INTERFACE TECNOLÓGICA

BLOCKCHAIN: uma tecnologia além da criptomoeda virtual

BLOCKCHAIN: a technology beyond virtual cryptocurrency

Victor Ayres Francisco da Silva – victor.ayres@outlook.com
Faculdade de Tecnologia de Taquaritinga (FATEC) – SP – Brasil
Maria Aparecida Bovério – mariaboverio@hotmail.com
Universidade Estadual Paulista (UNESP) – *Campus* de Rio Claro – SP –Brasil
Faculdade de Tecnologia de Sertãozinho (FATEC) – SP – Brasil

DOI: 10.31510/infa.v15i1.326

RESUMO

Este artigo tem o objetivo de investigar o que é a tecnologia *blockchain*, demonstrar sua história e, principalmente, as possíveis aplicações desta tecnologia relativamente nova em diversas áreas, explicando sua relevância no universo digital e na segurança do conectado século XXI. A pesquisa é de caráter bibliográfico e discorre, inicialmente, sobre a metodologia da pesquisa e em seguida, trata das teorias envolvendo essa tecnologia apresentando brevemente sua história, a forma de seu funcionamento e sua relação com o *Bitcoin.* No entanto, o foco principal do artigo é a tecnologia *blockchain* e não nas criptomoedas virtuais e, por isso, explica também suas características e limitações, visando compreender quais são os benefícios da implementação desta tecnologia em aplicações de diversas áreas. Como resultados, a pesquisa bibliográfica apresenta as diferentes gerações e exemplos de aplicações possíveis, em processo de implementação ou até mesmo em utilização dessa tecnologia considerada inovadora, cujo impacto é semelhante ao surgimento da *Internet*. Concluiu-se que tal tecnologia apesar de ainda estar em seus primeiros anos de vida apresenta inúmeras possibilidades de aplicações em áreas além das criptomoedas virtuais, garantindo maior segurança e menor custo a partir de várias iniciativas que possibilitam uma revolução da distribuição de dados atuais na qual a tecnologia *blockchain* encontra-se como protagonista e em constante evolução.

Palavras-chave: *Blockchain*. Segurança Digital. Tecnologias. Criptomoeda. *Bitcoin*.

ABSTRACT

This article aims to investigate what is blockchain technology, demonstrate its history and, above all, the possible applications of this relatively new technology in several areas, explaining its relevance in the digital universe and the security of Connected 21st century. The research is of bibliographic character and initially discourses on the methodology of research and then deals with the theories involving this technology presenting briefly its history, the form of its functioning and its relationship with Bitcoin. However, the main focus of the article is the blockchain technology and not in the virtual cryptocurrency and therefore explains its characteristics and limitations, aiming to understand what the benefits of are implementing this technology in applications of various Areas. As a result, the bibliographic research presents the different generations and examples of possible applications, in the process of implementation or even in the use of this technology considered innovative, whose impact is similar to the emergence of the Internet. It was concluded that such technology

although still in its first years of life presents numerous possibilities of applications in areas beyond the virtual cryptocurrency, guaranteeing greater security and lower cost from various initiatives that enable A revolution of the current data distribution in which blockchain technology is a protagonist and in constant evolution.

Keywords: Blockchain. Digital Security. Technologies. Cryptocurrency. Bitcoin.

1 INTRODUÇÃO

Este artigo de caráter bibliográfico propõe-se a investigar o que é a tecnologia *blockchain*, apresentar sua história e principalmente as possíveis aplicações desta tecnologia relativamente nova em diversas áreas, explicando sua relevância no universo digital e na segurança do conectado século XXI. A seção 2 apresenta a metodologia da pesquisa aplicada no desenvolvimento do artigo, a seção 3 apresenta os conceitos do *blockchain*, uma breve sua história, seu funcionamento e sua relação com o *Bitcoin*, sem a pretensão de aprofundar o assunto, principalmente porque o foco do presente artigo centra-se na tecnologia *blockchain* e não nas criptomoedas virtuais, além de demonstrar quais são as suas características e limitações do *blockchain*. A seção 4 trata das teorias envolvendo essa tecnologia e tem por objetivo compreender os conceitos referentes às suas diferentes gerações, quais os benefícios a aplicação desta tecnologia pode trazer, podendo assim, justificar a sua relevância e a importância da sua integração com a segurança do mundo digital. São apresentados exemplos de possíveis aplicações em processo de implementação ou até mesmo em utilização dessa tecnologia inovadora e, para finalizar o artigo, a seção 5 apresenta as considerações finais.

2 METODOLOGIA DE PESQUISA

O método de pesquisa adotado no desenvolvimento deste artigo foi a pesquisa bibliográfica. De acordo com Pizzani et al. (2012, p. 54), a pesquisa bibliográfica é realizada por meio de fontes de pesquisa, livros, artigos, periódicos, simpósios, *sites* da internet referentes ao tema em estudo, ou seja, a pesquisa bibliográfica pode ser definida como “a revisão da literatura sobre as principais teorias que norteiam o trabalho científico”. Portanto, “a pesquisa bibliográfica é uma das etapas da investigação científica e - por ser um trabalho minucioso - requer tempo, dedicação e atenção por parte de quem resolve empreendê-la”. (PIZZANI et al. 2012, p. 53).

3 *BLOCKCHAIN*: A TECNOLOGIA POR DETRÁS DO *BITCOIN*

Seria impossível explanar sobre a tecnologia *blockchain* sem relacioná-la com as criptomoedas virtuais, mais precisamente o *Bitcoin*, pois a existência de ambos está profundamente relacionada. O *Bitcoin* pode ser definido segundo Swan (2015) como uma moeda digital independente de um banco ou governo que utiliza técnicas de criptografia para realizar transferências e pagamentos em seu sistema, e junto com o advento da moeda surgiu uma nova tecnologia voltada para resolução do problema do "gasto duplo", a tecnologia *blockchain* ou *Distributed Ledger Technology* (DLT).

"O *blokchain* surgiu com a criptomoeda *Bitcoin* e tinha por objetivo ser um livro-razão em que todas as transações financeiras de todos os usuários de *Bitcoin* ficassem armazenadas de forma a não ocorrer o problema de gasto duplo [...]" explicam Lucena e Henriques (2016, p. 1). Verifica-se que os autores reafirmam a relação entre o *Bitcoin* e a tecnologia *blockchain*, sendo essa a responsável por toda a segurança e armazenamento das transações da criptomoeda virtual; com outro ponto de vista pode-se definir a tecnologia como um banco de dados decentralizado.

A mesma definição é apresentada por Swan (2015) onde o *blockchain* é o livro-razão público onde todas as transações de uma criptomoeda virtual são armazenadas, sendo que novos blocos de armazenamento são adicionados constantemente por meio da mineração, isto quando se analisa o *blockchain* pelo ponto de vista das criptomoedas virtuais, já que existem diversas alternativas ao *Bitcoin* que utilizam a mesma premissa.

3.1 A origem do *blockchain*

De acordo com Ulrich (2014) e Lucena e Henriques (2016) originalmente o *blockchain* foi idealizado por um programador anônimo sob o pseudônimo de Satoshi Nakamoto, em 2009, como uma forma de resolver o problema do "gasto duplo", pois nas transações *online* sempre era necessário um terceiro para intermediá-las, mas para sua criptomoeda virtual, o *Bitcoin*, esse problema foi resolvido removendo a necessidade do intermediário.

Nakamoto propôs que ao armazenar toda as transações em uma lista encadeada e de acesso livre para qualquer membro da rede, os dados se tornariam públicos e removeria a necessidade de um intermediário gerenciador para a rede e para as transações, explicam

Lucena e Henriques (2016), ou seja, assim formou-se o conceito inicial da *blockchain*, originalmente o livro-razão não centralizado das transações *Bitcoin*.

3.2 O funcionamento do *blockchain* no *Bitcoin*

Para explicar o funcionamento do *blockchain*, novamente o *Bitcoin* entra em foco, por ser a maior aplicação que utiliza essa tecnologia atualmente. O funcionamento do *blockchain* é fundamentado por cinco princípios idealizados por Nakamoto e utilizados nas criptomoedas virtuais, explicam Lucena e Henriques (2016, p. 2), que são: "funções de mão única" (*hash*), "registro do tempo de criação ou modificação do arquivo" (*timestamp*), "assinatura digital do autor da alteração do arquivo", "rede descentralizada *peer-to-peer"*, "mecanismo de geração de um novo bloco do *blockchain"*.

De acordo com Kurose e Ross (2006, p. 533) "[...] uma função de *hash* pega uma entrada de dados, m, e processa uma cadeia de tamanho fixo conhecida como *hash*", ou seja, essa função de mão única gera uma cadeia de tamanho fixo que é improvável de retornar ao valor de entrada (*input*), por isso mão única. Lucena e Henriques (2016) explicam que o *blockchain* utiliza a função *hash* com o intuito de impossibilitar modificações dos arquivos digitais armazenados dentro deles, além de cada novo bloco utilizar a saída (*output*) da função do bloco anterior para gerar um novo bloco, interligando todos os blocos, por isso o nome *blockchain*, de maneira que qualquer modificação afetaria todos os blocos depois dele, sendo assim facilmente identificado por todos na rede.

O *timestamp* tem como finalidade dificultar e impossibilitar fraudes no *blockchain*. Nakamoto (2008, p. 2) explica que "o *timestamp* prova que os dados devem ter existido no momento, obviamente, para entrar no *hash*", ou seja, comprovando a existência na hora do registro no *blockchain*. "A assinatura digital, por sua vez, visa garantir que toda e qualquer alteração em algum elemento pertencente a determinado nó da rede *blockchain* foi realizada pelo proprietário do par de chaves pública e privada daquele nó", explicam Lucena e Henriques (2016, p. 2), assim acrescentando mais um elemento de segurança ao *blockchain*, identificando o proprietário ou portador das chaves pública e privada garantindo que somente ele realize modificações. Para Kurose e Ross (2006, p. 530) "a assinatura digital é uma técnica criptográfica usada para cumprir essa finalidade no mundo digital", uma forma de garantir a propriedade de um arquivo ou dado.

Segundo Swan (2015) a combinação da rede *peer-to-peer* com a criptografia de chaves pública e privada no *blockchain*, foi a principal forma de resolver o problema de gasto duplo. "A rede descentralizada *peer-to-peer*, por sua vez, é crucial para o funcionamento de um *blockchain*, pois desta forma todas as alterações (acréscimos) no mesmo podem ser conferidas e aceitas (ou rejeitadas) pela maioria dos *peers* [...]", complementam Lucena e Henriques (2016, p. 2) demonstrando a importância da rede *peer-to-peer* para o *blockchain*.

O mecanismo de geração de novos blocos do *blockchain*, no caso das criptomoedas virtuais é chamado de mineração. Esse processo utiliza várias operações matemáticas complexas que resultando em uma competição entre os mineradores, aquele que achar primeiramente a solução, insere um novo bloco ao *blockchain*, e é recompensando com um bônus normalmente alguma quantia da criptomoeda, explica Swan (2015). Segundo Ulrich (2014, p. 20) "no caso do *Bitcoin*, a busca não é por números primos, mas por encontrar a sequência de dados (chamada de "bloco") que produz certo padrão quando o algoritmo "*hash*" do *Bitcoin* é aplicado aos dados". Segundo Ulrich (2014, p. 20) "quando uma combinação ocorre, o minerador obtém um prêmio de bitcoins [...]", ou seja, no caso das moedas digitais, a mineração é uma forma de manter o *blockchain* funcionando, adicionando novos blocos, aumentando assim sua capacidade de armazenamento e retribuindo aqueles que o fazem.

Nakamoto (2008) propôs que os blocos do *blockchain* armazenassem os dados das transações em forma de uma árvore de Merkler (*Merkler tree*), pois assim evitaria que o *hash* dos blocos fosse quebrado. Segundo Lucena e Henriques (2016) cada transação tem seu *hash* calculado, usando também o *hash* da transação anterior, e quando o valor final das transações é obtido, recebe o nome de *Merkler root* ou raiz de Merkler, e por fim é calculado a raiz de Merkler junto com a do bloco anterior do *blockchain*.

3.3 As características e limitações do *blockchain*

O *blockchain* pode apresentar vários usos além das criptomoedas, assim cada limitação ou característica pode se tornar uma vantagem ou desvantagem de acordo com sua aplicação. De acordo com Swan (2015) vários desafios técnicos foram encontrados na tecnologia, seja ela em modelos genéricos ou modelos específicos, vários desenvolvedores pensam em soluções próprias para superá-los e assim continuar o desenvolvimento da indústria do *blockchain.*

Nesse sentido, explica Swan (2015), não existe uma concordância de qual o melhor caminho para a evolução da tecnologia, alguns defendem que o padrão seja o *blockchain* do

Bitcoin. Por ter surgido junto com o *blockchain* e estarem profundamente conectados, além de possuir a maior infraestrutura e usuários, adotar o *blockchain* do *Bitcoin* pode gerar uma base padronizada para a tecnologia. Mas outros defendem *blockchains* independentes do *Bitcoin*, seja com novos ou separados, como *Ethereum* ou *Hyperledger*, ou até mesmo tecnologias que não se não usam *blockchain*, como o *Ripple*, completa Swan (2015), demonstrando as incertezas da evolução da tecnologia que pode prejudicar seu uso em larga escala no futuro. Swan (2015) listou as principais limitações que a padronização do *blockchain* do *Bitcoin* tem que superar para poder aumentar seu uso para as mais diferentes áreas:

- Taxa de Transferência (*Throughput*): a capacidade de realizações de transações por segundo (tps) é de apenas 7 tps, mas os desenvolvedores argumentam que caso seja necessário é possível aumentar tps. De acordo com o autor outras redes de processamento de transações como a Visa, realiza 2.000 tps normalmente e 10.000 quando ocorre um pico.
- Latência (*Latency*): cada transação realizada sofre de uma grande latência de no mínimo dez minutos para ser confirmada, caso a transação seja muito grande é possível levar horas, por motivo de segurança, antes da confirmação. O autor ressalta que a Visa leva apenas alguns segundos antes da confirmação.
- Tamanho e largura de banda (*Size and bandwidth*): com o aumento de números de transações como uma exigência para uma utilização global, haveria a consequência direta no aumento de tamanho. Segundo o autor caso seja realizado 150.000 tps, a quantidade de dados gerada seria de 214 PB (*Petabyte*) ou 224395264 GB (*Gigabyte*) por ano, esse aumento recebe o nome de "inchaço" (do inglês *bloat*), por ter como principal característica a descentralização, e o fato de não possuir um *Big Data* para armazenar dado, a utilização em larga escala é dificultada.
- Segurança (*Security*): umas das maiores preocupações quanto a segurança reside na centralização do registro das transações. Teoricamente se a competição para registrar novos blocos se concentra em apenas um minerador ou poucos mineradores, seria possível tomar o controle do *blockchain* e realizar o gasto duplo em sua própria conta, essa ameaça recebe o nome de "ataque de 51 por cento" (do inglês *51-percent attack*), isso representaria uma catástrofe completa e o fim do "*trueless*", termo em inglês que pode ser traduzido para algo como "sem confiança" no qual para realizar uma transação com *Bitcoin* não é necessário confiança entre as partes da transação, apenas no sistema.

- Desperdício de recursos (*Wasted resources*): “a mineração extrai uma enorme quantidade de energia, toda desperdiçada”, mas esse desperdício que torna a mineração confiável, entretanto, não traz benefício nenhum além da mineração. (SWAN, 2015, p. 83).
- Usabilidade (*Usability*): a *application Programming Interface* (API) do *Bitcoind*, programa que implementa o protocolo *Bitcoin* para a chamada de procedimento remoto, é complexa e oposta a padronização de outras API’s modernas existentes no mercado.
- Cadeias múltiplas (*multiple chains*): com a possível popularização do *blockchain* e o surgimento de novos *blockchains*, se tornaria cada vez mais fácil realizar um “ataque de 51 por certo” nos *blockchains* menores, ou ainda pior, caso seja realizado bifurcações nos *blockchains*, sendo impossível integrar esses dados novamente.

4 AS GERAÇÕES E APLICAÇÕES DA TECNOLOGIA *BLOCKCHAIN*

A inovação que a tecnologia *blockchain* trouxe estende-se para além das criptomoedas virtuais, segundo Lucena e Henriques (2016) a sua importância pode ser equiparada com o surgimento da *Internet*. A redação do The Economist (2015) em um artigo especial, classificou a tecnologia *blockchain* como “a próxima grande coisa” e explica que falta apenas um *software* assassino ou “*killer app*” para que encontre um uso para ela, do mesmo jeito que os navegadores tornaram a *Internet* útil, para que comece a crescer sua popularidade.

Empresas como a *Telegram*, responsável por um dos aplicativos de mensagens instantâneas mais utilizados do mundo, pretende investir em seu próprio *blockchain* em uma rede chamada *Telegram Open Network* (TON) na qual o *blockchain* fará parte. Com isso a empresa buscaria lançar sua própria criptomoeda virtual, chamada “*Gram*” e integraria vários serviços ao seu mensageiro criptografado relacionado a sua moeda digital, explica Sumares (2018) e de acordo com Matos (2017) algumas *startups* brasileiras já estão começando a utilizar a tecnologia no Brasil.

4.1 *Blockchain* 1.0, *Blockchain* 2.0 e *Blockchain* 3.0

De acordo com Swan (2015, p. 9) “[...] a tecnologia *blockchain* começa a deixar evidente que é potencialmente uma tecnologia extremamente disruptiva, que poderia ter a capacidade de reconfigurar todos os aspectos da sociedade e suas operações” e por razão de todo esse potencial e conveniência, a autora explana que todas as diferentes atividades que o

blockchain pode desempenhar foram fragmentadas em três gerações ou categorias. No entanto, para Gates (2017) a divisão é feita em apenas duas gerações, sendo que a segunda geração de Gates engloba a segunda e a terceira geração de Swan em uma só.

A primeira geração foi denominada *Blockchain* 1.0: moedas digitais, marcada pelo surgimento da tecnologia e pelas criptomoedas virtuais, explica Swan (2015). No que tange à tecnologia *blockchain* "[...] pode se tornar a Internet do Dinheiro conectando as finanças da mesma forma que a Internet das Coisas (IoT) conecta as máquinas" (SWAN, 2015, p. 5). Ou seja, a primeira geração apresenta uma grande importância da revolução, na criação do conceito de criptomoedas virtuais e na forma atual que realizamos transações pela *internet*.

Segundo Gates (2017) a segunda geração recebe o nome de *Blockchain* 2.0: contratos inteligentes e surgiu com o lançamento do *blockchain* do *Ethereum*, um ambiente que utiliza uma máquina virtual para executar aplicações descentralizadas que aceita apenas sua própria criptomoeda digital chamada *Ether* como forma de pagamento para a execução da máquina virtual, os contratos inteligentes e as aplicações descentralizadas é a evolução que a segunda geração trouxe. Para Swan (2015) enquanto a primeira geração é marcada pela descentralização do dinheiro, a segunda é pela descentralização dos mercados de forma genérica. Além disso, Swan (2015, p. 10) explica que usando o *blockchain* do *Bitcoin* ou utilizando seu próprio separado "[...] ainda utilizam o mesmo modelo de arquitetura técnica descentralizada da pilha de três camadas: *blockchain*, protocolo e moeda", mesmo em gerações diferentes o *blockchain* não muda sua arquitetura, apenas sua finalidade, a principal diferença entre Gates e Swan é que para Swan a segunda geração engloba apenas as áreas financeira e econômica, as outras áreas pertencem a terceira geração.

Para Gates (2017) não existe essa divisão entre a segunda e a terceira geração de Swan, pois na ótica do autor é apenas uma. Swan (2015) explica que a terceira geração recebe o nome de *Blockchain* 3.0: aplicações eficientes e coordenadas além das criptomoedas, economia e mercados. Essa geração é marcada pelo uso do *blockchain* pelas ciências de forma geral, onde indivíduos contribuem de forma individual com o poder computacional para pesquisas e projetos, mas também essa geração contempla outras áreas diferentes de finanças, economia e mercados, como áreas governamentais.

4.2 As aplicações da tecnologia

Como a primeira geração da tecnologia *blockchain* é basicamente as criptomoedas virtuais, serão abordadas as gerações posteriores. A segunda geração de Gates apresenta muita utilidade para o mercado, principalmente relacionada a áreas financeiras e governamentais. Gates (2017) lista algumas atividades na área financeira que o *blockchain* pode desempenhar ou já desempenha em algumas instituições no mundo:

- Transferências de valor entre companhias e países pode se beneficiar com o aumento da velocidade das transações usando a tecnologia *blockchain*.
- A substituição das várias camadas de autenticação pela tecnologia *blockchain* pode dar transparência as diversas transações.
- A utilização da tecnologia *blockchain* para substituir intermediários no mercado de compra e vendas de ações.
- Livros-razão manuais sendo substituído pela tecnologia tanto em administrações públicas como em privadas.

Ainda segundo Gates (2017) o *The Bank of England* está investindo nessa tecnologia com um time totalmente dedicado, espera-se aumentar a defesa contra *ciberataques* e tornar as transações mais rápidas. Além disso, essa primeira etapa a tecnologia será usada apenas internamente, mas espera-se que até 2020, o banco abra a tecnologia para mais empreendimentos que desejam utilizá-la. Para Swan (2015, p. 10) "todas as transações financeiras podem ser aplicadas a tecnologia *blockchain*" e segundo a autora isso inclui até mesmo *crowdfunding*, ou financiamento coletivo, fundos mútuos e pensões. Além disso a autora explica que registros públicos também podem utilizar a tecnologia, como títulos de propriedades, passaportes, certificados de casamento, certificados de óbito, entre outros, mas esses pertencem a terceira geração na ótica de Swan,

Gates (2017) concorda que o *blockchain* tem várias utilizadas além da área financeira e principalmente na segurança digital. O autor define algumas áreas que o *blockchain* pode desempenhar além das áreas financeiras e econômicas:

- Identidades digitais: Lucena e Henriques (2016, p. 03) explanam que como a tecnologia *blockchain* é resistente a alterações "é esperado que identificadores pessoais (carteira de identidade, passaporte, carteira de motorista, cartão de crédito, etc.) alcancem outro patamar de segurança, se a eles for aplicado as características de um *blockchain*", Gates (2017, p. 67) acrescenta ainda que a tecnologia pode resolver boa parte das falhas de

segurança atuais nas identidades digitais e explica que “um sistema de identificação baseado no *blockchain* fornece assinaturas digitais usando criptografia”, pois “[...] são únicos, irrefutáveis, seguros e quase impossível de duplicar ou acessar sem autorização”, ou seja, por tratar de dados sensíveis, a tecnologia forneceria um nível de segurança muito maior que o atual.

- Votação eletrônica: de acordo com Gates (2017, p. 67) “a votação eletrônica é uma tecnologia que falhou em ser implementada com sucesso em vários países por causa dos riscos de segurança e preocupação com a privacidade”. Além disso, segundo Lucena e Henriques (2016, p. 03) “os principais modelos atuais de votações eletrônicas são centralizados e a totalização dos votos é normalmente realizada após a transferência do conteúdo da memória de cada urna para o órgão controlador da eleição” e, desta forma, segundo os autores permite brechas para a adulteração dos votos antes das transferências, Gates (2017) propõe que um sistema de votação baseado na tecnologia *blockchain* seria capaz de aumentar a acessibilidade das pessoas as eleições, principalmente por causa que o sistema poderia verificar se um voto foi transferido com sucesso e garantir a privacidade do eleitor.
- Saúde e registros médicos: Para Swan (2015, p. 59) os “registros médicos pessoais poderiam ser armazenados e administrados via *blockchain* como um vasto sistema de prontuários médicos eletrônicos”. Para Gates (2017) um sistema de prontuário médico decentralizado que pode ser acessado por médicos, enfermeiros, hospitais, entre outros pode salvar vidas, principalmente se for em casos de complicação cirúrgica, pois o cirurgião de plantão pode ter acesso a todo histórico médico do paciente, desde o tipo sanguíneo até alergias a medicamento.
- Certificados acadêmicos: Gates (2017) explica que a tecnologia pode trazer transparência para os registros acadêmicos, poupando dinheiro na verificação manual e impossibilitando fraudes sobre os certificados.
- Mídias digitais: para Lucena e Henriques (2016, p. 3) “o uso de *blockchain* na distribuição de conteúdo multimídia poderá fazer com que qualquer arquivo de música ou filme possa ser utilizado apenas pelo dono de determinado nó, impossibilitando a cópia [...]”. Além disso Gates (2017) explica que a tecnologia pode mudar totalmente o meio que as músicas são vendidas e distribuídas para os usuários e a forma que os artistas licenciam os arquivos.
- Armazenamento em nuvem: para Lucena e Henriques (2016, p. 03) “[...] será cada vez mais comum encontrar no futuro sistemas de armazenamento distribuídos baseados

no conceito de *blockchain*". Segundo Gates (2017) armazenamentos em nuvem centralizado são vulneráveis, por esse motivo o autor propõe um sistema de armazenamento descentralizado usando a tecnologia *blockchain*.

Outras áreas que podem se beneficiar evoluir com a tecnologia *blockchain* segundo Gates (2017) e Swan (2015) são: aluguel de carros, compartilhamentos de carona, propriedades, aluguel de apartamentos, indústria de viagens, programas de fidelidade/recompensas, indústria de apostas, contratos inteligentes, entre outras.

Existem algumas implementações da tecnologia em algumas áreas, desde empresas até governos já reconheceram as possibilidades que o *blockchain* oferece e já estão começando a implementação em alguns setores. Segundo a redação da Forbes (2017) a cidade de Dubai planeja implantar a tecnologia até 2020 e se tornar o primeiro governo do mundo a usar largamente o *blockchain*, e com isso a cidade esperar economizar US$ 1.5 bilhões anualmente. Outro governo que começou a implementar a tecnologia é o da Estônia. De acordo com Gates (2017) e Hernandez (2017) os registros médicos dos cidadãos estão disponíveis em um portal gratuitamente para 98% da população do país, além de já estar desenvolvendo um sistema de identificação digital baseado na tecnologia. O governo da Dinamarca usou em 2014 a tecnologia para votações eletrônicas em pequena escala, explica Gates (2017). Inclusive o Brasil já começou a dar seus passos na implementação do uso do *blockchain*, existe o estudo de implantar a tecnologia para armazenar as assinaturas de petições para criação de projeto de leis, explica Payão (2017). E de acordo com Gates (2017) empresas como a *Spotify*, uma gigante do *streaming* de músicas, já comprou uma *startup* que desenvolveu um sistema baseado no *blockchain* que permite aos artistas criar registros digitais para músicas no *blockchain* do *Bitcoin,* e a empresa espera com o tempo criar um ambiente de pagamentos mais transparente para os artistas no seu serviço.

5 CONSIDERAÇÕES FINAIS

O propósito deste artigo foi investigar a tecnologia que possibilitou a criação do *Bitcoin*, a tecnologia *blockchain*, demonstrar sua importância e relevância em diversas aplicações. Em relação as teorias envolvidas, conclui-se que a tecnologia *blockchain* nasceu como o livro-razão descentralizado da criptomoeda virtual *Bitcoin*, mas diversas iniciativas buscam se aprofundar nos desenvolvimentos de aplicações baseadas na tecnologia para

otimizar custos e/ou garantir maior privacidade, pincipalmente com dados sensíveis como na identificação digital e em votação eletrônica.

O *Bitcoin* revolucionou o mundo das transações e pagamentos digitais, mas por ser independente e decentralizada, vários governos buscam formas de regularizar ou simplesmente banir as transações com a criptomoeda, pois elas são relativamente difíceis de rastrear. Além do fato de que o preço da moeda enfrenta sequentes quedas, principalmente por causa de cercos de diversos governos que estão proibindo, em seus respectivos países, as transações ou comercialização do *Bitcoin*. Em uma visão mais pessimista, caso a moeda deixe de existir algum dia, toda inovação e a revolução que a tecnologia *blockchain* trouxe com o advento da criptomoeda virtual, beneficiará várias áreas diferentes da financeira, podendo até mesmo salvar vidas em sistemas de prontuários descentralizados ou garantindo o direito de exercer a cidadania, por meio do voto com transparência, privacidade, segurança e principalmente confiança no sistema.

Conclui-se, finalmente, que mesmo tendo seu início como personagem secundário, por detrás do *Bitcoin*, a tecnologia *blockchain* encontra-se em ascensão no mundo da tecnologia para se tornar a protagonista na revolução da distribuição de dados atuais, desde de serviços de armazenamento em nuvem até a forma que exercemos o direito ao voto. A *blockchain* promete garantir transparência, segurança e privacidade, despertando interesse em outras diversas áreas que buscam utilizar essa tecnologia, tudo isso atrelado a possibilidade de diminuir custos e melhorar o acesso a diversos serviços, demonstrando que a tecnologia está em constante evolução.

REFERÊNCIAS

FORBES. **Dubai irá se tornar o primeiro governo movido por blockchain**. Disponível em: <http://forbes.uol.com.br/negocios/2017/12/dubai-ira-se-tornar-o-primeiro-governo-movido-por-blockchain/>. Acesso em: 12 jan. 2018.

GATES, Mark. **Blockchain:** Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. Breinigsville, Pensilvânia: Createspace Independent Publishing Platform. 2017. 126 p.

HERNANDEZ, Raphael. **Governo da Estônia usa blockchain para guardar registros de pacientes**. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/04/1875751-governo-da-estonia-usa-blockchain-para-guardar-registros-de-pacientes.shtml>. Acesso em: 12 jan. 2018.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006. 634 p.

LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. **Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum**. In: IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP, 9, 29-30 de setembro, Campinas, São Paulo, 2016. Disponível em: <http://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf>. Acesso em: 06 jan. 2018.

MATOS, Felipe. **Fintechs usam blockchain para simplificar crédito no Brasil**. 2017. Disponível em: <http://link.estadao.com.br/blogs/felipe-matos/fintechs-usam-blockchain-para-simplificar-credito-no-brasil/>. Acesso em: 05 jan. 2018.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 05 jan. 2018.

PAYÃO, Felipe. **Brasil poderá usar Ethereum para armazenar votos de cidadãos**. 2017. Disponível em:< https://www.tecmundo.com.br/seguranca/125809-brasil-usar-ethereum-armazenar-votos-cidadaos.htm>. Acesso em: 05 jan. 2018.

PIZZANI, Luciana et al. **A arte da pesquisa bibliográfica na busca do conhecimento**. In: Revista Digital de Biblioteconomia e Ciência da Informação, Campinas, São Paulo, v.10, n. 1, p.53-66, jul. 2012. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/1896>. Acesso em: 06 jan. 2018.

SUMARES, Gustavo. **Telegram pretende arrecadar mais de R$ 3,88 bilhões com sua própria criptomoeda**. 2018. Disponível em: <https://olhardigital.com.br/noticia/telegram-pretende-arrecadar-mais-de-r-3-88-bilhoes-com-sua-propria-criptomoeda/73384>. Acesso em: 11 jan. 2018.

SWAN, Melanie. **Blockchain:** Blueprint for a New Economy. Sebastopol, California: O'Reilly Media Inc., 2015. 149 p.

THE ECONOMIST. **The next big thing**. Disponível em: <https://www.economist.com/news/special-report/21650295-or-it-next-big-thing>. Acesso em: 11 jan. 2018.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 106 p.