CIÊNCIA EM EVIDÊNCIA

BITCOIN, ETHEREUM E XRP: UMA ANÁLISE HISTÓRICA DAS CRIPTOMOEDAS E SUAS TECNOLOGIAS

Angelo Pisani Neto[1] e Gustavo Matarazzo[2]

[1]Tecnólogo em Análise e Desenvolvimento de Sistemas
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP
Capivari, SP, Brasil

[2]Docente Área de Gestão
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP
Capivari, SP, Brasil

angeloneto_11@hotmail.com, gustavo.matarazzo@ifsp.edu.br

Resumo

O dinheiro é indispensável para o ser humano e apresenta constantes evoluções. Com o avanço da tecnologia, diversos meios de pagamento surgiram e dentre eles é possível destacar as criptomoedas, um assunto recente que tem sido apresentado em diversos meios, sobretudo, como uma possibilidade de investimento. Nesse contexto, o presente trabalho tem como objetivo analisar as características tecnológicas chaves das três criptomoedas que ocupam, atualmente, os maiores índices de capitalização de mercado, sendo elas: Bitcoin, Ethereum e XRP. Para atingir tal objetivo, assumiu-se nesta pesquisa um posicionamento de natureza qualitativa. Aplicou-se técnicas descritivas para retraçar os históricos e a descrição de suas tecnologias chave. Como resultados, a presente pesquisa demonstrou que as criptomoedas apresentam objetivos diferentes, no entanto, utilizam-se da mesma tecnologia de transação, a *peer-to-peer*. As tecnologias de *blockchain*, mineração e *proof-of-work* são utilizadas de maneiras distintas por cada uma das criptomoedas. Por fim, considera-se que trabalhos como esse são importantes por colocarem luz nas tecnologias implementadas. Como limitações, ressalta-se o estudo em três casos.

Palavras-chave: Tecnologia; Criptomoedas; *Blockchain*; Bitcoin; Pagamentos.

BITCOIN, ETHEREUM AND XRP: A HISTORICAL ANALYSIS OF CRYPTOMOEDES AND THEIR TECHNOLOGIES

Abstract

Money is indispensable for humans and is constantly evolving. With the advancement of technology, several payment methods have emerged and among them it is possible to highlight cryptocurrencies, a recent subject that was presented in various media, mainly as a possibility of investment. Therefore, this paper aims to analyze the three cryptocurrencies that occupy the highest market capitalization indexes, namely: Bitcoin, Ethereum and XRP. To achieve this goal, a qualitative approach was assumed in this research. Descriptive techniques were applied to retrace the histories and the description of their key technologies. As a result, the present research demonstrated that cryptocurrencies have different objectives, however, it uses the same peer-to-peer transaction technology. Blockchain, mining and proof-of-work technologies are used in different ways. Finally, it is considered that works like this are important because they shed light on the implemented technologies. Limitations include the application in three cases.

Keywords: Tecnologies; Criptocurrencies; Blockchain; Bitcoin; Payment.

1. INTRODUÇÃO

A moeda é uma velha conhecida dos seres humanos, surgiu como uma forma primitiva de troca, na qual as pessoas trocavam bens que possuíam por outros que desejavam, sem equivalência de valor. A partir disso, a moeda foi se consolidando e mudando sua forma: de metais preciosos como cobre, prata e ouro para papéis moeda e, mais recentemente, pequenos pedaços de plástico conhecidos como cartão de crédito (BANCO CENTRAL DO BRASIL, 2019). A evolução continua e, com a popularização da internet, surgiu um novo método de pagamento, as moedas digitais.

Em 2008, o pseudônimo Satoshi Nakamoto fez a publicação de um artigo intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Vendo a necessidade de colocar a moeda a nível de código computacional, Nakamoto (2008) propôs então, a moeda digital mais conhecida atualmente, o Bitcoin. Não se sabe muito a respeito do autor, há pessoas que acreditam que Satoshi Nakamoto não seja uma pessoa, mas sim um grupo.

O artigo apresentava um sistema de pagamento eletrônico ponto a ponto, baseado em provas criptografadas, as quais tornam possíveis duas partes interessadas transacionarem diretamente uma com a outra, sem a necessidade de um intermediário confiável (NAKAMOTO, 2008). Garantindo assim uma ideia central para o uso da moeda digital, que se esquiva de fraudes e apresenta custos de transação menores.

Outro termo que passou a se tornar conhecido a partir da publicação do artigo foi o "*Blockchain*". O que torna comum a confusão entre os termos Bitcoin e *Blockchain*. De maneira geral, entende-se que o Bitcoin é o ativo financeiro transacionado na Internet, enquanto o *Blockchain* é a tecnologia base para as transações (GUIA DO BITCOIN, 2019).

Diante desses elementos, uma moeda digital pode ser definida como uma cadeia de assinaturas digitais, na qual cada proprietário transfere a moeda para o próximo assinando digitalmente o *hash* da transação anterior e a chave pública do próximo proprietário (NAKAMOTO, 2008).

Algumas moedas digitais chamam a atenção pelo seu preço e capitalização de mercado. Sendo uma tecnologia de grande vicissitude, as criptomoedas têm chamado cada vez mais a atenção de investidores financeiros. A moeda digital mais conhecida do público em geral é a Bitcoin, mas além dela, há outras milhares de criptomoedas espalhadas pela Internet. A partir de uma visão a respeito da quantia financeira movimentada, estima-se que o valor das três principais moedas em capitalização de mercado (Bitcoin, Ethereum e XRP) seja de 717,2 bilhões de reais segundo as cotações do site CoinMarketCap (2019), o que representa, aproximadamente, 80% do mercado total.

Porém, as criptomoedas em geral continuam sendo uma temática pouco explorada. Percebe-se que o conhecimento tecnológico acerca deste tema não é popularizado, e que mesmo em alguns setores de tecnologia da informação, não se têm conhecimento sobre os seus funcionamentos. Ao se realizar um levantamento de artigos dos últimos dez anos e efetuar uma análise qualitativa de seus resumos, identificou-se que as pesquisas são, majoritariamente, aprofundadas e/ou aplicadas sem o intuito de democratizar os conhecimentos.

Portanto, o presente trabalho visa responder a seguinte questão de pesquisa: quais as principais características tecnológicas que possibilitam a existência de criptomoedas, mais especificadamente, Bitcoin, Ethereum e XRP? E tem como objetivo geral mapear os componentes tecnológicos chave que possibilitam a existência das três criptomoedas mencionadas.

2. REFERENCIAL TEÓRICO

2.1 Trocas, moedas, dinheiro e tecnologia: uma perspectiva histórica

De acordo com a Casa da Moeda do Brasil (2019), a ideia de pagamento surgiu nos primórdios da vida humana, com a evolução do homem primitivo, o qual começou a buscar conforto e itens para sua necessidade pessoal, dando início às trocas. Sendo assim, o sistema monetário passou por diversas mudanças, é possível ressaltar, em seu início, o papel dos objetos como formas de pagamento. Com a descoberta do metal e seus utensílios, caracterizados pela necessidade de certa habilidade para serem produzidos, facas e outros utensílios metálicos passaram a ser utilizados para trocas, até que, em VII a.C., houve o surgimento das moedas, caracterizadas por serem pequenas peças de metal com peso e valor definidos.

Metais preciosos, como ouro, prata e cobre, logo se impuseram como moedas, devido à raridade, beleza e costumes religiosos. Posteriormente, na idade média, o papel moeda emergiu, primeiramente como recibos preenchidos à mão. Com o passar do tempo, o governo começou a conduzir a emissão do papel moeda, com as chamadas cédulas, que perpetuam contemporaneamente (BANCO CENTRAL DO BRASIL, 2019).

Diante desse primeiro cenário de desenvolvimento das moedas e das próprias relações sociais que envolvem a humanidade e a economia, torna-se interessante explorar a relação entre meios de pagamento e tecnologia.

Os meios de pagamento e as formas de executar transações financeiras foram diretamente afetadas pela evolução tecnológica. A forma física abriu espaço para o processamento de dados, e a principal função dos meios de pagamento eletrônicos passou a estar relacionada com a transferência de informações de forma rápida (FUZITANI, 2007). Essa evolução das formas de pagamento está inserida no contexto da “Convergência Digital”, que influencia diretamente nas decisões de compra e, consequentemente, na economia mundial.

Após o cartão de crédito se estabelecer, em 1970, e o cartão de débito substituir em grande parte o cheque, os bancos começaram a investir e experimentar outros meios para a expansão do mercado. Um exemplo é o caso das milhas áreas, que passou a envolver a indústria de aviação, influenciando diretamente no número de viagens. O exemplo de milhas, propicia o surgimento de dispositivos como as “milhas voadas”, que abrangem outros mercados, por exemplo, os programas de hotéis e locadoras de automóveis. Tal fato cria diversos vínculos entre empresas de ramos diferentes (FARIAS, 2017).

Nesse contexto, diferentes possibilidades foram criadas e movimentaram as formas como pessoas e organizações movimentam a economia. Mais especificamente, em 2008, um

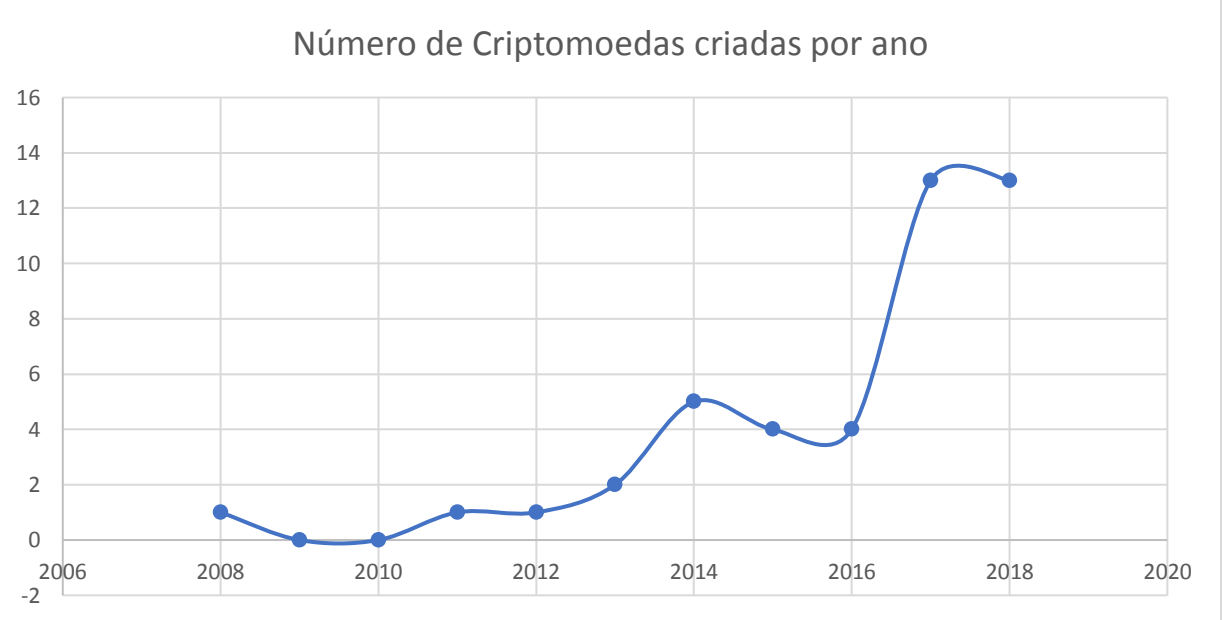
artigo abriu outras possibilidades para os meios de pagamentos. Nakamoto (2008) apresentava, de maneira geral, a ideia de uma moeda virtual, e o funcionamento da tecnologia que propiciava sua existência, posteriormente, denominada de *Blockchain*. Surgiu, então, o conceito de Bitcoin, uma moeda totalmente virtual, que não se enquadrava em uma situação legal consistente e desprovida de centralizações, como bancos, para executar transações. Tratar-se-á de tal temática a seguir.

2.2 Criptomoedas

De acordo com o site CoinMarketCap (2019), atualmente, existe mais de 2300 criptomoedas catalogadas.

Ao se fazer um sobrevoo sobre as 50 primeiras criptomoedas do ranking de capitalização de mercado do site CoinMarketCap (2019), é possível observar o movimento de criação e ascensão das moedas digitais. Desde 2008, com a primeira criptomoeda, até o final de 2018, pode-se perceber que a criação dessas moedas virtuais se popularizou. Ressalta-se a alta considerável de criação de criptomoedas apresentada a partir de 2016 (Figura 1).

Figura 1 - Número de Criptomoedas criadas de 2008 a 2018



Fonte: Elaborado pelo autor com base em dados do CoinMarketCap (2019).

Visto que existem milhares de criptomoedas catalogadas no site CoinMarketCap (2019) e o gráfico ilustrado na figura 1 foi criado com base nas 50 maiores em capitalização de mercado, é possível afirmar que as moedas mais recentes têm figurado dentre as mais valiosas.

Nesse sentido, entende-se que o *Blockchain* é a tecnologia central para a criação e desenvolvimento de todas essas criptomoedas.

2.3 *Blockchain*

Com a publicação do artigo de Satoshi Nakamoto (2008), no qual foram difundidas as principais perspectivas tecnológicas da criptomoeda Bitcoin, explica-se também as primeiras noções de *Blockchain*. Segundo Mattila (2016), essa tecnologia tem potencial para impactar todos os setores e camadas da sociedade, pois é transparente e redefine a segurança nas relações de troca de informações e valores. Com isso, tornou-se base para a moeda digital e, posteriormente, para diversos outros fins.

Inicialmente, a tecnologia *blockchain* foi disseminada como solução para o problema de gastos duplos da criptomoeda Bitcoin. Funciona a partir de uma chave privada criptografada (secreta como uma senha) e uma chave pública compartilhada com todas as outras partes da rede, cada bloco criado por uma transação possui uma espécie de impressão digital chamada *hash*, que se trata de um algoritmo matemático criptografado e extremamente difícil de ser revertido (NAKAMOTO, 2008).

Em um contexto abrangente, o *blockchain* pode ser considerado uma cadeia de blocos que utiliza diversas tecnologias para criptografia, estrutura de dados e outras técnicas matemáticas. Com isso, há a possibilidade de criação de ativos digitais nas fases de mineração, pré-mineração ou contratos inteligentes, o que resulta em transações por duas partes, sem a intervenção de um terceiro, garantindo autenticidade, devido às assinaturas digitais criptografadas e a corrente de transações, a qual permite o acesso à trajetória do dado transacionado do seu último destino à sua origem. (LEWIS, 2018).

Trata-se, portanto, de uma base de dados distribuída, gerida de forma descentralizada e compartilhada por uma rede *peer-to-peer*, a qual os participantes a armazenam e a mantém. Nesse sentido, funciona como um livro-razão público e compartilhado, que cresce à medida que novas transações são feitas e consequentemente novos blocos são criados (FORMIGONI FILHO; BRAGA; LEAL, 2017).

Por ser confiável, esta cadeia de blocos está se expandindo, podendo ser utilizada para comunicações em cadeia de fornecimento, contratos inteligentes, gerenciamento de identidades e outras aplicações. (CHICARINO et al., 2019).

Segundo Lewis (2018), a melhor definição para o *blockchain* é de que se trata de uma palavra que representa um conjunto de tecnologias que possibilitam os ativos digitais serem criados e transmitidos ponto a ponto com garantia de autenticidade e de que não foram falsificados ou alterados, sem a necessidade de confiar em um terceiro. Dado esse primeiro panorama teórico acerca das moedas, tecnologias e do *blockchain*. A seguir, serão apresentados os aspectos metodológicos da presente pesquisa.

3. PROCEDIMENTOS METODOLÓGICOS

Nesta seção, serão demonstrados os procedimentos adotados para a realização deste trabalho, que se trata de uma pesquisa de natureza qualitativa e de caráter descritivo.

A pesquisa qualitativa, segundo Creswell (2013), reflete a forma em que o pesquisador se empenhou para fazer o estudo, depende da análise de dados e imagens, não se preocupando tanto com números. Também envolve a discussão do objeto estudado, comentários do pesquisador e os procedimentos gerais realizados para a coleta e análise dos dados. Portanto, a estrutura de um projeto qualitativo pode variar consideravelmente entre pesquisadores.

Ao efetuar uma pesquisa de caráter descritivo, faz-se necessário diversas informações, observações e registros sobre o assunto a ser tratado, sem que haja alteração de dados, a fim de descobrir as características do objeto de estudo, com a maior precisão possível (CERVO; BERVIAN; DA SILVA, 2006). Entre os exemplos de pesquisa descritiva, encontra-se o estudo de caso.

Portanto, para este estudo foram realizadas buscas em periódicos e sites específicos a fim de obter informações sobre o histórico das três criptomoedas que foram estudadas (Bitcoin, Ethereum e XRP), e de suas principais tecnologias. Foram encontrados, no portal de periódicos CAPES, um total de 164 artigos revisados por pares envolvendo as palavras-chave: "*Cryptocurrency*", "*Blockchain*" e "*Technology*". Após um filtro a partir de uma análise qualitativa de seus resumos e introduções, 19 artigos foram escolhidos. Além destes, diversos outros artigos, sites e livros foram estudados a fim de finalizar esta pesquisa, levantando os resultados que serão demonstrados a seguir.

4. RESULTADOS

4.1 Bitcoin

A criptomoeda mais conhecida atualmente, o Bitcoin (BTC), surgiu após a publicação do artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", pelo pseudônimo de Satoshi Nakamoto, em 2008. O documento propõe uma moeda para pagamentos digitais ponto a ponto, permitindo que transferências digitais sejam realizadas sem o auxílio de uma instituição

financeira para intermediá-las. Portanto, basta um sistema de pagamento eletrônico com base em provas criptografadas ao invés de confiança, o que permite duas partes interessadas transacionem entre si sem a necessidade de uma terceira parte confiável (NAKAMOTO, 2008).

Como é citado no título do artigo de Nakamoto, o modelo de transferência de dados é o *peer-to-peer* (P2P), traduzido literalmente como ponto a ponto. Segundo Vicente (2017), é uma das principais tecnologias utilizadas para que as moedas digitais possam ser transacionadas, pois possibilita a troca direta de dados em grande escala e trabalha no formato de rede de computadores, no qual cada usuário conectado realiza funções de servidor e cliente e seu objetivo é a transmissão de arquivos.

Os Bitcoins são gerados por um processo chamado de mineração, esse processo é caracterizado por adicionar registros ao livro razão público do Bitcoin, o *blockchain*, uma cadeia de blocos que confirma as transações para toda da rede, evitando assim os gastos duplos ou reuso da criptomoeda, como citado por Nakamoto (2008).

A mineração do Bitcoin é feita por meio da resolução de problemas matemáticos complexos segundo tentativa e erro. Tais problemas são criados por uma tecnologia denominada *Proof-of-Work* (PoW) ou prova de trabalho. (GERVAIS et al., 2016).

Introduzido por Nakamoto (2008) em seu artigo, o Bitcoin emprega um PoW baseado em *hash*, com a criptografia SHA-256. Quanto maior o poder computacional, mais rápido será a resolução dos problemas e consequentemente a construção dos blocos no *blockchain*, portanto, devido a essa demanda de computadores superpotentes, entusiastas criaram circuitos integrados específicos de aplicativo (ASICs), ou seja, máquinas próprias para a solução de problemas complexos.

A mineração é intencionalmente projetada para ser difícil e complexa, limitando assim o número de blocos encontrados, e tem como principal objetivo, a definição dos históricos de transação. Após a descoberta de um bloco, o seu minerador recebe um certo número de bitcoins como recompensa, tal número varia de acordo com a quantidade de blocos minerados na rede, e taxas pagas pelos usuários que fazem transações (BITCOIN WIKI, 2019).

4.2 Ripple

A empresa OpenCoin, fundada em 2012, foi responsável pelo desenvolvimento do protocolo de transação Ripple (RTXP) e sua rede de pagamento e trocas. Renomeada um ano

depois, em 2013, para Ripple Labs Inc., trata-se de uma empresa de capital privado com diversos investidores, como Seagate Technology e Google Ventures (FRIED, 2018).

O protocolo de pagamento Ripple, como é chamado, possui sua própria criptomoeda, o XRP e ocupa a terceira posição no ranking de capitalização das criptomoedas, segundo cotações do site CoinMarketCap (2019). Refere-se a um protocolo de pagamento de código aberto, disponível para o público e que suporta, em sua rede, diferentes tipos de moedas.

Apesar de ter como base um código aberto, a implantação atual do Ripple é gerenciada exclusivamente pelo Ripple Labs, que busca permitir pagamentos seguros e instantâneos. Os nós de uma rede Ripple podem ser divididos em três tipos: aqueles que fazem e/ou recebem pagamentos; facilitadores comerciais e validadores que executam o protocolo a fim de validar transações (ARMKNECHT *et al*., 2015).

Segundo Fried (2018) o XRP foi criado para resolver uma grande resistência existente em transações internacionais, devido a ganância de bancos, que lucram milhões de dólares com taxas de transação. Esta moeda pode aumentar pagamentos mais rapidamente, executar liquidações instantâneas e manter as taxas de transação muito mais baixas.

Ao contrário das criptomoedas citadas anteriormente, a XRP não pode ser minerada. O Ripple utiliza um algoritmo de consenso (RPCA) a partir de uma verificação por seus nós, para manter a concordância na rede e evitar bifurcações. Segundo Armknecht *et. al*. (2015) tal protocolo passa por três fases:

- Fase de coleta: os servidores de validação coletam as transações que são recebidas da rede, em seguida verificam sua autenticidade, por meio do *ledger* da transação, da chave pública do emissor e da validade da assinatura;
- Fase de consenso: processo iterativo, no qual os servidores na rede processam e enviam propostas, os validadores, por meio do processo de consenso, devem concordar com a transação, até que a grande maioria deles (80%) chegue a um acordo sobre o conjunto de transações que está sendo validada;
- Fase de fechamento: cada servidor de validação encaminha um *hash* assinado, assim que uma *ledger* de transação obtém uma maioria de 80% dessas assinaturas, ela é considerada validada e então, fechada. A partir do momento em que uma *ledger* é fechada, outra que foi coletada entra para a fase de consenso, iniciando uma nova rodada.

Isso demonstra uma grande diferença com as outras duas criptomoedas anteriormente descritas. O Bitcoin e o Ethereum utilizam *Proof-of-Work* por meio de mineração, para verificar as transações e garantir a descentralização da criptomoeda. Em contrapartida, o XRP utiliza o método de consenso, descrito acima, para que suas transações sejam validadas, portanto, o XRP não pode ser minerado (SILKJÆR, 2019).

Ao ser criado, segundo o site oficial XRPL ORG (2019), foram gerados 100 bilhões de XRP e não é possível criar mais essa criptomoeda. Desta quantia, 20% foram distribuídos para os fundadores do projeto e os outros 80 bilhões ficaram com a empresa Ripple Labs. Sendo assim, o XRP não pode ser considerado como totalmente descentralizado, tal qual Bitcoin e Ethereum. Além disso, ao serem feitas transações via XRP, uma pequena fração é destruida, devido aos custos de transação. O que faz com que a criptomoeda seja, naturalmente, deflacionária. Entretanto, essa destruição não oferece riscos à existência da criptomoeda.

4.3 Ethereum

Apesar da moeda Ether ser uma das maiores em questão de capital de mercado, segundo o site CoinMarketCap (2019), com aproximadamente US$ 18,2 bilhões, é importante entender que o Ethereum é mais do que uma moeda digital. Trata-se de um *blockchain* programável, que permite aos desenvolvedores criarem e implantarem aplicativos descentralizados, denominados DApps (ETHEREUM ORG, 2019).

A intenção do Ethereum, segundo Buterin (2014) é fundir o potencial de *scripting, altcoins e meta-protocols* que existem no *blockchain*, permitindo que os desenvolvedores consigam criar aplicativos que unam paradigmas, como escalabilidade, funcionalidade e facilidade, ao mesmo tempo. O Ethereum faz isso construindo um *blockchain* com uma linguagem de programação completa e integrada, o que proporciona que qualquer pessoa escreva contratos inteligentes e DApps.

Entretanto, para que um usuário escreva contratos inteligentes ou desenvolva aplicativos, é necessário participar da rede Ethereum. Lewis (2016) diz que, para se conectar a essa rede, explorar seu *blockchain*, fazer transações ou minerar novos blocos faz-se necessário a execução de um cliente Ethereum. O que torna o computador do cliente um nó, fazendo-o participar da rede.

Assim como outros *blockchains*, o Ethereum possui sua criptomoeda nativa, o Ether (ETH). De acordo com o site oficial Ethereum.org (2019) o ETH se assemelha ao Bitcoin por ser uma criptomoeda *peer-to-peer*, podendo ser transacionada para qualquer lugar do mundo

sem a necessidade de terceiros envolvidos no processo, também é descentralizada e não possui nenhum órgão que a controle.

Outra semelhança se dá na sua mineração. O ETH possui um sistema de PoW parecido com o do bitcoin, no qual mineradores competem entre si para descobrir novos blocos, e a partir disso, serem recompensados. Quanto maior o preço da moeda digital, mais mineradores são atraídos, dificultando cada vez mais a mineração (SASSANO 2019).

Ressalta-se que o Ethereum utiliza um sistema de PoW com o algoritmo de mineração ETHash, que tem como principal diferencial, o consumo total da banda de acesso à memória disponível na placa de vídeo, ou seja, processamento gráfico. Portanto, essa moeda é minerada por *Graphics Processing Units* (GPUs) contemporâneas, que utilizam as tecnologias mais recentes de entrada e saída, o que impossibilita sua mineração a partir de circuitos integrados próprios (ASICs), pois esses não possuem processamento gráfico (SUKHAREV; SILNOV, 2018).

4.4 Síntese dos Resultados

Após a descrição das criptomoedas que ocupam as três melhores posições no ranking de capitalização de mercado, construiu-se um quadro comparativo (Quadro 1), que lista as informações das moedas digitais e suas tecnologias.

Quadro 1: Comparativo entre as criptomoedas estudadas.

TECNOLOGIAS	BITCOIN	XRP	ETHEREUM
Ano de criação	2008	2012	2015
Preço unitário	$7,493.49 USD *	$0.278491 USD *	$162.17 USD *
Função	Moeda digital criada para realização de transferências sem o auxílio de intermediários.	Rede de pagamentos para empresas e bancos, com transações instantâneas.	Plataforma para contratos inteligentes e aplicativos descentralizados.
Tecnologia de transação	*Peer-to-Peer (p2p)*	*Peer-to-Peer (p2p)*	*Peer-to-Peer (p2p)*
Blockchain	Utilizado para validar transações na rede.	Permite validação de transações por meio de "votação" dos nós da rede, que garante a autenticidade da transação.	Plataforma programável, possibilitando a criação de aplicativos descentralizados e contratos inteligentes.
Mineração	Soluções de problemas matemáticos por tentativa e erro. Minerado principalmente por máquinas próprias denominadas ASICs.	Não é minerada.	Soluções de problemas matemáticos por tentativa e erro. Minerado através de processamento gráfico (GPU).
Proof-of-work	Criptografia SHA-256.	Método de consenso (RPCA).	Criptografia ETHash.

Fonte: Elaborado pelo autor.

* Data da cotação – 23 de outubro de 2019

5. CONSIDERAÇÕES FINAIS

O presente trabalho propôs, como objetivo geral, mapear os componentes tecnológicos chaves que possibilitam a existência das três criptomoedas, segundo a capitalização de mercado, Bitcoin, Ethereum e XRP. Para isso, empregou-se a revisão bibliográfica como técnica central a fim de retraçar os históricos de tais moedas digitais e então descrever suas principais tecnologias.

É possível notar conceitos tecnológicos em comum entre as moedas digitais, principalmente com relação à tecnologia de transação, isto é, o *peer-to-peer* é aplicado nas três criptomoedas estudadas. Entretanto, nota-se que o objetivo de cada moeda se difere e, com isso,

tecnologias são moldadas para atingi-los. A partir disso, tecnologias chaves como o *blockchain* e o conceito de mineração são diferentes em todas as moedas digitais vistas neste trabalho.

É importante ressaltar que tal temática abordada é relativamente nova e está em ascensão, não só nas áreas de tecnologia. Portanto, este trabalho visa a inserção do público no tema de moedas digitais, trazendo os principais conceitos para entender a funcionalidade de uma criptomoeda. É possível estender tal estudo para um maior aprofundamento de cada tecnologia envolvida, principalmente o *blockchain*, que pode ser programável e está se expandindo para além da criptomoeda, tornando-se disruptivo para diversas áreas.

Referências

ARMKNECHT, F. *et al*. Ripple: Overview and outlook. **Trust and Trustworthy Computing**, Trust and Trustworthy Computing - 8th International Conference, p. 163-180, 2015. DOI 10.1007/978-3-319-22846-4_10. Disponível em: <https://pure.unic.ac.cy/en/publications/ripple-overview-and-outlook> Acesso em: 24 set. 2019.

BANCO CENTRAL DO BRASIL. **Origem e evolução do dinheiro.** 2019 Disponível em: <https://www.bcb.gov.br/acessoinformacao/legado?url=https:%2F%2Fwww.bcb.gov.br%2Fhtms%2Forigevol.asp> Acesso em: 14 out. 2019.

BITCOIN WIKI. **Mining.** Disponível em <https://en.bitcoin.it/wiki/Mining> Acesso em 19 de Julho de 2019.

BUTERIN, V. A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. **Ethereum White Paper**, p. 1-36, 14 jan. 2014. Disponível em: <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> Acesso em: 2 ago. 2019.

CASA DA MOEDA DO BRASIL. **Origem do Dinheiro**. Brasil, 2019. Disponível em: <https://www.casadamoeda.gov.br/portal/socioambiental/cultural/origem-do-dinheiro.html> Acesso em: 8 out. 2019.

CERVO, A. L; BERVIAN, P. A; DA SILVA, R. **Metodologia cientifica**. 6º. ed. Pearson Prentice Hal, 2006. 159 p. ISBN 8576050471.

CHHANGA D. **What is Blockchain Technology?**, 2018 Disponível em <https://idevji.com/what-is-blockchain-technology/> Acesso em: 5 de junho de 2019.

COIN MARKET CAP. **Top 100 Cryptocurrencies by Market Capitalization**. 2019. Disponível em <https://coinmarketcap.com/&gt> Acesso em: 23 de outubro de 2019.

CRESWELL, J. W. **Research Design: Qualitative, Quantitative, and Mixed Methods Approaches**. 4º. ed. California: SAGE Publications, 2013. 273 p. ISBN 1452226105.

DE FARIAS, L. M. **INOVAÇÃO TECNOLÓGICA E EXPANSÃO DO ACESSO AOS SERVIÇOS BANCÁRIOS: A EVOLUÇÃO DO MERCADO BRASILEIRO DE MEIOS DE PAGAMENTOS ELETRÔNICOS E O DISPOSITIVO MOBILE**. Orientador: Marcelo

Milan. 2017. 88 f. Dissertação (Mestrado em Economia) - Faculdade de Ciências Econômicas da UFRGS, Porto Alegre, 2017.

ETHEREUM ORG. **Learn**. 2019. Disponível em: <https://ethereum.org/beginners/> Acesso em: 2 agosto de 2019.

FRIED, J. **What is Ripple? How Does it use XRP to Leverage Instant Liquidity? | Ripple Explained Simply**. 13 ago. 2018. Disponível em: <https://achainofblocks.com/2018/08/13/what-is-ripple-use-xrp-instant-liquidity-crypto-2019/> Acesso em: 24 set. 2019.

FORMIGONI FILHO, J. R.; BRAGA, A. M.; LEAL, R. L. V.. Tecnologia Blockchain: Uma visão geral**. Harvard business review,** v. 6, n. 2, p. 6, 2017.

FUZITANI, E. A. **MEIO ELETRÔNICO DE PAGAMENTO E DESEMPENHO NO VAREJO: Estudo comparativo de setores na adoção de um cartão de loja como meio de pagamento**. Orientador: Antonio Carlos Aidar Sauaia. 2007. Trabalho de Conclusão de Curso (Faculdade de Economia, Administração e Contabilidade da USP) - USP, 2007.

GERVAIS, A. et al. **On the Security and Performance of Proof of Work Blockchains**. p. 3–16, 2016.

GUIA DO BITCOIN. **Bitcoin e Blockchain para leigos.** Disponível em: <https://guiadobitcoin.com.br/bitcoin-e-blockchain-para-leigos/> Acesso em: 12 de maio de 2019.

LEWIS, A. **What is Blockchain?** 2018. Disponível em: <https://bitsonblocks.net/2018/10/24/what-is-blockchain/> Acesso em: 18 de junho de 2019.

LEWIS, A. **A gentle introduction to Ethereum** 2016. Disponível em: <https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/> Acesso em: 2 de agosto de 2019.

L CHICARINO, V. R. et al. Uso de Blockchain para Privacidade e Segurança em Internet das Coisas. **Minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg2017**, n. November, p. 51, 2017.

MATTILA, J. The blockchain phenomenon - The Disruptive Potential of Distributed Consensus Architectures. **BRIE Working Paper 2016-1**, v. 2420, n. May 2016, p. 1–25, 2016.

SASSANO, A. **Why Ether is Valuable**. 7 jan. 2019. Disponível em: <https://medium.com/ethhub/why-ether-is-valuable-2b4e39e01eb3>. Acesso em: 5 ago. 2019.

NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Www.Bitcoin.Org**, p. 1–9, 2008.

SILKJÆR, T. **14 Common Misunderstandings About Ripple And XRP**. 7 mar. 2019. Disponível em: https://www.forbes.com/sites/thomassilkjaer/2019/03/07/14-common-misunderstandings-about-ripple-and-xrp/#cd1ba1f71d0b. Acesso em: 30 set. 2019.

SUKHAREV, Pavel V.; SILNOV, Dmitry S. Asynchronous Mining of Ethereum Cryptocurrency. **2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)**, St. Petersburg, Russia, p. 1-5, 8 nov. 2018. Disponível em: https://ieeexplore.ieee.org/document/8524929. Acesso em: 13 ago. 2019.

VICENTE, R. J. A Criptomoeda Como Método Alternativo Para Realizar Transações Financeiras. **Revista Maiêutica, Indaial**, v. 2, n. 1, p. 85–94, 2017. Disponível em: <https://publicacao.uniasselvi.com.br/index.php/TI_EaD/article/view/1692>.

XRLP ORG. **XRP**. 2019. Disponível em: <https://xrpl.org/xrp.html> Acesso em: 30 set. 2019.