

A IMPORTÂNCIA DA *BLOCKCHAIN* PARA A SEGURANÇA E APLICAÇÃO EM CRIPTOATIVOS – UMA REVISÃO BIBLIOGRÁFICA

Rodolfo Rosa¹
Guilherme Lavinias Rabello¹
Stenio Coutinho Balduino²
Vinicius Silva Araújo²
Brenno Do Vale Rosa³
Bernardo Goytacazes de Araujo⁴
Renata Aparecida Fontes⁵

rosa.rod156@gmail.com

ÁREA DE CONHECIMENTO: Ciências sociais e aplicadas

PALAVRAS-CHAVE: bitcoin, *ethereum*, *blockchain*, segurança, aplicação.

INTRODUÇÃO

Introduzida em 2008, juntamente à bitcoin, a tecnologia *blockchain* permite o armazenamento descentralizado de informações. Estas são transações entre duas partes, denominada transação *peer-to-peer* (P2P), que deve ser validada na rede *blockchain* por outros *peers*, os conhecidos mineradores ou *miningpools*, um grupo de mineradores (RODRIGUES, 2017). As informações de transação permanecem públicas na rede *blockchain*, atualizadas pelos participantes da mesma que possuem cópias de todas as transações ocorridas na rede, mantendo um registro em livro razão descentralizado (VIANNA, SILVA, PEINADO, 2020). O processo de mineração, no caso do bitcoin e outras criptomoedas, consiste no uso de operações matemáticas complexas que devem ser solucionadas. O minerador que soluciona primeiro uma operação recebe uma quantia ou fração de criptomoedas (BOVÉRIO, SILVA, 2018). O mais popular criptoativo, a bitcoin, certamente disseminou a troca de valores monetários como a maior aplicação da *blockchain*, mas ela vai além disso, podendo ser aplicada para realização de *smart contracts*, armazenamento de dados descentralizados com segurança, registros de patentes, direitos de propriedade ou

¹ Acadêmico do 2º período do curso de Ciências Contábeis da Faculdade Vértix Trirriense – Univértix.

² Acadêmico do 4º período do curso de Administração da Faculdade Vértix Trirriense – Univértix.

³ Acadêmico do 1º período do curso de Administração da Faculdade Vértix Trirriense – Univértix.

⁴ Graduado em Filosofia pela UFJF. Especialista em Filosofia Moderna e Contemporânea, pela UFJF. MBA em Gerenciamento de Projetos pela UGF RJ, Mestrando em Educação pela UNEATLANTICO. Sec. Municipal de Planejamento e Projetos da PMTR. Docente na Faculdade Vértix Trirriense (Três Rios)

⁵ Farmacêutica Bioquímica Mestre em Ciências Farmacêuticas - Professora da Faculdade Vértix Trirriense.

royalties, transporte de documentos digitais com ou em áreas como logística, saúde, educação e finanças. As maiores vantagens e características destas tecnologias, destacadas em diversos trabalhos, são confiança e segurança (VIANNA, SILVA, PEINADO, 2020)(COUTINHO, BEZERRA, MAIA, 2021). Assim, o presente trabalho teve como objetivo realizar uma breve revisão bibliográfica sobre a importância da *blockchain* para a segurança e aplicação em criptoativos. Trabalhos como este são importantes, pois permitem compreender melhor o mecanismo de mineração que confere a esta tecnologia a capacidade de prover confiança e segurança em aplicações diversas.

METODOLOGIA

Trata-se de um estudo de revisão bibliográfica realizada em agosto e setembro de 2022, onde foram utilizados artigos pesquisados na plataforma de busca Google Acadêmico. Os descritores utilizados foram: bitcoin, *ethereum*, *blockchain*, segurança, aplicação. Como critérios de inclusão foram considerados artigos, teses e dissertações dos últimos seis anos. Foram excluídos trabalhos em outros formatos textuais e que não apresentavam como assunto principal a temática buscada.

RESULTADOS E DISCUSSÕES

O pseudônimo Satoshi Nakamoto foi o responsável por idealizar a bitcoin, com o objetivo de remover a necessidade de um intermediário para assegurar a inexistência de gasto duplo (BOVÉRIO, SILVA, 2018). A tecnologia utilizada para isto é a *blockchain*, que em sua concepção junto ao bitcoin, armazena a informação de transação monetária entre duas partes, *peer-to-peer* (P2P), em uma cadeia de blocos na qual um bloco novo deve estar atrelado exclusivamente a um bloco anterior (RODRIGUES, 2017)(PACHECO, ARAUJO, TAVARES, 2018). Para ser inserido na rede, um bloco de informações possui dados identificadores, são estes: o tamanho do bloco, contador de transações, as transações e um cabeçalho, no qual há o número de versão do protocolo, *hash* do bloco pai, *hash* da raiz da árvores de Merkle do bloco formado, instante de criação do bloco, grau de dificuldade da mineração e o número de validação da solução de mineração, chamado Nance (RODRIGUES, 2017)(GOULART, MARTINS, 2021). Cada novo bloco de informações é validado na rede, pelo processo de mineração. Neste processo, um *peer* ou grupo de *peers*, mineradores, deve resolver um problema matemático complexo, gerando uma competição entre mineradores, na qual o primeiro a encontrar a solução insere o novo bloco na rede, sendo recompensado com uma quantia da criptomoeda (BOVÉRIO, SILVA, 2018)(GOULART, MARTINS, 2021). Todos os participantes de uma *blockchain* são nós e cada vez que um novo bloco é adicionado a rede, esta informação é validada por todos os outros e é armazenada. Há 5 princípios fundamentais para o *blockchain*: *Peer-to-Peer* (P2P), pagamentos online entre duas partes sem intermediários; Ausência de autoridade central, sem um intermediador o gasto duplo é evitado; *Proof-*

of-work, um registro que impede adulterações, pois o esforço computacional para realizá-lo é impraticável; Consenso entre a maioria, o aceite da maioria dos membros da rede de um novo bloco; Sincronização, caso um nó saia da rede temporariamente, deve aceitar um novo bloco de maior tamanho em sua volta. O *blockchain* possui 3 nomeadas gerações, que se dividem por suas formas de aplicação ao longo do tempo: Geração 1, das criptomoedas; Geração 2, dos contratos inteligentes e instituições descentralizadas; Geração 3, da aplicação fora do âmbito financeiro, entrando na esfera governamental, também. A tecnologia após sua terceira geração, permite uso em áreas como Direitos autorais, identidades virtuais e telecomunicações (MARTINELLI, PINTO, 2019). Outra variação de aplicação, os contratos inteligentes já estão recebendo investimentos por gigantes tecnológicas do vale do silício e do mundo, como Google, IBM, Oracle e Porshe. A tecnologia permite a transmissão de documentos digitais dentro de uma empresa e todas suas unidades, de maneira segura e ágil, evitando problemas como vazamentos, além de potencialmente promover reduções de custo na sincronização de documentos entre empresas com filiais diversas (LIMA, HITOMI, OLIVEIRA, 2018). Segundo estudo realizado por VIANNA, SILVA E PEINADO, em 2020, de 15 artigos analisados sobre possíveis aplicações da tecnologia *blockchain*, em 70% das categorias a característica segurança destaca-se, em 54% a confiança.

CONSIDERAÇÕES FINAIS

Entende-se, portanto, que o mecanismo de mineração, a validação em múltiplos nós, o registro em livro razão público e o encadeamento de blocos são fatores determinantes para o uso da tecnologia *blockchain* em aplicações diversas, sejam elas criptomoedas, contratos inteligentes, documentos digitais, registros de direitos e propriedades, pois são capazes de prover a transação de informação com segurança, inviolabilidade dos dados e fácil verificação em registro público. Vale ressaltar que, como tecnologia surgida em 2008, são necessário estudos posteriores sobre a mesma e seu desenvolvimento.

REFERÊNCIAS

BOVÉRIO, M. A.; SILVA, V. A. F. DA. BLOCKCHAIN: uma tecnologia além da criptomoeda virtual. **Revista Interface Tecnológica**, São Paulo, [s. l.], v. 15, n. 1, p. 109–121, 2018.

COUTINHO, E. F.; BEZERRA, W. L. B.; MAIA, D. Uma Análise Inicial sobre a Aplicação de Blockchain na Sociedade. **Anais II Workshop sobre as implicações da computação na sociedade(WICS)**, p. 45-56, Rio Grande Do Sul, 2021. Disponível em: <https://sol.sbc.org.br/index.php/wics/article/view/15963> Acesso em:28/08/2022

GOULART, B. B.; MARTINS, P. J. **Aplicação da tecnologia blockchain no**

armazenamento de documentos. UNESCO, Santa Catarina, 2021. Disponível em: <http://repositorio.unesc.net/handle/1/9140> Acesso em:06/09/2022

LIMA, B. H. N.; HITOMI, F. A. C.; OLIVEIRA, G. S. de. Aplicação da tecnologia blockchain em ambientes corporativos. **Fasci-tech**, São Paulo, v. 1, n. 13, p. 6-13, 2018.

MARTINELLI, T.; PINTO, G. S. BLOCKCHAIN: comparação evolutiva utilizando Bitcoin e Ethereum. **Revista Interface Tecnológica**, São Paulo, [s. l.], v. 16, n. 1, p. 146–157, 2019.

PACHECO, L. M.; ARAÚJO, B.; TAVARES, F. O. A Bitcoin e o seu desenvolvimento: Estudo aplicado a uma amostra representativa. **REVISTA ESPACIOS**, Caracas, Acesso em:09/09/2022, ISSN 0798 1015 Vol. 39 (Nº 34), Ano 2018, Disponível em: <https://www.revistaespacios.com/a18v39n34/in183934.html>

RODRIGUES, C. K. D. S. Uma análise simples de eficiência e segurança da Tecnologia Blockchain. **Revista de Sistemas e Computação - RSC**, Bahia, v. 7, n. 2, p. 147-162, 2017.

VIANNA, F. R. P. M.; SILVA, P. C. G. D.; PEINADO, J. O Blockchain e suas aplicações para além das criptomoedas: Uma revisão sistemática de literatura. **Revista de tecnologia aplicada (RTA)**, São Paulo, v.9, n. 1, p. 67-81, 2020.