ANÁLISE DA APLICAÇÃO DA TECNOLOGIA DE BLOCKCHAIN EM ELEIÇÕES DEMOCRÁTICAS

Álvaro Barros de Carvalho

IFSP, Cubatão, SP, Brasil

Bruno de Oliveira Silva

IFSP, Cubatão, SP, Brasil

Saulo Silva Castilhos

IFSP, Cubatão, SP, Brasil

**RESUMO**

O atual sistema de votação em urnas eletrônicas revolucionou a democracia brasileira em diversos campos, mas ainda existe desconfiança de parte da população em relação à sua credibilidade. Estuda-se a aplicação da inovação tecnológica *Blockchain* em sistemas eleitorais, analisando características fundamentais como vulnerabilidade à ameaças e praticidade de implantação.

**Palavras–chave:** Blockchain. Democracia. Votações.

**Abstract:**

The current voting system in ballot boxes revolutionized Brazilian democracy in a lot of ways, but the population still does not trust the system entirely. The possibility of a electoral system based on Blockchain technology is studied by analyzing crucial caracteristics such as vulnerability to attacks and practicality of implantation.

**Keywords:** *Blockchain. Democracy. Elections.*

**INTRODUÇÃO**

O Brasil encontra-se em uma crise política, com desesperança da população em meio a inúmeros escândalos de corrupção. Essa crise se torna especialmente visível em época de eleição, onde o cidadão apresenta desconfiança nos políticos e no sistema eleitoral. Discute-se soluções mais seguras e transparentes para o modelo democrático do país.

Para organização de um pleito eleitoral encontram-se dificuldades como elevados custos, praticidade de implantação, suscetibilidade à adulteração na apuração dos votos e garantia do registro da opinião de cada eleitor.

Dentro das soluções idealizadas, a tecnologia *Blockchain* é uma opção popular e promissora, possibilitando a realização de votações completamente seguras por meio de um telefone celular. Com um cadastro prévio de cada eleitor, é possível a emissão de seus votos, de qualquer localidade, através da rede mundial de computadores.

Este artigo visa demonstrar as fragilidades do sistema eletrônico de votação atualmente utilizado no Brasil, apresentar a tecnologia blockchain e seu possível uso para sistema de votações de menor custo, transparentes e com maior confiabilidade.

**AS URNAS ELETRÔNICAS**

A urna eletrônica foi utilizada pela primeira vez nas eleições de 1996. De lá para cá, o equipamento tem evoluído para proporcionar cada vez mais segurança para o processo eleitoral. Parte dessa evolução se deve à realização dos Testes Públicos de Segurança (TPS) do Sistema Eletrônico de Votação, que têm por objetivo fortalecer a confiabilidade, a transparência e a segurança da votação e da apuração, propiciando melhorias em todo o processo eleitoral.

(Eleições Seguras: testes públicos e auditorias garantem segurança do processo eleitoral brasileiro; Disponível em: <https://bit.ly/2qRt9l3>; Acesso em 2018)

Na primeira edição do TPS em 2009, os pesquisadores interessados não tiveram acesso ao código-fonte do sistema, mas eles conseguiram quebrar o sigilo do voto pela captura de frequências de rádio emitidas pelo teclado da urna, posteriormente o TSE alegou ter blindado o teclado contra esse tipo de ataque.

Dessa vez sem um Termo de Sigilo, em 2012 os especialistas puderam examinar o código-fonte do sistema, onde foram descobertas as primeiras vulnerabilidades de software. Em uma eleição simulada, os pesquisadores puderam recuperar um número suficiente de votos na ordem em que foram coletados devido a um problema no mecanismo RDV (Registro Digital de Voto) que é um software responsável por embaralhar os votos e que fica armazenado em cartão de memória. Ainda nessa edição do TSP os especialistas alertaram o TSE sobre falhas de projeto incluindo o compartilhamento em massa de chaves criptográficas, inclusive em local inseguro e escolha inadequada de algoritmos.

Somente em 2016 os TPS foram novamente abertos, porém com obrigatoriedade dos pesquisadores assinarem um Termo de Sigilo. Vulnerabilidades mais graves foram encontradas, o primeiro ataque foi a forja de códigos de verificação de BUs validados pelo SA (Sistema de Apuração) em caso de contingência [TSE 2016].

Se por um lado o TSE alega que o processo eleitoral têm se tornado mais seguro, especialistas que participaram do último teste demonstraram diversas fragilidades do sistema e pedem maior transparência no processo.

De acordo com Aranha (2018) o sistema de votações através de urnas eletrônicas utilizado no Brasil apresenta falhas graves de segurança e que poderiam comprometer diversos aspectos do sistema eleitoral como sigilo dos votos, integridade na apuração, dentre outros problemas que não puderam ser verificados devido ao tempo limitado e restrições na condução das testes de vulnerabilidade.

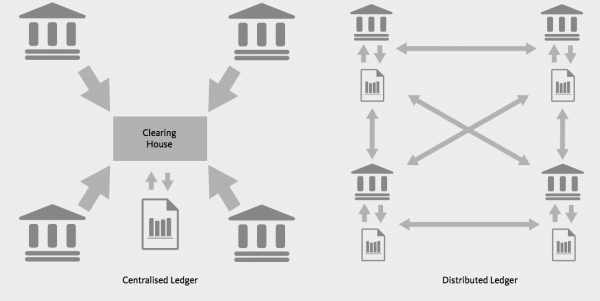
**A TECNOLOGIA BLOCKCHAIN**

As *Blockchains* são geralmente reconhecidas pelas criptomoedas, em especial a Bitcoin. São uma espécie de banco de dados distribuídos que armazenam e registram transações permanentemente e à prova de qualquer forma de adulteração dos seus registros. Essas qualidades lhe renderam incrível interesse de pesquisadores e investidores da era da informação, que afirmam que a tecnologia pode revolucionar áreas muito além da economia e com implantações mais úteis do que criptomoedas.

O Bitcoin é uma ideia genial. A tecnologia me impressiona, mas parece servir para outra coisa. Eu penso em Bitcoin como um experimento; não é uma característica permanente de nossas vidas. Enfatizamos o Bitcoin, mas devemos ampliá-lo para *Blockchain*, que terá outras aplicações.

(Shiller, Robert, Vencedor do prêmio Nobel de Economia; Disponível em <https://bit.ly/2zU8MaG>; Acesso em 2018; tradução livre do grupo)

A epidemia da *Blockchain* consiste no conceito de descentralização do controle da informação. É uma base de dados distribuída, logicamente e fisicamente, em diversos servidores e computadores. Quando existe um poder no controle de um sistema de informações, este se torna totalmente dependente, enquanto em um sistema descentralizado há uma dependência dos integrantes do ecossistema para garantir integridade, resultando em um efeito democrático da informação, onde não basta uma vontade unilateral de um indivíduo no controle, e sim do acordo dos demais integrantes.



Fonte: Santander Innoventures (2018, p. 14).

Além da descentralização do controle da informação, as *Blockchains* contam com mais uma medida de segurança, com os *ledgers,* ou livros-razão. *Ledgers* distribuídos são dados compartilhados, replicados e sincronizados espalhados digitalmente pelos integrantes da rede. Este documento virtual é encriptado e protegido contra qualquer revisão e alteração da informação nele contida. Cada integrante da rede, os blocos, contém *hashes* que vinculam e indicam informação importante na base de dados. Esses blocos de informações são visíveis e qualquer participante que conceda seu poder computacional ao sistema tem acesso.

Cada bloco processa cada transação utilizando as instruções em seus livros-razão, atingindo as próprias conclusões e depois fazendo uma votação com a conclusão. Depois, com a maioria dos integrantes atingindo uma mesma conclusão, o consenso é atingido e o *ledger* distribuído é atualizado com essa conclusão, e cada integrante mantém o seu *ledger* idêntico. Assim, as máquinas estão sempre sincronizadas e a desconexão de algum bloco da rede não afeta o sistema.

Essa rede de integrantes pode ser pública ou privada, mantendo a diferença na arquitetura e disposição dos *ledgers*. Nas redes públicas, como é o caso das criptomoedas, um único *ledger* é compartilhado pela rede e é acessível por todos que participam. A rede de computadores então compete para processar transações, processo chamado de mineração.

As redes privadas também contém apenas um único *ledger*, porém somente os participantes selecionados podem verificar dados além dos próprios registros. A rede é executada por administradores que controlam a quantidade e disponibilidade dos integrantes.

As criptomoedas serviram de um experimento social (incluir citação de Robert Shiller) sobre a integridade da tecnologia de *blockchain*. Os principais problemas de segurança reportados a respeito das criptomoedas são de sistemas construídos fora da rede, ao redor, como serviços que oferecem carteiras virtuais que são constantemente alvos de ataques.

Assim, mesmo com a concepção inicial das *Blockchains* para trocas financeiras, elas apresentam características que dão oportunidades para aplicação em outras áreas. Em especial, características como a confiabilidade dos dados registrados provenientes da eliminação de partes intermediárias, transparência na consulta desses dados e consistência garantida com os *ledgers*, e a confiabilidade do sistema, resultante da descentralização da rede, que dificulta instabilidades de infraestrutura e ataques maliciosos.

**O SISTEMA ELEITORAL BASEADO EM BLOCKCHAINS**

A eleição democrática se baseia na ideia de que cada cidadão representa um voto e que o direito do voto é universal. Para garantir essas qualidades a contagem dos votos e a acessibilidade do eleitor em registrar seu voto são fundamentais. As urnas eletrônicas atualmente implementadas não são suficientes na garantia da democracia, e a tecnologia *Blockchain* pode ser a solução.

A Estônia, em 2005, implementou sistemas de votação *on-line* através da *Internet*. *Internet voting*, ou *i-Voting¹[[1]](#footnote-1)* é o sistema que permite que eleitores registrem seus votos de qualquer computador desde que esteja conectado à *Internet* em qualquer parte do mundo.

A Aliança Liberal da Dinamarca, em 2014, foi o primeiro partido político a implementar a *Blockchain* em um sistema de votação[[2]](#footnote-2), sendo utilizada em uma votação interna em Hvidovre, ocorrida em Copenhague.

Também existem *startups* que propõem a implementação de *Blockchains* em sistemas de votação, como é o caso da *Follow my Vote[[3]](#footnote-3)* e *Bit Congress[[4]](#footnote-4)*.

Em território brasileiro, a primeira aplicação da *Blockchain* para sistemas de votação é o aplicativo para celulares Mudamos+ do Instituto de Tecnologia e Sociedade do Rio (ITS).

Com a introdução da tecnologia na política, abre-se um infinito de oportunidades para construção de novas formas de participação da população. A *Internet* é uma poderosa ferramenta para informar os cidadãos e cidadãs sobre como estes podem participar mais ativamente da vida política de seu bairro, cidade, estado e país.

(Instituto de Tecnologia e Sociedade do Rio (ITS), Projetos de lei de iniciativa popular no Brasil (2017); Disponível em <https://bit.ly/2HGk8Tl >; Acesso em 2018)

No caso do sistema eleitoral brasileiro, a *blockchain* teria uma autoridade central, a Justiça Eleitoral, e portanto seria uma *blockchain* privada, diferente da *Bitcoin* que é pública.

**CONCLUSÃO**

A tecnologia *Blockchain* para a evolução e refinamento do sistema eleitoral e democrático brasileiro não é uma idéia para um futuro distante. Diferente do que se pensa, a tecnologia já existe e já foi experimentada com aplicações semelhantes.

A nova era da informação e as pesquisas realizadas com as *Blockchains* garantem que a tecnologia resulte em maior respeito à opinião do eleitor, manifestada pelo seu voto, quando comparada com o atual modelo das urnas eletrônicas no Brasil.

**REFERÊ NCIAS**

ARANHA, D. F. et al. *Vulnerabilidades no software da urna eletrônica brasileira.* In: DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO (CIC/UnB), CENTRO DE INFORMÁTICA (CPD/UnB) - UNIVERSIDADE DE BRASÍLIA , 2013, Brasília.

ALECRIM, E. *O que é Blockchain: significado e funcionamento*, 2017. Disponível em: <https://bit.ly/2T5G67w >. Acesso em: 2018.

ARRUDA, Guilherme Oliveira. *A Tecnologia A Serviço Da Democracia: O Processo Eleitoral Na Era da Informação.* Revista da Advocacia Pública Federal, setembro 2018.

COMETTI, Natalia Paola de Vasconcelos. *Um Estudo Sobre A Tecnologia Blockchain e Sua Aplicação Em Sistemas de Votação.* 1. ed. Recife: Universidade Federal de Pernambuco, janeiro de 2016. Ciência da Computação – Centro de Informática da Universidade Federal de Pernambuco.

TAPSCOTT, Don: TAPSCOTT, Alex. *Blockchain Revolution: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo.* São Paulo: SENAI-SP Editora, 2016.

1. *iVoting*; Disponível em <<https://bit.ly/2CTyyQR>>; Acesso em 2018 [↑](#footnote-ref-1)
2. *Danish political party unleashes blockchain voting;* Disponível em <https://bit.ly/2JYQWbi/>; Acesso em 2018. [↑](#footnote-ref-2)
3. *Follow my Vote;* Disponível em <https://bit.ly/1Bhm1PC>; Acesso em 2018. [↑](#footnote-ref-3)
4. *Bit Congress;* Disponível em <https://bit.ly/2Har1Lc>; Acesso em 2018. [↑](#footnote-ref-4)