos são publicados no portal do TSE (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

Os resultados recebidos somente são processados se houver uma correspondência anterior entre uma urna específica e a seção para a qual foi preparada, a tabela de correspondência tem como objetivo validar se o resultado a urna não é proveniente de uma urna não preparada para seção, gerando uma pendencia para o Juiz Eleitoral analisar. A tabela de correspondência é única na urna para cada eleição (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

O Registro Digital do Voto (RDV) é o arquivo onde armazena os votos dos eleitores em uma urna eletrônica, tem como objetivo registrar os votos exatamente como foram digitados pelos eleitores, visando garantir o sigilo do voto, registrando em posições aleatórias do arquivo. É permitida a obtenção dos arquivos pelos partidos políticos e às coligações se julgarem necessários, permitindo assim, que seja executado uma auditoria externa. Através deste arquivo é emitido a zerésima, indicando que a urna não possui votos registrados e o boletim de urna com o totalizador dos votos contido no final da eleição (TRIBUNAL SUPERIOR ELEITORAL, 2021c).

A preparação das urnas eletrônicas para a eleição ocorre em duas etapas: cerimônia de assinatura digital e lacração dos sistemas eleitorais e a cerimônia de geração de mídias, preparação e lacração das urnas eletrônicas, somente após essas cerimônias a urna eletrônica se torna apta para participar do pleito (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

1.2.2 Cerimônia de assinatura digital e lacração dos sistemas eleitorais

A cada pleito o Tribunal Superior Eleitoral (TSE) realiza a Cerimônia de Assinatura Digital e Lacração dos Sistemas Eleitorais. O evento legitima os programas que serão utilizados nas urnas eletrônicas e equipamentos correlatos para o pleito. No encerramento da cerimônia, os arquivos dos sistemas devem estar assinados por meio de certificação digital e também fisicamente, pelo presidente do TSE e pelo diretor-geral da Polícia Federal. A cerimônia de lacração está prevista na Resolução TSE nº 23.611/2019 (TRIBUNAL SUPERIOR ELEITORAL, 2021d).

A legislação estabelece como uma das formas de fiscalização do processo eleitoral o acompanhamento do desenvolvimento dos softwares que serão instalados nas urnas eletrônicas e funcionarão durante as eleições, por partidos políticos, pela Ordem dos Advogados do Brasil (OAB) e pelo Ministério Público até seis meses antes das eleições, culminando com os procedimentos de lacração dos programas confeccionados para o pleito. A Resolução do TSE nº 23.550/2017 ampliou tal acesso aos representantes do Congresso Nacional, do Supremo Tribunal Federal, da Controladoria-Geral da União, da Polícia Federal, da Sociedade Brasileira da Computação, do Conselho Federal de Engenharia e Agronomia e dos departamentos de tecnologia da informação de universidades (TRIBUNAL SUPERIOR ELEITORAL, 2021d).

> As assinaturas digitais geram uma blindagem em todos esses programas e ainda garantem a autoria e a integridade das informações. Cada uma das assinaturas feitas hoje gera um resumo digital. Seria como uma lauda, onde se faz uma análise de algoritmos matemáticos e ali é gerado um dígito verificador. Se for alterado um ponto ou uma vírgula, por exemplo, esse dígito verificador não confere mais. Isso garante a integridade da urna (TRIBUNAL SUPERIOR ELEITORAL, 2021d).

Os programas lacrados são distribuídos para os TREs para que possam ser inseridos nas urnas eletrônicas, juntamente com os dados dos eleitores e dos candidatos, cada TRE tem sua própria cerimônia de preparação e carga (TRIBUNAL SUPERIOR ELEITORAL, 2021d).

1.2.3 Cerimônia preparação e lacração das urnas eletrônicas

A cerimônia de geração de mídias, preparação e lacração das urnas eletrônicas é um dos procedimentos que visa de assegurar a segurança e o sigilo do voto do cidadão (TRIBUNAL SUPERIOR ELEITORAL, 2021e).

A urna eletrônica utiliza dois tipos de mídia, uma em formato de cartão de memória, também conhecido como flash card e outra em formato exclusivo da Justiça Eleitoral conhecida como memória de resultado. A primeira etapa de preparação é concluída após a instalação de sistema operacional, programas, bibliotecas e dados eleitorais. A segunda e última etapa é concluída com a realização de vários testes para comprovar o correto funcionamento (TRIBUNAL SUPERIOR ELEITORAL, 2021e).

Após as urnas eletrônicas receberem os programas com dados dos candidatos e dos respectivos eleitores da seção de votação, uma porcentagem de urnas é selecionada por entidades e instituições presentes para a realização de testes, sendo pelo menos uma por zona eleitoral. Em seguida, é realizada a lacração física do compartimento, com selo fabricado pela Casa da Moeda seguindo os critérios e modelos contido na Resolução do TSE nº 23.552/2017 (TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO, 2021).

Com isso, todas as urnas, inclusive as de contingências, são as que vão receber a justificativa de ausência, estarão prontas para serem utilizadas durante o pleito, não podendo haver mais nenhuma alteração. Depois de preparadas e lacradas, as urnas só realizam operação em dia e horário determinado, ou seja, na data definida para a eleição (TRIBUNAL SUPERIOR ELEITORAL, 2021f).

A cerimônia pública é divulgada no Diário da Justiça Eletrônico (DJE) e pode ser acompanhada por partidos políticos, coligações, Ministério Público, Ordem dos Advogados do Brasil (OAB) e cidadãos interessados (TRIBUNAL SUPERIOR ELEITORAL, 2021f).

1.2.4 Dia da eleição

O mesário é o representante da Justiça Eleitoral que compõe a mesa receptora de votos, assim que liga a urna é impresso um comprovante que mostra que não há votos computados no equipamento, a zerésima. O sistema só permite que a urna seja aberta para votação na hora definida pelo TSE (TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, 2019).

Durante o período de votação, é feito a validação e identificação do eleitor pelo mesário, verificando se está apto a votar, só então a votação é autorizada, em seguida e realizada uma validação da identidade por identificação biométrica (TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, 2019).

O eleitor finalizando a votação começa o registro para contagem de votos e o trabalho de segurança, garantindo que não haja alteração e fraude. Após a conclusão da votação, o sistema criptografa os dados, faz o registro digital do voto e cria uma assinatura digital para ele, que funciona como um certificado de

inviolabilidade. Se alguém tentar alterar o voto, a urna para de funcionar e a tentativa de fraude é detectada (TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, 2019).

No encerramento das seções de votação, o mesário imprime cinco vias do boletim de urna, com o número de votos registrados para cada candidato e o pen drive contendo a memória de resultado, é retirado da urna e levado pelo mesário ao cartório eleitoral. Os dados criptografados são enviados à central de contagem do TRE, via rede virtual privativa e protegida da Justiça Eleitoral. Na central de totalização, um software confere a autenticidade das informações, decodifica os dados e faz a contagem geral de votos no Estado. Por fim, o TSE faz a leitura das bases de dados dos TREs, recebe e consolida os votos e divulga a contagem em tempo real de todos os votos de todos os Estados (TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, 2019).

1.2.4.1 Votação paralela

A votação paralela funciona da seguinte forma: os participantes recolhem uma cédula da urna lacrada, revelam aos fiscais e demais presentes, os candidatos escolhidos e, em seguida, digitam os números correspondentes no Sistema de Apoio à Votação Paralela e na urna eletrônica. Todo o processo é fiscalizado e filmado. A fiscalização da votação paralela tem como objetivo a verificação da assinatura digital, a verificação do resumo digital, a comparação do resultado da votação por cédula com o resultado do boletim de urna, verificação da filmagem do procedimento e do registro do sistema e a verificação do Registro Digital do Voto (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

É mais um mecanismo da Justiça Eleitoral utilizada para comprovar a credibilidade do sistema eletrônico de votação. Ocorre no dia das eleições é são convidados fiscais de partidos políticos e coligações, representantes da Ordem dos Advogados do Brasil, bem como entidades representativas da sociedade. É realizada em local designado pelos tribunais regionais eleitorais após o sorteio de duas a quatro urnas eletrônicas na véspera da eleição. Simultaneamente à votação oficial é apresentada auditoria de verificação do funcionamento das urnas eletrônicas (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

1.2.5 Teste Público de Segurança

Com objetivo de dar mais transparência e contribuir para o aperfeiçoamento da urna eletrônica, em 2015 o TSE publicou a Resolução TSE nº 23.444/2015 que determina que os Testes Públicos de Seguranças sejam realizados a cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais (TRIBUNAL SUPERIOR ELEITORAL, 2021b).

1.2.5.1 Testes Públicos de Segurança do Sistema Eletrônico de Votação 2017

A Justiça Eleitoral promoveu, nos dias 28, 29 e 30 de novembro de 2017, a 4ª edição dos Testes Públicos de Segurança do sistema eletrônico de votação, em busca da participação da sociedade para o aperfeiçoamento da urna eletrônica (TRIBUNAL SUPERIOR ELEITORAL, 2021g).

A cada TPS os investigados encontram contribuições importantes, a edição de 2017 foram apresentadas evidências relevantes em seus planos de testes a respeito da segurança da urna eletrônica, a partir do ambiente criado para a realização dos testes. O Grupo 1, coordenado pelo professor Diego de Freitas Aranha, obtiveram sucesso na execução de quatro planos de teste. O investigador individual Cássio Goldschmidt obteve achados parciais, mas não completou todos os passos previstos. O Grupo 4, com três integrantes, coordenado por Ivo de Carvalho Peixinho, obteve sucesso parcial na execução de um plano de teste (TRIBUNAL SUPERIOR ELEITORAL, 2017a).

O Grupo 1 coordenado pelo professor Diego Aranha, teve como principal objetivo detectar e utilizar uma sequência de vulnerabilidade para injetar código de autoria nos programas da urna eletrônica antes do processo de carga (TRIBUNAL SUPERIOR ELEITORAL, 2017a).

> “Essa instalação é realizada a partir de um cartão de memória preparado pelos TREs, chamado flash de carga, que pode instalar software em até dezenas de urnas. As vulnerabilidades necessárias para isso foram encontradas na decifração do cartão de memória para revelar seu conteúdo, a partir da captura da chave criptográfica diretamente do código-fonte; e na existência de bibliotecas de código cujas assinaturas não eram verificadas pelo sistema, problema causado por uma combinação de erros de programação e falha procedimental. O relatório do TSE é bem detalhado ao descrever contramedidas, mas essencialmente o corpo técnico do Tribunal deve trabalhar em aprimorar o processo de autenticação do software para evitar injeção de código intruso e mover as chaves criptográficas armazenadas diretamente no código-fonte para lugares de armazenamento

> mais seguro", explica Diego Aranha (TRIBUNAL SUPERIOR ELEITORAL, 2017a).

O plano de teste do investigador individual, Cássio Goldschmidt, tinha como objetivo fazer uma revisão de código e teste dinâmico de geração das mídias para preparação da urna eletrônica. As recomendações geradas pelo investigador foram, a primeira, durante a revisão do código-fonte, o investigador encontrou uma fragilidade no sistema que possibilita inserir código malicioso sem detecção dentro de fotos dos candidatos que serão carregados, a segunda refere-se à proteção contra transbordamento de dados (TRIBUNAL SUPERIOR ELEITORAL, 2017a).

> Esse tipo de exploração foi usado em muitos vírus famosos que abalaram a Internet, como o Code Red e o SQL slammer. Minha recomendação detalha como o TSE pode usar medidas de proteção proativas para prevenir um possível ataque de transbordamento de dados em todos os componentes do sistema. Informou investigador individual, Cássio Goldschmidt (TRIBUNAL SUPERIOR ELEITORAL, 2017a).

O Grupo 4 liderado por Ivo de Carvalho Peixinho ficou responsável pela execução do plano de teste "Extração de chave privada do Sistema Operacional da Urna Eletrônica". O grupo havia percebido do TPS, de 2016, era uma proteção no cartão o que impedia o carregamento do sistema operacional impossibilitando a instalação dos softwares em um PC tradicional. Segundo Peixinho, no TPS 2017, em um ambiente virtualizado é possível extrair a memória volátil da urna. A partir dessa extração é obtêm-se as chaves de criptografia utilizada para cifrar os arquivos que são usados na urna, incluindo programas, bibliotecas, arquivos de configurações e chaves de criptografia (TRIBUNAL SUPERIOR ELEITORAL, 2017a).

De acordo com o Relatório da Comissão Avaliadora do Teste Público de Segurança (2017), pode-se afirmar que nenhuma das vulnerabilidades apontadas neste TPS de 2017 poderia ser exercitada com o atual estado tecnológico de desenvolvimento do software da urna eletrônica, ressalta-se que os resultados apresentados não eximem a possibilidade da existência de outras vulnerabilidades não identificadas pelos investigadores (TRIBUNAL SUPERIOR ELEITORAL, 2018).

1.2.5.2 Testes Públicos de Segurança do Sistema Eletrônico de Votação 2019

Nos dias 25 a 29 de novembro de 2019, a Justiça Eleitoral promoveu, a 5ª edição dos Testes Públicos de Segurança do sistema eletrônico de votação, com o

objetivo de buscar a colaboração da sociedade brasileira para o aperfeiçoamento do sistema eletrônico (TIINSIDE, 2019).

A edição de 2019, contou com 22 investigadores, divididos em cinco grupos e três investigadores individuais, foram apresentados 13 planos de ataque. Dois planos de teste executado pelo Grupo 5 foram bem sucedidos. O Grupo 5 foi liderado por Paulo César Hermann Wanner em parceria com Ivo Peixinho e Galileu Batista de Souza, todos peritos da Polícia Federal, outro plano de teste que merece destaque foi do investigador individual Leonardo dos Santos (TIINSIDE, 2019).

O Grupo 5 liderado pelo perito da Polícia Federal Paulo César Hermann Wanner, apresentaram três planos de teste em que consistia na extração de dados e configuração do Kit JE Connect, na extração do conteúdo de disco criptografado do Subsistema de Instalação e Segurança - SIS e na instalação e execução do código arbitrário em uma máquina do Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica - GedaiUE para carregar dados falsos na urna eletrônica (TIINSIDE, 2019).

Através de engenharia reversa, foi possível obter a chave do disco criptografado do SIS, o Grupo 5 conseguiu montar o disco criptografado fora do ambiente SIS e, por consequência, a captura dos arquivos do GedaiUE, após alguns avanços as tentativas de execução do GedaiUE fora de uma instalação do sistema homologado pelo TSE não foram bem sucedidas. Vale ressaltar que houve um relaxamento de algumas barreiras de segurança, como fornecimento da senha de configuração e senha de usuários locais, o que permite definir que os ataques realizados pelo grupo teriam origem interna do TSE (TIINSIDE, 2019).

Sobre o plano de teste do investigador individual Leonardo dos Santos, conforme documento publicado, embora não tenha obtido sucesso em suas tentativas de identificação de padrões em circuito elétrico de uma urna eletrônica, foi sugerido pelo investigador, que os sinais sonoros emitidos pela urna eletrônica fosse diferenciado, atualmente o sinal sonoro emitido ao ligar e ao desligar a urna eletrônica é o mesmo sinal sonoro emitido no momento da votação, o que poderia levar ao entendimento de um início de votação fora do previsto para o início da sessão (TIINSIDE, 2019).

A Comissão Avaliadora incluiu algumas recomendações, a instituição de um Comitê de Assessoria Perene por considerar que os ajustes nos sistemas eleitorais são realizados de forma continuada, acompanhando as modificações propostas durante todo o ano e não apenas durante o TPS, outra sugestão importante é quanto a realização do TPS, entre as questões apontadas no relatório da comissão, está a possibilidade da equipe de apoio técnico dispor de tablets para que os investigadores entrem em contato com os responsáveis técnicos, bem como permitir a troca de informação entre os investigadores (TIINSIDE, 2019).

1.3 Eleição do Futuro 2020

Com objetivo de conhecer soluções de votação, preferencialmente on-line, o Diretor-Geral da Secretaria do Tribunal Superior Eleitoral publicou um edital de chamamento público às empresas e instituições de direito privado para demostrar seus sistemas de votação (TRIBUNAL SUPERIOR ELEITORAL, 2021i).

As soluções apresentadas pelas empresas precisavam atendar os requisitos mínimo: Identificar o eleitor, contabilizar o voto do eleitor identificado apenas uma vez, em que pese que o eleitor possa votar em mais de uma oportunidade, garantir o sigilo do voto do eleitor e possuir mecanismos de transparência e auditoria. (TRIBUNAL SUPERIOR ELEITORAL, 2021i).

O TSE selecionou 26 empresas, cada uma com uma solução diferente, para apresentarem seus projetos de como funciona o processo eleitoral. Entre as empresas selecionadas estão GoLedger, Waves Enterprise, OriginalMy, IBM e Criptonomia, que apresentaram soluções usando blockchain (EXAME, 2020).

2 DISTRIBUTED LEDGER TECHNOLOGY (DLT) E BLOCKCHAIN

Distributed Ledger Technology, DLT, em sua tradução livre, tecnologia de registros distribuídos, é uma estrutura de dados que permite sua distribuição geograficamente, sem a necessidade de está centralizada em um servidor, como é utilizada no banco de dados relacionais. Desta forma vários servidores que tratam simultaneamente da informação de armazenamento na base, sem que exista um administrador principal, o registro distribuído em mais de uma base de dados gerida por um coletivo de servidores. Cada servidor terá uma cópia das informações para quando houver alguma modificação, seja de fácil detecção, para que aconteça uma atualização da informação, existe a necessidade de os participantes da rede entrarem em consenso, só assim é possível modificar a informação. Uma das garantias de integridade das tecnologias DLT é a inexistência de autoridades centrais, por existirem diferentes interesses, cada um dos participantes pode auditar o funcionamento dos servidores (APD ASSOCIAÇÃO PARA O PROGRESSO DA DIREÇÃO, 2021).

Dentre os tipos de DLT o Blockchain obteve notoriedade após a implementação do Bitcoin.

> Bitcoin, então, não é um software, mas um protocolo e a denominação de uma moeda (ou ativo) virtual. É possível identificar três pilares básicos do Bitcoin: algoritmos criptográficos como assinaturas digitais e hashes; a estrutura de dados composta por blocos encadeados, o blockchain, o que seria a grande contribuição de Nakamoto[1]; e, finalmente, o mecanismo de prova de trabalho (ALMEIDA, 2018, p. 41).

Apresentam-se a seguir diversos conceitos utilizados por entidades internacionais:

> Um blockchain é um livro-razão colaborativo e resistente à violação que mantém registros transacionais. Os registros transacionais são agrupados em blocos. Um bloco é conectado ao anterior incluindo um identificador único que é baseado nos dados do bloco anterior. Como resultado, se os dados forem alterados em um bloco, seu identificador exclusivo muda, que pode ser visto em cada bloco subsequente. Este efeito dominó permite que todos os usuários dentro do blockchain saibam se os dados de um bloco anterior foram adulterados. Como uma rede blockchain é difícil de alterar ou destruir, ela fornece um método resiliente de manutenção colaborativa de registros (tradução livre) (NIST, 2021).
>
> Blockchain é uma nova tecnologia que possibilita que grandes grupos de pessoas ou organizações que podem não se conhecerem ou não confiarem

[1] **Satoshi Nakamoto** é o nome usado pela suposta pessoa ou pessoas com pseudônimo que criaram o white paper do Bitcoin e desenvolveram a referência original do Bitcoin.

> umas nas outras concordem coletivamente e registrem informações permanentemente sem a necessidade de uma autoridade terceirizada. Ao criar confiança nos dados de maneiras que não eram possíveis antes, o blockchain tem o potencial de revolucionar a forma como compartilhamos informações e realizamos transações on-line (tradução livre) (EUROPEAN COMMISSION, 2021).

Vale ressaltar que a blockchain do Bitcoin tinha a proposta de possibilitar transações monetárias, desta forma não havia como adicionar condições elaboradas a essas transações. Vitalik Buterin[2], propôs uma plataforma para desenvolvimento de aplicações descentralizadas chamada de Ethereum, com suporte para contratos inteligentes (em inglês, smart contracts) o que elevou a tecnologia blockchain a outro patamar, uma vez que era possível executar de forma autônoma e confiável um aplicativo, previamente aprovado por duas ou mais partes (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

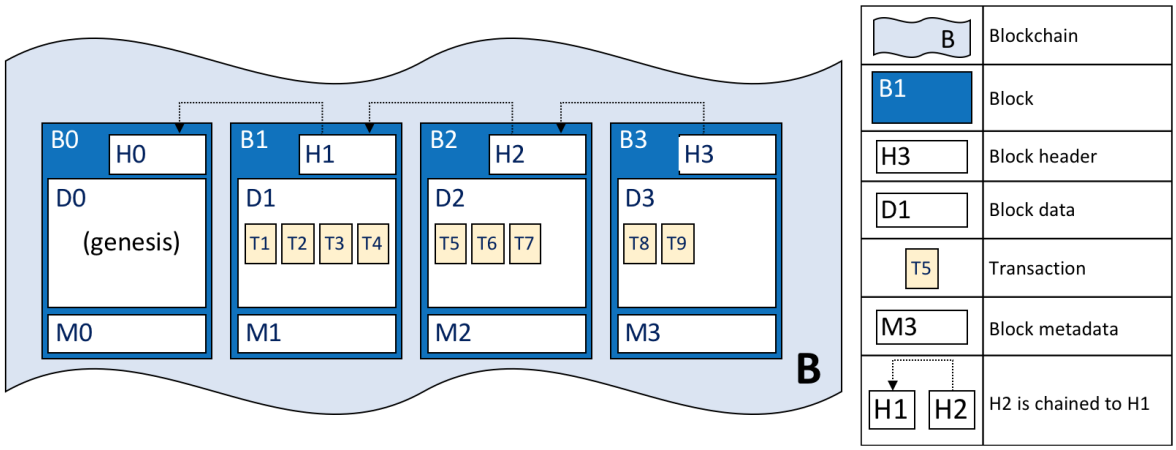
> É preciso observar que a transformação tecnológica vai além da inovação trazida pelas blockchains do Bitcoin e Ethereum. Segundo o Gartner, até 2023 a tecnologia blockchain suportará o movimento global e o rastreamento de dois trilhões de dólares de bens e serviços anualmente. A empresa de consultoria também afirma que a blockchain tem, no mínimo, o potencial de otimizar e, possivelmente, transformar de forma disruptiva os serviços públicos (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

2.1 Blockchain

O blockchain é uma estrutura de dados que armazena transações organizadas em blocos, os blocos são encadeados sequencialmente, servindo como um sistema de registros distribuídos. O cabeçalho inclui metadados como um número único que referência o bloco, o horário de criação do bloco e um apontador para o hash do bloco anterior, além do próprio hash do bloco. Os dados geralmente incluem uma lista de transações válidas e os endereços das partes, de modo que é possível associar uma transação às partes envolvidas (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

[2] **Vitalik Buterin** é um programador e escritor russo canadense mais conhecido como um dos cofundadores da Ethereum.

Figura 3: Estrutura de uma blockchain



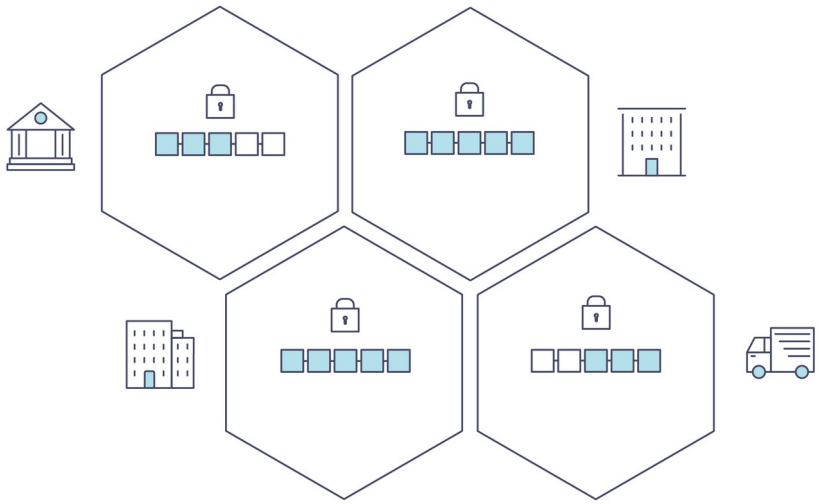
Fonte: Hyperledger Fabric

Os registros de blockchain são descritos como descentralizados porque são replicados entre todos participantes. A descentralização reflete a maneira como as informações podem ser auditadas pelos participantes (HYPERLEDGER FABRIC, 2021).

2.1.1 Rede blockchain

Uma rede blockchain é uma infraestrutura técnica que fornece serviços de livro-razão e contrato inteligente para os aplicativos. Inicialmente, os contratos inteligentes são usados para gerar transações que são subsequentemente distribuídas para todos os participantes da rede onde são gravados de maneira imutável em sua cópia do livro-razão (HYPERLEDGER FABRIC, 2021).

Figura 4: Rede blockchain



Fonte: Hyperledger Fabric

As informações registradas em uma rede blockchain utiliza técnicas criptográficas que garantem que uma transação adicionada ao livro-razão não possa ser modificada. Essa propriedade de imutabilidade facilita a determinar a origem das informações, uma vez que a transação é adicionada no livro-razão, os participantes tem a confiança que as informações não foram alteradas (HYPERLEDGER FABRIC, 2021).

2.1.2 Tipos de blockchain

Segundo a Comissão Europeia, as diferentes arquiteturas adotadas por uma blockchain podem ser classificadas de acordo com a abertura quanto à validação das transações e a participação na realização de transações. Assim, são descritos na literatura os seguintes tipos. Quanto à validação das transações temos as não permissionadas, qualquer um dos participantes que compõem a rede distribuída tem permissão para validar ou confirmar transações e as permissionadas onde apenas alguns participantes selecionados podem validar ou confirmar transações. As blockchains permissionadas são comumente encontradas em ambientes corporativos e na administração pública (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

Em relação as transações temos as públicas, onde neste tipo qualquer um dos participantes que compõem a rede pode participar de transações e as privadas no qual penas participantes selecionadas podem participar em transações (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

Podem ser enumerados quatro tipos principais: blockchain permissionada públicas, blockchain não permissionada públicas, blockchain permissionada privada e blockchain não permissionada privada (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

a. Blockchain permissionada pública: são as que permitem qualquer usuário com conexão à internet realizar uma transação e visualizar o log de transações, mas apenas uma parte restrita e capaz de participar do mecanismo de consenso.

b. Blockchain não permissionada pública: são as que permitem qualquer participante poder participar do mecanismo de consenso, além de permitir que qualquer usuário com conexão à internet, realize e visualize as transações no log.

c. Blockchain permissionada privada: somente usuários com permissão podem efetuar transações e visualizar os logs, o proprietário da blockchain define quais participantes podem fazer parte do mecanismo de consenso.

d. Blockchain não permissionada privada: somente usuários com permissão podem efetuar transações e visualizar os logs, porém todos participantes da rede podem participar dos mecanismos de consenso.

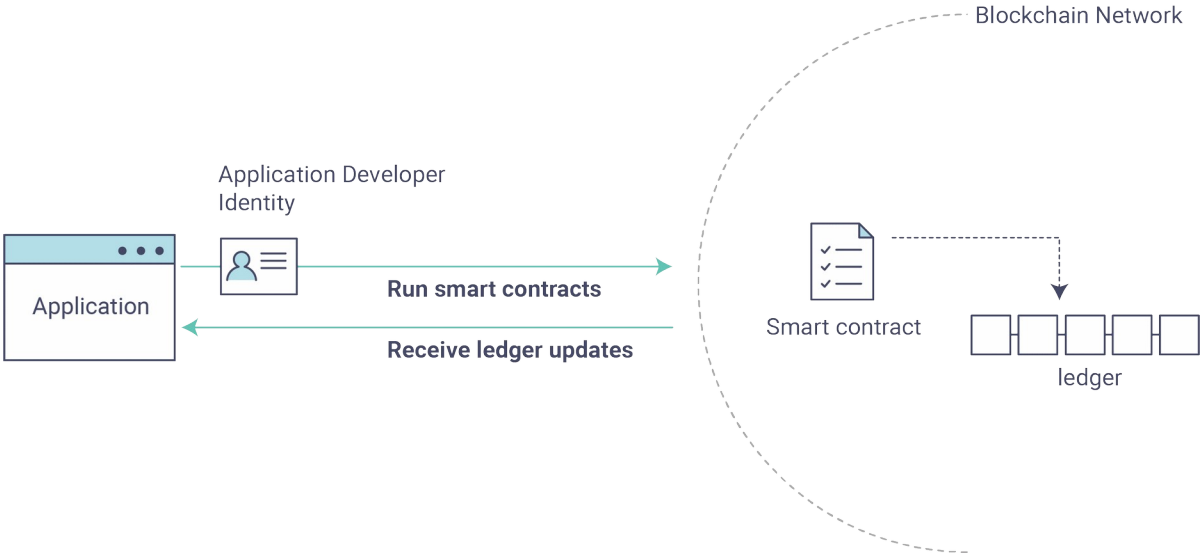
Outra perspectiva que pode ser utilizada para classificar uma blockchain é de acordo com as permissões quanto às operações de leitura, quem pode acessar o livro-razão e visualizar as transações, em relação a escrita, quem pode criar transações, e em relação ao commit[3], e quem atualiza o estado do livro-razão. Diferentes combinações podem ser feitas para adequar às necessidades de um determinado ecossistema (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

[3] **Commit** é um processo para tornar permanente um conjunto de alterações. O uso deste processo é comum na conclusão de uma transação.

2.1.3 Consórcio

Consórcio é uma coleção de organizações que fazem parte de uma rede blockchain. Essas organizações que formam o consórcio fornecem uma infraestrutura técnica de serviços para acesso ao livro-razão e aos contratos inteligentes para aplicativos. Os aplicativos podem ser usuários finais, administradores da rede, servidores, entre outros atores ou dispositivos que tenham acesso a rede blockchain. Os contratos inteligentes são usados para gerar transações que são subsequentemente distribuídas para todos os participantes da rede onde são gravados de maneira imutável em sua cópia do livro-razão (HYPERLEDGER FABRIC, 2021).

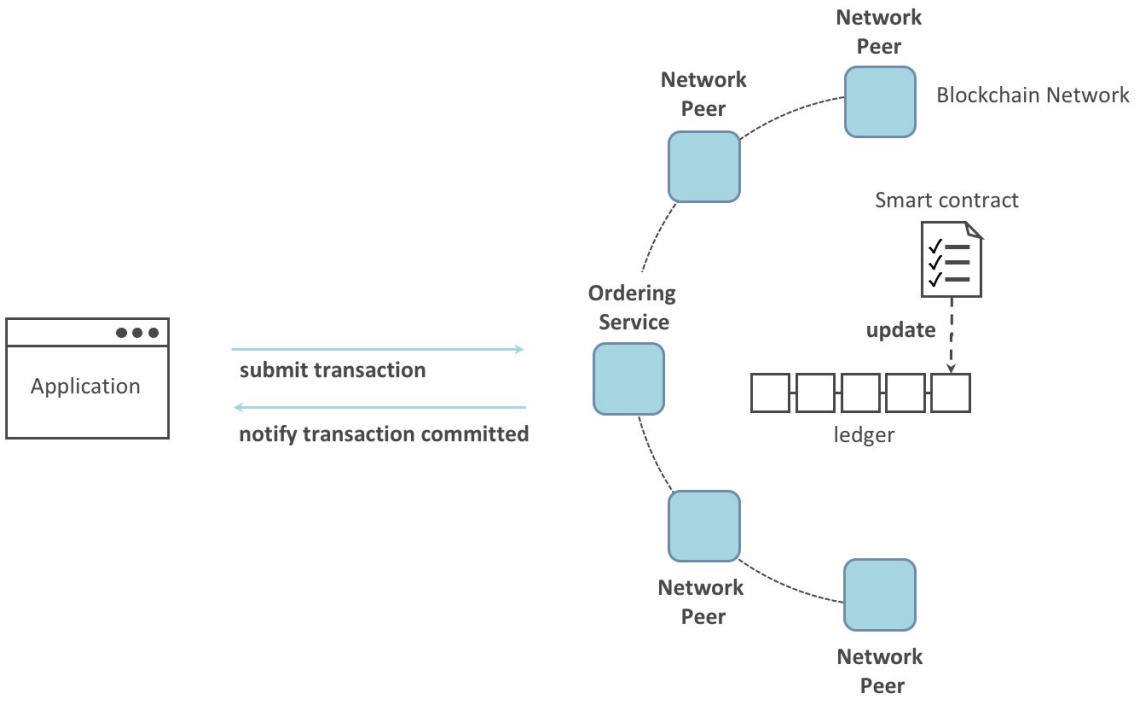
Figura 5: Comunicação entre aplicativo e a rede blockchain.



Fonte: Hyperledger Fabric

Para o aplicativo ter acesso a consulta e a atualização do livro-razão é bastante simples. O aplicativo envia uma transação para a rede blockchain, quando a transação é validada e confirmada, o aplicativo recebe uma notificação com o status da transação. A rede blockchain envolve a transação em um processo de consenso pelo qual os diferentes componentes da rede trabalham para garantir que cada transação proposta para o livro-razão seja válida e executada em uma ordem acordada e consistente pelo mecanismo de consenso, permitindo que as organizações do consórcio tenham acesso ao livro-razão (HYPERLEDGER FABRIC, 2021).

Figura 6: Comunicação entre aplicativo e a rede blockchain 2.



Fonte: Hyperledger Fabric

2.1.4 Livro-razão (Ledger)

O livro-razão distribuído pode ser visto como um registro de transações ou contratos mantidos de forma descentralizada em diferentes locais, eliminando a necessidade de uma autoridade central para controlar o armazenamento dos dados, é a estrutura de dados, em que transações são registradas e o estado global do sistema é mantido. O livro-razão mantém-se completamente replicado para todos participantes rede (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

Um ataque cibernético em um livro-razão distribuído é mais difícil de ser executado, devido as suas cópias serem distribuídas a todos participantes. Para um ataque ser bem sucedido a um livro-razão, o agente malicioso precisa atacar simultaneamente todos participantes, o que aumenta a dificuldade exponencialmente a cada novo participante da rede. Além disso, os registros distribuídos são resistentes a alterações maliciosas por um único participante da rede, uma vez que todos participantes precisam entrar em consenso para aceitar a alteração (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

O elemento de descentralização das tecnologias de livro-razão distribuído cria um sistema no qual todas as transações são compartilhadas, verificadas e aceitas por todos participantes da rede, eliminando a necessidade de intermediários (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

2.1.5 Contratos Inteligentes (Smart Contracts)

Um contrato inteligente funciona como um aplicativo distribuído confiável, que garante sua segurança e confiabilidade no blockchain e do consenso subjacente entre os participantes. É a lógica de negócios de um aplicativo em uma rede blockchain. Não são apenas um mecanismo para encapsular informações e mantê-las de uma forma simples na rede, também podem ser escritos para permitir que os participantes executem certos aspectos das transações automaticamente (HYPERLEDGER FABRIC, 2021).

O conceito de contrato inteligente foi definido por Nick Szabo, pesquisador em criptografia e especialista em Direito. Szabo define contrato inteligente como cláusulas contratuais embutidas em hardware e software, que tornam a violação destas cláusulas proibitivas sob o ponto de vista computacional, portanto, não vantajosa a um possível violador (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

> Dessa forma, define-se smart contract como programa de computador digital, quase inviolável, imperativo e desenvolvido para executar um negócio jurídico previamente pactuado, desde que reduzido à linguagem computacional apropriada (algoritmos). Será ele expresso em um termo digital que representará ipsis litteris o molde contratual. O contrato inteligente será armazenado e executado em uma base de banco de dados descentralizado (blockchain), para gerá-lo autônoma e automaticamente desde sua formação à sua extinção - incluindo condições, termos, encargos, e eventuais cláusulas de responsabilidade civil - com auxílio de softwares e hardwares, sem a interferência de terceiros, objetivando a redução de custos de transação e eventuais despesas judiciais, desde que aplicados princípios jurídicos e econômicos compatíveis com a relação contratual instaurada. A título elucidativo, como a tecnologia da criptomoeda Ethereum foi especificamente desenvolvida para atuar como smart contract, conduz seu modelo simplificado de execução para visualização de um contrato inteligente (DIVINO, 2019).

Figura 7: **Contrato Inteligente**

Fonte: Hyperledger Fabric

Uma rede blockchain utiliza contratos inteligentes para fornecer acesso controlado ao livro-razão o que possibilita acesso a uma séria de funções operacionais, atualização de registro, executar transações automáticas, consulta, entre outras. Segundo Szabo um contrato inteligente pode ser caracterizado pelo atingimento de quatro objetivos principais: observabilidade, verificabilidade, privacidade e obrigatoriedade (TRIBUNAL DE CONTAS DA UNIÃO, 2020 apud SZABO, 1996).

a. Observabilidade: É a habilidade de verificar se as partes envolvidas no contrato cumpriram a sua parte, ou seja, se o resultado esperado segundo a lógica computacional do contrato inteligente foi alcançado;

b. Verificabilidade: É a possibilidade de uma das partes envolvidas reclamar que o contrato foi cumprido ou violado;

c. Privacidade: O conhecimento sobre o conteúdo e a execução do contrato deve ser distribuído apenas na medida certa, ou seja, o mínimo possível de dados deve ser compartilhado;

d. Obrigatoriedade: O contrato é executado de forma obrigatória, em sua completude, conforme programado em seu código-fonte, sem margem para interpretações diversas.

Devido às suas características, DLTs são ambientes ideais para definição e execução de contratos inteligentes, tornando as ideias de Szabo aplicáveis. O uso da blockchain, criptografia e algoritmos de consenso, entre outras tecnologias, dão sustentação aos contratos inteligentes. A utilização de contratos inteligentes provê as seguintes vantagens: transparência, menor prazo para execução, precisão, segurança, rastreabilidade, menor custo e confiança (TRIBUNAL DE CONTAS DA UNIÃO, 2020 apud SZABO, 1996).

a. Transparência: contratos inteligentes podem ser escritos e verificados a qualquer momento por todas as partes envolvidas. E o mais importante, a execução do contrato fica totalmente registrada, reduzindo o número de disputas judiciais em torno de sua definição e execução;

b. Menor prazo para execução: intermediários humanos podem causar todo tipo de atraso na elaboração e execução de contratos. A eliminação dos passos manuais torna, portanto, a execução do contrato mais rápida e eficiente;

c. Precisão: como o contrato é descrito por um algoritmo computacional, sua execução é precisa, salvo se houver erro de programação. Qualquer condição não cumprida no contrato gera erro de execução. Contratos em papel podem dar margem a interpretações diversas, causando imprecisão;

d. Segurança: a infraestrutura de DLT garante a segurança em contratos inteligentes, que são assinados por chaves criptográficas e não podem ser violados por terceiros sem permissão de acesso;

e. Rastreabilidade: todos os dados, de cada execução das “funções” do contrato ficam armazenados na DLT, permitindo que a execução do contrato seja aditável a qualquer tempo;

f. Menor custo: por sua natureza digital e eliminação de intermediários, os contratos inteligentes reduzem os custos de execução;

g. Confiança: as características citadas acima levam à maior confiança entre as partes envolvidas no contrato.

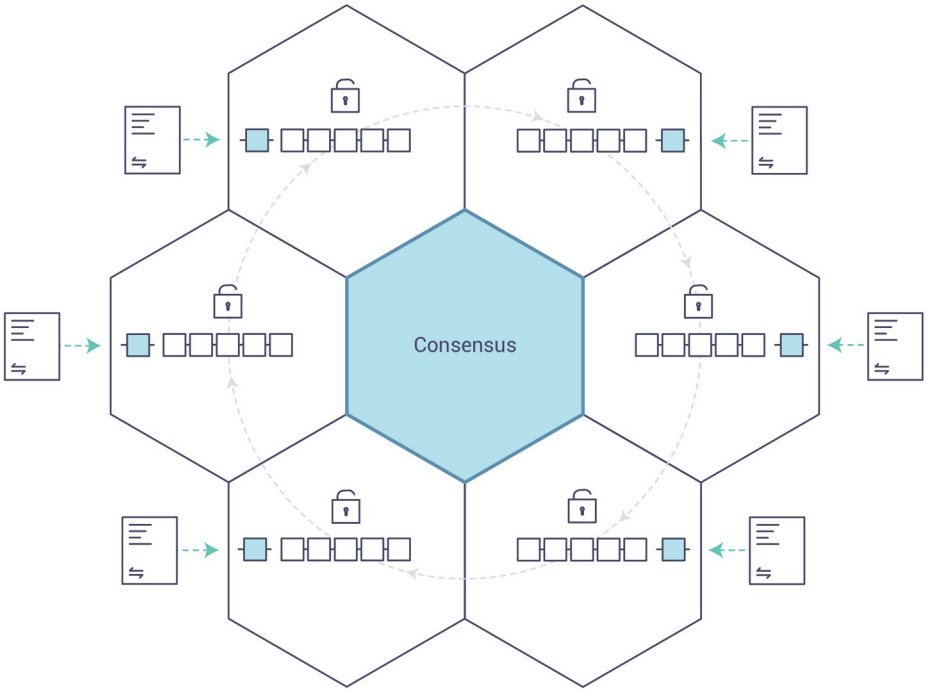
2.1.6 Mecanismos de consenso

O mecanismo de consenso são regras e procedimentos pelos quais os participantes de uma rede distribuída concordam com a validação da transação. Para cada transação a ser registrada em um livro-razão, ela primeira precisa ser aprovada pelos nós validadores da rede, caso contrário, é automaticamente rejeitada (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

Funciona da seguinte maneira, sempre que uma transação é encaminhada na rede blockchain, os participantes primeiramente validam a transação segundo regras pré-definidas, se os participantes concordarem com sua legitimidade, a transação é encaminhada para os outros nós validadores da rede e aguardam em um pool[4] de transações, um aspecto fundamental da tecnologia distribuída é determinar qual usuário adiciona o próximo bloco, assim que um nó é eleito ou torna-se apto a criar um bloco, este novo bloco é adicionado à cadeia anterior de blocos de forma imutável, contendo as transações mantidas em seu pool de transações, dessa maneira, a sequência de blocos mais recente mantém uma visão compartilhada e acordada do estado atual da blockchain (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

[4] **Pool** é uma área de armazenamento temporário.

Figura 8: Consenso



Fonte: Hyperledger Fabric

Vale ressaltar que, as atualizações no livro-razão só serão efetuadas se as regras ditadas através mecanismo de consenso for aceita por todos participantes da rede. (TRIBUNAL DE CONTAS DA UNIÃO, 2020)

2.1.7 Criptografia

A criptografia é um dos pilares fundamentais nos quais a tecnologia blockchain se baseia, permitindo o funcionamento da rede, garantindo os mecanismos de consenso entre os participantes e a integridade do livro-razão. Podemos citar a utilização de algoritmos criptográficos de chaves públicas, funções de hash e assinaturas digitais. Uma função criptográfica que é extremamente importante neste contexto é o hashing[5]. (BINANCE ACADEMY, 2018)

O Hashing são utilizando nos algoritmos de consenso para validar transações, o algoritmo de Proof of Work (na tradução prova de trabalho) é usado

[5] **Hashing** é um processo pelo qual um algoritmo conhecido como função hash recebe uma entrada de dados, o input, de qualquer tamanho e retorna uma saída, output, determinada que contém um valor de comprimento fixo.

para obter consenso entre os participantes. No blockchain, os hashes são usados como identificadores exclusivos para blocos de dados. O hash de cada bloco é gerado em relação ao hash do bloco anterior, utilizado para ligação dos blocos, formando uma cadeia de blocos da blockchain. Além disso, o hash do bloco depende dos dados contidos nesse bloco, o que significa que qualquer alteração feita nos dados exigiria uma alteração no hash do bloco, o hash de cada bloco é gerado com base nos dados contidos nesse bloco e no hash do bloco anterior. Esses identificadores de hash desempenham um papel importante na garantia da segurança e imutabilidade das informações contida na blockchain (BINANCE ACADEMY, 2018).

2.1.8 Tokens

Tokens, em plataformas distribuídas, utilizam os mesmos princípios que são utilizados, por exemplo, em um voucher de viagem, um ingresso para um show, um cartão de embarque ou até mesmo uma cédula de votação ou moeda. O token são representações de um direito, crédito, vantagem, benefício, ou qualquer outra coisa que represente um valor no mundo real (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

> Em plataformas distribuídas, os tokens representam algo com valor no “mundo real” ou um direito de acessar produtos e serviços disponibilizados por outras pessoas, comunidade de pessoas ou empresas (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

A tokenização descreve o processo de transferência de direitos de um ativo físico ou digital para uma representação digital. Essa representação digital denominada de token. Esse token fornece o direito a esse ativo e a capacidade de negociá-lo e rastreá-lo digitalmente (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

Existem três tipos principais de ativos digitais baseados em DLT, segundo o Tribunal de Contas da União (2020):

a. Tokens de pagamento (payment tokens): Destinadas a operar como moedas fiduciárias tradicionais, são sinônimos de criptomoedas, utilizados tão somente para troca de valores entre partes em uma plataforma de blockchain, os tokens de pagamento podem ser utilizados como meio de troca por quaisquer bens ou serviços e,

possivelmente, também como reserva de valor. Bitcoin é o exemplo mais conhecido;

b. Tokens utilitários (utility tokens): Seu uso principal é para facilitar a troca ou o acesso a bens ou serviços específicos. Eles podem atuar como uma licença para permitir o acesso do titular a um determinado serviço. Representa o direito de acesso, mas não a propriedade de um ativo;

c. Tokens de segurança (security tokens): Estes tokens são designados como ativos negociáveis mantidos para fins de investimento e classificados como um título de acordo com as leis aplicáveis, também conhecido como Tokens de Ativos (asset tokens).

Os primeiros sistemas de blockchain, como Bitcoin, foram projetos voltados exclusivamente para realizarem transferências de valores em moedas digitais, sendo que sua lógica de transação implementa um sistema baseado em tokens. A limitação desses sistemas é que apenas registram os saldos digitais associados a identidades ou endereços, juntamente com uma autenticação e as respectivas assinaturas digitais. Por outro lado, sistemas baseados em contratos inteligentes têm a capacidade de implementar qualquer rotina de software, incluindo a lógica de tokens digitais, possibilitando executar, de forma autônoma, lógicas complexas e fluxos de trabalho em código de computador com o qual todos os participantes autorizados podem auditar (TRIBUNAL DE CONTAS DA UNIÃO, 2020).

Por fim, uma outra classificação sobre tokens que merece ser citada e que é utilizada pela OECD são os Natives Tokens. É importante para uma organização diferenciar tokens que representam ativos reais que estão fora da blockchain é os tokens que representa ativos nativos da blockchain (OECD ILIBRARY, 2021).

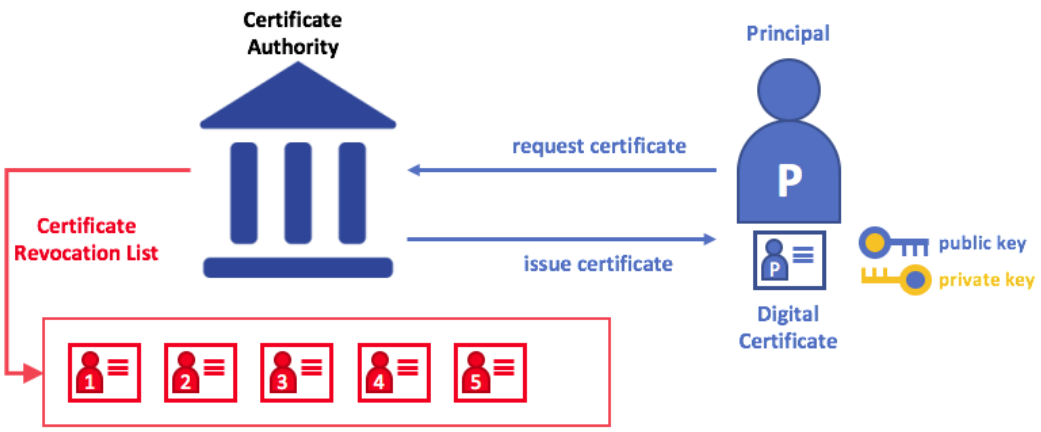
2.1.9 Certificado digital e Autoridades de certificadora

As especificações dos padrões para o certificado digital X.509, infraestrutura de chave pública (PKI) para a internet encontra-se na RFC 5280. Esta especificação define o perfil do formato e da semântica dos certificados e a lista de

revogação de certificados (CRLs) para a PKI na Internet (HYPERLEDGER FABRIC, 2021).

PKI é a estrutura de chave pública que é composta por autoridade de certificação (CA), que emitem certificados digitais para diversos atores, que as usam para se autenticar nas mensagens que trocam em um ambiente seguro. A lista de revogação de certificados (CRL) de uma CA constitui uma referência para os certificados que não são mais validos. A revogação de um certificado pode ocorrer por vários motivos, por exemplo, se a chave privada do certificado for exposta (HYPERLEDGER FABRIC, 2021).

Figura 9: Autoridade Certificadora

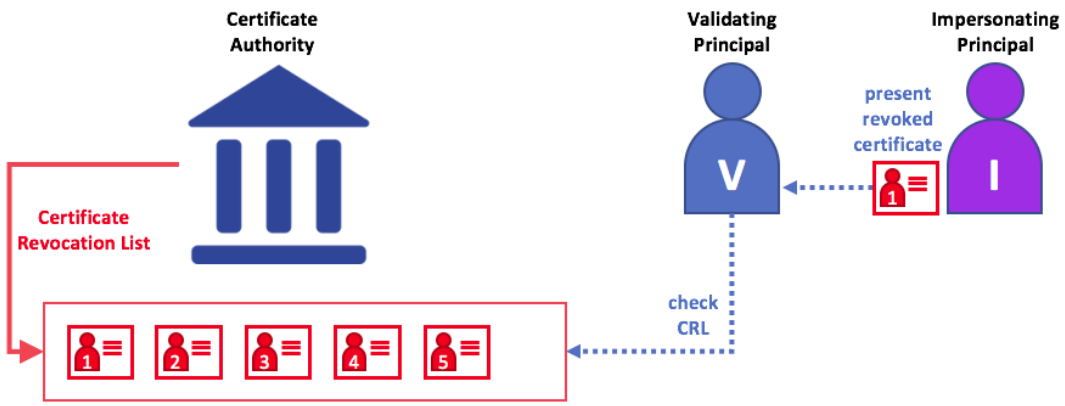


Fonte: Hyperledger Fabric

Algumas das autoridades certificadoras (CAs) mais populares da Internet são Symantec originalmente Verisign, GeoTrust, DigiCert, entre outros. O modelo adotado pelo Brasil foi o de certificação raiz única, sendo que o Instituto Nacional de Tecnologia da Informação, desempenha o papel de Autoridade Certificadora Raiz – AC-Raiz, tem o papel de credenciar e descredenciar os demais participantes da cadeia e supervisionar e fazer auditoria em todos processos. A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão por meio das CAs, essas entidades públicas ou privadas, subordinada à hierarquia do ICP-Brasil que são responsáveis por gerenciar os certificados digitais (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2020).

Lista de revogação de certificados (CRL) é uma lista de referência a certificados que uma CA sabe que foi revogado. Não existe a necessidade de consultar a CRL, causando uma vulnerabilidade na validação, pois pode aceitar uma identidade comprometida, um certificado revogado é diferente de um certificado expirado, a ação de revogar um certificado não o torna expirado (HYPERLEDGER FABRIC, 2021).

Figura 10: FNA Diagrama Certificado revogado.



Fonte: Hyperledger Fabric

Um certificado digital é um documento criptográfico que contém um conjunto de atributos relacionados ao titular do certificado. O tipo mais comum de certificado é aquele compatível com o padrão X.509, que permite a codificação dos detalhes de identificação de uma entidade em sua estrutura (HYPERLEDGER FABRIC, 2021).

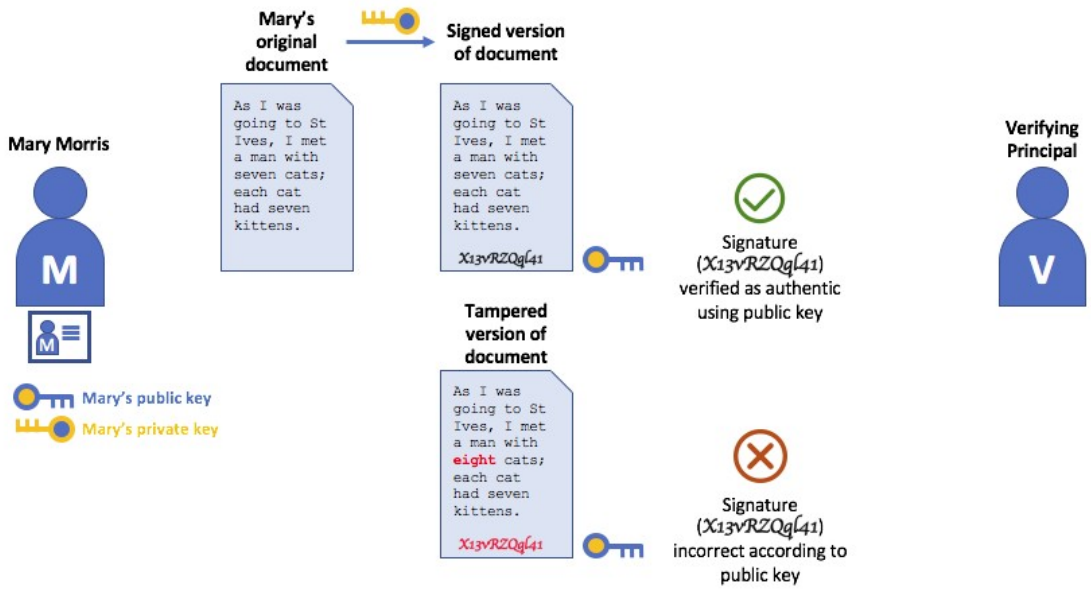
2.1.10 Assinatura digital

Em uma comunicação computacional segura a autenticidade e integridade são conceitos muito importantes, pois a autenticação exige que as partes que trocam mensagens tenham certeza da identidade de quem a enviou, para ter integridade significa que não possa ter sido corrompida, ou modificada, durante sua transmissão. Os mecanismos de autenticação que dependem de assinaturas digitais, permitem que uma parte assine digitalmente suas mensagens. A assinatura digital fornece integridade a mensagem assinada (HYPERLEDGER FABRIC, 2021).

As assinaturas digitais exigem que cada parte mantenha duas chaves criptograficamente conectadas, conhecida como chave pública e a chave privada.

Uma chave pública é amplamente disponibilizada e atua como âncora de autenticação e uma chave privada é usada para produzir assinaturas digitais. Os destinatários das mensagens assinadas digitalmente podem verificar a origem e a integridade da mensagem recebida, verificando se a assinatura anexada é válida sob a chave pública do remetente. O relacionamento entre as chaves é matematicamente exclusivo de tal forma que a chave privada usada para produzir uma mensagem assinada, apenas na mesma mensagem, a chave pública correspondente pode simetrizar (HYPERLEDGER FABRIC, 2021).

Figura 11: Assinatura digital



Fonte: Hyperledger Fabric

2.1.11 Características da blockchain

A tecnologia blockchain é considerada revolucionária. Abaixo serão listadas algumas de suas características, segundo o Tribunal de Contas da União (2020):

a. Transparência: as informações ficam disponíveis para qualquer participante.

b. Segurança: todas as transações feitas são criptografadas, o nível de segurança é muito mais alto.

c. Rastreabilidade: o blockchain permite aos participantes inserir regras para as suas transações. Com isso é possível rastrear uma operação a fim de identificar inconsistências.

d. Imutabilidade: esta é uma das principais características da blockchain as informações não podem ser corrompidas ou alteradas, as transações feitas não podem ser editadas ou removidas do livro-razão.

e. Irrefutabilidade: o uso da criptografia de chaves públicas ou assimétrica serve como uma base para a autenticação dos usuários da rede. Com o uso de um método que utiliza a chave privada do seu par de chaves e funções de hash, um participante é capaz de realizar assinaturas digitais sobre as transações, servindo como uma prova inegável de que é o emissor de determinada mensagem, garantindo o não repúdio da transação.

2.2 Privacidade nas redes blockchain

A tecnologia blockchain não pode garantir a privacidade transacional uma vez que as transações são visivelmente públicas. Estudos recentes mostrou que as transações de Bitcoin podem ser vinculadas para revelar informações transacional de um determinado usuário utilizando um endereço IP, mesmo que a transação seja traduzida pelo endereço de rede ou firewall, cada usuário pode ser identificado exclusivamente por um conjunto de nós aos quais ele se conectou na rede blockchain, esse conjunto de informação pode levar a origem da transação (WANG et al., 2018).

Wang et al., (2018) descreve que muitas soluções foram propostas para melhorar o anonimato do blockchain, que poderia ser aproximadamente categorizado em dois tipos duas soluções.

> Mixing. No blockchain, os endereços dos usuários são pseudônimos. Mas ainda assim é possível vincular endereços à identidade real do usuário, já que muitos usuários fazem transações com o mesmo endereço frequentemente. O serviço de mixing é um tipo de serviço que fornece anonimato pela transferência de fundos de vários endereços de entrada para várias saídas endereços. Por exemplo, o usuário Alice com o endereço A deseja enviar alguns fundos para Bob com o endereço B. Se Alice fizer uma transação diretamente com o endereço de entrada A e saída endereço B, o relacionamento entre Alice e Bob pode ser revelado. Para que Alice pudesse enviar fundos para um intermediário confiável Carol. Em seguida, Carol transfere fundos para Bob com múltiplas entradas c1, c2, c3, etc., e

> múltiplas saídas d1, d2, B, d3, etc. Endereço de Bob B também está contido nos endereços de saída. Portanto, fica mais difícil revelar o relacionamento entre Alice e Bob. No entanto, o intermediário pode ser desonesto e revelar informações privadas de Alice e Bob propositalmente. Também é possível que Carol transfere os fundos de Alice para seu próprio endereço em vez do endereço de Bob. Mixcoin fornece um método simples para evitar comportamentos desonestos. O intermediário criptografa os requisitos dos usuários, incluindo quantia de fundos e data de transferência com sua chave privada. Então, se o intermediário não transferiu o dinheiro, ninguém poderia verificar se o intermediário trapaceou. No entanto, o roubo é detectado, mas ainda não impedido. Coinjoin depende de um servidor de mixagem central para embaralhar endereços de saída para evitar roubo. E inspirado em Coinjoin, CoinShuffle usa mixnets de descriptografia para embaralhamento de endereços (tradução livre) (WANG et al., 2018).

> Anonymous. Em Zerocoin, uma prova de conhecimento zero é usada. Mineiros não tem que validar uma transação com assinatura digital, mas para validar moedas pertencem a uma lista de moedas válidas. A origem do pagamento é desvinculada das transações para evitar análises de gráfico de transação. Mas ainda revela o destino e os valores dos pagamentos. Zerocash foi proposto para resolver este problema. Em Zerocash, zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). Os montantes das transações e os valores das moedas detidas pelos usuários são ocultados (tradução livre) (WANG et al., 2018).

2.3 Vulnerabilidade da blockchain

Apesar da inovação proposta pela tecnologia de registro distribuído, ainda existem muitas limitações e pontos falhos. Segundo Phan, Li e Mentzer (2019), existem vulnerabilidades e falhas relevantes nas criptomoedas, contratos inteligentes e a blockchain em si, algumas serão expostas a seguir.

a. Ataque dos 51%: acontece quando agentes maliciosos conseguem controlar a maior parte do mecanismo de consenso de uma rede distribuída, ou seja, 51%.

b. Ataque de negação de serviço: o ataque de negação de serviço, DDoS, envolve o comprometimento de vários sistemas através da sobrecarga causando a indisponibilidade dos serviços disponíveis na rede blockchain.

c. Ataque Sybil: esse tipo de ataque acontece quando agente malicioso utilizam pseudônimos de identidade para ganhar mais controle sobre o mecanismo de consenso da rede blockchain, dessa forma é possível recusar a transmissão de blocos validos e atrapalhar a comunicação da rede.

d. Ataques em contratos inteligentes: podem haver falha de segurança durante a implementação do contrato inteligente, o que possibilita um agente malicioso utilizar essa falha para poder modificar o livro-razão.

e. Ataque man-in-the-middle: o ataque man-in-the-middle (MitM) acontece com a interceptação de uma transação. Nesse cenário, o atacante tem a possibilidade de alterar a mensagem enviando uma transação modificada para rede de consenso.

2.3.1 Ataque de 51%

Do ponto de vista da mineração, um atacante, ou grupo de atacantes distribuídos em rede, poderiam tentar controlar a maioria do poder de mineração da rede blockchain; em ataque conhecido como Ataque de 51%. Impedindo, portanto, que novas transações pudessem ser confirmadas. E ainda, poderiam reverter transações já realizadas anteriormente. No entanto, a probabilidade de um ataque desse tipo acontecer é mínima, porque um usuário mal intencionado precisaria de muito poder computacional. Para poder iniciar um ataque desse tipo, seria necessário gastar uma quantia enorme de dinheiro para adquirir hardware de mineração capaz de competir com o restante da rede, sem contar a quantidade de energia necessária para viabilizar todo esse poder de processamento. Nem mesmo os computadores mais poderosos atualmente poderiam competir com os milhões de outros computadores da rede blockchain e realizar um ataque de 51% (BINANCE.COM, 2021).

2.3.2 Ataque de negação de serviço

Um ataque desse tipo visa ofuscar a visão de um participante da rede peer-to-peer, para provocar interrupções gerais ou com o objetivo de preparação para ataques mais sofisticados. Em um eclipse attack, o agente malicioso garantirá que todas as conexões do alvo sejam feitas por nós controlados pelo invasor. O agente inundará o alvo com seus próprios endereços de IP, aos quais a vítima irá provavelmente se conectar ao reiniciar seu software. Pode haver uma reinicialização forçada (ou seja, através de um ataque DDoS no alvo) ou o invasor pode simplesmente esperar até que a reinicialização ocorra (BINANCE.COM, 2021).

Depois que ocorre o ataque, a vítima, sem perceber, fica sujeito a investidas dos nós maliciosos, sem visão da rede mais ampla, possibilitando receber dados incorretos provenientes do invasor (BINANCE.COM, 2021).

Ainda não houve graves consequências resultantes deste ataque. Entretanto, apesar das medidas de segurança adicionadas à rede, a ameaça ainda existe. A defesa mais eficiente é a que consegue tornar os ataques financeiramente inviáveis (ANTONOPOULOS, 2017, p. 147).

2.3.3 Ataques Sybil

Durante um ataque do tipo Sybil, os invasores podem simular participantes falsos na rede, capazes de recusar o recebimento ou transmissões dos blocos, bloqueando os participantes honestos. Em um ataque Sybil de grande escala, onde o invasor se torna capaz de controlar 51% dos nodes da rede, se torna possível modificar a ordem das transações e prevenir que transações sejam confirmadas, reverter transações, possibilitando o gasto duplo (BINANCE.COM, 2021).

A blockchain utiliza diversos algoritmos para se defender de ataques Sybil. Os principais algoritmos são Proof of Work (PoW), Proof of Stake (PoS), e Delegated Proof of Stake (DpoS) (BINANCE.COM, 2021).

2.4 Exemplos recentes de sistema de votação baseado em blockchain

Em dezembro de 2017, o programa Active Citizen (Cidadão Ativo) da cidade de Moscou começou a usar um blockchain para votar e tornar os resultados da votação publicamente auditáveis. As questões discutidas pela comunidade são colocadas para votação, após isso, é movida para o sistema de votação eletrônica usando um blockchain. Muitos residentes de Moscou não têm tempo para participar de reuniões presencial. Assim, as reuniões mudaram para a plataforma on-line da Digital Home (Casa Digital). Em dezembro de 2017, os residentes começaram a usar um blockchain para votar e os resultados eram auditáveis publicamente. As autoridades municipais acreditam que os vizinhos devem ter um ambiente conveniente para influenciar suas condições de vida. Os funcionários também acreditavam que um blockchain aumentaria a confiança entre os cidadãos e o governo (KSHETRI; VOAS, 2018).

Depois que a votação é concluída, os resultados são listados em um livro contendo todas as pesquisas anteriores. As pesquisas mais populares relataram ter de 137.000 a 220.000 participantes. Em um desses casos na plataforma Ethereum, os cidadãos indicaram suas preferências por relocação temporária se o prédio em que moravam fosse demolido para ser substituído por um prédio melhor. A plataforma atingiu um pico de aproximadamente 1.000 transações por minuto. Não está claro se a plataforma pode lidar com o volume se uma proporção maior dos 12 milhões de cidadãos de Moscou participar da votação (KSHETRI; VOAS, 2018).

Em março de 2017, a província sul-coreana de Gyeonggi-do empregou um sistema de votação baseado em blockchain para votar no Projeto de Apoio à Comunidade Ddabok. Nove mil residentes votaram usando uma plataforma de blockchain desenvolvida pela startup de tecnologia financeira coreana Block que incluía contratos inteligentes. Os votos, resultados e outros dados relevantes foram armazenados em um blockchain. Nenhuma administração ou autoridade central foi envolvida neste processo e esta foi a primeira vez que a Coreia do Sul aplicou tal tecnologia (KSHETRI; VOAS, 2018).

Os acionistas da empresa de tecnologia da Estônia LVH Group que são cidadãos ou residentes eletrônicos da Estônia agora podem usar o sistema de votação baseado em blockchain para tomar decisões relacionadas à governança corporativa. Eles podem fazer login usando sua identidade nacional on-line verificada e votar na assembleia geral anual de LVH. A Estônia planeja adotar blockchain em uma série de áreas, como um projeto de residência eletrônica, que permite aos cidadãos estrangeiros estabelecerem uma empresa dentro da jurisdição da Estônia, e na saúde, protegendo o armazenamento de dados de saúde e permitindo o monitoramento em tempo real das condições do paciente. (KSHETRI; VOAS, 2018)

Nas eleições gerais de Serra Leoa de março de 2018, a startup suíça de blockchain Agora forneceu uma contagem parcial dos resultados eleitorais. A startup Agora foi um dos observadores credenciados que forneceu uma contagem independente para comparação e descreveu as eleições em Serra Leoa como um

caso de uso em vez de uma implementação de um sistema eletrônico de votação (KSHETRI; VOAS, 2018).

Nasdaq[6] construiu e operou quatro interfaces de usuário baseadas na web para sistema de votação utilizando blockchain. O sistema emite ativos com direito a voto e ativos com token de voto para cada acionista de uma empresa. Um usuário pode gastar tokens de voto para lançar votos em cada item da agenda da reunião se esse usuário possuir o ativo de direito de voto relacionado (KSHETRI; VOAS, 2018).

[6] **Nasdaq**, sigla de National Association of Securities Dealers Automated Quotations (Associação Nacional de Corretores de Títulos de Cotações Automáticas) é a segunda maior bolsa de valores dos Estados Unidos na qual se encontram grandes empresas de tecnologia como eletrônica, informática, biotecnologia e telecomunicações.

3 BLOCKCHAIN NO SISTEMA ELETRÔNICO DE VOTAÇÃO E DE TOTALIZAÇÃO DOS VOTOS

A Resolução nº 23.603, publicado em 12 de dezembro de 2019 pelo Tribunal Superior Eleitoral está sendo usado para o entendimento das responsabilidades das entidades fiscalizadoras sempre tendo em vista que a resolução interessou o Sistema Eletrônico de Votação e Totalização de Votos, existe neste presente momento, com objetivo de propor um cenário para uma rede blockchain mais próxima do cenário real.

3.1 Rede Blockchain

Atendendo os procedimentos de fiscalização e auditoria do sistema eletrônico de votação, existentes na Resolução nº 23.603, somente participantes identificados poderão ingressar nos procedimentos de fiscalização e auditoria das transações e dessa forma alguns participantes selecionados poderão validar e confirmar as transações no livro-razão utilizando o mecanismo de consenso, podendo a rede ser classificada como blockchain permissionada privada.

Uma rede blockchain pode ter vários consórcios, portanto a maioria das redes blockchain contém apenas um consórcio. As organizações que compõem o consórcio para formar a rede blockchain determina suas permissões através de um conjunto de políticas que são acordadas quando a rede é configurada, as políticas de rede podem mudar, após a configuração, mediante ao acordo das organizações do consórcio (HYPERLEDGER FABRIC, 2021).

3.1.1 Consórcio Justiça Eleitoral

Essa coleção de entidades que dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação descrita na Resolução TSE nº 23.550/2017 do Tribunal Superior Eleitoral podem formar um consórcio para fornecer uma infraestrutura técnica de serviço para acesso ao livro-razão e aos contratos inteligentes. Deve-se observar a capacidade técnica e a responsabilidade de cada organização de acordo com a legislação vigente e acordo prévio das entidades.

Aconselha-se o convite do Exército Brasileiro para o Consórcio Justiça Eleitoral com a finalidade de gerenciar os algoritmos de criptografia utilizado na rede blockchain, uma vez, que para pesquisar o assunto deve ser tratado como objeto de segurança nacional.

O convite pode se estender também ao SERPRO e ao ICP-Brasil para gerenciamento das carteiras digitais e certificados digitais respectivamente utilizando biometria. O Banco Central e a Casa da Moeda podem ser convidadas para ser gerencia a tokenização das cédulas de votação e a representação do token representativo a e-cédula.

Figura 12: Consórcio Justiça Eleitoral

Fonte: Autor

3.1.2 Consórcio TRE

A tecnologia utilizada para criação da rede blockchain deve permitir a criação de um canal de comunicação entre todos os TREs, garantindo as autonomias dos tribunais reginais, permitindo todo gerenciamento do canal de comunicação, permitindo os TREs administrar seus próprios consórcios garantindo a autonomia dos poderes.

3.2 Identificação dos atores

Para participar de um consórcio de uma rede blockchain existe a necessidade de um ator se identificar utilizando um certificado digital. Um ator pode ser um usuário final, eleitor, mesário, juiz, ministro, urna eletrônica, administrador da rede, celular, notebook, computadores pessoais, servidores, organização, entre outros atores que desempenha um papel dentro de um consórcio.

Em 2017, o Tribunal Superior Eleitoral fez um acordo com o ICP-Brasil que permitirá a emissão de certificados digitais para a segurança da urna eletrônica e o fornecimento de certificados digitais para funcionários do Poder Judiciário, essa parceria também permitirá a criação de um canal de comunicação para a consulta biométrica dos requerentes de um certificado digital do ICP-Brasil (TRIBUNAL SUPERIOR ELEITORAL, 2017b).

> "O emprego de tecnologias biométricas representa a possibilidade de implantarmos uma identificação mais segura para os cidadãos brasileiros. A base de dados que a Justiça Eleitoral tem trabalhado diuturnamente para construir é composta hoje por elementos de extrema integridade e unificação, razão pela qual o emprego da biometria está sendo ampliado nas diversas esferas governamentais, a fim de dar maior agilidade e segurança à concretização de políticas públicas, por meio da uniformização dos cadastros de beneficiários, com remoção de duplicidade e correção de erros de registro", disse Gilmar Mendes. O ministro classificou a cooperação entre a Justiça Eleitoral e o ITI como um passo significativo na direção da formação de um e-government, ou seja, um governo eletrônico no qual a prestação de serviços públicos pode ser feita pelos meios digitais (TRIBUNAL SUPERIOR ELEITORAL, 2017b).

No final deste acordo de cooperação, o Tribunal Superior Eleitoral possuirá uma Autoridade Certificadora para Justiça Eleitoral, AC-JE.

> Gastão Ramos[7] acredita que a celebração do acordo tem grande importância tanto para o ITI quanto para a Justiça Eleitoral. "Nós faremos uma parceria em que será realizada uma consulta à base biométrica do TSE e, em contrapartida, o ITI estará ajudando na criação da AC-JE. Esse é um passo muito importante que será dado para a massificação do certificado digital. Hoje o certificado digital tem uma importância enorme em todos os processos de governo, e é muito importante contarmos com a segurança da biometria", ressaltou (TRIBUNAL SUPERIOR ELEITORAL, 2017b).

Para poder consumir determinados serviços de uma rede blockchain existe a necessita de uma identidade digital. A importância dessa identificação, determina as permissões exatas dos recursos e acessos as informações que os

[7] Gastão Ramos (2017), ocupava o cargo de Diretor-Presidente do Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal, vinculada à Casa Civil da Presidência República e responsável pelo ICP-Brasil.

atores terão em um consórcio. Para as redes blockchain permissionadas privadas torna-se um requisito obrigatório (HYPERLEDGER FABRIC, 2021).

3.2.1 Criação de certificado digital utilizando biometria

Em setembro de 2015, Lacerda descreve que o Comitê Gestor da ICP-Brasil aprovou o uso de sistema biométrico na verificação dos requerentes no processo de emissão do certificado digital. (LACERDA, 2015)

Desta forma, o Consórcio Justiça Eleitoral poderá ofertar aos eleitores a comodidade de emitir seu próprio certificado digital sem a necessidade de comparecer a uma Zona Eleitoral no papel de Agente de Registro (AR). O certificado digital emitido pelo celular tem a mesma garantia de autenticidade, confidencialidade e integridade à troca de informações eletrônicas que a emissão do AR.

Tabela 1: Eleitorado com identificação biométrica em março 2021.

Eleitorado	**Eleitorado com identificação biométrica**
146.024.498	119.1852.60

Fonte: Tribunal Superior Eleitoral, 2021j

3.3 Privacidade do Eleitorado

De acordo com Wang et al. (2018), a comunicação de uma rede blockchain podem levar a exposição da comunicação por meio de análise de rede expondo os eleitores e suas cédulas de votação. Essa exposição leva a reconstrução histórica dos votos o que é proibida por diversos instrumentos da lei. A execução das eleições remotas não pode garantir a privacidade que as pessoas têm quando votam em uma cabine de votação. O eleitor pode ser coagido a registrar o voto incorretamente ou o dispositivo pode estar comprometido. Sendo um dos motivos sociais para não realização de eleições on-line.

> O sufrágio secreto impede, em teoria, que o voto de opinião não sucumba frente ao voto de escambo. Afinal, no Brasil ainda há quem se obrigue a votar por qualquer trocado; por um par de sapatos, um saco de farinha. A nossa imensa massa de iletrados (RORIZ, 2013 apud VIANNA, 1995).

Devido a sensibilidade do vínculo do eleitor com a cédula de votação, aconselha-se que esse vínculo nunca seja criado, nem mesmo com todo amparo tecnológico e criptográfico existente. A imutabilidade da informação e a publicidade

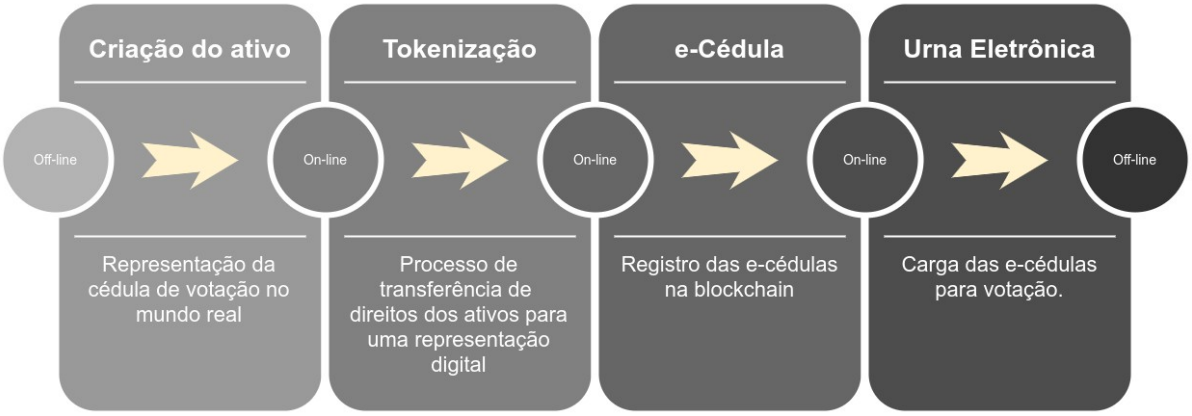
do livro-razão da rede blockchain torna o vínculo do eleitor com a cédula de votação vulnerável, uma vez que a evolução dos hardwares possibilita que uma criptografia segura se torne vulnerável.

Para impossibilitar uma reconstrução histórica dos votos e satisfazer a privacidade de cada eleitor atendendo a legislação eleitoral utilizaremos a urna eletrônica do Sistema Eletrônico de Votação para essa análise da rede blockchain do Consórcio Justiça Eleitoral.

3.4 e-Cédula

A representação da cédula de votação dentro de uma rede blockchain e possível através do processo de tokenização, descrito na seção Token.

Figura 13: Processo tokenização para criação da e-Cédula.



Fonte: Autor

O Consórcio Justiça Eleitoral deverá ser responsável pela criação da e-cédulas. Seguem as etapas do processo de criação das e-cédulas:

1. Criação do ativo para representação das cédulas de votação, será a representação de um direito legal.
2. Tokenização é o processo de transferência de direitos de um ativo para uma representação digital. Será a representação do voto de um eleitor na cédula de votação, para um determinado cargo, partido ou coligação, representação de voto nulo ou voto em branco.
3. Para fornecer esse ativo a capacidade de rastreá-lo digitalmente, as e-cédulas deverão estar presente nas redes blockchain assim concluindo processo de criação. Com intuito de aumentar a transparência,

auditoria e segurança o rastreamento da e-cédula deverá ser público na rede blockchain.

4. Os votos deverão ser registrados na e-cédula utilizando as urnas eletrônicas. Ressalto que a arquitetura da urna eletrônica permite a identificação do eleitor e habilitação para votação sem identificação do votante na e-cédula, mantendo o sigilo do voto.

As e-cédulas geradas deverão ser de propriedade do Tribunal Superior Eleitoral, que poderá transferir exclusivamente para os tribunais regionais eleitorais de cada estado da federação, que por suas atribuições e autonomia deverão carregar as e-cédulas nas urnas eletrônicas. Somente as urnas eletrônicas poderão transferir as e-cédulas para os respectivos candidatos, partidos ou coligações, votos nulos ou votos brancos. As transferências contidas nas urnas eletrônicas serão concluídas no encerramento da sessão eleitoral após a transferência dos dados criptografados para Consórcio TRE para processamento.

Figura 14: Ciclo de propriedade da e-cédula durante seu ciclo de vida.

Fonte: Autor

3.5 Urna eletrônica

A arquitetura da urna eletrônica permite ao eleitor a execução do seu direito ao voto sem a necessidade de sua identificação na cédula, o terminal do mesário possibilita a identificação do eleitor, em alguns modelos através da biometria, com a validação do eleitor o terminal do mesário envia um sinal para o terminal de votação habilitando-o para uso do votante (TRIBUNAL SUPERIOR ELEITORAL, 2021a).

O sinal enviado pelo terminal do mesário não identifica o eleitor para enviar o sinal para o terminal de votação. O flash card memória de resultado contido na urna eletrônica deve ser atualizado para fazer os registros das e-cédulas,

registrando as e-cédulas em posições aleatórias, sem o armazenamento de data e hora, com objetivo de impedir a identificação no eleitor.

O terminal do mesário deverá ter um flash card de memória de resultado para poder fazer o registro do eleitor na blockchain, ressalto que esse registro não deve ser vinculado a e-cédula e ficará disponível para o eleitor através de uma carteira digital tendo a finalidade de comprovação de participação da eleição, por parte do eleitor e pelos consórcios participantes da rede blockchain. Visa possibilitar o eleitor auditar a participação da eleição e o momento de encerramento do processamento da urna eletrônica que foi utilizada para registro do voto, assim aumentando significadamente a transparência do pleito, permitindo confrontar as informações impressas no boletim de urna com as informações contidas na rede blockchain.

Outra característica importante da urna eletrônica e o fato de o equipamento funcionar de forma isolada e não possuir nenhum componente que possibilidade sua conexão externa, o sistema operacional Linux contido na urna é preparado pela Justiça Eleitoral de forma a não incluir nenhum mecanismo de software que permita a conexão com redes ou o acesso remoto (COIMBA, 2014).

No encerramento das seções de votação, o pen drive contendo a memória de resultado, é retirado da urna eletrônica e levado pelo mesário ao cartório eleitoral, os dados criptografados são enviados ao consórcio do TRE via uma rede virtual privada e protegida da Justiça Eleitoral. Os contratos inteligentes aprovados pelo consórcio serão responsáveis por verificar a autenticidade das e-cédulas, validar a informação de votação e fazer a contagem geral dos votos por urna eletrônica, sessão de votação, município e estado da federação. Por fim, o TSE faz a validação dados recebidos na rede blockchain, consolida os votos encaminhados pelos Estados Federativos e divulga os resultados em tempo de execução.

3.6 Contrato inteligente

Um contrato inteligente, funciona como um aplicativo distribuído confiável, que garante sua segurança e confiabilidade na rede blockchain e do consenso subjacente entre os participantes sendo a representação da legislação vigente.

Para execução do contrato inteligente pelos participantes do Consórcio da Justiça Eleitoral e Consórcio TRE, precisa seguir as seguintes etapas para disponibilização na rede blockchain:

1. Implementação do contrato inteligente, de acordo com a legislação do Direito Eleitoral, toda interação com o livro-razão da blockchain utilizará os contratos inteligentes;
2. Instalação do contrato inteligente por todas entidades que utilizará o recurso desenvolvido;
3. Aprovação do contrato inteligente pelas entidades que fizeram a instalação. Precisam ter quórum suficiente de aprovação para que seja permitido a execução nos canais de comunicação dos consórcios.

A aprovação do contrato inteligente é uma etapa muito importante, permite a participação das entidades no processo de desenvolvimento dos contratos inteligentes, a validação da execução do código fonte. Aumentando a transparência e auditoria no processo eleitoral.

Os processos do pleito eleitoral deverão ser representados através de contratos inteligentes que serão acessados através de interfaces disponíveis pelos consórcios responsáveis pelo desenvolvimento dos softwares.

3.7 Considerações finais

Buscando compreender os limites de segurança e auditoria da tecnologia blockchain a partir das informações coletadas através de pesquisa acadêmica foi possível evidenciar que a tecnologia tem potencial para prover mudanças significativas nos processos eleitorais existentes oferecendo uma nova possibilidade para países democráticos evoluírem seus processos de papel e caneta para um processo tecnológico ganhando mais eficiência na segurança da informação.

Destaco que o Brasil leva grande vantagem em relação a outros países para essa evolução uma vez que utiliza o Sistema Eletrônico de Votação e Totalização de Votos por mais de duas décadas assim garantindo a democracia brasileira.

A imutabilidade do livro-razão garante a integridade dos ativos mantendo registro de transações. Os registros são replicados para os participantes dos

consórcios oferecendo novas possibilidades de auditoria e transparência para o pleito. A autenticidade é não-repúdio das transações são garantidas através de identidade digital e são validadas por um mecanismo de consenso antes de serem registradas. Essas características são essenciais para a confiabilidade da tecnologia blockchain. Estendendo essas características e confiabilidade para Sistema Eletrônico de Votação e Totalização de Votos destaco que a tokenização dos ativos uma das principais vantagens da segurança de informação no processo eleitoral. Como demonstrado no estudo a tokenização da e-cédula possibilita novas formas de auditoria e aumentando a transparência na utilização das cédulas durante o processo eleitoral.

Outra vantagem que vale destacar é sobre a aprovação do código-fonte disponível para execução na rede blockchain pelo consórcio, a informação registrada no livro-razão precisa ser válida de acordo com a implementação dos contratos inteligentes. Esse procedimento visa aumentar a qualidade do código-fonte que compõe os contratos inteligentes permitindo que todos participantes possam garantir que as execuções dos softwares sigam os requisitos da legislação do Direito Eleitoral.

Considerando que há riscos presentes na privacidade do eleitor na implementação do processo eleitoral utilizando a tecnologia blockchain o que pode levar a falta de ética no voto, manchando a reputação da democracia brasileira. O conhecimento empírico do Tribunal Superior Eleitoral teve a solução do problema democrático descrito antes da apresentação da tecnologia blockchain proposta por Nakamoto no paper do Bitcoin. A arquitetura de hardware da urna eletrônica está desenhada para habilitar o terminal de votação sem a identificação do eleitor, assim viabilizando a implementação da tecnologia blockchain no Sistema Eletrônico de Votação e Totalização dos Votos seguindo os processos executados pelo Tribunal Superior Eleitoral. Dessa forma destaca-se como uma vantagem para implementação da tecnologia blockchain no Sistema Eletrônico de Votação e Totalização de Votos é o projeto arquitetural do hardware da urna eletrônica permitindo a privacidade do eleitor na rede blockchain, precisando apenas de atualizações nos softwares de votação e totalização conforme descrito neste estudo.

CONCLUSÃO

As leituras acerca da tecnologia blockchain enquanto um novo fenômeno em várias áreas negociais provocou a necessidade de aprofundamento e compreensão da sua capacidade enquanto uma inovação. A partir das características da tecnologia e de informações que emergiram das leituras optou-se pelo campo das governamentais, mais especificamente a inovação do processo eleitoral, como área de investigação.

Nesse contexto, é importante destacar que o objetivo do desenvolvimento da pesquisa foi guiado pelas seguintes inquietações: Quais são os limites de segurança e auditoria e quais são as possibilidades de evolução utilizando a tecnologia blockchain para execução das eleições utilizando o Sistema Eletrônico de Votação e Totalização dos Votos do Tribunal Superior Eleitoral? Existe a possibilidade das eleições on-line? O eleitor pode auditar a cédula de votação?

As indagações instigaram a condução do presente estudo que buscou, mediante o objetivo geral, analisar os aspectos de segurança da informação do Sistema Eletrônico de Votação e Totalização dos Votos e as possibilidades da evolução para utilização da tecnologia blockchain mediante um estudo de caso.

Da mesma forma, o estudo de caso demostrou a possibilidade de evolução do Sistema Eletrônico de Votação e Totalização de Votos para utilização da tecnologia blockchain permitindo a descentralização do processo eleitoral criando uma infinidade de novos mecanismos de auditoria. Outro ganho importante para o processo eleitoral seria a disponibilidade, integridade e confiabilidade em um ambiente descentralizado. Os participantes terão acesso as informações de votação e codificação dos contratos inteligentes disponível pelo Consórcio da Justiça Eleitoral, permitindo que todos participantes possa auditar as informações contida na rede blockchain.

Sobre a possibilidade de eleições on-line e auditoria do eleitor na cédula de votação utilizada, ressalto que a tecnologia blockchain há riscos na garantia da privacidade do eleitor, desta forma, o estudo de caso se baseou na utilizada da urna eletrônica e os processos existentes no Tribunal Superior Eleitoral. A e-cédula permite ao eleitor a verificação de propriedade do token durante todo o período do processo eleitoral, após a tokenização é possível acompanhar o token em todo

processo até a chegada na urna eletrônica. Após a votação é importante identificar de qual urna eletrônica partiu o voto para determinado candidato sem a identificação do eleitor.

A e-cédula sugerida é vista como uma solução alternativa a impressão do voto na urna eletrônica, aumentando significantemente a transparência do processo eleitoral. A impressão do voto poderia ser vista como retrocesso tecnológico devido ao volume de papel gerado.

Por fim, verificou-se que a solução blockchain pode ser utilizada para execução do processo eleitoral, no entanto a tecnologia não garante a privacidade do eleitor. O projeto arquitetural da urna eletrônica resolve essa problemática. Este estudo de caso não se debruçou sobre a evolução da urna eletrônica viabilizando transações off-line e como continuidade desse trabalho, sugere-se a produção de dissertações e pesquisas sobre as possíveis evoluções da urna eletrônica é a incorporação das transações off-line no mecanismo de consenso de uma rede blockchain.

REFERÊNCIAS

ALMEIDA, RAFAEL SARRES DE. A Revolução do Blockchain - Conheça a história dessa tecnologia e como ela promete mudar o mundo. Revista iMasters, São Paulo, edição 25, p.40-47, mar. 2018. Disponível em: https://issuu.com/imasters/docs/25. Acesso em: 6 fev. 2021.

ANTONOPOULOS, ANDREAS M.. Mastering Bitcoin: Programming the Open Blockchain. Open Edition. 2º Edition. p. 41

APD ASSOCIAÇÃO PARA O PROGRESSO DA DIREÇÃO. Principais diferenças entre DLT e blockchain. Disponível em: https://www.apd.pt/principais-diferencas-entre-dlt-e-blockchain/. Acesso em: 6 fev. 2021.

BINANCE ACADEMY. O que faz uma Blockchain segura?. Disponível em: https://academy.binance.com/pt/articles/what-makes-a-blockchain-secure. Acesso em: 09 fev. 2021.

BINANCE.COM. Ataques Sybil. Disponível em https://academy.binance.com/pt/articles/sybil-attacks-explained. Acessado em 09 de fev. 2021.

BINANCE.COM. O que é um Ataque de 51%?. Disponível em https://academy.binance.com/pt/articles/what-is-a-51-percent-attack. Acessado em 09 de fev. 2021.

BINANCE.COM. O que é um Eclipse Attack? Disponível em https://academy.binance.com/pt/articles/what-is-an-eclipse-attack. Acessado em 09 de fev. 2021.

BRASIL. Constituição Da República Federativa Do Brasil De 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 fev. 2021.

BRASIL. Lei n. 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 4 fev. 2021.

CANOTILHO, J.J. Gomes. Direito Constitucional e Teoria da Constituição. 7ª ed. Coimbra: Almedina, 2003.

COIMBA, Rodrigo Carneiro Munhoz. Por que a urna eletrônica é segura. In: TRIBUNAL SUPERIOR ELEITORAL. Revista Eletrônica da EJE ano IV, n. 6. 2014. Disponível em: https://www.tse.jus.br/o-tse/escola-judiciaria-eleitoral/publicacoes/revistas-da-eje/artigos/revista-eletronica-eje-n.-6-ano-4/por-que-a-urna-eletronica-e-segura. Acesso em: 9 mar. 2021.

DE TOLEDO, Maria Fernanda Pessatti. Os Direitos Políticos na Constituição Federal de 1988. 2016. Disponível em: http://genjuridico.com.br/2016/05/16/os-direitos-politicos-na-constituicao-federal-de-1988/. Acesso em: 4 fev. 2021.

DIVINO, Sthéfano. Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios. São Paulo: Editora Plenum, 2019. Disponível em: https://www.researchgate.net/publication/328838400_SMART_CONTRACTS_CONCEITOS_LIMITACOES_APLICABILIDADE_E_DESAFIOS. Acesso em: 09 fev. 2021.

EUROPEAN COMMISSION. Blockchain Technologies. 2021. Disponível em: https://ec.europa.eu/digital-single-market/en/blockchain-technologies. Acesso em: 6 fev. 2021.

EXAME. TSE testa projetos para ‘eleições do futuro’ baseados em blockchain. 2020. Disponível em: https://exame.com/future-of-money/blockchain-e-dlts/tse-testa-projetos-para-eleicoes-do-futuro-baseados-em-blockchain/. Acesso em: 04 fev. 2021.

FERREIRA, Maurício Pinto. Comentários à Constituição Brasileira. Vol. 3. São Paulo: Saraiva, 1992, p. 212.

FUNDAÇÃO CENTROS DE REFERÊNCIA EM TECNOLOGIAS INOVADORAS. Urna Eletrônica Brasileira, 2021. Disponível em: https://www.certi.org.br/pt/casosdesucesso-urna-eletronica-brasileira. Acesso em: 4 fev. 2021.

GOMES, Luiz Flávio. Voto secreto e democracia no brasil. Disponível em: https://professorlfg.jusbrasil.com.br/artigos/121932388/voto-secreto-e-democracia-no-brasil. Acesso em: 19 fev. 2021.

HYPERLEDGER FABRIC. Introdução. Disponível em: https://hyperledger-fabric.readthedocs.io/pt/latest/blockchain.html. Acesso em: 04 fev. 2021.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. ICP-Brasil. 2020. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em: 09 fev. 2018.

KSHETRI, Nir; VOAS, J. Blockchain-Enabled E-Voting, 2018. Disponível em: https://ieeexplore.ieee.org/document/8405627. Acesso em: 19 fev. 2021.

LACERDA, Eduardo. A biometria na ICP-Brasil. 2015. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/indice-de-noticias/a-biometria-na-icp-brasil. Acesso em: 09 fev. 2018.

MENDES, Antônio Carlos. Introdução à Teoria das Inelegibilidades. São Paulo: Malheiros, 1994, p. 74.

MORAES, Alexandre de. Direito Constitucional. 13ª ed. Editora Atlas. 2003. p. 234.

NIST. Blockchain. 2021. Disponível em: https://www.nist.gov/blockchain. Acesso em: 6 fev. 2021.

OECD ILIBRARY. Chapter 11. Artificial intelligence, blockchain and quantum computing. 2021. Disponível em: https://www.oecd-ilibrary.org/sites/c51bcfeb-en/index.html?itemId=/content/component/c51bcfeb-en#section-232. Acesso em: 09 fev. 2021.

RORIZ, Rodrigo Matos. O direito ao voto secreto nas democracias modernas: breves reflexões sobre a Ação Direta de Inconstitucionalidade 4543, dez 2013. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/37545/o-direito-ao-voto-secreto-nas-democracias-modernas-breves-reflexoes-sobre-a-acao-direta-de-inconstitucionalidade-4543. Acesso em: 19 fev. 2021.

SZABO, Nick. Smart Contracts: Building Blocks for Digital Markets, 1996. Disponível em: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 09 fev. 2021.

TEIXEIRA, Tarcisio; ESTANCIONE, Laura Maria Brandão. Urna eletrônica e voto impresso: a segurança no Direito Eleitoral. 2016. Disponível em: https://www.conjur.com.br/2016-mai-11/urna-eletronica-voto-impresso-seguranca-direito-eleitoral. Acesso em: 4 fev., 2021

TIINSIDE. TSE divulga relatório final dos testes das urnas de 2019 para consulta. 2019. Disponível em: https://tiinside.com.br/10/12/2019/tse-divulgado-relatorio-final-dos-testes-das-urnas-de-2019-para-consulta/. Acesso em: 04 fev. 2021.

TRIBUNAL DE CONTAS DA UNIÃO. Sumário Executivo Levantamento da Tecnologia Blockchain. 2020. Disponível em: https://portal.tcu.gov.br/data/files/59/02/40/6E/C4854710A7AE4547E18818A8/Blockchain_sumario_executivo.pdf. Acesso em: 04 fev. 2021.

TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO. Em cerimônia pública, Justiça Eleitoral gera mídias, prepara e lacra urnas. 2021f. Disponível em: https://www.tre-sp.jus.br/imprensa/noticias-tre-sp/2018/Setembro/em-cerimonia-publica-justica-eleitoral-gera-midias-prepara-e-lacra-urnas. Acesso em: 04 fev. 2021.

TRIBUNAL REGIONAL ELEITORAL DE SERGIPE. Segurança no Processo Eleitoral. 2019. Disponível em: https://www.tre-se.jus.br/imprensa/noticias-tre-se/2019/Julho/seguranca-no-processo-eleitoral. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Acordo entre ITI e Justiça Eleitoral dá mais segurança à urna eletrônica e aos certificados digitais, 2017b. Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/acordo-entre-iti-e-justica-eleitoral-garante-mais-seguranca-a-urna-eletronica-e-a-emissao-de-certificados-digitais. Acesso em: 07 mar. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Biometria atual por UF. 2021j. Disponível em: https://www.tse.jus.br/eleitor/biometria/biometria-atual-uf. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Identificação de soluções para modernização do processo eleitoral 2020. 2021i. Disponível em: https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/audiencia-publica/identificacao-de-solucoes-para-modernizacao-do-processo-eleitoral-2020. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Investigadores do TPS relatam experiência no evento e falam sobre achados relevantes encontrados. 2017a.Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2017/Dezembro/investigadores-do-tps-relatam-experiencia-no-evento-e-falam-sobre-achados-relevantes-encontrados. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Preparação das urnas. 2021e. Disponível em: https://www.tse.jus.br/eleicoes/processo-eleitoral-brasileiro/logistica-e-preparacao/preparacao-das-urnas. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Registro digital do voto. 2021c. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/registro-digital-do-voto. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Respostas às vulnerabilidades e sugestões de melhorias encontradas no Teste Público de Segurança 2017. 2018. Disponível em: https://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017-1527192798117/at_download/file. Acesso em: 19 mar. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Segurança. 2021b. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Testes Públicos de Segurança do Sistema Eletrônico de Votação 2017. 2021g. Disponível em: https://www.tse.jus.br/eleicoes/eleicoes-2018/testes-publicos-de-seguranca-do-sistema-eletronico-de-votacao. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. TSE conclui Cerimônia de Assinatura Digital e Lacração dos Sistemas Eleitorais. 2021d. Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2020/Outubro/tse-conclui-cerimonia-de-assinatura-digital-e-lacracao-dos-sistemas-eleitorais. Acesso em: 04 fev. 2021.

TRIBUNAL SUPERIOR ELEITORAL. Urna eletrônica. 2021a. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/urna-eletronica. Acesso em: 4 fev. 2021.

WANG, Huaimin; ZHENG, Zibin;XIE, Shaoan;DAI, Hong-Ning;CHEN, Xiangping. Blockchain challenges and opportunities: a survey. Revista Brasileira de Administração. 2018. Disponível em: https://www.researchgate.net/publication/328271018_Blockchain_challenges_and_opportunities_a_survey. Acesso em: 17 mar. 2021.