INTERFACE TECNOLÓGICA

CRIPTOMOEDA NANO E SUA ARQUITETURA BASEADA EM GRAFOS ACÍCLICOS DIRIGIDOS – DAG

NANO CRYPTOCURRENCY AND ITS ARCHITECTURE BASED ON DIRECTED ACYCLIC GRAPHS - DAG

Julio Elias Nogueira - julionogueira97@hotmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Eder Carlos Salazar Sotto – eder.sotto@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v19i2.1495
Data de submissão: 01/09/2022
Data do aceite: 28/11/2022
Data da publicação: 20/12/2022

RESUMO

A tecnologia da informação tem trazido importantes mudanças e o mundo passou a ser movido pela era digital. Assim como vários setores e produtos, o mundo viu surgir a moeda digital como forma de melhorar as transações de compras e vendas da internet. As criptomoedas surgem como uma realidade importante, no entanto, na sua criação apresentaram alguns erros, os quais foram sanados através do aperfeiçoamento, surgindo assim a criptomoeda Nano. O objetivo deste estudo é mostrar os principais conceitos técnicos da arquitetura de Directed Acyclic Grafh de tradução Grafos Acíclicos Dirigidos (DAG) em criptomoeda, evidenciando as características que tornam a Nano como uma moeda de transações instantâneas em virtude de sua arquitetura. O artigo é de Revisão Bibliográfica, com consultas de artigos e documento que trazem como foco o assunto discutido. A literatura aponta a Criptomoeda Nano uma moeda digital de grande potencialidade e que apresenta poucos índices de erros, fator de grande importância para o mercado virtual.

Palavras-chave: Nano. Criptomoeda. Grafos Acíclicos Dirigidos.

ABSTRACT

Information technology has brought about important changes and the world has been moved by the digital age. Like many sectors and products, the world has seen the emergence of digital currency as a way to improve internet shopping and sales transactions. Cryptocurrencies appear as an important reality, however, in their creation they presented some errors, which were remedied through improvement, thus the Nano cryptocurrency appeared. The aim of this study is to show the main technical concepts of the Directed Acyclic Graphics (DAG) architecture in cryptocurrency, highlighting the characteristics that make Nano a currency of instant transactions due to its architecture. The article is for Bibliographic Review, with consultations of articles and documents that focus on the subject discussed. The literature points to Nano Cryptocurrency as a digital currency of great potential and with few error rates, a factor of great importance for the virtual market.

Keywords: Nano. Cryptocurrency. Directed Acyclic Graphics.

1 INTRODUÇÃO

A evolução tecnológica tem atingido todos os setores da sociedade. A informatização tem sido um aspecto de extrema necessidade para as organizações, fator importante para tornar o trabalho mais ágil e mais seguro.

Em 2008 surge a moeda digital Bitcoin, essa criptomoeda tinha como objetivo melhorar as transações ocorridas no mundo virtual. No entanto, essa moeda sofreu transformações para que seus possíveis problemas fossem solucionados.

Dentre esses problemas estava o alto consumo de energia e a escalabilidade limitada, fatores que aumentaram o custo dessas moedas e diante de um mercado, muitas vezes em crise, essas situações são insatisfatórias.

Em 2014 como forma de solucionar os problemas das criptomoedas, surge a Criptomoeda Nano com maior potencialidade, a qual tem sua arquitetura estruturada através de DAGs e dos *block lattice.*

O fato de utilizar blocos individuais para as transações traz para a criptomoeda Nano maior escalabilidade, rapidez nas transações, menor uso de energia e a coloca dentro de contexto de maior satisfação para quem deseja e precisa utilizar a moeda digital para as suas transações.

A Arquitetura da criptomoeda Nano baseada em DAG é o que realmente a torna uma moeda mais potente e de transação mais rápida?

O objetivo deste estudo é mostrar os principais conceitos técnicos da arquitetura de Grafos Acíclicos Dirigidos (DAG) em criptomoeda, evidenciando as características que tornam a Nano como uma moeda de transações instantâneas em virtude de sua arquitetura.

A arquitetura da Engenharia de Software precisa ter amplo conhecimento sobre o funcionamento das criptomoedas, as quais tendem ser inseridas cada vez mais em um mercado com grande potencialidade e vivência virtual.

Em um futuro não tão distante as moedas virtuais farão parte da maioria das transações de compra e venda da internet, dentro desse contexto precisam ser amplamente estudadas e reformuladas para que se alcance excelência.

2 ARQUITETURA DA CRIPTOMOEDA NANO

2.1 *Blockchain*

A tecnologia *blockchain* geralmente é utilizada para que seja feita a autenticação de identidades definidas das funções computacionais de conclusiva e inflexível, que acontece por meio de sua chave ou cadeia de blocos. Foi criada em 2008 como forma de fundamentar a criação e troca da criptomoeda Bitcoin, sem que para isso existisse uma autoridade central de controle, e suas implementações foram lançadas em 2009 (MAGAZZENI, 2017).

Mougayar (2017) descreve que a tecnologia *blockchain* oferece um novo modelo como forma de trazer confiança em transações entre pares, podendo ter sua eficiência, validade e funcionalidade provada de forma atemporal, por meio de operações, contratos e propriedades inteligentes.

Como resumo o *blockchain* nada mais é do que um registro de informações distribuído e formado por uma cadeia de blocos dados, os quais são conectados uns aos outros por um sistema que utiliza funções hash criptográficas (CHERVINSKI; KREUT, 2019).

Chervinski e Kreut (2019) descrevem que as criptomoedas só puderam existir e trazer descentralização e maior privacidade devido à tecnologia dos *blockchains.*

2.2 Criptomoeda Nano

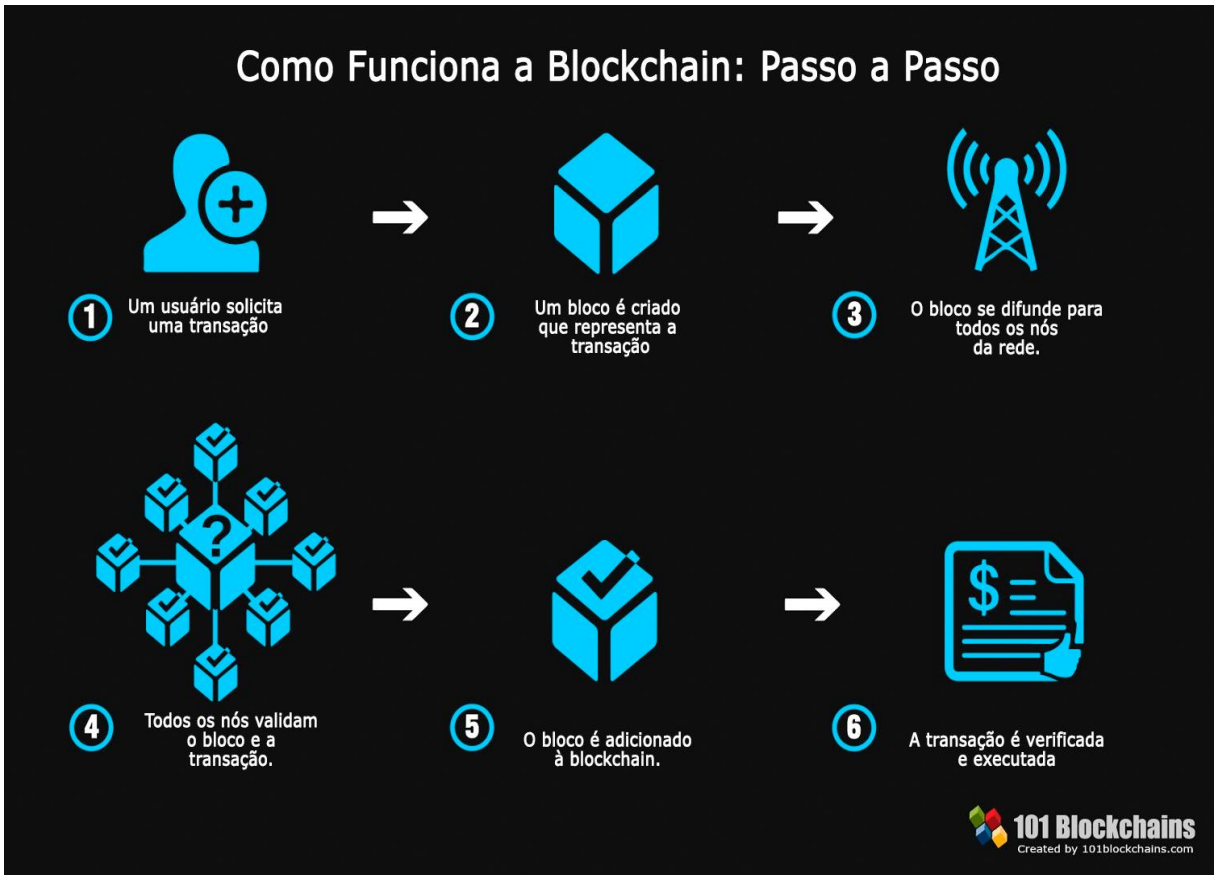
Antes de tudo é preciso entender o conceito das criptomoedas. Segundo o guia do Bitcoin (2018) criptomoedas são moedas que utilizam como proteção de seus dados sistemas de criptografia, utilizam também a criptografia para instituir novas unidades e admitir suas transações, por meio de cálculos realizados por supercomputadores conexos (nodes ou nós) na rede *blockchain* de maneira descentralizada. Um dos modelos mais conhecidos de criptomoeda é o Bitcoin (BTC).

Atualmente existem mais de 5000 tipos de criptomoedas, e a cada dia mais e mais modelos de moedas digitais são criadas. A principal característica da criptomoeda é a descentralização, ou seja, todo o procedimento de processo e transações são realizadas de forma coletiva na rede, sem que haja um supervisor ou uma autoridade central, sendo assim, o mercado é baseado na lei da oferta e da procura, o que acaba por gerar um certo risco financeiro (GUIA BITCOIN, 2018).

Em 2008 é publicado um artigo por Satoshi Nakamoto (pseudônimo) que descrevia a primeira criptomoeda descentralizada do mundo, o Bitcoin. O descritor do Bitcoin afirmava que junto com a criação da moeda virtual havia solucionado a questão da dupla despesa em moeda, por meio de uma base de dados que distribuída, a qual combinava criptografia, teoria dos jogos e ciência da computação (NAKAMOTO, 2008).

A Figura 1 traz exemplo de como funciona o *Blockchain*, estrutura da moeda Bitcoin.

Figura 1: Como funciona o *Blockchain*



Fonte: Lamouier (2018)

Sanchez (2012) ressalta que diferente dos papéis moedas, o Bitcoin não é estruturado em prata e nem ouro, e sim em provas matemáticas, sendo o primeiro meio digital para a troca de valor e isso só foi possível pelo desenvolvimento da *Blockchain* (cadeia de blocos). O Bitcoin é gerado por uma rede compartilhada de um livro público, que utiliza as tecnologias *Blockchain*, as quais gravam e validam cada transação.

Segundo Bitcoin trade (2019) sob a perspectiva da bitcoin Colin LeMahieu, de Minessota, desenvolvedor de software, em 2010 começou a estudar a moeda virtual e fazer uma análise acerca dos problemas que essa nova moeda poderia trazer no futuro.

Em 2014 Colin iniciou a elaboração e execução de um projeto de desenvolvimento de uma nova moeda isenta desses problemas. Os principais problemas a serem solucionados eram referentes a ineficiência energética, baixa escalabilidade (demora no tempo de processamento) e demora no tempo da confirmação das transações.

O problema da escalabilidade de cada bloco na *blockchain* é sua capacidade limitada de armazenamento de dados. Sobre o tempo de confirmação o mesmo é de 164 minutos e sobre a ineficiência energética a rede Bitcoin tem um consumo estimado em 27,28TWh por ano, consumindo em média 260KWh por transação (BITCOIN MEDIA, 2019).

Colin deu o nome a nova moeda de Raiblocks, a qual através de uma análise de estratégia de *marketing*, *rebranding* que tem a finalidade de mudar o visual da marca, logomarca e outros, mudaram o nome de *Raiblocks* para Nano Criptomoeda, essa mudança ocorreu em 2018 (BITCOIN TRADE, 2019).

De acordo com LeMahieu (2014) o sistema de consenso tem como característica importante o fornecimento de transações mais rápidas e mais determinado preservando um sistema forte e descentralizado. O autor descreve que algumas criptomoedas usam como estrutura os *blockchain*s, já a Nano usa como estrutura o *block lattice* (bloco de rede). Dentro deste contexto cada conta possui sua *blockchain* (cadeia da conta) equivalente ao histórico de transações/saldo da conta.

A moeda Nano tem seus consensos sob transações conflitantes através de um sistema de votação balanceada pelo saldo, já a criptomoeda Byteball alcança seu funcionamento e consenso sendo dependente de uma cadeia principal, com observatórios honestos, reputados e confiáveis, já a IOTA tem seu consenso através de transações empilhadas. Dentre as criptomoedas a Nano está e desenvolvimento e tem maior performance (LEMAHIEU, 2014).

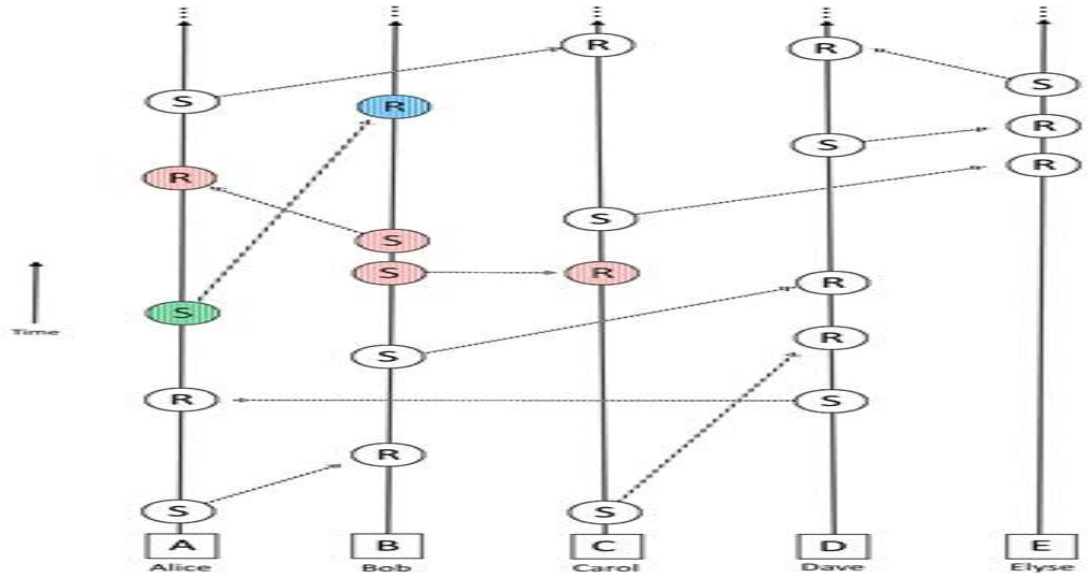
Traiders (2017) esclarece que na Nano cada *blockchain* das contas só pode ser atualizada pelo seu proprietário, o que permite que cada *blockchain* é atualizada de forma imediata e assíncrona ao resto da rede de blocos, o que permite que as transações sejam rápidas.

De acordo com o autor os blocos só podem ser adicionados pelos proprietários de forma individual. Transferir fundos de uma conta para a outra requer dois tipos de transação: uma delas é de envio que deduz o valor do saldo do remetente, a outra transação se refere ao

recebimento adicionando o valor do saldo da conta receptora. Vale ressaltar que a transação de recebimento pode acontecer a qualquer momento, e o destinatário não precisa estar online no processo de transação de envio.

A Figura 2 traz exemplo do procedimento *block lattice*.[1]

Figura 2: Representação Visual de transações assíncronas de *block lattice*



Fonte: Spillen (2018)

Segundo LeMahieu (2014) a cadeia só tem permissão de atualização pelo proprietário da conta, o que permite que a conta seja atualizada instantaneamente de forma assíncrona ao resto da *block lattice*, resultando em transações rápidas.

O protocolo Nano é tão leve, que cada transação cabe dentro do tamanho mínimo de pacote User Datagran Protocol (UDP) para ser transmitido pela internet. Em relação a Nano os requerimentos de hardware para os nós são os menores possíveis, mesmo porque os nós têm como função gravar e transmitir blocos para a maioria das transações (LEMAHIEU, 2014).

Sobre a efetividade da criptomoeda Nano, Coin (2020) no final de junho de 2018, diz que a Nano foi classificada como a mais rápida de todas as criptomoedas em intervalos de transação, os intervalos de confirmação de suas transações eram de três segundos. De acordo com o autor seu registro demonstra 2 GB, e é pequena frente ao tamanho de sua rede, que

[1] Receiving (R) de tradução recebendo e Synchronise (S) sincronizar.

possui mais de um TB, sendo assim, segundo a ideia de que o hardware é de baixo uso de energia pode ser executado com nós com registro completo ou com histórico reduzido.

Segundo LeMahieu (2014, p. 2) é importante ressaltar que a Nano possui alguns componentes como: conta, bloco transação, registro e nó. Abaixo estão brevemente explicados cada um dos componentes:

- Conta - uma conta é a parte de chave pública do par de chaves de uma assinatura digital, a chave pública, que seria o endereço é compartilhada com outros, já a chave privada é secreta;
- Bloco Transação- a transação é referente a ação e o bloco refere-se a codificação digital da transação;
- Registro – esse componente é um conjunto global de contas, onde cada conta tem sua própria cadeia de transações;
- Nó – é uma parte de software rodando em um computador que está sujeito ao protocolo Nano e que participa da rede Nano.

Traiders (2017) explica que embora a criptomoeda Nano tenha grande eficiência e segurança, pode sofrer ataques por partes maliciosas, as quais tem como objetivos ganhos financeiros ou queda no sistema.

Segundo LeMahieu (2014), a Nano é a primeira criptomoeda baseada em Grafos Acíclicos Dirigidos (DAG).

Após a criação da criptomoeda Nano, outras foram criadas baseadas em DAG, entre as mais notáveis a DagCoin/Byteball e a IOTA (RIBEIRO; RAISSAR, 2015; POPOV, 2017).

Serrano (2019) corrobora com o pensamento dos demais autores citados e explica que a Nano é uma moeda descentralizada, sem taxas, sustentável e incrivelmente rápida considerada como parte da terceira geração de criptomoedas. Ela é uma DAG, feita com a finalidade de ser simples e para sanar os problemas de insuficiência das outras criptomoedas.

O objetivo da moeda Nano é ser intuitiva, de fácil uso, sem taxas, com ampla velocidade de fácil acesso para todos. A Nano é uma moeda global que não precisa de muitos equipamentos para manter a sua rede, uma vez que é energicamente econômica, mas muito escalável segundo o aumento do hardware, o que aumenta a sua capacidade de transações por segundo, bem como a segurança e a descentralização (SERRANO, 2019).

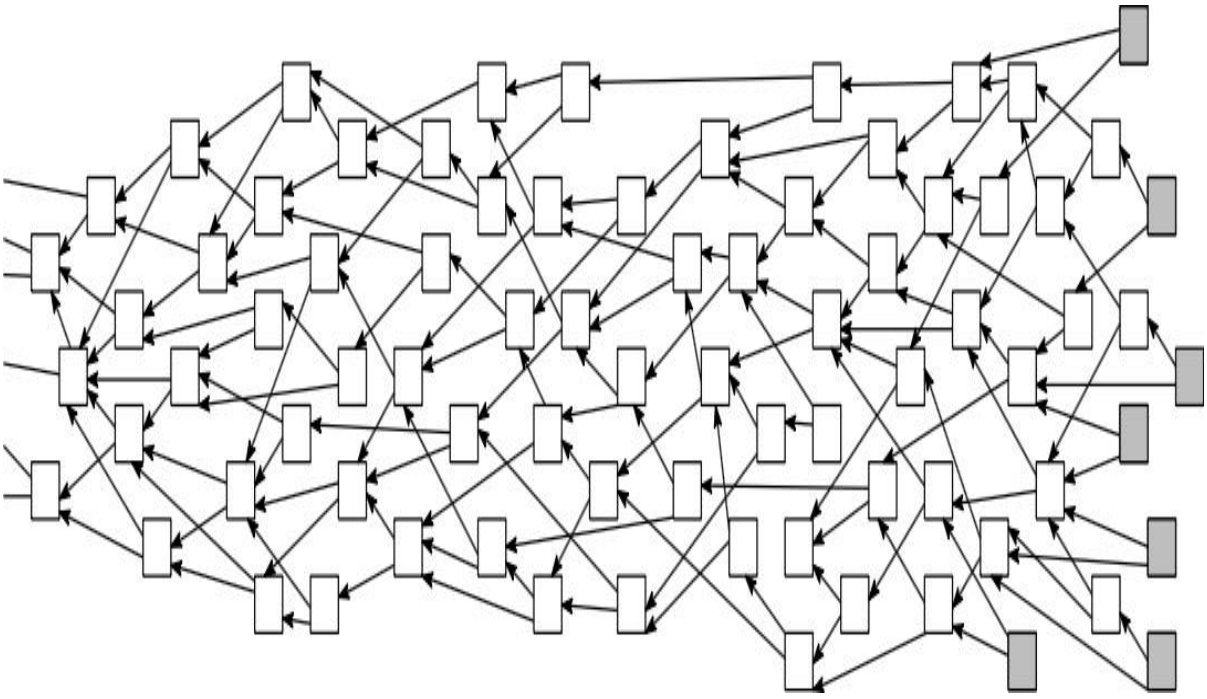
2.3 Grafos Acíclicos Dirigidos

Segundo Popov (2017) no campo da Ciência da Computação e Matemática, o DAG é um grafo direcionado e sem ciclos, conectando-se às outras arestas, o que denota que é impossível cursar todo o grafo a partir de uma borda. O autor explica que as bordas do grafo têm o segmento de apenas um caminho. O grafo é uma estrutura de lugar onde cada nó se encontra em uma ordem definida.

A DAG é, na verdade uma estruturação de dados, exemplificando, quando acontece uma transação, como compra, venda ou mesmo uma negociação, em uma criptomoeda tradicional, essa transação é agrupada em bloco, os quais tem um tamanho e um espaço predefinidos, esses blocos formam a *blockchain*. A estrutura da DAG permite transações individuais e como elas se interagem no quadro do *blockchain* em si (BITDEGREE, 2020).

A Figura 3 traz um exemplo de DAG.

Figura 3: Exemplo de DAG



Fonte: Popov, 2017

Popov (2017) explica que uma das características importantes da DAG é que esta é extremamente escalável, no entanto, a sua desvantagem é que não é extremamente segura, já o *blockchain* traz extrema segurança. O autor ressalta que a criptomoeda Nano tem como

objetivo somar o melhor dos dois mundos, a escalabilidade da DAG e a segurança da *blockchain.*

3 METODOLOGIA

A metodologia utilizada foi de Revisão Bibliográfica, onde foram consultados artigos que possuíam como tema o foco deste estudo. Os critérios de inclusão dos artigos foram a data de publicação (últimos 10 anos) e o idioma (língua portuguesa).

Ao total foram encontrados 12 documentos que fundamentaram o estudo.

4 RESULTADOS E DISCUSSÃO

Comben (2019) afirma que o modelo DAG é mais eficiente em relação ao que tange o armazenamento de dados e funciona como uma estrutura em árvore, aceitando um maior número de transações que podem ser validadas ao mesmo tempo.

Coin (2020) explica que em DAG, as conexões que ligam os círculos são as ligações entre transações. O autor explica que pelo modelo DAG os nós estão conectados semelhantemente aos ramos de uma árvore.

Um nó pode ter mais do que uma raiz, ou seja, os usuários não precisam esperar que uma transação seja concluída para que outra possa ser iniciada. Dessa forma, alguns autores destacam que o modelo DAG, pode melhorar o uso de uma rede, tornando-a mais escalável, fator ocasionado porque quanto mais nós desenvolvidos ao mesmo tempo, maior rapidez no processamento das transações, diferente dos *blockchains* (COIN, 2010).

Comparando-se a criptomoeda Nano com a Bitcoin é importante entender: a segunda organiza suas transações em blocos, o que leva um tempo de processamento de 10 minutos por bloco, para que a transação aconteça, ela deve ser incluída em um bloco e este deve ser minerado, como forma de garantir a segurança, as transações não são completas até ela ser adicionada a um bloco e alguns blocos são adicionados por cima, o que resulta em transações que podem demorar horas. Já com a Nano cada transação é individual, cada bloco é único e é capaz de ser processado de forma instantânea pela rede (TRAIDERS, 2017).

Comben (2019) explica que futuramente o modelo DAG pode substituir *blockchains,* devido a sua estrutura mais eficaz de armazenar dados e processar transformações online. O autor também explica que o modelo DAG pode resolver o problema da descentralização, além

de que uma rede alimentada por uma estrutura baseada em DAG pode se prestigiar com os melhores recursos de segurança.

O modelo DAG tem toda a estrutura e eficácia para se tornar *blockchain* 3.0, mas esse novo modelo ainda está em fase inicial e ainda há muitos caminhos a serem descobertos no que se refere a essa nova tecnologia. Embora o modelo DAG permita alta escalabilidade, tem suas desvantagens em redes pequenas as quais estão mais suscetíveis a ataques.

5 CONCLUSÃO

Diante de um mundo altamente voltado para a era digital, em que muitas transações são realizadas pela internet e de forma virtual, as criptomoedas surgiram como forma de modernidade e de tornar essas transações cada vez mais potencializadas, efetivas e seguras.

A primeira moeda, o Bitcoin embora tenha mostrado sua importância trouxe problemas que não a tornaram eficiente. A busca para melhorar essa realidade fez surgir novas criptomoedas, com arquiteturas diferentes e que trouxeram a resolução dos problemas encontrados na Bitcoin.

A Nano criptomoeda com sua estrutura baseada em DAG e *block lattice* apresenta eficiência, transações rápidas e menor consumo de energia, fatores importantes para moedas digitais que tem tentado a todo custo ganhar o mercado virtual.

No entanto, é preciso ressaltar que em relação à segurança a criptomoeda Nano não está livre de invasões, fator que precisa ser estudado e revisto para que os problemas sejam sanados. Uma das características mais importantes das moedas virtuais é garantir a segurança das transações e isso deve ser então uma das prioridades.

Assim como a Bitcoin teve sua estrutura de funcionamento reformulada a Nano precisa de adequações para alcançar a excelência e satisfazer as necessidades de seus usuários.

RFERÊNCIAS

BASS, L., CLEMENTS, P., KAZMAN, R. **Software Architecture in Practice,** Second Edition, Addison Wesley. 2003. Disponível em: http://www.garcia.pro.br/EngenhariadeSW/artigos%20engsw/art%204%20-%20Revista%20Engenharia%20de%20Software%20-%20edicao%206%20-%20fundamentos%20de%20Arquitetura%20de%20Software.pdf. Acesso em: 25 mar. 2022.

BITDEGREE. **Nano Coin- tudo o que você precisa saber sobre a XRB**. 2020. Disponível em: https://br.bitdegree.org/crypto/tutoriais/nano-coin. Acesso em: 2 abr. 2022.

BITCOIN. Guia do Bitcoin. **O que são criptomoedas**? 2018. Disponível em: https://guiadobitcoin.com.br/criptomoedas/. Acesso em: 30 mar. 2022.

CHERVINSKI, J. O. M, KREUTZ, D. Introdução às tecnologias dos blockchains e das criptomoedas. **Revista Brasileira de Computação Aplicada. v. 11, n. 3, p. 12-2, 2019.** Disponível em: http://seer.upf.br/index.php/rbca/article/view/9394. Acesso em: 10 abr. 2022.

COIN, B. N. **Investindo em *blockchain*s alternativos**: Nano. 2020. Disponível em: https://www.moneytimes.com.br/investindo-em-*blockchain*s-alternativos-parte-2-nano/. Acesso em: 12 mar. 2022.

COMBEN, C. **Quais criptomoedas usam uma estrutura baseada em DAG e por quê**? 2019. Disponível em: https://coinrivet.com/pt/cryptocurrencies-dag-model/. Acesso em: 2 abr. 2022.

LAMOUIER, L. **O Guia Definitivo Da Tecnologia Blockchain**: uma revolução para mudar o mundo. 2018. Disponível em: https://101blockchains.com/pt/tecnologia-blockchain-guia/. Acesso em: 30 mar. 2022.

LEMAHIEU, C. **Nano**: Uma Criptomoeda com Rede Distribuída sem Taxas. 2014. Disponível em: https://content.nano.org/whitepaper/Nano_Whitepaper_br.pdf#:~:text=As%20transa%C3%A7%C3%B5es%20sem%20custos%20e,ideal%20para%20transa%C3%A7%C3%B5es%20de%20consumidores.&text=Os%20acrescidos%20tempos%20de%20transa%C3%A7%C3%A3o,para%20o%20dia%20a%20dia. Acesso em: 20 mar. 2022.

MAGAZZENI D., P. McBurney and W. Nash, "Validation and Verification of Smart Contracts: A Research Agenda**," Computer**. v. 50, n. 9, , p 50-57, 2017. Disponível em: http://www.sadsj.org/index.php/revista/article/view/178/157. Acesso em: 20 abr. 2022.

MOUGAYAR, W. 2017. **Blockchain para negócios:** promessa prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books

NAKAMOTO, S. **Bitcoin**: A peer-to-peer electronic cash system. 2008. Disponível em: http://bitcoin.org/bitcoin.pdf. Acesso em: 20 mar. 2022.

POPOV, S. **"The tangle,"** 2016. Disponível em: https://content.nano.org/whitepaper/Nano_Whitepaper_br.pdf#:~:text=As%20transa%C3%A7%C3%. Acesso em: 23 mar. 2022.

RIBERO, Y.; RAISSAR, D. **Dagcoin whitepaper**. 2015. Disponível em: https://content.nano.org/whitepaper/Nano_Whitepaper_br.pdf#:~:text=As%20transa%C3%A7%C3%B5es%20sem%20custos%20e,ideal%20para%20transa%C3%A7%C3%B5es%20de%20consumidores.&text=Os%20acrescidos%20tempos%20de%20transa%C3%A7%C3%A3o,para%20o%20dia%20a%20dia. Acesso em: 20 mar. 2022.

SANCHEZ, D. **Man Mises on the Basics of Money** 2012. Disponível em: https://mises.org/library/mises-basics-money. Acesso em: 12 mar. 2022.

SERRANO, R. M. **Fique por dentro do mundo das criptos disponíveis no App Monnos.** 2019. Disponível em: https://monnos.com/blog/fique-por-dentro-do-mundo-das-criptos-disponiveis-no-app-monnos/. Acesso em: 25 mar. 2022.

SPÍNOLA, R. O.; BARCELOS, R. F. **Fundamentos da Arquitetura de Software**. 2015. Disponível em: http://www.garcia.pro.br/EngenhariadeSW/artigos%20engsw/art%204%20-%20Revista%20Engenharia%20de%20Software%20-%20edicao%206%20-%20fundamentos%20de%20Arquitetura%20de%20Software.pdf. Acesso em: 10 ago. 2020.
TRAIDERS, M. **Nano- FAQs**. 2017. Disponível em: https://criptobitbr.wordpress.com/. Acesso em: 23 fev. 2022.

SPILLEBEEN, I. **Blockchain Decrypted**: The Block Lattice - em profundidade. 2018. Disponível em: https://steemit.com/blockchain/@iwan.spillebeen/blockchain-decrypted-the-block-lattice-in-depth. Acesso em: 30 mar. 2022.

WASSERMAN, A. I. **Tool Integration in software engineering environments**. In: F. Longe d., SOFTWARE ENGINEERING ENVIRONMENTS. p. 138-150. Berlin: Springer-Verlag, 1996.