ISSN 2675-9934

# Boletim de Políticas Públicas

Observatório Interdisciplinar de Políticas Públicas «Prof. Dr. José Renato de Campos Araújo» (EACH/USP)

№20 março/2022

OIPP

# Potenciais aplicações e benefícios na utilização de sistemas blockchain para a gestão pública

**Anderson Ribeiro[29], José Carlos Vaz[30]**

## 1. Introdução

A tecnologia *blockchain*, tem se mostrado fundamental para a gestão de transações financeiras, sobretudo no mercado de trocas de moedas digitais, conhecidas popularmente como criptomoedas. Nos últimos tempos, eclodiram uma série de discussões sobre outras possíveis aplicações, sobretudo para a gestão de dados massivos. Tais discussões alcançam também o setor público. Como por exemplo, em 2019, quando o Tribunal Superior Eleitoral (TSE) publicou o 3º Volume dos Estudos Eleitorais[31], com o seguinte tema: ''A segurança da democracia e o *blockchain*'', apresentando uma contribuição ao debate sobre a aplicação desta tecnologia, para dados públicos e prestação de serviços de governos. Pensando nisso, o Grupo de Estudos de Tecnologia e Inovação para a Gestão Pública (GETIP) e o Observatório Interdisciplinar de Políticas Públicas "Prof. José Renato de Campos Araújo" (OIPP) buscam entender os potenciais usos, benefícios e capacidades demandadas para a aplicação de sistemas baseados em *blockchain* na gestão pública. Esses esforços se configuram em uma iniciativa de pesquisa, apresentada neste artigo, juntamente com os primeiros resultados produzidos.

29 Discente de Gestão de Políticas Públicas da EACH-USP e de Direito da FADISP. Pesquisador associado ao GETIP e OIPP.
30 Doutor em Administração, professor do curso de Gestão de Políticas Públicas da EACH-USP, coordenador do GETIP e pesquisador do OIPP.
31 Tribunal Superior Eleitoral. Estudos eleitorais. vol. 13, n. 2. 2019. Disponível em: http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/5852

## 2. O que é blockchain

A tecnologia *blockchain* foi pensada para tornar possível negociações na internet, sem que houvesse a necessidade de uma conexão real entre os negociantes ou um terceiro interlocutor, apenas a validação pela própria rede. Em outubro de 2008 foi publicado, sob o pseudônimo de Satoshi Nakamoto, o primeiro documento[32] sobre a tecnologia, onde se apresentoua prova de conceito necessária, para que em 2009 fosse desenvolvido o primeiro sistema baseado em *blockchain*, dando origem a primeira moeda digital, popularmente conhecido como Bitcoin (BTC),

Desde então, surgiram centenas de iniciativas de implementação de redes *blockchain* que originaram centenas de tipos de cripto-ativos, que são comprados e vendidos aos milhares em *exchanges* (plataformas de negociação digitais), criando um ecossistema de negociação milionário. Essas negociações são possíveis uma vez que a rede é programada para processar e validar milhares de transações por segundo, garantindo que tudo o que for definido como necessário será estritamente checado, sendo facilmente identificável as transações que não cumprirem os requisitos estabelecidos pela rede (Pinhão, 2018).

A seguir, serão abordadas as principais características dos sistemas *blockchain,* que permitem a construção de uma rede de dados imutável e altamente verificável.[33]

**a) Chaves de acesso (pública e privada):** funcionam como autorizações, necessárias para a para a validação das informações na rede. A tecnologia usualmente utilizada se baseia em RSA, embora existam outros modelos de aplicação criptográfica que podem ser explorados (VALID, 2019[34]). A chave privada é análoga

32 NAKAMOTO. S. Bitcoin: a Peer-to-Peer Electronic Cash System. 2008. Acesso em 25 de Janeiro de 2022. Disponível em: http://users.encs.concordia.ca/~clark/biblio/bitcoin/Nakamoto%202008.pdf

33 Nota: não é objetivo deste trabalho aprofundar-se nos detalhes técnicos do funcionamento dos sistemas, que podem ser obtidos em dois trabalhos, denominados ''A systematic review of blockchain'' (Chen, 2019) e ''Blockchain Technology Overview'' (Yaga, 2018).

34 VALID. C. Os 10 tipos mais utilizados de criptografia. Cryptoid. 2019. Acesso em 03 de Fevereiro de 2022. Disponível em: https://cryptoid.com.br/valid/tipos-de-

a uma assinatura digital, que permite o acesso e certifica a ciência do usuário sobre suas transações, existindo apenas uma chave por usuário, sendo única cada assinatura digital. A chave pública, por sua vez, é o acesso utilizado pela própria rede para fazer a checagem e confirmação ou negativa dos dados daquela transação (Olnes, 2017). Essas chaves fazem a encriptação e decriptação[35] das informações, tornando possível o envio dos dados de maneira segura e sigilosa dentro da rede.

**b) Blocos com criptografia (HASH) encadeados:** trata-se da principal característica responsável por tornar o sistema imutável. A partir de seus protocolos de assinaturas digitais, explicados no capítulo anterior, é atribuída uma sequência criptográfica que serve como um identificador daquele dado na rede (Carback, 2019). Esses registros de identificação digitais são chamados de Hashes, e são determinados pelo conteúdo daquele bloco, e colocados em uma sequência encadeada, na qual o endereço do bloco anterior guarda estrita relação com o do bloco posterior e assim sucessivamente. Considerando que é feita uma transação denominada de **A**, ela irá gerar um **HASH A,** e será armazenada no sistema, quando for feita uma segunda transação, chamada de **B**, o **HASH B** será o produto de **HASH A + HASH B,** *ad infinitum*. Este processo de identificação sincronizada dos dados na rede é chamado de efeito cascata, onde o sistema automaticamente isola as alterações maliciosas, protegendo o conjunto de dados que se seguem naquela cadeia, dando ao sistema características imutáveis. O Hash mais utilizado pelas redes *blockchain* ao redor do mundo é o SHA256, que resume a informação do bloco em um código de 64 caracteres, entre letras e números (Gómez, 2019).

---

criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/#:~:text=O%20RSA%20funciona%20da%20seguinte,mas%20somente%20decifradas%20pela%20privada.

35 Nota: Encriptação e decriptação: Encriptar uma sequência de informações é atribuir para ela um certificado digital, transformando aquela informação em um código, possibilitando o transporte dos dados dentro de uma rede com segurança. Decriptação é o processo que funciona como uma espécie de tradução daquele código, tornando novamente possível a leitura do texto na linguagem humana.

**c) Contratos inteligentes e Protocolos de Consenso:** os contratos inteligentes são as regras definidoras do protocolo de consenso, que são parâmetros no qual se baseiam os algoritmos validadores rede, para garantir que os blocos não contenham transações inválidas (Alketbi, 2021). São as métricas que os algoritmos da validação, chamados de ‘’nós’’ ou “elos”, vão se basear para atribuir legitimidade a uma transação. Os ‘’*smart contracts*’’ são definidos no processo de construção da rede e só podem ser alterados mediante a aprovação de 50% + 1 dos validadores ativos, garantindo uma camada a mais na garantia de legitimidade dos dados validados.

## 3. Elementos para a construção de um instrumento de análise do potencial de uso do blockchain no setor público

Foi conduzida uma revisão na literatura sobre *blockchain* e suas aplicações no setor público. A busca de textos relevantes teve como procedimentos o levantamento orientado por palavras-chaves nas plataformas: ‘’Google Acadêmico’’, ‘’Scielo’’, e no ‘’banco de dados de teses da USP’’. As palavras chaves utilizadas foram: ‘’blockchain’’, ‘’blockchain in government’’, ‘’blockchain applications’’ e ‘’blockchain implementation’’. Priorizou-se as discussões que tratavam da implementação no setor público, uma vez que parte da literatura discute os benefícios desta aplicação em sistemas relacionados ao mercado privado, sobretudo financeiro. Também houve prioridade na seleção de obras que abordassem casos práticos de utilização dessas redes por governos, além de textos publicados em outros meios além de periódicos acadêmicos, como relatórios e publicações técnicas especializadas.

O quadro abaixo apresenta uma sistematização das análises de possíveis aplicações agrupadas por tipos de uso, empregando como categorias analíticas: benefícios gerados; direitos promovidos; atributos utilizados e órgãos públicos diretamente envolvidos, além de identificar as referências encontradas na literatura.

Quadro 01 - Possíveis aplicações do blockchain na gestão pública

| Tipos de uso | Aplicação | Benefícios / Direitos | Principais atributos utilizados | Órgãos públicos diretamente envolvidos | Autor(a) / Referências |
|---|---|---|---|---|---|
| **Registro de dados Públicos estáveis** | Criação de documentos identidade de (ID) | Proteção contra falsificações;<br><br>Sistema de verificação dinâmico descentralizado | Alta verificabilidade<br><br>imutabilidade<br><br>integração e cruzamento de dados | Secretarias do desenvolvimento econômico | ALKETBI. A. et al.[36]<br><br>OLNES. S. et al.[37] |
| | Registros de títulos imobiliários | Velocidade no processo de validação dos dados para registro de imóveis<br><br>Facilidade de verificação do registro por terceiros | Alta verificabilidade<br><br>Imutabilidade<br><br>Validação dos dados | Secretarias de habitação | JANSSENS. A. [38]<br><br>JORGE. V. et al.[39] |
| | Registros Eleitorais | Registro independente dos votos<br><br>Verificação da cadeia de contagem | Imutabilidade<br>Alta verificabilidade<br>Validação dos dados<br>Descentralização | Tribunal Superior Eleitoral - TSE | KIM, p et al.[40]<br><br>SILVA. M.[41]<br><br>TARASOV. P. et al.[42] |

36ALKETBI. A. et al. Blockchain for Government Services – Use Cases, Security Benefits and Challenges. University of Sharjah. Sharjah. 2019. Acesso em 02 de Fevereiro de 2022. Disponível em: https://ieeexplore.ieee.org/document/8368494

37 OLNES. S. et al. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. ScienceDirect. 2017. Acesso em 03 de Fevereiro de 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0740624X17303155

38 JANSSENS. A. The Use and Acceptance of Blockchain Technology for Land Registration. Thesis - Business information Management. São Paulo. 2019

39 JORGE. V. et al. Implementação da tecnologia disruptiva do blockchain no enfrentamento à corrupção. Enfrentamento da Corrupção e Investigação Criminal Tecnológica. São Paulo. 2020. Acesso em 03 de Fevereiro de 2022. Disponível em: https://www.higorjorge.com.br/wp-content/uploads/2020/08/amostra-enfrentamento-da-corrupcao-inv-crim-tecn.pdf

40 KIM p et al. E2E verifiable blockchain voting system using homomorphic encryption. Journal Of Critical Reviews. 2020. Acesso em 01 de fevereiro de 2022. Disponível em: https://www.researchgate.net/publication/356083929_E-voting_System_Using_Homomorphic_Encryption_and_Blockchain_Technology_to_Encrypt_Voter_Data

41 SILVA. M. **A segurança da Democracia e o Blockchain.** Caderno de Estudos Eleitorais do TSE. vol. 13. 2019. Acesso em 02 de fevereiro de 2022. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/5961

42 TARASOV. P. et al. **The future of E-voting.** School of Computer Science and Statistics, Trinity College Dublin, University of Dublin, Ireland. 2019. Acesso em: 01 de fevereiro de 2022. Disponível em: https://www.researchgate.net/publication/321803764_THE_FUTURE_OF_E-VOTING

| | | | | | |
|---|---|---|---|---|---|
| | | Registros imutáveis | | | |
| **Registro de dados públicos dinâmicos** | Plataforma unificadas com dados sociais | Integração de dados para priorização na adoção de políticas<br><br>oferecimento de serviços pelo cruzamento de dados (análise de crédito, por exemplo) | imutabilidade<br><br>integração e cruzamento de dados<br><br>validação dos dados | Secretárias de assistência social | HENG. H.[43] |
| | Validação contratos licitatórios | identificação de incongruências no processo<br><br>Facilidade na verificação dos dados | descentralização<br><br>integração e cruzamento dos dados<br><br>Imutabilidade<br><br>validação dos dados | Controladorias e Órgãos de fiscalização internos | JORGE. V. et al.<br><br>OLNES. S. |
| | Gestão da saúde clínica e preventiva | Registros dinâmicos e autenticados do quadro clínico | descentralização<br><br>integração e cruzamento de dados | Secretarias da Saúde | HOLBI. M. et al.[44] |

Observou-se dois grandes grupos de tipos de uso para a tecnologia: O primeiro grupo advém da necessidade de se armazenar registros públicos por um longo período de tempo, tornando aquele dado imutável e de fácil verificação interna e externa. O segundo grupo consiste em registros que precisam ser atualizados em um curto período de tempo, onde os algoritmos contidos na *blockchain* são uma opção considerável de gestão dinâmica dessas informações, levando-se em conta a capacidade de validação da rede.

---

[43] HENG. H. **The Application of Blockchain Technology in E-government in China**. School of Information Management, Sun Yat-sen University. Guangzhou, China. 2016. Acesso em 02 de fevereiro de 2022. Disponível em: https://ieeexplore.ieee.org/document/8038519

[44] HOLBI. M. et al. **A systematic Review of the use of blockchain in Healthcare.** Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor 2000. Acesso em 01 de fevereiro de 2022. Disponível em: https://www.researchgate.net/publication/328208535_A_Systematic_Review_of_the_Use_of_Blockchain_in_Healthcare#:~:text=The%20findings%20indicate%20that%20blockchain,of%20frameworks%2C%20architectures%20or%20models.

### 3.1 Registros de dados públicos estáveis

A categoria dos registros públicos estáveis compreende todas as transações que geram um único tipo de registro, podendo servir como base legítima para outros processos governamentais como exemplificado no texto do autor chamado Ahmedi Alketbi (2019), no qual é relatada uma colaboração entre o Governo da Estônia e uma empresa chamada ‘’Bitnation’’ que possibilitou o uso de blockchain para autenticar certidões de nascimento, testamentos, contratos comerciais com averbação em registro público e títulos de propriedade. Os títulos de propriedades também tiveram destaque na literatura em análise, como no o texto de Anne Janssens (2019), no qual a autora argumenta que a tecnologia pode possibilitar a criação de um único histórico imutável dos títulos de propriedades, a um custo e tempo reduzidos, se comparado ao modelo tradicional adotado pelos cartórios de registro de público.

Os estudos de sistemas eleitorais também se utilizaram do tema, produzindo apontamentos encontrados nas obras de Hyunyeon Kim (2020), e no 13º volume do Caderno de Estudos Eleitorais do Tribunal Superior Eleitoral - TSE (2019). Ambos apontam critérios de viabilidade técnica para a integração no sistema eleitoral, dando força à hipótese de criação de um sistema blockchain gerido pelo TSE, que pode se beneficiar das características de imutabilidade e auditabilidade nas operações realizadas, tendo potencial para a ampliar o acompanhamento e credibilidade da população no processo eleitoral.

### 3.2 Registros de dados públicos dinâmicos

A categoria dos registros públicos dinâmicos, compreende os dados que precisam ser atualizados constantemente, demandando uma alta capacidade de escala na validação das informações. De acordo com a literatura observada, a alocação de informações em um sistema blockchain pode servir como um banco de dados

eficiente para cruzamento de informações que necessitem alto grau de verificabilidade, como por exemplo a experiência chinesa relatada no texto do autor chamado Heng Hou (2016), no qual o governo criou um sistema de monitoramento da qualidade dos produtos ofertados nas feiras e mercados, com parte de uma política de incentivo à boa alimentação, onde as informações relatadas pelas empresas eram checadas pela rede e então divulgadas aos órgãos competentes e aos cidadãos

Outro tema recorrente na literatura é a utilização dos contratos inteligentes para garantir o cumprimento dos princípios da administração pública, que são regulamentados por normas próprias, e dão legitimidade às operações que envolvem o Estado. Poderia ser empregada a tecnologia para validação de contratos licitatórios, o que poderia contribuir para a celeridade e padronização dos elementos que tornam legítimos essas operações que envolvem dinheiro público, como descrito no artigo com ênfase no uso da tecnologia para o combate à corrupção, de Higor Jorge (2020). Em sentido próximo, mas para outra finalidade o texto do autor Marko Houbi (2019), trabalha a ideia de utilização da rede para cuidar dos registros médicos, validando as informações a partir do cruzamento dos novos dados com as informações alocadas na rede em consultas anteriores, permitindo também a criação de um histórico capaz de contribuir na orientação dos tratamentos no sistema único de saúde (SUS).

Também podem-se observar os atributos do blockchain em relação as potenciais aplicações identificadas, conforme apresentado no quadro abaixo:

Quadro 02 - Correlação entre atributos do *blockchain* e possíveis aplicações

| **Aplicação** | **Características utilizadas** | | | | |
|---|---|---|---|---|---|
| | **Imutabilidade** | **Alta verificabilidade** | **Validação dos dados** | **Integração e cruzamento de dados** | **Descentralização** |
| Criação de documentos identidade de (ID) | **X** | **X** | **X** | | |
| Registros de títulos imobiliários | **X** | **X** | **X** | | |
| Registros Eleitorais | **X** | **X** | **X** | | **X** |
| Plataforma unificadas com dados sociais | **X** | | **X** | **X** | |
| Validação contratos licitatórios | **X** | | **X** | **X** | **X** |
| Gestão da saúde clínica e preventiva | | | | **X** | **X** |

Fonte: Elaboração própria.

Percebe-se que há uma predominância nas propostas de utilização do *blockchain* no que tange à imutabilidade e validação dos dados, sobretudo em registros estáveis. Há também uma correlação entre as características de integração e cruzamento nas atividades que envolvam dados dinâmicos. A descentralização se apresenta como mais evidente nos sistemas que envolvem dados sensíveis, que necessitam de controle e ciência por órgãos de controle internos e externos.

## 4. Considerações Finais

Neste trabalho, discutiu-se caminhos e benefícios que podem resultar da apropriação desta tecnologia pela gestão pública.

Porém, o aprofundamento da pesquisa deverá considerar os desafios de implementação desses sistemas. O primeiro desafio refere-se ao estabelecimento da confiança pública em sistemas autônomos, o que demanda uma compreensão das lógicas de validação da rede. De nada adiantaria investimento para a implantação de um sistema eleitoral baseado em *blockchain*, se a população não entendesse quais são os protocolos de segurança que garantam a imutabilidade dos votos. O primeiro desafio precede qualquer debate de natureza técnica, pois se trata de uma questão cultural. Outro desafio consiste no próprio desenvolvimento natural da tecnologia, que por ter potencial para mudar a forma como o Estado produz, armazena e processa informações para gestão e prestação de serviços, há uma série de iniciativas em desenvolvimento que buscam adaptar e aplicar os seus conceitos às necessidades públicas. No entanto, ainda há um longo caminho a ser percorrido para tornar possível a sua utilização no dia a dia da gestão pública.

Na continuidade da pesquisa, o presente modelo poderá ser empregado para avaliar as possibilidades de aplicação no sistema público para prestação de serviços e gestão de políticas, com base nas demandas específicas daquele sistema de transação. Buscar-se-á compreender também as capacidades estatais que precisam ser mobilizadas e aprimoradas para a implementação de sistemas de informações baseados em *blockchain* para uso do Estado e sociedade.

## Referências Bibliográficas

Bit2Me Academy. **O que é SHA-256?** Acesso em 04 de Fevereiro de 2022. Disponível em: https://academy.bit2me.com/pt/algoritmo-sha256-bitcoin/#:~:text=Outra%20peculiaridade%20do%20algoritmo%20de,codifica%C3%A7%C3%A3o%20de%20256%20bits%20e

GRIGORIEV. D. **RSA and redactable blockchains**. Eprint. 2022. Acesso em 02 de Fevereiro de 2022. Disponível em: https://eprint.iacr.org/2020/069.pdf

MARINS, L. **Administração pública precisa superar desafios para implantar tecnologia blockchain.** Livecoins. 2020. Acesso em 20 de Janeiro de 2022. Disponível em: https://livecoins.com.br/administracao-publica-precisa-superar-desafios-para-blockchain-diz-tcu/

PINHÃO. K. **Blockchain - Uma forma fácil de entender a tecnologia que mudará os mundos jurídico e financeiro**. P e K Advogados. 2018. Acesso em 02 de Fevereiro de 2022. Disponível em: https://direitoparatecnologia.com.br/blockchain-forma-facil-de-entender/

YAGA. D et al. **Blockchain technology overview.** National Institute of Standards and Technology of the U.S. Department of commerce. 2018.