# O Uso de Blockchain em Eleições: Análise sobre as possíveis vulnerabilidades

REVISTA ELETRÔNICA MULTIDISCIPLINAR
UNIFACEAR

Nicolas Addor
*Pontifícia Universidade Católica do Paraná*

**RESUMO**
O presente trabalho pretende analisar, de forma crítica, a inciativa de se utilizar a tecnologia blockchain em eleições. Inicialmente, é necessário apresentar o contexto e a metodologia utilizada. Trata-se em um projeto de pesquisa em andamento, feito pelo autor com objetivo de uma futura publicação em periódico. Utilizou-se de metodologia hipotético-dedutiva, buscando fontes bibliográficas para o embasamento teórico. A ideia transmitida pelo blockchain é a desnecessidade de identidades emitidas centralmente (como CPF ou RG). Os usuários utilizam, ao contrário, uma chave digital única e intransferível, que não as identificam e que serviria como um conta digital. Fato é que essa chave pode ser criada a qualquer momento e, caso seja perdida, não há a possibilidade de recuperá-la. Isso obrigaria camadas adicionais de tecnologia para permitir a identificação e validação dos votos dos eleitores, bem como garantir o escrutínio secreto e a verificação do registro do voto. Além disso, para tentar solucionar a problemática de acesso do eleitor a sua chave digital, que o privaria de seu direito ao voto, seria necessário um controle, ao menos em parte, de bancos de dados que associem a chave ao eleitor, o que implicaria na necessidade de autoridade ou autoridades centrais para servir como validador, fato que afastaria a ideia de privacidade do usuário e, ao mesmo tempo, voltaria na problemática que o blockchain tenta solucionar, que é a fraude de eleições por estar à mercê de administradores que podem decidir quais votos serão contados. Dessa maneira, a tecnologia pode funcionar perfeitamente como simples registro de votos, mas para associá-los aos eleitores, a ideia por trás da tecnologia deveria que ser deturpada.

*Palavras chave:* Eleições; Blockchain; privacidade; identidade; fraude eleitoral.

***ABSTRACT***
*The paper intends to analyze, critically, the initiative of using blockchain technology in elections. Initially, it is necessary to present the context and methodology used. This is an ongoing research project, done by the author for the purpose of a future publication in a journal. It was used a hypothetical-deductive methodology, searching for bibliographic sources for the theoretical basis. The idea conveyed by the blockchain is the lack of centrally issued identities (such as CPF or RG). Users, on the other hand, use an unique, non-transferable digital key that does not identify them and serve as a digital account. The fact is that this key can be created at any time and if it is lost there is no possibility of recovering it. This would require additional layers of technology to enable identification and validation of voters' votes, as well as ensuring the secret ballot and verification of voter registration. In addition, in order to solve the problem of voters' access to their digital key, which would deprive them of their right to vote, it would require a control at least in part of databases that associate the key with the voter, which would imply the need for authority or central authorities to serve as a validator, a fact that would remove the idea of user privacy and, at the same time, return*

*to the problem that the blockchain tries to solve, which is the election fraud because it is at the mercy of administrators who can decide which votes will be counted. In this way, the technology can work perfectly as simple registration of votes, but to associate them with the voters, the idea behind the technology should be misrepresented.*
*Key Words: Elections; Blockchain; privacy; identity; electoral fraud.*

## 1. INTRODUÇÃO

As transformações tecnológicas que se propagaram nas décadas iniciais do século XXI faz vivenciar e provocar discussões sobre as relações sociais e tradições anteriormente enraizadas na sociedade. Entende-se que a sociedade perpassa pela quarta revolução industrial, que é, para Klaus Schwab, o evento onde ocorre a interação dos domínios físicos, digitais e biológicos. Complementa, ademais, que "nessa revolução, as tecnologias emergentes e as inovações generalizadas são difundidas muito mais rápida e amplamente do que nas anteriores, as quais continua a desdobrar-se em algumas partes do mundo">.[1]

Nesse mesmo sentido, Manuel Castells, em anos anteriores, também contextualiza:

> O cerne da transformação que estamos vivendo na revolução atual refere-se às tecnologias de processamento de informação e comunicação. A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor à vapor à eletricidade, aos combustíveis fósseis e até mesmo à energia nuclear, visto que a geração e a distribuição de energia foram o elemento principal na base da sociedade industrial.[2]

É sabido que a tecnologia blockchain surgiu sob o contexto do uso de criptomoedas, especialmente com a difusão do bitcoin. A revolução por detrás das moedas digitais merece destaque: ela objetiva garantir maior segurança, retirar intermediários, diminuir as taxas e assegurar a transparência e, ao mesmo tempo, a privacidade nas transações bancárias que são realizadas na rede.

É possível conceituar a tecnologia blockchain como uma espécie de "livro-razão" distribuída e controlada de forma descentralizada por uma infinidade de computadores. Sem um intermediário ou uma autoridade central fiscalizando e participando das transações, a tecnologia nascente afirma que possibilita dar mais segurança aos usuários, além de reduzir os custos e evitar fraudes bancárias.

[1] SCHWAB, Klaus. **A quarta revolução industrial.** São Paulo: Edipro, 2016. p. 16 – 17.
[2] CASTELLS, Manuel. **A sociedade em rede.** 18. ed. São Paulo: Paz&Terra, 2017. p. 88.

Dessa maneira, a tecnologia da criptomoeda considera que o pagamento, feito de forma eletrônica, "seja baseado em prova criptográfica em vez de confiança, permitindo que duas partes interessadas negociem diretamente entre si sem a necessidade de um terceiro confiável. As transações que são computacionalmente impraticáveis de reverter protegeriam os vendedores de fraude e mecanismos de depósito de rotina poderiam ser facilmente implementados para proteger os compradores."[3]

O grande pilar para a existência da tecnologia blockchain é a criação e difusão da internet na sociedade em geral. De fato, a teia mundial (*world wide web*), organizou os sítios da internet por informação e não por localização e ofereceu aos usuários um sistema fácil de pesquisa para a procura das informações desejadas.[4]

Foi com a tecnologia comunicacional em rede que se maximizou as chances para a expressão e mobilização de projetos alternativos que emergiram da sociedade para desafiar as autoridades.[5] Realmente, com o advento da internet, novas formas de negócio emergiram, meios de comunicação tiveram que ser alterados, milhares de novos *playes* entraram em setores econômicos tradicionais e não tradicionais.

Para Castells, "A rápida difusão da internet a partir de meados dos anos 1990 em diante resultou na combinação de três fatores: a descoberta tecnológica da grande rede de computadores; a mudança institucional no gerenciamento da internet; as grandes mudanças no comportamento cultural e social: individuação e interligação."[6]

---

[3] No idioma original: *"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."* Em: NAKAMOTO, Satoshi. **Bitcoin:** a peer-to-peer electronic cash system. Disponível em: <bitcoin.org/bitcoin>. Acesso em: 07 set. 2018, p.1.

[4] CASTELLS, Manuel. **A sociedade em rede.** 18. ed. São Paulo: Paz&Terra, 2017. p. 105.

[5] CASTELLS, Manuel. **O poder da comunicação.** 2. ed. São Paulo: Paz&Terra, 2017. p. 35.

[6] CASTELLS, Manuel. **O poder da comunicação.** 2. ed. São Paulo: Paz&Terra, 2017. p. 36 – 37.

## 2. ELEIÇÕES E BLOCKCHAIN

O poder político e a ordem social são elementos baseados na eficiência do controle exercido pelos atores dominantes sobre o processo de comunicação. Ele pode se dar a partir da pregação de um púlpito, linha editorial de um jornal ou mesmo a programação da televisão. Quanto maiores e mais verticais as organizações de comunicação forem, o envio de mensagens será cada vez mais concentrado, e mais o receptor da mensagem será individualizado e controlado.[7]

A exemplo da internet, "A difusão de redes de comunicação horizontal e os múltiplos pontos de entrada no sistema de comunicação local/global modificaram profundamente a prática de poder em várias dimensões institucionais e sociais, aumentando a influência da sociedade civil e de atores sociopolíticos não institucionais na forma e na dinâmica das relações de poder."[8]

Vislumbrado o potencial uso da tecnologia, viu-se movimentos iniciais, com o fim de assegurar eleições mais seguras, de utilizar o blockchain como uma nova tecnologia de controle e contagem de votos. Como exemplo, o estado de Virgínia Ocidental[9], nos Estados Unidos, realizou os primeiros testes com um grupo seleto de eleitores, tendo uma experiência positiva.

Em outro exemplo, em Serra Leoa, mais especificadamente na região da capital do país, as eleições presidenciais foram feitas com o apoio do blockchain para autenticar as eleições. Uma empresa privada de origem Suíça foi contratada para esse serviço. No caso, na capital de Serra Leoa, "os votos foram registrados como blocos em um arquivo de blockchain privado mantido pelo sistema eleitoral do país. Apenas pessoal autorizado tinha acesso a esse arquivo, e qualquer modificação nesse sistema deixaria rastros."[10]

O voto seria exercido por meio de uma chave privada, por onde seria enviada a declaração do voto e a escolha do candidato. Os eleitores, no caso, terão o único

---

[7] CASTELLS, Manuel. **O poder da comunicação.** 2. ed. São Paulo: Paz&Terra, 2017. p. 32.
[8] CASTELLS, Manuel. **O poder da comunicação.** 2. ed. São Paulo: Paz&Terra, 2017. p. 34.
[9] **EUA: Virgínia Ocidental conclui primeiras eleições estaduais apoiadas no blockchain.** Disponível em: <https://br.cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections>. Acesso em: 08 set. 2018.
[10] MULLER, Leonardo. **Primeira eleição do mundo auditada por blockchain é realizada em Serra Leoa.** Disponível em: **<**https://www.tecmundo.com.br/software/128285-primeira-eleicao-mundo-auditada-blockchain-realizada-serra-leoa.htm>. Acesso em: 07 set. 2018.

dever de se responsabilizar em resguardar tal conta para deter o direito ao voto e fiscalizar qual foi a escolha eleitoral realizada.[11]

## 3. PROBLEMÁTICAS OCULTAS

Apesar da tecnologia blockchain ser uma tentativa bastante promissora de dar para as atividades práticas do dia-a-dia um controle descentralizado, é incipiente afirmar que sua inserção, sem qualquer precaução, não acarretará quaisquer problemáticas.

É necessário advertir: “Em meio a crescente ideia de inovação nas tecnologias digitais, em especial o blockchain, verificam-se passagens de enunciações aquém de seu âmbito funcional e fático. Diversos artigos e publicações não realizam a adequada análise deste instituto e reproduzem eventuais características que não são compatíveis esse instituto” [sic].[12]

Algumas afirmações que são necessárias maiores reflexões são:

- A ideia de que Blockchain ser *trusless*. Em outras palavras, é afirmação de que não é necessária a confiabilidade entre os usuários que utilizam do sistema. “É fato que as operações realizadas via Blockchain reduzem a necessidade de confiança entre as partes, porém não a elimina completamente”.[13] A confiança nos operadores partícipes e na criptografia utilizada ainda são pré-requisitos subjetivos para a utilização.

- A ideia de que o Blockchain é imutável. Existe a possibilidade de mutabilidade desde que haja um conflito entre a validação de um número relativo de usuários e a informação a ser checada, haverá a incompatibilidade e possivelmente ocorrerá a exclusão dos blocos conflitantes. Em outra situação, no caso de um sistema blockchain privado, os operadores podem utilizar de um significativo recurso computacional para reescrever a criptografia.[14]

---

[11] LEE, Kibin *et al.* Electronic voting service using block-chain. **Journal of digital forensics, security and law,** v.11, n.2, p.123-136, 2016, p.128.

[12] DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios.**RJLB,** a. 3, n. 6, p.2771 – 2808, 2018. p. 2779.

[13] DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios.**RJLB,** a. 3, n. 6, p.2771 – 2808, 2018. p. 2779.

[14] De acordo com entendimento de Sthéfano B. S. Divino, em concordância com Garrick Hileman e Michael Rauchs. DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios.**RJLB,** a. 3, n. 6, p.2771 – 2808, 2018. p. 2779 – 2780.

- A ideia de que o Blockchain é inviolável. Apesar da utilização em massa de criptografia, a mera aplicação de códigos matemáticos não torna o sistema totalmente seguro. Caso comprometida uma das chaves privadas de alguns dos participantes da rede, a possibilidade de todo aquele banco de dados em que ele fora desenvolvida ser alvo de ataques e modificações é eminente.[15]

- A ideia de que o Blockchain é o meio que garante a veracidade. “Ocorre que nas transações realizadas via Blockchain não há a checagem de seu conteúdo para afirmar a veracidade ou precisão dos dados informacionais que compõem o bloco. Portanto, o blockchain verificará apenas os procedimentos formais e objetivos para a validação da informação inserida”.[16]

Assim, o uso da tecnologia em eleições deve ser visto com cautela. Isso porque, como assenta Jesse Dunietz[17], a tecnologia pode funcionar perfeitamente como simples registro de votos. No entanto, há algumas problemáticas que a tecnologia blockchain não resolveria em sua utilização específica nas eleições:

a) a chave privada digital, de acordo com a tecnologia de acesso aberto do blokchain, pode teoricamente ser criada a qualquer momento;

b) caso a chave privada seja perdida por qualquer motivo, não haveria a possibilidade de recuperá-la;

c) Em razão da necessidade de controle de registro e segurança em caso de perda de chaves privadas, os Estados se veriam obrigados a estabelecer camadas adicionais de tecnologia para permitir a identificação e validação dos votos dos eleitores, bem como garantir o escrutínio secreto e a verificação do registro do voto;

d) Além disso, para tentar solucionar a problemática de acesso do eleitor a sua chave digital, que o impediria de exercer seu voto, o que forçaria algum tipo de controle dos bancos de dados que associem a chave ao eleitor, bem como invalide a chave olvidada, fato que implicaria na necessidade deter uma autoridade ou um

---

[15] De acordo com entendimento de Sthéfano B. S. Divino, em concordância com Garrick Hileman e Michael Rauchs. DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios.**RJLB,** a. 3, n. 6, p.2771 – 2808, 2018. p. 2780.

[16] De acordo com entendimento de Sthéfano B. S. Divino, em concordância com Garrick Hileman e Michael Rauchs. DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios.**RJLB,** a. 3, n. 6, p.2771 – 2808, 2018. p. 2780-2781.

[17] DUNIETZ, Jesse. **Are blockchains the answer for secure elections? Probably not.** Disponível em: <https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probablynot/?utm_source=twitter&utm_medium=social&utm_campaign=sa-editorial-social&utm_content=&utm_term=tech_news_text_&sf195670481=1>. Acesso em: 07 set. 2018.

agrupamento de autoridades centrais para servir como validador e controlador das chaves privadas.

e) Visto que a necessidade de uma autoridade central seria premente para assegurar a idoneidade do processo, isso afastaria a ideia de privacidade do usuário, algo basilar na proposta das criptomoedas;

f) Ademais, volta-se ao problema o blockchain tenta solucionar, que é retirar a necessidade de ter uma terceira pessoa no ato de transação eletrônica, para verificação. Outrossim, com uma autoridade central, o sistema estará novamente à mercê de administradores, que podem decidir quais votos serão contados;

## 4. CONSIDERAÇÕES FINAIS

Apesar de defender que o blockchain é uma tecnologia inovadora para buscar descentralizar a tomada de decisão, a utilização em eleições democráticas deve ter cautelas, pois seria necessário, por exemplo, vincular a conta e o voto a um eleitor, o que exigiria um banco central para checagem dos dados. Tal situação, que é imperiosa para uma eleição sem fraudes, segue o sentido contrário da ideia de privacidade das transações e desnecessidade de intermediários que a tecnologia promete.

## 4. REFERÊNCIAS


CASTELLS, Manuel. **A sociedade em rede.** 18. ed. São Paulo: Paz&Terra, 2017.

CASTELLS, Manuel. **O poder da comunicação.** 2. ed. São Paulo: Paz&Terra, 2017.

DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios.**RJLB,** a. 3, n. 6, p.2771 – 2808, 2018.

DUNIETZ, Jesse. **Are blockchains the answer for secure elections? Probably not.** Disponível em: < https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probablynot/?utm_source=twitter&utm_medium=social&utm_campaign=sa-

editorial-social&utm_content=&utm_term=tech_news_text_&sf195670481=1>. Acesso em: 07 set. 2018.

**EUA: Virgínia Ocidental conclui primeiras eleições estaduais apoiadas no blockchain.** Disponível em: <https://br.cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections>. Acesso em: 08 set. 2018.

MULLER, Leonardo. **Primeira eleição do mundo auditada por blockchain é realizada em Serra Leoa.** Disponível em: <https://www.tecmundo.com.br/software/128285-primeira-eleicao-mundo-auditada-blockchain-realizada-serra-leoa.htm>. Acesso em: 07 set. 2018.

NAKAMOTO, Satoshi. **Bitcoin:** a peer-to-peer electronic cash system. Disponível em: <bitcoin.org/bitcoin>. Acesso em: 07 set. 2018.

LEE, Kibin *et al.* Electronic voting service using block-chain. **Journal of digital forensics, security and law,** v.11, n.2, p.123-126, 2016.

SCHWAB, Klaus. **A quarta revolução industrial.** São Paulo: Edipro, 2016.