https://doi.org/10.54795/RejuBEsp.DirDig.227

CRIPTOATIVOS

CRYPTOASSETS

CARLOS EDUARDO DA SILVA CAMILLO
Juiz de direito do Tribunal de Justiça do Estado da Bahia – TJBA. Pós-graduado em Direito Público pela Universidade Gama Filho. Pós-graduado em Direito para Carreira da Magistratura pela Escola da Magistratura do Estado do Rio de Janeiro – Emerj.
https://orcid.org/0000-0003-4010-2477

RESUMO

O presente estudo visa trazer as principais funcionalidades dos criptoativos e sua aplicação no mundo jurídico. A pesquisa teve por base livros que trouxeram a história da criptografia que, desenvolvida, originou os criptoativos. Buscou-se demonstrar a criação das criptomoedas com a publicação do The White Paper de Satoshi Nakamoto, considerado o primeiro projeto de criptomoedas e criador do Bitcoin. No trabalho, com base nos escritos de Satoshi, é possível identificar que o Bitcoin (criptoativos) utiliza um livro denominado Blockchain, sendo um *log* de transações que registra todo o movimento da cripto utilizando *hashes* que trabalham como carimbo, cada transação emite um *hash* que é imutável, registrando toda a operação. Para que a rede funcione, deve haver uma prova de trabalho, denominada Proof of Work – PoW, em que os usuários verificam os blocos e se os *hashes* são oriundos dos blocos transacionados. Após essa explicação do funcionamento dos *blockchains,* o trabalho demonstra a aplicabilidade dessa tecnologia no Direito e no dia a dia, demonstrando o início da regulamentação

das criptomoedas no Brasil por meio do Banco Central e da Comissão de Valores Mobiliários – CVM, e no final de 2022, pela Lei n. 14.478/2022.

Palavras-chave: criptografia; segurança; quebra de criptografia; Bitcoin; Satoshi Nakamoto; criptoativos; Blockchain; Hash; mercado; regulação de mercado.

ABSTRACT

This study aims to bring the main features of cryptocurrencies and their application in the legal world. The research was based on historical books that brought the history of cryptography that developed cryptocurrencies. It sought to demonstrate the creation of cryptocurrencies with the publication of Satoshi Nakamoto's White Paper, considered the first cryptocurrency project and creator of Bitcoin. Based on Satoshi's writings, it is possible to identify that Bitcoin (cryptocurrency) uses a book called Blockchain, which is a log of transactions that records all movement of the cryptocurrency using hashes that work as stamps, each transaction emits an immutable hash, recording all O operations for the network to work, there must be a proof of work called (PoW), where users verify the blocks and if the hashes are from the transacted blocks. After this explanation of the functioning of blockchains, the study demonstrates the applicability of this technology in Law and everyday life, demonstrating the beginning of the regulation of cryptocurrencies in Brazil through the Central Bank and the Securities and Exchange Commission, and by the end of 2022, through Law No. 14,478/2022.

Keywords: cryptography; security; cryptography break; Bitcoin; Satoshi Nakamoto; cryptoassets; Blockchain; Hash; market; market regulation.

SUMÁRIO

1 Introdução. 2 História da criptografia. 3 Criação do Bitcoin. 4 Blockchain. 5 Estrutura lógica dos blockchains. 6 Mercado descentralizado e o Direito. 7 Conclusão. Referências.

1 INTRODUÇÃO

As criptomoedas ou criptoativos são uma realidade atualmente. Para entender como chegamos a essa tecnologia, temos que buscar a origem da criptografia, remontando a milhares de anos, desde o Antigo Egito até os dias atuais, tal arte de embaralhar (criptografar) e codificar mensagens é o meio mais seguro de manter segredos e, agora, o dinheiro em transações entre pessoas, dando segurança às operações e facilitando a vida das pessoas, sem que o Estado intervenha em tais avenças. Contudo, para evitar o cometimento de crimes como o de lavagem de dinheiro (*money laundry*), é necessário que se tenha o mínimo de regulação e controle, o que contraria a criação das criptos conforme se extrai da obra The White Paper de Satoshi Nakamoto. Diante desse dilema, a Comissão de Valores Mobiliários – CVM e o Banco Central iniciaram a regulamentação para evitar que criminosos evadissem divisas através dos criptoativos e também não lavassem dinheiro por meio desses ativos. O legislador pátrio atento à modernidade, criou a Lei n. 14.478/2022, que regulou as operações de criptoativos em território brasileiro.

2 HISTÓRIA DA CRIPTOGRAFIA

A criptografia é a arte e a ciência de proteger informações secretas mediante a codificação para garantir o segredo entre o

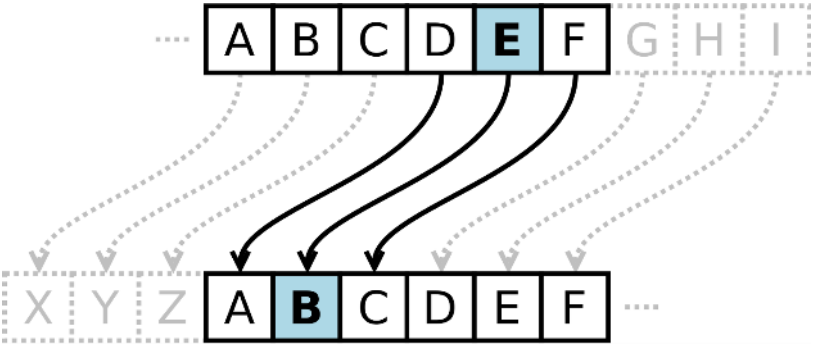
comunicador e o receptor. Tal arte tem sido usada há milhares de anos, desde o Antigo Egito, em que os hieróglifos eram usados para escrever mensagens secretas, até a Guerra Fria, quando a criptografia era usada para proteger informações militares e diplomáticas, e foi utilizada para vencer a Segunda Guerra Mundial. Na Idade Média, os monges usavam a criptografia para escrever textos sagrados e os comerciantes usavam para proteger informações comerciais.

Na Antiguidade, a literatura diz que a Cifra de César foi uma das primeiras criptografias registradas em papel e posta para estudos.

> A Cifra de César, também conhecida como Cifra de Troca, utilizada para proteger comunicações governamentais, é uma técnica de cifragem por substituição na qual cada letra é substituída por outra, que está logo após ela, definida por um número fixo. Por exemplo, ao utilizar o número três, cada letra do texto original será substituída pela letra que está três posições sucessivas, ou seja, para formar o texto cifrado a letra A torna-se D, B se torna E, e assim por diante (Sales, 2015 *apud* Silva, 2019, p. 16).

Vejamos o esquema das Cifras de César:

Figura 1 – Cifras de César



Fonte: Wikimedia commons (2023)

O uso das máquinas de criptografia visava proteger as comunicações militares. Uma das mais famosas máquinas era conhecida como Enigma, que era usada para codificar mensagens transmitidas por rádio. Essa máquina foi responsável por diversos ataques dos militares nazistas aos Aliados, e matou milhares de soldados durante o período da guerra, pois sua criptografia não era decifrada pelos militares aliados.

Essa principal ferramenta alemã, a Enigma, era uma máquina eletromecânica que funcionava com base em um conjunto de rotores que mudavam a configuração da criptografia a cada tecla pressionada. Isso tornava a decodificação das mensagens extremamente difícil, pois era necessário conhecer a configuração exata dos rotores.

A Alemanha também usou outras máquinas de criptografia, como a Lorenz e a Siemens e Halske T52. As máquinas de criptografia da Alemanha eram consideradas as mais avançadas da época, e quebrá-las era considerado um grande desafio, visto que não existia tecnologia disponível para consertá-las.

O empenho intelectual e os esforços dos Aliados para quebrar a criptografia da Alemanha foram conhecidos como Operação Ultra, que teve como objetivo interceptar e decodificar as mensagens da Enigma, e foi um dos segredos mais bem guardados da guerra.

A quebra da criptografia alemã foi um dos principais fatores que ajudou os Aliados a vencer a Segunda Guerra Mundial. A informação obtida por meio da decodificação das mensagens criptografadas permitiu que os Aliados tomassem decisões estratégicas mais informadas e evitassem armadilhas alemãs.

Sabemos que os nazistas usaram máquinas de criptografia avançadas, como a Enigma, durante a Segunda Guerra Mundial para proteger suas comunicações militares. Os Aliados, liderados pelos britânicos, trabalharam duro para quebrar essa criptografia, o que

foi fundamental para vencer a guerra. Os esforços para quebrar a criptografia foram conhecidos como Operação Ultra.

Existe a chamada criptografia simétrica, também conhecida como criptografia de chave secreta, que é uma das formas mais antigas de criptografia. Nessa técnica, a mesma chave é usada para cifrar e decifrar a mensagem. Um exemplo é a Cifra de César, usada pelo General romano Júlio César, em que cada letra do texto original é deslocada por um número fixo de posições.

Criptografia de chave pública, também conhecida como criptografia assimétrica, foi desenvolvida no século XX. Nessa técnica, existem duas chaves: uma chave pública, que é compartilhada, e uma chave privada, que é mantida em segredo. Isso permite que as pessoas possam cifrar mensagens usando a chave pública, mas apenas a pessoa com a chave privada pode decifrá-las.

O sistema de criptografia tem sido essencial para a segurança das comunicações eletrônicas e para a privacidade dos dados. Com o avanço da tecnologia, a criptografia tem se tornado cada vez mais complexa e sofisticada. Atualmente, a criptografia é usada em muitas áreas, como segurança de redes, criptomoedas, assinatura eletrônica, entre outras.

3 CRIAÇÃO DO BITCOIN

Muitos não sabem, mas temos o precursor do Biticoin, o chamado Bit Gold, criado em 1998, por Nick Szabo, que foi um experimento em que se buscava a criação de uma moeda digital para ter uma forma de pagamento descentralizado.

O Bit Gold foi um sistema descentralizado para a criação e a transferência de propriedade de ativos digitais, que se baseia na ideia de usar a prova criptográfica de trabalho para criar um ativo digital, que

é escasso e verificável. O conceito de Bit Gold nunca se desenvolveu completamente, mas é considerado um precursor importante para o desenvolvimento do Bitcoin e de outras criptomoedas.

Temos que a criação do Bitcoin se deu em 2009 por uma pessoa ou grupo de pessoas usando o pseudônimo Satoshi Nakamoto, utilizando vários fundamentos do Bit Gold (Campos, 2020, p. 31). Ele é uma criptomoeda descentralizada e é considerado o primeiro dinheiro digital descentralizado do mundo.

O Bitcoin é baseado em uma tecnologia chamada Blockchain, que é uma forma de registro distribuída que permite que as transações sejam registradas e verificadas sem a necessidade de uma autoridade central. O objetivo original do Bitcoin era disponibilizar uma forma de pagamento eletrônico sem a necessidade de intermediários, como bancos. Satoshi Nakamoto descreve bem isso em sua obra The White Paper – Bitcoin: a peer-to-peer electronic cash system:

> The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.
>
> We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were

> received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received (Nakamoto, [20--]).

Estruturalmente, o Bitcoin é baseado em uma rede de computadores distribuídos que mantêm uma cópia atualizada do registro de todas as transações realizadas na rede. Essas transações são registradas em um livro-razão descentralizado chamado Blockchain. Cada nova transação é adicionada ao Blockchain como um "bloco" e é confirmada por outros usuários da rede antes de ser adicionada à cadeia. Isso garante a segurança e a imutabilidade dos registros. Além disso, o Bitcoin usa criptografia para garantir a segurança das transações e a privacidade dos usuários.

Para entendermos o Bitcoin, temos que saber que é uma criptomoeda descentralizada, ou seja, não é controlada por nenhum governo, banco ou instituição financeira. Em vez disso, é mantida e controlada pela rede de usuários que participam da mineração do Bitcoin.

Os mineradores são responsáveis por confirmar as transações e adicioná-las ao Blockchain. Eles fazem isso resolvendo problemas matemáticos complexos para adicionar um novo bloco à cadeia. Como recompensa, eles recebem uma certa quantidade de Bitcoins. Isso incentiva as pessoas a participarem da rede e a contribuírem para a segurança dela.

Sendo a oferta máxima de Bitcoins de 21 milhões de unidades, e atualmente mais de 18 milhões foram mineradas. O processo de mineração também garante que a moeda seja escassa e seu valor tende a aumentar ao longo do tempo.

Aliás, o Bitcoin usa a tecnologia Peer-to-Peer – P2P, ou seja, as transações são feitas diretamente entre os usuários, sem a necessidade de intermediários. Isso torna o Bitcoin uma forma de pagamento rápida, segura e descentralizada. A tecnologia P2P é

criada por desenvolvedores de *software* que trabalham em projetos para criar sistemas descentralizados que permitem a comunicação e o compartilhamento de informações entre usuários diretamente, sem a necessidade de intermediários. Isso é feito por meio de uma combinação de protocolos de rede, algoritmos de roteamento e criptografia.

Os protocolos de rede são usados para estabelecer comunicação entre os diferentes nós da rede P2P. Eles permitem que os usuários se conectem uns aos outros e troquem informações. Algoritmos de roteamento são usados para garantir que as informações cheguem ao destinatário correto. Eles também permitem que os usuários encontrem outros usuários na rede e estabeleçam conexões com eles.

Diante disso, vemos que a criptografia é usada para garantir a segurança das informações transmitidas na rede. Isso garante que as informações sejam protegidas de acessos não autorizados, bem como a privacidade dos usuários.

É importante notar que a tecnologia P2P está em constante evolução, e novas melhorias e desenvolvimentos estão sendo feitos continuamente para tornar as redes P2P mais seguras, escaláveis e eficientes.

4 BLOCKCHAIN

Blockchain é uma tecnologia de registro distribuído que tem o potencial de mudar a forma como as empresas e os indivíduos gerenciam e compartilham informações e valores. Ele é o fundamento por trás das criptomoedas, como o Bitcoin, mas tem muitas outras aplicações além disso.

A principal característica do Blockchain é a sua descentralização. Ao contrário de um banco ou outra instituição financeira centralizada, não há uma autoridade central que controle a rede Blockchain. Em vez

disso, a rede é mantida por uma série de nós, que são computadores conectados que mantêm uma cópia do livro-razão e participam na validação e no registro de novas transações.

Outra característica importante do Blockchain é a sua segurança. As transações são registradas de maneira críptica e segura, o que torna muito difícil alterar transações registradas anteriormente na cadeia de blocos. Além disso, como o Blockchain é descentralizado, ele é resistente a ataques e fraudes, pois é preciso controlar a maioria dos nós da rede para realizar qualquer tipo de alteração.

Vemos que o Blockchain tem muitas aplicações além das criptomoedas. Na indústria financeira, por exemplo, ele pode ser usado para aumentar a eficiência e reduzir os custos das transações financeiras, além de oferecer maior segurança e transparência. Na gestão de ativos, ele pode ser usado para registrar e transferir ativos digitais de maneira segura e eficiente. Na votação eletrônica, ele pode ser usado para garantir a integridade e a transparência do processo de votação.

Além disso, em Supply Chain, o Blockchain pode ser usado para rastrear e registrar a origem e a propriedade dos produtos, assim como para aumentar a transparência e a confiabilidade no processo de compra e venda.

É uma tecnologia promissora com múltiplas aplicações e potencial para transformar vários setores. Enquanto ainda estamos vendo o seu potencial total, é claro que a tecnologia Blockchain tem o potencial de mudar a forma como lidamos com transações e compartilhamos informações e valores.

Blockchain pode ser aplicado ao Direito de várias maneiras, algumas das quais incluem:

Registro de propriedade: o Blockchain pode ser usado para registrar e armazenar informações sobre propriedades, incluindo histórico de transações e documentos legais. Isso pode tornar o

processo de transferência de propriedade mais rápido e seguro, além de ajudar a prevenir fraudes.

Contratos inteligentes: os contratos inteligentes são programas que podem ser executados automaticamente no Blockchain. Eles podem ser usados para automatizar processos legais, como pagamentos automáticos, quando certas condições são atendidas. Isso pode tornar os contratos mais seguros e eficientes.

Prova de identidade: o Blockchain pode ser usado para armazenar informações de identidade de forma segura e compartilhar essas informações com as partes interessadas. Isso pode ajudar a prevenir fraudes e a garantir que apenas as pessoas certas tenham acesso a certas informações.

Prova de propriedade intelectual: o Blockchain pode ser usado para registrar e armazenar informações sobre propriedade intelectual, como patentes, direitos autorais e marcas comerciais. Isso pode ajudar a prevenir violações de propriedade intelectual e a garantir que os direitos dos titulares sejam protegidos.

Registro de votos eletrônicos: o Blockchain pode ser usado para registrar e armazenar informações sobre votos eletrônicos de forma segura e transparente. Isso pode ajudar a garantir a integridade do processo eleitoral e a aumentar a confiança dos eleitores.

Registro de ativos digitais: o Blockchain pode ser usado para registrar e armazenar informações sobre ativos digitais, como *tokens* de segurança, moedas virtuais e outros ativos digitais. Isso pode ajudar a garantir a transparência e a segurança das transações de ativos digitais.

Gestão de documentos legais: o Blockchain pode ser usado para armazenar e compartilhar documentos legais de forma segura e transparente. Isso pode ajudar a garantir a autenticidade dos documentos e a facilitar o acesso a eles.

Análise de dados: o Blockchain pode ser usado para coletar e armazenar informações sobre transações e atividades legais, que podem ser usadas para análise de dados e geração de *insights*. Isso pode ajudar a identificar tendências e padrões que podem ser úteis para tomar decisões estratégicas.

Resolução de disputas: o Blockchain pode ser usado para armazenar informações sobre disputas legais e fornecer evidências para auxiliar na resolução de disputas. Isso pode ajudar a tornar o processo de resolução de disputas mais justo e eficiente.

Transparência regulatória: o Blockchain pode ser usado para registrar e armazenar informações sobre atividades reguladas, como transações financeiras, para ajudar a garantir a transparência e a conformidade regulatória.

É importante notar que, embora o Blockchain tenha muito potencial para aplicações no Direito, ainda há desafios a serem superados, como a questão da regulamentação, a proteção de dados e a questão da jurisdição. Além disso, é importante que os profissionais do Direito se familiarizem com a tecnologia e seus potenciais impactos para poder aplicá-los de forma adequada.

5 ESTRUTURA LÓGICA DOS BLOCKCHAINS

A segurança do Blockchain é garantida por vários fatores. Um deles é a descentralização da rede, ou seja, a falta de um único ponto de falha. Como o Blockchain é mantido por uma rede de computadores distribuídos, é muito difícil para os *hackers* atacarem a rede e alterarem os dados. Além disso, a criptografia é usada para garantir a segurança das transações e a privacidade dos usuários.

Outro fator importante é a imutabilidade dos registros, ou seja, uma vez que um bloco é adicionado à cadeia, ele não pode ser alterado ou excluído. Isso garante a integridade dos dados e evita fraudes.

A mineração também é importante para a segurança do Blockchain. Os mineradores são responsáveis por confirmar as transações e adicioná-las ao Blockchain. Eles fazem isso resolvendo problemas matemáticos complexos para adicionar um novo bloco à cadeia. Isso incentiva as pessoas a participar da rede e a contribuir para a segurança dela.

Existem outras medidas de segurança que podem ser implementadas para proteger o Blockchain, como a gestão de chaves privadas, a autenticação de multifatores e a auditoria de segurança.

A segurança do Blockchain é garantida pela descentralização, criptografia, imutabilidade dos registros, mineração, e outras medidas de segurança adicionais que podem ser implementadas. No entanto, é importante lembrar que a segurança não é algo absoluto, e mesmo as redes Blockchain podem ser vulneráveis a ataques cibernéticos.

Veremos a seguir que a estrutura lógica de um Blockchain é composta por três elementos principais: blocos, transações e nós.

Blocos: cada bloco contém uma série de transações e é adicionado à cadeia de forma cronológica. Cada bloco também contém um cabeçalho, que inclui informações como a data e a hora da criação do bloco, a *hash* do bloco anterior e a *hash* do próprio bloco. Porém, a capacidade de armazenar as informações dentro dos blocos não é abundante, sendo limitada ao que faz com que utilize o chamado GAS.

Esse GAS é a uma unidade de medida.

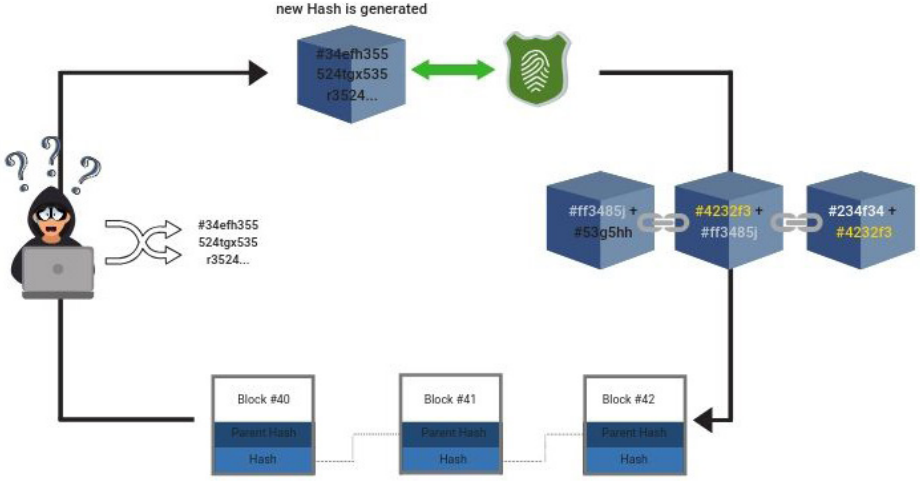
E o que é um *hash*?

> Um hash é como um aglomerado de caracteres que identifica determinado bloco (como que a sua própria impressão digital) e este serve exatamente para identificar cada bloco e determinar a sua ordem na Blockchain conjuntamente

> com os selos temporais/timestamps que indicam o tempo a que o bloco foi criado. Assim o bloco 2 contém o *hash* que identifica o bloco 1 bem como o seu próprio *hash* identificador. Portanto o *hash* é o elemento de ligação entre os blocos (Freire, 2021, p. 18).

O esquema dos *hashs* é representado na presente figura:

Figura 2 – Hashs



Fonte: Nirolution ([2019])

As transações são as operações registradas no Blockchain. Elas podem incluir transferências de valor, contratos inteligentes e outras operações.

Os nós são os computadores que participam da rede e mantêm uma cópia atualizada do Blockchain. Eles podem ser usados para validar transações, adicionar novos blocos à cadeia e manter a integridade da rede.

É importante notar que existem diferentes tipos de Blockchain: público, privado e de consórcio. Cada tipo de Blockchain tem suas próprias características e implicações para a segurança e a privacidade.

Analisando a estrutura lógica de um Blockchain e sua composição por blocos, transações e nós. Os blocos contêm uma série de transações e são adicionados à cadeia de forma cronológica, cada um com um cabeçalho que inclui informações como a data e a hora da criação do bloco, a *hash* do bloco anterior e a *hash* do próprio bloco. As transações são as operações registradas no Blockchain, como transferências de valor, contratos inteligentes e outras operações. Os nós são os computadores que participam da rede e mantêm uma cópia atualizada do Blockchain, que podem ser usados para validar transações, adicionar novos blocos à cadeia e manter a integridade da rede.

Vemos que a *hash* é uma função matemática que transforma dados de entrada de qualquer tamanho em um valor de saída fixo, chamado *hash*. No contexto do Blockchain, as *hashes* são usadas para identificar de forma única cada bloco e cada transação na rede.

Cada bloco no Blockchain contém uma *hash* única que é gerada a partir do conteúdo do bloco. Isso inclui a *hash* do bloco anterior, ou seja, a *hash* do bloco anterior é incluída no cabeçalho do novo bloco, criando uma cadeia de blocos. Isso garante a integridade dos dados, visto que qualquer alteração no bloco anterior iria alterar a *hash* do bloco atual e todos os seguintes.

Assim, cada transação também tem uma *hash* única, que é usada para identificá-la e garantir a sua integridade. Isso é importante para assegurar que as transações sejam válidas e não tenham sido modificadas durante a transmissão.

O processo de criação de uma *hash* é chamado de *hashing* e é realizado por algoritmos específicos, como o SHA-256 (Secure

Hash Algorithm 256 bits), que é utilizado no Bitcoin. Esse algoritmo é considerado altamente seguro e difícil de ser quebrado.

De certo que as *hashes* também são usadas na mineração, onde os mineradores precisam resolver problemas matemáticos complexos para encontrar a *hash* correta de um novo bloco. Isso é conhecido como Prova de Trabalho (Poof of Work – PoW) e é uma forma de garantir a segurança da rede e evitar ataques de spam.

As *hashes* são usadas no Blockchain para identificar de forma única cada bloco e transação, garantir a integridade dos dados e manter a segurança da rede. Elas são geradas por meio de algoritmos de *hash* específicos e são usadas na mineração para garantir a segurança da rede.

Sabemos que as *hashes* também são usadas para garantir a privacidade das transações, visto que as informações são codificadas e só as chaves privadas dos envolvidos podem acessar essas informações.

Dessa forma, as *hashes* também são usadas para criar endereços de carteira, que são usados para enviar e receber transações. Esses endereços são gerados a partir das chaves públicas dos usuários e são usados como identificadores únicos na rede.

Uma das características fundamentais do Blockchain são as *hashes*, pois garantem a integridade, a segurança e a privacidade das informações registradas na rede. Elas também são usadas para criar endereços de carteira e garantir a privacidade das transações.

6 MERCADO DESCENTRALIZADO E O DIREITO

A regulamentação das criptomoedas nos Estados Unidos é realizada por várias agências governamentais, incluindo a Securities and Exchange Commission – SEC, a Commodity Futures Trading Commission – CFTC e o Financial Crimes Enforcement Network –

FinCEN. A SEC regulamenta as criptomoedas que são consideradas valores mobiliários, enquanto a CFTC regulamenta as criptomoedas que são consideradas *commodities*. FinCEN regulamenta as criptomoedas no que diz respeito à lavagem de dinheiro e outros crimes financeiros. Além disso, as leis estaduais também podem ter regulamentos específicos para criptomoedas.

Em geral, as criptomoedas são consideradas como ativos especulativos e não há um regulamento específico para elas, no entanto, a SEC tem estabelecido algumas regulamentações para Initial Coin Offerings – ICOs. Algumas corretoras de criptomoedas e casas de câmbio também estão sendo regulamentadas pelo governo.

Os mercados descentralizados, como o Bitcoin e outras criptomoedas, têm se tornado cada vez mais populares e estão crescendo rapidamente, mas ainda estão em fase inicial de regulamentação no Brasil. Em geral, o Direito brasileiro ainda está se adaptando para lidar com essas novas tecnologias e suas implicações legais.

Em 2019, o Banco Central do Brasil – BCB emitiu uma carta circular que declarou que as criptomoedas não são consideradas moedas legais no país. No entanto, o BCB também reconheceu o potencial dessas tecnologias e tem trabalhado para desenvolver regulamentações que possam proteger os consumidores e prevenir fraudes, sem impedir o desenvolvimento desses mercados.

A Comissão de Valores Mobiliários – CVM do Brasil também tem se posicionado sobre o assunto, emitindo instruções sobre a oferta e negociação de ativos digitais, como criptomoedas e *tokens*. A CVM tem estabelecido regras para garantir a transparência e a segurança dessas operações e tem trabalhado para evitar a utilização desses ativos para lavagem de dinheiro ou outras atividades ilegais.

Em busca de uma regulamentação para evitar crimes financeiros e controlar o mercado, a CVM vem emitindo instruções para regular

a oferta e negociação de criptomoedas e outros ativos digitais. Em 2017 a CVM emitiu a Instrução n. 590, que estabeleceu regras para a oferta pública de valores mobiliários, incluindo *tokens* criptográficos. Essa instrução estabeleceu requisitos de divulgação, governança corporativa e registro para emissores de *tokens*.

Foram emitidos alertas e orientações, pela CVM, para os investidores sobre os riscos associados à negociação de criptomoedas e outros ativos digitais, além do esforço para evitar a utilização desses ativos para lavagem de dinheiro ou outras atividades ilegais.

O Parecer de Orientação CVM n. 40, de 11 de outubro de 2022, é uma orientação da CVM do Brasil que trata da negociação de criptoativos no país, estabelecendo regras para as corretoras e bolsas de criptoativos. O parecer tem como objetivo garantir a transparência e a proteção do investidor, bem como prevenir a lavagem de dinheiro e outras atividades ilegais relacionadas à negociação de criptoativos.

Esse ato normativo da CVM exige que as corretoras e as bolsas de criptoativos sejam registradas e regulamentadas e que cumpram regras específicas em relação à governança corporativa, gestão de riscos e segurança da informação. Elas também estão obrigadas a implementar medidas para prevenir a lavagem de dinheiro e o financiamento ao terrorismo, além de serem obrigadas a reportar qualquer transação suspeita às autoridades competentes.

Tal resolução também estabelece regras para a negociação de criptoativos, exigindo que as corretoras e as bolsas forneçam informações claras e precisas sobre os ativos negociados e suas características.

Para que a regulamentação pudesse ser efetiva, o legislador ordinário editou a Lei n. 14.478/2022, denominada pelo mundo jurídico de Marco Legal das Criptomoedas.

A citada lei elenca o que é ativo digital, conceituando como:

> Art. 3º Para os efeitos desta lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, não incluídos:
> I - moeda nacional e moedas estrangeiras;
> II - moeda eletrônica, nos termos da Lei n. 12.865, de 9 de outubro de 2013;
> III - instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e
> IV - representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros (Brasil, 2022).

A Lei n. 12.865 de 2013 trouxe o conceito de moeda eletrônica, em seu art. 6º, inciso VI, vejamos:

> Art. 6º Para os efeitos das normas aplicáveis aos arranjos e às instituições de pagamento que passam a integrar o Sistema de Pagamentos Brasileiro (SPB), nos termos desta Lei, considera-se:
> VI - moeda eletrônica - recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento (Brasil, 2013).

A legislação brasileira trouxe essa inovação para tentar regular o mercado de moedas eletrônicas, mas os criptoativos não são em si moedas eletrônicas, como os NFTs, que são imagens geradas com *hash* que as permitem negociar em Blockchain, garantindo a transação, e tais dispositivos não foram abarcados pela norma.

Vimos que a criação do Bitcoin foi justamente para evitar que tais ativos fossem regulados e administrados pelos governos, dentro dos conceitos de anarquia, o livre mercado e o Estado mínimo. A legislação

posta vai na contramão da essência dos criptoativos, visto que busca regulamentar e controlar as transações por meio da lei.

7 CONCLUSÃO

Vimos que a criptografia foi uma forma matemática criada pelo homem para poder transmitir mensagens sem que fossem interceptadas e interpretadas pelo interceptador. Com a evolução humana, a forma de criptografar foi se desenvolvendo até chegarmos no chamado Blockchain.

Com a criação do Bitcoin e com o tempo outros criptoativos, visando à descentralização dos ativos sem a interferência do Estado, em uma grande demonstração do liberalismo e libertarismo, os governos passaram a procurar meios de controlar essas transações como a fundamentação de tentar evitar crimes tributários e crimes de lavagem de dinheiro.

O legislador pátrio buscou amarrar os ativos digitais existentes no mercado, contudo, tal legislação não pode abarcar o que a tecnologia nos demonstra que irá acontecer, novas e novas formas de transações virtuais que estão por vir irão fazer que tais legislações sejam alteradas na mesma velocidade que a tecnologia avança.

Desse modo, qualquer legislação posta pelo Estado deverá ser dinâmica, deixando para o BCB e para a CVM realizarem as alterações por meio de sua independência política e seu poder regulador.

Portanto, a atuação do BCB e da CVM é importante para garantir a segurança e a regulamentação adequadas do mercado de ativos digitais, mas também é importante que a independência desses órgãos seja preservada para que eles possam tomar decisões baseadas em evidências e sem pressões políticas.

No final, a interação entre tecnologia, regulamentação e mercado é complexa e requer uma abordagem cuidadosa e equilibrada para garantir a segurança e a eficiência do sistema financeiro, bem como a proteção dos direitos e interesses dos usuários, visto que a aplicação da tecnologia dos Blockchains pode ajudar a Administração Pública a ter um controle e uma credibilidade verificada digitalmente em todos os seus processos, inclusive no sistema financeiro com a criação de moedas digitais em substituição às cédulas de papel e moedas cunhadas em metal.

REFERÊNCIAS

BACK, Adam. **Hashcash – a denial of service counter-measure**. [*S. l.*]: Hashcash, 1st Aug. 2002. Disponível em: http://www.hashcash.org/papers/hascash.pdf. Acesso em: 20 jan. 2023.

BANCO CENTRAL DO BRASIL. **Estatística do setor externo**. Brasília: BCB, 26 ago. 2019. Disponível em: https://www.bcb.gov.br/content/estatisticas/hist_estatisticassetorexterno/201908. Acesso em: 22 mai.2023.

BAYER, Dave; HABER, Stuart; STORNETTA, W. Scott. Improving the efficiency and reliability of digital time-stamping. *In*: CAPOCELLI, Renato; DE SANTIS, Alfredo; VACCARO, Ugo (ed.). **Sequences II**: Methods in Communication, Security and Computer Science. New York: Springer, 1993. p. 329-334.

BRASIL. **Lei n. 12.865, de 9 de outubro de 2013**. Autoriza o pagamento de subvenção econômica aos produtores da safra 2011/2012 de cana-de-açúcar e de etanol que especifica e o financiamento da renovação e implantação de canaviais com equalização da taxa de juros [...]. Brasília, DF: Presidência da República, 2013.

BRASIL. **Lei n. 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros [...]. Brasília, DF: Presidência da República, 2022.

BRASIL. **Parecer de Orientação CVM n. 40. de 11 de outubro de 2022**. Os CriptoAtivos e o Mercado de Valores Mobiliários. Brasília, DF: CVM, 2022. Disponível em: https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html. Acesso em: 11 set. 2023.

CAMPOS, Emília Malgueiro. **Criptomoedas e Blockchain**: o direito no mundo digital. 2. ed. Rio de Janeiro: Lumen Juris, 2020.

FILE: Cesar cipher left shift of 3.svg. *In*: WIKIMEDIA Commons. [San Francisco, CA: Wikimedia Foundation, 2023]. Disponível em: https://commons.wikimedia.org/w/index.php?curid=30693472. Acesso em: 11 set. 2023.

FREIRE, João Pedro. **Blockchain e smart contracts**: implicações jurídicas. Coimbra: Almedina, 2021.

HABER, Stuart; STORNETTA, W. Scott. How to time-stamp a digital document. **Journal of Cryptology**, [*s. l.*], v. 3, p. 99-111, 1991.

HABER, Stuart; STORNETTA, W. Scott. Secure names for bit-strings. *In*: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 4., 1997, [Zurich]. **Proceedings** [...]. [Zurich]: ACM, April 1997. p. 28-35.

MERKLE, Ralph C. Protocols for public key cryptosystems. *In:* SYMPOSIUM ON SECURITY AND PRIVACY, 1980, Sunnyvale. **Proceedings** [...]. Sunnyvale: IEEE Computer Society, April 1980, p 122- 133.

NAKAMOTO, Satoshi. **Bitcoin**: A peer-to-peer electronic cash system. [*S. l.: s. n.*], [20--].

NIROLUTION. What is a Blockchain Hash Function? Best Hash Explanation. **Nirolution**, [*s. l.*], 2018. Disponível em: https://nirolution.com/blockchain-hash-function/. Acesso em: 11 set. 2023.

SILVA, Willian Wallace de Matteus. **A evolução da criptografia e suas técnicas ao longo da história**. 2019. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Instituto Federal Goiano, Goiás, 2019. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1/tcc_Willian_Wallace_de_Matteus_Silva.pdf. Acesso em: 10 jan. 2023.