XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

LITON LANES PILAU SOBRINHO

LUIZ ERNANI BONESSO DE ARAUJO

AIRES JOSE ROVER

FERNANDO GALINDO AYUDA

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires José Rover; Fernando Galindo Ayuda; Liton Lanes Pilau Sobrinho; Luiz Ernani Bonesso de Araujo.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-629-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Direito, Governança e Novas Tecnologias.

O presente Grupo de Trabalho, baseia-se na problemática dos impactos das novas tecnologias, a partir de sua regulação, interferências e impactos da Governança. O objetivo do mesmo é ampliar as discussões e reflexões acerca das pesquisas realizadas sobre a temática com a finalidade de buscar a difusão do conhecimento científico para a melhoria e para o benefício da sociedade atual. O paradoxo das novas tecnologias e seus impactos no sistema jurídico vislumbram uma necessidade de readequação e mostram-se preocupantes, pois nos últimos anos a velocidade e a quantidade de acontecimentos observados no mundo inteiro dão um tom dramático à sensibilidade e impactos das novas tecnologias nas relações de governança e regulação. O desenvolvimento tecnológico tem trazido grandes avanços e, em contrapartida, uma insegurança em relação aos limites impostos as relações do sistema jurídico e da governança. Vivencia-se uma crise paradoxal, principalmente pela incerteza dessas relações. Com todos os avanços e o desenvolvimento de novas tecnologias na área jurídica e de governança, se está diante de um paradoxo, ou seja, o Estado cada vez mais reduzindo o investimento em pesquisas e deixando para a iniciativa privada dominar o campo das novas tecnologias. Assim, resta a dúvida de qual é o papel do Estado, uma vez que, em assim sendo, a sociedade fica à mercê do mercado. Nesse sentido, faz-se necessário repensar a dinâmica dessas relações. Outrossim, os trabalhos apresentados neste GT tratam dessas reflexões necessárias para o amadurecimento e para a assimilação de seus impactos. Os organizadores agradecem a todos os colegas pesquisadores e autores que contribuíram com seus excelentes trabalhos, estes que compõem esta publicação. Sendo assim, constata-se que houve comprometimento na investigação das mais diversas temáticas aqui trabalhadas, o que permitirá ao leitor uma leitura acurada e esclarecedora dessa obra.

CONSIDERAÇÕES SOBRE A UTILIZAÇÃO DO BLOCKCHAIN NO SISTEMA DE VOTAÇÃO ELETRÔNICO

CONSIDERATIONS ON THE USE OF BLOCKCHAIN IN THE ELECTRONIC VOTING SYSTEM

Ana Luísa Teotônio Josafá Simão

Resumo

O presente artigo busca analisar de que forma a tecnologia blockchain poderia ser utilizada no sistema eletrônico de votação em vigor no Brasil a fim de prover maior segurança às eleições. Para isso, buscou-se estudar as principais características do sistema de votação eletrônico atual, passando pela evolução história do sistema de votação brasileiro, do voto impresso até a implementação das urnas eletrônicas. Ademais, foram analisados os mecanismos de integridade e auditabilidade do sistema atual, identificando as principias vulnerabilidades apontadas por profissionais da área de tecnologia da informação, bem como as vantagens em relação ao modelo anteriormente adotado. Em seguida, buscou-se apresentar, de forma sintética, como funciona a tecnologia blockchain e suas principais características. Por fim, questiona-se se a utilização do blockchain pode ser útil para aprimoramento do sistema de votação eletrônico, delineando-se os desafios e oportunidades geradas pela utilização de blockchain no sistema de votação. Conclui-se que, embora a utilização da tecnologia blockchain possa oportunizar maior segurança às eleições, qualquer mudança no sistema de votação deve ser feita de forma gradual.

Palavras-chave: Blockchain, Urna eletrônica, Sistema de votação eletrônica, Auditabilidade, Democracia

Abstract/Resumen/Résumé

This article seeks to analyze how blockchain technology could be used in the electronic voting system in force in Brazil in order to provide greater security for elections. For this, we sought to study the main characteristics of the current electronic voting system, going through the historical evolution of the Brazilian voting system, from the printed vote to the implementation of electronic voting machines. Furthermore, the integrity and auditability mechanisms of the current system were analyzed, identifying the main vulnerabilities pointed out by professionals in the information technology area, as well as the advantages in relation to the model previously adopted. Then, we sought to present, in a synthetic way, how blockchain technology works and its main characteristics. Finally, it is questioned whether the use of blockchain can be useful for improving the electronic voting system, outlining the challenges and opportunities generated by the use of blockchain in the voting system. It is concluded that, although the use of blockchain technology can provide greater security for elections, any change in the voting system must be done gradually.

Keywords/Palabras-claves/Mots-clés: Blockchain, Electronic ballot box, Electronic voting system, Auditability, Democracy

1 INTRODUÇÃO

Recentemente, muito tem se debatido acerca da audibilidade do voto e integridade das eleições, culminando na discussão acerca da necessidade voto impresso. Embora a discussão tenha retornado com maior força na conjuntura política atual, o Supremo Tribunal Federal (STF), ao apreciar a o artigo 59-A da Lei das Eleições (Lei nº 9.504/1997), incluído pela Lei nº 13.165/2015, no bojo da Ação Direta de Inconstitucionalidade (ADI) nº 5889, declarou inconstitucional a impressão do voto eletrônico, por colocar em risco o sigilo e a liberdade do voto. Na ocasião do deferimento da medida cautelar, o relator, Ministro Gilmar Mendes, destacou que a lei impôs uma modificação substancial no sistema de votação, sem, contudo, oferecer meios para a execução da medida, de forma que que a implantação deveria ser gradual e ser feita conforme a disponibilidade de recursos e as possibilidades do Tribunal Superior Eleitoral (TSE). Por sua vez, no julgar o mérito, o Relator incorporou como razões de decidir os fundamentos do voto do Ministro Alexandre de Moares (BRASIL, 2021a, p.24-25):

> Não é possível fazer uma mudança tão abrupta no processo eleitoral, colocando em risco a segurança das eleições e gastando recursos de forma irresponsável. A implantação da impressão do registro do voto precisa ser gradual.
> (...)
> No entanto, a maioria entendeu pela inconstitucionalidade da norma, uma vez que violaria a liberdade e o sigilo do voto. Dessa forma, adoto como razões de decidir os fundamentos do voto do Ministro Alexandre de Moares:
>
> > "(...)Então, como eu disse, o sigilo deve ser garantido antes, durante e depois para se evitar exatamente eventuais programas eletrônicos de conferência retroativa. Ou seja, **a possibilidade, a meu ver, que traz o art. 59-A, principalmente seu parágrafo único, de identificação de quem votou, de quebra do sigilo, e, consequentemente, de diminuição da liberdade do voto, pois a pessoa poder se sentir ameaçada, seria, no modelo que o art. 59-A trouxe, um retrocesso aos avanços democráticos que o Brasil fez para se garantir realmente uma eleição livre, uma eleição em que as pessoas possam escolher aqueles que elas preferem.** E a urna eletrônica, como deveria realmente ter realizado, tomou cuidado de se permitir voto em branco, porque também é uma opção o voto em branco; há possibilidade, não há o botãozinho, mas há possibilidade do voto nulo, que também é uma opção, ou seja, não há nada aqui que distancie o exercício da soberania popular, o exercício da cidadania no voto eletrônico. (…)
> > Aqui, volto a dizer, o art. 59-A, especialmente seu parágrafo único, na opção – e legitimamente o legislador tem o direito constitucional de optar como será o voto – híbrida, fere o sigilo do voto, a liberdade do voto, porque tem uma alta potencialidade de identificação do eleitor. Essas duas características são constitucionais, previstas tanto no art. 14 quanto no art. 60, §4º: a liberdade do voto e o voto sigiloso.
> > Dessa forma, resumindo e indo para o final, não se trata da questão de custos. O legislador pode fazer uma opção legítima; que se volte o voto no papel; por um modelo híbrido que não tenha essa potencialidade lesiva à liberdade do voto, ao sigilo do voto, essa também seria uma opção do próprio legislador. **Aqui, não é uma questão de economicidade, de maior celeridade, ou não, na votação, se vai atrasar ou não, mas uma questão de cunho eminentemente constitucional. O art. 59-A, caput, e seu parágrafo único atentam contra duas das principais características do voto: o voto sigiloso e o voto livre.** (...)" (grifos nossos)

Essa não foi a primeira tentativa de implementar o voto impresso como documento de auditoria em papel conferível pelo eleitor (*voter verifiable paper audit trail*): em 2013 o Supremo Tribunal Federal julgou inconstitucional o art. 5º da Lei nº 12.034/2009 pelas mesmas razões, ao apreciar a Ação Direta de Inconstitucionalidade (ADI) nº 4.543/DF.

Mais recentemente, o voto impresso voltou a ser discutido em razão da consulta pública acerca da Sugestão nº 9/2018 ("Voto Impresso em 100% das urnas"), que já contou com a participação de mais de dois milhões de pessoas até 12/07/2021, segundo consta no portal e-Cidadania do Senado Federal. O voto impresso também foi assunto na Câmara dos Deputados em razão da propositura da Proposta de Emenda Constitucional (PEC) nº 135/2019, que tornava obrigatória a impressão de cédulas físicas, conferíveis pelo eleitor na votação e apuração de eleições, plebiscitos e referendos, rejeitada pela Câmara dos Deputados em 10/08/2021 por 218 deputados, não alcançando o quórum necessário de 308 votos favoráveis.

O sistema de voto com urnas eletrônicas tal como ocorre no Brasil é o maior do mundo, não existindo qualquer país com número de habitantes maior ou semelhante que possua uma eleição cuja execução e apuração ocorram de forma tão célere como em nosso país. Em que pese não se ignore que a discussão acerca da integridade das eleições e auditabilidade do voto não seja necessariamente movida por uma demanda genuína de transparência, podendo existir interesses escusos na movimentação realizada por partidos políticos e segmentos sociais em torno do voto impresso; considerando o contexto atual, questiona-se se utilização da tecnologia *blockchain* poderia contribuir para garantir maior segurança às eleições, suprimindo, assim, a demanda de auditabilidade que surge nas discussões relativas à voto impresso. Isto é, e se as discussões acerca da necessidade de maior transparência e audibilidade das urnas eletrônicas ensejassem aperfeiçoamento do sistema eletrônico de votação, fazendo uso de novas tecnologias, tal como *blockchain*, e deixassem de ser pautadas pelo retorno do voto impresso que, no Brasil, já foi alvo de diversas fraudes ao longo da história? Importante ressaltar que a inovação é um dos princípios seguidos pelo Tribunal Superior Eleitoral no que concerne ao sistema de votação, havendo já, inclusive, inciativas nesse sentido, como veremos no curso deste artigo.

Há que se destacar que a utilização do voto impresso para que o eleitor faça a conferência visual do voto acarretaria gastos na ordem de R$ 2,5 bilhões.(JORNAL DO COMÉRCIO, 2021) Nunca é demais lembrar que a experiência mal sucedia em 2002 (em que 7.128.233 eleitores de 150 municípios espalhados por todo país, tiveram seu voto impresso): houve aumento do tamanho das filas, número significativo de eleitores que saíram da cabine

eleitoral sem confirmar o voto impresso e inúmeras falhas verificada no módulo impressor da urna. (TSE, 2021a)

A seguir, trataremos do sistema de voto atual, abordando as conquistas e desafios atuais; posteriormente, discorreremos acerca do funcionamento da tecnologia *blockchain*, considerando as possibilidades de aplicações jurídica; para, ao fim, refletirmos quanto à utilização do *blockchain* no sistema de votação no Brasil.

2. SISTEMA DE VOTAÇÃO ELETRÔNICA

Conforme parágrafo único do art. 1º da Constituição da República, "[t]odo poder emana do povo, que o exerce por meio de representantes eleitos ou indiretamente (...)." Quanto ao voto, o caput do art. 14, dispõe que "[a] soberania popular será exercida pelo sufrágio universal e pelo voto direto e secreto, com valor igual para todos (...)".

O sigilo do voto e sua inviolabilidade também são evidenciados na legislação infraconstitucional. A Lei nº 9.504/97, em seu art. 61, prevê que "[a] urna eletrônica contabilizará cada voto, assegurando-lhe o sigilo e inviolabilidade, garantida aos partidos políticos, coligações e candidatos ampla fiscalização." (BRASIL, 2021b)

Destaca-se também o art. 59 da Lei nº 9.504/97, que estipula que a votação e totalização dos votos ocorrerá de forma eletrônica — salvo situações de caráter excepcionais autorizadas pelo TSE em que será permitida a utilização de cédulas em papel —; informações que devem constar no painel da urna eletrônica; ordem de votação, recursos que permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor; além da assinatura digital do arquivo de votos, a fim de impedir a substituição de votos. Em complemento, o art. 66 da Lei nº 9.504/97 estabelece mecanismos de fiscalização e auditoria de todas as fases do processo de votação, apuração das eleições e do processamento eletrônico da totalização dos resultados. Relevante, ainda, o art. 67 que prevê que "[o]s órgãos encarregados do processamento eletrônico de dados são obrigados a fornecer aos partidos ou coligações, no momento da entrega ao juiz encarregado, cópias dos dados do processamento parcial de cada dia, contidos em meio magnético". (BRASIL, 2021b)

Passemos a seguir, a um breve resumo do contexto de criação da urna eletrônica.

2.1. A CRIAÇÃO DA URNA ELETRÔNICA

As urnas eletrônicas foram concebidas a partir dos trabalhos executados pela comissão de notáveis criada pelo TSE em 1995 e constituída por juristas, cientistas políticos e especialistas em tecnologia da informação. As comissões de notáveis eram divididas entre

cinco subcomissões temáticas, quais sejam, Código Eleitoral e Organização da Justiça Eleitoral, presidida pelo Ministro Marco Aurélio; Partidos Políticos, presidida pelo Ministro Diniz de Andrada; Sistema Eleitoral ou de Voto, presidida pelo Ministro Torquato Jardim; Financiamento de Campanhas, presidida pelo Ministro Pádua Ribeiro; Informatização do voto, presidida pelo Ministro Ilmar Galvão.

Após a conclusão do trabalho realizado pelas subcomissões temáticas, foi criado o grupo de trabalho a partir do relatório expedido pela subcomissão de informatização do voto, com o objetivo de criar o protótipo de uma urna eletrônica, realizar testes e fiscalizar o procedimento licitatório para a aquisição das urnas eletrônicas. Assim, finalmente, as urnas eletrônicas foram utilizadas pela primeira vez nas eleições municipais de 1996.

A opção pela informatização do voto se deu em razão das diversas fraudes que que caracterizavam o processo eleitoral. A urna eletrônica é fruto de um longo processo histórico que começou com a criação da Justiça Eleitoral, passando pela instituição da cédula única, pela criação da folha individual de votação, pela construção do cadastro eletrônico e pelo processamento eletrônico do resultado eletrônico das eleições. A utilização da urna eletrônica foi importante para a superação de mazelas que contaminavam as eleições, tais como o mapismo, o aproveitamento de votos em branco e a falsificação de cédulas. Nesse sentido, Carlos Mário da Silva Velloso, ex-ministro e ex-presidente do STF e do TSE, assevera que:

> E porque o voto informatizado tornara-se o nosso ideal maior? É que, nas apurações manuais com as cédulas de papel, campeava o mapismo, fraude abominável que elegia e deselegia candidatos. Acabávamos de tomar conhecimento de extensa fraude eleitoral nas eleições de 1994, no Rio de Janeiro. Parte delas chegou a ser anulada. Se isso ocorria no Rio de Janeiro, tambor do Brasil -- o que lá ocorre repercute no Brasil inteiro -- o que não estaria ocorrendo em outros Estados? Era preciso, portanto, afastar a mão humana das apurações, tema de conversas intermináveis entre o ministro Sepúlveda Pertence, então presidente do TSE, alguns juízes e eu. E ele dizia: - caberá a você, que me sucederá na presidência, informatizar o voto, única forma de acabar com a praga do mapismo e mazelas outras. (VELLOSO, 2015, p. 13-14)

A implementação da urna eletrônica foi gradual: nas eleições de 1996, foi informatizado um terço dos votos de um eleitorado de cerca de 101 milhões de eleitores; nas eleições de 1998, mais um terço dos eleitores; por fim, nas eleições de 2000, foram informatizados todos os votos, totalizando 109 milhões de eleitores.

2.2 INTEGRIDADE E AUDIBILIDADE DAS URNAS ELETRÔNICAS

Incialmente, cabe destacar que a urna eletrônica não é conectada à internet ou a qualquer tipo de rede, de forma que o *software* da urna não pode ser alterado remotamente. Os softwares são elaborados por servidores do Tribunal Superior Eleitoral, sob a fiscalização de partidos políticos e das coligações, da Ordem dos Advogados do Brasil, do Ministério Público,

da Polícia Federal, do Congresso Nacional, do Supremo Tribunal Federal, da Controladoria-Geral da União, da Sociedade Brasileira de Computação, do Conselho Federal de Engenharia e Agronomia, do Conselho Nacional de Justiça, do Conselho Nacional do Ministério Público, Tribunal de Contas da União, das Forças Armadas e de entidades privadas brasileiras, sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao Tribunal Superior Eleitoral e Departamentos de tecnologia da informação de universidades credenciadas junto ao Tribunal Superior Eleitoral (estas duas últimas deverão manifestar seu interesse por meio de ofício dirigido à Presidência do Tribunal Superior Eleitoral a partir de 7 (sete) meses antes do primeiro turno das eleições), que terão acesso ao código-fonte seis meses antes do início das eleições. (TSE, 2021b)

Os softwares contam como mais de trinta camadas de segurança a fim de protegerem o sistema de tentativa de invasão. Há ainda o log da urna, responsável por registrar as operações realizadas na urna, tais como horário em que a urna foi ligada, horário em que os eleitores são habilitados, horário em que a urna foi desligada, emissão de relatórios, aplicativos executados, ajustes de data e hora, procedimentos de contingência. (TRE, 2021a)

Desde 2009, são realizados testes públicos de segurança, nos quais as urnas são submetidas, durante uma semana, a ataques de convidados técnicos de computação, investigadores e hackers, para investigação de problemas ou fragilidades no hardware e software da urna eletrônica que, uma vez identificadas, serão resolvidas anteriormente à realização das eleições. Após a finalização do processo de elaboração, os softwares são assinados digitalmente e lacrados pelo TSE, Ministério Público, representantes de partidos políticos e da OAB.

No dia da eleição, far-se-á a *auditoria de verificação de autenticidade e integridade do sistema eleitoral* antes do início do pleito. Nesta modalidade de auditoria, partidos políticos, representantes da OAB e do Ministério Público e cidadãos interessados poderão verificar se as assinaturas digitais dos softwares instalados nas urnas eletrônicas coincidem com as assinaturas digitais dos softwares lacrados pelo TSE, em um número determinado de seções eleitorais do estado sorteadas na véspera da eleição, em audiência pública realizada no TRE. Em seguida, cada urna sorteada emitirá um relatório de resumos digitais dos arquivos nela instalados, os quais poderão ser conferidos com a lista publicada no *site* do TSE. (TRE, 2021a)

Os votos de cada um dos eleitores são armazenados em um arquivo denominado Registro Digital do Voto (RDV) de forma aleatória, não permitindo qualquer tipo de associação entre votos e os eleitores, com vistas a garantir o sigilo do voto. A partir dele, são emitidos o a Zerésima e o Boletim de Urna.

No dia da eleição, cabe ao presidente da mesa receptora de votos, realizar a impressão da Zerésima, a fim de demonstrar que não há votos na urna antes do início oficial da votação. Por sua vez, o Boletim da Urna é o relatório final que registra (i) a data da eleição; (ii) a identificação do município, da zona eleitoral e da seção; (iii) a data e o horário de encerramento da eleição; (iv) o código de identificação da urna; (v) a quantidade de eleitores aptos; (vi) a quantidade de eleitores que compareceram; (vii) a votação individual de cada candidato; (viii) os votos para cada legenda partidária; (ix) os votos nulos e brancos; (x) a soma geral dos votos; (xii) quantidade de eleitores cuja habilitação para votar não ocorreu por reconhecimento biométrico; (xiii) código de barras bidimensional (Código QR). (TSE, 2021c) São impressas cinco cópias do Boletim da Urna: uma é afixada na porta da seção eleitoral para que qualquer cidadão tenha acesso; a segunda é entregue a fiscais de partidos políticos; a terceira permanece com o presidente da mesa receptora para ser comparada com o Boletim de Urna divulgado pelo TSE e as últimas duas são entregues à Junta Eleitoral com os demais documentos da seção eleitoral. Além das vias obrigatórias do boletim de urna, podem ser impressas até 5 vias adicionais, caso assim seja solicitado pelos fiscais de partidos, coligações, imprensa e Ministério Público.

Por fim, uma cópia do Boletim da Urna também fica gravada na mídia removível, criptografada, para ser utilizada na fase de apuração dos resultados. Acrescenta-se que os Boletins de Urna possuem QR Code que pode ser lido utilizando-se um aplicativo desenvolvido pela Justiça Eleitoral ("Boletim na mão"). Assim, qualquer pessoa poderá escanear o QR Code, conferir o resultado do pleito em seu celular e confrontar os resultados apurados por seção eleitoral e com o resultado da totalização final, disponibilizados no *site* do TSE.

O presidente da mesa da seção eleitoral entrega um envelope lacrado e assinado pelos membros da mesa ao órgão central da Justiça Eleitoral, contendo o *pen drive* da urna eletrônica (mídia móvel chamada Memória de Resultado), as duas vias do Boletim de Urna, a Zerésima, o Boletim de Justificativa, Boletim de Identificação dos mesários, Ata da Mesa, cadernos de votação, formulários de justificativa e demais materiais exigidos pela Justiça Eleitoral. O *pen drive* é criptografado, sendo lido apenas pelo computador do órgão central da Justiça Eleitoral.

No dia da eleição, há ainda a *auditoria de funcionamento das urnas eletrônicas sob condições normais de uso*, conhecida também como votação paralela. Através desse procedimento, busca-se comprovar se o voto digitado na urna pelo eleitor é devidamente computado e se coincide com a apuração feita pelo TSE. Para tanto, na véspera da eleição, é simulada a votação em cédula de uma seção eleitoral que de fato existe, e, no dia eleição, os mesmos votos são digitados na urna eletrônica, de modo que fique evidenciada a coincidência

dos resultados. Todo o processo é monitorado por câmeras de vídeo e funciona da seguinte forma: algumas urnas do estado, sendo ao menos uma da capital, são sorteadas à véspera da eleição, a depender do número de seções eleitorais do estado (em 2020, noventa e três urnas passaram por essa auditoria em todo território brasileiro) (TSE, 2021d); após o sorteio das seções, os respectivos juízes eleitorais são notificados para que procedam ao recolhimento da urna sorteada e aguardem a coleta da urna eletrônica; em seguida, as urnas eletrônicas sorteadas são transportadas até o local de realização de auditoria e são substituídas por outras urnas nas seções eleitorais; representantes dos partidos políticos e das coligações preenchem cédulas de papel, em quantidade correspondente ao número de eleitores registrados nas respectivas seções eleitorais, com votos nos candidatos oficiais, nulos ou brancos; as cédulas de papel são guardadas em urnas de lona lacradas; no dia da eleição, em paralelo com a votação oficial, funcionários da Justiça Eleitoral digitam, em computadores e nas urnas sorteadas, os votos contidos nas cédulas de papel; após o encerramento da votação, os votos registrados nas urnas sorteadas são apurados e verifica-se se a totalização feita pelos computadores coincide com o resultado das respectivas urnas eletrônicas e com os votos contidos nas urnas de lona. (TRE, 2021b)

Os partidos políticos, as coligações, bem como os representantes da OAB e do Ministério Público são convidados a participarem das cerimônias de geração de mídias e de cargas das urnas eletrônicas, além de acompanharem a auditoria de verificação da autenticidade e integridade dos sistemas instalados e auditoria de funcionamento das urnas eletrônicas sob condições normais de uso. Aliás, os partidos e coligações poderão fiscalizar todas as fases do processo de votação e apuração das eleições, processamento eletrônico da totalização dos resultados; bem como poderão constituir sistema próprio de fiscalização, apuração e totalização dos resultados. (BRASIL, 2021b)

Assim, é possível realizar a auditoria do processo eleitoral em diversos momentos: verificação do resumo digital; reimpressão do boletim de urna; comparação entre o boletim impresso e o boletim recebido pelo sistema de totalização; verificação de assinatura digital dos softwares instalados na urna; comparação dos relatórios e das atas das seções eleitorais com os arquivos digitais da urna; auditoria do código-fonte lacrado e armazenado no cofre do TSE; recontagem dos votos por meio do Registro Digital do Voto (RDV); comparação da recontagem do RDV com o boletim da urna. (TSE, 2021e)

Cabe ressaltar que, desde a criação da urna eletrônica, os componentes de hardware e software passaram por atualizações técnicas de componentes como processador/CPU, memória, armazenamento e sistema operacional, a fim de oferecer uma solução mais robusta e completa.

A longo dos últimos vinte e quatro anos, a urna eletrônica emagreceu de doze quilogramas para oito quilogramas, reduziu de tamanho em 20% e aumentou sua autonomia em 50%. (ZANINI, 2021)

Em nível internacional, os sistemas eletrônicos de votação surgiram como uma forma de automatização da apuração, bem como sua aceleração, além de mitigação de erro humano e de fraudes.(PETERSEN e JAECKS, 2021) No caso brasileiro, o antigo sistema de votação em cédulas de papel e de apuração manual, propiciava diversas fraudes eleitorais, tais como, utilização de urnas de lona com votos já realizados, alteração de votos na contagem, alteração de votos nulos e brancos que iam para candidatos específicos no processo de registro de voto. O Brasil era palco de diversas fraudes eleitorais, endo emblemático o caso das eleições do Rio de Janeiro de 1994, em que a atuação do crime organizado promoveu a venda de votos, fraudes em urnas e adulteração de mapas de votação, levando à anulação das eleições para deputados federais e estaduais, por unanimidade, pelo TRE-RJ.[1] Em contraste, ao longo dos mais de vinte anos de utilização da urna eletrônica, nunca houve qualquer comprovação de fraude, segundo o TSE. (TSE, 2021f)

Em que pese os mecanismos de auditabilidade já apresentados, dúvidas acerca da integridade das unas são suscitadas pela sociedade civil e por partidos políticos, como se observa nas recentes propostas de implementação do voto impresso. Passadas duas décadas da criação das urnas eletrônicas, existem questionamentos frequentes sobre a segurança do mecanismo, principalmente no que se refere à possibilidade de fraudes no sistema informático utilizado pela urna, por exemplo, a alteração do código-fonte por um técnico do TSE para beneficiar o candidato A ou B. (SILVA, 2021) Discute-se especialmente o acesso ao código-fonte, atualmente permitido a apenas um grupo restrito. Além disso, nos testes de segurança realizados deste 2009 foram encontradas diversas vulnerabilidades (ainda que corrigidas posteriormente pelo TSE). Por exemplo, em 2012, o professor Diego Aranha e sua equipe quebraram o protocolo de segurança da urna e acessaram os registros digitais dos votos, conseguindo colocar os votos na ordem em que forma votados; e, em 2017, adulteraram o software de votação e o funcionamento da urna, alterando as mensagens exibidas ao eleitor na urna para fazer propaganda de um certo candidato, além de modificarem o Boletim de Urna. (MELLO, 2021)

Desde sua criação algumas vulnerabilidades foram apontadas no sistema eletrônico de votação, tais como, fraude dos mesários; presença de chaves de criptografia na memória volátil,

[1] Dois anos depois, contudo, o TSE concluiu que, apesar das provas de fraudes, o montante de votos fraudados não influenciou no resultado das eleições.

isto é, visível no código-fonte; verificação de integridade inadequada, uso de chave única para cifragem dos dados; utilização de algoritmos obsoletos; quebra de sigilo do registro digital do voto. (FERRÃO, 2019) Embora muitos desses aspectos tenham sido analisados e melhorados pelo TSE, persiste a alegação de que todos os mecanismos de auditagem disponíveis hoje em dia dependem do software, de forma que se o programa fosse adulterado, haveria comprometimento de todas as checagens e, consequentemente, o sigilo e a segurança das eleições. Ou seja, argumenta-se que a correspondência entre a intenção do eleitor e o resultado da eleição dependeria da qualidade do software de votação e de sua resistência contra manipulação por agentes internos e externos (SILVA, 2021); contrapondo-se o TSE ao afirmar que este problema é resolvido com o Registro Digital do Voto (RDV), que armazena de forma aleatória o voto de cada eleitor nas urnas. (MELLO, 2021)

Em meio a estas questões, e considerando que participação em testes públicos de segurança é limitada, urge questionar se a utilização do *blockchain* poderia ser uma forma de conciliar transparência, auditabilidade e segurança do sistema de votação com a confidencialidade e a privacidade dos votos.

3. *BLOCKCHAIN*

3.1 COMO FUNCIONA A TECNOLOGIA *BLOCKCHAIN*

Com o lançamento do Bitcoin em 2008, a tecnologia *blockchain* ganhou relevância e passou-se a discutir suas múltiplas possibilidades de aplicações. A concepção do *blockchain* se entrelaça com surgimento da criptomoeda *Bitcoin*, através da publicação do *whitepaper* "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (NAKAMOTO, 2021) no fórum *P2P Foundation*, pelo pseudônimo de Satoshi Nakamoto em 2008. No entanto, as funcionalidades do *blockchain* extrapolam transações financeiras, podendo ser utilizada, por exemplo, em substituição aos registros de públicos, realização de eleições, *smart contracts*, gestão de cadeia de suprimentos, armazenamento em nuvem. (WÜST e GERVAIS , 2018)

Sem a pretensão de se esgotar o que é ou como funciona o *blockchain*, faz-se necessário um delineamento de suas principais características, para que assim seja possível refletirmos acerca de sua aplicação nas votações brasileiras.

Segundo Wust e Gervais (2018, p.1):

> O nome *blockchain* deriva de sua estrutura técnica - uma cadeia de blocos. Cada bloco está vinculado ao bloco anterior com um *hash* criptográfico. Um bloco é uma estrutura de dados que permite armazenar uma lista de transações. As transações são criadas e trocadas por pares da rede *blockchain* e modificam o estado da *blockchain*. Como tal, as transações podem trocar valores monetários, mas não estão restritas a apenas

> transações financeiras e, por exemplo, permitem a execução de código arbitrário dentro dos chamados contratos inteligentes.

Percebe-se, portanto, que *blockchain* é uma cadeia de blocos ordenados nos quais são armazenadas transações com registro de data e hora. Cada transação adicionada a rede é validada e, somente depois, é inserida no bloco. Assim, apenas quando a capacidade de armazenamento de um bloco está completa, ocorre um processo de validação por meio de um protocolo, e o bloco finalmente é adicionado à cadeia, em um processo que, em alguns tipos de *blockchain*, é conhecido como mineração.

Os blocos são vinculados por meio de um código criptografado através da função *hash*, tornando o registro dos dados na cadeia praticamente imutáveis. Dessa forma, cada bloco faz referência ao bloco antecedente, denominado *parent block* por meio do armazenamento do *hash* deste, de forma que cada bloco conterá seu próprio conteúdo (transações mais recentes), além do *hash* do bloco anterior, e, com essas duas informações, gerará seu próprio *hash* (*hash* do *child block*). O *hash* é uma espécie de "impressão digital", uma função que codifica uma mensagem ou arquivo em letras ou números, não sendo possível obter o mesmo *hash* de objetos digitais distintos. Isto é, o *hash* é a assinatura do conteúdo do bloco; caso uma informação seja alterada, o *hash* será modificado.

Blockchain é um sistema descentralizado, isto é, não possui um servidor central, uma terceira pessoa responsável por validar e garantia a segurança do sistema. O *blockchain* faz uso de rede *peer-to-peer*, de forma que cada transação é verificada e armazenada por todos os *nós* (pares, computadores participantes da corrente), de forma que a própria rede de participantes se torna o intermediário que garante a confiabilidade dos dados, valida as transações e guarda o histórico de cada transação. A verificação das transações é feita através de um mecanismo de consenso denominado *proof-of-work,* que se baseia na solução de um problema matemático pelos próprios participantes.

Quando os *nós* (também chamados de mineradores) descobrem o resultado da prova de trabalho, a solução do problema matemático é propagada na rede os demais nós, que verificam se o resultado encontrado está correto. Caso esteja, o novo bloco é validado e passa a fazer parte da cadeia de blocos. A adição do bloco à cadeia somente ocorre quando a validação é concluída pela maioria dos participantes, garantindo um alto grau de segurança e confiabilidade ao sistema.

Para garantir a integridade do processo de troca de informação entre os *nós* do *blockchain* utiliza-se a criptografia. Assim, apesar de as transações serem distribuídas na rede

entre todos os participantes, o anonimato é garantido por meio da criptografia assimétrica (ou criptografia de chaves públicas e privadas).

Por se tratar de um sistema descentralizado, o *blockchain* promove maior segurança e a transparência às transações. Dessa forma, caso ocorra um ataque malicioso em um ou mais computadores, o registro da informação permanecerá integro e seguro com os demais participantes da rede. Isso ocorre pois a alteração de um bloco específico, por menor que seja, ensejaria a alteração o seu *hash*, assim como o de todos os blocos posteriores. Na prática, para a realização desse tipo de alteração, exigir-se-ia um grande poder computacional, tornando inviável tal tarefa na maioria dos casos e levando a uma quase imutabilidade da *blockchain* e impermeabilidade de ataques. Matheus Passos Silva (2021, p. 130-131) explica melhor como funciona essa imutabilidade:

> A imutabilidade é decorrente não apenas do número crescente de confirmações, mas também – e principalmente – pelo fato de que como cada bloco tem seu próprio hash que depende do conteúdo ali armazenado, eventuais tentativas de alteração do conteúdo do bloco gerariam um novo hash, conflitando com o hash original. Verifica-se, portanto, que a decisão de gravar ou não um novo bloco na blockchain depende do consenso entre os usuários e não apenas da "vontade" da entidade controladora da rede. A título de exemplo, imagine o leitor que no bloco "A" seja gravada a palavra "lápis", identificando-se tal objeto como um "mecanismo que permite a escrita em papel". O bloco "A" criaria, neste exemplo hipotético, o hash número 5, correspondente ao número de letras da palavra "lápis". Os computadores conectados a esta rede verificariam que a palavra realmente possui cinco letras e, portanto, confirmariam que o hash do bloco "A" corresponde ao número 5. Entretanto, suponha-se que alguém mal-intencionado decidisse alterar o conteúdo do bloco "A" de "lápis" para "caneta", argumentando que este segundo objeto também é um "mecanismo que permite a escrita em papel". Se tal alteração fosse válida o cálculo matemático indicaria que agora o hash do bloco "A" seria 6. Porém, já foram feitas inúmeras confirmações referentes ao hash do bloco "A" como sendo 5, não 6. Tal alteração, portanto, seria invalidada pelos próprios computadores pertencentes à rede, pois todos eles já gravaram o número 5 como sendo o hash do bloco "A", não o número 6.

Vejamos agora como as características do sistema *blockchain* podem ser úteis para aprimoramento do sistema de votação eletrônico.

3.2 UTILIZAÇÃO DO *BLOCKCHAIN* EM SISTEMAS DE VOTAÇÃO

Inicialmente, é importante ressaltar que outros países e regiões do mundo já utilizaram *blockchain* em votações. É o caso, por exemplo, da Serra Leoa (eleições de 2018), Colômbia (em 2016, para quem estava fora do país e quisesse participar do plebiscito de tratado de paz com as FARC), Rússia e do estado da Virgínia nos Estados Unidos (eleições estaduais e federais em 2018 para militares e civis residentes no exterior). E, em 2020, o TSE realizou testes com sistemas baseados em *blockchain* em um projeto denominado "Eleições do Futuro", buscando avaliar possíveis inovações no sistema eleitoral. (EXAME, 2021)

A quase imutabilidade das informações já adicionadas à cadeia de *blockchain* é uma de suas principais vantagens, visto que para fraudar a eleição, o agente malicioso teria que alterar todos os registros de pelo menos metade da rede. Além disso, a utilização desta tecnologia tem potencial para aumentar celeridade (resultado seria gerado segundos após o encerramento das eleições), a transparência (cada eleitor poderia monitorar todos os votos, verificando se o voto foi realmente contabilizado para o candidato escolhido) e a eficiência do processo eleitoral, (em razão da redução do custo advinda da mobilização da estrutura necessária para a realização das eleições, como transporte e preparação das urnas, auxílio-alimentação dos mesários, apoio técnico-administrativo e o auxílio das Forças Armadas).

Em 2020, o orçamento da Justiça Eleitoral para as Eleições municipais de 2020 previa despesas equivalentes a R$ 106,6 milhões para o transporte e apoio operacional relativos às urnas eletrônicas; além de R$ 93,7 milhões para a alimentação dos mesários; R$ 89,7 milhões para apoio administrativo, técnico e operacional; R$ 40,7 milhões destinado ao auxílio das Forças Armadas e R$ 25 milhões para os materiais de consumo, votação, apuração, justificação, diplomação e divulgação de resultados, entre outras despesas. (TSE, 2021g) Assim, no caso de utilização e *blockchain*, os eleitores poderiam votar de qualquer local do mundo, utilizando apenas um celular ou computador, contribuindo para economia nos custos envolvidos na organização das eleições.

Além disso, a facilidade e rapidez promovidas por não precisar se deslocar até a seção eleitoral para votar podem contribuir para aumentar a participação democrática. E é bom ressaltar que a utilização de aplicativos pelos eleitores já ocorre através do e-título, tida como a via digital do título de eleitor. Através do aplicativo e-título, o eleitor tem acesso a informações junto à Justiça Eleitoral, como emissões de certidões eleitorais, consulta de débitos, cadastramento como mesário voluntário, além de proporcionar ao eleitor a possiblidade de justificar sua ausência no dia das eleições.

É importante que deixar claro que a *blockchain* utilizada no sistema de votação deve ser privada, isto é apenas membros autorizados pela Justiça Eleitoral poderiam encadear os blocos, gravando dados no sistema, e apenas a Justiça Eleitoral poderia confirmar a autenticidade dos dados enviados.

Contudo, persistem as preocupações quanto ao sigilo e liberdade do voto. O fato de o cidadão ter a chave privada para verificar seu voto não impede a compra e manipulação do voto, vez que o eleitor pode ser coagido a compartilhar sua chave privada de sua identidade digital. Além disso, em se tratando de uma votação realizada em celulares e computadores, há incremento dos riscos de coação, haja vista que não há um ambiente controlado como é o que

atualmente se dá as eleições. Uma possibilidade seria um modelo híbrido, em que o eleitor continuaria se dirigindo à seção eleitoral para votar na urna eletrônica, mas esta urna eletrônica estaria conectada ao sistema *blockchain.* No entanto, esta alternativa acabaria por obstaculizar uma das principais vantagens da utilização da tecnologia *blockchain*, que é reduzir os custos resultantes da logística complexa que envolve uma eleição. Outra alternativa seria permitir que o cidadão vote quantas vezes quiser antes do encerramento das eleições, de forma que, como o voto posterior cancelaria o voto anterior, o eleitor teria a opção de alterar o seu voto, resistindo a eventuais pressões que venha a sofrer. (SILVA, 2021)

Além disso, a utilização de um sistema *blockchain* significa que as eleições, ao contrário do que ocorre com as urnas eletrônicas, estaria conectada a uma rede. Atualmente, como já mencionado, o *software* da urna não pode ser alterado remotamente, mas com a utilização de *blockchain* as eleições estariam sujeitas à ataques remotos, ainda que de forma pouco provável.

Outrossim, há de se ter conta que o acesso à internet não é um direito fundamental. Em uma país em que 12,8 milhões de lares não tem acesso à internet (AGÊNCIA BRASIL, 2021), é inviável exigir um dispositivo conectado à internet para o exercício do direito de voto.

Outro desafio seria a verificação da identificação do eleitor no processo eleitoral. A identificação do eleitor deve ser autenticada por impressão digital ou reconhecimento facial, a fim de garantir que quem está votando é quem de fato deveria estar votando.

4. CONCLUSÃO

A tecnologia cada vez mais faz parte da avida das pessoas. Atualmente conseguimos fazer compras online e já há diversas profissões que são desempenhadas de maneira 100% remota, mas a participação eleitoral ainda precisa ser exercida de forma presencial em determinado local em contramão à Era Digital, em que informação e a tecnologia atuam para facilitar a comunicação, transferência de dados e transações comerciais. (MIT TECHNOLOGY REVIEW, 2021)

No entanto, a tecnologia *blockchain* é relativamente nova, demandando testes para que seja verificada sua real viabilidade no processo eleitoral brasileiro, de forma que qualquer mudança deve ocorrer de forma gradual, com uma adequada conscientização da população e desenvolvimento de técnicas capazes de garantir a segurança do sistema eleitoral.

Assim, sua introdução poderia ocorrer através do uso em votações menores, como votações para decidir a utilização e um espaço público, o nome de um parque, a realização de uma obra pública.

5. REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA BRASIL. *Sobe para 82,7% percentual de domicílios com internet, diz IBGE*. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-04/sobe-para-827-percentual-de-domicilios-com-internet-diz-ibge>. Acesso em 27/09/2021.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 5589/DF*. Relator: Ministro Gilmar Mendes. Brasília, 16 de agosto de 2020. Disponível em: < https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344589336&ext=.pdf>. Acesso 20/07/2021 (a).

BRASIL. *Lei nº 9.504, de 30 de setembro de 1997*. Estabelece normas para eleição. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9504.htm> Acesso em 23/09/2021 (b).

CÂMARA DE DEPUTADOS. *Proposta de Emenda Constitucional nº 135/2019*. Autoria: Deputada Bia Kicis. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1807035&filename=PEC+135/2019>. Acesso em 12/07/2021.

EXAME. *TSE vai testar eleições com blockchain no Brasil em 15 de novembro.* Disponível em: <https://exame.com/future-of-money/blockchain-e-dlts/tse-teste-eleicao-com-blockchain-no-brasil/>. Acesso em 27/09/2021.

JORNAL DO COMÉRCIO. *Voto impresso vai custar R$ 2,5 bilhões ao TSE.* Disponível em: <https://www.jornaldocomercio.com/_conteudo/2017/07/politica/575305-voto-impresso-vai-custar-r-2-5-bilhoes-ao-tse.html>. Acesso em 23/09/2021.

MELLO, Patrícia Campos. *Só Brasil, Bangladesh e Butão usam urna eletrônica sem comprovante do voto impresso.* Folha de São Paulo, 9 de junho de 2021. Disponível em: <https://www1.folha.uol.com.br/poder/2021/06/so-brasil-bangladesh-e-butao-usam-urna-eletronica-sem-comprovante-do-voto-impresso.shtml>. Acesso em 23/09/2021.

MIT TECHNOLOGY REVIEW. *Eleições americanas e blockchain*. Disponível em: <https://mittechreview.com.br/eleicoes-americanas-e-blockchain/>. Acesso em 27/09/2021.

PETERSEN, Steven; JAECKS, Howard. *Combination electronic and paper ballot voting system*. Disponível em:

<https://patentimages.storage.googleapis.com/39/be/66/93e35d8b4de022/US20040169077A1.pdf>. Acesso em 27/07/2021.

SENADO FEDERAL. E-cidadania. *Sugestão nº 9 de 2018 (SUG 9/2018*). Disponível em: < https://www12.senado.leg.br/ecidadania/visualizacaomateria?id=132598>. Acesso em 12/07/2021.

SILVA, Matheus Passos. *A segurança da democracia e a blockchain*. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao2/article/viewFile/1073/911>. Acesso em 23/09/2021.

TRE. *Segurança do processo eletrônico de votação.* Disponível em: <https://www.tre-mg.jus.br/eleicoes/seguranca-do-processo-eletronico-de-votacao>. Acesso em 23/07/2021a.

TRE. *Saiba como funciona as auditorias nas urnas no dia da eleição*. Disponível em: <https://www.tre-sp.jus.br/imprensa/noticias-tre-sp/2020/Novembro/saiba-como-funcionam-as-auditorias-nas-urnas-no-dia-da-eleicao>. Acesso em 24/07/2021b.

TSE. *Sério Voto Impresso: primeira experiência com impressão do voto foi nas eleições de 2002*. Disponível em <https://www.tse.jus.br/imprensa/noticias-tse/2017/Fevereiro/serie-voto-impresso-primeira-experiencia-com-impressao-do-voto-foi-nas-eleicoes-de-2002>. Acesso em 23/09/2021a.

TSE. *Resolução nº 23.603, de 12 de dezembro de 2019*. Dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação. Disponível em: < https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-603-de-12-de-dezembro-de-2019>. Acesso em 23/07/2021b.

TSE. *Resolução nº 23.611, de 19 de dezembro de 2019*. Dispõe sobre os atos gerais do processo eleitoral para as Eleições 2020. Disponível em: < https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-611-de-19-de-dezembro-de-2019-1>. Acesso em 23/07/2021c.

TSE. *Veja como é feita a auditoria de funcionamento da urna eletrônica*. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2020/Dezembro/veja-como-funciona-a-auditoria-de-funcionamento-das-urnas-eletronicas>. Acesso em 23/07/2021d.

TSE. *Auditoria*. Disponível em: <https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/como-realizar-auditoria>. Acesso em 23/07/2021e.

TSE. *Série Desvendando a Urna: já foram comprovadas fraudes na urna eletrônica?* Disponível em:

<https://www.tse.jus.br/imprensa/noticias-tse/2020/Outubro/serie-desvendando-a-urna-ja-foram-comprovadas-fraudes-na-urna-eletronica>. Acesso em 27/07/2021f.

TSE. *Eleições 2020: custo do pleito deve girar em torno de R$ 647 milhões*. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2020/Outubro/eleicoes-2020-custo-do-pleito-deve-girar-em-torno-de-r-647-milhoes>. Acesso em 27/09/2021g.

VELLOSO, Carlos Mário da Silva. Urnas Eletrônicas: um pouco de sua história. In: *Balanço das Eleições/2014*, TSE. Brasília, DF, 2015.

WÜST, Karl; GERVAIS, Arthur. *Do you need a Blockchain?* 2018 Crypto Valley Conference on Blockchain Technology - CVCBT. New York: Institute of Electrical and Electronics Engineers - IEEE. p. 01-10, June. 2018.

ZANINI, Fábio. *Pai da Urna Eletrônica Preocupa-se com Futuro de sua Cria*. Folha de S.Paulo. 14 de abril de 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/04/pai-da-urna-eletronicapreocupa-se-com-futuro-de-sua-cria.shtml. Acesso em: 23/07/2021.