TECNOLOGIA BLOCKCHAIN: uma nova relação de confiança

Neide Pereira de Oliveira

neidenpo@gmail.com

Recebido em: 03/02/2021.

Aprovado em: 31/03/2023.

DOI: 10.18406/2359-1269v8n12021281

Resumo
A tecnologia Blockchain, pode ser definida como o sustentáculo das criptomoedas, ou seja, compila os dados de envio e recebimento de criptomoedas, como por exemplo, o Bitcoin. Este trabalho objetiva apresentar mais informações sobre a plataforma tecnológica Blockchain, demonstrar seu momento atual, suas aplicações nas diversas áreas e os impactos sociais, utilizando-se o método dedutivo que se constitui de um processo de análise da informação através do raciocínio lógico, aliado a pesquisa na literatura. Ante o exposto, conclui-se que a utilização de tal ciência é abrangente garante a confidencialidade e segurança dos dados transacionados de maneira distribuída, entretanto, trata-se de uma tecnologia que está em constante evolução.
Palavras-chave: Blockchain; Bitcoin; Ponto-a-Ponto.

Abstract
Blockchain technology can be defined as the mainstay of cryptocurrencies, that is, it compiles data for sending and receiving cryptocurrencies, such as Bitcoin. This work aims to present more information about the Blockchain technological platform, demonstrate its current moment, its applications in different areas and social impacts, using the deductive method that consists of a process of information analysis through logical reasoning, combined with literature search. In view of the above, it is concluded that the use of such science is comprehensive, guarantees the confidentiality and security of data transacted in a distributed way, however, it is a technology that is constantly evolving.
Keywords: Blockchain; Bitcoin; Point to point.

Introdução

O aumento do uso e interesse público pela plataforma tecnológica Blockchain, conhecida globalmente devido à aplicação Bitcoin, também chamada criptomoeda ou moeda digital, plataforma esta que possui propriedades intrínsecas, tais como, segurança, resiliência, inviolabilidade e imutabilidade para o registro e histórico de transações.

Este artigo visa apresentar mais informações sobre a plataforma tecnológica Blockchain demonstrando seu momento atual, suas aplicações nas diversas áreas e os impactos sociais, diante deste paradigma baseado em uma nova relação confiança.

Material e métodos

Foi utilizado o método dedutivo que se constitui de um processo de análise da informação através do raciocínio lógico e a dedução para busca de respostas sobre determinado assunto, associado à metodologia de pesquisa bibliográfica, por meio de fontes recentes, como artigos, livros e revistas científicas. Através do levantamento bibliográfico pautado sobremaneira a partir

da busca eletrônica, foram selecionados materiais cujos critérios de inclusão foram artigos que abordam a temática, disponíveis nas bases de dados pré-definidas e publicados em português, no período entre janeiro de 2014 a fevereiro de 2022.

Consideradas as seguintes etapas para elaboração desta pesquisa: estabelecimento da hipótese e objetivo da revisão; estabelecimento de critérios de inclusão de artigos; definição das informações a serem extraídas dos artigos selecionados; análise dos resultados e discussão.

A questão norteadora deste trabalho partiu da elucidação da questão: a tecnologia Blockchain pode ser considerada de confiança descentralizada?

As palavras-chave utilizadas foram: Blockchain. Bitcoin. Ponto-a-Ponto. A busca foi realizada pelo acesso on-line utilizando os seguintes critérios de inclusão: artigos que abordam a temática, nos idiomas inglês e português, no período compreendido entre janeiro de 2014 a fevereiro de 2022.

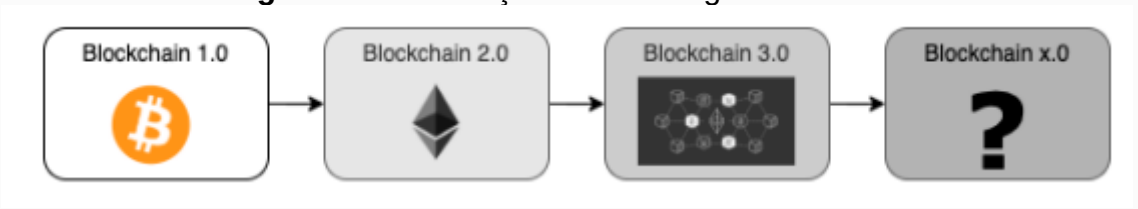
A busca cruzada se deu utilizando as palavras-chaves: blockchain; bitcoin; ponto-a-ponto.

Os artigos foram selecionados a partir do título e resumo que abordavam o assunto em questão, com a utilização do método dedutivo, partindo-se de uma premissa geral a específica, onde se buscam as conclusões.

Resultados e discussão

Segundo Wu *et al.* (2019) a tecnologia blockchain está em constante evolução, e cada qual possui um marco, a primeira versão da blockchain teve como marco principal o lançamento do Bitcoin, em 2009, assim a comunidade tecnológica tomou conhecimento de um engenhosa combinação de técnicas como o uso de uma rede P2P, elementos criptográficos, livro-razão público e a eliminação da terceira parte de confiança sustentando as transações de uma criptomoeda, algo que somente era imaginado em pesquisas académicas ou na ficção científica.

Figura 1 – A evolução da tecnologia Blockchain

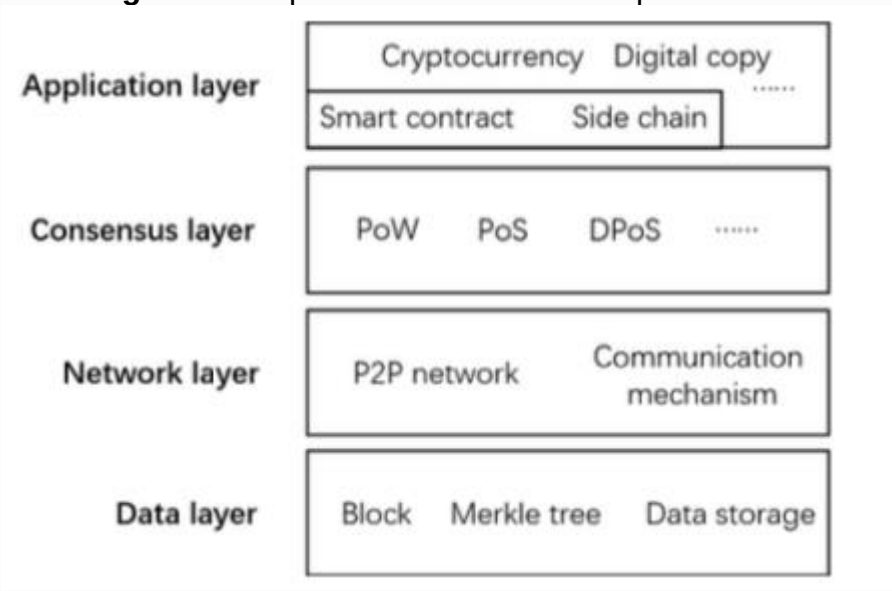


Fonte: Wu *et al.* (2019)

Abijaude *et al.* (2021) afirmam que os elementos básicos e seminais dessa tecnologia, combinados de forma engenhosa, sustentam de forma teórica/prática o desenvolvimento de aplicações descentralizadas, dentre elas as diversas criptomoedas, são: a criptografia que satisfaz os requisitos de segurança do sistema e das aplicações, destacando os recursos mais utilizados resumos criptográficos (funções hash) e as assinaturas digitais; o consenso distribuído que permite que participantes distribuídos coordenem as suas ações, de forma a alcançar decisões comuns, e assim garantir a manutenção da consistência dos seus estados (safety) e o progresso do sistema (liveness), apesar da existência de falhas; o livro razão (ledger) distribuído é uma estrutura de dados imutável, em que transações são registradas e o estado global do sistema é mantido replicado em todos os nós da rede P2P.

Esses autores destacam que a blockchain é amplamente utilizada em campos como indústria, governo, saúde, logística, comércio, além das moedas virtuais, entre outros, sendo que esta tecnologia possui uma arquitetura dividida em quatro camadas, classificadas por Wu et al. (2019), sendo elas: (a) dados, onde se encontram os blocos, o armazenamento de dados e a estrutura de árvore utilizada; (b) rede, onde se encontra a rede P2P e os mecanismos de comunicação; (c) consenso, onde naturalmente estão os protocolos de consenso; e, (d) aplicação, onde estão os contratos inteligentes, as criptomoedas e as sidechains.

Figura 2 - Arquitetura blockchain em quatro camadas



Fonte: Wu *et al.* (2019)

Apesar de certa relutância do uso das moedas digitais ou criptomoedas por boa parte da população, a cada dia estas ganham adeptos e defensores. Para Benicio *et al.* (2014) as criptomoedas chamam atenção por suas técnicas de criptografia em seus protocolos de controles das transações mundiais, possibilitando tanto a troca como a geração de novas moedas digitais.

O que está por detrás dessas transações é uma rede de computadores com um banco de dados distribuído, que possui um gerenciamento descentralizado, segundo Pires (2017), umas das criptomoedas pioneiras e mais conhecidas, o bitcoin ou BTC foi desenvolvida a partir de uma arquitetura de redes de computadores descentralizada, configurada por pontos de articulação interconectados via P2P (peer-to-peer, conhecida como rede ponto-a-ponto), onde os registros dos dados transacionados na rede P2P são operados em uma cadeia de blocos de algoritmos, que realiza o processamento dos dados por meio de criptografia.

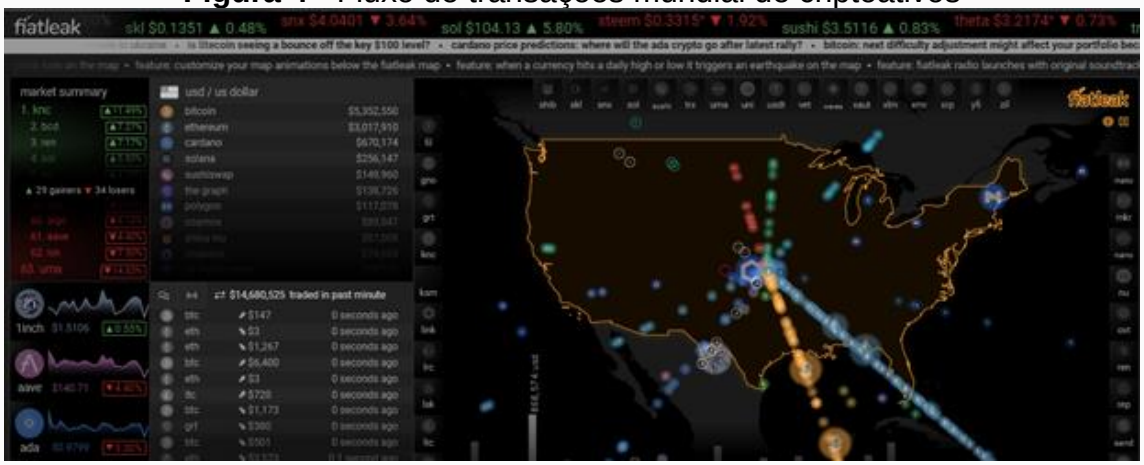
Pires (2017) sugere a consulta ao site Fiatleak para verificação de informações geográficas, em tempo real na internet, sobre a circulação diária e o fluxo mundial de moedas para BTC, assim sendo possível estabelecer uma estimativa temporal sobre o fluxo mundial de moedas para BTC no ciberespaço.

Figura 3 - Fluxo de comercialização mundial de Bitcoins

Fonte: Fiatleak (2018).

Atualmente tal site tomou maiores proporções possuindo uma gama maior de dados representando transações de diversos tipos de criptomoedas em todo o mundo, possuindo um design gráfico com uma tela muito mais informativa e interativa.

Figura 4 - Fluxo de transações mundial de criptoativos



Fonte: Fiatleak (2021)

Mendes (2017) afirma que as transações de bitcoin são verificadas, prevenindo gasto duplo, utilizando-se a criptografia de chave pública, exigindo que a cada usuário sejam determinadas duas chaves, uma privada, que é mantida em segredo, e uma pública, utilizando-se para tanto da tecnologia de blockchain.

Importante notar que a moeda bitcoin demanda grande poder computacional, uma vez que utiliza o algoritmo Proof-of-Work (Protocolo Prova de Trabalho ou PoW), conhecido como o algoritmo de consenso, cuja função é

tornar possível o consenso em uma rede descentralizada, o que aumenta substancialmente o consumo de tempo, de energia, e de hardware, bem como evita que usuários ajam com maliciosidade (MENDES, 2017).

Santos *et al.* (2016) classificam os usuários do sistema Bitcoin em três classes: os mineradores produzem novas moedas, por meio de programação ao retirá-los do código-mãe e colocá-los em circulação; os clientes utilizam a moeda como meio de pagamento. E, ainda os verificadores que a cada transação financeira do sistema, fazem análises dos códigos 24 horas por dia, autorizam a concretização do meio de troca e recebem por meio de taxas seus pagamentos.

As transações que ocorrem na criptoeconomia são registradas um grande banco de dados público, que contém o histórico de todas as transações realizadas, como fosse uma espécie de livro-razão público e distribuído, as novas transações são verificadas contra a blockchain (cadeia de blocos) de modo a assegurar que os mesmos bitcoins não tenham sido previamente gastos, eliminando assim o problema do gasto duplo, assim a rede global peer-to-peer, composta de milhares de usuários, torna-se o próprio intermediário (ULRICH, 2014).

Corrobora Greve *et al.* (2018) ao afirmar que a blockchain é o resultado de uma engenhosa combinação de técnicas robustas provenientes da computação distribuída confiável (tolerância a falhas bizantinas, sistemas P2P), criptografia (chave assimétrica, funções hash, desafios criptográficos) e teoria dos jogos (mecanismos de incentivos).

A falha bizantina ocorre quando um ou mais componentes falham e não há informações precisas sobre qual componente falhou ou se as informações do sistema estão corretas; enquanto os sistemas P2P possuem a premissa que ambas os pares dividem os mesmos recursos de forma igualitária; em relação as chaves de criptografia elas se diferenciam da seguinte forma: a chave assimétrica é composta por dois tipos de chaves de segurança uma privada (conhecida somente pelo proprietário) e a outra pública (amplamente disseminada); funções hash são valores determinísticos e respondem aos parâmetros das variáveis fornecidas pelo algoritmo, o hash resultante é um identificador que possui apenas uma entrada de dados e é único e irreversível; e o desafio criptográfico são desafios matemáticos criptográficos complexos

Revista Eixos Tech | ISSN 2359-1269 | v.08 | n.1 | 2021

gerados a cada transação para custear seu processamento (ABIJAUDE *ET AL.*, 2021).

A teoria dos jogos é um conceito da área econômica que investiga padrões comportamentais nos negócios, mercados e consumidores, no caso das criptomoedas, como a bitcoin por exemplo, os jogos teóricos criam situações em que é possível examinar o comportamento dos nós de uma rede, com base nos mecanismos de incentivos proporcionados pelo protocolo, que tem como consideração as mais prováveis e racionais decisões (DE PAULA, 2019).

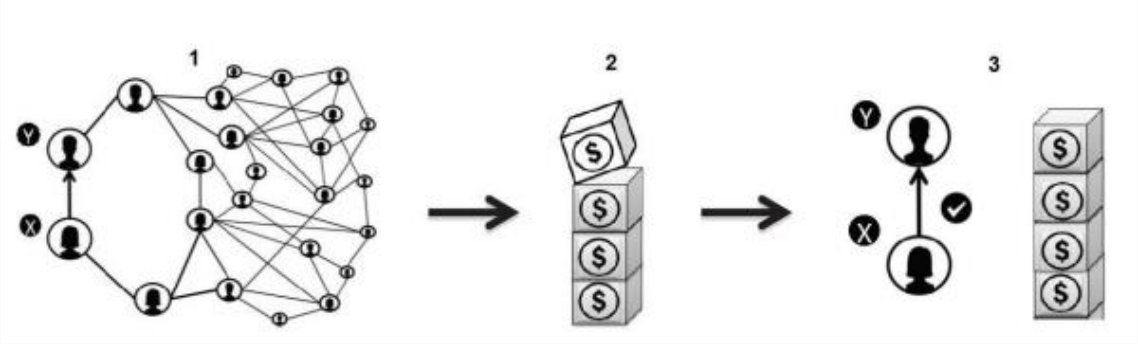
Segundo Greve *et al.* (2018) vários desafios computacionais são encarados, entre eles a realização de consenso numa rede aberta (com participantes desconhecidos e em escala planetária); tolerância a falhas bizantinas (ainda que se tenham participantes anônimos); resistência ao ataque de duplo-gasto (double-spending, ou seja, quando um usuário consegue gastar as mesmas moedas digitais mais de uma vez) o que dá garantia aos ativos transacionados (exemplo: moedas digitais) para que não sejam gastos duplamente e indo além do seu valor em posse; resistência a ataques Sybil (ataques as sistemas online onde um indivíduo tenta assumir o controle da rede criando múltiplas contas, nodes ou poder de computação), contra usuários maliciosos que se personificam em outros (exceto se possuírem acesso a sua chave privada); garantia da auditabilidade, autenticidade, não repúdio e integridade em escala global de todas as transações validadas e armazenadas no livro-razão distribuído.

A blockchain é conhecida como livro-razão público, por conter todo histórico de transações realizadas, armazenadas e verificadas por todos os nós da rede, Tapscott e Tapscott (2017) afirmam que a blockchain promove uma democracia realmente participativa, uma vez que com o uso do modelo de contratos inteligentes registrados em livros-razão públicos torna-se a gestão governamental de fato transparente.

De Paula (2019) propõe um modelo de processo de consenso dos blockchains com transações válidas, representada na figura 4. Onde, no item 1: X realiza transação para Y, e a transação sendo aceita pelos nodos, é propagada para os outros nodos. No item 2: a validação dos nodos gera consenso, que propagam a transação até o bloco em formação. Enquanto

finalmente no item 3 quando o bloco se completa de transações validas, B recebe a transação válida de A.

Figura 5 - Processo de consenso no blockchain

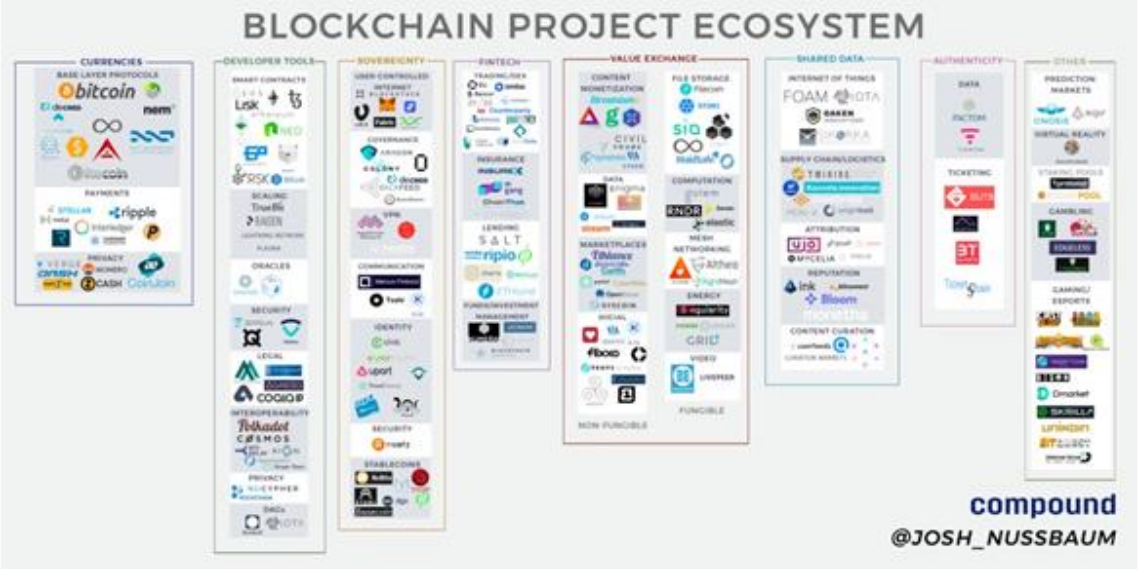


Fonte: De Paula (2019).

Assim, a cadeia de blocos (com ligações criptográficas) se desponta em um cenário altamente propicio para a grande variedade de conteúdos digitais, ultrapassando as barreiras territoriais e cognitivas, sendo muito mais do que somente transações de moedas virtuais, possui grande potencial de atender diversos setores como a indústria, os cuidados de saúde, a educação e pesquisa, os governos e dentre outros.

Na área de saúde, para McFarlane *et al.* (2017), o blockchain Patientory Blockchain Network desponta como uma solução para sistemas de registros médicos eletrônicos (EMR), constituindo uma rede de saúde P2P, com uma base de dados descentralizada, sendo uma cadeia de blocos, não possui um ponto central de falha, e possui uma maior capacidade de suportar ataques maliciosos, tendo em vista que uma vez que uma blockchain e seus contratos inteligentes são configurados, os parâmetros tornam-se absolutos.

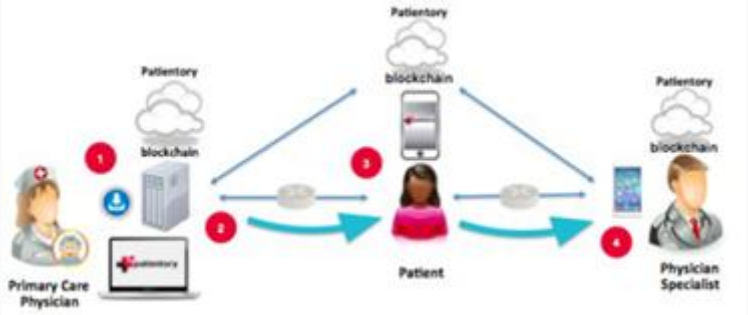
Figura 6 - Mapa do ecossistema projeto blockchain



Fonte: Adaptado Nussbaum (2017)

Segundo esses autores a entidade possui um servidor público com a característica de ser um Servidor de Chamada de Procedimento Remoto (Remote Procedure Call - RPC) que atua como uma interface para uma implementação privada da Blockchain da Ethereum (permissionided blockchain). Esta rede de nós da blockchain, só está autorizada a interagir com os outros nós da blockchain, uma entidade de chave autoral, uma instalação de armazenamento compatível.

Figura 7 - Relação Paciente x Provedor



Fonte: Adaptado McFarlane *et al.* (2017)

No meio científico a blockchain vem de encontro às necessidades e aspectos críticos da comunicação da ciência (Scholarly Communication), e pesquisa científica, o que inclui transparência, confiança, reprodutibilidade e crédito, resolvendo alguns dos problemas como custos, abertura e

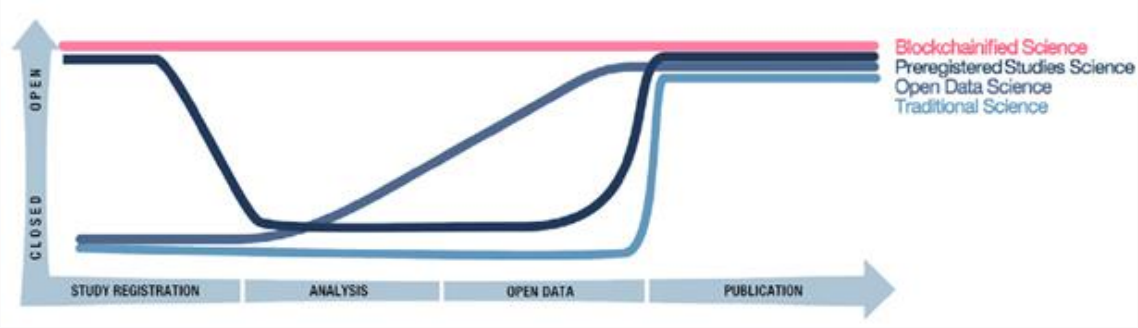
acessibilidade universal a informações científicas, oferecendo a geração descentralizada e autorregulada de dados, a partir de uma infraestrutura compartilhada, onde todas as transações são salvas e armazenadas.

Figura 8 - Comunicação científica e pesquisa

Fonte: adaptado de Sibi (2021).

Segundo o Relatório “Blockchain for Research” (VAN ROSSUM, 2017), o blockchain poderia abrir o processo de pesquisa, enquanto a ciência tradicional torna-se aberto no ponto de publicação, através de uma ciência "blockchained" (algo traduzido como ciência com uso da blockchain) partindo do pré-registro de estudos e até a publicação de dados, fazendo que a pesquisa se abra em vários estágios, de uma maneira mais abrangente, pois o ambiente se torna verdadeiramente colaborativo, além de dificultar fraudes como plágio ou qualquer tipo de apropriação indevida do conteúdo do estudo em desenvolvimento.

Figura 9 - Ciência “blockchained” do processo de pesquisa até a publicação



Fonte: Adaptado Relatório “Blockchain for Research” (VAN ROSSUM, 2017).

Para Issler e Issler (2017), é importante a discussão do uso da tecnologia blockchain como um aliado ao Registro Público, garantindo os

princípios de publicidade, autenticidade, segurança e eficácia dos contratos. Isso seria possível com a utilização do recurso de contrato inteligente, onde há inserção de obrigações autoexecutáveis, devido a autonomia (estando em andamento, sua execução é automática); a autossuficiência (recursos próprios - armazenamento e processamento); e a descentralização (servidores distribuídos e auto executados em vários nós da rede).

Outro atrativo segundo eles é o registro de propriedades inteligentes (smart property), essas propriedades permitem o controle da propriedade e do acesso a determinado ativo, fazendo com que ele seja registrado como um recurso digital na blockchain. Existem algumas cidades brasileiras pioneiras com projetos pilotos na utilização da tecnologia blockchain no registro de imóveis, por exemplo, as cidades de Morro Redondo e Pelotas, visando à redução de custos, a melhora da precisão, da segurança e da transparência, utilizando o serviço da empresa Ubitquity LLC.

Enquanto Abijaude *et al.* (2021) apontam como uma possível evolução do uso da blockchain a associação com a tecnologia IoT (Internet of Things ou Internet das Coisas), os dispositivos IoT atuais incluem smartphones, eletrodomésticos inteligentes, veículos, sensores internos e externos, e as chamadas casas inteligentes, considerando-se que a tecnologia blockchain envolve muitos elementos além de simplesmente conectar blocos em uma cadeia, que ao se adicionar elementos de IoT, esta complexidade ganha novos contornos que precisam ser desvendados.

Além dessas questões a associação do blockchain com outras tecnologias a saber, por exemplo, computação quântica, computação em nuvem e névoa, big data, inteligência artificial e realidade virtual, para cada uma destas tecnologias há desafios de pesquisa em aberto. A inteligência artificial tem recebido grande parte da atenção das pesquisas nos últimos anos, assim como, a computação em nuvem/névoa tem como uma grande dificuldade o estabelecimento de um ambiente seguro, a realidade virtual também possui desafios de pesquisa em aberto, os aplicativos big data possuem grande potencial, e a computação quântica, os protocolos criptográficos usados pela blockchain são suscetíveis a ataques pelo desenvolvimento de um computador quântico (ABIJAUDE *ET AL.*, 2021).

Abre-se também uma discussão a nível do campo jurídico, como afirmam Antunes *et al.* (2015), com o advento da tecnologia descentralizada e sem uma regulamentação governamental, especialmente se tratando de moedas eletrônicas ou virtuais, como o Bitcoin que apesar de trazer ao mundo inovações que impactam na maneira como a sociedade utiliza e pensa o dinheiro, ainda restam dúvidas de como impedir e controlar o seu uso em atos lícitos e sobretudo nos atos ilícitos, neste caso como ocorre em transações da *deep web* (web profunda), onde comercializam desde anabolizantes a drogas ilícitas, assim como de sequestros a lavagem de dinheiro.

Contudo, esses problemas não são exclusivos do uso de moedas como o Bitcoin, pois qualquer outra moeda apresenta vulnerabilidades que permitem atos ilícitos, levando a fragilidade do controle por parte do Estado sobre crimes contando apenas com regulações e fiscalizações.

Conclusão

A plataforma tecnológica blockchain é um campo vasto e ainda muito pouco explorado, sendo discutida e aplicada por grupos restritos de profissionais da tecnologia da informação, apesar de estar sendo inserida cada vez mais nas atividades cotidianas.

A blockchain vai além de ser uma mudança de paradigma tecnológico, trata-se de uma mudança da perspectiva cultural, pois se considera naturalmente ser mais fácil de controlar e confiar àquilo que está centralizado, neste aspecto a blockchain rompe com esse pensamento à medida que garante a confidencialidade e segurança dos dados transacionados de maneira distribuída em um complexo intricado de protocolos, criptografia e poder computacional.

Se a blockchain teve sua ascensão graças à moeda virtual bitcoin, atualmente sua aplicação abrange vários cenários além do econômico, como o registro de imóveis, saúde, educação e pesquisa, entre outros.

Conclui-se a utilização de tal tecnologia é abrangente e que são necessários mais pesquisas e estudos sobre esse assunto, em vista que está em constante evolução.

Referências

ABIJAUDE, Jauberth Weyll; GREVE, Fabíola; SOBREIRA, Péricles de Lima. Blockchain e Contratos Inteligentes para Aplicações em IoT - Uma Abordagem Prática. 40ª Jornada de Atualização em Informática (JAI 2021). **SBCOpenLib**. DOI: https://doi.org/10.5753/sbc.6757.3.4. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/book/67. Acesso em: 25/02/2022.

ANTUNES, Felipe da Silva; FERREIRA, Natasha Alves; BOFF, Salete Oro. **Bitcoin** - Inovações, Impactos no Campo Jurídico e Regulação para Evitar Crimes na Internet. Anais do 3º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. Universidade Federal de Santa Maria - UFSM. Santa Maria - RS, 2015.

BENICIO, Alberto Ayres; DA CRUZ, Alessandro Rodrigues; SILVA, Marlon Wanger Souza. Bitcoin a Moeda Digital que se tornou realidade. **Revista Científica da UNESC**, v. 12, n. 15 (2014).

DE PAULA, William Ribeiro. **Blockchain e sua Correlação com Teoria dos Jogos**. 2019. Disponível em: https://www.ime.usp.br/~map/tcc/2019/WilliamRibeiroV1.pdf. Acesso em: 25/02/2022.

FIATLEAK. **Fiatleak**. Acesso em: 10 jun. 2018. Disponível em: http://fiatleak.com/

GREVE, Fabíola; SAMPAIO, Leobino; ABIJAUDE, Jauberth; COUTINHO, Antonio; VALCY, Ítalo; QUEIROZ, Sílvio. **Blockchain e a Revolução do Consenso sob Demanda**. Capítulo 5. Disponível em: <http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/Capitulo5.pdf>. Acesso em: 15/06/2018.

ISSLER, Pedro Augusto Lamana; ISSLER, Paulo Vinícius Lamana. Discussões sobre o uso da tecnologia Blockchain aliada ao Registro Público brasileiro. In: Congresso Internacional de Direito e Contemporaneidade, 4, Santa Maria, 2017. Anais. Santa Maria: **UFSM -** Universidade Federal de Santa Maria, 2017.

MCFARLANE, Chrissa; BEER, Michael; BROWN, Jesse; PRENDERGAST, Nelson. **Patientory**: Uma rede P2P de Saúde de Armazenamento de Registros Médicos v1.0. Abril de 2017.

MENDES, Ana Carolina Camargo. Moeda Eletrônica Bitcoin: Análise do Uso na Cidade de Brasília – DF. **Revista Científica Multidisciplinar Núcleo do Conhecimento**. Edição 03. Ano 02, Vol. 01. pp 37-73, Junho de 2017.

NUSSBAUM, Josh. **Techcrunch**. Disponível em <https://techcrunch.com/2017/10/16/mapping-the-blockchain-project-ecosystem/>. Acesso em: 10 jun. 2018.

PIRES, H. F. **Bitcoin**: a moeda do ciberespaço. Geousp – Espaço e Tempo, v. 21, n. 2, p. 407-424, agosto. 2017. ISSN 2179-0892.

SANTOS, Osvaldo Amaral dos; FELIPE, Noelia; Correia, Paulo Cruz. Impactos Econômicos Da Criptomoeda Bitcoin. II Encontro Anual de Iniciação Científica. **Universidade Estadual do Paraná**. Campus Paranavaí, 25 a 27 de outubro de 2016.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**. Editora SENAI-SP, São Paulo, 2017.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. Instituto Ludwig von Mises Brasil. São Paulo, 2014. 100p.

VAN ROSSUM, Joris. Blockchain for Research. **Digital Science** (2017). figshare. Paper. Disponível em: <https://figshare.com/articles/_/5607778>. Acesso em: 15/06/2018.

WU, Mingli; WANG, Kun; CAI, Xiaoqin; GUO, Song; GUO, Minyi; RONG, Chunming. A comprehensive survey of blockchain: From theory to IoT applications and beyond. **IEEE Internet of Things Journal**, v. 6, n. 5, p. 8114-8154, 2019. DOI: 10.1109/JIOT.2019.2922538. Disponível em: https://ieeexplore.ieee.org/abstract/document/8735815. Acesso em: 25/02/2022.