A APLICABILIDADE DA CRIPTOGRAFIA BLOCKCHAIN NAS ELEIÇÕES COMO GARANTIA DO PROCESSO ELEITORAL E DA DEMOCRACIA [1]

THE APPLICABILITY OF BLOCKCHAIN CRYPTOGRAPHY ON ELECTIONS AS ELECTORAL PROCESS AND DEMOCRACY GUARANTEE

Rijkaard Dantas de Santana[2**]

[1] Grupo de Trabalho V. Sistema de Administração, Regulação, Normatização e Controle das Eleições.

[2**] Advogado. Graduado em Direito pela UNIFACISA. Especializando em Direito Digital e Compliance. rijkaard.dantas@gmail.com

RESUMO: O desenvolvimento humano sempre foi pautado pela constante busca pela criação ou aprimoramento das práticas para ampliar as possibilidades de atuação do homem. Em meio a essa realidade desenvolvimentista é que surge a internet e a virtualização como fator de intensa transformação das interações humanas, ocorrendo um processo de empoderamento político, monetário e cultural do homem individualmente considerado. Essa nova perspectiva social do homem impacta as velhas estruturas de poder, exigindo maior participação e certificação pelo indivíduo, sendo possível por meio das aplicações da internet e de protocolos de criptografia como o Blockchain. Por meio desse é possível a realização de eleições em que a validação é realizada por todos os eleitores, garantindo assim um processo eleitoral limpo e assegurando o voto de cada eleitor. Mais do que processo eleitoral, essa realidade impacta sobre a liberdade do voto e da ordem constitucional, ocorrendo uma mudança da cultura política. O estudo é realizado pelo método hipotético dedutivo, com revisão bibliográfica e análise comparativa do Brasil e outros países.

PALAVRAS-CHAVE: Blockchain. Empoderamento político. Processo eleitoral.

ABSTRACT: Human development has always been guided by the constant search for the creation or improvement of the practices to expand the possibilities of human performance. In the midst of this developmental reality is that the internet and virtualization appear as a factor of intense transformation of human interactions, occurring a process of political, monetary and cultural empowerment of the individual man considered. This new social perspective of man impacts the old power structures, requiring greater participation and certification by the individual, being possible through Internet applications and cryptographic protocols such as Blockchain. By means of these it is possible to hold elections in which validation is carried out by all voters, thus ensuring a clean electoral process and ensuring the vote of each voter. More than electoral process, this reality impacts on the freedom of the vote and the constitutional order, taking place a change of the political culture. The study is carried out by the hypothetical deductive method, with bibliographical review and comparative analysis of Brazil and other countries.

KEYWORDS: Blockchain. Political empowerment. Electoral process.

1 INTRODUÇÃO

O processo de desenvolvimento social é imanente a sociedade pois há uma busca constante por novas práticas, ou aperfeiçoar das já existentes, seja nas relações pessoais, culturais, econômicas ou políticas. De modo que esses processos de mudança se desenvolvem sob o curso natural social ou por situações humanas forçadas em razão da necessidade, mas em ambas partem da vontade humana.

De modo que a internet e a virtualização das relações são notoriamente as mais impactantes transformações humanas no século XXI, modificando as consolidadas estruturas de manutenção do poder político e monetário. Concedendo maiores possibilidades aos indivíduos, mesmo considerados isoladamente e mais ainda quando coletivamente aglutinados. Possibilitando aos usuários a liberdade de atuação contra estrutural, trazendo maior controle na condução do processo decisório.

Sendo o controle decisório um elemento de grande importância no curso histórico da humanidade, pois o controle do Estado por grupos políticos é uma constante na sociedade para manutenção de um *status quo* favorável as suas ideias ou ideologias do grupo e a condição dos ditamos de toda a sociedade. Todavia, mesmo observando estruturas democráticas de exercício do poder político eleitoral existem interferências internas ou externas capazes de comprometer todo o processo eletivo e, portanto, como consequência última, burlar a liberdade e vontade de escolha individual do cidadão, o eleitor.

Porém, entre as muitas possibilidades e criações impactadas pela internet acha-se o *Blockchain*. Trata-se de software de protocolo de criptografia que surgiu associada a criptomoeda *Bitcoin*, desenvolvida por Satoshi Nakamoto, que atua em rede com todos os usuários para validação de transações econômicas de modo descentralizado, direto entre os usuários além de tornar a informação imutável. Contudo, as suas funcionalidades ultrapassam a segurança computacional das moedas digitais, mas para governos e setores industriais e comerciais.

Assim, associando o empoderamento político do indivíduo pela internet e as funcionalidades da integração e protocolos de segurança, especialmente o *Blockchain*, é

possível se pensar em um processo eleitoral mais seguro, livre de interferências externas, auditado por todos os eleitores.

Mas mais do que controle do processo eleitoral por meio da criptografia *Blockchain* garantindo assim um processo eleitoral livre e democrático, o impacto dessa nova tecnologia e da presença de internet, alicerçada no princípio da liberdade, nos fundamentos da sociedade pode modificar o entendimento do exercício do direito político e constitucional pelo cidadão. A consequência última é a mudança para a plena liberdade do exercício do sufrágio, especialmente do voto, tornando-o não obrigatório.

Assim, o objetivo desse estudo concentra-se em observar a viabilidade e a aplicabilidade da criptografia *Blockchain* no processo eleitoral como garantia da maior participação e controle por parte do cidadão, garantindo assim um processo eleitoral democrático. Mais ainda, verificar o impacto sob o aspecto jurídico que a ideia de liberdade que a internet confere aos indivíduos na ordem constitucional como mais um elemento na busca da efetivação da plena democracia na sociedade brasileira.

Para tanto, a metodologia a ser utilizada no estudo se desenvolvera com a revisão bibliográfica sobre a temática, seja com autores nacionais e internacionais. Observar de modo comparativo as experiências que internacionalmente estão sendo aplicadas e trazer para a realidade da ordem jurídica e política do Brasil. Tudo isso em observância ao método hipotético dedutivo, tendo como hipótese a aplicação da *Blockchain* no processo eleitoral e a dedução das implicâncias e desdobramentos na cultura democrática e constitucional do Brasil.

2 ORIGEM DA TECNOLOGIA BLOCKCHAIN COM O BITCOIN E O SEU FUNCIONAMENTO

No ano de 2008 o mundo encontrava-se imerso em uma das mais graves crise econômica do capitalismo, sendo essa uma realidade cíclica em razão da estrutura comercial e monetária adotada pela sociedade. E em meio a instabilidade monetária que permeava a época é que Satoshi Nakamoto, desenvolvedor computacional anônimo, lançou para o mundo em 31 de outubro de 2008 o documento "Bitcoin: Um sistema de dinheiro eletrônico ponto-a-ponto" (NAKAMOTO, 2008).

Naquele documento o entusiasta desenvolvedor apontava os caminhos técnicos para a criação da criptomoeda *Bitcoin*. A criação de uma moeda digital e descentralizada tem por essência a ruptura com o cenário monetário tradicional, retirando dos bancos públicos a prerrogativa monopolista de emitir moeda e realizar todas as transações econômicas entre as pessoas, ou seja, ser o terceiro de boa-fé a validar as negociações, de modo que o *Bitcoin* pode ser definido como:

> Trata-se de uma moeda digital ou unidade monetária, também conhecida como criptomoeda. Ela funciona por meio de uma criptografia, ou seja, um conjunto de técnicas que protegem uma informação para garantir que ela só seja decifrada por quem conhece o código, garantindo a segurança do Bitcoin.
>
> No entanto, a moeda digital tem o código aberto. Isso significa que o acesso é livre para qualquer pessoa, sendo esta uma moeda gerenciada pelos próprios usuários e sem a necessidade de nenhum intermediador, como o Banco Central ou mesmo as empresas de cartão. **Para simplificar o conceito, podemos dizer o que é Bitcoin: um novo meio de pagamento utilizado em transações online. Essa tecnologia permite a realização de pagamentos eletrônicos com a mesma eficiência daqueles feitos com as cédulas usadas no mundo físico**. (ROLIM, 2018, grifo nosso)

Logo, as transações realizadas pela plataforma do *Bitcoin* não necessitam de certificação de um terceiro precisamente em razão da tecnologia que dá suporte ao sistema, o *Blockchain*. Portanto, suprimindo a necessidade do banco para validar a transação, por exemplo, de transferências entre contas correntes.

Todavia, o *Bitcoin* não foi a primeira tentativa de criação de uma moeda digital, em outras épocas tentou-se criar, sob o mesmo fundamento, as criptomoedas, como se tem em registros

> Uma das primeiras moedas digitais foi a Digicash, criada por Chaum, e depois foi vendida e usada apenas para assentos bancários. Houve muitos outros esforços durante esses anos que tentaram criar a moeda da Internet perfeita, como a Hashcash, E-gold e Bitgold (BITCOIN, 2017)

Ocorre que em todas essas situações pretéritas sempre houve o constante problema da duplicidade da moeda, ou seja, em transações econômicas é necessário certificar que a moeda não seja utiliza duas vezes pela mesma pessoa, do contrário a mesma moeda estaria sendo duplicada e não estaria saindo de uma pessoa para outra, gerando desvalorização da moeda. De modo que esse é o trabalho desempenhado pelos bancos quando alguém realiza uma transação bancária, esse assegurando que realmente o dinheiro saiu de uma conta para outra.

Porém, diferentemente das tentativas anteriores de criação de moedas digitais, o *Bitcoin* possui o suporte técnico da criptografia *Blockchain* que é um código aberto, no qual qualquer usuário pode verificar a autenticidade das transações utilizando o número da assinatura digital, podendo ser definido com mais precisão nas seguintes palavras:

> A blockchain é a rede de blocos onde estão registradas todas as transações com o bitcoin. Do início do funcionamento da rede até os dias atuais, todas as transações são mantidas nos blocos da rede (daí vem o nome "blockchain" = cadeia de blocos).
>
> Essa rede de blocos possui duas características principais: pode ser auditada por qualquer pessoa e é praticamente inviolável.
>
> Embora nenhuma transação possua identificações diretas de quem participou dela (como nome, documentos ou e-mail), cada uma delas possui uma assinatura digital, também chamada hash. Essa assinatura é única de cada transação – é impossível haver duas transações com o mesmo hash. Através dela é possível verificar na blockchain quando a operação foi feita, com data e hora completas, de quanto foi a transferência e quais endereços participaram. (ROLIM, 2017)

O *Blockchain* funciona como um protocolo de certificação em que todos os usuários, em rede, validam as transações realizadas com o *Bitcoin* substituindo as atribuições de certificação do banco e suprimindo o problema da duplicidade da moeda, assegurando a lisura e validade das transações em razão da sua tecnologia.

Assim, todas as transações possuem um número de registro público e privado, que por sua vez são conectadas as demais transações, criando uma sequência que se fecha em um bloco que é conectado a outro e assim sucessivamente. Criando assim uma longa cadeia de blocos que todos os usuários certificadores possuem individualmente.

De modo que a segurança garantida pelo *Blockchain* é praticamente inviolável, pois para modificar qualquer transação registrada em algum bloco é necessária força computacional capaz de modificar todos os registros dos blocos em todos os acessos de todos os usuários simultaneamente. Pois ao entrar em rede para validação, todo os usuários necessariamente armazenam a informação consigo, ou seja, cada um possui a extensão completa das transações. Assim, se só uma sequência de blocos estiver alterada é porquê essa não é a verdadeira.

Portanto, o princípio de aplicação do *Blockchain* é o de segurança e descentralização do controle de validação das transações. Não se limitando as moedas digitais, mas de diversas transações, retirando uma terceira pessoa obrigatória, com

reconhecimento público ou o próprio Estado, e passando a ser validada pelos usuários em rede, armazenando as informações permanentemente nos blocos.

Assim, necessário observar que *Bitcoin* e *Blockchain*, apesar de criados sob a mesma circunstância, são distintos e cada qual possui uma aplicação diferente. Para tanto, muito se espera das funcionalidades do *Blockchain*, como se apercebe:

> **O Blockchain tem a oportunidade de encolher completamente o mundo como nós o conhecemos. As fronteiras entre países e empresas seria completamente eliminado. Transações e comércios através do bloco seria ainda mais fácil e não haveria dificuldade em trabalhar com empresas em qualquer lugar**. Transações seriam imediatas e as empresas poderiam interagir no exterior apenas tão facilmente como o faria se estivessem vizinhos diretos.
>
> Em última análise, a face dos negócios iria mudar completamente. Modelos atrás de empresas mudaria, oportunidades de carreira seriam abertos, e o comércio se tornaria muito mais fácil. Empresas grandes e pequenas com as mesmas chances e oportunidades e não haveria quase nada que impedisse que as empresas pequenas tivessem o mesmo impacto que as empresas grandes atualmente possuem. (COOPER, 2017, posição 517, grifo nosso)

As possibilidades de aplicação do *Blockchain* são diversas e sua amplitude ainda por ser descoberta em razão da inovação, não contando para mais de 10 anos de funcionamento da tecnologia, mas que se alarga constantemente. De modo que diante das aplicações já descritas entre outras a utilização em situações de Estado, especialmente as eleições, objeto central desse estudo, tendo sua aplicabilidade já cogitada, observe-se:

> Impactos sobre o governo
>
> Com a temporada atual das eleições provocando mais debate sobre como o governo pode controlar melhor nossas eleições e entregar serviços seguros, a emergente tecnologia blockchain pode oferecer uma solução. **Ao fornecer segurança e transparência – a redução do risco de crime e permitindo que todos possam auditar os resultados, a solução blockchain poderia reformular o futuro das eleições americanas**.
>
> [...]
>
> Este exclusivo – e aparentemente contraditória – combinação de atributos **torna a tecnologia blockchain uma opção intrigante para permitir potencialmente aplicações do governo de votar digitalmente**, identificação digital para registros de saúde, obras digitais e auditorias fiscais (DANIEL, 2017, posição 634-653, grifo nosso).

Assim, entre as muitas aplicações comerciais e governamentais questiona-se a sua utilização no processo eleitoral como garantia de segurança e transparência dos resultados do processo democrático.

3 O ATUAL PROCESSO ELEITORAL BRASILEIRO, CUSTOS E PROBLEMAS

O processo eleitoral brasileiro, na acepção mais ampla da palavra processo, compreendendo o ato de votação, totalização e divulgação de resultado, além do alistamento eleitores, cadastramento das candidaturas e diplomação dos eleitos é modernamente organizado pela Justiça Eleitoral. De modo que a estrutura desta justiça tem como órgão de cúpula o Tribunal Superior Eleitoral, e tendo em cada Estado da Federação o Tribunal Regional Eleitoral, além dos juízes eleitorais e juntas eleitorais.

Cada estamento da Justiça Eleitoral é responsável pela administração do processo eleitoral no âmbito municipal, estadual e federal, atuando todos em conjunto para a cooperação e otimização na condução do processo para se evitar conflito de informações ou incongruências em qualquer das fases das eleições. Necessário observar ainda as quatro funções da Justiça Eleitoral, sendo essas administrativa, jurisdicional, normativa e consultiva, todavia, aqui restringir-se-á a uma análise da função administrativa desta justiça sobre a condução do processo eleitoral, tal qual já definido.

Sob este aspecto, a Justiça Eleitoral vem inovando tecnologicamente desde o ano de 1996, ano de implantação das urnas eletrônicas com os sucessivos sistemas operacionais que davam suporte funcional. Na primeira geração de sistema tendo o DRE (*Direct Recording Electronic*), na segunda o IVVR (*Independent Voter Verifiable Record*) e em terceira geração o sistema E2E (End-to-End verifiability), sendo esse último atualmente utilizado por alguns Estados da Federação dos EUA, conforme elenca Faria (2017).

E desde o ano de 2008 o Tribunal Superior Eleitoral tem investido na implantação da identificação biométrica dos eleitores para maior segurança do processo eleitoral. De modo que todo o investimento para o processo tem um custo ao erário, como anunciado no ano processo eleitoral do ano de 2016 "as Eleições Municipais de 2016 vão custar R$ 600 milhões aos cofres públicos, segundo estimativas do presidente do (Tribunal Superior Eleitoral), ministro Gilmar Mendes", segundo o R7 (2016).

Ademais, apesar de todo o investimento em segurança e criptografia no processo eleitoral, as ocorrências de falhas e violação ao sistema são constantes, comprometendo a lisura e transparência na condução do processo democrático. Em testes realizados pelo próprio Tribunal Superior Eleitoral para as eleições de 2018, técnicos conseguiram invadir e decifrar informações sobre a votação:

> Especialistas em informática participaram nesta sexta-feira (01/12) de teste público de segurança das urnas eletrônicas a serem usadas na eleição de 2018 e conseguiram decifrar arquivos internos do equipamento.
>
> Segundo o coordenador de sistemas eleitorais do Tribunal Superior Eleitoral (TSE), José de Melo Cruz, é "possível" que os técnicos tenham conseguido identificar como foi o último voto registrado numa urna. (Ramalho, 2017)

Logo, apesar de todo investimento com dinheiro público e evolução a tecnologia utilizada pelo Tribunal Superior Eleitoral para administração da coleta, totalização e divulgação do resultado do processo eleitoral brasileiro recorrentemente apresenta falhas. Tal prática provoca insegurança jurídica para os eleitos e, principalmente, para os eleitores, pois trata-se da representatividade da população para o exercício constitucional dos desígnios do Estado brasileiro.

4 APLICABILIDADE TÉCNICA DO BLOCKCHAIN NAS ELEIÇÕES E A MUDANÇA DE CULTURA ELEITORA E DEMOCRÁTICA

Como já observado, o *Blockchain* funciona de forma técnica como um livro razão em que todas as transações são registradas e certificadas pelos usuários, garantindo assim com transparência e segurança precisamente pela forma com que está estruturado.

Segurança e transparência são objetivos permanentes no processo eleitoral, pois trata-se da concretização do processo democrático, no qual o cidadão no gozo pleno de sua capacidade política exerce o direito de votar e escolher seus representantes. Logo, a condução do processo eleitoral é importante para o processo democrático pois trata diretamente da legitimidade e representatividade da população, não podendo haver interferência que altere ou venha a causar riscos a vontade de cada eleitor.

De modo que ao observar a história do processo eleitoral brasileiro, não observando as restrições a quem tinha o direito de votar, mas restringindo ao próprio processo, tem-se um procedimento arcaico e manual até o ano de 1996 quando iniciou a instauração das urnas de votação e apuração eletrônica, concretizado só no ano de 2000 nas eleições para prefeito e vereadores.

Mas como já observado no tópico anterior, o atual processo eleitoral brasileiro, apesar do investimento em modernização e digitalização, o que gera um elevado custo

operacional, constantemente enfrenta questionamentos sobre a validade do processo, fato que gera indubitável insegurança para o sistema democrático.

Assim, observando a funcionalidade e aplicações do *Blockchain* é que se pode pensar em um processo eleitoral descentralizado, público e com registros permanentes e de livre acesso. Operacionalmente o procedimento se daria sob a seguinte perspectiva:

4.1 A aplicação técnica da criptografia Blockchain nas eleições

A proposta prática de aplicação da tecnologia *Blockchain* em um processo eleitoral tem por base a tese técnica desenvolvida por Pires (2016, pág. 46-49) em sua obra conclusiva, conforme Anexo A. Na oportunidade o autor desenvolve a utilização da *Blockchain* do *Bitcoin* em um cenário contido de 10 (dez) pessoas e 03 (três) candidatos, comprovando assim a funcionalidade do sistema.

Contudo, em um cenário mais amplo e diversificado como é a hipótese das eleições brasileiras, a utilização do *Blockchain* não seria a utilizada pelo *Bitcoin*. Mas a própria rede *Blockchain* operaria em parceria com o Tribunal Superior Eleitoral (TSE). Portanto, seria um sistema de votação fechado para os eleitores alistados, conferindo a cada eleitor uma chave de acesso pública e privada, garantindo assim a segurança do processo, para proceder com a votação em um candidato.

Assim, cada leitor terá um único voto, podendo a transação para cada candidato ser realizado de qualquer dispositivo eletrônico no tempo limite em que o sistema do *Blockchain* estiver aberto para votação e ocorrendo todo processo de validação pelos usuários.

Ou seja, o Tribunal Superior Eleitoral não funcionaria como certificador do processo eleitoral, mas como um observador e condutor do processo de votação e a validação realizada nos blocos do *Blockchain*, na qual o acesso é público e as informações imutáveis.

Candidato terá um código de clara identificação. O eleitor faz a leitura deste respectivo código do candidato e transfere para esse a sua unidade de valor, seu voto, para aquela categoria de votação.

Apesar de ser uma informação pública e verificável por todos ao longo de todo o processo de votação, o quantitativo de votos para cada candidato será exposto e toda a cadeia de blocos de votação aberta, aberto tão somente a chave pública de cada eleitor, não violando a privacidade e o sigilo do voto.

4.2 A mudança de paradigma cultural e jurídico com a aplicação do Blockchain

Como já aduzido, o desenvolvimento dos softwares *Bitcoin* e *Blockchain* de modo simultâneo em um momento de crise econômica, logo, de impulsionamento forçado em razão de uma necessidade humana, carrega consigo traços ideológicos liberais ou libertadores. Sendo essa uma mentalidade que permeia a internet, como se observa na Declaração de Independência do Ciberespaço de John Perry Barlow, de 08 de fevereiro de 1996, na qual o mesmo aduz que:

> Não temos governos eleitos, nem mesmo é provável que tenhamos um, então eu me dirijo a vocês sem autoridade maior do que aquela com a qual a liberdade por si só sempre se manifesta.
>
> Eu declaro o espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor. Vocês não têm direito moral de nos impor regras, nem ao menos de possuir métodos de coação a que tenhamos real razão para temer. (BARLOW, 1996)

De modo que a governança da internet ainda é um aspecto social e antropológico a ser enfrentado pelos governos, pois a liberdade é a premissa de uso do sistema capaz de inovar e causar rupturas com os velhos paradigmas em razão de sua plataforma virtualizada.

Logo, a implementação dos novos métodos criados no ambiente virtualizado no mundo real pode ser ideologicamente conflituoso, criando situações de ruptura de estruturas. A aplicação do *Blockcahin* em um processo eleitoral pressupõe a segurança de dados, descentralização e, principalmente, liberdade, tal como na aplicação do sistema ao sistema das criptomoedas como *Bitcoin*, instituindo um sistema *peer-to-peer* (P2P) ou pessoa para pessoa, eliminando a necessidade de intermediação dos bancos. Assim, mais do que um sistema de segurança, o *Blockchain* é um meio de liberdade.

Todavia, a Constituição Federal de 1988 instituiu no artigo 14, §1º que o voto é obrigatório:

> Art. 14. A soberania popular será exercida pelo sufrágio universal e pelo voto direto e secreto, com valor igual para todos, e, nos termos da lei, mediante:

> § 1º O alistamento eleitoral e o voto são:
>
> I - **obrigatórios para os maiores de dezoito anos**;
>
> II - facultativos para:
>
> a) os analfabetos;
>
> b) os maiores de setenta anos;
>
> c) os maiores de dezesseis e menores de dezoito anos. (BRASIL, 1988, grifo nosso)

O constituinte originário de 1988 entendeu necessária a obrigatoriedade do voto após um longo período de restrição do exercício pleno dos direitos políticos durante o regime militar. Também entendendo a melhor doutrina que a obrigatoriedade é decorrente do espírito democrático:

> É importante que se compreenda o espírito do voto obrigatório. Ele não significa uma restrição à liberdade do povo**. O seu objetivo é compelir o eleitor a comparecer à zona eleitoral para manifestar uma preferência**. Esta, por sua vez, dentro de uma concepção democrática, é livre e soberana, resumindo-se na utilização da urna eletrônica e, finalmente, na assinatura na folha individual de votação. (BULOS, 2009, pág. 497, grifo nosso)

De plano acha-se visível o antagonismo entre a realidade de liberdade intrínseca ao sistema *Blockchain* e a Constituição Federal de 1988 com a obrigatoriedade do voto. Ou seja, a forma de aplicação de voto descentralizada, certificada de forma pública e plenamente segura pelo *Blockchain* faculta ao eleitor a não votar, pois parte-se do pressuposto de um regime plenamente democrático, não havendo que se falar em obrigatoriedade como normatiza a CF de 1988.

Ou seja, as aplicações das novas tecnologias, especialmente o *Blockchain*, advindas da criação virtual possibilitam uma mudança de paradigma sobre o pensamento do regime político do Estado, ou da estrutura constitucional. De modo que um novo modelo democrático pode ser inaugurado pelas novas práticas virtuais que ampliam as possibilidades políticas em razão da condição social que a própria sociedade se submeteu, o da transparência e conectividade dos atos públicos, gerando maior controle social.

Evidente que se tratam elementos jurídicos distintos, o primeiro é um fato social decorrente de uma criação humana que impacta toda a coletividade, podendo vir a se tornar uma norma quando do

5 EXPERIÊNCIAS CIVIS E GOVERNAMENTAIS NO USO DO BLOCKCHAIN

Apesar de o governo brasileiro ainda não possuir qualquer perspectiva prática de utilização da tecnologia *Blockchain* no processo eleitoral, em diversos outros países as experiências são crescentes, servindo como laboratório de funcionamento para confirmação da aplicabilidade do protocolo de criptografia.

Já existem processos eleitorais realizados integralmente utilizando a criptografia *Blockchain*, é o exemplo da eleição presidencial em Serra Leoa, como se observa:

> **O sistema foi implantado pela fundação Agora, que oferece solução de votação digital baseada em blockchain para governos e instituições, e executado confidencialmente pelo Comitê Eleitoral Nacional de Serra Leoa com o apoio da empresa**. Ele fornece informações em tempo real para os funcionários designados e confiáveis que acompanham todo o processo.
>
> Para a Agora, essa experiência pode ser o primeiro passo em um plano tecnológico ainda maior. **A empresa confirmou que já está em diálogo com países interessados em suas futuras eleições, pois o uso da Blockchain pode resolver muitos problemas de ceticismo, como é comum, por exemplo, nos Estados Unidos, que é costumeiro em solicitar a recontagem de votos**. (RIGGS, 2018, grifo nosso)

Mas mais do que as aplicações eleitorais, a utilização no âmbito civil e comercial tem se alargado, como é observado no exemplo da Estônia, observe-se:

> Na Estônia, país com a ICP - Infraestrutura de Chaves Públicas - mais utilizada do mundo, os cidadãos são identificados com um cartão de identificação qual está vinculado seu par de chaves criptográficas, algo parecido com o e-CPF aqui no Brasil. Com esta identidade os cidadãos podem acessar contas bancárias, verificar as notas escolares dos filhos, gravar testamentos, encriptar documentos, assinar contratos e realizar mais uma série de atividades sobre o blockchain. Cidadãos da Estônia ainda podem usar sua identidade digital para acessar os serviços do bitnation.co, uma plataforma para o provimento de serviços de cartório em âmbito internacional, construídos sobre o blockchain do bitcoin. Nessa plataforma é possível emitir certidão de nascimento e de casamento, contratos de negócio e realizar doações para projetos de ajuda humanitária [Walport, 2016] [Scott, 2016]. (PIRES, 2016, pág. 44-45)

Ampliando mais ainda as funcionalidades do *Blockchain*, o governo de "Dubai, por exemplo, decidiu que todos os documentos dos órgãos públicos da cidade trafeguem via um blockchain governamental até 2020" (MONTEIRO, 2017). E ainda, mesmo que diante do antagonismo com as moedas digitais, diversos bancos que atuam multinacionalmente têm estudado a implementação do *Blockchain* em seus sistemas operacionais:

> Nos últimos quatro anos, o setor financeiro investiu US$ 1,4 bilhão em pesquisas sobre a tecnologia, segundo o Fórum Econômico Mundial**. Bancos como Goldman Sachs, Santander, UBS, Itaú e Bradesco estão testando o uso dessa ferramenta.**
>
> A ideia é acabar com o uso de intermediários e, assim, reduzir o custo das operações. Se isso acontecer, os bancos não teriam mais a necessidade de certificar as transações feitas de um usuário para outro usando o Sistema de Pagamentos Brasileiro (SPE).

> **Lá fora, o Citi e o JP Morgan, estão, em parceria com a IBM, estudando uma forma de substituir o sistema atual, chamado de SWIFT, pelo Blockchain**. (LOUREIRO, 2017, grifo nosso)

No Brasil, os bancos também estão observando a implementação da tecnologia por meio da iniciativa da Federação do Bancos (Febraban):

> No Brasil, o primeiro teste formal da nova tecnologia ocorreu em abril, quando um grupo de trabalho na Febraban (federação dos bancos) formado por 16 entidades – entre elas os cinco maiores bancos do país, o Banco Central e a Bolsa B3 – apresentou uma simulação de compartilhamento de cadastro com dados de clientes fictícios.
>
> [...]
>
> "O Blockchain permite ter mais eficiência operacional, que é o que todos os bancos procuram", diz Adilson Fernandes da Conceição, coordenador do grupo de trabalho da Febraban (BRANT, 2017)

Assim, as aplicações comerciais e governamentais, especialmente em processo eleitoral, do *Blockchain* é uma realidade em expansão no mundo e no Brasil, devendo se considerar a sua presença cada vez mais constante no cotidiano das pessoas.

De modo que as aplicações tecnológicas, especificamente do *Blockchain*, revelam uma permanente busca por segurança de dados, redução de custos e maior eficiência na prestação do serviço, seja no setor público ou privado, além de transparência social. Sendo que essa realidade que permeia a nova sociedade que se constrói alicerçada sobre as novas tecnologias, mudando os paradigmas culturais e legais.

6 CONSIDERAÇÕES FINAIS

Como observado, a tecnologia *Blockchain*, que surgiu de forma simbiótica com a criptomoeda *Bitcoin*, ganha novos campos de aplicação em razão do suporte técnico que oferece, como a validação de informações por todos os usuários, segurança com a imutabilidade dos dados e o sigilo nas operações, eliminando a presença de um terceiro obrigatório nas relações comerciais.

Assim, o *Blockchain* é um fator disruptivo ao processo natural de condução da vida social e política, tudo advindo das funcionalidades que a internet e a computação moderna possibilitam aos usuários. E em razão de sua plataforma virtualizada pode-se programar sem modificar a condição física dos elementos envolvidos, até mesmo podendo ser desfeito sem mudar o *status*.

De modo que a utilização do *Blockchain* é ampla e diversificada, seja no âmbito civil, comercial, financeiro e principalmente governamental sempre com o objetivo de se obter segurança e imutabilidade de dados, certificação das informações para sua validade por todos os usuários.

A entronização dessa tecnologia nos sistemas governamentais objetiva consagrar a publicidade e lisura dos atos públicos, evitando-se a corrupção e o uso indevido do erário e do poder público, conferindo assim ao povo maior controle sobre as ações dos seus governos. Ao passo que no setor privado se obtém a celeridade nos processos comerciais e civis, verificação e segurança das informações a um custo menor.

Ademais, no que concerne a implantação do processo eleitoral, tem-se por viável tecnicamente a utilização da tecnologia *Blockchain* nas eleições brasileiras com o objetivo de se conceder segurança, seja incorporando ao atual modelo, com a utilização das urnas eletrônicas, ou migrando para um sistema próprio que possibilite os usuários ou eleitores utilizarem os seus próprios dispositivos para realizarem a votação.

De modo que todas essas funcionalidades da tecnologia são, em essência, a busca constante por um processo eleitoral aberto, seguro e democrático. Livrando a manifestação popular de qualquer interferência que macule a legitimidade conferida pelo eleitor ao seu representante. Portanto, deve-se sempre observar a importância na condução das eleições, sendo esse um meio, não um fim em si mesmo, pois o seu fim é a legitimação para representação popular.

Mais ainda, considerando a hipótese de utilização da tecnologia *Blockchain* nas eleições brasileiras, o impacto político e democrático que pode provocar no atual sistema é imensurável, podendo modificar todo o sistema eleitoral, instituições de coligações partidárias, modelos de propaganda e publicidade das campanhas, além da própria regra de obrigatoriedade do voto, no nosso entendimento incompatível com a democracia.

Assim, além de sua viabilidade técnica entendemos ser uma tecnologia disruptiva para o próprio e contínuo processo democrático da sociedade brasileira, sendo necessário se ampliar os estudos para posterior e plena implantação nas eleições brasileiras.

REFERÊNCIAS

BARREIROS NETO, Jaime. **Histórico do processo eleitoral brasileiro e retrospectiva das eleições**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 14, n. 2162, 2 jun. 2009. Disponível em: <https://jus.com.br/artigos/12872>. Acesso em: 14 mar. 2018.

BITCOIN, Editorial do Guia do. **Como surgiram as criptomoedas? A "Economia Digital" foi criada graças ao Bitcoin**. Guia do Bitcoin. São Paulo, p. 100-130. 13 jun. 2017. Disponível em: <https://guiadobitcoin.com.br/como-surgiram-as-criptomoedas-a-economia-digital-foi-criada-gracas-ao-bitcoin/>. Acesso em: 19 jan. 2018.

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF, 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 10 jan. 2018.

BULOS, Uadi Lammêgo. **Constituição Federal Anotada**/ Uadi Lammêgo Bulos – 9ª Ed. Rev e atual. até a Emenda Constitucional n. 57/2008 – São Paulo: Saraiva, 2009.

CASTILLO, Michael del. **Sierra Leone Secretly Holds First Blockchain-Audited Presidential Vote**. Coindesk. Londres. 17 mar. 2018. Disponível em: <https://www.coindesk.com/sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote/>. Acesso em: 17 mar. 2018.

COOPER, Jimmy. **Blockchain para principiantes: tudo o que você precisa saber sobre a tecnologia blockchain e como está a criar uma revolução**/ Jimmy Cooper. 1ª Ed. Amazon Digital Services LLC. Arquivo Kindle, 2017.

FARIA, Marcelo. **Brasil é único país do mundo que utiliza urnas eletrônicas inauditáveis e obsoletas**. ILIPS Brasil. São Paulo. 04 out. 2017. Disponível em: <http://www.ilisp.org/artigos/brasil-e-unico-pais-do-mundo-que-utiliza-urnas-eletronicas-inauditaveis-e-obsoletas/>. Acesso em: 03 abr. 2018.

LOUREIRO, Rodrigo. **Blockchain, tecnologia da Bitcoin, seduz os bancos**. Isto É. São Paulo. 12 dez. 2017. Disponível em: <https://www.istoedinheiro.com.br/blockchain-tecnologia-da-bitcoin-seduz-os-bancos/>. Acesso em: 13 mar. 2018.

MONTEIRO, João. **Blockchain pode ser usado para tornar eleições mais seguras**. Ipnews. São Paulo. 31 ago. 2017. Disponível em: <https://ipnews.com.br/blockchain-pode-ser-usado-para-tornar-eleicoes-mais-seguras/>. Acesso em: 15 mar. 2018.

NAKAMOTO, Satoshi. **Bitcoin: Um sistema de dinheiro eletrônico ponto-a-ponto**/ Satoshi Nakamoto- Tradução: Leandro Guerra. 31 out. 2008. Disponível em: <https://rdstation-static.s3.amazonaws.com/cms/files/36895/1505219221Bitcoin_-_Um_Sistema_de_Dinheiro_Eletrnico_Ponto-a-Ponto.pdf>. Acesso em: 28 dez. 2017.

PIRES, Timoteo Pimenta. **Tecnologia Blockchain e suas Aplicações para provimento de transparência em transações eletrônicas**. 2016. 56 pág. TCC (Graduação) - Curso de Engenharia de Redes de Comunicação, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, 2016. Disponível em: <http://bdm.unb.br/bitstream/10483/16252/1/2016_TimoteoPimentaPires_tcc.pdf>. Acesso em: 14 mar. 2018.

RAMALHO, Renan. **Técnicos conseguem invadir urna eletrônica durante teste; TSE diz que falhas serão corrigidas**. G1. Brasília. 01 dez. 2017. Disponível em: <https://g1.globo.com/politica/noticia/tecnicos-identificam-falhas-em-urna-eletronica-e-tse-diz-serao-corrigidas.ghtml>. Acesso em: 05 abr. 2018.

RIGGS, Wagner. **Serra Leoa é o Primeiro País a Usar Blockchain em Eleição Presidencial**. Portal do Bitcoin. São Paulo. 09 mar. 2018. Disponível em: <https://portaldobitcoin.com/serra-leoa-e-o-primeiro-pais-usar-blockchain-em-eleicao-presidencial/>. Acesso em: 16 mar. 2018.

ROLIM, Luciano. **O que é bitcoin? Tudo o que você precisa saber**. Atlas Project. São Paulo. 11 jan. 2018. Disponível em: <https://atlasproj.com/blog/o-que-e-bitcoin/>. Acesso em: 17 jan. 2018.

_____. **Blockchain: Entenda o que é e como funciona essa tecnologia revolucionária**. Atlas Project. São Paulo. 11 jan. 2018. Disponível em: < https://atlasproj.com/blog/blockchain-como-funciona/>. Acesso em: 17 jan. 2018.

R7, Editorial. **Justiça Eleitoral estima em R$ 600 mi custo das Eleições 2016**. R7. Brasília, p. 100-120. 25 jul. 2016. Disponível em: <http://r7.com/lD63>. Acesso em: 03 abr. 2018.

ULRICH, Fernando. **Bitcoin: a moeda da era digital**/ Fernando Ulrich. 1ª Ed. - São Paulo: Editorado Instituto Ludwig Von Mises Brasil, 2014

ANEXO A

4. Proposta de Simulação de Votação

A simulação a seguir apresenta de maneira simples como a tecnologia do blockchain pode ser útil em um cenário de votação. Para simplificar a simulação e apresentar apenas os aspectos essenciais da tecnologia foi utilizado o próprio blockchain do bitcoin e os registros de voto computados a partir das transações.

Para contextualizar a votação, consideramos um cenário de eleição de representante de turma. A turma conta com 10 alunos votantes e 3 candidatos (incluídos no grupo dos 10 votantes): Bob, Alice e Charlie. A turma deve decidir de maneira democrática e utilizando o blockchain do bitcoin quem será o representante.

A descrição do processo de votação e os resultados podem ser visualizado nas etapas a seguir:

Etapa I - Identificação dos candidatos

Na primeira etapa, cada um dos candidatos recebe uma chave pública e uma representação em QR Code desta chave. Esta chave será utilizada pelos alunos da turma para realizar a votação. A chaves privadas correspondentes dos candidatos não serão utilizadas e devem ser descartadas.

Alice

1Gdnxs3GsdFzJUKiy6cJAs
nVU14RG8xfad

Bob

19XT9GYdU4L9dPjvMLVxNKU9T
MW4SH34qb

Charlie

1DzQA9g7BReCWRCtPfGP74
bJh7RAzQufdc

Etapa II - Identificação dos eleitores

Nesta etapa cada eleitor recebe um par de chaves pública e privada com o qual poderá realizar o seu voto. Serão gerados 10 pares de chaves, a chave pública caracteriza o aluno apto para a votação e a chave privada garante que o aluno assinou o voto enviado.

Para fazer a distribuição das chaves de votação é utilizado um sistema de impressão de chaves em papel, o BitcoinPaperWallet, que funcionará como uma cédula de votação. Nesta cédula está gravada a chave pública e privada do aluno e ele é responsável pela manutenção e privacidade destas informações. Além disso, cada cédula é previamente carregada com 1,1 mBTC para permitir o registro dos votos no blockchain. Uma cédula com o par de chaves é mostrada na Figura 4.1:

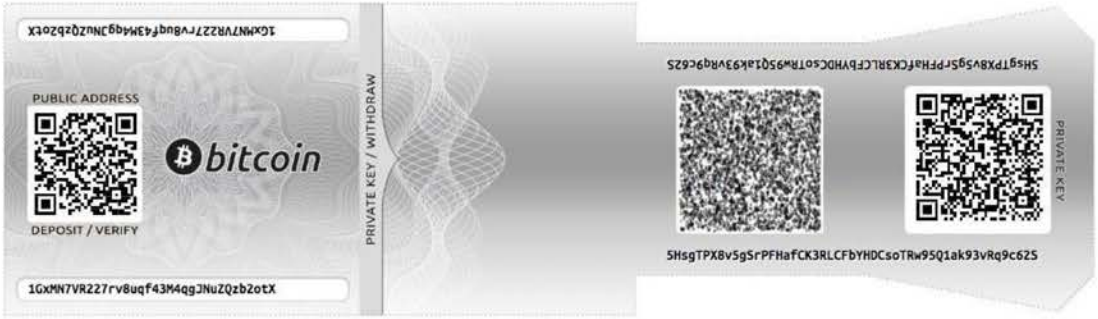

Figura 4.1 Cédula com chave pública e privada (criado com a ferramenta online BitcoinPaperWallet)

Etapa III. Votação

Após cada aluno receber a sua cédula de votação o processo segue para a etapa de votação. Cada aluno deve utilizar o seu par de chaves pública e privada para realizar uma transação com o candidato em que deseja votar. Nesta simulação, foi utilizada a ferramenta Blockchain Wallet para realizar as transações. A figura 4.2 apresenta informações da transação realizada com a cédula da Figura 4.1, a partir de consulta realizada na ferramenta online Blockchain Explorer.

Figura 4.2 Informações da transação no Blockchain Explorer

Percebe-se que o endereço de origem da transação é a chave pública da Figura 4.1 e o endereço de destino da transação é a chave pública do candidato Charlie. O número na parte superior da imagem é o Id da transação obtido a partir do seu hash. Nesta simulação foi utilizado 1 mBTC como valor de referência.

Etapa IV - Resultado e Conferência

Após todos os alunos terminarem de votar, o resultado da votação pode ser obtido a partir de uma consulta ao Blockchain Explorer pelos endereços dos candidatos. A quantidade de transações e de bitcoins recebidos indicam a quantidade de votos de cada candidato. A figura 4.3 apresenta esta relação.

Summary		**Transactions**	
Address	1Gdnxs3GsdFzJUKiy6cJAsnVU14RG8xfad	No. Transactions	4
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.004 BTC
		Final Balance	0.004 BTC
Summary		**Transactions**	
Address	19XT9GYdU4L9dPjvMLVxNKU9TMW4SH34qb	No. Transactions	1
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.001 BTC
		Final Balance	0.001 BTC
Summary		**Transactions**	
Address	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc	No. Transactions	5
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.005 BTC
		Final Balance	0.005 BTC

Figura 4.3 Quantidade de Transações e Bitcoins recebidos por cada candidato

O resultado aponta para uma vitória do candidato Charlie com 5 votos, enquanto Alice e Bob obtiveram 4 e 1 votos respectivamente. Uma consulta a todas as transações realizadas nesta simulação de eleição pode ser encontrada no apêndice A.

4.1 Observações

Faz-se agora algumas considerações a partir da observação dos resultados desta simulação.

O blockchain do bitcoin não foi projetado para votação. Trata-se de uma adaptação de um sistema de transação financeira para um sistema de voto. Mas há algumas propriedades desta tecnologia muito úteis em um processo de votação:

- A possibilidade de identificação de cada voto, sem necessariamente identificar o votante;
- A descentralização do processo de verificação dos votos;
- A auditabilidade do processo de contagem dos votos;
- A segurança na autenticidade do voto provida pela criptografia assimétrica;

Talvez, a maior dificuldade de implementação deste processo seja a manutenção e distribuição das chaves criptográficas aos eleitores. Alguns exemplos citados no capítulo 3 mostram que esta não é uma tarefa impossível, mas exige a estruturação de uma ICP eficiente e, em um cenário de eleição nacional, de um trabalho conjunto entre ICP-Brasil e TSE.

Destaca-se ainda que, conquanto o sistema seja bastante simples e necessitaria de grandes adaptações para uma eleição de médio e grande porte, algumas adaptações podem ser feitas para permitir a utilização da tecnologia em eleições menores como eleições de DCE, reitoria, conselhos administrativos e outras eleições realizadas em ambientes internos de organizações. Além disso, adaptações menores permitiriam a sua utilização para assinatura de Projeto de Lei de iniciativa popular pelos cidadãos.