RECETT
REVISTA ELETRONICA CIENTIFICA DA
ESCOLA TÉCNICA TUPY

BLOCKCHAIN: A TECNOLOGIA QUE ESTÁ MUDANDO O MUNDO

Germano Sprotte, Vinicius Gabriel Azevedo, Gabriel Rieper[1]
Talita Caroline Oliveira Schmitt, Valter Niehues[2]

RESUMO

O surgimento do Bitcoin, junto com sua tecnologia de base, o Blockchain, começaram por revolucionar o mercado financeiro com a proposta de um sistema totalmente descentralizado. Essa tecnologia oferece um sistema de ponto-a-ponto, não necessitando de intermediários, assim, reduzindo a burocracia, o tempo, e as altas taxas cobradas por bancos e casas de câmbio em geral. Este artigo foi feito por meio de uma pesquisa teórica exploratória enriquecida com artigos científicos e sites especializados no assunto, que juntos abordam o tema Blockchain. Destacando suas aplicações a nível mundial, averigua sua segurança, explicando seu funcionamento e o surgimento dessa tecnologia, bem como, a sua evolução. Nesse, ressalta-se também os importantes resultados e benefícios que essa tecnologia traz ao mundo. Concluindo que esta, ainda é uma tecnologia muito nova que está sendo aos poucos aderida pela população, mas com potencial para mudar a forma como muitas coisas vem sendo feitas há vários anos.

Palavras-chave*:* Bitcoin, Blockchain*,* Criptomoedas*, Smart Contracts, Ethereum, peer-to-peer.*

ABSTRACT

The emergence of Bitcoin, along with its basic technology, Blockchain, began by revolutionizing the financial market with the proposal of a totally decentralized system. This technology offers a point-to-point system, requiring no intermediaries, thus reducing bureaucracy, time, and the high fees charged by banks and bureaux de change in general. This article was made through an exploratory theoretical research enriched with scientific articles and specialized websites, which together approach the theme Blockchain. Highlighting its applications worldwide, it ascertains its safety, explaining its operation and the emergence of this technology, as well as its evolution. In this, it is also highlighted the important results and benefits that this technology brings to the world. Concluding that this is still a very new technology that is being gradually adhered to by the population but with potential to change the way many things have been done for several years.

[1] Acadêmicos autores do texto.
[2] Professor Orientador e Co-orientador do texto.

Keywords: Bitcoin, Blockchain, Criptomoedas, *Smart Contracts, Ethereum, peer-to-peer.*

1. INTRODUÇÃO

Este trabalho foi feito com base em uma pesquisa exploratória, abordando o tema Blockchain, centralizado no potencial dessa tecnologia revolucionária.

O objetivo geral deste trabalho é analisar as possibilidades de aplicações do Blockchain, bem como mostrar o quão importante é essa tecnologia que vem revolucionando o mundo. Além de mostrar de onde surgiu, como funciona e quão segura pode ser a rede Blockchain.

O trabalho está organizado em 3 capítulos, sendo o primeiro para o desenvolvimento do tema, o segundo optamos por abordar a metodologia usada que foi uma pesquisa teórica exploratória enriquecida com artigos científicos e sites especializados no assunto. O terceiro capítulo foi utilizado para explicar os resultados e discussões que surgiam no decorrer do trabalho.

2. SURGIMENTO DO BITCOIN/BLOCKCHAIN

Segundo Ulrich (2016), “ Bitcoin é uma forma de dinheiro, assim como o Real, Dólar ou Euro, com a diferença de ser puramente digital (criptomoeda) e não ser emitido e intermediado por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro. ”

A tecnologia por trás dessa criptomoeda chama-se Blockchain, um sistema *A Peer-to-peer Eletronic Cash System* (Sistema de dinheiro ponto-a-ponto) de código aberto, que nasce junto do Bitcoin para resolver o gasto duplo, que é basicamente a possibilidade de um usuário gastar duas vezes o mesmo dinheiro.

Antes do Bitcoin, outros projetos de moedas digitais falharam por não conseguirem resolver o problema do gasto duplo. Em 2008, foi publicado em uma comunidade de

criptografia, um *paper* de um pseudônimo, *Satoshi Nakamoto*, que dizia ter criado um sistema puramente *peer-to-peer (P2P)*, uma criptomoeda chamada Bitcoin (BTC). Em 2009, *Nakamoto* disponibilizou o sistema para mineração e transação do Bitcoin ao público (MATOS, 2018).

2.1 COMO FUNCIONA O BLOCKCHAIN

O Blockchain é uma rede distribuída, não existe intermediários para realizar e validar uma transação, muito menos alguém para cobrar altas taxas de operação. Basicamente todos os computadores dentro dessa rede (também conhecidos como nós) precisam reconhecer a transação para ela se tornar válida.

A unidade de informação no Blockchain é chamada de transação, não necessariamente representa dinheiro, ativos financeiros, pode ser qualquer coisa, desde música, até uma propriedade. Cada usuário e transação possui uma identificação própria, de modo que sem esses dados de identificação é impossível saber quem está por trás daquele processo. Assim, há a transparência, partindo do pressuposto que a transação está registrada em todos os computadores da rede e qualquer um pode ver, e ao mesmo tempo privacidade, já que se necessitam os dados de identificação da transação e das partes envolvidas para visualização. Dentro do Blockchain essas transações serão agrupadas em formas de blocos, é daqui que o nome da ferramenta se origina (PROOF, 2016).

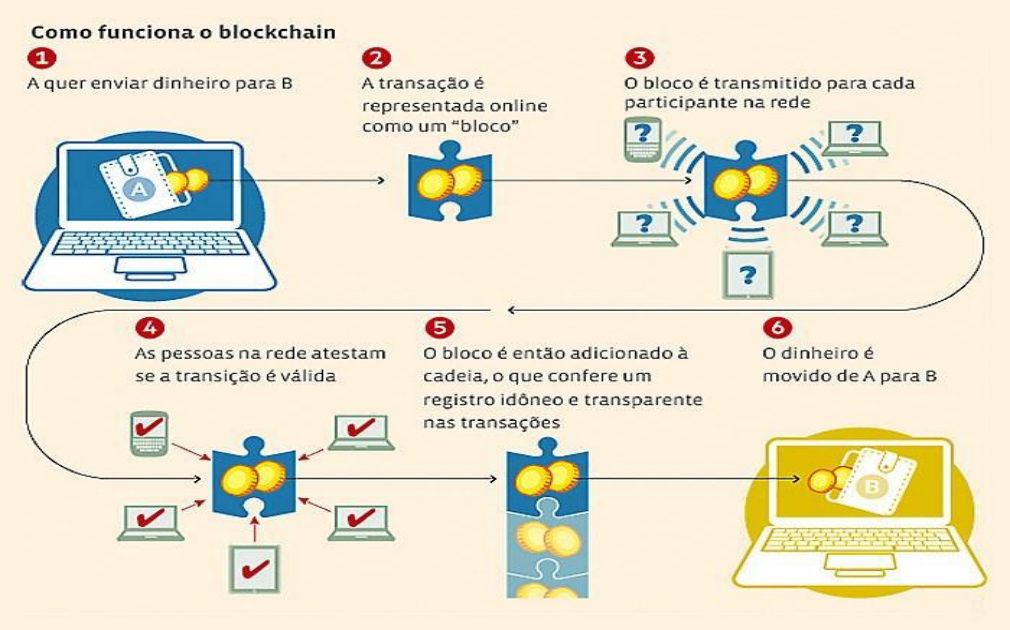
Para os blocos serem feitos é preciso respeitar algumas regras como: um tamanho máximo de transações que um bloco pode comportar e conter apenas transações que sejam verificadas como válidas, onde as duas partes envolvidas tenham aceitado a troca. Enquanto as transações esperam para serem adicionadas em algum bloco, elas ficam temporariamente em uma estrutura chamada de *pool*. Os computadores da rede competem entre si para ver quem consegue encontrar um bloco válido primeiro dentro da *pool*. O computador que encontra um bloco válido avisa os demais para que se faça a checagem e que haja um consenso de validação. Assim que validado pela rede, o bloco ganha um *Proof*

of Work (POW), um *hash*, código composto por números encriptados que serve como um "protocolo" de que aquela transação é válida. E um *Proof of Stake* (POS), um protocolo que certifica que aquele usuário é dono daquela informação.

Após o bloco ser criado e validado pela rede, ele será adicionado a cadeia de blocos da rede, o Blockchain. Esse novo bloco é inserido de modo sintagmático, dessa forma, uma das características essenciais do bloco é fazer referência ao bloco anterior, contendo informações do bloco anterior no novo bloco. Sempre de modo criptograficamente seguro (PROOF, 2016).

Na Figura 1, pode-se observar um exemplo prático de uma transação de criptomoeda via Blockchain.

Figura 1: Como funciona o Blockchain



Fonte: Navcom (2018).

2.2 SEGURANÇA DO BLOCKCHAIN

No Blockchain, a confidencialidade é garantida pela criptografia, que utiliza uma estrutura de chaves públicas e privadas. A *PKI* (*public key infrastructure*) é composta de pares de chaves públicas e privadas para garantir que somente participantes envolvidos em uma transação visualizarão a informação. Quando um remetente envia um dado para

um destinatário, o remetente utiliza a chave pública do destinatário para encriptar o dado. Somente o destinatário, com a chave privada que lhe corresponde, poderá des-encriptar a informação (MADEIRA, 2017).

Blockchain também garante a unicidade e a “não obstrução” da informação, graças a geração de uma chave *hash*, própria do *set* de informação já criptografada. Adicionalmente, Blockchain garante a veracidade do remetente mediante uma assinatura digital. Para gerar esta assinatura, Blockchain adiciona uma chave privada própria do emissor (criptografia simétrica) no dado original, executa o *hashing* da informação criptografada e a re-encripta com a chave pública do receptor. Mediante este processo, o dado é assinado digitalmente pelo emissor (certificado auto assinado) (MADEIRA, 2017).

Ainda segundo Madeira (2017), “Para que alguém não autorizado consiga quebrar esta arquitetura de segurança, deverá investir uma capacidade computacional de um supercomputador, que consumira 263 *Terawatts* por hora (TWh) e contar com 1 bilhão de anos de tempo livre. ”

2.3 *Smart Contracts*

Em sua primeira geração, o Blockchain era usado apenas como base de funcionamento para o Bitcoin, sendo uma forma segura para transferir Bitcoins, ou outras criptomoedas, de uma pessoa para outra.

Em 2014, inicia-se a segunda geração dessa tecnologia com o surgimento do *Ethereum*, uma plataforma de código aberto, que aplica os conceitos do Blockchain em outras áreas que não sejam só o dinheiro. Essa plataforma trouxe a possibilidade de desenvolvedores criarem contratos inteligentes (*Smart Contracts*) que são executados automaticamente quando certas condições são cumpridas. Todas as transações e contratos estabelecidos dentro da rede *Ethereum* são pagas em *Ether* (Criptomoeda exclusiva dessa rede, ETH). A partir disso, as aplicações do Blockchain (item 2.4) se expandiram ainda mais (ETHEREUM FOUNDATION, 2018; CRUZ, 2018).

2.4 APLICAÇÕES DO BLOCKCHAIN

Sendo o Blockchain uma tecnologia de código aberto, que pode ser utilizada e reinventada por qualquer pessoa, temos infinitas possibilidades de aplicações.

Segundo Tapscott (2016) essa é a oportunidade de criar uma economia compartilhada real. Empresas como *Uber* ou *AirBNB* são identificadas como parte de uma economia compartilhada, mas elas são um sucesso justamente porque não dividem nada. Essas companhias são agregadoras de serviços. Se o *Uber* ou *AirBNB* fossem uma aplicação distribuída em uma Blockchain, o *AirBNB* poderia se chamar *BAirBNB*, ou, *BlockchainAirBNB*. Nele, você acharia um lugar para passar uns dias, usando apenas uma base de dados baseada em Blockchain, sem intermediários. Automaticamente você cria um *Smart Contract* com o locador, aparece no local, abre a porta, e um pagamento parcial é registrado no contrato. Então, na saída, você fecha a porta e o pagamento completo é feito e também registrado. Você faz sua avaliação do local por meio de estrelas e tudo é imutável, pois está registrado dentro de uma Blockchain. Não há necessidade de uma empresa como a *AirBNB* para intermediar, pois tudo pode ser feito pelas próprias partes interessadas (KOHN, 2018).

No mundo da música, por exemplo, o Blockchain pode-se garantir os direitos autorais dos compositores. A cantora britânica *Imogen Heap* está criando uma plataforma baseada em Blockchain chamada de *Mycelia*. Esta rede Blockchain permite que o artista coloque sua música dentro de um *Smart Contract* e o próprio contrato gerencia o seu uso. Para escutá-la, você paga X, para colocá-la em um filme paga outro valor, para usá-la como *ringtone*, outro valor. Desta forma, a música se torna um negócio e protege os direitos do artista, coletando *royalties*. Isso não está restrito a músicos, mas cientistas, jornalistas, escritores e artistas de diversas áreas (KOHN, 2018).

Com a Internet das Coisas (*IoT*) ganhando popularidade, e vários objetos se tornando “Inteligentes”, esses, precisarão registrar suas informações. Uma lâmpada que compra energia de uma empresa distribuidora, por exemplo, poderá fazer negócios sozinha se tiver sua identidade registrada em uma Blockchain. Um exemplo é a *Brooklin MicroGrid*, uma distribuidora de energia feita por pessoas e baseada em Blockchain. Essa rede de pessoas possui painéis solares em suas casas e um vende energia para o outro por meio da

Blockchain, sem precisar de intermediadores, pois os dispositivos são registrados na cadeia de blocos (KOHN, 2018).

3. MATERIAIS E MÉTODO

O artigo consiste em uma pesquisa teórica exploratória, onde foram abordados assuntos diretamente relacionados ao tema e também assuntos relevantes, que justificam o tema escolhido. Por ser um trabalho de pesquisa exploratória, não haverá descritivo de materiais e procedimentos técnicos.

4. RESULTADOS E DISCUSSÕES

Mostrou-se nesse artigo o potencial da tecnologia em questão que, desde 2008, quando surgiu junto ao Bitcoin, vem revolucionando a forma como coisas já denominadas “tradicionais” vem sendo feitas.

Primeiramente resolvendo o problema do gasto duplo e possibilitando uma forma de dinheiro puramente digital e descentralizada. Dessa forma o Blockchain muda o velho conceito de mercado financeiro, com moedas inflacionárias emitidas por governos. Com o Bitcoin não há inflação, devido ao mesmo possuir um protocolo (Protocolo Bitcoin) que define uma quantidade finita de moedas há serem “mineradas” (21 milhões de BTC), dentre outras regras (PIROPO, 2014). Tem-se como resultado, uma alternativa de dinheiro viável e segura as pessoas.

Ao separar Blockchain do Bitcoin, e aplicar seu conceito a outras áreas do cotidiano, o mesmo mostrou trazer benefícios incríveis. A rede Ethereum trouxe a possibilidade de usuários criarem contratos inteligentes e auto executáveis, resultando na diminuição de taxas por terceiros, e na confiança das partes entre si. Devido ao fato desse contrato ser estruturado em Blockchain, uma vez estabelecidos os termos, o contrato só é executado se todos os termos forem cumpridos.

5. CONCLUSÃO

Neste trabalho ficou evidenciado que a tecnologia Blockchain vem trazendo grandes avanços nas atividades cotidianas em razão da possibilidade de enviar unidades de Criptomoedas para qualquer lugar mundo de forma rápida, segura e imune a praticamente qualquer tipo de fraude. Além disso, proporciona mudanças também principalmente pelo fato de possibilitar que sejam realizadas transações que vão além de valores, pelo fato da segunda geração dessa tecnologia chamada contratos inteligentes (*Smart Contracts*), sem deixar citar a segurança e aplicações do Blockchain.

Sendo assim, é possível concluir que o Blockchain ainda é uma tecnologia muito nova, mas que vem crescendo de forma exponencial, devido a todos seus protocolos de segurança e confiança. É uma questão de tempo até que a mesma ganhe mais popularidade, mudando muitos mercados já considerados tradicionais.

REFERÊNCIAS

ENTENDA BLOCKCHAIN EM MENOS DE 15 MINUTOS: NÃO É MAGIA, É TECNOLOGIA. NÃO É MAGIA, É TECNOLOGIA. 2016. Disponível em: <https://www.proof.com.br/blog/blockchain/>. Acesso em: 22 maio 2018.

NAVCOM. **Blockchain e Bitcoin.** 2018. Disponível em: <http://navcombrasil.com.br/2018/04/09/blockchain-e-bitcoin/>. Acesso em: 24 maio 2018.

MADEIRA, Bernardo de Souza. **Desmistificando a Segurança no Blockchain e entendendo o Potencial:** Privacidade e segurança dos bens. 2017. Disponível em: <https://cryptoid.com.br/banco-de-noticias/o-blockchain-e-seguro/>. Acesso em: 29 maio 2018.

ULRICH, Fernando. **Dez formas de explicar o que é Bitcoin.** 2014. Disponível em: <http://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/3160782/dez-formas-explicar-que-bitcoin>. Acesso em: 22 maio 2018.

BANDINELLI, Diéferson. **Uma breve história sobre a Blockchain.** 2017. Disponível em: <https://atlasproj.com/blog/uma-breve-historia-sobre-blockchain/>. Acesso em: 31 maio 2018.

MATOS, David. **Big Data e as Oportunidades com Blockchain:** O Que é Blockchain?. 2018. Disponível em: <http://www.cienciaedados.com/big-data-e-as-oportunidades-com-blockchain/#comments>. Acesso em: 03 jun. 2018.

ETHEREUM FOUNDATION (Zug) (Org.). **Ethereum Project.** 2018. Disponível em: <https://www.ethereum.org/>. Acesso em: 4 jun. 2018.

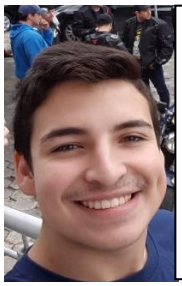
O QUE é Ethereum?: Definição de Ethereum. Definição de Ethereum. 2018. Disponível em: <https://www.buybitcoinworldwide.com/pt-br/ethereum/>. Acesso em: 04 jun. 2018.

KOHN, Stephanie. **Blockchain além da Bitcoin: 8 aplicações inovadoras.** 2018. Disponível em: <https://canaltech.com.br/mercado/blockchain-alem-da-bitcoin-8-aplicacoes-inovadoras-108566/>. Acesso em: 07 jun. 2018.

PIROPO, B.. **Bitcoin: uma moeda imune à inflação.** 2014. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2014/02/bitcoin-uma-moeda-imune-inflacao.html>. Acesso em: 13 jun. 2018.

BIOGRAFIA SINTETIZADA DOS AUTORES

Gabriel Rieper – Técnico em Informática (Cursando), Ensino Médio (Concluído



Germano Sprotte – Técnico em Informática (Cursando), Ensino Médio (Concluído)

Vinícius Gabriel Azevedo – Técnico em Informática (Cursando).