UNIVERSIDADE FEDERAL DO PIAUÍ – UFPI

CENTRO DE EDUCAÇÃO ABERTA E A DISTÂNCIA – CEAD/UFPI

CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

MONOGRAFIA

Registro Distribuído de Votação Eletrônica: Desenvolvendo e Testando um Sistema Usando Blockchain

Rammyres José Oliveira Pereira

Campo Maior - PI

Fevereiro de 2021

Rammyres José Oliveira Pereira

Registro Distribuído de Votação Eletrônica: Desenvolvendo e Testando um Sistema Usando Blockchain

Monografia submetida ao Curso de Bacharelado de Sistemas de Informação como requisito parcial para obtenção de grau de Bacharel em Sistemas de Informação.

Orientador: Antônio da Paixão de Freitas e Silva
Coorientador: Leonardo Ramon Nunes de Sousa
Coorientador: Marcos Antônio dos Santos

Campo Maior - PI

Fevereiro de 2021

Rammyres José Oliveira Pereira

Registro Distribuído de Votação Eletrônica: Desenvolvendo e Testando um Sistema Usando Blockchain

Monografia submetida ao Curso de Bacharelado de Sistemas de Informação como requisito parcial para obtenção de grau de Bacharel em Sistemas de Informação.

Trabalho _____. Campo Maior - PI, ____ de _____ de 2020:

Antônio da Paixão de Freitas e Silva
Orientador

Leonardo Ramon Nunes de Sousa
Coorientador

Marcos Antônio dos Santos
Coorientador

Valquíria Cardoso da Silva
Professora Convidada

Daniela Carla da Silva
Professora Convidada

Campo Maior - PI
Fevereiro de 2021

Lista de abreviaturas e siglas

BCS	Blockchain-based crowdsourced systems
BEV	Blockchain Enabled Voting
DLT	Distributed Ledger Technology
DoS	Denial of Service
ECDSA	Elliptic Curve Digital Signature Algorithm
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
JSON	JavaScript Object Notation
P2P	Peer to Peer
QR Code	Quick Response Code
SBSeg	Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais
SBC	Single Board Computer
UTXO	Unspent Transactions Output

Sumário

Resumo

O objetivo deste trabalho é discutir as tecnologias de votação eletrônica, além de apresentar uma nova alternativa, baseada na tecnologia blockchain, o Registro Distribuído de Votação Eletrônica, bem como discutir seus resultados. Historicamente votar é parte do cotidiano das democracias e com o crescimento delas, organizar o processo de votação e apurar os resultados se tornou cada vez mais desafiador. Por causa disso mecanismos eletrônicos e automáticos para apuração eleitoral se tornaram comuns. O Brasil adotou seu sistema de votação eletrônico na década de 90, entretanto o mesmo tem sido criticado por falhas e falta de transparência. Em 2008 a tecnologia blockchain foi exposta ao mundo, permitindo sistemas transparentes, mas que preservam a privacidade, despertando a atenção de especialistas, que tem se debruçado para criar um sistema de votação baseado em blockchain. Para atender propósito o RDVE será desenvolvido e testado através de eleições simuladas e coleta dos produtos das votações. Como resultado pretendemos avaliar o *software* proposto e analisar sua adequação para atendimento aos quesitos de confidencialidade, confiabilidade e auditabilidade.

Palavras-chave: eleição, votação, eletrônica, digital, blockchain, registro.

Abstract

This paper aims to discuss the voting technologies and propose a BEV alternative, the RDVE (*Registro Distribuido de Votação Eletrônica*), as solution to, at least, some of the issues we discuss here, and analyze its results. Voting is part of our daily life throughout the history of all democracies, and following their growth, the difficulties in the voting processes and tallying grew in size and complexity. Becausue of this, electronic and automated schemas for ballot processing and counting became commonplace. Brazil adopted its Direct-Recording Electronic Voting Scheme in the 1990s, but, due to failures poited by experts and lack of transparency it has been heavily criticized. In 2008 the blockchain technology was introduced, enabling transparent, yet private, systems, drawing attention from many in industries like finance and e-Government, which in turn has been working towards a secure eletronic voting system. As result we intend to assess the RDVE as solution, specialy aiming its requisites: confidenciality, trustworthiness and auditability.

Keywords: ballot, blockchain, elections, electronic, tallying, voting.

1 Introdução

Votar é um princípio básico das democracias, das antigas até as modernas e tem sido associado a capacidade popular de tomar decisões e governarem as si próprias. Registros de sistemas de votação datam desde o século VI a.c. (BLACKWELL, 2003), quando foi introduzido o modelo ateniense de democracia. Os gregos votavam através dos *ostracon*, fragmentos de cerâmica que retinham, por exemplo, o nome dos cidadãos da *Pólis* que poderiam ser banidos (ostracismo).

Ao longo da história o modelo ateniense foi incorporado por outras culturas, como a romana, que adaptaram o conceito de votação através das *leges tabellariae* (*garbinia*, *cassia*, *papiria* e *caelia*) nas decisões populares nos *Comitia* e eleições de magistrados durante o século II a.c. (YAKOBSON, 1995) e avançou até as democracias modernas, que incorporaram conceitos de segredo e privacidade, principalmente através do chamado Voto Australiano (NEWMAN, 2003) ainda no século XIX.

O aumento do número de votantes, no entanto, passou a tornar-se um problema. Para exemplificar, o número de votantes nos Estados Unidos em eleições presidenciais subiu de menos de 75.000 em 1800 (VOTE ARCHIVE, 2015) para mais quase 136.000.000 em 2016 (VOTE ARCHIVE, 2016). Essa evolução no ínterim exigiu mudanças de estratégias, já que o sistema de contagem voto a voto mostrou-se ineficiente na contagem de tal volume de votos (BATTAGLINI; MORTON; PALFREY, 2007).

Ainda durante o século XIX as primeiras tentativas de criação de meios automatizados de votação e contagem foram criados, como a “Máquina de Votar Elétrica” de Wood (1898). Durante o século XX muitas tentativas foram abordadas, com o virtual monopólio dos modelos de votação do AVM Corporation nos anos 60 a 80 como destaque (JONES; SIMONS, 2012). O Brasil começou a ponderar a utilização de modelos eletrônicos a partir da década de 80 (BRASIL, 2014), passando a implantar o atual modelo durante a década de 90.

O modelo adotado por aqui, no entanto, não se livrou de críticas. Durante a primeira e segunda décadas dos anos 2000 problemas como violação do sigilo do voto e execução de código arbitrário puderam ser detectados nas urnas eletrônicas (GRAAF, 2017), tornando-se alvo de críticas de especialistas (ARANHA et al., 2018) e de discussões populares (PAYÃO, 2018).

Ao mesmo tempo uma revolução começou a se desenhar com base numa nova maneira de representar dados transacionais. (NAKAMOTO, 2008) publicou um artigo descrevendo o que passou a se chamar *blockchain*, uma cadeia crescente de blocos

de dados, encadeados entre si através de *hashes* (o bloco atual sempre possuí o *Hash* do último bloco). Internamente os blocos são formados por listas de dados, que por sua vez estão conectados entre si através de uma árvore de *hashes*. Todos os nós da rede recebem as transações dela e criam seus próprios blocos e cadeias de dados, impedindo assim a inclusão de dados espúrios; ao manter evidências em diversos computadores diferentes, impede-se que uma transação existente em apenas um nó, ou numa minoria deles, seja considerada válida.

Isso trouxe ao cenário mundial a ideia de introduzir essa tecnologia para resolução de diversos problemas, como cadeia de propriedade de imóveis e automóveis, transações financeiras, etc. Algumas abordagens para solução serão tratadas ao longo deste trabalho.

A proposta deste trabalho é discutir essas abordagens, um breve histórico, além de introduzir uma nova proposta, o Registro Distribuído de Votação Eletrônica (RDVE), que tenta permitir a coleta e processamento de votos utilizando registro distribuído em blockchain, bem como discutir sua viabilidade sob aspectos como confiabilidade, confidencialidade e auditabilidade.

2 Justificativa

Desprende-se da análise da legislação vigente em relação as Eleições no Brasil a necessidade da manutenção de dois conceitos aparentemente antagônicos entre si: privacidade e publicidade; enquanto é preponderante para manutenção da liberdade de escolha do eleitor, é necessário que o eleitor seja identificado através de dados públicos e a divulgação irrestrita dos resultados das votações.

A utilização do atual protocolo eleitoral, muito embora preveja mecanismos para garantir que o voto não será associado a seu emissor e haja ampla divulgação dos resultados das votações, a ausência de transparência em várias das etapa não deixa claro como essas proteções são executadas, não parecendo que sejam suficientes para atender aos critérios acima. Os *softwares* e produtos de votação são sigilosos e não há como analisá-los.

Tecnologias emergentes, como as apresentadas neste trabalho, entretanto são fortemente amparadas em privacidade e publicidade simultâneas. Os protocolos utilizados habitualmente enfocam na manutenção do segredo das identidades das partes que realizam as transações, entretanto todos os registros dessas transações são públicos e acessíveis a todos os usuários da rede, inclusive para os que não fizeram parte delas. A publicidade é tão relevante, que só quando a maioria dos nós da rede podem ter acesso e validar os dados de certa transação é que ela se torna válida, preceito conhecido como consenso, não podendo mais ser revertida.

Assim sendo nos parece que a utilização dessas tecnologias, com as adaptações necessárias ao atendimento de certas questões legais, é uma alternativa viável para criação de um sistema eleitoral que agregue as características essenciais aqui discutidas.

3 Problematização

Questões relacionadas à segurança e privacidade do modelo de votação brasileiro, especialmente a Urna Eletrônica Brasileira, tem sido recorrentes. Em seu livro O Mito da Urna o professor da UFMG, Dr. Jeroen Van de Graaf (2017), explora diversas falhas no nosso modelo de urna eletrônica. Falhas atribuídas a possibilidade de violação de privacidade, violação da integridade dos votos ou recuperação da ordem de votação são discutidas extensivamente no trabalho.

O professor Dr. Van de Graaf também cita trabalhos do Dr. Diego Aranha, que dedicou atenção especial a falhas contidas na urna eletrônica brasileira, como seu artigo apresentado no SBSeg (ARANHA et al., 2018), em que detalha a possibilidade de execução de código arbitrário na urna e seu relatório produzido com base na análise direta do software da urna, “Vulnerabilidades no *software* da urna eletrônica brasileira” (ARANHA et al., 2014), há menção de erros preocupantes, como a possibilidade de recuperação da ordem dos votantes, implicando em violação de sigilo de voto, além de demonstração de que o processo de cifragem é inadequado e o algoritmo obsoleto.

Diversas são as críticas traçadas pelos especialistas citados, e muitas são replicadas pelo público geral, que se foca especialmente na falta de transparência do processo e ausência de auditoria pública.

O que se questiona neste trabalho é a possibilidade de utilização das tecnologias discutidas, especialmente o Registro Distribuído, para conseguir sanar os problemas levantados, especialmente a ausência de transparência e os questionamentos quanto a privacidade do voto.

4 Hipotese

Qual a efetividade do uso de tecnologias emergentes para criação de um protocolo de votação eletrônico descentralizado, que atenda aos prerrequisitos de confidencialidade, confiabilidade e auditabilidade?

5 Objetivos

5.1 Objetivo Geral

O objetivo deste trabalho é, após analise da literatura existente utilizar *blockchain* para criar um protocolo para votação distribuído, conforme premissas estabelecidas na hipótese.

5.2 Objetivos Específicos

A fim de atingir este objetivo geral, os seguintes objetivos serão seguidos:

- Desenhar o protocolo para comunicação entre os nós;
- Implementar uma prova-de-conceito em python; e
- Efetuar testes públicos para coleta de dados da prova-de-conceito quanto a adequação a hipótese.

6 Revisão Bibliográfica

A tecnologia blockchain foi primeiro descrita por Nakamoto (2008), em seu artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", para descrever um sistema de movimentações financeiras eletrônicas. A ideia essencial seria encadear blocos de transações, ligados entre si através do *hash*, já que cada bloco conteria o *hash* do bloco anterior. As transações seriam assíncronas, propagadas através de uma rede Ponto-a-Ponto, em que cada nó processaria e persistiria a transação em sua própria cadeia, mantendo as evidências de cada transação em uma Arvore de *Hashes* (MERKLE, 1988), também conhecida como Árvore de Merkle, impedindo que uma delas possa ser registrada mais de uma vez. As transações não estariam ligadas a contas, mas a pares de chaves assimétricas, tornando-as virtualmente anônimas. Os nós também precisariam de gasto computacional para computar o *Hash* de cada bloco (NAKAMOTO, 2008), utilizando um sistema de *Proof of Work* (GERVAIS et al., 2016), derivado do algoritmo de prevenção de Negação de Serviço Hashcash (BACK et al., 2002), desestimulando as tentativas de forjar blocos, já que tal custo seria muito elevado.

A estrutura pensada por Nakamoto estaria protegida contra problemas básicos de redes distribuídas, entre eles a Falha Bizantina (LAMPORT; SHOSTAK; PEASE, 1982), que descreve como um nó dispersando informações falsas ou falhas, numa rede distribuída em anel, pode influenciar toda a rede. Outro problema potencialmente resolvível pela proposta, neste caso relacionado aos sistemas financeiros eletrônicos, e bastante relevante nesse contexto, é o problema do gasto duplo (BRANDS, 1993), que permite um usuário utilizar mais de uma vez um *token* representativo de um valor. A tecnologia de encadeamento de blocos passou a ser conhecida como blockchain e as tecnologias baseadas nela são popularmente conhecidas como Registro Distribuído (SUNYAEV, 2020).

Essa abordagem despertou interesse de diversas indústrias, especialmente a financeira (CAHILL et al., 2020), fazendo com que muitos acadêmicos também se voltassem para o assunto. Várias análises sucederam a publicação e posterior popularização do Bitcoin e das tecnologias que emergiram a partir dele. Questões tão diversas, que vão a simples cópias do produto original (conhecidas como *Altcoins*) (NGUYEN et al., 2019), até a aplicação em cadeias de produção e tributação distribuídas (CHOI; LUO, 2019) foram descritas na literatura desde então.

Em consequência dessa popularidade, questões sobre segurança passaram, também, a serem alvo de constante escrutínio. Ma et al. (2020) propuseram uma aná-

lise detalhada, após pesquisa em diversas plataformas colaborativas baseadas em blockchain, demonstrando impactos da tecnologia em si, em aspectos relevantes tratados neste trabalho, como privacidade e confiabilidade, utilizando exemplos práticos de tecnologias já implementadas, como registros médicos.

No mesmo sentido se pronunciaram Zhong e Huang (2020), quando analisaram superficialmente os chamados BCS (*Blockchain-based crowdsourced systems*), focando nos aspectos mais primordiais do Bitcoin e outras Criptomoedas, como segurança e privacidade, da mesma forma que Feng et al. (2019), que especificaram as ameaças mais comuns a serviços baseados na tecnologia, como o comprometimento da privacidade e disponibilidade da rede (ataques DoS), além de relatarem como a implementação correta de um registro distribuído pode contribuir para mitigar tais problemas.

Considerando as características da blockchain, muitos trabalhos continuaram a seguir, Lier (2017) trata de diversos aspectos metafilosóficos do tema, como as possibilidades de integração entre sistemas ciber-físicos e, obviamente seu uso em sistemas de votação, além da votação interna, para aquisição de consenso. Não demorou para que ideias sobre *e-Government* surgissem e abordassem a utilização dessas tecnologias para permitir o registro de eleições, que de forma geral são conhecidos pela sigla BEV (*blockchain enabled voting*).

Onik et al. (2019) descreve em seu trabalho *"Privacy-aware blockchain for personal data sharing and tracking"* mecanismos para registro de informações pessoais, mantendo a privacidade e com mecanismos para controle do compartilhamento dessas informações, baseados nas tecnologias discutidas neste trabalho. No mesmo sentido se pronunciaram Warkentin e Orgeron (2020), ao analisarem a "Tríade da CIA" (i.e. confidencialidade, disponibilidade e integridade) aplicada as tecnologias de blockchain, Noções extraídas da análise também levam em conta a impossibilidade de reversão de atos registrados ou negação de sua autoria, o que tornaria a abordagem relevante para sistemas governamentais, como o exemplo citado no trabalho (WARKENTIN; ORGERON, 2020), no estado de Illinois, onde foram testados diversos usos de registros distribuídos em seu governo.

Diversos usos para *e-Gov* foram propostos recentemente (ØLNES; UBACHT; JANSSEN, 2017), como modelos de registros de veículos, antecedentes criminais, dentre os diversos usos possíveis. Kshetri e Voas (2018b) vão mais a fundo, destacando que tais sistemas podem prevenir corrupção e fraudes, em decorrência da publicidade preponderante dos registros e sua forçosa imutabilidade.

Elisa et al. (2018), em seu artigo "*A framework of blockchain-based secure and privacy-preserving E-government system*" delineia de forma bem detalhada mecanismo de funcionamento de sistemas de *e-Government* baseados em registro dis-

tribuído, de forma geral, incluindo todos os serviços de G2G, G2C e G2B.

Historicamente o TSE (BRASIL, 2014) demonstrou interesse em informatizar o sistema de votação Brasileiro desde a década de 80, tomando medidas para informatização das Urnas durante a segunda metade da década de 90. O modelo brasileiro de votação eletrônica atualmente é adotado em todo o território nacional, para todas as eleições majoritárias e proporcionais.

O impacto da confiança da população em tecnologias como essa já foi explorando, para o uso em sistemas governamentais complexos, como o sistema de votação brasileiro. Moura e Gomes (2017), apresentaram a percepção negativa dos atuais sistemas eletrônicos de votação, bem como a visão positiva de um sistema baseado em blockchain.

As ideias, no geral, dão conta que um sistema de votação BEV seria percebido como mais transparente, confiável e auditável, já que seu resultado, o Registro Distribuído, é público e disponibilizado a todos os nós e clientes ligados a rede.

Curran (2018) cita as dificuldades do dito *E-Voting*, que é o termo genérico para votações eletrônicas que não dependam de maquinário específico, e habitualmente propõem a utilização de meios eletrônicos para apuração de votos online, com o uso de aplicativos e *websites*. Potenciais falhas e abertura a fraudes, além das dificuldades de auditar tais sistemas são citados como principais motivos da rejeição da adoção desse modelo.

Dificuldades para atrair eleitores, especialmente os mais jovens, mais facilmente atraídos por tecnologia e menos por ambientes burocráticos, causando aumentos sucessivos das abstenções, também são dificuldades trazidas as eleições, tanto tradicionais em papel, quanto as utilizado sistemas de votação eletrônico. Entretanto vê a possibilidade de inclusão de sistemas com blockchain para registro e apuração de votos como um meio de desenvolvimento de *apps* e *websites* suficientemente confiáveis para registro de votações eletrônicos.

Dentre os possíveis resultados citados por Curran (2018) também constam possibilidades, julgadas por muitos como necessárias, de auditabilidade, tanto individual (i.e., o eleitor é capaz de verificar seu próprio voto) como publica (i.e., é possível a qualquer pessoa auditar a votação como um todo).

Abuidris, Kumar e Wenyong (2019) fizeram uma pesquisa sobre uma série de soluções propostas para os conceitos levantados por Curran. Os estudiosos identificaram, pelo menos, seis propostas, dentre elas os sistemas *Follow My Vote*, *Agora* e *Polys*, que tem relativa notoriedade.

Todos esses sistemas têm, como funções básicas, a persistência dos votos em um Registro Distribuído, entretanto com grande enfoque em soluções que não

dependam de pontos de coleta de votos, nem maquinário específico, já que eles serão colhidos através de *apps* ou *websites*. Os autores também fizeram uma análise comparativa a respeito de diversas características das soluções, como auditabilidade, descrita nos trabalhos como “verificabilidade” (tradução livre), tanto individual como pública (descrita como “universal”), e listaram objetivos a serem alcançados em soluções futuras, como um meio de identificar eleitores, sem comprometer o sigilo do voto, tornar as experiências de usuários simples o bastante a fim de tornar o acesso fácil a todos os segmentos da população, mecanismos para garantir a escalabilidade e expansão da base de usuários, além de meios para aprimorar a velocidade para inserção dos votos e do processo de apuração.

Wang et al. (2018), em seu artigo *Large-scale Election Based On Blockchain*, propuseram a ideia de um sistema de contratos inteligentes, codificados sobre a plataforma de criptomoedas Ethereum. A proposta, conforme apresentada utilizaria Encriptação homomórfica e assinatura em anel, a fim de preservar a integridade e anonimato da votação na rede, o que implicaria na preservação da privacidade no sistema; todas as fases, incluindo o registro do eleitor e a apuração dos votos seriam completamente anônimos, o que inviabilizaria um processo de auditoria externa.

Srivastava, Dhar Dwivedi e Singh (2018) apresentaram artigo descrevendo um protocolo de votação usando uma das formas de blockchain, desenvolvido com base numa tecnologia derivada deste, que permite a formação de grafos acíclicos, enfatizando a privacidade.

As ideias quanto as implementações dos sistemas de votação são diversas, especialmente quando tomamos analogias aos maiores sistemas de uso de registros distribuídos, que são as criptomoedas.

A ideia mais comum é a de gerar “carteiras” onde cada usuário (eleitor) recebe uma “moeda” e pode “gastá-la” em um voto, como descrito por Kshetri e Voas (2018a). Os autores classificam esse ramo de estudo de *Blockchain Enabled Voting*, ou BEV, que possui as aplicações e modelos já levantados anteriormente, entretanto enfocando a tecnologia para diversos tipos de votações, inclusive as que não envolvam cargos eletivos, como plebiscitos e consultas públicas. Uma vantagem, no entanto, enfatizada pelos autores, está na dificuldade ou impossibilidade de criar votos falsos, ou fraudes no próprio registro de votação, o que parece ser um tema comum em todos os trabalhos até aqui descritos. Da mesma forma se posicionam Agbesi e Asante (2019), que apresentaram em Copenhagen um protocolo bastante detalhado de votação, também baseado na ideia da criação de carteiras e distribuição de moedas previamente a votação.

Temores de fraudes costumam ser ideias centrais da literatura do tema, como mencionado por Zhang, Wang e Xiong (2020). Um dos principais propósitos de siste-

mas com registro distribuído de votos seria dificultar ao máximo o uso de mecanismos fraudulentos de votação e registro, quer pela exploração de falhas nos *software* ou pelo uso de mecanismos sociais. Uma das ideia ventiladas seria a concessão de "recompensas"para bons eleitores e registradores de votos, bem como penalidades para os suspeitos de fraudes. Do mesmo modo se pronunciam Zhou et al. (2020), numa análise preliminar sobre os principais mecanismos de privacidade nos sistemas de votação eletrônica disponíveis, a saber: assinaturas cegas, em anel ou por delegação.

Li et al. (2020) propuseram a combinação das tecnologias aqui descritas com a Internet das Coisas, permitindo sistemas de contagem automática de votação, com *software* executando em maquinário de baixo custo, tornando a captura e processamento de votos amplamente acessível e uma votação de grande porte barata; tal posição foi compartilhada em proposta de Krishnamurthy, Rathee e Jaglan (2020), que também detalharam diversos mecanismos de segurança associados a mecanismos de votação e contagem.

A performance de sistemas blockchain para votação também foi abordado em trabalhos anteriores. Os tempos de entrada e apuração podem ser fatores preponderantes, entretanto quando ajustados apropriadamente podem propiciar velocidade suficiente para que seu uso possa ser levado em consideração para grandes projetos de BEV (KHAN; ARSHAD; KHAN, 2020).

Conforme se conclui, a utilização de BEV foi bastante escrutinada nos últimos anos, em vários aspectos e sob diversos prismas. A concordância das diversas publicações do uso de blockchain para *e-Gov* e, especialmente para votação, parece estar se formando. Sistemas informatizados inovadores, baseados em *hardware* de baixo custo e *software* alicerçado em tecnologias emergentes podem ser capazes de produzir sistemas de votação com publicidade e confidencialidade, termos aparentemente antagônicos, mas necessários a um sistema que atenda a proposta deste trabalho. A combinação dos elementos apresentados podem apresentar respostas a questionamentos históricos da votação eletrônica, como a possibilidade de auditoria e manutenção da privacidade dos votantes, tornando o registro distribuído uma alternativa aparentemente viável e eficaz.

7 Metodologia

O método escolhido para atingimento dos objetivos aqui descritos é a experimentação, através da implementação de uma prova de conceito baseado no modelo proposto e a realização de votações simuladas, utilizando-se esse *software*, procedendo a coleta do produto da execução para apuração e análise utilizando-se uma abordagem qualitativa. Este trabalho abordará sistemicamente o processo de produção e testes, registrando estes processos e seus resultados.

A solução será implementada para execução em hardware genérico, com a configuração composta especificamente de uma placa SBC (*Single Board Computer*, ou computador de placa única) Raspberry Pi, telas sensíveis ao toque com câmera embutida. Além da plataforma será desenvolvido um aplicativo, para o sistema operacional Android, que permitirá a gestão das identificações dos usuários, através de pares de chaves ECDSA, além de permitir a comunicação com o hardware através de *QR Codes*. Os produtos das votações serão colhidos em memória *flash* (pendrives ou cartões de memória) e analisados através de *software* automatizado. Eles também terão seus resultados armazenados de forma pública, para inspeção pelos interessados. Por fim o resultado será processado através de uma rede distribuída P2P.

O *software* de coleta e dos nós da rede distribuída serão criados desenvolvidos em Python, o *app* será desenvolvido em Dart.

Considerando os aspectos subjetivos levantados neste trabalho, referentes a conceitos como confiabilidade, privacidade, etc., nos parece haver a necessidade de uma posição interpretativa quanto ao conjunto de ações essenciais a conclusão das ações descritas nos objetivos, bem como a análise de seus resultados. A partir daí será necessário explorar as possibilidades de utilização do modelo descrito acima, através de experimentação.

De forma resumida:

- Abordagem: qualitativa;
- Posição epistemológica: interpretativa;
- Método de pesquisa: experimental;
- Finalidade: exploratória;
- Técnica de coleta: observação direta; e
- Técnica de análise: análise de conteúdo.

8 Proposta de trabalho

Blockchain se tornou um assunto recorrente nos últimos anos. O assunto tem se tornado relevante, tanto pela adoção massiva em criptomoedas, como pelo recente interesse do sistema financeiro tradicional. Em movimento inédito a China tem testado uma versão digital do Yuan (CARVALHO, 2020). O interesse chegou também ao Brasil e o Banco Central tem ventilado a possibilidade de um Real Digital, baseado em DLT (TECMUNDO, 2021).

As tendências de agregar a tecnologia aos sistemas de votação existente também tem ganhado momento. Trabalhos como Patidar e Jain (2019), Mpekoa e Greunen (2017), Ahmed et al. (2020), Bistarelli et al. (2019) e Yi (2019) tem demonstrado a tendência da comunidade acadêmica quanto ao uso das tecnologias aqui discutidas. O interesse também foi despertado o interesse do TSE (GUSSON, 2020).

A proposta deste trabalho, a fim de testar hipótese apresentada, seria o desenvolvimento de provas de conceito, com base em um protocolo desenhado para comunicação entre nós e testes públicos, entretanto a abordagem foi dificultada pela pandemia mundial de COVID-19. Assim sendo, a fim de dar prosseguimento a testagem da hipótese, dois aplicativos, detalhados adiante, foram desenvolvidos e testados, a fim de aferir a hipótese deste trabalho.

9 Resultados

Considerando a bibliografia explorada, foram detectadas tendências nas pesquisas atuais. Os modelos mais comuns de estruturas utilizadas pelos pesquisadores mundo afora incluíam, principalmentel *apps* para coleta e processamento dos dados da votação.

A partir da proposta de trabalho foram desenvolvidos dois aplicativos, RDVE Wallet e RDVE Coleta.

9.1 Estrutura básica do projeto

É preciso, antes de detalhar de forma mais aprofundada os resultados do desenvolvimento, explicar alguns conceitos básicos utilizados em tecnologias de registro distribuído.

9.1.1 Chaves assimétricas

São pares de chaves utilizados para identificar os usuários em transações computacionais. O par de chaves é composto por uma chave privada, que é capaz de produzir uma assinatura única e identificável, vinculada ao usuário que a gerou. A validação é feita através da utilização de uma chave pública, que é disponibilizada publicamente. Cada par de chaves é único e são vinculados um ao outro de forma que dados assinados por uma chave privada só podem ser validados por sua respectiva chave pública.

9.1.2 Endereço

O endereço é uma particularidade de sistemas *blockchain*. Trata-se de uma versão reduzida da chave pública do usuário, processada por diversos algoritmos criptográficos de assinatura.

No caso especifico do sistema RDVE a chave pública passa pelos seguintes algoritmos, nesta ordem:

- SHA256
- SHA256
- RIPEMD-160

- a representação hexadecimal do sumário RIPEMD-160 recebe o prefixo 'x00'
- Os quatro últimos dígitos do sumário SHA256 do item anterior é anexado ao final da *string* formada pelo sumário RIPEMD-160 e o prefixo 'x00'
- o resultado da ultima transformação é representado como uma numero Base 58.

Em protocolos como o Bitcoin a chave pública não é divulgada fora das *wallets*, em decorrência da possibilidade de, no futuro, a utilização do Algoritmo de Shor permita a obtenção da chave privada a partir da chave pública (MAVROEIDIS et al., 2018).

Ainda que um computador quântico com *Qubits* suficientes para o processamento de um algoritmo de fatoramento de grandes números ainda não esteja no horizonte, a solução utilizada no Bitcoin pode implicar na resistência a tal brecha no futuro e foi adotada neste trabalho.

9.1.3 UTXO (Unspent Transactions Output)

O Saldo de Transações Não-Gasto (UTXO) é uma lista, composta por todos os endereços registrados na rede, seu saldo atual e uma lista interna contendo todas as transações em que aquele endereço foi parte, seja de entrada ou saída. A lista é produzida a partir do processamento das transações existentes nos blocos, permitindo uma leitura mais simples dos saldos, sem a necessidade de procurar cada uma das transações nos blocos.

9.1.4 Assinatura por delegação

Assim como as chaves, o endereço identifica os usuários em uma rede *blockchain*, mas, no caso especifico deste trabalho, também identifica as urnas, permitindo que os eleitores transfiram seus saldos de votos para elas, permitindo que as urnas assinem as cédulas virtuais de votação no momento da coleta dos votos.

9.1.5 Bloco Registros

Os blocos registros são blocos que contém as transações de criação de endereço, funcionando de forma similar a um banco de dados contendo endereços de todos os participantes da rede, incluindo ID dos eleitores, mesários e urnas (gerados a partir do algoritmo UUID4), nomes dos eleitores, apelidos e números dos candidatos.

9.1.6 Cédula

É a abstração de uma cédula em papel, contendo campos específicos para assinatura (produzida pela urna) e o endereço de destino, referente ao candidato votado.

9.1.7 Requisição de votação

É a transação pela qual o eleitor transfere para urna seu saldo no sistema, permitindo que a mesma requeira uma cédula para que o eleitor registre seu voto. A requisição de votação também funciona como prova de comparecimento do usuário.

9.1.8 Bloco Produtos de Votação

É o resultado da votação, produzido pelas urnas e contém as transações de transferências dos saldos dos eleitores para as urnas (uma unidade por vez) e das urnas para os candidatos, conforme votação.

9.2 RDVE Wallet

O primeiro aplicativo, desenvolvido em linguagem *Dart* utilizando-se o *framework Flutter* foi o *Wallet* RDVE Wallet[1], que permite a identificação do usuário no sistema.

O aplicativo possui um módulo principal, capaz de gerar e gerenciar chaves criptográficas que identificam o usuário.

[1] Código fonte disponível em <https://github.com/rammyres/rdve_wallet>

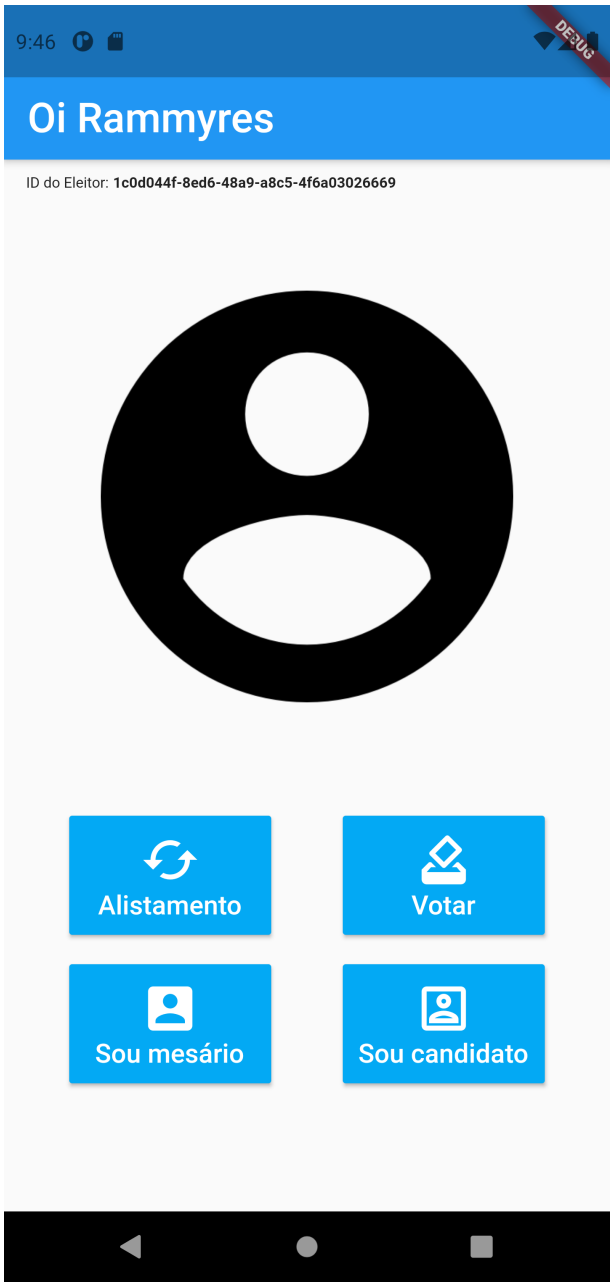

Figura 1 – Módulo principal do RDVE Wallet

A ID do eleitor identifica o mesmo dentro de todo o sistema, inclusive quado o mesmo se candidatar a cargo eletivo. Uma vez registrado no sistema o usuário pode requerer seu alistamento como eleitor, utilizado o módulo alistamento.

Figura 2 – Módulo de alistamento

De forma similar, existem módulos para registro como operador de urna (mesário) e candidatura. No primeiro caso não há geração de novas chaves criptográficas.

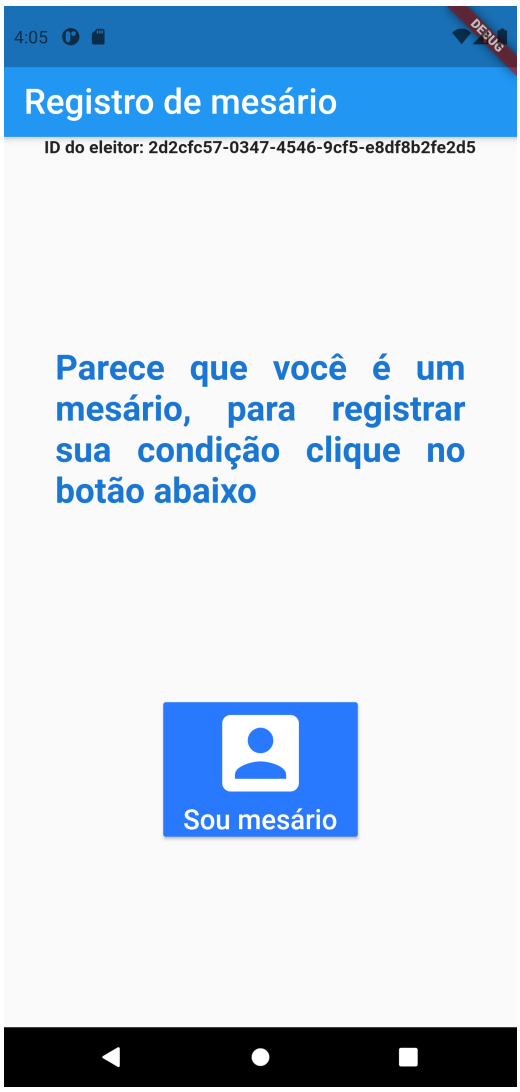

Figura 3 – Módulo de registro do operador de urna

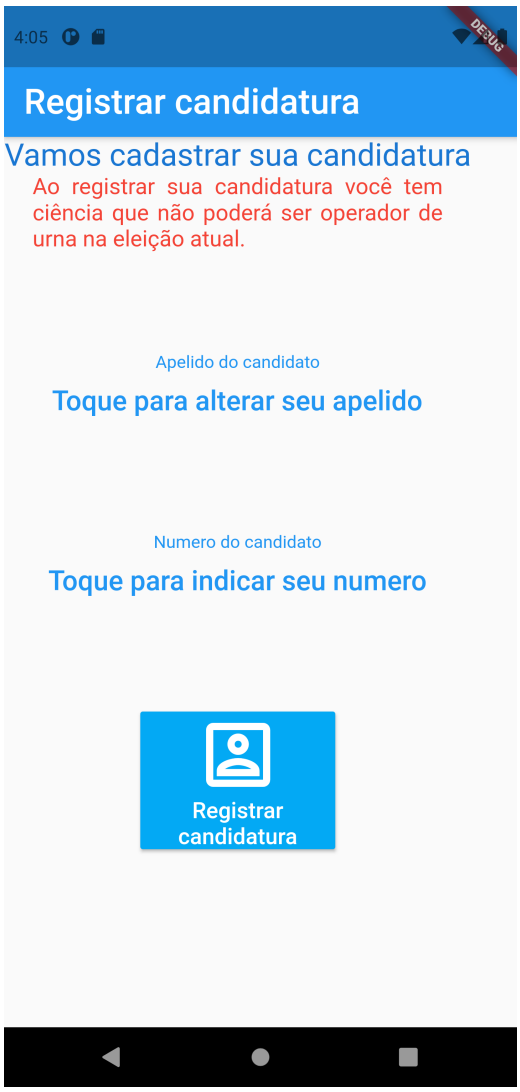

Figura 4 – Módulo de registro de candidatura

A comunicação com o sistema de coleta utiliza o mesmo princípio, gerando QR Codes contendo os dados necessários ao cadastramento de operadores e candidatos.

Por fim o módulo de operação de urna permite que o mesário libere o alistamento eleitoral, o registro de candidatura e o voto.

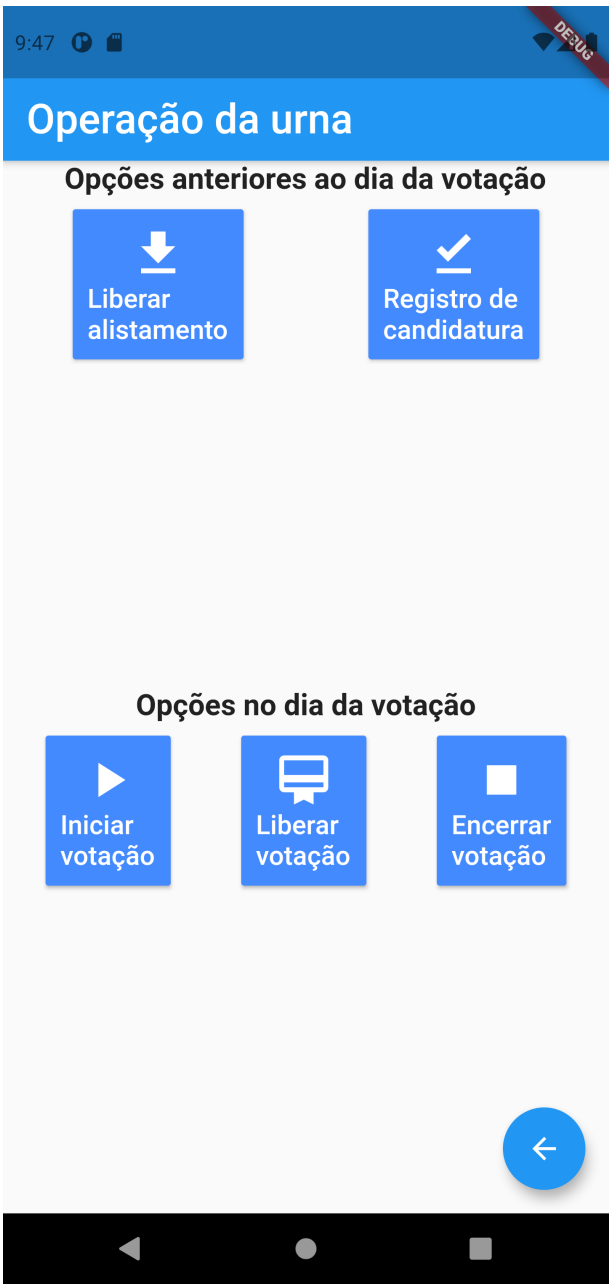

Figura 5 – Módulo de operação das urnas

9.3 RDVE Coleta

O RDVE Coleta[2] foi projetado em Python como um amalgama de dois projetos separados, o RDVE Coleta em si e o RDVE Urna.

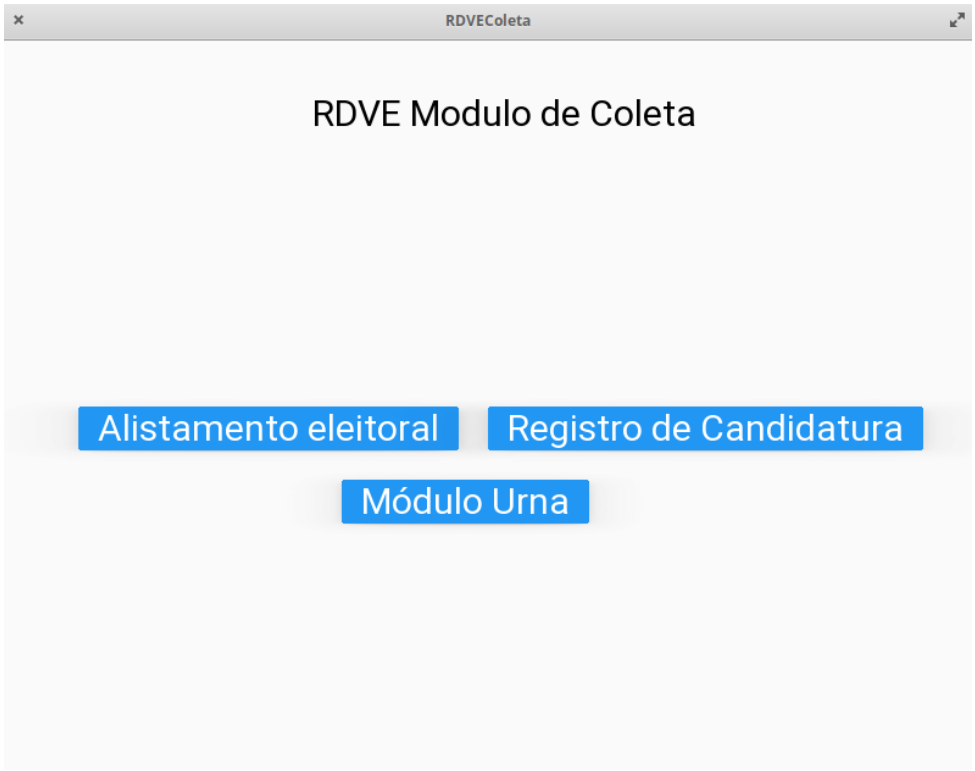

Figura 6 – Sistema RDVE Coleta

O RDVE Coleta registra eleitores e candidatos, bem como as requisições de votação, cédulas e os produtos de votação. Cada voto registrado na urna é procedido por uma aleatorização da lista de cédulas e somente ao final os votos, novamente embaralhados, tem seus hashes incluídos na Árvore de Merkle, impedindo que se possa recuperar a ordem de votação por meios indiretos.

9.4 Resultados Obtidos

A partir da execução dos aplicativos descritos foi possível realizar votações simuladas sem participações de terceiros, em decorrência da pandemia mundial de COVID-19.

Os registros representaram os dados inseridos e, em decorrência da forma de representação, mantiveram-se fidedignos e foi possível recuperar os estados registrados através da persistência dos objetos descritos acima como texto em formato JSON. Os arquivos de registro e produtos de votação compreendiam blocos íntegros e todos

[2] Código fonte disponível em <https://github.com/rammyres/rdve_coleta>

os seus registros tinham entradas em sua Árvores de Merkle que podiam ter provas efetivamente produzíveis.

Nas simulações não foi possível recuperar a ordem da votação ou cruzar o voto com o eleitor que o produziu. Em inspeção manual também foi possível verificar que o UTXO tinha saldos compatíveis com as transações existentes nos blocos de produtos de votação.

10 Discussão

Levando em conta a tendência nas pesquisas mundiais e os resultados dos testes deste trabalho, a possibilidade de utilização de *blockchain* para a construção de sistemas de votação, dotados de confidencialidade, confiabilidade e auditabilidade, parece viável.

Todos os dados produzidos nos aplicativos aqui descritos são persistidos como arquivos ou dados JSON, meio legível não só para computadores, mas facilmente acessíveis para humanos, o que permite um elevado grau de auditabilidade. O padrão é aberto e tem suporte em virtualmente todas as linguagens modernas, incluindo as duas principais adotadas neste trabalho, Dart e Python, o que permitiria o desenvolvimento de ferramentas para auditar grandes volumes de dados. Os votos, especificamente, também são embaralhados o suficiente para impedir a recuperação da ordem de entrada na urna. Por fim, considerando princípios gerais da criptografia, como a impossibilidade de reversão e negação da origem, pelo uso de assinaturas criptográficas na assinatura do alistamento de eleitores, registro de candidatos, requisições de votação, cédulas, registros e produtos de votação, permitem o rastreio completo de todo o processo de votação, inspirando grande grau e confiabilidade.

Muito embora ainda esteja em fases iniciais e maiores pesquisas se mostrem necessárias, inclusive com envolvimento de mais partes e ampliação dos sistemas para abranger modelos mais complexos de votação, como votações para cargos múltiplos, nos parece que o refinamento do projeto RDVE, como um todo, demonstra viabilidade.

11 Conclusão

Muito se tem discutido sobre DLT e, mais recentemente, BEV. A tecnologia empolga e traz consigo possibilidades grandes quanto ao futuro. As características inerentes a tecnologia trazem consigo grandes oportunidades e grandes desafios, entretanto a evolução tem sido significativa nos doze anos desde que o artigo de Nakamoto (2008) foi publicado.

O presente trabalho foi baseado em diversos trabalhos recentes sobre a tecnologia e suas implicações no sistema eleitoral e outros ramos do e-Government.

Com todas as considerações feitas, como a necessidade de mais pesquisas e ampliação dos mecanismos para testes, conforme expressado no capitulo anterior, nos parece que a proposta do projeto RDVE demonstrou ser capaz de produzir uma solução que atende aos requisitos da hipótese e viável para uso prático no mundo real, dado o amadurecimento necessário das ferramentas desenvolvidas.

Referências

ABUIDRIS, Y.; KUMAR, R.; WENYONG, W. A Survey of Blockchain Based on E-voting Systems. In: **Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications**. New York, NY, USA: ACM, 2019. p. 99–104. ISBN 9781450377430. Disponível em: <https://dl.acm.org/doi/10.1145/3376044.3376060>. Citado na página 23.

AGBESI, S.; ASANTE, G. Electronic Voting Recording System Based on Blockchain Technology. **2019 12th CMI Conference on Cybersecurity and Privacy, CMI 2019**, 2019. Citado na página 24.

AHMED, M. R. et al. The future of electronic voting system using blockchain. **International Journal of Scientific and Technology Research**, International Journal of Scientific and Technology Research, v. 9, n. 2, p. 4131–4134, feb 2020. ISSN 22778616. Citado na página 29.

ARANHA, D. F. et al. **Execução de código arbitrário na urna eletrônica brasileira**. Natal, 2018. 57–70 p. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/4243>. Citado 2 vezes nas páginas 11 e 15.

ARANHA, D. F. et al. (In)segurança do voto eletrônico no Brasil. **Cadernos Adenauer 1/2014: Justiça Eleitoral**, Fundação Konrad Adenauer, p. 117–133, 2014. Disponível em: <http://www.kas.de/wf/doc/13775-1442-5-30.pdf>. Citado na página 15.

BACK, A. et al. Hashcash-a denial of service counter-measure. 2002. Citado na página 21.

BATTAGLINI, M.; MORTON, R.; PALFREY, T. Efficiency, Equity, and Timing of Voting Mechanisms. **American Political Science Review**, v. 101, n. 3, p. 409–424, aug 2007. ISSN 0003-0554. Disponível em: <https://www.cambridge.org/core/journals/american-political-science-review/article/efficiency-equity-and-timing-of-voting-mechanisms/72BF17BBF736854F4EE11CEDA8A11A86>. Citado na página 11.

BISTARELLI, S. et al. End-to-End Voting with Non-Permissioned and Permissioned Ledgers. **Journal of Grid Computing**, Springer Netherlands, 2019. ISSN 15729184. Citado na página 29.

BLACKWELL, C. W. **Evidence for Athenian Democracy**. 2003. Disponível em: <https://www.stoa.org/demos/article{_}evidence@page=1{&}greekEncoding=Unicode>. Citado na página 11.

BRANDS, S. Untraceable Off-line Cash in Wallet with Observers. In: **Advances in Cryptology — CRYPTO' 93**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993. p. 302–318. Disponível em: <http://link.springer.com/10.1007/3-540-48329-2_26>. Citado na página 21.

BRASIL, T. S. E. **Conheça a história da urna eletrônica brasileira, que completa 18 anos**. 2014. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2014/Junho/

conheca-a-historia-da-urna-eletronica-brasileira-que-completa-18-anos>. Citado 2 vezes nas páginas 11 e 23.

CAHILL, D. et al. I am a blockchain too: How does the market respond to companies' interest in blockchain? **Journal of Banking & Finance**, v. 113, p. 105740, apr 2020. ISSN 03784266. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0378426620300078>. Citado na página 21.

CARVALHO, C. **Mirando hegemonia do dólar, moeda digital da China começa a ser aceita em compras online - Gizmodo Brasil**. 2020. Disponível em: <https://gizmodo.uol.com.br/china-moeda-digital-compras-online-dolar/>. Citado na página 29.

CHOI, T.-M.; LUO, S. Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes. **Transportation Research Part E: Logistics and Transportation Review**, v. 131, p. 139–152, nov 2019. ISSN 13665545. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S1366554519311494>. Citado na página 21.

CURRAN, K. E-Voting on the Blockchain. **The Journal of the British Blockchain Association**, v. 1, n. 2, p. 1–6, dec 2018. ISSN 25163949. Disponível em: <https://jbba.scholasticahq.com/article/4451-e-voting-on-the-blockchain>. Citado na página 23.

ELISA, N. et al. A framework of blockchain-based secure and privacy-preserving E-government system. **Wireless Networks**, dec 2018. ISSN 1022-0038. Disponível em: <http://link.springer.com/10.1007/s11276-018-1883-0>. Citado na página 22.

FENG, Q. et al. A survey on privacy protection in blockchain system. **Journal of Network and Computer Applications**, v. 126, p. 45–58, jan 2019. ISSN 10848045. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S1084804518303485>. Citado na página 22.

GERVAIS, A. et al. On the security and performance of proof of work blockchains. In: **Proceedings of the 2016 ACM SIGSAC conference on computer and communications security**. [S.l.: s.n.], 2016. p. 3–16. Citado na página 21.

GRAAF, J. Van de. **O mito da urna: desvendando a (in)segurança da urna eletrônica**. 2017. Disponível em: <www.o-mito-da-urna.org>. Citado 2 vezes nas páginas 11 e 15.

GUSSON, C. **TSE testa eleições com blockchain pelo celular mas desafio é garantir que não ocorra compra de voto e segurança**. 2020. Disponível em: <https://cointelegraph.com.br/news/tse-tests-elections-with-blockchain-but-challenge-is-to-ensure-that-vote-buying-does-not-take-place> Citado na página 29.

JONES, D.; SIMONS, B. **Broken Ballots: Will your vote count?** 1. ed. [S.l.]: Stanford: Center For The Study Of Language And Information, 2012. 420 p. Citado na página 11.

KHAN, K. M.; ARSHAD, J.; KHAN, M. M. Investigating performance constraints for blockchain based secure e-voting system. **Future Generation Computer Systems**, v. 105, p. 13–26, apr 2020. ISSN 0167739X. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167739X19310805>. Citado na página 25.

KRISHNAMURTHY, R.; RATHEE, G.; JAGLAN, N. An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices. **Wireless Networks**, v. 26, n. 4, p. 2391–2402, may 2020. ISSN 1022-0038. Disponível em: <http://link.springer.com/10.1007/s11276-019-02112-5>. Citado na página 25.

KSHETRI, N.; VOAS, J. Blockchain-Enabled E-Voting. **IEEE Software**, v. 35, n. 4, p. 95–99, jul 2018. ISSN 0740-7459. Disponível em: <https://ieeexplore.ieee.org/document/8405627/>. Citado na página 24.

KSHETRI, N.; VOAS, J. Blockchain in Developing Countries. **IT Professional**, v. 20, n. 2, p. 11–14, mar 2018. ISSN 1520-9202. Disponível em: <https://ieeexplore.ieee.org/document/8338009/>. Citado na página 22.

LAMPORT, L.; SHOSTAK, R.; PEASE, M. The Byzantine Generals Problem. **ACM Transactions on Programming Languages and Systems (TOPLAS)**, v. 4, n. 3, p. 382–401, jul 1982. ISSN 0164-0925. Disponível em: <http://dl.acm.org/doi/10.1145/357172.357176>. Citado na página 21.

LI, Y. et al. A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. **IEEE Transactions on Dependable and Secure Computing**, p. 1–1, 2020. ISSN 1545-5971. Disponível em: <https://ieeexplore.ieee.org/document/9031381/>. Citado na página 25.

LIER, B. van. Can Cyber-Physical Systems Reliably Collaborate within a Blockchain? **Metaphilosophy**, v. 48, n. 5, p. 698–711, oct 2017. ISSN 00261068. Disponível em: <http://doi.wiley.com/10.1111/meta.12275>. Citado na página 22.

MA, Y. et al. A survey of blockchain technology on security, privacy, and trust in crowdsourcing services. **World Wide Web**, v. 23, n. 1, p. 393–419, jan 2020. ISSN 1386-145X. Disponível em: <http://link.springer.com/10.1007/s11280-019-00735-4>. Citado na página 21.

MAVROEIDIS, V. et al. The Impact of Quantum Computing on Present Cryptography. mar 2018. Disponível em: <http://arxiv.org/abs/1804.00200http://dx.doi.org/10.14569/IJACSA.2018.090354>. Citado na página 32.

MERKLE, R. C. A Digital Signature Based on a Conventional Encryption Function. In: . [s.n.], 1988. p. 369–378. Disponível em: <http://link.springer.com/10.1007/3-540-48184-2_32>. Citado na página 21.

MOURA, T.; GOMES, A. Blockchain Voting and its effects on Election Transparency and Voter Confidence. In: **Proceedings of the 18th Annual International Conference on Digital Government Research**. New York, NY, USA: ACM, 2017. p. 574–575. ISBN 9781450353175. Disponível em: <https://dl.acm.org/doi/10.1145/3085228.3085263>. Citado na página 23.

MPEKOA, N.; GREUNEN, D. van. E-voting experiences: A case of Namibia and Estonia. In: **2017 IST-Africa Week Conference (IST-Africa)**. IEEE, 2017. p. 1–8. Disponível em: <http://ieeexplore.ieee.org/document/8102303/>. Citado na página 29.

NAKAMOTO, S. **Bitcoin: a peer-to-peer electronic cash system**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Citado 3 vezes nas páginas 11, 21 e 43.

NEWMAN, T. Tasmania and the Secret Ballot. **Australian Journal of Politics and History**, v. 49, n. 1, p. 93–101, mar 2003. ISSN 0004-9522. Disponível em: <http://doi.wiley.com/10.1111/1467-8497.00283>. Citado na página 11.

NGUYEN, T. V. H. et al. Bitcoin return: Impacts from the introduction of new altcoins. **Research in International Business and Finance**, v. 48, p. 420–425, apr 2019. ISSN 02755319. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0275531918309553>. Citado na página 21.

ØLNES, S.; UBACHT, J.; JANSSEN, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. **Government Information Quarterly**, v. 34, n. 3, p. 355–364, sep 2017. ISSN 0740624X. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0740624X17303155>. Citado na página 22.

ONIK, M. M. H. et al. Privacy-aware blockchain for personal data sharing and tracking. **Open Computer Science**, v. 9, n. 1, p. 80–91, apr 2019. ISSN 2299-1093. Disponível em: <https://www.degruyter.com/view/journals/comp/9/1/article-p80.xml>. Citado na página 22.

PATIDAR, K.; JAIN, S. Decentralized E-Voting Portal Using Blockchain. In: **2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)**. IEEE, 2019. p. 1–4. ISBN 978-1-5386-5906-9. Disponível em: <https://ieeexplore.ieee.org/document/8944820/>. Citado na página 29.

PAYÃO, F. 92% dos brasileiros não confiam na urna eletrônica. **Tecmundo**, São Paulo, 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/133524-92-brasileiros-nao-confiam-urna-eletronica.htm>. Citado na página 11.

SRIVASTAVA, G.; Dhar Dwivedi, A.; SINGH, R. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. In: **Proceedings of the 15th International Joint Conference on e-Business and Telecommunications**. SCITEPRESS - Science and Technology Publications, 2018. p. 508–513. ISBN 978-989-758-319-3. Disponível em: <http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006881905080513>. Citado na página 24.

SUNYAEV, A. Distributed Ledger Technology. In: **Internet Computing**. Cham: Springer International Publishing, 2020. p. 265–299. Disponível em: <http://link.springer.com/10.1007/978-3-030-34957-8_9>. Citado na página 21.

TECMUNDO. **E-BRL: o real digital está chegando? - TecMundo**. 2021. Disponível em: <https://www.tecmundo.com.br/mercado/210178-brl-real-digital-chegando.htm>. Citado na página 29.

VOTE ARCHIVE. **U.S. Presidential Election, 1800**. 2015. Disponível em: <https://votearchive.com/us-pres-elect-1800/>. Citado na página 11.

VOTE ARCHIVE. **U.S. Presidential Election, 2016**. 2016. Disponível em: <https://votearchive.com/us-pres-elect-2016/>. Citado na página 11.

WANG, B. et al. Large-scale Election Based On Blockchain. **Procedia Computer Science**, v. 129, p. 234–237, 2018. ISSN 18770509. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S1877050918302874>. Citado na página 24.

WARKENTIN, M.; ORGERON, C. Using the security triad to assess blockchain technology in public sector applications. **International Journal of Information Management**, v. 52, p. 102090, jun 2020. ISSN 02684012. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S026840121930060X>. Citado na página 22.

WOOD, F. S. **ELECTRIC VOTING MACHINE**. 1898. Disponível em: <https://patents.google.com/patent/US616174>. Citado na página 11.

YAKOBSON, A. **Secret Ballot and Its Effects in the Late Roman Republic**. Franz Steiner Verlag, 1995. v. 123. 426–442 p. ISSN 00180777. Disponível em: <http://www.jstor.org/stable/4477105>. Citado na página 11.

YI, H. Securing e-voting based on blockchain in P2P network. **Eurasip Journal on Wireless Communications and Networking**, Springer International Publishing, v. 2019, n. 1, dec 2019. ISSN 16871499. Citado na página 29.

ZHANG, S.; WANG, L.; XIONG, H. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. **International Journal of Information Security**, v. 19, n. 3, p. 323–341, jun 2020. ISSN 1615-5262. Disponível em: <http://link.springer.com/10.1007/s10207-019-00465-8>. Citado na página 24.

ZHONG, S.; HUANG, X. Special focus on security and privacy in blockchain-based applications. **Science China Information Sciences**, v. 63, n. 3, p. 130100, mar 2020. ISSN 1674-733X. Disponível em: <http://link.springer.com/10.1007/s11432-020-2781-0>. Citado na página 22.

ZHOU, Y. et al. An improved FOO voting scheme using blockchain. **International Journal of Information Security**, v. 19, n. 3, p. 303–310, jun 2020. ISSN 1615-5262. Disponível em: <http://link.springer.com/10.1007/s10207-019-00457-8>. Citado na página 25.

Glossário

Árvore de Merkle é a estrutura de dados em forma de árvore binária, onde cada nó terminativo (folha) contém o *hash* de um bloco de dados e cada nó não-terminativo possui os *hashes* de seus dois nós filhos. O calculo da prova da existência de um dado na árvore tem complexidade $O(\log n)$.

BCS *Blockchain-based crowdsourced systems* são sistemas colaborativos, em que os dados recebidos são originados por um conjunto de usuários .

BEV *Blockchain Enabled Voting*, ou Votaçao Eletrônica Capacitada por Blockchain é o termo cunhado por Kshetri e Voas para designar os sistems de votação eletrônica construidos sobre essa tecnologia.

Comitia literalmente comícios, eram assembléias populares em que os magistrados romanos punham em votações propostas de leis e julgamentos, sem deliberação dos votantes e com aplicação a uma só classe, como o *Consilium plebis*, que criava leis que só se aplicavam aos plebeus .

Criptomoeda é um ativo digital, desenhado para funcionar como meio de troca, onde a propriedade desses ativos é registrada em um banco de dados distribuído, formado por diversos computadores em rede P2P, usando criptografia forte para controlar a posse, transferências e criação desses ativos, além de permitir verificar a posse dos mesmos .

DLT *Distributed Ledger Technology*, ou tecnologias de registro distribuído são tecnolgias derivadas da *blockchain* não utilizados por criptomoedas.

DoS É uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores, através da requisição constante do mesmo serviço repetidas vezes, em um curto espaço de tempo .

e-Gov ver e-Government .

e-Government Governo Eletrônico consiste no uso das tecnologias da informação — além do conhecimento nos processos internos de governo — e na entrega dos produtos e serviços do Estado para seus próprios entes (G2G), seus cidadãos (G2C) bem como à indústria (G2B) e no uso de ferramentas eletrônicas e tecnologias da informação para aproximar governo e cidadãos. .

ECDSA *Elliptic Curve Digital Signature Algorithm* ou algoritmo de assinatura digital em curva elíptica é um algoritmo de assinatura digital, que se baseia na estrutura algébrica dessas curvas em campos finitos, permitindo um melhor aproveitamento de sistemas caóticos .

Encriptação homomórfica diz-se dos métodos de encriptação que permitem que os dados cifrados por uma pessoa sejam usadas por uma segunda, sem que a última tenha conhecimento do conteúdo original .

Ethereum é um sistema *open source* de blockchain descentralizado, usado principalmente pela criptomoeda Eth, que contém a capacidade de criar e enforçar contratos inteligentes .

G2B ver e-Government .

G2C ver e-Government .

G2G ver e-Government .

Hash (ou soma) são mapeamentos de dados de tamanhos variáveis em dados de tamanho fixo, através de um algoritmo que transaciona os dados por diversos circuítos, físicos ou virtuais.

Internet das Coisas é um conjunto de dispositivos computacionais, eletrônicos (digitais e mecânicos), identificados em uma rede, que tem a capacidade de transferirem dados entre si, sem interferência humana .

JSON *JavaScript Object Notation*, ou notação de objetos JavaScript, formato de transmissão de dados e de arquivos formados por pares atributo-valor, que são humanamente legíveis.

P2P *Peer to peer* ou par a par, é uma rede descentralizada, onde os nós se comunicam entre si livremente, sem a necessidade de nós integradores ou servidores .

Proof of Work (prova de trabalho) é o protocolo utilizado para deter ataques de negação de serviço exigindo trabalho, na forma de tempo de processamento, de alguém que requisita um serviço .

Pólis era o centro admnistrativo e religioso das cidades gregas antigas .

QR Code *Quick Response Codes* referem-se a códigos bidimensionais, formados por uma matriz de quadrados de tamanhos variáveis, que podem ser facilmente lidos por maquinas equipadas com câmeras .

Qubit unidade básica da computação quântica, equivalente ao *bit* na computação binária tradicional.

Raspberry Pi é uma placa *Single Board Computer* desenvolvida no Reino Unido pela Raspberry Pi Foundation. .

Single Board Computer referem-se a placas únicas, contendo todos elementos como memória e processador integrados e consistem em um computador funciona .

Sistema ciber-físico é um sistema em que os mecanismos de atuação são controlados ou monitorados por algoritmos.

Wallet trata-se de um aplicativo que faz o gerenciamento de chaves criptográficas em sistemas *blockchain*.