Aplicabilidade do Blockchain no setor público

Luiz Miguel Santos Rodrigues
Fatec Praia Grande
luizmiguel.srodrigues@gmail.com

Profa. Me. Renata Neves Ferreira
Fatec Praia Grande
renata.ferreira@fatec.sp.gov.br

RESUMO

Nesse artigo apresentaremos o funcionamento básico da tecnologia *blockchain*, considerada uma das tecnologias mais promissoras da atualidade, e algumas iniciativas de possíveis aplicações no setor público. Buscaremos mostrar seu possível impacto, os benefícios de sua utilização, assim como os desafios a serem observados para implementação ampla desta tecnologia. Destacamos a ascensão da tecnologia *blockchain* como uma ferramenta disruptiva, indicando um crescente interesse e investimento no uso da tecnologia no setor público de vários países, apresentamos casos de uso específicos, como: o projeto de um sistema global de identificação de viajantes, iniciativa do Fórum Econômico Mundial, a desestatização do BNDES – Banco Nacional de desenvolvimento, projeto de iniciativa do BNDES, no Brasil, e o projeto americano para monitoração da saúde da população, iniciativa do Centro de Controle e Prevenção de Doenças (CDC) dos Estados Unidos. Conclui-se que a utilização da tecnologia *blockchain* tem potencial para aprimorar a execução de processos governamentais, mas ressaltamos a necessidade de esforços contínuos para superar obstáculos e maximizar seu potencial.

PALAVRAS-CHAVE: Blockchain, estratégia de negócios, algoritmos de consenso, inovação, governança.

ABSTRACT

In this article we will present the basic functioning of blockchain technology, considered one of the most promising technologies today, and some initiatives for possible applications in the public sector. We will seek to show its possible impact, the benefits of its use, as well as the challenges to be observed for the broad implementation of this technology. We highlight the rise of blockchain technology as a disruptive tool, indicating a growing interest and investment in the use of technology in the public

sector of several countries, analyzing specific use cases, such as: the project of a global traveler identification system, an initiative of the Forum World Economy, the American project to monitor the health of the population, an initiative of the Center for Disease Control and Prevention (CDC) in the United States, and the privatization of the BNDES – National Development Bank, a project initiated by the BNDES, in Brazil. It is concluded that the use of blockchain technology has the potential to improve the execution of government processes, but we emphasize the need for continuous efforts to overcome obstacles and maximize its potential.

KEYWORDS: *Blockchain, business strategy, consensus algorithms, innovation, governance.*

INTRODUÇÃO

A aplicação da tecnologia *blockchain* emergiu como uma inovação que transcende as fronteiras do setor financeiro e permeia diversas esferas da sociedade. Seu potencial para revolucionar os processos governamentais e a prestação de serviços públicos tem atraído crescente atenção de acadêmicos, especialistas e governos ao redor do mundo. Este artigo explora a utilização estratégica da tecnologia *blockchain* no contexto da administração pública, e será apresentado no seguinte formato: No capítulo 1, apresentamos uma análise do surgimento e evolução da tecnologia *blockchain*, destacando sua origem no movimento Cypherpunk; No capítulo 2, abordaremos uma visão geral da tecnologia *blockchain*, a evolução de sua maturidade e principais vantagens da sua aplicação; No capítulo 3, destacamos a iniciativas da aplicação de *blockchain* no setor público, apresentamos casos de uso específicos, como: o projeto de um sistema global de identificação de viajantes, iniciativa do Fórum Econômico Mundial, a desestatização do BNDES – Banco Nacional de desenvolvimento, projeto de iniciativa do BNDES, no Brasil, e o projeto americano para monitoração da saúde da população, iniciativa do Centro de Controle e Prevenção de Doenças (CDC) dos Estados Unidos, em seguida apresentamos os desafios para uma aplicação mais ampla no setor público. Por fim, no capítulo 4, apresentamos as considerações finais. A metodologia utilizada na elaboração deste

artigo foi baseada em pesquisa bibliográfica, estudo sistematizado desenvolvido com base em material publicado desde 2008, em livros, artigos e meios eletrônicos, cujo conteúdo seja coerente com o objetivo da análise.

1 O SURGIMENTO DA TECNOLOGIA BLOCKCHAIN: UMA ANÁLISE DA SUA EVOLUÇÃO E CONTRIBUIÇÃO DE DIVERSOS ATORES.

A tecnologia *blockchain* e seu complexo ecossistema, que compreende a criptografia como modo de descentralização, tem como base na apreciação pela liberdade, privacidade e transparência nas transações entre pessoas, iniciou-se na década de 1990, em que jovens entusiastas da criptografia, professores, matemáticos e *hackers*, se reunia principalmente em fóruns e listas de discussão na internet. Em 1993 foi publicada a lista de discussão cypherpunks@toad.com. Hughes (1993), menciona a importância do anonimato em seu manifesto Cypherpunk, definindo que. “Um sistema anônimo capacita os indivíduos a revelar sua identidade quando desejado e somente quando desejado, esta é a essência da privacidade”.

O movimento Cypherpunk é fortemente representado na comunidade de criptografia e é amplamente reconhecido como a força impulsora por trás do avanço da tecnologia *blockchain* e das criptomoedas, como o Bitcoin. Muitas das ideias e conceitos propostos pelos Cypherpunks ainda são atuais e influentes, abrangendo questões como: privacidade na era digital, segurança da informação e proteção contra a vigilância digital.

Um dos precursores do movimento Cypherpunk, foi David Lee Chaum, nascido em 1955, pesquisador, cientista da computação, e inventor americano, foi um entusiasta e precursor da tecnologia. Chaum (1981), propôs um sistema de votação confiável para eleições públicas por meio eletrônico. O título original é “Correio eletrônico não rastreável, endereços de retorno e pseudônimos digitais” e a assinatura cega para pagamentos não rastreáveis foi a primeira abordagem ao dinheiro digital via criptografia de assinatura às cegas, sem identificação, para pagamentos não rastreáveis. Os conceitos propostos por Chaum (1981), para criptomoedas eram

poderosos e de grande simplicidade, mas estavam além das capacidades técnicas da época, se destacaram como: o Protocolo de zero conhecimento, criado por Gilles Brassard e Cláudio Crepeau, onde foram desenvolvidos canais seguros, que permitem que as transações sejam feitas sem deixar vestígios do remetente, do destinatário e do que foi enviado. (Chaum; Brassard; Crépeau, 1988); o dinheiro eletrônico não rastreável em colaboração com Fiat Masters e Moni Naor, que implementa transações *offline* com sistema de detecção de gastos duplos. (Chaum; Fiat; Naor, 1990), e a criação da empresa Digicash sediada em Amsterdã para comercializar suas ideias de pesquisa. (Chaum, 1995). De posse de uma nova forma de lidar com o dinheiro, um novo padrão de proteção da privacidade pessoal surgiu, juntamente com uma abordagem mais segura para gerenciar registros circulando na rede, embora ainda centralizado em torno da Digicash de David Chaum.

Segundo artigo publicado pela Binance (2018), foi em 1991 que os cientistas da computação Stuart Haber e W. Scott Stornetta apresentaram uma solução computacionalmente viável para registros digitais que possibilitava a geração de documentos com registro de data que não poderiam ser adulterados. A partir dessa solução, foi concebida a ideia que daria origem à tecnologia *blockchain*. A Binance (2018) descreve a solução de Stuart Haber e W. Scott Stornetta, como um sistema baseado em uma cadeia de blocos criptograficamente protegidos para armazenar documentos com registro de data e hora, no qual foram incorporadas, em 1992, as Merkle tree[1], tornando o processo mais eficiente e possibilitando a coleta de múltiplos documentos em um único bloco. Apesar de seu potencial e vantagens, a tecnologia não obteve ampla adoção, e a patente expirou em 2004.

1.1 A CRIAÇÃO DO BITCOIN E DO PROTOCOLO DE SEGURANÇA DESCENTRALIZADO.

[1] **Merkle tree** é uma estrutura de dados na tecnologia *blockchain*, inventada por Ralph Merkle nos anos 1980. Incorporada ao sistema de Stuart Haber e W. Scott Stornetta em 1992, essa árvore otimizou a criação de registros digitais, permitindo a coleta eficiente de vários documentos em um bloco. Essa inovação foi crucial para a evolução da tecnologia *blockchain*.

A tecnologia *blockchain* teve seus princípios moldados, mediante os ideais de liberdade e privacidade de transações entre indivíduos do movimento Cypherpunk, no entanto, este novo modo de registro de dados digital, emergiu com o *whitepaper*[2], escrito pela figura de Satoshi Nakamoto no ano de 2008. Segundo Evans (2014) “Satoshi Nakamoto é um pseudônimo usado pelo criador do Bitcoin em comunicações por *e-mail*, postagens em fóruns e publicações como o Bitcoin *whitepaper*”. Porém, não é possível ter certeza sobre a identidade real de Satoshi Nakamoto.

Segundo Nakamoto (2008, p. 1), a tecnologia foi concebida como um “Um sistema baseado em tecnologia puramente ponto a ponto, e a criação de uma moeda digital que poderia ser enviada diretamente de uma parte a outra sem passar por uma instituição financeira”. Nakamoto (2008), propôs um sistema independente de intermediários e instituições financeiras, para validação de transações financeiras. A tecnologia *blockchain* é a base para a criação da primeira criptomoeda, o BitCoin. Conforme descreve Couto (2022, p. 12), a ferramenta criada por Nakamoto, surgiu para que as transações entre as moedas fossem seguras e não precisassem de um agente intermediário entre as partes, ou seja, as operações seriam feitas diretamente.

> “No seu aspecto mais básico, é um código-fonte aberto: qualquer um pode, gratuitamente, baixá-lo, executá-lo e usá-lo para desenvolver novas ferramentas para o gerenciamento de transações on-line. Como tal, ele tem potencial para desencadear inúmeras novas aplicações, além da capacidade iminente de transformar muitas coisas.” (Tapscott; Tapscott, 2016, p. 32)

A *blockchain* é uma tecnologia nova, com um grande potencial disruptivo nos modelos de negócios de diversas áreas, sendo estudada para moldar uma nova era da economia digital e gerar confiança entre todos os envolvidos. O sistema é conhecido como "protocolo de segurança" e consiste em uma cadeia de blocos com o objetivo principal de garantir a descentralização, assegurando que as transações sejam enviadas e validadas pela rede (Narayanan; Clark, 2017). Em outras palavras, quanto maior for a rede, mais segura ela será, pois mais computadores validarão as informações antes de serem adicionadas ao bloco. De acordo com a *Global Blockchain Business* Council (2022), promovida pela principal associação global da

[2] **Whitepaper** é um documento técnico que fornece informações detalhadas sobre um assunto específico, projetado para fornecer uma visão geral clara e concisa do tópico em questão. É comumente usado em áreas como negócios, tecnologia, finanças e ciência.

indústria, a tecnologia *blockchain* visa criar um ecossistema global seguro e funcional, e busca envolver agentes de mudanças, governos e reguladores para desenvolver uma sociedade mais equitativa. Destacando-se em setores como finanças, seguros, governo, cadeia de suprimentos, agricultura, mercado imobiliário, energia, saúde, mídia, ambiente e processos de negócios.

2 TECNOLOGIA BLOCKCHAIN: UMA VISÃO GERAL.

A tecnologia *blockchain* pode ser considerada como um grande banco de dados, descentralizado, de acordo com Morabito (2017, p. 4), "A tecnologia *blockchain* refere-se a um banco de dados distribuído e criptografado, que é um depositário de informações que não podem ser revertidas e são incorruptíveis".

> "Cada transação ou evento digital no registro de livro razão público tem de ser autenticado através do acordo de mais de metade dos participantes na rede. Isso implica que nenhum participante ou usuário como indivíduo pode modificar quaisquer dados dentro de um blockchain sem o consentimento de outros usuários (participantes)." (Morabito, 2017, p. 4)

Uma rede *blockchain* pode ser considerada uma tecnologia de registro distribuído *distributed ledger technology*[3] (DLT), o que consiste em uma tecnologia de contabilidade distribuída, uma infraestrutura que permite que os nós da rede[4] possam verificar, validar e armazenar informações de modo sincronizado e criptografado, através de protocolos. (World Economic Forum, 2022). Vasarhelyi & Dai (2017) definem então *blockchain* como um sistema onde as transações armazenadas em blocos são mantidas entre diversos computadores conectados a uma rede *peer-to-peer*[5] que utilizam algoritmos para verificar as transações.

---

[3] **Distributed ledger technology** é um conjunto de tecnologias que permite a criação de registros compartilhados, descentralizados e imutáveis, sem a necessidade de uma autoridade central para validar as transações. É utilizada para criar redes *peer-to-peer* seguras e transparentes. O *blockchain* é uma das tecnologias de registro distribuído mais conhecidas e utilizadas atualmente.

[4] **Nós da rede** os nós da rede são as máquinas conectadas à rede compartilhada através da internet – elas armazenam cópias da blockchain e compartilham informações com outras máquinas.

[5] **Peer-to-Peer (P2P)** é um modelo de arquitetura de rede de computadores em que cada dispositivo conectado na rede atua tanto como cliente quanto como servidor, compartilhando recursos e serviços

Este protocolo de verificação tecnológica dificulta a apropriação indevida do sistema ou manipulação de dados, pois exige autorização da maioria dos usuários para qualquer atividade na rede. Essa característica fundamental do *blockchain*, segurança, é assegurada, com operações assinadas digitalmente para identificação de dados, endereços públicos, horários e datas, aumentando a resistência a fraudes nas transações. Segundo Couto (2022), resume-se o *blockchain* como:

> "A tecnologia *blockchain* pode ser definida como uma cadeia de blocos, ou um banco de dados descentralizado e distribuído por consenso em uma rede digital. As transações digitais são registradas em blocos de informações sequenciais, conformando um encadeamento de blocos irrefutável" (Couto, 2022).

Para garantir a segurança da rede e a validação do bloco, foi proposto por Nakamoto (2008), a prova de trabalho, *'proof of work'* (PoW), que é responsável pela geração de cada código *hash* do bloco. Segundo Morabito (2017), o algoritmo que é executado na PoW, apresenta uma lógica matemática complexa, que utiliza uma função de *hash*[6], a *SHA (Secure Hash Algorithm) -256*[7]. Assim cada bloco, de uma cadeia *blockchain*, tem uma assinatura de função *hash*. aplicados na execução da lógica da tecnologia. Esse algoritmo de consenso é um conjunto de regras que governa uma rede *blockchain*.

Este protocolo de verificação da tecnologia permite que seja cada vez mais difícil que usuários mal-intencionados possam pegar o domínio do sistema ou manipular dados, posto que toda atividade feita na rede precisa ser autorizada pela maioria dos usuários, garantindo uma das características fundamentais do *blockchain*: a segurança. As operações também são assinadas digitalmente, permitindo identificar dados e suas partes correspondentes, por endereço público, horários e datas de operação, dificultando mais ainda fraudes nas transações.

---

diretamente com outros dispositivos, sem a necessidade de uma autoridade central para gerenciar as conexões ou os dados transmitidos. Nesse modelo, todos os dispositivos têm as mesmas capacidades e responsabilidades, criando uma rede descentralizada e distribuída.

[6] Um **código *hash*** é um código criptografado resumo, gerado oriundo de um conjunto de dados, através de uma função matemática, neste caso a SHA 256.

[7] O **SHA-256 (Secure Hash Algorithm-256)** é uma função de hash criptográfica que gera uma sequência alfanumérica de 256 bits, fornecendo segurança e integridade aos dados. Amplamente utilizado em tecnologias como blockchain, é essencial para garantir a autenticidade e a proteção contra alterações indesejadas nas informações.

2.1 ALGORITMOS DE CONSENSO EM BLOCKCHAIN: O PROCESSO DE ADIÇÃO DE NOVOS BLOCOS À BLOCKCHAIN.

De acordo com a proposta de Nakamoto (2008),na rede *blockchain* do BitCoin, novas transações são transmitidas para todos os nós da rede *blockchain*, cada nó coleta as transações em um bloco. A compreensão da função dos nós, que retêm cópias da *Blockchain* e transmitem informações de transações e blocos recentes entre si, é bem conhecida. Entretanto, a questão que se apresenta é como se dá o processo de adição de novos blocos a *blockchain*.

> "Não há uma única fonte responsável por informar o que deve ser feito. Como todos os nós têm o mesmo poder, é necessário haver um mecanismo que decida de forma precisa quem pode adicionar novos blocos a *blockchain*. É necessário um sistema que torne a fraude dispendiosa e que recompense usuários por atuarem de forma honesta. Qualquer usuário racional escolherá agir de maneira econômica" (Binance Square, 2020).

Como a rede é permitida a qualquer pessoa (*permissionless*), a criação de blocos precisa ser acessível, isso permite que os usuários participem da criação de blocos. No entanto, se houver qualquer tentativa de fraude, todos os membros da rede estarão cientes. Chamamos esses mecanismos de Algoritmos de Consenso, pois permitem que os participantes da rede cheguem a um consenso sobre qual deve ser o próximo bloco a ser adicionado.

De acordo com Maldonado (2020), os chamados "mineradores" são os encarregados de gerar novos blocos e adicioná-los ao final da cadeia de blocos no sistema *blockchain*. Conforme o protocolo estabelecido pelo Bitcoin, eles precisam realizar esse processo aproximadamente a cada dez minutos. Cada bloco minerado contém informações detalhadas sobre as transações realizadas durante um determinado período. Quando estes blocos são adicionados ao final da cadeia, ela é atualizada com base nas informações contidas nestes blocos. A mineração é amplamente considerada o algoritmo de consenso mais utilizado no setor de criptomoedas. Ela envolve a utilização do algoritmo *Proof of Work* (PoW) para validar transações no *blockchain*. Nakamoto também acrescenta que a *PoW,* resolve outro problema:

> “A prova de trabalho também resolve o problema de determinar a representação na tomada de decisão majoritária. Se a maioria fosse baseada em um endereço IP-um-voto, poderia ser subvertida por alguém capaz de alocar muitos endereços IP. A prova de trabalho é essencialmente um-CPU-um-voto. A decisão majoritária é representada pela cadeia mais longa, com o maior esforço de prova de trabalho investido nela. Se a maioria do poder de CPU é controlada por nós honestos, a cadeia honesta crescerá mais rapidamente e ultrapassará quaisquer cadeias concorrentes. Para modificar um bloco anterior, um atacante teria que refazer a prova de trabalho do bloco e de todos os blocos posteriores e, em seguida, alcançar e ultrapassar o trabalho dos nós honestos”. (Nakamoto, 2008, p. 3)

Considerando as informações apresentadas por Maldonado (2020), na mineração de criptomoedas os usuários disponibilizam recursos computacionais para resolver um quebra-cabeça proposto pelo protocolo, exigindo operações de *hash* em dados do bloco. O *hash* deve ser inferior a um valor específico, sendo impossível prever o resultado. Os mineradores realizam busca aleatória, ajustando os dados até encontrar uma solução válida, assegurando assim a segurança e integridade da *blockchain*. Isso se deve ao fato de que um minerador não receberá retorno do seu investimento caso não consiga minerar blocos válidos. Conforme Binance Academy (2023) destaca, o *PoW*, impulsionado pelo Bitcoin, envolve competição entre mineradores para validar blocos, garantindo a segurança por meio da resolução de problemas complexos. No *proof of stake (PoS),* ao contrário, os validadores propõem blocos e são recompensados, necessitando de apostar (*staking)* e arriscar fundos em caso de proposta inválida.

> “Com o *Proof of Stake* (PoS), não existe um custo externo. Em vez de mineradores, existem validadores que propõem (ou “forjam”) blocos. Eles podem usar um computador comum para gerar novos blocos, mas devem colocar uma parte significativa de seus fundos em jogo (*stake*) para ter esse privilégio. O valor de *staking* é uma quantidade predefinida da criptomoeda nativa da *Blockchain*, conforme as regras de cada protocolo”. (Binance Academy, 2023)

Apesar da eficiência energética e descentralização, o *proof of stake* enfrenta críticas quanto à centralização inicial da distribuição de *tokens* e à segurança diante

de ataques de 51%[8]. Em resumo, a escolha entre *proof of work* e *proof of stake* depende das necessidades e metas específicas de cada *blockchain*.

2.2 A MATURIDADE DA TECNOLOGIA BLOCKCHAIN E SUAS VANTAGENS.

A aplicação da tecnologia *blockchain* tem evoluído, ao realizar uma comparação com as fases propostas por Swan (2015) para a análise de maturidade do *blockchain*, é possível constatar fases de desenvolvimento do *blockchain*. Conforme demonstra a figura 01.

Figura 01- Classificação dos setores identificados conforme maturidade de desenvolvimento do *blockchain*

Blockchain 1.0	Blockchain 2.0	Blockchain 3.0
Mineração Finanças	Segurança da informação Gestão da informação	Governança Energia Biotecnologia Mídias Integração com outras tecnologias

Fonte: Magalhães (2020).

Conforme Magalhães (2020, p. 64), no que se refere ao "*blockchain* 2.0", verifica-se uma ênfase em aplicações voltadas à segurança e gestão da informação, com o uso da criptografia e dos contratos inteligentes. Especificamente, pode-se mencionar o desenvolvimento de soluções orientadas para a preservação de identidade *online* e aprimoramento de questões financeiras relacionadas à escalabilidade da tecnologia. Por outro lado, observa-se que a maioria dos setores identificados se concentra no "*blockchain* 3.0", que se caracteriza pela aplicação da tecnologia em soluções voltadas a interesses diversos da sociedade. Nesse sentido,

[8] O **ataque de 51**% é um tipo de ataque em *blockchain* que ocorre quando um grupo de usuários mal-intencionados controla mais de 50% do poder computacional de uma rede, permitindo que possam alterar transações, reescrever o histórico da *Blockchain* e realizar possivelmente gastos duplos.

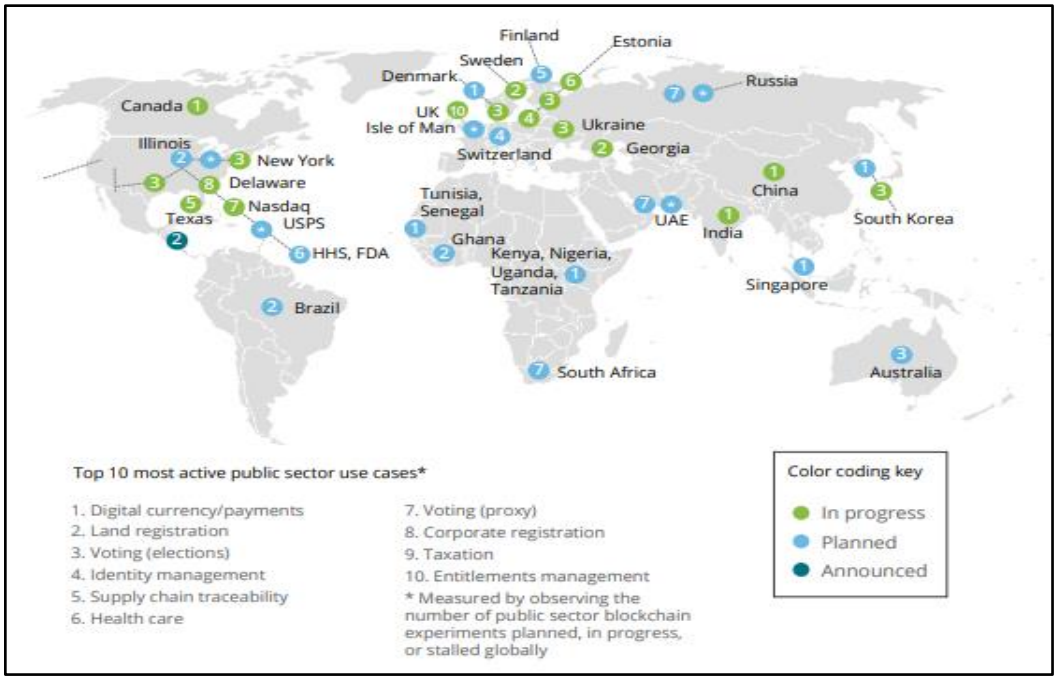
destaca-se a utilização do *blockchain* em setores como governança, energia, biotecnologia, mídias e integração com outras tecnologias disruptivas, especialmente a IoT[9]. Esses exemplos indicam uma expansão e diversificação do uso do *blockchain*, visando gerar novos formatos de entrega de valor por meio de produtos e serviços. Morabito (2017, p. 26), destaca as vantagens que a tecnologia pode trazer para o mundo dos negócios hoje: usuários capacitados a controlar suas informações, durabilidade, confiabilidade e longevidade das transações, processos com integridade, transparência, imutabilidade, transações mais rápidas com custos mais baixos e sem intermediários.

3 INICIATIVAS E DESAFIOS DA APLICAÇÃO DE BLOCKCHAIN NO SETOR PÚBLICO.

Existem diversas iniciativas de aplicação da tecnologia *blockchain* em diversos departamentos governamentais em diferentes países do mundo. Em 2017, a Deloitte, em parceria com a Universidade Fletcher School da Tufts, realizou um levantamento das iniciativas anunciadas, planejadas ou em progresso no setor público. A figura 02 apresenta a quantidade de projetos em cada país e os casos de uso concretizados em cada nação. A utilização da tecnologia *blockchain* no setor público apresenta potenciais benefícios, como transparência, eficiência, segurança e redução de custos em diversos processos governamentais. Alguns casos de uso incluem a votação eletrônica, a gestão de identidade digital, o monitoramento de viajantes, a gestão de registros médicos entre outros. (Killmeyer; White; Chew, 2017)

[9] **IoT** é a sigla em inglês para "Internet das Coisas" e se refere a um conceito tecnológico que representa a conexão de diversos dispositivos e objetos à internet, permitindo a comunicação entre eles e a coleta de dados em tempo real.

Figura 02: Uso tecnologia *blockchain* ao redor do mundo.



Fonte: Killmeyer, White e Chew (2017, p. 5).

Os resultados do levantamento realizado pela Deloitte e a Universidade Fletcher School da Tufts demonstram haver um crescente interesse e investimento no uso da tecnologia *blockchain* no setor público, com uma quantidade significativa de projetos em andamento em diversos países ao redor do mundo. No entanto, é importante destacar que ainda existem desafios a serem enfrentados, como questões regulatórias, de interoperabilidade e de adoção em massa da tecnologia (Killmeyer; White; Chew, 2017). A seguir apresentamos três iniciativas da implementação desta tecnologia, para solução de negócios governamentais.

3.1 ESTUDO DE CASO – O PROJETO SECURE DIGITAL ID.

A Organização Mundial de Turismo da ONU prevê um aumento de 50% nas viagens transfronteiriças na próxima década, tornando a verificação de identidades mais desafiadora. Um estudo da INTERPOL destaca a ineficácia dos programas existentes de viajantes de confiança. O Fórum Econômico Mundial, em parceria com

a Accenture e outros, propõe um sistema de Identidade Digital de Viajante Conhecido baseado em tecnologia *blockchain* e biometria. (Accenture, 2020) A descentralização do *blockchain* assegura a segurança das informações, enquanto a biometria vincula dados físicos e digitais para verificar identidades. Testes piloto estão em andamento, destacando a necessidade de soluções inovadoras diante do aumento das viagens transfronteiriças. O uso da tecnologia *blockchain* promete segurança avançada e controle do acesso aos dados pessoais pelos viajantes, incentivando a adoção por governos e organizações. (Global Blockchain Business Council, 2020)

3.2 ESTUDO DE CASO – BANCO NACIONAL DE DESENVOLVIMENTO (BNDES).

O Banco Nacional de Desenvolvimento (BNDES) implementou um projeto para utilizar a tecnologia *blockchain* na desestatização de serviços ou ativos públicos no Brasil. Esse projeto foi criado para aumentar a transparência e a rastreabilidade dos processos públicos, especialmente devido a situações de corrupção no país. A tecnologia *blockchain* foi utilizada em duas etapas do processo de desestatização: no registro de prestação de serviços e no fluxo de pagamentos realizados pelo BNDES às empresas especializadas. A utilização do *blockchain* permite o registro imutável dos documentos disponibilizados pelas consultorias e o pagamento automatizado e digital. O projeto não alterou todos os processos do BNDES, mas remodelou duas de suas etapas, aprimorando o processo na totalidade. Isso permite uma melhor auditoria futura e o registro de todos os trabalhos realizados pelas consultorias. O estudo apresentado por Arantes Jr (2018) destaca a importância do uso da tecnologia *blockchain* nessas etapas do processo de desestatização para aumentar a transparência e a eficiência dos processos públicos.

3.3 ESTUDO DE CASO – MONITORANDO A SAÚDE DA NAÇÃO COM TECNOLOGIA BLOCKCHAIN.

Diariamente, médicos e pacientes geram extensos volumes de dados de saúde, cuja coleta é desafiadora devido à sensibilidade das informações. O Centro de Controle e Prevenção de Doenças (CDC) dos Estados Unidos, enfrentando queda nas taxas de resposta em suas pesquisas, estabeleceu uma parceria com a IBM. Juntos, buscam implementar uma solução baseada em *blockchain* para controlar o acesso e a movimentação eficiente de conjuntos de dados sensíveis, com potencial de transformar a resposta do governo a crises de saúde. Embora promissora, a transição para um sistema interoperável baseado em *blockchain* enfrenta desafios no vasto e fragmentado sistema de saúde americano, requerendo a cooperação de diversas partes interessadas, incluindo o setor privado, cujo envolvimento dependerá de demonstrações contínuas de economia de custos por meio de provas de conceito e projetos-piloto. (Global Blockchain Business Council, 2018)

3.4 DESAFIOS PARA ADOÇÃO DA TECNOLOGIA BLOCKCHAIN.

A partir dos resultados deste levantamento, é possível afirmar que há um crescente interesse e investimento no uso da tecnologia *blockchain* no setor público, com uma quantidade significativa de projetos em andamento em diversos países ao redor do mundo. Embora a tecnologia *blockchain* seja altamente promissora, ainda existem obstáculos a serem superados e a aquisição da experiência é de extrema importância para todos os setores envolvidos em pesquisa e desenvolvimento das plataformas tecnológicas baseadas em DTL. Morabito (2017, p. 27), apresenta também os desafios para a adoção desta nova tecnologia e que podem dificultar a implementação, entre os quais elencamos: as regras do estado regulatório das criptomoedas (os governos não chegaram a um consenso sobre como a tecnologia pode ser utilizada no setor financeiro global); preocupações com a segurança cibernética da rede *blockchain* (apesar da utilização de algoritmos de criptografias fortes); vulnerabilidade do *software*; preocupação da integração da nova tecnologia com os sistemas legados das organizações; preocupação com entendimento da tecnologia para o desenvolvimento do *software* implantado; a natureza descentralizada das informações na rede *blockchain*; aceitação cultural da tecnologia pela organização para o sucesso de sua implantação; e, por fim, os custos da

implementação da tecnologia pela organização. Portanto, a utilização da tecnologia *blockchain* no setor público ainda é uma área em desenvolvimento, mas apresenta um grande potencial para transformar como os governos prestam e controlam seus serviços.

4 CONSIDERAÇÕES FINAIS

A tecnologia *blockchain* emergiu como uma poderosa ferramenta que transcende seu papel inicial no mundo das criptomoedas. Inicialmente concebida por entusiastas do movimento Cypherpunk, a *blockchain* evoluiu mediante várias fases de desenvolvimento, desde sua aplicação inicial em finanças e mineração (*blockchain* 1.0) até sua expansão para questões de segurança, identidade e governança (*blockchain* 2.0) e finalmente abrangendo uma ampla gama de setores e interesses da sociedade (*blockchain* 3.0). A aplicação da *blockchain* no setor público tem demonstrado grande potencial, em diversas áreas. Podemos considerar a tecnologia *blockchain* como promissora para criação, evolução e otimização de processos de diversos setores, contribuindo para eliminação de barreiras financeiras e de inclusão social. Apesar dos progressos realizados, os desafios regulatórios, de interoperabilidade e de adoção em massa ainda precisam ser superados. O futuro da *blockchain* no setor público depende da contínua disseminação de casos de uso, envolvimento de especialistas em processos de negócios e resolução desses desafios. À medida que mais governos adotam a tecnologia *blockchain*, aumenta o potencial de revolucionar a forma de como prestam serviços e interagem com seus cidadãos. Os países serão impactados por esses novos tipos de sistemas computacionais, que permitirão maior integridade, preservação de direitos, segurança e inclusão, poder e valor ao cidadão. Concluímos assim que a *blockchain* tem potencial para aprimorar processos governamentais, mas ressaltamos a necessidade de esforços contínuos para superar obstáculos e maximizar seus benefícios.

REFERÊNCIAS

ACCENTURE. WEF Known Traveller Digital ID. **Digital identity**, 2020. Disponivel em: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-122/accenture-ktdi-video-transcript.pdf#zoom=50. Acesso em: 18 outubro 2023.

BINANCE ACADEMY. A história da Blockchain. **Binance Academy**, 2018. Disponivel em: https://academy.binance.com/pt/articles/history-of-blockchain. Acesso em: 15 novembro 2022.

_____. Binance Academy. **O que é uma blockchain e como ela funciona?**, 2023. Disponivel em: https://academy.binance.com/pt/articles/what-is-blockchain-and-how-does-it-work. Acesso em: 23 agosto 2023.

BINANCE SQUARE. O que é a Tecnologia Blockchain? Guia Definitivo. **Binance**, 2020. Disponivel em: https://www.binance.com/en-IN/feed/post/583946. Acesso em: 15 novembro 2022.

CHAUM, David Lee. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. **Technical Note Programming Techniques and Data Structures**, Berkeley, fevereiro 1981. 84-88.

_____, David Lee. Ecash. **Chaum**, 1995. Disponivel em: https://chaum.com/ecash/. Acesso em: 15 novembro 2022.

_____, David Lee; BRASSARD, Gilles ; CRÉPEAU, Claude. Minimum Disclosure Proofs of Knowledge. **Journal of computer and system sciences**, Amsterdam, 1988. 156-189.

_____, David Lee; FIAT, Amos ; NAOR, Moni. Untraceable Electronic Cash. **Advances in Cryptology**, Berlin, 1990. 319-327.

COUTO, Gabriele Nogueira. A TECNOLOGIA DO BLOCKCHAIN: REVISÃO DA LITERATURA. **Universidade de Brasília (UnB)**, Brasília, 2022. 1-34. Disponivel em: https://bdm.unb.br/bitstream/10483/32052/1/2022_GabrieleNogueiraCouto_tcc.pdf.

DAI, Jun ; VASARHELYI, Mikios. Toward Blockchain-Based Accounting and Assurance. **Journal of Information Systems**, junho 2017. Disponivel em: https://www.researchgate.net/publication/317416300_Toward_Blockchain-Based_Accounting_and_Assurance. Acesso em: 23 novembro 2022.

EVANS, David S. Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. **University of Chicago**, Chicago, p. 1-28, abril 2014. Disponivel em: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2349&context=law_and_economics. Acesso em: 16 novembro 2022.

GLOBAL BLOCKCHAIN BUSINESS COUNCIL. Monitoring the Nation's Health. **Global Blockchain Business Council Use Cases**, 8 novembro 2018. Disponivel em: https://gbbcouncil.org/wp-content/uploads/2019/10/Monitoring-the-Nations-Health.pdf. Acesso em: 18 outubro 2023.

_____. Secure Digital Identification System for Global Travelers. **Global Blockchain Business Council Use Cases**, 2020. Disponivel em: https://gbbcouncil.org/wp-content/uploads/2019/07/Secure-Digital-ID.pdf. Acesso em: 18 outubro 2023.

_____. Global Blockchain Business Council. **Use case library**, 2022. Disponivel em: https://gbbcouncil.org/wp-content/uploads/2021/06/Using-Smart-Contracts-to-Underwrite-Climate-Risk_.pdf. Acesso em: 18 outubro 2023.

HUGHES, Eric. A Cypherpunk's Manifesto. **Activism.net**, 1993. Disponivel em: https://www.activism.net/cypherpunk/manifesto.html. Acesso em: 23 março 2023.

JR, Gladstone Arantes. Biblioteca Digital do BNDES. **Banco Nacional do Desenvolvimento Econômico e Social**, 2018. Disponivel em: https://web.bndes.gov.br/bib/jspui/handle/1408/18820. Acesso em: 18 dez. 2022.

KILLMEYER, Jason ; WHITE, Mark ; CHEW, Bruce. Blockchain basics for government. **Will blockchain transform?**, 2017. 1-20. Disponivel em: https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf. Acesso em: 18 novembro 2022.

MAGALHÃES, Kalilita Ester. MODELOS DE NEGÓCIOS: UM ESTUDO SOBRE O IMPACTO DA BLOCKCHAIN. **REPOSITORIO PUCSP Teses e Dissertações dos Programas de Pós-Graduação da PUC-SP**, São Paulo, 2020. Disponivel em: https://ariel.pucsp.br/bitstream/handle/23818/1/Kallita%20Ester%20Magalh%c3%a3es.pdf.

MALDONADO, José. Mineração de Bitcoin Como você cria um bloco? **Bit2me Academy**, 2020. Disponivel em: https://academy.bit2me.com/pt/minera%C3%A7%C3%A3o-de-bitcoin-como-criar-um-bloco/. Acesso em: 23 novembro 2022.

MORABITO, Vicenzo. **Business Innovation Through Blockchain:** The B³ Perspective. 1ª. ed. [S.l.]: Springer, 2017. ISBN ISBN-10 : 331948477X.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. **Bitcoin Org**, 2008. Disponivel em: https://bitcoin.org/bitcoin.pdf. Acesso em: 12 março 2023.

NARAYANAN, Arvind ; CLARK, Jeremy. Bitcoin's Academic Pedigree: The concept of cryptocurrencies is built from forgotten ideas in research literature. **ACM Digital Library**, julho 2017. 1-30. Disponivel em: https://dl.acm.org/doi/pdf/10.1145/3134434.3136559. Acesso em: 18 novembro 2022.

SWAN, Melaine. **Blockchain:** Blueprint for a New Economy. 1ª. ed. [S.l.]: O'Reilly Media, 2015. ISBN ISBN-10 : 9781491920497.

TAPSCOTT, Don ; TAPSCOTT, Alex. **Blockchain revolution**. 1ª. ed. São Paulo: Senai, 2016. ISBN ISBN: 978-8583937890.

WORLD ECONOMIC FORUM. World Economic Forum. **17 ways technology could change the world by 2027**, 2022. Disponivel em: https://www.weforum.org/agenda/2022/05/17-ways-technology-could-change-the-world-by-2027/. Acesso em: 18 outubro 2023.