centro universitário
unifacvest

# Blockchain e Criptomoedas

# *Blockchain*

## Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Discutir o conceito de *blockchain*.
- Identificar aspectos de segurança do *bockchain*.
- Analisar o funcionamento das moedas virtuais.

## Introdução

O saber popular, principalmente o que nossos pais e avós sempre disseram, é que não se pode confiar em nada que se compre pela internet. No entanto, o *blockchain* é uma tecnologia que veio para mudar o conceito de segurança.

Neste capítulo, você conhecerá o *blockchain*, perpassando pelo seu histórico e sua evolução, bem como suas definições e contribuições para o avanço da "segurança" na troca de informações pela internet. Além disso, entenderá como funciona a negociação das moedas virtuais (também conhecidas como criptomoedas) e como esse fenômeno relativamente novo impactou, impacta e ainda impactará muito na vida de todos. Por fim, compreenderá como o *blockchain* e as moedas virtuais mudaram a forma de pensar em transações via internet.

## O que é *blockchain*

De acordo com Lyra (2018), ao se pensar no conceito de *blockchain*, é preciso, inicialmente, entender o conceito de centralização e descentralização no que tange às informações e às transações, principalmente quando se trata de valores, visto que o conceito de *blockchain* nasceu da ideia de descentralizar as transações realizadas.

Por exemplo, na compra de um veículo, você negocia o preço com o vendedor, e, depois, vocês vão a um cartório para "oficializar" o acordo que firmaram. Nesse caso, o cartório centraliza o papel de garantidor do processo,

ele é o acreditador de que ambos "falam" a verdade. Já no caso do *blockchain*, a ideia é exatamente o contrário disso, ou seja, acabar com a centralização.

O conceito de *blockchain* (ou cadeia de dados), da forma que se conhece, surgiu em 2008, de acordo com registros históricos. Representa, basicamente, uma forma de validar uma transação financeira ou um registro (LYRA, 2018). Foi desenvolvido para dar mais segurança às transações digitais, tendo em vista que ocorre sempre por meio de uso tecnológico da internet e de negociações *on-line* (RIBEIRO, 2017). O *blockchain* é a inovação que está por trás da moeda digital.

Apesar de o *blockchain* estar intrinsicamente ligado às criptomoedas, incluindo as principais delas — Bitcoin, a Litecoin ou Ethereum —, já se pode encontrar o seu uso em diversos setores e áreas, visto que já existem projetos com essa tecnologia para outros fins.

A Figura 1, a seguir, demonstra de forma básica como funciona o *blockchain* e sua estruturação. É importante destacar a forma como se constituem os blocos em cadeia (*blockchain*).

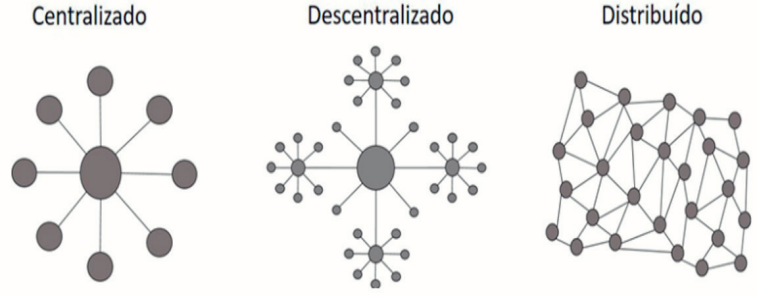


**Figura 1.** Centralização e descentralização proposta pelo *blockchain*.
*Fonte:* Adaptada de Lyra (2018).

## Principais elementos do *blockchain*

Antonopoulous (2014) esclarece os principais pontos que compõem o *blockchain*:

- **Nós**: o *blockchain*, na verdade, consiste em transações verificadas e validadas por cada ponto que recebe a transação realizada (*peer-to-*

*-peer*, ou ponto a ponto), em que cada nó da cadeia tem a função de validador da operação realizada pelos outros nós — daí vem o conceito de descentralização, discutido anteriormente.

- **Endereço ou chave privada**: idêntico a um *e-mail*, em que se pode mandar e receber blocos para outros componentes da cadeia — esse endereço é criptografado, único e individual.
- ***Token***: pode assumir vários papéis nessa transação eletrônica por meio de *blockchain*, tais como: votos, registros, atestados, utilitários, direitos de propriedade, etc.
- **Criptografia**: é o que torna o *blockchain* algo único, visto que cálculos matemáticos permitem que, a cada vez que é feita uma transação, a informação se torne uma nova chave, tornando impossível quebrar o código e descobrir a transação realizada.
- ***Timestamp***: um servidor de carimbo de tempo, que adiciona um carimbo com data e hora na transação realizada, e, a cada vez que recebe um carimbo de tempo, gera um histórico, formando uma corrente desses dados.
- **Bloco**: bloco é a definição dada a um conjunto de transações realizadas, carimbadas com carimbo de data e hora, adicionado à rede de blocos.

**Saiba mais**

O futuro do *blockchain*, como sua própria origem traz, será a descentralização, inclusive de tecnologias e de *players* que dominam e dominarão esse mercado. Veja, no *link* a seguir, um exemplo de empresa que vem se destacando em transações financeiras por meio do uso de *blockchain*.

**https://qrgo.page.link/AcqGL**

## Segurança

*Blockchain* nada mais é que um histórico das transações públicas que são compartilhadas por todos os usuários, gerando um histórico de registro das transações realizadas naquele nó, com o carimbo de registro de data e hora, que garante a segurança do que está sendo negociado.

Sendo assim, de acordo com Lyra (2018), dentro de um contexto de segurança em que o *blockchain* garante as suas operações, tem-se o seguinte fluxo:

1. Um nodo (nó – usuário) desbloqueia suas moedas virtuais (ou documentos e informações), criando um histórico de transação com o endereço do destinatário e o *token* da transação.
2. O sistema de *blockchain* verifica nos seus registros anteriores se quem está enviando a quantia realmente a possui de transações anteriores encriptadas, fazendo, então, a transação atual para o destino.
3. A transação chega ao bloco em formação, que valida as informações e efetiva a transação.
4. As transações aprovadas e encerradas são enviadas para o sistema, gerando um histórico daquilo que foi realizado, com o carimbo de data e hora de cada operação.
5. Após todos esses passos, a transação se encerra, e a quantia chega ao seu receptor de destino, informado no passo 1, gerando um histórico de valor que será analisado sempre que o detentor fizer uma nova transação.

O que tornou o *blockchain* muito mais famoso e talvez tenha sido o divisor de águas para essa tecnologia foi o *blockchain* 2.0, pois foi quando ele deixou de ser pensado apenas para moedas virtuais, passando a ser pensado para transações de informações e de dados.

Mas como funciona o *blockchain* 2.0 e por que ele é encarado como revolucionário? O *blockchain* 2.0 formou uma segunda camada no protocolo do *blockchain*, tornando-se revolucionário pelo fato de estar apto a trafegar e a garantir a segurança do que se trafega por ele, visto que a essência da segurança do *blockchain* (seja o 1.0 ou o 2.0) é a verificação *peer-to-peer* (ponto a ponto).

Devido a descentralizar as operações, sendo validado e verificado constantemente por todos que operam e se utilizam das transações, essa nova fase de criação de utilização do *blockchain* também teve como nome *smart contracts*, ou contratos inteligentes, em português, exatamente pela não existência da necessidade de um cartório ou de algum órgão governamental para garantir que o contrato é valido e será cumprido.

Mesmo que o comércio de moedas virtuais seja o melhor exemplo de *blockchain* (talvez o mais didático para o entendimento do seu funcionamento), não é o único, visto que, como mencionado, é constante a evolução e as novas aplicações dessa tecnologia visando a melhorar a segurança em operações de dados. Veja um exemplo de uso do *blockchain* a seguir.

**Exemplo**

Em uma reportagem da InforChannel (ZADAIN, 2019), tem-se a aplicação de *blockchain* na colheita. Segundo Marco Antônio Salvo, consultor Nacional da Sankhya (importante empresa de ERP para negócios), como existem as *fintechs* (nome dado a empresas que trabalham com finanças e são altamente tecnológicas) e muitas possibilidades de uso de *blockchain*, ele dá como exemplo o GPS e a colheitadeira, em que somente quando uma grande empresa disser que adotou a tecnologia é que os demais elos da cadeia também podem passar a utilizá-la.

Mas como essa tecnologia pode ser usada em colheitadeiras? Elas automaticamente fazem o mapeamento da área a ser colhida, enviam esses dados pela internet (assim como os registros de vendas de moedas), e estes são validados e registrados em blocos, onde recebem um carimbo de validação, que servirá para usos futuros.

## *Sidechain*

Os protocolos de *cryptocurrencies* serviram de base para a criação de novos protocolos de segurança para o tráfego de informações e mesmo banco de dados, sendo o mais utilizado atualmente o Omni, que possui como codinome *treechain* (cadeia de árvores) ou *sidechain*, como é mais conhecido. Mas o que é um *sidechain*?

Os entusiastas e utilizadores dos protocolos de *cryptocurrencies* acreditavam que, assim como a internet, os protocolos de segurança das criptomoedas e mesmo dos *smart contracts* seriam melhores se fossem divididos em camadas, em que cada camada serviria de segurança para a próxima, formando uma espécie de ecossistema de proteção entre as camadas subjacentes, bem como uma interdependência entre elas, que é o grande segredo do *blockchain*, sendo que cada camada necessitaria de novos *softwares* e protocolos que permitissem a adesão das camadas anteriores.

Nesse contexto de melhoria de segurança, surge, em 2014, a Ethereum, que é o contrário do *blockchain*, como base do Bitcoin. Tendo como principal diferença o fato de que, na plataforma de *blockchain* da Ethereum (tida como *opensource*), qualquer indivíduo ou empresa pode criar e manipular as camadas e suas atribuições, desde que aceitos pelos nodos que já estão estabelecidos, gerando uma descentralização sem precedentes na era dos *blockchain*.

Desse modo, apesar desse assunto ainda ser novo e atual, passa constantemente por modificações, a cada momento surgindo uma nova forma de utilizar o *blockchain* para novos negócios e para garantir a segurança de negócios que já operam. O *blockchain* pode ser considerado a tecnologia do futuro da segurança de informações e transações, uma vez que, por não ter necessidade de um terceiro garantidor, o próprio sistema, por meio dos seus blocos e de suas camadas, garante a segurança e a fidedignidade do processo como um todo.

**Saiba mais**

No *site* da Associação Brasileira de Lawtechs e Legaltechs, disponível por meio do *link* abaixo, é possível observar um pequeno histórico do *blockchain*, bem como o seu funcionamento no aumento de segurança em transações específicas com documentos. Lembre-se de que o *blockchain* nasceu como transação financeira, mas seu uso como segurança vai muito além disso.

**https://qrgo.page.link/McQCP**

## As moedas virtuais

Martini (2017) destaca que a aplicação mais famosa é o Bitcoin. O Bitcoin está intimamente ligado ao conceito de *blockchain*, uma vez que foi na criação da moeda em si que se propagou e disseminou o conhecimento mundial acerca dessa nova forma de criptografar e garantir a segurança das informações, o *blockchain*.

Então é correto associar Bitcoin e *blockchain*? Sim, é correto associar o Bitcoin ao *blockchain*, mas, ao contrário, a réplica já não se faz verdadeira, visto que o *blockchain* rompeu a ligação com moedas virtuais e começou a ser utilizado para vários tipos de transações, bem como em criação de banco de dados, devido à sua estrutura de funcionamento e à sua forma de garantir a segurança dos dados por meio de nós e blocos seguros e descentralizados.

O Bitcoin tem uma história interessante e uma evolução de preços surpreendente. Tudo começou em 2008, quando o seu criador, com o codinome de Satoshi Nakamoto, criou o conceito e a operacionalização do *peer-to-peer*

(ponto a ponto) com checagem e garantia descentralizada, tornando, assim, o Bitcoin a primeira moeda descentralizada.

Pelo fato de ter checagem pelos próprios usuários de ponto a ponto nas cadeias de *blockchain*, o Bitcoin não necessita da regulamentação de bancos e governos como as moedas tradicionais e, por consequência, não se delimita aos impostos e às taxas que são cobrados por essas entidades centralizadoras quando o assunto é moeda (MARTINI, 2017).

A forma de negociar Bitcoin e a certificação de segurança que o *blockchain* fornece podem ser observadas a seguir (MARTINI, 2017).

1. O **usuário A** envia uma quantidade de Bitcoin para o **usuário B**.
2. A transação integra um bloco dentro da rede.
3. O bloco é transmitido a cada membro da rede.
4. Os membros decidem que a transação é válida.
5. O bloco é acrescentado ao *blockchain* de forma irremediável e irrefutável, e transação se torna visível a todos.
6. O usuário B recebe os Bitcoins.

Por se tratar de uma moeda virtual, sua compra e venda devem ser feitas normalmente por meio da rede mundial de computadores, a Internet. Existem empresas (que nasceram após o surgimento do *blockchain* e das moedas virtuais) que fazem a comercialização dessas moedas, sendo necessário que o comprador crie uma carteira, para que se torne apto a fazer as transações que deseja. Essas empresas que comercializam a moeda com os indivíduos não possuem características de bancos ou de governos, como cerceadores e reguladores do sistema, apenas operam como *blockchain* maiores, responsáveis pelos blocos menores, que são os individuais.

Segundo Martini (2017), em um cenário em constante evolução, ainda inovador e desconhecido em vários aspectos, é importante que se saiba com quem está se negociando, pois o *blockchain* é seguro, mas talvez as pessoas por trás de empresas de fachada possam estar aplicando golpes, por isso a necessidade ainda de saber a fundo quais instituições estão sendo utilizadas para fazer suas transações, sejam financeiras ou mesmo de dados e informações.

Mas não somente de pontos positivos e alegrias vive a moeda virtual, segundo a UOL Economia (BITCOIN..., 2017, documento *on-line*), "No momento, o Bitcoin existe praticamente sem nenhuma regulação", e essa falta de regulação pode, de alguma forma, prejudicar a confiabilidade da moeda diante de mercados e consumidores. Outro ponto preocupante

citado é o fato de que essas moedas têm sido muito usadas na *deep web* (i.e., uma parte da *web* que não pode ser acessada por um navegador de internet normal), tornando-se malvistas, devido à destinação das suas negociações realizadas.

Outra preocupação é em relação à volatilidade da moeda, fato que fez com que a China e a Coreia do Sul barrassem o lançamento de novas moedas virtuais, visto que podem ser consideradas para usos especulativos. No entanto, o maior impacto que a moeda sentiu até o momento foi quando a autoridade financeira do Reino Unido comunicou a investidores que eles teriam a chance de perder dinheiro caso viessem a negociar com novas moedas virtuais de algumas empresas, processo este conhecido como *initial coin offerings* ou ICO (BITCOIN..., 2017).

***Link***

Por meio do *link* disponível a seguir, você terá acesso ao *site* do Mercado Bitcoin, que comercializa a moeda virtual Bitcoin, em que se pode observar o volume comercializado, além do valor que a moeda tem no momento e o histórico do valor, semelhante a como funciona o mercado na Bolsa de Valores.

**https://qrgo.page.link/v7VLL**

## Evolução do valor do Bitcoin

Em relação à evolução do valor de mercado do Bitcoin, pode-se destacar como grande ponto de ruptura e ascensão o ano de 2013, pois foi quando a população mundial tomou conhecimento do fenômeno Bitcoin. O Bitcoin acabou tendo um pico de supervalorização em 2018, mas em 2019 chegou aos menores patamares desde seu lançamento. Isto demonstra ainda uma característica de volatilidade desta moeda.

O desafio inicial para o Bitcoin (como moeda virtual) foi conquistar a confiança das pessoas e, depois, enfrentar o desafio (que, aliás, está sendo enfrentado até o momento) de conseguir não cair na teia da burocratização e das legislações dos países e dos bancos, que, em conjunto, acabam tentando proteger o sistema financeiro já existente e que opera por séculos.

Vale ressaltar que o Bitcoin não teve negociação inicialmente, sendo o primeiro registro de negociação de 2010, tendo, assim, tido como padrão

adotado o valor de US$ 0 para o ano de 2009. O que se repetiu no ano de 2010, em que o valor registrado foi de US$ 0,34, tendo apenas em 2012 e 2013 os primeiros relatos de aumento de preço considerável da moeda virtual, sendo registrado, ainda em 2013, o rompimento da barreira dos US$ 1.000.

Todavia, foi entre os anos de 2017 e 2019 que a moeda realmente deslanchou e acumulou ganhos muito altos e representativos, chegando, no ano de 2018, ao ápice de US$ 20.000, o que não se manteve, pois houve uma queda, chegando nos atuais US$ 12.000, que está longe de ser uma cotação ruim para quem saiu de 0, há cerca de 10 anos.

Mas a pergunta que fica é: como se determina o preço da moeda Bitcoin? Ao contrário das moedas "normais", que são regidas por governos e bancos centrais, não há preço oficial para o Bitcoin, o que parece estranho em um primeiro momento. O que se tem é o conjunto de várias médias baseadas em casas de câmbio globais que determinam o preço médio.

Existem dois índices que podem ser "tidos" como balizadores do preço, são eles: o Bitcoin Average e o CoinDesk. Entretanto, é normal que o Bitcoin seja vendido e comprado a um preço diferente da média nas casas de câmbio. Sendo assim, considera-se o preço da moeda pela média do valor de comercialização a nível mundial.

Com a mesma ideia da raridade do ouro, o Bitcoin foi criado por Satoshi Nakomoto com um suprimento fixo e imutável de 21 milhões de moedas. Com mais da metade desse valor já produzida, essa "falta" de moeda fará o preço aumentar cada dia mais, assim como acontece com o ouro. Várias pessoas foram sábias ou sortudas o suficiente para ganhar, comprar ou minerar Bitcoin antes que ele tivesse seu valor elevado. Por exemplo, acredita-se que o criador do Bitcoin, Satoshi Nakomoto, tenha em torno de um milhão de Bitcoins, ou 4,75% da oferta total (de 21 milhões). Se Satoshi soltar essas moedas no mercado, a oferta resultante faria o preço entrar em colapso. Apenas como curiosidade, desconsiderando a desvalorização oriunda dessa ação de Satoshi, e imaginando que ele venda suas 1 milhão de moedas a US$ 12.000, imagine a fortuna que ele teria.

## Exemplo

Na Figura 2, pode-se observar a evolução do valor de um Bitcoin ao longo dos anos, desde seu completo desconhecimento até os dias atuais. Pode-se constatar que, em 2018, ele teve um grande salto, seguido de uma queda, e atualmente está em ascensão novamente.

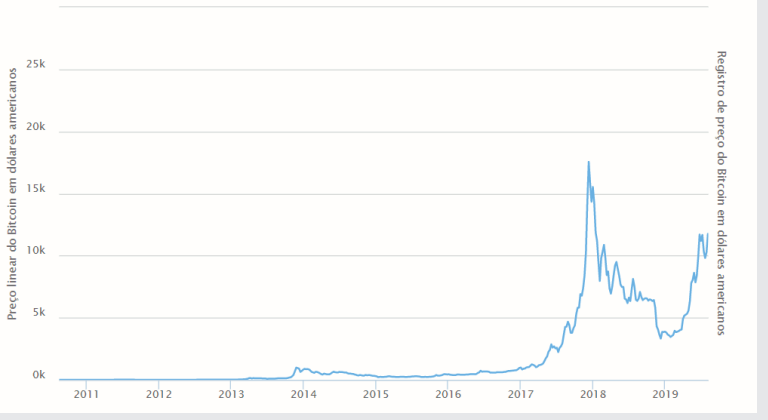


**Figura 2.** Gráfico do histórico de preço do Bitcoin.

***Fonte:*** Adaptado de Gráfico... (2019, documento *on-line*).

## Referências

ANTONOPOULOS, A. M. *Mastering Bitcoin*: unlocking digital cryptocurrencies. 1st ed. Sebastopol: O'Reilly Media, 2014.

BITCOIN: o que é e como funciona a moeda virtual. *UOL Economia*, 2017. Disponível em: https://economia.uol.com.br/noticias/bbc/2017/12/11/bitcoin-o-que-e-e-como--funciona-a-moeda-virtual.htm?cmpid=copiaecola. Acesso em: 13 ago. 2019.

GRÁFICO do histórico do preço do Bitcoin. *Buy Bitcoin Worldwide*, 2019. Disponível em: https://www.buybitcoinworldwide.com/pt-br/preco/. Acesso em: 13 ago. 2019.

LYRA, J. G. *Blockchain e organizações descentralizadas*. São Paulo: Brasport, 2018.

MARTINI, R. *Sociedade da informação*: para onde vamos. São Paulo: Trevisan Editora, 2017.

RIBEIRO, G. O que é Blockchain? *Techtudo*, 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/11/o-que-e-blockchain.ghtml. Acesso em: 13 ago. 2019.

ZADAIN, P. Colheita promissora. *Infor Channel*, 2019. Disponível em: http://inforchannel.hospedagemdesites.ws/magazine/2019/03/06/colheitapromissora/. Acesso em: 13 ago. 2019.

## Leitura recomendada

ASSAF NETO, A. *Mercado financeiro.* 14. ed. São Paulo: Atlas, 2018.

# Registro eletrônico

## Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Definir *blockchain*.
- Avaliar o uso da *blockchain* no âmbito dos cartórios e registros de imóveis.
- Explicar o que são registros eletrônicos e centrais eletrônicas.

## Introdução

O Poder Judiciário e as serventias extrajudiciais têm se somado à tecnologia para facilitar, desburocratizar, agilizar e trazer mais segurança e garantias à sociedade. Além do uso da inteligência artificial, por exemplo, surge também a possibilidade de inovação por meio da tecnologia *blockchain*, que representa maior tranquilidade em transações realizadas pela internet. Além disso, o próprio registro eletrônico — regulamentado pelo Provimento nº. 47, de 18 de junho de 2015, do Conselho Nacional de Justiça (CNJ), e implantado por todas as serventias brasileiras, por meio das centrais eletrônicas — demonstra grande avanço dos registros de imóveis quanto ao fornecimento e recebimento de documentos e prestação de informações.

Neste capítulo, você vai ler sobre a *blockchain*, bem como sobre a sua relação com os cartórios e o registro eletrônico previsto no Provimento nº. 47/2015 do CNJ.

## *Blockchain*

A *blockchain* é uma das maiores inovações desde o surgimento da internet. Como o nome já sugere, *blockchain* se trata de uma **cadeia de blocos**. Cada bloco dessa cadeia contém uma quantidade de informações. Cada bloco tem um *hash* (impressão digital de um dado), que garante que seja único, além de um *hash* do bloco anterior, que traz todo o histórico da movimentação. De acordo com Alves *et al.* ([201-], documento *on-line*): "*Blockchain* é uma tecnologia

que faz uso de uma arquitetura distribuída e descentralizada para registrar transações de maneira que um registro não possa ser alterado retroativamente, tornando este registro imutável".

Para Jeff Garzik (ALENCAR, 2016, documento *on-line*), o pioneiro do *bitcoin*, as "[...] *blockchains* são bancos de dados imutáveis e distribuídos. Eles são infraestrutura tecnológica". A *blockchain* é uma tecnologia de armazenamento de dados em uma rede, de forma criptografada e baseada em consenso (todos os pontos devem concordar que os dados são autênticos).

> De acordo com Ulrich (2014) e Lucena e Henriques (2016) originalmente o *blockchain* foi idealizado por um programador anônimo sob o pseudônimo de Satoshi Nakamoto, em 2009, como uma forma de resolver o problema do "gasto duplo", pois nas transações *on-line* sempre era necessário um terceiro para intermediá-las, mas para sua criptomoeda virtual, o *Bitcoin*, esse problema foi resolvido removendo a necessidade do intermediário (SILVA; BOVÉRIO, 2018, documento *on-line*).

A *blockchain* serve, primeiro, para a transferência de valores pela internet de forma confiável. A ideia da *blockchain* é que exista um livro-razão, público e aberto, para que todos consigam verificar as transações realizadas, se ocorridas de fato ou não. A tecnologia *blockchain* já é utilizada em vários contextos, sendo os principais:

- moedas digitais (criptomoedas, como o *bitcoin*);
- contratos inteligentes (*smartcontracts*);
- *softwares* (por exemplo, jogos de computador).

De acordo com Carvalho *et al.* (2017, documento *on-line*):

> O *blockchain* é uma inovação tecnológica de alcance bem mais amplo que as chamadas criptomoedas que nele se baseiam e tem potencial para transformar extensivamente os sistemas de pagamentos e o conjunto das práticas do sistema monetário e financeiro. O desdobramento mais conhecido são as criptomoedas, adjetivo que destaca a utilização de técnicas que permitem proteger dados transmitidos e armazenados de forma descentralizada.

Quando não há *blockchain*, os dados são inseridos por meio de vários computadores e ficam armazenados em uma base centralizada, por meio de uma entidade centralizadora. Por exemplo, no caso do sistema financeiro, a entidade centralizadora é o banco, que controla a transação com o dinheiro. Na *blockchain*, por outro lado, não há centralização. Há uma distribuição dos dados em toda a rede.

A Figura 1, utilizada por Ronan Damasco (2017 *apud* PRADO, 2017), diretor nacional de tecnologia da Microsoft, na sua palestra sobre *blockchain* na conferência Web.br 2017, ilustra o que é *blockchain*.

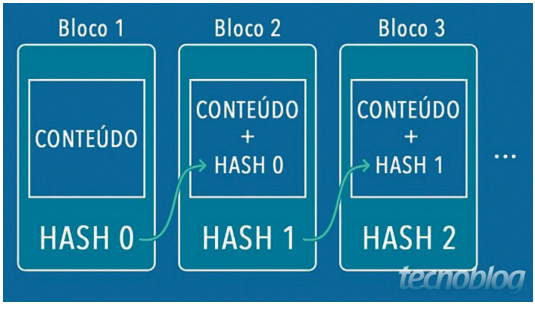


**Figura 1.** A *blockchain* é uma rede que funciona com blocos encadeados muito seguros que sempre carregam um conteúdo junto a uma impressão digital.

***Fonte:*** Prado (2017, documento *on-line*).

Esse formato (*blockchain*) traz segurança e torna muito difícil fraudar o sistema. Quanto mais a rede cresce, mais segura ela fica, já que mais se distribuem os dados.

### Exemplo

Um exemplo de uso da *blockchain*, além de criptomoedas, é o sistema Storj.io, que faz o armazenamento na nuvem de forma descentralizada. Enquanto Google Drive e Dropbox usam servidores para fazer o armazenamento, o Storj pega o arquivo e divide em centenas de pedaços criptografados, sendo que cada pedacinho fica armazenado em um computador diferente (que recebe uma recompensa para armazenamento), de forma que as pessoas não terão acesso a esse arquivo e, mesmo que o vissem, acessariam apenas um pedaço dele, não sendo possível acessá-lo como um todo. Apenas o dono, com o seu *login*, consegue acessar o referido arquivo por completo. Se algum computador for invadido, perderá apenas parte do arquivo; ou seja, será possível recuperá-lo por meio de outros pedaços salvos.

A promessa da *blockchain* por uma internet descentralizada é oferecer mais segurança, já que os *hackers* não terão um único servidor para atacar. Serão milhões de computadores ligados à *blockchain* armazenando esses dados; ou seja, não será possível derrubar tudo.

A *blockchain* é a grande revolução da tecnologia da informação, podendo ser comparada até mesmo ao surgimento da internet. Conforme Swan (2015), a *blockchain* foi fragmentada em três gerações distintas, de acordo com as atividades que essa inovação tecnológica pode desempenhar.

A primeira geração, chamada de ***blockchain* 1.0**, refere-se ao surgimento das moedas digitais, as criptomoedas, e às transações realizadas na internet: "[...] pode se tornar a Internet do Dinheiro conectando as finanças da mesma forma que a Internet das Coisas (IoT) conecta as máquinas" (SWAN, 2015, p. 5).

A segunda geração, chamada de ***blockchain* 2.0**, refere-se aos contratos inteligentes e às aplicações descentralizadas, como no caso da *Etherum* (ambiente que executa aplicações descentralizadas e aceita apenas sua própria moeda como forma de pagamento da transação — a *Ether*).

Para Swan (2015), a terceira geração, chamada de ***blockchain* 3.0**, refere-se ao uso da *blockchain* pelas ciências em geral, contemplando inclusive áreas governamentais.

A *blockchain* traz, como um dos seus principais pilares, a segurança, garantindo integridade, confidencialidade e disponibilidade à segurança dos computadores. Além disso, a *blockchain* tem como pilar fundamental a sua arquitetura descentralizada, distribuída de forma que os registros ficam armazenados em diversas máquinas, e não apenas em um único servidor. Ainda, a *blockchain* garante a integridade dos dados, já que, por ter a estrutura distribuída e encadeada em blocos, uma tentativa de alteração de um dado deve desencadear a estrutura de todos os blocos que contêm aquela informação.

Por fim, também é pilar fundamental da *blockchain* a imutabilidade, já que nenhum dado pode ser apagado ou alterado de seu bloco, em virtude da ordenação cronológica dos blocos, sendo considerado uma verdadeira linha do tempo de tudo que está nele registrado.

A tecnologia *blockchain*, em resumo, traz celeridade nas transações realizadas, mais transparência, substitui intermediários no mercado de compra e venda de ações e substitui livros-razões, seja no âmbito público ou privado. Além disso, como um fator extremamente importante, a *blockchain* consegue prevenir ciberataques, trazendo mais segurança às transações, podendo ainda ser usada para registro em nuvem, transparência a registros acadêmicos, administração e armazenamento de registros médicos, entre outros.

**Fique atento**

O ataque DDOS é o ataque de *hacker* com inúmeros acessos a um servidor ou *site*, fazendo com que tenha mais acessos do que de fato aguenta. O uso da *blockchain*, por se tratar de uma rede descentralizada e distribuída em blocos, consegue evitar esse ataque.

## *Blockchain* no âmbito dos cartórios e registros de imóveis

Os serviços notariais e registrais exercem uma verdadeira função social e, portanto, são de extrema importância à regulação e segurança da vida em sociedade, já que trazem consigo confiabilidade e são voltados para efetividade da segurança jurídica. Assim, os notários e registradores exercem um múnus público. O serviço prestado no Brasil, especificamente, tem elevado grau de organização e efetividade, motivo pelo qual serve de referência para outros países, com reconhecimento internacional pelo modelo utilizado.

**Saiba mais**

Nos termos do art. 236 da Constituição Federal, os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público. Assim, apesar do seu exercício se dar de forma particular, possui natureza pública, conforme já decidido por inúmeros tribunais, incluindo o Supremo Tribunal Federal (STF).

A atividade notarial e registral encontra-se presente em praticamente todos os atos da vida de um ser humano. Ao nascer, ao casar, ao comprar e vender, ao instituir empresa, ao cobrar dívidas e ao morrer.

Os cartórios são responsáveis pela desjudicialização de ações e desburocratização de problemas, tornando mais fácil e ágil o dia a dia da sociedade. Os notários e registradores, por sua vez, ao serem procurados pelo cidadão, prestam o serviço de forma eficiente, rápida, econômica e segura, o que confere ao usuário maior confiabilidade na resolução do seu problema. Em relação à tecnologia *blockchain*, por outro lado, não se pode negar que também traz

extrema eficiência, funcionando como um livro-razão, em que os registros podem ser arquivados seguramente.

Assim, o uso da *blockchain* pelos cartórios aumenta a segurança e efetividade já desenvolvidas e fornecidas pelos serviços notariais e registrais. No entanto, há uma discussão polêmica sobre a possibilidade de extinção dos cartórios com o uso e a ampliação da *blockchain*. Conforme Gonzaga (2017, documento *on-line*), "[...] esta tecnologia irá disruptir com o modelo que os cartórios atuam, pois ela age como um livro de contas digital, confiável, imutável, visível para todos os participantes, que mostra todos os elementos da transação de forma transparente e por um custo extremamente barato". Inclusive, uma empresa estrangeira, a Ubiquity, desde 2017, tem testado a tecnologia *blockchain* em dois cartórios de registro de imóveis no Brasil, nos municípios de Pelotas e Morro Redondo, no Rio Grande do Sul. Todavia, a *blockchain* veio para melhorar o serviço prestado pelos cartórios. Importante salientar que a *blockchain* não guarda documentos, pois quem guarda os documentos é o cartório.

Conforme previsto pela Corregedoria-Geral de Justiça (CGJ) do estado de Minas Gerais no art. 5º do Provimento nº. 260/2013/CGJ/MG, por exemplo, são princípios norteadores da atividade notarial e registral:

> Art. 5º O serviço, a função e a atividade notarial e de registro se norteiam pelos princípios específicos de cada natureza notarial e registral, além dos seguintes princípios gerais:
> I — da fé pública, a assegurar autenticidade dos atos emanados dos serviços notariais e de registro, gerando presunção relativa de validade;
> II — da publicidade, a assegurar o conhecimento de todos sobre o conteúdo dos registros e a garantir sua oponibilidade contra terceiros;
> III — da autenticidade, a estabelecer uma presunção relativa de verdade sobre o conteúdo do ato notarial ou registral;
> IV — da segurança, a conferir estabilidade às relações jurídicas e confiança no ato notarial ou registral;
> V — da eficácia dos atos, a assegurar a produção dos efeitos jurídicos decorrentes do ato notarial ou registral;
> VI — da oficialidade, a submeter a validade do ato notarial ou registral à condição de haver sido praticado por agente legitimamente investido na função;
> VII — da reserva de iniciativa, rogação ou instância, a definir o ato notarial ou registral como de iniciativa exclusiva do interessado, vedada a prática de atos de averbação e de registro de ofício, com exceção dos casos previstos em lei;
> VIII — da legalidade, a impor prévio exame da legalidade, validade e eficácia dos atos notariais ou registrais, a fim de obstar a lavratura ou registro de atos inválidos, ineficazes ou imperfeitos (MINAS GERAIS, 2013, documento *on-line*).

Dessa forma, por exemplo, a *blockchain* não consegue substituir a maioria desses princípios, como é o caso dos princípios da fé pública, da publicidade, da oficialidade e da legalidade. Se os cartórios fossem substituídos por *blockchain*, quem seria o responsável por fazer uma prévia análise do registro? Quem faria a qualificação de um título? Quem teria a fé pública para certificar o título apresentado como autêntico de boa-fé e válido? Com essas perguntas, chegamos à conclusão de que não haveria quem o fizesse.

Não se pode confundir fé pública com apenas a simples assinatura ou carimbo do registro dado pelo tabelião ou registrador. A fé pública vai muito além. A fé pública é concedida pelo Estado ao delegatário, não sendo um atributo transferível à *blockchain*. Por outro lado, não se pode esquecer que os cartórios trazem consigo o pilar da publicidade, tornando os registros oponíveis *erga omnes*, reconhecido por lei, sendo que tal qualidade não pertence à *blockchain*. Logo, se há registro perante a *blockchain*, mas não há perante o cartório, não se pode alegar o conhecimento de todos a respeito daquele registro.

Além disso, pelo princípio da oficialidade, a validade do ato notarial ou registral deve ser submetida à condição de haver sido praticado por agente legitimamente investido na função, o que também não pode ser substituído pela *blockchain*. Assim, vemos que a *blockchain* não vai substituir os registros de imóveis, mas vai somar-se a eles, trazendo melhorias na prestação de serviço ao cidadão. Em verdade, a segurança do cartório, somada à *blockchain*, é a ideia perfeita de segurança jurídica.

Hoje, inclusive, os cartórios de registro de imóveis já contam com o registro eletrônico, criado por meio do Provimento nº. 47/2015 do CNJ (BRASIL, 2015), que permite, entre outras atividades, a recepção e o envio de títulos em formato eletrônico para registro.

**Saiba mais**

Você conhece a *Notarchain*? No *site* a seguir, é possível autenticar documentos, vídeos e fotos na *blockchain* dos notários sem a necessidade de certificado digital.

**https://www.e-notariado.org.br/**

# Registros eletrônicos e centrais eletrônicas

A seguir, serão abordados os registros eletrônicos e as centrais eletrônicas.

## Registros eletrônicos

Em 2009, com o advento da Lei nº. 11.977, de 7 de julho, foi criado o registro eletrônico de imóveis (BRASIL, 2009). Nos termos do art. 37 do referido diploma legal, os serviços de registros públicos de que trata a Lei nº. 6.015, de 31 de dezembro de 1973, observados os prazos e as condições previstas em regulamento, deveriam instituir um sistema de registro eletrônico, de forma que (art. 39) os atos registrais praticados deveriam ser inseridos no sistema de registro eletrônico, no prazo de até 5 anos a contar da publicação da Lei nº. 11.977/2009, devendo atender aos requisitos da Infraestrutura de Chaves Públicas Brasileira (ICP) e à arquitetura de Padrões de Interoperabilidade de Governo Eletrônico (*e-Ping*).

A intenção da Lei nº. 11.977/2009 foi, com a criação do sistema de registro eletrônico de imóveis, facilitar as transações imobiliárias (BRASIL, 2009). Desde então, houve a expectativa de instalação do registro eletrônico no Brasil. Após, foi efetivamente instituído e regulamentado pela Corregedoria Nacional de Justiça, por meio do Provimento nº. 47/2015 do CNJ (BRASIL, 2015), o Sistema de Registro Eletrônico de Imóveis (SREI).

**Saiba mais**

Por meio do SREI, é possível proceder à visualização de matrículas, pesquisa eletrônica para localização de titularidade de imóveis, pedidos de certidões digitais de matrículas, entre outros serviços, sem ter que ir a um cartório, pelo menos na parte de registro.

A inovação do registro eletrônico permite ainda que os registros de imóveis acompanhem a evolução da tecnologia e reduzam o prazo médio para entrega dos documentos. A implantação do registro eletrônico envolveu diversas etapas, sendo a primeira consistente no intercâmbio de documentos e informações entre os cartórios, o Poder Judiciário, a Administração Pública e o público em geral.

Nos termos do art. 2º do Provimento nº. 47/2015 do CNJ, o sistema de registro eletrônico de imóveis deverá ser implantado e integrado por todos os oficiais de registro de imóveis de cada estado, do Distrito Federal e dos territórios, e compreende:

> Art. 2º [...]
> I — o intercâmbio de documentos eletrônicos e de informações entre os ofícios de registro de imóveis, o Poder Judiciário, a administração pública e o público em geral;
> II — a recepção e o envio de títulos em formato eletrônico;
> III — a expedição de certidões e a prestação de informações em formato eletrônico; e
> IV — a formação, nos cartórios competentes, de repositórios registrais eletrônicos para o acolhimento de dados e o armazenamento de documentos eletrônicos (BRASIL, 2015, documento *on-line*).

Além disso, o Provimento nº. 47/2015 do CNJ ainda prevê que os documentos eletrônicos apresentados aos ofícios de registro de imóveis, ou por eles expedidos, deverão ser assinados com uso de certificado digital, segundo a ICP, e observarão a arquitetura do *e-Ping*.

Com relação aos livros do registro de imóveis, estes continuarão a ser escriturados e mantidos segundo a Lei nº. 6.015/1973, sem prejuízo da escrituração eletrônica em repositórios registrais eletrônicos.

Por outro lado, nos termos do art. 7º do Provimento nº. 47/2015 do CNJ, os repositórios registrais eletrônicos receberão os dados relativos a todos os atos de registro e aos títulos e documentos que lhes serviram de base, de forma que — para a criação, atualização, manutenção e guarda permanente dos repositórios registrais eletrônicos — deverão ser observados:

> Art. 7º [...]
> I — a especificação técnica do modelo de sistema digital para implantação de sistemas de registro de imóveis eletrônico, segundo a Recomendação n. 14, de 2 de julho de 2014, da Corregedoria Nacional de Justiça;
> II — as Recomendações para Digitalização de Documentos Arquivísticos Permanentes de 2010, baixadas pelo Conselho Nacional de Arquivos — Conarq; e
> III — os atos normativos baixados pelas Corregedorias Gerais de Justiça dos Estados e do Distrito Federal e dos Territórios (BRASIL, 2015, documento *on-line*).

Por fim, os registros de imóveis não poderão (art. 8º do Provimento nº. 47/2015 do CNJ):

> Art. 8º [...]
> I — recepcionar ou expedir documentos eletrônicos por *e-mail* ou serviços postais ou de entrega;
> II — postar ou baixar (*download*) documentos eletrônicos e informações em *sites* que não sejam os das respectivas centrais de serviços eletrônicos compartilhados; e
> III — prestar os serviços eletrônicos referidos neste provimento, diretamente ou por terceiros, em concorrência com as centrais de serviços eletrônicos compartilhados, ou fora delas (BRASIL, 2015, documento *on-line*).

**Fique atento**

A inovação do registro eletrônico é um verdadeiro marco histórico, há muito tempo esperado. No aspecto técnico do cartório, o registro eletrônico possibilita trabalhar de forma mais ágil e com mais eficiência, conseguido oferecer rapidez e segurança jurídica nas transações imobiliárias. Para a sociedade, torna-se atendido o anseio de segurança e rapidez nas transações imobiliárias.

## Centrais eletrônicas

Com o intuito de operacionalizar o registro eletrônico, foram criadas as centrais eletrônicas de registro de imóveis. Estas deverão ser criadas em cada estado e no Distrito Federal. Elas terão o dever de proceder ao intercâmbio de documentos eletrônicos e de informações entre os ofícios de registro de imóveis, o Poder Judiciário, a Administração Pública e o público em geral.

Nos termos do art. 3º do Provimento nº. 47/2015 do CNJ, as centrais de serviços eletrônicos compartilhados serão criadas pelos respectivos oficiais de registro de imóveis, mediante ato normativo da CGJ local (BRASIL, 2015). Haverá uma única central de serviços eletrônicos compartilhados em cada um dos estados e no Distrito Federal.

Nos locais em que não forem possíveis ou convenientes a criação e a manutenção de serviços próprios, o tráfego eletrônico será feito mediante central de serviço eletrônico compartilhado que já esteja funcionando em outro estado ou

no Distrito Federal. As centrais de serviços eletrônicos compartilhados conterão indicadores somente para os ofícios de registro de imóveis que as integrem.

As centrais de serviços eletrônicos compartilhados vão coordenar-se para que se universalize o acesso ao tráfego eletrônico e se prestem os mesmos serviços em todo o País. Em todas as operações das centrais de serviços eletrônicos compartilhados, serão obrigatoriamente respeitados os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e, se houver, dos registros.

As centrais de serviços eletrônicos compartilhados deverão observar os padrões e requisitos de documentos, de conexão e de funcionamento da ICP e da arquitetura do *e-Ping*. Por meio das centrais, os pedidos serão enviados ao ofício de registro de imóveis competente, que será o único responsável pelo processamento e atendimento a respeito do registro eletrônico. Os oficiais de registro de imóveis deverão manter, em segurança e sob seu exclusivo controle, indefinida e permanentemente, os livros, classificadores, documentos e dados eletrônicos, respondendo por sua guarda e conservação.

As centrais, portanto, possibilitam o armazenamento, a concentração e a disponibilização de informações dos cartórios de registro de imóveis, por meio eletrônico e de forma integrada.

## Referências

ALENCAR, W. Blockchain: aplicado ao registro de imóveis. *In:* ENCONTRO DOS OFICIAIS DE REGISTRO DE IMÓVEIS DO BRASIL, 43., 2016, Salvador. [*Apresentação*]. Salvador: IRIB, 2016. Disponível em: https://irib.org.br/files/palestra/xliii-tema-07.pdf. Acesso em: 16 set. 2019.

ALVES, P. H. *et al.* Desmistificando Blockchain: conceitos e aplicações. *In:* MACIEL, C.; VITERBO, J. (org.). *Computação e sociedade*. Porto Alegre: Sociedade Brasileira de Computação, [201-]. Disponível em: http://www-di.inf.puc-rio.br/~kalinowski/publications/AlvesLNRLK19.pdf. Acesso em: 11 set. 2019.

BRASIL. Conselho Nacional de Justiça. Provimento nº. 47, de 18 de junho de 2015. Estabelece diretrizes gerais para o sistema de registro eletrônico de imóveis. *Diário da Justiça*, 19 jun. 2015. Disponível em: https://www.cnj.jus.br/busca-atos-adm?documento=2967. Acesso em: 11 set. 2019.

BRASIL. Lei nº. 11.977, de 7 de julho de 2009. Dispõe sobre o Programa Minha Casa, Minha Vida — PMCMV e a regularização fundiária de assentamentos localizados em áreas urbanas; altera o Decreto-Lei nº. 3.365, de 21 de junho de 1941, as Leis nº. 4.380, de 21 de agosto de 1964, nº. 6.015, de 31 de dezembro de 1973, nº. 8.036, de 11 de maio de 1990, e nº. 10.257, de 10 de julho de 2001, e a Medida Provisória nº. 2.197-43, de 24 de agosto de 2001; e dá outras providências. *Diário Oficial da União*, 8 jul. 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l11977.htm. Acesso em: 11 set. 2019.

CARVALHO, C. E. *et al*. Bitcoin, criptomoedas, blockchain: desafios analíticos, reação dos bancos, implicações regulatórias. *In:* FÓRUM LIBERDADE ECONÔMICA, 2017, Mackenzie. *Anais* [...]. São Paulo, 2017. Disponível em: https://www.mackenzie.br/fileadmin/OLD/62/ARQUIVOS/PUBLIC/SITES/ECONOMICA/2017/Carvalho__Pires__Artioli__Oliveira_-_Bitcoin__criptomoedas..._Encontro_Mackenzie.pdf. Acesso em: 11 set. 2019.

GONZAGA, L. Blockchain vs cartórios: como a tecnologia vai fortalecer o setor imobiliário. *StartSe*, 2017. Disponível em: https://startse.com/noticia/blockchain-vs-cartorios-como-tecnologia-vai-fortalecer-o-setor-imobiliario. Acesso em: 11 set. 2019.

MINAS GERAIS. Tribunal de Justiça do Estado de Minas Gerais. Provimento nº. 260/2013/CGJ/MG. Codifica os atos normativos da Corregedoria-Geral de Justiça do Estado de Minas Gerais relativos aos serviços notariais e de registro. *Diário da Justiça eletrônico*, 29 out. 2013. Disponível em: http://www8.tjmg.jus.br/institucional/at/pdf/cpr02602013.pdf. Acesso em: 11 set. 2019.

PRADO, J. O que é blockchain? [indo além do bitcoin]. *Tecnoblog*, 2017. Disponível em: https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin/. Acesso em: 11 set. 2019.

SILVA, V. A. F.; BOVÉRIO, M. A. Blockchain: uma tecnologia além da criptomoeda virtual. *Interface Tecnológica*, v. 15, n. 1, p. 109-212, 2018. Disponível em: https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/download/326/217/. Acesso em: 11 set. 2019.

SWAN, M. *Blockchain:* blueprint for a new economy. Sebastopol: O'Reilly Media, 2015.

# Introdução ao Direito digital

*Louise Heine*

**OBJETIVOS DE APRENDIZAGEM**

- Conceituar algoritmos, dados, inteligência artificial, *big data* e *blockchain*.
- Definir direito ao esquecimento e a posição do Supremo Tribunal Federal sobre o tema.
- Reconhecer o papel do compartilhamento internacional de dados e da respectiva cooperação entre países.

## Introdução

Há quem sustente que, atualmente, vivemos a Quarta Revolução Industrial, cuja pedra fundamental seria a inovação tecnológica. Como toda transformação disruptiva da sociedade, esta não pode ser ignorada pelas ciências jurídicas: é preciso entender como o Direito se relaciona com as inovações que vêm impactando a sociedade de uma forma geral, alterando, de maneira profunda, a vida humana, o Estado, a regulação e os direitos. Nesse contexto, o Direito Digital surge como um meio de adequar a realidade judicial e legislativa a essa nova realidade, sem abandonar princípios essenciais, como o da segurança jurídica.

Como a Era Digital avança em um ritmo mais rápido do que o ordenamento jurídico, surgem lacunas legais, que não abarcam os comportamentos e as relações oriundas da tecnologia. Até que o Estado se adapte, criando regras, a regulamentação existente e novas dinâmicas tendem a encontrar solução no Poder Judiciário. Diante da ausência de legislação específica, não é raro que o Poder Judiciário, sendo provocado, termine por legislar por meio de uma decisão.

No campo do Direito, portanto, as mudanças na sociedade, incluindo a nova realidade digital, devem ser analisadas para que as normas tradicionais possam sofrer as adaptações necessárias. Do mesmo modo, outras normas estão surgindo, diretamente relacionadas com o Direito Digital, e por isso é fundamental conhecer seus principais conceitos, desdobramentos e impactos na vida das pessoas, assunto do qual trataremos neste capítulo. Além disso, definiremos direito ao esquecimento, com destaque para o atual posicionamento do Supremo Tribunal Federal (STF) sobre o tema, e explicaremos o papel do compartilhamento internacional de dados.

## Conceitos fundamentais

Antes de mais nada, tratando-se de tecnologia da informação, é preciso definir alguns termos essenciais para entender como funcionam os sistemas e as máquinas. Para o Direito, essa conceituação é indispensável, pois os regramentos e as decisões judiciais deverão levar em consideração o significado de cada termo e a que se refere.

### Algoritmos

Os algoritmos são imprescindíveis para os sistemas digitais. Embora hoje sejam amplamente empregados na informática, o conceito surgiu de aplicações matemáticas. *Grosso modo*, caracterizam-se por conter, obrigatoriamente, uma norma estabelecida para um procedimento que, quando empregada, produzirá um resultado, passando por algumas etapas. Assim, os algoritmos formam uma sequência de atos lógicos, raciocínios, instruções, operações, todos ordenados para alcançar um objetivo, de modo que todas as etapas devem ser seguidas.

O algoritmo deve sempre ter claros seu objetivo e a finalidade para a qual se destina. Assim, quando as informações são fornecidas, o processamento delas segue um padrão de tratamento para fornecer um resultado. Com base nisso, é possível perceber que o algoritmo tem uma entrada (*input*) e uma saída (*output*) de informações, a exemplo das instruções do que e de como algo deve ser feito. Segundo Frazão (2018), os algoritmos têm sido utilizados para respostas de questões objetivas e, ainda, para decidir sobre questões subjetivas, complexas e que envolvem juízos sofisticados de valor, como estas: Quem deve ser contratado para trabalhar em uma empresa? Que contrato deve ser celebrado e em quais bases? Qual é a probabilidade de reincidência de determinado criminoso?

É pelo uso dos algoritmos que as máquinas conseguem aprender. Conforme vai recebendo mais informações, o algoritmo vai ficando mais complexo, mais especializado e mais capaz de englobar múltiplas situações. Assim, trabalha com códigos variáveis e comandos de repetição. Uma sequência de algoritmos pode formar um programa de computador ou a funcionalidade de um aplicativo.

### *Fique atento*

Os algoritmos impactam a forma como enxergamos o mundo, atuando sobre o comportamento humano ao influenciarem as escolhas. Segundo Hoffman-Riem (2019), muitas atividades cotidianas, sobretudo nosso consumo midiático, são influenciadas, de forma implícita, pelos algoritmos. Os algoritmos, para o autor, podem ser capazes de observar o comportamento humano, identificando os interesses com o intuito de prever necessidades e atitudes futuras. A isso, chamamos de **capacidade preditiva**.

O fato de os algoritmos terem a capacidade de ampliar seu espectro de atuação por meio dos dados que recebem não significa dizer que não falham. Podem ocorrer comportamentos imprevisíveis ou não éticos, com a discriminação algorítmica, como resultado da programação que foi feita. A discriminação algorítmica nem sempre acontece por um ato intencional. Ela consiste em categorizar pessoas por alguma característica identificada pela programação dos algoritmos e que pode não ser verdadeira.

## Dados

Os dados, em um conceito adequado à realidade digital, são as informações coletadas, inseridas e fornecidas para determinada finalidade. Atualmente, essas informações são valiosas e circulam mundialmente. São os dados que abastecem os algoritmos, de modo que a inclusão daqueles nos sistemas são os *inputs*, que receberão tratamento para chegar a uma resposta: o *output*.

Os dados são o principal ativo de boa parte das organizações e movem a economia digital, de modo que protegê-los de forma consistente é fundamental para a preservação do Estado Democrático de Direito e das liberdades públicas. Portanto, proteger os dados é uma forma de proteger os cidadãos e a sociedade. No Brasil, o Marco Civil Regulatório da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 [LGPD]) trazem previsões legais sobre como os dados devem ser tratados, direitos e obrigações das pessoas físicas e

jurídicas, consequências do descumprimento, obrigações e deveres do Poder Público, entre outras.

A LGPD brasileira foi inspirada na legislação da União Europeia, a GDPR ("General Data Protection Regulation"). Basicamente, a GDPR objetiva proteger o titular do dado pessoal, obrigando os serviços de coleta de dados a informar claramente que o fazem. No Brasil, o foco da LGPD também é a proteção de dados pessoais da pessoa natural, sejam eles sensíveis ou não. Nas palavras de Haikal e Pinheiro (2013), a proteção dos dados pessoais tem, como premissa, a defesa da privacidade. Com a privacidade assegurada de maneira apropriada, as liberdades individuais estarão protegidas.

### *Fique atento*

É importante esclarecer que a lei brasileira prevê as obrigações para quem detém os dados pessoais dos usuários em qualquer meio, estejam eles conectados ou não à internet, sejam físicos ou digitais. Além disso, é clara ao determinar que os dados pessoais a serem protegidos se referem à pessoa identificada ou identificável, ou seja, havendo, no cadastro, qualquer meio de determinar a identidade do usuário.

## Inteligência artificial

Inteligência artificial é uma tecnologia utilizada por sistemas, máquinas e computadores que simulam o pensamento humano para a tomada de decisões, o aprendizado e a execução de tarefas, no intuito de prever comportamentos e resultados, entre vários outras aplicabilidades, de forma autônoma. A inteligência artificial, então, abastecida com dados, funciona com a utilização de algoritmos, produzindo previsões. Algumas das decisões automatizadas, quando se referem a um indivíduo, são baseadas em métodos para a análise de grande volume de dados. Essas informações podem resultar em riscos ou ofensas aos direitos individuais, como autonomia, igualdade e personalidade.

Lyon (2003) refere que a sociedade, hoje, caracteriza-se pelas relações remotas, de modo que os dados pessoais se transformaram em uma forma de representação das pessoas, sendo determinantes para abrir ou fechar as portas de oportunidades e acessos. Nesse sentido, Doneda *et al.* (2018) atentam para o fato de que as decisões automatizadas também têm potencial para violar os direitos fundamentais, o que pode ser minimizado pelo cumprimento de determinados parâmetros éticos e legais que assegurem a transparência a respeito do uso das informações, bem como a correção e atualização das informações que servem como *input* do algoritmo.

### *Fique atento*

A inteligência artificial permite, à máquina, aprender, em um processo chamado de ***machine learning***. A partir do abastecimento com dados, seguindo os passos do algoritmo e treinos, a máquina é capaz de aprender, ampliar sua atividade e fornecer respostas às questões. Outro termo importante é ***deep learning***, que consiste na maneira de estruturação da inteligência artificial inspirada no funcionamento das redes neurais dos animais. Os circuitos de programação do algoritmo são feitos em camadas, variando a complexidade, os tipos de dados e o modo de tratamento para gerar a resposta.

## *Big data*

Muito se ouve falar sobre *big data*, uma das palavras do momento quando o assunto é tecnologia. O termo é utilizado para remeter a uma grande quantidade de dados, um conjunto que expressa uma coleção imensa de tipos de dados com qualidade diversificada, com fontes variadas e enorme capacidade de processamento rápido. Seu uso serve para diversos fins, tanto para entes privados quanto públicos. Segundo Hoffmann-Riem (2019), os dados não são coletados, acumulados, analisados e utilizados apenas no âmbito da economia privada, mas, também, em âmbito estatal. Porém, os dados pessoais também integram o *big data*, então a preocupação da LGPD é extensiva a ele.

### *Fique atento*

Hoffmann-Riem (2019) afirma que o significado de algoritmos para a seleção e o controle de comportamentos é impulsionado pela disponibilidade do *big data*, que, por sua vez, é uma consequência da algoritmização.

Conforme Laney (2001), são três as características do *big data*: volume, variedade e velocidade. Uma das possibilidades de utilização do *big data* é por meio da inteligência artificial, pois são empregados diferentes procedimentos analíticos para cada diferente finalidade, que é definida conforme o algoritmo programado. A inteligência artificial, então, é capaz de acessar informações do *big data* e processar para uma finalidade, conforme a programação do algoritmo.

## *Blockchain*

No ano de 2018, o Superior Tribunal de Justiça (STJ) analisou um caso considerado paradigma envolvendo instituição financeira. No voto, ao se manifestar, a Ministra Nancy Andrighi definiu que *blockchain* é um tipo de tecnologia que não depende de organização centralizada de dados para intermediar o armazenamento de dados e as operações digitais. Nas palavras de Porto, Lima Júnior e Silva (2019, p. 12), *blockchain* "[...] corresponde à base de armazenamento e registro de dados integralmente digital, na qual podem ser realizados negócios e operações financeiras por meio da codificação computacional".

Silva e Sousa (2019) mencionam que essa ferramenta foi desenvolvida para servir às áreas financeiras e empresariais, promovendo garantias, como a segurança jurídica, para os *smart contracts*. Funciona, portanto, como blocos de informações e transações regidos por um código, autoexecutável, que permite a execução de contratos e negociações. De fato, o *blockchain* foi criado para servir como suporte para a criação do Bitcoin, uma criptomoeda. É como se fosse um livro-registro cujos dados podem ser acessados por todos, permitindo a transação de valores sem uma instituição financeira como intermediária. Essa cadeia de dados é armazenada e reunida em blocos com uma função *hash*, que Narayanan *et al.* (2016) definem como a característica de imutabilidade, uma vez que os dados são armazenados e submetidos a uma função e, depois disso, não podem ser alterados.

Aqueles que utilizam a tecnologia do *blockchain* desempenham um papel importante, visto que podem monitorar o cumprimento e a execução dos termos codificados, mantendo o anonimato, o que fortalece a noção de segurança do sistema. O uso dessa tecnologia, assim, como enfatiza Lafarre e Elst (2018 *apud* PORTO; LIMA JÚNIOR; SILVA, 2019, p. 14), torna possível que haja a "[...] transparência e a confiabilidade das informações reunidas na rede sem a necessidade de uma instituição centralizadora para outorgar autorização e assumir a responsabilidade pela verificação da veracidade dos dados inseridos e das transações efetuadas". Porto, Lima Júnior e Silva (2019) comentam que essa tecnologia tem vasta possibilidades de aplicações, além da criptomoeda, como o registro de propriedades, comprovações de autoria e propriedade intelectual, contratos automatizados, remessas internacionais de valores, emissão de títulos privados, organizações descentralizadas autônomas, etc. O Governo do Brasil, por exemplo, utiliza essa tecnologia para autenticar documentos.

## Cidadania digital

Falar em cidadania é falar no exercício de direitos por parte dos indivíduos. Em uma sociedade, todos os indivíduos que têm direitos também têm deveres. Assim, surgem as noções de obrigações e responsabilidades. Quando se transporta isso para a área do Direito Digital, entendendo o indivíduo como um cidadão digital, na medida em que consome dados, fornece dados e tem acesso a eles o tempo todo por meio de informações, percebe-se o quão necessária é a observância aos princípios da privacidade, da intimidade e da liberdade de expressão. Todos esses direitos, como fundamentais, são capazes de limitar o outro quando extrapola, no caso concreto, seu bom uso, causando dano moral ou patrimonial. Surge, daí, o dever de indenizar.

A cidadania digital é conectada com a noção da ética e das boas práticas no ambiente digital. Com o crescente aumento das redes sociais, todos os indivíduos têm a possibilidade de se expressar, de opinar e de se manifestar sobre algum assunto. É o pleno exercício da liberdade de expressão. Todavia, não deve servir de justificativa para constranger o outro. A ética e a boa-fé objetiva devem prevalecer tanto nas relações pessoais quanto nas relações virtuais.

Outro aspecto a se considerar é a solução de conflitos pelos meios digitais. Isso ocorre tanto pelo acesso ao Poder Judiciário pelos meios digitais quanto por mediações e negociações feitas pela internet. Já existem, inclusive, serviços de mediação de conflitos por meio da internet. Seja qual for o meio, as pessoas cada vez mais estão praticando atos da vida cotidiana pela internet. Na esfera pública, os órgãos administrativos já divulgam, no ambiente virtual, seu portal da transparência, empresas privadas divulgam seus balancetes anuais, é possível declarar o imposto de renda pela internet, as notas fiscais já são eletrônicas, há serviços relativos à Previdência Social que apenas são prestados por meios digitais, etc. Enfim, há uma vasta utilização dos meios digitais pelas pessoas, de modo que dados pessoais são fornecidos a todo momento.

Para Doneda (2011), é fundamental que se reconheça a necessidade de proteção de dados como um direito autônomo e fundamental para a proteção da personalidade em prol das garantias constitucionais de igualdade, liberdade e dignidade da pessoa humana, proteção da intimidade e da vida privada. A cidadania digital é uma realidade e uma necessidade para otimizar a vida das pessoas e informar, de maneira transparente, dados do Poder Público, além de uma ferramenta de acesso a serviços e informações. Por meio de senhas e assinaturas digitais, é possível transitar, virtualmente,

pelos mais diversos setores, praticando os mais variados atos. Porém, não se deve esquecer de que, para que isso aconteça, dados pessoais são inseridos e circulam nesse ambiente. Nesse sentido, medidas protetivas sobre o tratamento e a finalidade desses dados devem ser cumpridas por todos, sejam entes privados ou públicos.

### *Fique atento*

Você já ouviu falar do termo ***fintech***? As *fintechs* são *startups* que usam a tecnologia aplicada ao mercado financeiro. Seus objetivos incluem aumentar a agilidade das transações financeiras e de investimentos, de forma segura, prática e totalmente digital.

## O direito ao esquecimento no Brasil

O direito ao esquecimento vem sendo discutido há algum tempo no Brasil. Em países da União Europeia, ele é reconhecido pelas Cortes desde 2014. Em decisão proferida sobre esse direito, foi decidido que o Google deveria, por si, avaliar cada pedido de retirada de notícias ou de informações sobre alguém, mediante requerimento, analisando se o conteúdo ofende algum direito do requerente ou se há um interesse público na manutenção da informação. Esse direito, portanto, consiste na possibilidade de requerer, judicialmente, a exclusão de um fato ocorrido no passado, de dados, notícias e qualquer divulgação em meio digital que cause dor ou constrangimento a uma pessoa. O exercício desse direito não tem relação com a veracidade ou não dos fatos, de modo que é possível pedir o esquecimento de quaisquer fatos, verdadeiros ou não.

### *Fique atento*

Na internet, as informações circulam de maneira muito rápida. Os motores de busca são capazes de identificar pessoas e apresentar notícias bastante antigas, de forma que é possível levantar a história pregressa de qualquer pessoa. Algumas informações, porém, podem estar desatualizadas, enquanto outras podem não ser apresentadas dentro do contexto. O que se deve ter em mente é que o direito ao esquecimento tem relação com a reputação, a honra, a privacidade e possíveis sentimentos negativos que a divulgação daquela informação pode fazer emergir. Em oposição a esse direito, estão o direito à informação e o conhecimento considerado de interesse público.

O direito ao esquecimento, por ter como motor motivador um fator subjetivo, é um direito personalíssimo. A Lei nº 12.965/2014, conhecida como "Marco Civil Regulatório da Internet", prevê a possibilidade de requerer a exclusão de informações sobre o usuário por ofensa a algum direito Brasil (2014). Essa exclusão, porém, refere à retirada de conteúdos considerados ilícitos, postados por terceiros, e deverá ser julgada por juízes de direito, afastando, dos provedores de internet, a discricionariedade pela retirada da informação. O Poder Judiciário deverá pesar, no caso, o direito à liberdade de expressão e à informação em oposição ao direito de privacidade. Não deixa de ser, então, um embate entre direitos fundamentais. Moreira (2016) aponta que o um não anula o outro, mas eles impõem, ao intérprete, a composição dos conflitos de interesses para determinar os limites concretos aos princípios em choque.

A existência do direito ao esquecimento foi reconhecida e aplicada no Brasil antes do surgimento de uma legislação específica, por meio do Enunciado 531 (aprovado durante a VI Jornada de Direito Civil, em 2013), o qual prevê que "A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento" (BRASIL, [2013], documento *on-line*). Atualmente, no Brasil, além de na Constituição Federal, o direito ao esquecimento encontra respaldo legal no Marco Civil da Internet, no Código de Defesa do Consumidor, na Lei de Cadastro Positivo, na Lei de Acesso à Informação e na LGPD. Moreira (2016) afirma que, nesse contexto, a LGPD desponta como um novo e importante arsenal para contribuir com a efetividade da proteção aos direitos da personalidade garantidos na Carta Magna.

O direito ao esquecimento como um direito fundamental associado à dignidade da pessoa humana e à inviolabilidade pessoal, ao encontro do que preveem os arts. 1º, III, e 5º, X, da Constituição Federal (BRASIL, [2020a]). Esse direito, em que pese não seja considerado como fundamental pelo ordenamento jurídico, tem vínculo íntimo com cláusulas pétreas. Os autores justificam essa posição pela observação do que ocorre no Direito Penal, quando um indivíduo que passa por um processo, tendo ou não condenação, não deve ter seu registro informacional permanente usado contra ele para evitar que ocorra uma condenação perene por fatos do passado.

Para Sarlet (2015), é possível existir um direito fundamental implícito, como seria o caso do direito ao esquecimento. Em outros termos, esse reconhecimento na categoria de direito fundamental pode ser deduzido de direitos expressos, como, por exemplo, os direitos da personalidade. Segundo o autor, na cláusula geral de proteção e promoção da personalidade,

é possível contemplar a proteção que levaria ao reconhecimento do direito ao esquecimento como um direito fundamental.

Nesse contexto, importa mencionar que os ministros do STJ já reconheceram o direito ao esquecimento com fundamento nos direitos de personalidade. Seria, por isso, um direito considerado privado, com forte componente subjetivo. Quando há casos de conflitos entre direitos fundamentais, eles devem ser resolvidos utilizando o sopesamento ou o balanceamento para atingir um equilíbrio.

## O entendimento do Supremo Tribunal Federal

No Brasil, já foram julgados alguns casos de direito ao esquecimento. Alguns reconhecidos, outros não. Em fevereiro de 2021, o STF (2021, documento *on-line*), julgando caso que considerou de repercussão geral, firmou o seguinte entendimento:

> É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social — analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível.

Por maioria dos votos, foi negado provimento ao Recurso Extraordinário 1010606, Brasil (2016), com repercussão geral reconhecida, do famoso caso Aída Curi, vítima de um homicídio célebre nos anos 1950, ocorrido em Copacabana, no Rio de Janeiro. Os familiares da vítima solicitaram o direito ao esquecimento, alegando grande sofrimento com a divulgação e a veiculação de uma reconstituição do caso, que foi ao ar em 2004, no programa "Linha Direta", da TV Globo, sem sua autorização. Nesse conflito de direitos, foi argumentado que o caso era considerado de domínio e interesse públicos, fazendo parte da história da cidade e sendo, assim, de conhecimento geral. A exibição do episódio em rede nacional e a veiculação pela internet, no entendimento dos Ministros, não deveria ser excluída, pois ofenderia a liberdade de expressão e o direito à informação.

Tal decisão do STF pode ser entendida como na contramão das tendências mundiais. Isso porque, no mundo atual do fluxo de informações, há uma tendência cada vez maior à proteção de dados e informações individuais. Ainda que haja muito espaço para discussões sobre os direitos envolvidos, pela fixação da tese acima, a tendência é que o posicionamento do STF seja adotado pelo Judiciário brasileiro nos demais casos que versarem sobre o tema.

### *Saiba mais*

Em 1958, Aída Jacob Curi foi vítima de violência seguida de morte pelas mãos de três jovens, que, por fim, a atiraram do alto de um edifício na Av. Atlântica, em Copacabana, no Rio de Janeiro. Ronaldo Guilherme de Souza, o principal dos acusados, foi submetido a três julgamentos, tendo sido condenado à pena de oito anos e nove meses de reclusão por homicídio e tentativa de estupro.

## O compartilhamento internacional de dados e a cooperação entre países

A LGPD trouxe uma nova perspectiva sobre o compartilhamento de dados entre países. Nos termos da Lei, o titular dos dados é a pessoa natural identificada ou identificável por eles (BRASIL, [2020b]). Os dados e, por consequência, a pessoa merecem proteção, uma vez que a circulação de informações nos meios digitais nem sempre consegue dar segurança sobre a destinação e o tratamento dos dados.

A Lei também faz uma distinção sobre os dados considerados sensíveis, que são aqueles que carregam informações sobre "[...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, [2020b], documento *on-line*). Todos esses dados, sensíveis ou não, merecem proteção e são objeto da Lei, ainda que a coleta não tenha sido feita de maneira *on-line*. Isso amplia o leque de proteção, incluindo qualquer cadastramento em meio físico do titular dos dados que serão tratados. Por "tratamento de dados", a Lei estabelece que é todo e qualquer tipo de manipulação realizada com informações pessoais, seja a coleta, a reprodução, o acesso, o armazenamento ou a distribuição. O titular tem o direito a receber todas essas informações de quem coleta os dados, podendo, ainda, solicitar sua exclusão da base de dados ou a correção de dados incompletos ou errados.

Sobre o tratamento de dados pessoais de crianças e adolescentes, refere o art. 14, Brasil ([2020b], documento *on-line*):

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Daí se tira que a legislação teve especial cuidado ao tutelar os dados de menores, observando as disposições do Estatuto da Criança e do Adolescente. Nota-se que os dados pessoais, sendo de menores ou não, observam a exigência de um consentimento do titular ou pessoa responsável. Essas exigências são impostas tanto ao Poder Público quanto às pessoas de direito privado. A exceção, porém, é que o Poder Público pode tratar dados pessoais sem pedir o consentimento do titular sempre que for necessário para a execução de políticas públicas. Além disso, pela LGPD ([2020b], documento *on-line*), poderá tratá-los de maneira diferente em casos excepcionais, como nos casos de:

> [...] segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, que serão tratados de acordo com legislação específica, que contenha medidas proporcionais e necessárias para que o tratamento de dados pessoais atenda ao interesse público.

É possível, com essa previsão legal, que os Poderes públicos compartilhem, entre si, os dados pessoais.

No Capítulo V da referida Lei, são estabelecidos os requisitos e a possibilidade para a transferência internacional de dados, que apenas é permitida aos países ou organismos que tenham um grau de proteção de dados pessoais compatíveis com o que a Lei brasileira prevê. São estabelecidas, também, as formas como o controlador pode garantir o cumprimento das garantias e dos princípios a que o titular dos dados tem direito, conforme o inciso II do art. 33: "[...] a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos" (BRASIL, [2020b], documento *on-line*). Portanto, pode-se entender que as pessoas jurídicas de direito público poderão requerer que a Autoridade Nacional de Proteção de Dados (ANPD) avalie o nível de proteção de dados pessoais conferido por país ou organismo internacional para possibilitar o correto envio de dados. É o controlador quem deve garantir esse envio dentro da legalidade.

O art. 33 traz, conforme a LGPD, Brasil ([2020b], documento *on-line),* ainda, o seguinte:

> [...] II — quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV — quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V — quando a autoridade nacional autorizar a transferência;
> VI — quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII — quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> VIII — quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
> IX — quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Mais uma vez, é importante chamar a atenção para o consentimento do titular, de forma livre, informada e inequívoca para uma finalidade determi-

nada. Ou seja, o consentimento não pode conter qualquer tipo de coerção, devendo, o titular, também ser informado sobre a possibilidade de negar essa autorização e as possíveis consequências da negativa. A finalidade sempre deve ser clara e, havendo mais de uma, devem ser explanadas em separado, com as devidas aceitações.

Considerando que a transferência internacional de dados pode ser discutida internacionalmente, para que seja legal, em um contrato, deve respeitar os termos da Lei nº 9.307, de 23 de dezembro de 1996, conhecida como a "Lei da Arbitragem". Isso garantiria o processo probatório, evitando qualquer possibilidade de cerceamento de defesa. A LGPD tem, como princípio, a promoção de garantias e mecanismos protetivos aos direitos dos titulares; por isso, se um país ou organismo receptor dos dados transferidos não demonstrar o mesmo nivelamento de proteção, serão colocados em risco direitos e liberdades fundamentais legalmente protegidas no Brasil. O *Guia de Boas Práticas da LGPD,* Advocacia-Geral da União (2020), esclarece o art. 34 da LGPD, afirmando que o nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado será avaliado pela ANPD, que levará em consideração:

- as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
- a natureza dos dados;
- a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD;
- a adoção de medidas de segurança previstas em regulamento;
- a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais;
- outras circunstâncias específicas relativas à transferência.

O Brasil ainda não reconheceu qualquer outro país como tendo o desejado nível de proteção. Da mesma forma, também não teve esse reconhecimento por parte de autoridades estrangeiras. Assim, a transferência internacional de dados deve ser avaliada caso a caso, possibilitando a autorização ou a medida compensatória a ser adotada.

### *Exemplo*

O WhatsApp foi comprado pelo Facebook em 2014. No início de 2021, usuários começaram a ser notificados que haveria compartilhamento de dados entre essas duas plataformas. Isso levaria a uma alteração nos termos de uso do aplicativo, de modo que o usuário seria obrigado a concordar para continuar utilizando as funcionalidades. De uma forma geral, as reações foram negativas, e houve uma migração em massa para outros aplicativos de troca de mensagens. Isso fez com que as modificações não fossem implementadas. A Alemanha, por exemplo, declarou que essa integração é ilegal, ferindo a GDPR.

## Referências


ADVOCACIA GERAL DA UNIÃO. *Guia de boas práticas*: Lei Geral de Proteção de Dados (LGPD). Brasília: Advocacia Geral da União, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 29 abr. 2021.

BRASIL. Conselho da Justiça Federal. *Enunciado 531*. A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. VI Jornada de Direito Civil. Coordenador-Geral: Ministro Ruy Rosado de Aguiar. Brasília: Conselho da Justiça Federal, [2013]. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/142. Acesso em: 28 abr. 2021.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília: Presidência da República, [2020a]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, [2017]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2020b]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 abr. 2021.

BRASIL. Ministério da Economia. *Guia de elaboração de inventário de dados pessoais*: Lei Geral de Proteção de Dados Pessoais. Brasília: Ministério da Economia, 2020c. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf. Acesso em: 28 abr. 2021.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário RE 1010606/RJ*. Direito Civil. Responsabilidade Civil. Indenização por Dano Material. Direito de Imagem. Recorrido: Globo Comunicação e Participações S/A. Recorrente: Nelson Curi e outro(a/s). Relator: Ministro Dias Toffoli, 14 de novembro de 2016. Disponível em: http://www.stf.jus.br/portal/processo/verProcessoDetalhe.asp?incidente=5091603. Acesso em: 29 abr. 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico*, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 28 abr. 2021.

DONEDA, D. C. M. *et al*. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar: Revista de Ciências Jurídicas*, v. 23, n. 4, p. 1-17, 2018. Disponível em: https://doi.org/10.5020/2317-2150.2018.8257. Acesso em: 28 abr. 2021.

FRAZÃO, A. Dados, estatísticas e algoritmos. *Jota*, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017. Acesso em: 28 abr. 2021.

HOFFMANN-RIEM, W. Controle do comportamento por meio de algoritmos: um desafio para o Direito. *Revista Direito Público*, v. 16, p. 123-162, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3647. Acesso em: 28 abr. 2021.

LANEY, D. Gerenciamento de dados 3-D: controle de volume, velocidade e variedade de dados META Group Inc. *Gartner*, 2001.

LYON, D. (ed.). *Surveillance as social sorting*: privacy, risk, and digital discrimination. New York: Routledge, 2003.

MOREIRA, P. B. Direito ao esquecimento. *Revista de Direito*, v. 7, n. 2, p. 293-317, 2016. Disponível em: https://periodicos.ufv.br/revistadir/article/view/1572. Acesso em: 28 abr. 2021.

NARAYANAN, A. *et al*. *Bitcoin and cryptocurrency technologies*: a comprehensive introduction. Princeton: Princeton University Press, 2016.

PINHEIRO, P. P.; HAIKAL, V. A. A nova lei de crimes digitais. *Gazeta do Povo*, 2013. Disponível em: https://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy/. Acesso em: 28 abr. 2021.

PORTO, A. M.; LIMA JÚNIOR, J. M.; SILVA, G. B. Tecnologia Blockchain e Direito Societário: aplicações práticas e desafios para a regulação. *Revista de Informação Legislativa*, v. 56, n. 223, p. 11-30, 2019. Disponível em: https://www12.senado.leg.br/ril/edicoes/56/223/ril_v56_n223_p11.pdf/view. Acesso em: 28 abr. 2021.

SARLET, I. W. *Dignidade (da pessoa) humana e os direitos fundamentais na Constituição Federal de 1988*. 10. ed. Porto Alegre: Livraria do Advogado, 2015.

SILVA, A. R. S. S.; SOUSA, I. P. Blockchain e smart contracts: os impactos das novas tecnologias no direito. *Revista Brasileira de Direito e Gestão Pública*, v. 7, n. 5, p. 53-66, 2019. Disponível em: https://editoraverde.org/gvaa.com.br/revista/index.php/RDGP/article/view/7341. Acesso em: 28 abr. 2021.

SUPREMO TRIBUNAL FEDERAL. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. *Supremo Tribunal Federal*, 2021. Disponível em: http://stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=460414. Acesso em: 29 abr. 2021.

## Leituras recomendadas

FERNANDES, R. V. C.; COSTA, H. A.; CARVALHO, A. G. P. (coord.). *Tecnologia jurídica e direito digital*: I Congresso Internacional de Direito e Tecnologia — 2017. Belo Horizonte: Fórum, 2018.

MARTINI, S. R.; BERGSTEIN, L. G. Aproximações entre o direito ao esquecimento e a lei geral de proteção de dados pessoais (LGPD). *Revista Científica Disruptiva*, v. 1, n. 1, p. 160-176, 2019. Disponível em: http://revista.cers.com.br/ojs/index.php/revista/article/view/14. Acesso em: 28 abr. 2021.

NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. *Bitcoin*, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 28 abr. 2021.

NUNES, D. H.; LEHFELD, L. S. Cidadania digital: direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro. *Libertas: Revista de Pesquisa em Direito da UFOP*, v. 4, n. 2, p. 1-12, 2018. Disponível em: https://periodicos.ufop.br:8082/pp/index.php/libertas/article/view/1300. Acesso em: 28 abr. 2021.

### *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

# Tributação 4.0

*Louise Silveira Heine*

**OBJETIVOS DE APRENDIZAGEM**

- Reconhecer os desafios da tributação e dos serviços ligados às novas tecnologias.
- Analisar a possibilidade de tributação das criptomoedas.
- Definir *software* e a sua tributação.

## Introdução

O Estado é uma entidade soberana no que diz respeito à tributação. No ordenamento jurídico brasileiro, é a Constituição Federal que estabelece a competência tributária entre União, estados, municípios e Distrito Federal. O Código Tributário Nacional (CTN) é anterior à Constituição Federal de 1988, mas é vigente porque foi recepcionado por ela, ou seja, suas normas foram consideradas de acordo. Além desse código, há outros regramentos infraconstitucionais, e todos devem estar de acordo com a Carta Magna em forma e conteúdo, em todos os níveis do poder público. As normas estabelecem, além de critérios práticos para a tributação por meio das normas, princípios que devem ser respeitados, formando um sistema tributário que deve ser observado pelo contribuinte e pelo Estado.

Pela definição do art. 3º do CTN (BRASIL, 1966), o tributo é uma prestação pecuniária compulsória, ou seja, o pagamento é obrigatório, quando exigido, e em moeda, o que significa que deve ter valor certo, que não seja uma sanção a um ato ilícito, como uma multa, por exemplo. Além disso, é instituído por lei e cobrado administrativamente pelo poder público, de modo que só pode ser exigido mediante norma prévia e pelo órgão competente. Quando se fala em tributo, é mais comum que se pense em imposto; porém, ele se trata de apenas uma das espécies tributárias. Dentro da relação tributária, há o sujeito passivo, que deverá

pagar a obrigação (o contribuinte), o sujeito ativo, a quem se deve pagar o tributo, e o fato gerador, que é aquilo que acontece no mundo que causa a incidência da norma tributária, fazendo surgir a obrigação.

Analisando a sociedade atual, é possível identificar uma série de novas relações digitais e virtuais, passíveis de serem configuradas como fato gerador de tributo, e é sobre isso que falaremos neste capítulo. De fato, a legislação evolui de maneira lenta, e o processo legislativo brasileiro não consegue acompanhar a inovação. A tributação 4.0 surge, então, para abarcar as novas espécies tributárias presentes nas transações comerciais de todo o mundo. Novas formas de monetizar projetos, empresas e transações são próprias das novas tecnologias, e surgem novos modelos econômicos ligados ao ambiente tecnológico e digital em tudo que se refere a produtos, serviços e geração de renda. Nesse panorama, é necessário reconhecer e debater, como faremos aqui, os desafios que o Direito Tributário encontra ao se deparar com as novas formas de prestação de serviços que se relacionam às tecnologias. Isso implica gerar possíveis soluções para conflitos e impasses. Entre essas inovações, as criptomoedas têm destaque, pois são uma maneira recente de movimentar valores sem que seja necessária a intermediação de um banco. Outra questão que merece atenção e que será discutida a seguir é a tributação de *softwares*, visto que a maneira como são comercializados vem se alterando ao longo do tempo.

## Os desafios da tributação frente às novas tecnologias

A sociedade tem sido constantemente transformada pela tecnologia, de modo que maneira como as pessoas se relacionam e a maneira como são contratados os serviços e adquiridos os produtos também estão tomando novos rumos. Grande parte dos estabelecimentos comerciais não tem mais um local físico para o atendimento dos clientes. É possível que uma empresa escolha a sede jurídica, ou seja, o endereço oficial, conforme for mais favorável à carga tributária e, de qualquer lugar, comercialize seus produtos para o mundo. A economia digital pode acontecer de forma remota e atuar sem limites territoriais físicos.

Vieira e Mourão (2013) entendem que o Brasil não tem como passar ileso ao que chamam de "paradigma informacional", ou seja, a sociedade está caminhando para uma mudança, na qual a conexão virtual se torna cada vez mais presente. A legislação tributária precisa conhecer as relações referentes aos serviços das novas tecnologias para que se aplique a elas. Nesse

sentido, Pinheiro (2010) considera polêmica a vinculação dos tributos ao fato gerador acontecido no mundo virtual. Em que pese se assemelhe ou até se iguale aos fatos geradores das relações não virtuais, um dos desafios consiste em determinar quem são os sujeitos da obrigação tributária: quem é competente para tributar, a quem se deve pagar. Quando se fala em serviços digitais (aplicativos como *streaming*, carros compartilhados, hospedagem, etc.), deve haver uma norma tributária que defina o que tributar e qual tipo de tributo aplicar, bem como casos de isenção, imunidade ou até possíveis compensações.

É nesse cenário que a tributação vem enfrentando seus desafios. Lembre-se de que, para que um tributo seja devido, uma norma o deve ter definido anteriormente. Instituir um tributo, como assevera Machado (2013), vai além de uma instituição. São necessárias análises, formulação de hipótese de incidência, sujeitos, base de cálculo, alíquota, valor, tudo isso vinculado ao princípio da legalidade. A inovação tecnológica não pode ser ignorada pelo Direito Digital e seu ponto de congruência com a esfera tributária. Por sua vez, os institutos jurídicos, para viabilizar a tributação da inovação e da tecnologia, obrigatoriamente precisam observar os princípios basilares do Direto, principalmente os da isonomia e da legalidade para a atuação do Estado.

Observa-se que o rápido avanço digital, que origina novas maneiras de circulação de bens e relações de trabalho até então inexistentes e que conferiu, à informação, uma característica de bem intangível circulante com alto valor, deixou o Direito Tributário, como era conhecido, obsoleto. Isso se dá tanto na política fazendária quanto na política tributária, fazendo surgir uma lacuna jurídica. Correia Neto, Afonso e Fuck (2019) asseveram que, enquanto perdurar o descompasso entre a "nova economia" e os "velhos tributos", as empresas de tecnologia e de comércio eletrônico terão larga vantagem em detrimento de seus concorrentes tradicionais. O cenário fiscal favorece o crescimento desse segmento econômico. As lacunas legais são propícias, em especial se forem analisadas as questões tributárias, porque não se estabeleceu, ao certo, o que esses fatos geradores devem recolher aos cofres públicos e quem deve receber. Essa realidade não é verificada apenas no Brasil, mas em diversos países e organismos internacionais, onde a tributação dos negócios digitais vem sendo discutida.

### *Saiba mais*

Uma **lacuna jurídica** surge quando não existe uma lei específica perfeitamente aplicável ao caso, e o operador do Direito precisa, então, utilizar técnicas para adequar a legislação vigente ao fato.

Há, porém, certos cuidados que devem ser observados. Domingues (2020) chama a atenção para o possível risco de regular alguns temas sem amadurecer a ideia por meio de discussão no âmbito do Poder Legislativo e da sociedade civil. O autor enfatiza que normatizar comportamentos, inclusive pela imposição de sanções por seu descumprimento, exige debate e tempo, sob pena de piorar a sensação de insegurança jurídica. A ausência de norma específica, todavia, tem levado, ao Poder Judiciário, as questões relativas a contratos eletrônicos, propriedade industrial, tributação de aplicativos e *softwares*, operações societárias, transferência de tecnologia, transações financeiras incluindo criptomoedas e suas operações, obtenção e uso de informações pessoais, delitos informáticos, relações de trabalho e outras referentes à indústria digital.

Muito se tem falado sobre a indústria 4.0 e uma quarta revolução industrial, e Schwab (2016), o fundador do Fórum Econômico Mundial, apresenta três razões para sua tese de que está em andamento uma quarta e distinta revolução industrial:

1. a velocidade, que é percebida de maneira exponencial, não linear;
2. a amplitude e a profundidade, porque se trata da combinação de várias tecnologias que estão mudando paradigmas na economia, nos negócios, na sociedade e individualmente;
3. o impacto sistêmico, visto que altera todos os sistemas dentro da sociedade.

Para Schwab (2016), os dados e as informações têm um papel fundamental nessa nova realidade de tecnologia que está assumindo a principal característica da atual sociedade, que já é chamada de "sociedade 4.0", ultrapassando a indústria 4.0. Basta observar as inovações que surgiram com o *big data*, a internet das coisas, o uso da inteligência artificial e outras implicações que, em pouco tempo, tornaram-se triviais.

No âmbito do Direito Tributário, a aplicação das normas tem sido um desafio. Em outros tempos, o sistema tributário do Brasil detinha um alto índice de eficiência arrecadatória, mas dados demonstram que a carga tributária global brasileira, atualmente, recuou para menos de 33% do produto interno

bruto. Esse é um dos sinais de problema estrutural no sistema tributário. É notório que a inovação tecnológica traz impactos ao cenário econômico e faz caducar algumas propostas anteriores. Diante da nova economia e dos novos modelos do mercado de trabalho, a realidade tem superado as formas jurídicas.

Para planejar um sistema tributário eficiente e adaptado às novas tecnologias, é preciso elaborar um diagnóstico e planejar o que deve ser ajustado ou inovado do ponto de vista legal. Correia Neto, Afonso e Fuck (2019) listam três importantes características do sistema tributário brasileiro que se impõem como obstáculo à formulação legislativa que encerraria a questão das lacunas jurídicas frente à tributação das novas tecnologias:

1. a rigidez constitucional;
2. os conflitos federativos;
3. a autonomia financeira dos entes subnacionais.

Essas questões estão inter-relacionadas, sobretudo no que se refere à matéria constitucional, que diretamente implica nos tributos.

O problema da flexibilidade reside, exatamente, no ponto constitucional. O Brasil tem regras rígidas aplicadas ao sistema tributário nacional. Tanto a modernização quanto a adaptação às inovações e à economia digital levariam a alterações na Constituição Federal. Quanto aos conflitos federativos, são os conflitos de competência: saber a quem compete tributar o quê. Essas delimitações também são encontradas na Constituição Federal (BRASIL, 1988a). A divisão de competências foi formulada quando a economia se concentrava na produção e no comércio de bens físicos, com a maior parte dos serviços executada à prestação em pequena escala e em esfera local. Uma das principais diferenciações da prestação das novas tecnologias é que não existe mais uma fronteira local. Isso leva ao terceiro obstáculo, que se refere à autonomia federativa entre União, estados e municípios nas questões tributárias, com a impossibilidade de determinar o local do fato gerador. Assim, seria imprescindível criar meios de preservação da autonomia federativa.

## A tributação de plataformas digitais

O foco das atenções dos tributos aplicados às novas tecnologias teve início com a ampliação das plataformas de *e-commerce*, o comércio eletrônico, modalidade na qual são realizadas transações financeiras por meio de dispositivos e plataformas eletrônicas, como computadores e *smartphones*. Nessa

modalidade de transação, muitas vezes não é necessário ter ambiente físico nem estoque. Pinheiro (2010) diz que, por causa da expansão do *e-commerce* e o grande volume de negócios originados a partir dele, a discussão sobre o Direito Tributário nessa área se ampliou. Isso não quer dizer que seja preciso criar novos tributos, visto que o fato gerador é o mesmo. Há, porém, outros modelos de negócios que precisam receber maior atenção para que os tributos possam incidir. Veja-os a seguir.

- **Transporte individual de passageiros.** Há vários aplicativos que disponibilizam o mesmo serviço que anteriormente era exercido apenas pelos táxis. Nessa modalidade, por meio de um aplicativo, é possível solicitar uma corrida até determinado destino, sabendo, de antemão, quanto custará. Ainda, é possível realizar o pagamento por meio do próprio serviço, cadastrando um cartão de crédito. Os taxistas reclamam que há concorrência desleal e levantam, como principal argumento, a obrigação tributária que têm com os municípios, mas que os motoristas de aplicativos não têm. Em oposição a esse pensamento, os motoristas de táxi também contam com algumas isenções tributárias de que os motoristas de aplicativo não usufruem. Para que se estabeleça qualquer regramento tributário, o Estado deve analisar a esfera do contribuinte e do consumidor final, visto que, possivelmente, o valor do tributo será agregado ao custo da prestação do serviço. Um exemplo é o que aconteceu no município de São Paulo, onde o Decreto nº 58.981, de 10 de maio de 2016, regulamentou a atividade de transporte individual de passageiros por aplicativos. Para atuar nas regras da Prefeitura, o motorista terá de pagar uma outorga, para o uso das vias da cidade, de aproximadamente dez centavos por quilômetro rodado. As empresas dos aplicativos se manifestaram publicamente nos meios de comunicação, assinalando que esse valor passa a integrar o que é diretamente desembolsado pelo passageiro.
- **Serviços de hospedagem.** Os aplicativos que alugam lugares inteiros ou parte deles para hospedagem são concorrentes diretos dos serviços locais de hotelaria. Algumas leis e recomendações locais de cidades obrigam o anfitrião a recolher impostos, que são pagos pelo usuário e repassados ao órgão competente, em atendimento ao art. 128 do CTN, funcionando como uma substituição tributária. O usuário é informado sobre as taxas e algumas plataformas, como o Airbnb, por exemplo, já elucidam os termos tributários em meio à política de uso fornecida aos hóspedes. Há questões ainda um pouco controversas nesse caso,

como, por exemplo, a auferição de renda por pessoa física, que seria passível de gerar imposto de renda, a cobrança do Imposto Sobre Serviços (ISS) pelo município, tendo em vista a prestação de serviços, a possibilidade de optar pelo Simples, no caso de uma microempresa individual ser constituída para essa finalidade, etc.

- *Fintechs*. As *fintechs* são serviços financeiros que não são, necessariamente, ligados a um banco ou a uma instituição financeira tradicional. Essas empresas e seus aplicativos de produtos digitais e de prestação de serviços permitem uma vasta possibilidade de movimentação financeira, que vai desde negociação de dívidas até financiamentos e empréstimos. A tributação aplicável, todavia, em especial àqueles relacionados com os mercados financeiro e de capitais, ainda é indefinida. No entanto, um modelo de *fintech* já mostra, em seu portal, como ocorre a tributação. A Kickante é uma empresa que financia coletivamente projetos de organizações sociais, não governamentais e *crowdfundings*. Em seu *site*, é possível verificar o quanto de imposto de renda o doador pode abater de sua declaração e quanto imposto incide sobre o faturamento da campanha.

## Outras questões tributárias

Há outras questões que surgem como desafio à tributação. Por falta de uma legislação específica e por ser matéria constitucionalmente regulada, além das previsões do CTN, a circulação de valores escapa à carga tributária em algumas situações, como na tributação sobre a renda, sobre a qual incide a modalidade imposto de renda. O contribuinte desse imposto obedece aos ditames do art. 147 do Regulamento do Imposto de Renda (RIR). Não há mistério quanto à renda recebida no Brasil por residentes brasileiros. O que surge como ponto de análise é o caso em que pessoas jurídicas não domiciliadas em território nacional ou que não possuem filial, sucursal, representação ou agência no país são tributados na qualidade de não residentes, apenas nas situações em que seus "mandatários ou comissários" tenham resultado em operações realizadas no Brasil. Se inexistem as figuras de mandatários ou comissários realizando operações rentáveis no Brasil, não há recolhimento de imposto de renda por essa pessoa jurídica. Essa ausência de tributação pela não territorialidade pode ser uma maneira de beneficiar empresas que recebem valores no Brasil, por não nomearem mandatários no território nacional.

Outra situação a ser observada é o caso da tributação pelo comércio de bens intangíveis. No Brasil, a Constituição Federal distribui a competência da tributação sobre o consumo em duas possibilidades de incidência: os impostos sobre a circulação de riquezas (Imposto sobre Circulação de Mercadoria e Serviços [ICMS]; estados e Distrito Federal), sobre produtos industrializados (Imposto sobre Produtos Industrializados [IPI]; União) e sobre serviços (ISS; municípios), e as contribuições sociais sobre o faturamento das empresas (Programa de Integração Social e Programa de Formação do Patrimônio do Servidor Público [PIS/Pasep]) e Contribuição para o Financiamento da Seguridade Social (Cofins; União). Se for necessário tributar valor agregado, o que se tem de mais próximo é o ICMS. Os casos de aplicação de ICMS e ISS se confundem, a exemplo dos serviços de *streaming*.

### *Fique atento*

Cada município tem competência para definir como os aplicativos de transporte de passageiros vão atuar e quais taxas pagarão, se pagarão. Todavia, os municípios não podem legislar de maneira a ofender as regras das leis federais. O Supremo Tribunal Federal (STF) julgou casos nos quais municípios pretendiam proibir a prestação desses serviços. Na ocasião, o ministro Barroso destacou que a livre iniciativa é um dos fundamentos do Estado brasileiro e que o modelo previsto na Constituição é o da economia de mercado. "A lei não pode arbitrariamente retirar uma determinada atividade econômica do mercado, a não ser que haja fundamento constitucional", explicou o Supremo Tribunal Federal (2019, documento *on-line*). "No caso do transporte individual remunerado, não há nenhum princípio que prescreva a manutenção de um modelo específico, e a edição de leis proibitivas pautadas numa exclusividade inexistente do modelo de exploração por táxi não se conforma ao regime constitucional da livre iniciativa" (SUPREMO TRIBUNAL FEDERAL, 2019, documento *on-line*).

Com relação ao papel dos municípios e do Distrito Federal na regulamentação e na fiscalização do transporte individual de passageiros, o ministro ressaltou que essa competência não pode ser exercitada para interditar, na prática, a prestação desse serviço ao estabelecer medidas anticoncorrenciais nem contrariar os parâmetros fixados pelo legislador federal, que tem atribuição privativa na matéria.

## A tributação das criptomoedas

As criptomoedas, também chamadas de "moedas virtuais", circulam no mercado financeiro de maneira descentralizada, utilizando a tecnologia de *blockchain* e de criptografia para validar e assegurar as transações. As operações que utilizam essas moedas são efetivadas diretamente entre comprador e

vendedor, sem a participação das instituições financeiras. O *blockchain* é a tecnologia que oferece uma organização das transações, como um grande livro de registros que preserva a privacidade das relações financeiras ao mesmo tempo que fornece segurança.

As criptomoedas, para serem consideradas moedas, devem cumprir alguns requisitos, que são próprios e indispensáveis à moeda comum. Isso implica estar dentro do sistema de dinheiro que é criado, alterado, ingerido e fiscalizado pela única autoridade central, o Estado e seus agentes. No Brasil, o Estado tem o monopólio da emissão das moedas, conferido pela Constituição Federal, e o controle de moeda válida dentro da soberania do país. O art. 21, VII, da Constituição Federal define a competência do congresso nacional na função de dispor sobre matérias de moeda, seus limites de emissão e montante da dívida mobiliária federal, e, pelo art. 164, quem emite moeda é o Banco Central do Brasil (BRASIL, 1988a).

Uma moeda tem três funções: ser meio de troca, servir de unidade de conta e reserva de valor. As criptomoedas devem preencher esses mesmos requisitos. O intuito inicial e principal na concepção das moedas virtuais era de substitutivo da moeda corrente e de eliminação da ingerência de autoridades centrais e terceiros intermediários, reduzindo, por consequência, os custos de transação no uso de dinheiro. No que se refere ao caráter jurídico legal das criptomoedas, no cenário brasileiro, inexiste previsão ou norma específica na legislação. Hoje, mais de seis mil criptomoedas estão em circulação, e o *bitcoin*, que foi a primeira a surgir, representa mais da metade do mercado.

### *Saiba mais*

A primeira transação reconhecida com *bitcoin* foi realizada nos Estados Unidos, em maio de 2010, quando um programador da Flórida pagou, a um internauta, 10.000 *bitcoins* pela entrega de duas pizzas. Na época, esse valor equivalia a 42 dólares. Entre os anos de 2010 e 2012, o *bitcoin* foi consolidado no mercado financeiro como um ativo.

Segundo Meira, Costal e Luz (2017), os **criptoativos** funcionam com base em uma tecnologia de registro descentralizado, no qual é feita uma espécie de contabilidade ou livro-razão distribuído em uma rede ponto a ponto de computadores espalhados ao redor do mundo. Toda transação é registrada e divulgada na rede, e o aceite se dá apenas após um complexo sistema de validação, que envolve a maioria dos usuários. As criptomoedas são geradas por um processo chamado de **mineração**, que consiste em um método de validação da transação por meio da checagem das regras da rede. A veri-

ficação consiste na confirmação dos dados pela solução de um problema criptografado. Confirma a criação quem primeiro resolver o problema e validar as informações adicionadas à operação aos blocos anteriores no *blockchain*.

Para a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), uma **criptomoeda** é um ativo digital, negociável, que serve como meio de troca, uma unidade de conta ou reserva de valor, sem nenhuma vinculação legal a qualquer jurisdição. Sua unidade de valor expressa a capacidade de troca, a representação de um valor, não apenas sua conversão. A criptomoeda seria, então, um ativo de movimentação cujas aquisição e manutenção consolidariam o aumento patrimonial. O entendimento tributário, nesse sentido, enquadraria as relações de fatos geradores equivalentes aos que se tem por renda, podendo ser devido, então, o imposto correspondente. É importante esclarecer que não há renda ou provento passíveis de tributação quando não há, de fato, acréscimo patrimonial, conforme dispõe o art. 43 do CTN (BRASIL, 1966).

Para fins de tributação do imposto sobre a renda, é usada a chamada "teoria do acréscimo patrimonial", na qual a renda é considerada como todo ingresso líquido, em bens materiais, imateriais ou serviços avaliáveis em dinheiro, que importe incremento líquido do patrimônio de determinado indivíduo, em certo período, seja ela renda ou provento. Machado (2013) esclarece que, além de obter renda ou proventos, é preciso que esses valores sejam juridicamente disponíveis, o que representa a possibilidade que o contribuinte tem para deles usar e fruir, dentro dos limites da lei e do uso da propriedade. Ou seja, tem relação com o ingresso de forma legal no patrimônio. A tributação das transações financeiras realizadas com criptomoedas, portanto, preenchendo esses pontos, pode ser considerada fato gerador de imposto de renda, com a disponibilidade da aquisição do acréscimo patrimonial. Deve, assim, implicar aquisição de riqueza nova, que aumente o acervo patrimonial anterior.

A aquisição de criptomoeda que implique aumento patrimonial legal e disponível dá causa à incidência do imposto de renda. O art. 3º, § 3º, da Lei nº 7.713, de 22 de dezembro de 1988, estabelece que, na apuração do ganho de capital, serão consideradas as operações que importem alienação, a qualquer título, de bens ou direitos, inclusive de permuta (BRASIL, 1988b). Ou seja, ainda que a transação seja oriunda de troca, poderá incidir o tributo. É importante observar o momento em que se deu o fato gerador, a temporariedade, para definir de maneira correta o ano-base do exercício no qual deve ser declarada a transação.

A Instrução Normativa da Receita Federal do Brasil nº 1.888, de 3 de maio de 2019, dispõe sobre as obrigações acessórias relativas à realização de operações envolvendo criptoativos. A descrição é bastante objetiva ao mencionar que a normativa "[...] institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil" (BRASIL, 2019, documento *on-line*). O tratamento dispensado às criptomoedas é de representação digital de valores que podem ser usados como forma de investimento. Por isso, as pessoas físicas e jurídicas, residentes e domiciliadas no Brasil, e as corretoras de moedas digitais são obrigadas a informar quando e como as operações com essas moedas foram efetuadas. Não há a criação de um novo tributo nem uma modalidade diferente de imposto de renda; apenas a hipótese de incidência é ampliada.

Dias (2020) refere que as operações com as moedas virtuais podem acontecer para investimentos, negociações, remessas internacionais e blindagem contra estornos. A omissão na declaração das transações com criptomoedas pode fazer surgir consequências administrativas, civis, penais e tributárias, obrigando o contribuinte a recolher o imposto devido, acrescido com juros e multa. No que se refere a contribuições sociais, como o Programa de Integração Social (PIS), por exemplo, há dúvidas sobre a incidência em relação às alíquotas devidas pela pessoa jurídica pela oscilação referente ao valor da operação. Isso ocorre porque não é possível avaliar a liquidez da transação em moeda nacional por dois motivos: não existe um câmbio da criptomoeda e não existe um consenso sobre o critério temporal, ou seja, quando seria o momento da incidência do fato gerador da alíquota.

## Outras possibilidades de incidência tributária

Ultrapassada a questão da tributação por meio de imposto de renda, é importante analisar outras possibilidades de incidência tributária. Por se tratar de uma moeda virtual, pode fazer parte de diversas operações, que poderiam servir de fato gerador para a incidência tributária.

Ao se considerar o Imposto sobre Operações Financeiras (IOF) que incide sobre operações de câmbio, não se pode garantir a definição das criptomoedas como "moedas estrangeiras", o que geraria implicações tributárias. Isso porque não é uma moeda vinculada a alguma pátria, e sua origem se dá pela mineração. A competência tributária do IOF pertence à União, estabelecida pela Constituição Federal no art. 153, inciso V. Segundo o art. 63 do CTN, o imposto recai sobre operações de crédito, câmbio e seguro, assim como

operações envolvendo títulos imobiliários (BRASIL, 1966). Esse imposto é recolhido nas transações em instituições financeiras, e aqui reside outro ponto a ser analisado. A empresa de *exchange*, responsável pelas operações e transações com criptomoedas, para recolher esse imposto, deveria ser equiparada a uma instituição bancária.

O Imposto de Importação, por sua vez, tem o fato gerador descrito no art. 19, *caput*, do CTN, referindo-se à entrada de produtos estrangeiros no território nacional. O contribuinte é determinado pelo art. 22, podendo ser o importador ou a quem a ele se equiparar, sem distinção entre pessoa física ou jurídica (BRASIL, 1966). Quando um produto é adquirido no exterior, utilizando a criptomoeda como forma de pagamento, o imposto deve ser calculado com base no valor do produto em moeda nacional. A grande dúvida consiste em fazer a transformação do que foi pago para a liquidez da moeda corrente, uma vez que o câmbio da criptomoeda é variável, podendo valorizar ou desvalorizar. Tem-se, ainda, o problema da temporariedade, de saber quando se opera o fato gerador para o pagamento do imposto, visto que, nesse caso, inexiste legislação.

Já o ICMS é de competência dos estados e do Distrito Federal. Esse imposto incide sobre as operações relativas à circulação de mercadorias em geral, a prestação de serviços de transporte interestadual e intermunicipal, a prestação de serviços de comunicação, o fornecimento de mercadoria com prestação de serviços, a entrada de bens importados do exterior, o serviço prestado no exterior e a entrada no território estadual ou distrital de bens ou serviços provenientes de outra unidade federada. Quando da escrita deste capítulo, a questão da incidência do ICMS sobre a compra de criptomoedas estava para ser decidida em julgamento pelo STF, por meio da Ação Direta de Inconstitucionalidade (ADI) nº 5.958 (BRASIL, 2018).

As criptomoedas, para fins de ICMS, são classificadas como "bens e mercadorias digitais". É um bem intangível, então as operações com criptomoedas podem configurar o fato gerador do tributo. Todavia, ainda é necessário aguardar o posicionamento do STF para que haja segurança jurídica por meio do julgamento do caso paradigma. De um modo geral, quanto ao Imposto de Importação, ao Imposto de Exportação e ao ICMS, não restam dúvidas sobre a possibilidade de incidência sobre as criptomoedas e suas transações envolvidas. O Convênio ICMS nº 106, de 29 de setembro de 2017, inclui as criptomoedas como bens tributáveis, então a maior dúvida reside quanto ao fato gerador do IOF.

### *Saiba mais*

Para entender um pouco mais do *blockchain*, alguns conceitos são fundamentais. O primeiro deles é a **integridade da rede**, que prevê que a confiança é intrínseca, não extrínseca. A integridade está presente em toda etapa do processo, devido à criação de um mecanismo capaz dar credibilidade via criptografia inteligente a toda e qualquer transação por meio da rede. De forma complementar, temos o conceito de **poder distribuído**. Segundo Tapscott e Tapscott (2016), o sistema distribui poder por meio de uma rede ponto a ponto, sem qualquer central de controle, e nenhuma parte isolada pode alterar a rede sem o conhecimento dos demais nós.

Nesse sentido, os autores ressaltam que também são fundamentais os conceitos de **segurança** e **privacidade**. Medidas de segurança estão incorporadas na rede sem nenhum ponto de falha e fornecem não apenas confidencialidade, mas também autenticidade e aceitação geral entre os membros. Qualquer um que queira participar deve usar criptografia distribuída de chave pública. Ao eliminar a obrigação de confiar nas outras pessoas, o sistema elimina a obrigação de conhecer a identidade real dos demais nós, então não é requisito para a utilização do *software* o fornecimento de quaisquer dados pessoais.

A partir desses conceitos, chegamos ao de **direitos preservados**. Direitos de propriedade são transparentes e executáveis, e liberdades individuais são reconhecidas e respeitadas. O protocolo prova de trabalho (PoW, do inglês *proof of work*) exigido para originar as moedas também contém o registro cronológico das transações (e, portanto, de sua titularidade). O *blockchain* acaba por confirmar a propriedade de cada moeda em circulação, já que toda transação é imutável e irrevogável (TAPSCOTT; TAPSCOTT, 2016).

Além disso, **valor como incentivo** é outro conceito fundamental, que significa que o sistema alinha os incentivos de todos os participantes. Algum símbolo de valor é essencial para o alinhamento e manutenção do sistema. E, por fim, temos a **inclusão**, na medida em que a economia trabalha melhor quando ela funciona para todos. Assim, qualquer um pode utilizar a tecnologia do *blockchain* pela "verificação de pagamento simplificado", que pode funcionar até mesmo em celulares, de acordo com Tapscott e Tapscott (2016).

## O *software* e sua tributação

O ordenamento jurídico brasileiro conta com uma lei que relaciona programas de computador com *software*, definindo-o com o objetivo de proteger a criação do autor. Assim, prevê o desenvolvimento dos programas de computadores e sua criação, por serem fruto do esforço intelectual humano e de sua capacidade de solucionar problemas por meio da tecnologia da informação. A Lei nº 9.609, de 19 de fevereiro de 1998, define, no art. 1º, a natureza jurídica do **programa de computador** como estrutura organizada, em linguagem própria para tal, para utilização em *hardwares*, estes com suas funcionalidades de-

terminadas. Ou seja, o *software* será vinculado a uma aplicação, que é sua finalidade. No art. 2º, a referida lei confere, a esse bem incorpóreo, a mesma proteção qualificada ao direito autoral (BRASIL, 1998).

O *software* se diferencia do *hardware* porque o segundo é, obrigatoriamente, corpóreo, enquanto o primeiro confere utilidade à máquina a partir de sua instalação. O *software*, entendido como programa para fins de legislação, já foi comercializado de maneira física. A instalação em um *hardware* dependia da aquisição de componentes físicos, como CDs ou disquetes. O produto, todavia, era aquilo que estava contido nesses dispositivos e que passaria a funcionar no momento da instalação do *hardware*. O ponto central reside, aqui, em saber que o *software* que se adquire, ainda que fisicamente, confere, ao consumidor, não a propriedade daquela aplicação, mas sua **licença de uso**. Quando é necessária a instalação em mais de uma máquina, são adquiridas mais licenças.

Nos tempos atuais, a realidade de aquisição se modificou, e a instalação de um *software* é perfeitamente viável a partir do *download*. No caso dos aplicativos, o funcionamento é praticamente o mesmo. As operações com *software* são objeto de tributação pelo ISS, por definição constitucional. O *software*, em si, é considerado uma prestação de serviço, porque, quando é adquirido, o que se recebe não é um produto, mas uma licença de uso, e é recebida a cessão, ou seja, o direito de uso, a posse. Não havendo o que se falar em transferência de propriedade, esta será sempre do autor do *software*.

Com o aumento da circulação das relações de consumo envolvendo *software*, a Administração Pública passou a questionar a tributação aplicável, tentando descaracterizar a prestação de serviços existente, tributada pelo ISS para transferir a tributação para a incidência do ICMS de Transporte Interestadual e Intermunicipal e de Comunicação. O assunto foi discutido tendo por base a diferenciação entre o *software* customizado, encomendado e produzido para uma finalidade específica e o *software* "de prateleira", que é produzido em larga escala. Decidiu-se que incidiria ICMS sobre o *software* de suporte físico, produzido sem grau de customização, e ISS sobre o *software* customizado, pois entendeu-se que haveria uma prestação de serviço.

O assunto foi judicializado, e o STF julgou a ADI nº 1.945, sobre possível divergência na Lei Estadual nº 7.098, de 30 de dezembro de 1998, Mato Grosso (BRASIL, 1999). A lei previa a incidência de ICMS sobre operações de venda de *software* padronizado, adquirido por *download*, considerando o valor da operação como base de cálculo. Após muita discussão sobre o tema, em fevereiro de 2021, o entendimento majoritário do STF excluiu a incidência do

ICMS sobre o licenciamento ou a cessão de direito de uso de programas de computador. Nessas operações, incide o ISS.

### *Saiba mais*

Em 1999, o STF havia se manifestado de maneira diversa, entendendo pela possibilidade da cobrança de ICMS quando se adquirisse um *software* de "prateleira" por meios físicos. Apenas seriam tributados por ISS aqueles *softwares* que fosse encomendados para uma finalidade específica, feito sob demanda.

Outro debate que movimentava a disputa entre estados e municípios na guerra tributária dizia respeito aos *softwares* em nuvem, conhecidos como SaaS (*software as a servisse*, disponíveis em nuvem para que o usuário consiga utilizar conforme sua necessidade. No mesmo julgamento, os ministros do STF entenderam que o *software*, padronizado ou não, em qualquer de suas formas de disponibilização, inclusive física, não poderia ser tributado pelo ICMS, pois, por mais que seja legítima a incidência do ICMS sobre bens incorpóreos ou imateriais, em verdade o argumento central para a tomada da decisão não foi esse. A Corte decidiu que é indispensável, para que ocorra o fato gerador do ICMS, a transferência de propriedade do bem, o que não ocorre nas operações com *software*, visto que o que se tem é a licença. Os ministros analisaram o fornecimento de *software* personalizado por meio do comércio eletrônico direto e o SaaS, decidindo que, nessas operações, também incide o ISS, já que há, inequivocamente, prestação de serviço. Esse entendimento pode ser estendido aos aplicativos, visto que são equiparados aos *softwares*, porque o usuário, ao baixar e instalar, recebe o licenciamento do uso, não sua propriedade.

### *Exemplo*

Você já parou para ler o termo de licença de uso de um *software* ou aplicativo quando faz o *download*? Nele estão todas as informações sobre o uso e as boas práticas, bem como as informações sobre a licença daquela aplicação. O licenciamento de *software* funciona como um contrato estabelecido entre o fabricante e a pessoa física ou jurídica que o usará. É nesse termo que estão as possibilidades de restrições para *downloads*, instalações, manutenções, alterações, mudanças no código-fonte, uso de certas funcionalidades e distribuição. Essas licenças podem ser de diversas formas, como de código aberto, perpétua, temporária ou Saas, por exemplo. Ao final do termo, sempre é solicitado o aceite ao usuário. Ao clicar no botão, o usuário declara que leu, aceita e está de acordo com os termos, não podendo, depois, alegar desconhecimento.

# Referências

BRASIL. Constituição da República Federativa do Brasil de 1988. *Diário Oficial da União*, Brasília, 5 out. 1988a. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 maio 2021.

BRASIL. Instrução normativa nº 1.888, de 3 de maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). *Diário Oficial da União*, Brasília, 7 maio 2019. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592#:~:text=IN%20RFB%20N%C2%BA%201888%20%2D%202019&text=Institui%20e%20disciplina%20a%20obrigatoriedade,Federal%20do%20Brasil%20(RFB). Acesso em: 28 maio 2021.

BRASIL. Lei nº 5.172, de 25 de outubro de 1966. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. *Diário Oficial da União*, Brasília, 27 out. 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em: 28 maio 2021.

BRASIL. Lei nº 7.713, de 22 de dezembro de 1988. Altera a legislação do imposto de renda e dá outras providências. *Diário Oficial da União*, Brasília, 23 dez. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7713.htm. Acesso em: 28 maio 2021.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. *Diário Oficial da União*, 20 fev. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 28 maio 2021.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 1945 MC*. Relator: Octavio Galloti. Belo Horizonte, 21 jan. 1999. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=1747607. Acesso em: 28 maio 2021.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 5958*. Ação direta de inconstitucionalidade. Pedidos de ingresso como amici curiae. Requerimentos deferidos. Relator: Cármen Lúcia. Brasília, 11 jun. 2018b. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5484103. Acesso em: 28 maio 2021.

CORREIA NETO, C. de B.; AFONSO, J. R. R.; FUCK, L. F. A tributação na era digital e os desafios do sistema tributário no Brasil. *Revista Brasileira de Direito*, v. 15, nº 1, p. 145-167, 2019. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/3356. Acesso em: 28 maio 2021.

DIAS, H. R. A incidência da tributação nas operações com criptomoedas. *Cadernos Jurídicos da Faculdade de Direito de Sorocaba*, v. 2, nº 1, p. 126-134, 2020. Disponível em: https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/49. Acesso em: 28 maio 2021.

DOMINGUES, P. S. *Legislativo 4.0*: o desafio da criação de novas leis para um mundo em mutação. *In*: CZYMMECK, A. (ed.). *A quarta revolução industrial*: inovações, desafios e oportunidades. Rio de Janeiro: Fundação Konrad Adenauer, 2020. p. 35-58. (Cadernos Adenauer, 1).

MACHADO, H. de B. *Curso de Direito Tributário*. 34. ed. São Paulo: Malheiro Editores, 2013.

MEIRA, L. A.; COSTAL, G. Z.; LUZ, E. S. Criptomoedas: moedas, ativo financeiro ou uma nova tulipa? *Economic Analysis of Law Review*, v. 8, nº 2, p. 482-512, 2017. Disponível em: https://portalrevistas.ucb.br/index.php/EALR/article/view/10310. Acesso em: 28 maio 2021.

PINHEIRO, P. P. *Direito digital*. 4. ed. São Paulo: Saraiva, 2010.

SCHWAB, K. *A quarta revolução industrial*. São Paulo: Edipro, 2016.

SUPREMO TRIBUNAL FEDERAL. STF considera inconstitucional proibição por lei municipal de transporte individual por aplicativos. 2019. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=410556. Acesso em: 28 maio 2021.

TAPSCOTT, D.; TAPSCOTT, A. *Blockchain revolution*: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai, 2016.

VIEIRA, L. P.; MOURÃO, P. A. L. O impacto da revolução informacional sobre o direito tributário: os casos da imunidade do livro eletrônico e do Protocolo ICMS 21/2011. *In*: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 2., 2013, Santa Maria. *Anais eletrônicos* [...]. Disponível em: http://coral.ufsm.br/congressodireito/anais/2013/6-16.pdf. Acesso em: 28 maio 2021.

## Leituras recomendadas

ÁLVAREZ CUESTA, H. *El futuro del trabajo vs. el trabajo del futuro:* implicaciones laborales de la indústria 4.0. La Coruña: Colex, 2017.

BRASIL. Convênio ICMS 106, de 29 de setembro de 2017. Disciplina os procedimentos de cobrança do ICMS incidente nas operações com bens e mercadorias digitais comercializadas por meio de transferência eletrônica de dados e concede isenção nas saídas anteriores à saída destinada ao consumidor final. Diário Oficial da União, Brasília, 5 out. 2017. Disponível em: https://www.confaz.fazenda.gov.br/legislacao/convenios/2017/CV106_17. Acesso em: 28 maio 2021.

NASCIMENTO, C. V. do (coord.). *Comentários ao código tributário nacional*. Rio de Janeiro: Forense, 1999.

SOUSA, A. K. de M. *O desafio da tributação das criptomoedas sob a ótica do imposto de renda*. 2020. 63 f. Monografia (Graduação em Direito) — Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2020.

SZELBRACIKOWSKI, D. C. Novas tecnologias e a necessidade de reforma tributária. *In*: AFONSO, J. R.; SANTANA H. L. *Tributação 4.0*. São Paulo: Almedina, 2020.

### *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

# Aplicações de *blockchain*

*Leonardo Brendo Gomes Nascimento*

**OBJETIVOS DE APRENDIZAGEM**

- Apresentar exemplos de criptomoedas com *blockchain*.
- Integrar *blockchain* com criptomoedas.
- Aprofundar os exemplos de aplicação de tecnologias de *blockchain*.

## Introdução

O uso de criptomoedas e a popularização da *blockchain* tiveram início a partir do trabalho publicado pela personagem Satoshi Nakamoto, que propôs a moeda virtual *bitcoin* e sua *blockchain*. Essas iniciativas disruptivas possibilitaram a comercialização de recursos financeiros e, em seguida, o uso de ativos virtuais para representar recursos tangíveis e intangíveis, que vão desde patentes de *softwares* simples até a identificação de diamantes e de escrituras de imóveis luxuosos.

Bens tão estimados devem ser tratados com muita segurança, o que é oferecido pelas aplicações que usam *blockchains*. Estas estabelecem uma comunicação direta entre os envolvidos nas operações da rede, sem a necessidade de um agente validador das operações, além de utilizarem redes *peer-to-peer*. Ademais, é garantido um alto nível de segurança e integridade dos dados, visto que as informações de cada bloco da *blockchain* estão distribuídas entre os nós da rede.

Neste capítulo, você vai conhecer moedas digitais e plataformas bastante usadas atualmente, compreendendo o processo de integração das *blockchains* com suas criptomoedas. Além disso, vamos apresentar exemplos de técnicas computacionais aplicadas às *blockchains*.

## Criptomoedas e suas respectivas *blockchains*

É cada vez mais comum encontrarmos páginas de comércio eletrônico que usam criptomoedas, como, por exemplo, o *bitcoin*, o *ether* e o *monero*. Além disso, há empresas investindo altos valores em criptomoedas a fim de criar e aperfeiçoar novas aplicações nos mais diversos setores da sociedade (HOLLINS, 2018).

As criptomoedas são qualquer moeda comercializada no formato digital cuja segurança é garantida por mecanismos de criptografia. Sua principal característica é a ausência de um órgão que as regule ou de uma instituição centralizadora, o que torna seus usuários independentes, permitindo que eles se comuniquem diretamente, sem a burocracia de um terceiro validador das operações na rede (HOLLINS, 2018).

Tendo em vista a grande adesão às criptomoedas nas transações financeiras e em outras áreas do mercado de trabalho, bem como os inúmeros benefícios que elas oferecem a seus usuários, abordaremos nesta seção alguns exemplos desse tipo de moeda: o *bitcoin*, o *ether*, o IOTA e o ADA.

### *Bitcoin*

O *bitcoin* (ou BTC) é a criptomoeda mais usada e valorizada do mundo. Ela foi a primeira moeda virtual a surgir, desencadeando a revolução atual no mundo das criptomoedas e das *blockchains* (NAKAMOTO, 2008). A quantidade de *bitcoins* disponíveis é limitada, o que evita a inflação e a criação aleatória de unidades (HOLLINS, 2018).

O êxito do *bitcoin* se deve à tecnologia *blockchain*, isto é, um conjunto de blocos ligados entre si que é compartilhado entre seus usuários (NAKAMOTO, 2008). Dentro desses blocos, há um conjunto de informações imutáveis (data, hora, emissor, receptor, quantidade ou frações de *bitcoins* e outros aspectos das operações) sobre as transações financeiras que aconteceram ao longo do tempo — sendo esse conjunto conhecido como “livro razão”.

A *blockchain* do *bitcoin* insere datas e horas nas transações por meio de um *hash* em uma cadeia contínua. Para isso, é utilizado o algoritmo *proof of work* (PoW) à base de *hash* (usando-se o *hash* atual e o *hash* anterior), sendo realizados registros que não podem ser mudados sem que se refaça o PoW. Dessa forma, a cadeia mais longa serve como prova da sequência de eventos testemunhados, além de assegurar que ela veio do maior *pool* de CPUs (NAKAMOTO, 2008).

## *Ether*

A criptomoeda *ether* e sua *blockchain*, o *ethereum*, foram criadas em 2013, por Vitalik Buterin. O *ether* vem sendo bastante utilizado e valorizado no mundo eletrônico devido à sua atuação, que é bem diferente da do *bitcoin*. Ele é focado em contratos inteligentes (ou, em inglês, *smart contracts*), que viabilizam o uso de criptoativos (BUTERIN, 2013).

Desde sua criação, o *ether* foi focado em ativos no mercado financeiro, sendo popularizado por conta de sua plataforma, o *ethereum*. No *ethereum*, é possível negociar contratos inteligentes, que são executados automaticamente por meio de mecanismos ou protocolos digitais e não reversíveis (BUTERIN, 2013). Para usar a plataforma e criar seus contratos inteligentes, o usuário da *blockchain ethereum* precisa pagar uma taxa na criptomoeda *ether*.

## ADA

A criptomoeda ADA e sua *blockchain*, o *cardano*, foram idealizadas e implementadas em 2015, por Charles Hoskinson (que também foi um dos fundadores da plataforma *ethereum*). Atualmente o ADA é considerado uma das melhores criptomoedas para se investir, tendo uma capitalização de US$ 9 bilhões. O funcionamento da plataforma *cardano* é semelhante ao do *ethereum*: ele permite a criação de contratos inteligentes descentralizados mediante pagamento em sua moeda nativa, o ADA (AYDINLI, 2018).

O ADA é protegido por um protocolo que utiliza a prova de aposta, conhecido como "*ouroboros*" (protocolo de *blockchain* revisado por pares), possibilitando a execução de sua *blockchain* com e sem permissão. O *ouroboros* é reconhecido por ser uma forma mais confiável e escalonável de se prover a descentralização (AYDINLI, 2018).

## IOTA

A criptomoeda IOTA e sua pseudoblockchain, o *tangle*, foram criadas entre 2014 e 2015, por Sergey Ivancheglo, Serguei Popov, David Sønstebø e Dominik Schiener. Focado na indústria da Internet das Coisas (IoT, do inglês Internet of Things), o IOTA viabiliza a otimização de milhares de microtransações de forma altamente escalável, pois utiliza a estrutura de grafo acíclico direcionado (DAG, do inglês *directed acyclic graph*) (POPOV, 2018).

A principal característica dessa criptomoeda é o emaranhado de seus nós, que cria um DAG para armazenar transações de sua rede. O uso de DAG em *blockchains* indica a evolução dessa tecnologia, que passa a dispor de recursos indispensáveis para viabilizar micropagamentos aperfeiçoados de máquina para máquina (POPOV, 2018).

# Integração de *blockchain* com suas criptomoedas

A movimentação de criptoativos tornou-se uma atividade rotineira, possibilitando às pessoas que realizam transações financeiras pela internet vender, comprar, trocar ou financiar bens tangíveis (terras, casas, automóveis, etc.) ou intangíveis (direitos autorais, cópias autenticadas, certificados digitais, etc.) (TAPSCOTT; TAPSCOTT, 2016).

Dentre os mecanismos necessários para a realização dessas operações, destacam-se as aplicações de *blockchains*, especificamente a partir de sua segunda geração. A segunda e a terceira geração das *blockchains* viabilizaram, respectivamente, a comercialização de ativos digitais e as aplicações altamente distribuídas. A primeira geração, por sua vez, trabalhava apenas com operações financeiras, sendo o *bitcoin* o único recurso utilizado (MIERS *et al*., 2019).

### *Saiba mais*

Embora tenha ganhado destaque somente a partir da publicação do *whitepaper* "Bitcoin: a peer-to-peer electronic cash system", de Satoshi Nakamoto (2008), o conceito de *blockchain* já existia antes. Ele foi apresentado pela primeira vez no trabalho "Improving the efficiency and reliability of digital time-stamping", de Dave Bayer, Stuart Haber e W. Scott Stornetta (1993), que aborda correntes de blocos criptograficamente seguras.

Oferecendo segurança, transparência, integralidade e imutabilidade dos dados, as *blockchains* podem ser aplicadas em diversas áreas, como, por exemplo, saúde, educação, segurança, economia, entretenimento, política, cultura, tecnologia, setor automobilístico, entre outras.

Para demonstrar a aplicação das *blockchains* (contratos inteligentes), vejamos como ela ocorre na educação, especificamente na verificação e na emissão de documentação, como diplomas, arquivos pessoais, etc. Segundo Vidal (2020), os principais *stakeholders* de *blockchain* na educação são os avaliadores, os empregadores, os estudantes e os professores. Os avaliadores precisam de documentos válidos para se certificar de que as avaliações foram realizadas sem vazamentos ou colas, ao passo que os empregadores trabalham com a gestão e a organização de documentos. O uso das *blockchains* por estudantes e professores, por sua vez, está relacionado a aulas, patentes, direitos autorais, documentos de vínculo com a instituição, entre outros.

Veja na Figura 1 o fluxo de funcionamento da *blockchain* aplicada na verificação de documentos da aluna Joana, a partir da ferramenta Blockcerts, idealizada e implementada pelo Massachusetts Institute of Technology (MIT).

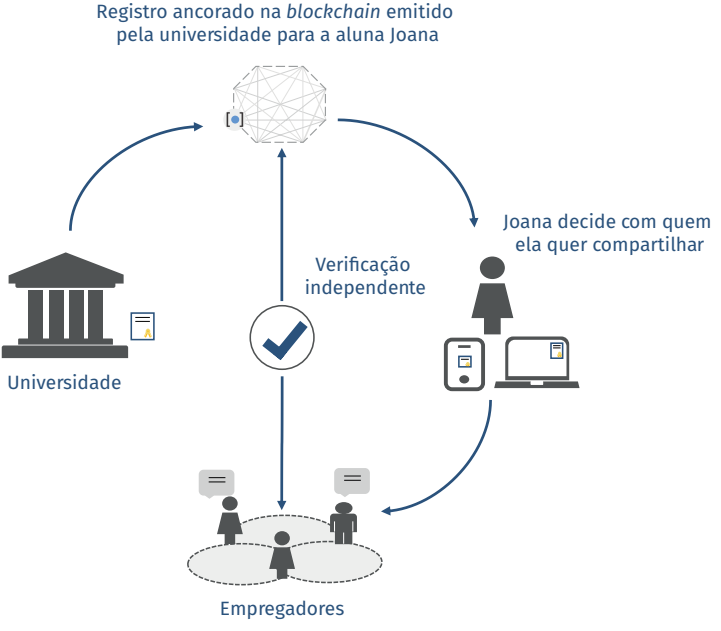


**Figura 1.** Verificação independente de documentos da aluna Joana por meio da *blockchain*.
**Fonte:** Adaptada de Vidal (2020).

Como se pode ver na Figura 1, a aluna Joana tem sua documentação da universidade verificada de maneira independente por meio da *blockchain* (especificamente a plataforma Blockcerts). Observe que Joana decide compartilhar seus arquivos com quem ela quiser e de forma direta, não precisando de um terceiro para analisar seus dados, pois a plataforma realiza tal análise. Ademais, note que Joana usa contratos inteligentes, uma vez que a Blockcerts é baseada na *blockchain ethereum*. O contrato inteligente usado é o mecanismo (protocolo ou *script*) criado automaticamente pela *blockchain* para verificar a veracidade dos documentos.

### *Saiba mais*

Você sabia que qualquer pessoa pode implementar sua própria *blockchain* e disponibilizar seus serviços? Com a alta de vendas e compras pela internet, os usuários estão buscando mais facilidades e vantagens em seus negócios. Em virtude desse mercado efervescente viabilizado pela internet, empresas, instituições e desenvolvedores de *software* estão propondo novos serviços descentralizados e distribuídos por meio das *blockchains*. Exemplos de serviços que usam *blockchains* na área da educação são o Blockcerts, o BTCert e o EduCTX.

## Tecnologias fundamentais para a *blockchain*

Nesta seção, você vai conhecer técnicas computacionais e conceitos fundamentais para viabilizar o funcionamento adequado da segunda maior *blockchain* usada no mercado, o *ethereum*, que foi utilizada como base para a elaboração da plataforma Blockcerts, por exemplo. É importante destacar que o *ethereum* é um conjunto de técnicas usadas colaborativamente para alcançar uma finalidade em comum — *blockchains* a partir da segunda geração. A seguir, serão detalhados alguns itens indispensáveis para compreender a estrutura do *ethereum*.

### Rede *peer-to-peer*

A rede *peer-to-peer*, também conhecida como P2P, é uma arquitetura de redes de computadores não centralizada, em que cada nó da rede pode disponibilizar ou consumir recursos e ser cliente ou servidor simultaneamente. Nesse formato de rede, não é necessário um servidor central para compartilhar as

informações, pois os dados são distribuídos em todos os usuários da rede (DRESCHER, 2018).

O *ethereum* usa massivamente esse tipo de arquitetura de redes de computadores. Isso porque ela possibilita que um nó da rede envie informações diretamente a outro nó da rede, o que aumenta o desempenho das transações realizadas em sua *blockchain*, pois não é necessário usar um terceiro para validar as operações (BUTERIN, 2013).

## Criptografia

A criptografia utilizada na *blockchain ethereum* é aplicada ponta a ponta e em todos os nós da rede. Se algum usuário ou nó da *blockchain* tentar inserir alguma informação maliciosa nos blocos ou burlar a imutabilidade dos dados na rede, ele terá de alterar todas as informações que foram encadeadas nos blocos (BUTERIN, 2013). A alteração de todas as informações só é possível por meio do uso correto de todos os *hashes* dos blocos ligados. Sendo assim, é necessária uma descoberta *hash* a *hash*, um trabalho que, embora seja matematicamente possível, tem pouca probabilidade de lograr êxito.

Para compreender com mais profundidade a criptografia aplicada ao *ethereum*, faz-se necessário conhecer o uso dos *hashes* nos blocos e o funcionamento dos algoritmos de consenso para escolher o nó minerador, bem como confirmar o nível de segurança usando as curvas elípticas (BUTERIN, 2013).

### *Hash*

De maneira semelhante à *blockchain* usada na moeda *bitcoin*, a plataforma *ethereum* usa o algoritmo de consenso PoW para escolher o novo minerador do bloco a ser inserido na rede. Há, porém, uma diferença entre essas plataformas: o *ethereum* usa o algoritmo ETHash, a fim de fortalecer suas transações e deixá-las mais rápidas e menores, aumentando o desempenho das operações que utilizam contratos inteligentes (HAN; FOUTRIS; KOTSELIDIS, 2019).

O algoritmo ETHash usa a função criptográfica Keccak-256, que foi utilizada para padronizar e aumentar a criptografia da SHA-3. A Keccak-256 usa a estratégia DAG e tem o comprimento de 256 bits, sendo fundamentada na abordagem conhecida como "construção de esponja" (HAN; FOUTRIS; KOTSELIDIS, 2019). A abordagem utilizada na Keccak-256 se apropria de uma ampla função estocástica, ou permutação aleatória, permitindo inserir (absorver) e emitir (espremer) qualquer quantidade de dados, atuando como uma função pseudoaleatória nas entradas anteriores (BUTERIN, 2013).

## Curvas elípticas

A criptografia baseada em curvas elípticas é um mecanismo confiável e eficiente quando comparado a outros mecanismos populares — como, por exemplo, o Rivest-Shamir-Adleman (RSA) —, pois precisa de menos processamento e volume de transmissão de dados, sendo considerado apropriado para aplicativos em *tablets* e *smartphones* (ANGULO, 2017). Esse algoritmo criptografa e descriptografa dados por pares de chaves públicas e privadas, e é usado na plataforma *ethereum* como um recurso importante para, em parceria com o algoritmo ETHash, garantir a segurança dos dados (BUTERIN, 2013).

Esse mecanismo é pertinente para a plataforma *ethereum* porque ajuda na criptografia das chaves públicas e privadas disponibilizadas ou não aos usuários da *blockchain* em questão. Isso porque, se um determinado usuário desejar dispor de um contrato inteligente, precisará ter um identificador que informe que ele é de fato dono do contrato inteligente em vigência (ANGULO, 2017).

Neste capítulo, foram abordadas as aplicações de *blockchains*, levando-se em consideração a integração com suas criptomoedas, seu contexto de uso e suas tecnologias fundamentais. Convém destacar que o funcionamento e as características de cada moeda digital são definidos por sua *blockchain*, o que inclui uma série de comportamentos particulares, que vão desde o formato de pagamento de taxas para usar a *blockchain* até o estilo de transações realizadas pelos usuários na rede. As tecnologias usadas nas criptomoedas e nas *blockchains* são ferramentas frequentemente encontradas no mercado de trabalho de tecnologia da informação, sendo, portanto, essencial ao profissional que deseja se tornar um especialista na área o domínio desse conhecimento teórico.

# Referências

ANGULO, R. J. O. *Criptografia de curvas elípticas*. 2017. 100 f. Dissertação (Mestrado em Matemáticas) — Universidade Federal de Goiás. Disponível em: https://repositorio.bc.ufg.br/tede/bitstream/tede/6976/5/Disserta%C3%A7%C3%A3o%20-%20Rigo%20Julian%20Osorio%20Angulo%20-%202017.pdf. Acesso em: 11 nov. 2021.

AYDINLI, K. *Performance assessment of Cardano*. Zurich: University of Zurich, 2018.

BAYER, D.; HABER, S.; STORNETTA, W. S. Improving the efficiency and reliability ofdigital time-stamping. *In*: CAPOCELLI, R.; SANTIS, A.; VACCARO, U. (ed.). *Sequences II*. [*S. l.*]: Springer, 1993. p. 329-334.

BUTERIN, V. A next generation smart contract & decentralized application platform. *Ethereum White Paper*, 2013.

DRESCHER, D. *Blockchain básico*: uma introdução não técnica em 25 passos. [*S. l.*]: Novatech, 2018.

HAN, R.; FOUTRIS, N.; KOTSELIDIS, C. Demystifying crypto-mining: analysis andoptimizations of memory-hard pow algorithms. *In*: IEEE INTERNATIONAL SYMPOSIUM ON PERFORMANCE ANALYSIS OF SYSTEMS AND SOFTWARE, 2019. *Anais* [...]. [*S. l.*]: IEEE, 2019. p. 22-33.

HOLLINS, S. *Bitcoin para iniciantes*: o guia definitivo para aprender a usar bitcoin e criptomoedas. [*S. l.*]: Createspace Independent Publishing Platform, 2018.

MIERS, C. *et al*. Análise de mecanismos para consenso distribuído aplicados a blockchain. *In*: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 19., 2019, São Paulo. *Anais* [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 91-139.

NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. *Bitcoin Whitepaper*, 2008. Disponível em: https://git.dhimmel.com/bitcoin-whitepaper/v/a5f36b332cb6a5fa9e-701886f376ac1ac2946d07. Acesso em: 11 nov. 2021.

POPOV, S. The tangle. *White paper*, v. 1, n. 3, Apr. 2018.

TAPSCOTT, D.; TAPSCOTT, A. *Blockchain revolution*: how the technology behind bitcoin is changing money, business, and the world. Penguin: Portfolio, 2016.

VIDAL, F. R. *Análise e aplicação da tecnologia blockchain na gestão de diplomas do ensino superior*. 2020. 139 f. Dissertação (Mestrado em Engenharia Informática, Ramo de Sistemas de Informação e Multimédia) — Universidade Fernando Pessoa, Porto, 2020.

## Leituras recomendadas

HANKE, T. Asicboost-a speedup for bitcoin mining. *ArXiv.org*, v. 1, Apr. 2016.

REVOREDO, T. *Blockchain*: tudo o que você precisa saber. [*S. l.*]: The Global Strategy, 2019.

### *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

# Bases técnicas de criptomoedas

*José Eugênio de Mira*

**OBJETIVOS DE APRENDIZAGEM**

- Apresentar o funcionamento das criptomoedas.
- Explicar os tipos de criptomoedas.
- Descrever o *white paper* das criptomoedas.

## Introdução

Sistemas confiáveis são a base das relações humanas desde os primórdios das civilizações. No entanto, com o aumento exponencial dos grupos humanos e a sua expansão pelo mundo, o comércio como sistema confiável passou a precisar de uma base material. São comuns, inclusive, situações em que um banco falido pode levar a um colapso no sistema financeiro, rompendo a cadeia de confiança entre clientes e instituições. Entender a dinâmica desse sistema é essencial para compreender como e por que surgiram a *blockchain* e as criptomoedas.

A *blockchain* e as criptomoedas nasceram do interesse de grupos em criar um sistema computacional capaz de garantir transições de valores em uma rede descentralizada, sem interferência de instituições ou do Estado e sem a necessidade de confiança entre as partes. A maneira como as criptomoedas surgiram, de forma anônima e descentralizada, está diretamente relacionada à preocupação desses grupos com questões envolvendo a liberdade e anonimato. Apesar disso, com o passar do tempo e o aumento dos interesses comerciais e institucionais sobre as criptomoedas, começaram a surgir soluções de transferência de valores que não necessariamente seguem os preceitos de anonimato, transparência e descentralização.

Neste capítulo, falaremos sobre as criptomoedas e as suas transações, sobretudo sobre como funcionam contratos inteligentes e como podem representar um avanço considerável em área de negócio e tecnologia, e até mesmo na área jurídica. Também veremos um pouco sobre as linguagens utilizadas na execução desses contratos e o conceito de *tokens*. Por fim, vamos definir o que são os *white papers* das criptomoedas.

## Como funcionam as criptomoedas?

A assinatura de documentos digitalmente, assim como o processo de certificação digital, pressupõe a existência de relações de confiança entre os emissores das mensagens ou entre os emissores e a entidade certificadora. Em alguns casos, porém, essa relação de confiança não pode ser estabelecida. A ***blockchain*** surgiu para solucionar esse problema por meio de uma cadeia de dados públicos, que torna todos os blocos de dados encadeados entre si (e daí o nome, *block chain*, ou corrente de dados). Para isso, usa conceitos como chave pública e privada e *hash*.

A primeira criptomoeda conhecida, o ***bitcoin***, surgiu como um valor a ser transacionado dentro da *blockchain*. É importante compreender que, nesse sentido, ambos os conceitos são de origem comum e indissociáveis. Os dados escritos na *blockchain*, a partir de quem controla as suas chaves, são divididos por todos os computadores que fazem parte da rede de *peers* (pontos) da *blockchain*. Assim, qualquer dado que seja registrado na *blockchain* fará parte de um registro público, descentralizado e inalterável.

Embora, na teoria, o armazenamento de dados dentro da *blockchain* sirva para os registros das transações ocorridas dentro da própria cadeia, como as trocas de criptomoedas entre os usuários da rede, qualquer registro pode ser inserido na *blockchain* a um pequeno custo conhecido como *fee* (a taxa de mineração).

### *Saiba mais*

Você sabe a diferença entre criptomoedas e moedas digitais? Embora todas as criptomoedas sejam moedas digitais, nem todas as moedas digitais são criptomoedas. Em entrevista ao *site* da CNN Brasil, o executivo Bruno Milanello, da corretora Mercado Bitcoin, explicou que o processo de pagamento intermediado por meio digital, ou seja, qualquer moeda eletrônica, pode ser considerado pagamento em moeda digital. No entanto, criptomoedas são descentralizadas, primando por valores como segurança e privacidade. Moedas digitais emitidas e/ou controladas por empresas ou governos, então, não poderiam ser consideradas criptomoedas (VITORIO, 2021).

Apesar de o conceito de *blockchain* basear-se no sistema desenvolvido para a criação e a transação de *bitcoins*, o seu formato de distribuição, acesso aos dados e criação de blocos encadeados pode ser utilizado por soluções descentralizadas de armazenamento de dados, garantindo a irreversibilidade de registros. Em um sistema de certificação digital, essa propriedade pode ser utilizada para garantir que, uma vez assinada, uma transação passe a ser reconhecida publicamente como válida. O sistema notarial poderia ser substituído por uma cadeia semelhante, em que qualquer pessoa ou instituição poderia registrar os seus dados e confirmar, aceitando ou rejeitando, transações.

No entanto, é importante destacar que, embora qualquer pessoa possa criar uma *blockchain* (uma vez que o programa tem código aberto, já tendo sido replicado para a criação de centenas outras criptomoedas e *blockchains* privadas), a *blockchain* responsável pelo *bitcoin* é única. Assim, *blockchain* pode se referir à cadeia ligada à criptomoeda *bitcoin* ou ao sistema por trás das redes distribuídas P2P (*peer-to-peer*) de registros imutáveis.

***Peer-to-peer network*** significa redes ponto a ponto, ou seja, redes descentralizadas, sem um computador centralizado, sem um servidor. Desde o final da era dos *mainframes*, grandes computadores corporativos centralizados, as redes de computadores passaram por um processo conhecido como *downsizing*, com computadores sendo transformados em estações de trabalho cada vez mais autônomas, que poderiam compartilhar recursos com outros na rede, bem como utilizar recursos de outros.

Essa proposta se popularizou com a internet e, logo nos primeiros anos do século XXI, surgiram os primeiros *softwares* de compartilhamento de arquivos distribuídos. Assim, quando um computador disponibiliza um arquivo, rapidamente este é copiado por outros e assim sucessivamente. Mesmo que o primeiro computador se torne indisponível, agora centenas ou milhares de cópias desse arquivo já foram copiados para outros computadores, que vão continuar compartilhando-o. Esse sistema se tornou popular ao permitir o compartilhamento de arquivos de áudio e vídeo por meio de programas de *torrent*.

Um ***torrent*** é um arquivo que contém os endereços de computadores que têm um determinado arquivo disponível. Ao ser compartilhado, o arquivo é atualizado, apontando para os novos computadores. A rede da *blockchain* funciona de forma análoga. Para fazer parte da rede, é preciso utilizar um *software* que se conecta à rede e faz uma cópia de todas as transações existentes, passando a colaborar nessa rede. Cada computador da rede é chamado de *node* (ou nó) e colabora recebendo todos os blocos da rede e realizando um processo que consiste basicamente em tentar "adivinhar" o próximo bloco válido, o que é feito por meio de uma *proof-of-work* (prova de

trabalho). Observe a descrição do *white paper* sobre o processo de trabalho da rede na *blockchain* do *bitcoin*:

> 1) Novas transações são transmitidas para todos os nós. 2) Cada nó coleta novas transações em um bloco. 3) Cada nó trabalha para encontrar uma *proof-of-work* complexa para o seu bloco. 4) Quando um nó encontra uma *proof-of-work*, ele transmite o bloco para todos os nós. 5) Os nós aceitam o bloco somente se todas as suas transações são válidas e já não foram gastas. 6) Os nós expressam sua aceitação do bloco, trabalhando na criação do próximo bloco na cadeia, usando o *hash* do bloco aceito como o *hash* anterior (NAKAMOTO, 2021, documento *on-line*).

Portanto, um **bloco** é um conjunto de transações, ou seja, um conjunto de alterações dos valores descritos na *blockchain*, transmitidas pela rede. Uma ***proof-of-work*** é uma comprovação de que determinado computador utilizou um tempo de processamento para realizar determinada tarefa proposta pelo código do *software* da *blockchain*. O processo de realização de uma prova de trabalho recebe uma recompensa em criptomoedas, e esse processo é chamado de **mineração**.

## Criptomoedas e contratos

A ideia de um sistema financeiro sem uma terceira parte confiável e à prova de falhas pode parecer muito boa para ser verdade, mas existem, inclusive, sistemas que já operam baseados nesses preceitos, movimentando, anualmente, alguns bilhões de dólares. Embora tenhamos o *bitcoin* como principal referência de criptomoeda, existe todo um ecossistema de criptomoedas, criadas a partir de *blockchains* com diferentes funções e, na maioria das vezes, oferecidas inicialmente nos eventos chamados de *initial coin offering* (oferta inicial de moedas), ou ICOs.

Uma **ICO** é uma oferta de criptomoeda relacionada a um determinado produto ou serviço. Ao lançar um ICO, o seu criador vende criptomoedas relacionadas no seu negócio, escritas em uma *blockchain*. Caso o produto ou serviço atenda aos requisitos prometidos, como no caso de uma *startup*, que promete uma rede social à prova de bisbilhoteiros, o valor dessa criptomoeda deve subir, acompanhando o seu sucesso, da mesma maneira como acontece com uma IPO (*initial public offering*, ou oferta pública inicial), quando uma empresa vende ações na bolsa de valores. Entretanto, em uma ICO, os *tokens* recebidos podem ser utilizados, posteriormente, na própria empresa. Um *token* de uma rede social poderia servir, por exemplo, para a compra de

publicidade na própria rede. Assim, quanto mais popular a rede se tornasse, mais valioso seria o *token*.

É claro que, uma vez que os *tokens* são dados, poderiam ser utilizados como moeda entre os próprios usuários da rede social, correto? Também poderiam ser utilizados como forma direta de pagamento ou como forma de premiar ou punir automaticamente usuários por determinados comportamentos na rede. Um usuário que infringisse as regras perderia os seus *tokens* ou uma parte deles, enquanto quem denunciasse um comportamento ilegal poderia ser premiado. O uso de *tokens* a partir de *blockchains* que vem sendo feito para estabelecer relações automáticas, por meio de transações autoexecutáveis, é chamado de **contrato inteligente**.

## DApps, DAOs e linguagens de programação

A *blockchain* do *bitcoin* tem um formato de programação conhecido como Bitcoin Script. Apesar de ser possível criar interações simples associadas à *blockchain*, essa linguagem tem as seguintes duas limitações no que diz respeito ao seu uso para criação de contratos inteligentes.

1. A linguagem não permite o uso de laços, ou seja, não é possível utilizar condições cíclicas. Isso está associado ao fato de que colocar condições em uma linguagem a torna mais pesada do ponto de vista de processamento. Quando se trata de processamento distribuído, como é o caso da *blockchain*, isso pode ser um problema.
2. Como a *blockchain* é única, caso um código malicioso fosse implantado, poderia se propagar continuamente pela rede, sendo impossível retirá-lo depois.

Pensando nisso, o russo Vitalik Buterin criou a linguagem Ethereum, que permite o desenvolvimento de aplicações distribuídas voltadas para contratos inteligentes. Enquanto na *blockchain* do *bitcoin* o foco são as transações de criptomoedas, na *blockchain* da Ethereum o foco são as execuções dos contratos inteligentes. Essas aplicações são executadas com cópias simultâneas e com regras de alteração previstas em código. Ao contrário do que aconteceria na *blockchain*, a rede do Ethereum distribui a sua execução em compartimentos, ou máquinas virtuais, que são ambientes seguros de execução de código. Dessa forma, o código malicioso fica "contido" ao ser executado, além de permitir que o código seja executado de forma

distribuída. Chamamos essas aplicações de **DApps** ou *descentralized apps* (aplicativos descentralizados).

## *Saiba mais*

Você certamente já ouviu falar de NFTs ou *non-fungible tokens* (tokens não fungíveis). Embora guarde uma certa relação, NFTs não são criptomoedas, mas certificados de autenticidade de arquivos digitais. Esse certificado de autenticidade é um código criptografado gerado a partir do arquivo original. Assim, mesmo que esse arquivo seja replicado, nunca vai conter o certificado que confere originalidade a ele. Essa inovação permitiu que artes digitais, *tweets* célebres e até mesmo memes fossem autenticados e vendidos. A correlação dos NFTs com as criptomoedas vêm do fato de ambos serem registrados na *blockchain*.

A Ethereum possui uma linguagem de programação própria, a Solidity. Essa linguagem difere levemente das linguagens comuns de programação, pois opera como uma máquina de estados. Uma **máquina de estados** é assim chamada porque não existe modificação diretamente no código; o que acontece é uma permissão de alteração, mas qualquer alteração obedece a duas regras:

1. a alteração, bem como o valor original, ficará permanentemente salva na *blockchain*;
2. a alteração tem um custo, que, no caso da Ethereum, é cotado em "gas", um *token* interno que compra poder de processamento dentro da rede.

Sabemos que a *blockchain* é imutável. O que podemos fazer, nesse caso, é gravar, na *blockchain*, o algoritmo, que seriam as condições do código, e o que pode ser alterado é só o estado do contrato: se teve as condições atendidas, se foi executado ou não. No Ethereum, qualquer alteração no estado das EVMs (*Ethereum virtual machines*) tem um custo, o que incentiva a criação de códigos eficientes. Segundo a documentação oficial do Solidity (c2017, documento *on-line*):

> Um contrato, no conceito do Solidity, é um conjunto de códigos (*functions*) e dados (*state*), que residem em um específico endereço na rede *blockchain* Ethereum. [...] Você pode pensar nisso como um único *slot* em um banco de dados que pode ser consultado e alterado chamando funções do código que gerencia o banco de dados. No caso do Ethereum, ele é sempre o contrato proprietário.

Além disso, os contratos podem se comunicar entre si, tornando possível a criação de um ecossistema automatizado de contratos inteligentes. Pensando em um sistema amplamente baseado em DApps, seria possível até mesmo a criação de empresas inteiras utilizando contratos inteligentes. Imagine uma máquina de refrigerantes conectada à internet, capaz de enviar uma mensagem ao seu fornecedor quando o seu estoque está baixo e de pagar o fornecedor automaticamente quando este realizar a reposição por meio de uma transação na *blockchain*. A máquina poderia, inclusive, recalcular os seus pedidos automaticamente com base nos refrigerantes mais pedidos ou solicitar manutenção após certa quantidade de vendas, ou mesmo pedir um carro autônomo para as entregas. A flexibilidade da linguagem implementada pelo Ethereum permite tanto a criação de outras submoedas quanto a sua utilização por meio de outros códigos.

Já existem, inclusive, organizações inteiras que funcionam por meio de contratos inteligentes descentralizados. As chamadas **DAOs** (*descentralized autonomous organizations*, ou organizações autônomas descentralizadas) utilizam as regras do algoritmo para implementar regras organizacionais rígidas, como direito a voto em um conselho de acionistas. Imagine uma empresa que oferece, automaticamente, uma vez por ano, o cargo de gerente ao melhor vendedor. Cada vendedor registraria as suas vendas no contrato inteligente da organização. Ao final do período, o contrato inteligente analisaria as médias de venda e elegeria o próximo gerente de forma transparente e à prova de indicações de favoritos ao cargo.

### *Fique atento*

Outro termo que tem se popularizado entre os usuários e entusiastas das criptomoedas é o DeFi, ou *descentralized finances* (finanças descentralizadas). Segundo o *site* Ethereum.org, DeFi é um termo que abrange produtos e serviços financeiros que podem ser utilizados por usuários da Ethereum e das suas criptomoedas, incluindo sistemas construídos com *blockchains* próprias. É importante frisar que a Ethereum não é apenas uma moeda, mas também um ecossistema que permite a criação e integração de outras criptomoedas e serviços.

Na prática, o uso de contratos inteligentes pode representar o fim da maneira como estamos acostumados a lidar com transações no dia a dia e, principalmente, com a qualidade de produtos e serviços. Se, atualmente, já temos sistemas que podem, por exemplo, autorizar a passagem em um pedágio ou realizar entregas de *pizzas* com *drones*, a utilização desses serviços de forma integrada com uma *blockchain* dispensaria uma terceira parte confiável, como uma operadora de cartões ou um banco. Seria como se você pagasse automaticamente por cada um desses serviços diretamente por meio da sua carteira de criptomoedas. E mais: caso o sensor térmico do seu *smartwatch* verificasse que o tempo de entrega e a temperatura da *pizza* estão fora do combinado ou, no caso de uma estrada com pedágios, o seu carro registrasse excesso de buracos na pista além do nível aceitável registrado em contrato, você seria prontamente ressarcido.

## *White papers*

As criptomoedas foram criadas a partir um processo de pesquisa elaborado pelo seu autor anônimo, Satoshi Nakamoto, aparentemente em colaboração com outras pessoas por meio de fóruns de conversa na internet. Embora o seu primeiro bloco tenha sido minerado em 2009, também o ano da sua primeira transação, o surgimento oficial da moeda foi marcado pelo evento de lançamento do seu *white paper*, chamado "Bitcoin: A Peer-to-Peer Electronic Cash System", que apresentou, pela primeira vez, o contexto completo da *blockchain* e do *bitcoin* em si. O documento, que surgiu em momento oportuno graças ao abalo de confiança gerado pela crise mundial de 2008, descrevia o que era e como funcionava o *bitcoin* de forma simples.

Em ciência, existem alguns modelos de publicação de propostas e de resultados. Uma das mais populares, o artigo científico, tem uma estrutura simplificada, em que uma ideia ou o resultado de um assunto específico é apresentado de forma concisa e pormenorizada, com referências e resultados. Conforme a descrição de Lozada e Nunes (2019, p. 238):

> [...] é um trabalho científico baseado em pequenos estudos, porém completos, que trata de uma questão científica. Ele se distingue dos diferentes tipos de trabalhos científicos pela sua reduzida dimensão e conteúdo. É normalmente publicado em revistas ou periódicos especializados, impressos ou eletrônicos. Tendo em vista que os artigos científicos são em sua maioria completos, permitem ao leitor, mediante a descrição da metodologia empregada, do processamento utilizado e dos resultados obtidos, repetir a experiência.

Embora guardem algumas semelhanças entre si, como o formato curto, a completude e a descrição de modo que os resultados possam ser replicados, um *white paper* é um documento de apresentação mais popular, mais técnico e menos científico. De acordo com o *site That White Paper Guy*, as principais características que definem um *white paper* não são um formato ou um tipo de publicação e material específicos: qualquer documento a partir de cinco ou seis páginas, com texto em formato narrativo, que apresente fatos de forma educativa, prática e facilmente aplicável é um ***white paper***. Além disso, *white papers* não têm objetivos comerciais, embora possam ser utilizados para esse fim. Veja, na Figura 1, uma das imagens originais (traduzida) do *white paper* do *bitcoin*.

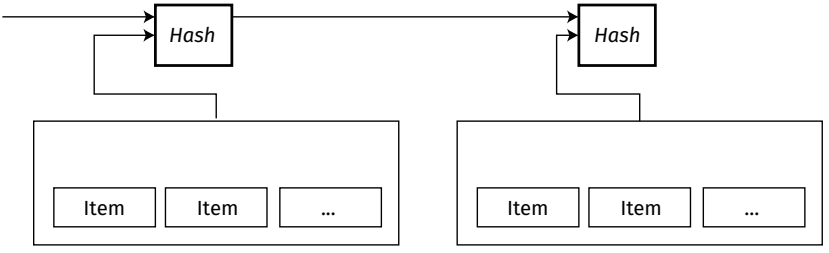


**Figura 1.** Formação do bloco encadeado no *white paper* do *bitcoin*.
**Fonte:** Adaptada de Nakamoto (2021).

É importante frisar que os *white papers* devem ser documentos não muito complexos do ponto de vista técnico, pois, no caso das criptomoedas, eles embasarão o investimento nos *tokens*. Assim, uma descrição precisa do produto e/ou serviço vinculado ao ICO ajuda a convencer os investidores a investirem no projeto das criptomoedas em questão. Enquanto, em uma IPO, a integridade de uma empresa é apurada por equipes de consultoria e auditoria fiscais e contábeis, o principal suporte da ICO para convencer os seus investidores é o *white paper*, que comunica a estrutura da moeda que está sendo criada, os seus objetivos e as suas principais características.

### *Saiba mais*

Em 1992, a professora americana Cynthia Dwork e o professor israelense Moni Naor apresentaram um trabalho que versava como sobre combater Spam no envio de *e-mail*. A proposta dos acadêmicos era de que, para cada *e-mail* enviado, um "custo" computacional fosse necessário. "Se eu não te conheço e você deseja me enviar uma mensagem, deve provar que gastou, digamos, dez segundos [...] apenas para mim e apenas para esta mensagem" (DWORK; NAOR, 2013, documento *on-line*, tradução nossa). Ou seja, em vez de simplesmente enviar o dado, o sistema tem que realizar um trabalho computacional; trabalho esse que envolve uma função que demanda certo custo matemático para ser calculada, mas que pode ser verificada com facilidade.

O trabalho apresentava uma das ideias fundamentais do trabalho de Satoshi, publicado mais de 15 anos depois. Ao ler a estrutura do artigo e compará-lo com o *white paper* dos *bitcoins*, fica clara a diferença entre os modelos: enquanto um se preocupa em comunicar resultados de uma pesquisa de forma geral, sem apresentar aplicações, o outro utiliza propostas já conhecidas para atender a fins objetivos e as apresenta em forma de inovação.

## Projetos e moedas

Embora apresentem os projetos mais conhecidos e, juntas, o maior *market cap* (valor de mercado), Bitcoin e Ethereum são apenas duas das quase seis mil criptomoedas existentes registradas até julho de 2021, segundo dados de reportagem da Você/SA (VERSIGNASSI, 2021). Segundo o autor, a fatia total de mercado dessas moedas gira em torno de US$ 1,44 trilhão, e as duas principais respondem por quase 65% desse valor. Outras, como a conhecida *dogecoin*, famosa graças ao milionário da área de tecnologia Elon Musk, tem um capital menor, mas ainda assim respeitável: por volta dos US$ 32 bilhões.

Devemos compreender o que faz um projeto diferenciar-se de outro e por que existem tantas criptomoedas diferentes. Em geral, pequenos detalhes, como segurança, tipo ou dificuldade para se minerar, controle dos detentores dos *tokens* sobre os projetos e privacidade, são pontos fulcrais. Em outros casos, até mesmo questões relacionadas ao fim do consenso sobre o *software* utilizado pode criar uma moeda, como é o caso do *hard fork* do *bitcoin*, que gerou uma nova criptomoeda, chamada de *bitcoin gold*.

### *Fique atento*

O termo *fork* é utilizado quando há uma bifurcação no desenvolvimento de um *software*, por exemplo, quando um desenvolvedor ou um grupo prefere seguir por um caminho diferente, criando uma versão nova a partir de uma base comum. Em criptomoedas, um *fork* é uma divisão que acontece na *blockchain* quando um grupo de pessoas decide validar um bloco diferente daqueles estabelecidos pelo consenso. Aqueles que aceitarem o bloco que implementa uma mudança de regras continuam fazendo parte da *blockchain*, mas os outros passam a ser incompatíveis, pois fizeram uma modificação no código do bloco ou mesmo no *software* do *node*. Isso cria uma divisão que, na prática, dão origem a uma *blockchain* e uma moeda completamente diferentes. O mais interessante é que, como todas as modificações ainda existem no *node* que implementou a alteração, qualquer pessoa que tivesse criptomoedas na versão antiga continuaria tendo as suas moedas; agora, nas duas versões.

Entre as criptomoedas mais conhecidas, algumas se destacam, seja pelas suas características, seja pela sua dominância no mercado. As informações sobre cada uma dessas criptomoedas fazem parte do seu *white paper*. Abaixo, descrevemos algumas das principais e das suas características, com informações extraídas de seus *white papers*, bem como as suas siglas (seguindo a codificação ISO 4217), pelas quais são identificadas nas *exchanges* (corretoras).

- *Cardano* (ADA): popular entre os usuários de criptomoedas e até entre pessoas ligadas ao mundo financeiro. O *white paper* dessa moeda promete interoperabilidade entre diferentes *blockchains*, o que permitiria, em tese, um sistema financeiro descentralizado, baseado unicamente em moedas digitais. Além disso, tem um sistema em que os detentores dessa criptomoeda podem validar transações apenas mantendo certa quantidade de moedas em uma carteira, recebendo, assim, taxas de transação (*fees*).
- *Dogecoin* (XDG): popularizada graças aos fóruns de internet e ao esforço de personalidades como o magnata da tecnologia Elon Musk. Com alta velocidade de transação e taxas baixas, foi pensada justamente para transações entre usuários. A moeda foi baseada em uma versão (*fork*) da criptomoeda *litecoin*, ela mesma baseada no *bitcoin* original.
- *Monero* (XMR): embora muito se diga sobre a irrastreabilidade do *bitcoin*, associada à possibilidade de crimes como de lavagem de dinheiro, todas as suas transações são transparentes e auditáveis, desde que se conheça a origem ou o destino dos valores. A moeda *monero*,

no entanto, foi pensada justamente para ser anônima, ocultando detalhes da transação.

- *Tether* (USDT): embora seja mais uma moeda digital, existem discussões se essa moeda controlada e emitida pela Bitifinex (uma das maiores corretoras de criptomoedas do mundo) seja uma criptomoeda, em razão de questões levantadas sobre as suas transparência e centralidade. A *tether* é o que chamamos de *stablecoin*, uma criptomoeda projetada para ter sempre o mesmo valor; no caso, atrelado ao dólar.

Além disso, os *white papers* das moedas podem conter informações técnicas mais específicas, como as que podem ser utilizadas para programadores criarem aplicações compatíveis com as suas *blockchain* (embora seja comum, em muitos casos, que todo o código-fonte das criptomoedas seja disponibilizado de forma completa para qualquer usuário). Além disso, grande parte dos projetos de criptomoedas é *open-source*, o que implica dizer que podem ser modificados à vontade para que outras criptomoedas sejam criadas a partir deles — assim como o *white paper* original do *bitcoin* permitiu o surgimento de milhares de outras criptomoedas.

Vale observar que não basta compreender o funcionamento, os diferentes tipos já criados, as funcionalidades (como os *smart contracts*) e a documentação que define as propriedades de cada uma das criptomoedas. Para se compreender a importância dessa inovação tecnológica e econômica, é importante reconhecer a filosofia por trás da sua criação, que envolve uma origem incerta e anônima em meio a uma das maiores crises do capitalismo da história. Assim, compreender no que consistem as criptomoedas não é apenas um objetivo em si, mas um esforço em identificar as necessidades da sociedade do futuro, que anseia por liberdade, estabilidade, privacidade e independência econômica. As criptomoedas são um sintoma de convulsões sociais que tiraram, durante todo o século anterior, os governos e as instituições do centro do debate macroeconômico e colocaram, no seu lugar, aquele que é certamente o ente mais importante e o único essencial de qualquer sistema econômico: o indivíduo.

## Referências

DWORK, C.; NAOR, M. *Princing via processing or combatting junk mail*. 2013. Disponível em: https://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf. Acesso em: 3 set. 2021.

LOZADA, G.; NUNES, K. S. *Metodologia científica*. Porto Alegre: Sagah, 2019.

NAKAMOTO, S. *Bitcoin*: um sistema de dinheiro eletrônico peer-to-peer. 2021. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf. Acesso em: 3 set. 2021.

SOLIDITY DOCS. *Introdução aos smart contracts*. c2017. Disponível em: https://solidity-pt.readthedocs.io/pt/latest/introduction-to-smart-contracts.html#um-simples-smart-contract. Acesso em: 3 set. 2021.

VERSIGNASSI, A. Quantas criptomoedas existem, afinal? *VC S/A*, 2021. Disponível em: https://vocesa.abril.com.br/blog/guru/quantas-criptomoedas-existem-afinal/. Acesso em: 3 set. 2021.

VITORIO, T. Entenda a diferença entre criptomoeda e moeda digital, como a estudada pelo BC. *CNN Brasil Businiess*, 2021. Disponível em: https://www.cnnbrasil.com.br/business/2021/08/04/entenda-a-diferenca-entre-criptomoeda-e-moeda-digital-como-a-estudada-pelo-bc. Acesso em: 3 set. 2021.

## Leituras recomendadas

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 4217*: currency codes. Genebra: ISO, 2015. (*E-book*).

RYKWALDER, E. A matemática por trás do Bitcoin: CoinDesk 2021. *Bitcoin on Air*, 2020. Disponível em: https://pt.bitcoinonair.com/math-behind-bitcoin. Acesso em: 3 set. 2021.

THAT WHITE PAPER GUY. *Frequently asked question*. 2005. Disponível em: https://thatwhitepaperguy.com/white-paper-faq-frequently-asked-questions/#what_is. Acesso em: 3 set. 2021.

THORNBURG, W. What is Ethereum? The ultimate beginners' guide. *Coin Central*, 2018. Disponível em: https://coincentral.com/what-is-ethereum-the-ultimate-beginners-guide. Acesso em: 3 set. 2021.

WHITEPAPER.IO. *Analyse cryptocurrency whitepapers*. 2017. Disponível em: https://whitepaper.io/. Acesso em: 3 set. 2021.

### *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

# Criptografia aplicada a *blockchain*

*Juliane Adelia Soares*

**OBJETIVOS DE APRENDIZAGEM**

- Conceituar criptografia com *blockchain*.
- Integrar criptografia com *blockchain*.
- Apresentar exemplos de criptografia com *blockchain*.

## Introdução

Novas tecnologias e novos dispositivos estão surgindo a todo momento para atender a demandas de diferentes áreas. Essa revolução tecnológica traz inúmeros benefícios para a sociedade, como, por exemplo, a realização de transações financeiras e compras *on-line*. No entanto, isso também gera diariamente um número considerável de dados, que ficam armazenados no ciberespaço e, assim, são mais facilmente acessados por cibercriminosos.

É, portanto, fundamental investir em sistemas seguros. Para atender a essa necessidade, tem-se mostrado uma alternativa bastante relevante a *blockchain*, um sistema de banco de dados descentralizado que armazena dados de transações. Estas, então, são efetuadas de forma rápida e mantidas em segurança com o uso da criptografia.

Neste capítulo, você vai conhecer os principais aspectos da criptografia no contexto de *blockchain* e compreender como essas duas tecnologias funcionam de maneira integrada. Por fim, vamos exemplificar a aplicação da criptografia na tecnologia *blockchain*.

## Criptografia no contexto de *blockchain*

Com o crescente número de dispositivos e sistemas tecnológicos, a segurança digital tem se tornado um fator de preocupação, pois os ataques de cibercriminosos estão a cada dia mais sofisticados. Isso também ocorre com a *blockchain*.

Segundo Bashir (2017), a *blockchain* pode ser definida de diferentes formas, a depender da maneira como ela é analisada. Algumas das definições existentes são as seguintes:

- mecanismo de consenso descentralizado, em que todos os pares eventualmente chegam a um acordo em relação ao estado de uma transação;
- livro-razão compartilhado e distribuído de transações, que são ordenadas e agrupadas em blocos; seu modelo distribuído serve como fonte única de verdade para todas as organizações que o utilizam;
- estrutura de dados, ou seja, pode ser considerado uma lista vinculada que utiliza ponteiros de *hash*, que são usados para apontar o bloco anterior.

Basicamente, a *blockchain* é um livro-razão distribuído ponto a ponto, que roda sobre a internet, criptograficamente seguro, imutável e que se atualiza apenas por consenso ou acordo entre pares. Em uma plataforma de *blockchain*, os pares podem trocar valores utilizando transações sem que seja necessário um arbitrador central confiável, o que faz com que nenhuma autoridade seja responsável pelo banco de dados (BASHIR, 2017).

O livro-razão facilita o processo de registro de transações e rastreamento de ativos (tangíveis e intangíveis) em uma rede de negócios. É grande o leque de coisas que podem ser rastreadas e negociadas em uma rede *blockchain* de modo que riscos e custos sejam reduzidos para todos os envolvidos. Como os negócios funcionam na base da informação, essa tecnologia é importante porque fornece imediatamente tais informações, que são compartilhadas, transparentes e podem ser acessadas somente por pessoas autorizadas. Na rede *blockchain*, podem-se rastrear pedidos, pagamentos, contas, produção, etc., sendo possível ver os detalhes de uma transação de ponta a ponta (GUPTA, 2017).

Como todos os participantes da rede *blockchain* têm acesso ao livro-razão distribuído e ao registro de transações (que é imutável), todas as transações são registradas uma única vez, eliminando-se duplicações. Dizer que os registros são imutáveis significa que, uma vez armazenados na *blockchain*, eles

não poderão mais ser alterados, e, em caso de erros, uma nova transação deverá ser adicionada, ficando ambas visíveis (GUPTA, 2017).

Cada uma das transações é registrada como bloco de dados, e os usuários escolhem as informações que serão registradas (quem, o quê, quando, onde, etc.). Cada um desses blocos está conectado aos anteriores e aos posteriores. Sendo assim, uma referência a um bloco anterior também é incluída ao bloco, caso não seja um bloco de origem. Geralmente, sua estrutura varia de acordo com o tipo e o *design* da *blockchain*, mas alguns atributos são essenciais para a funcionalidade do bloco, como o cabeçalho, os ponteiros para blocos anteriores, o carimbo de data e hora, o contador de transações, entre outros (BASHIR, 2017).

Garantir a segurança das informações do usuário e dos dados das transações é uma condição obrigatória em uma *blockchain*. Essa segurança pode ser obtida por meio da criptografia, que torna os dados incompreensíveis a fim de garantir sua confidencialidade. Para tanto, é usado um algoritmo, chamado de "cifra", e um valor secreto, denominado "chave". Se a chave secreta não for conhecida por quem obtiver o arquivo, não será possível descriptografá-lo, nem apreender qualquer informação sobre a mensagem criptografada (AUMASSON, 2018).

O funcionamento básico da criptografia é apresentado na Figura 1, em que se pode observar que o texto original é cifrado, sendo transformado em uma aparente pilha inútil de letras e números, e, em seguida, descriptografado, recuperando-se o texto original.

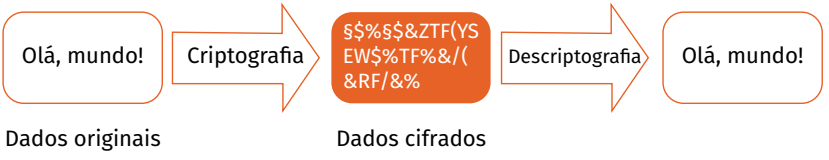


**Figura 1.** Esquema básico de criptografia.
**Fonte:** Adaptada de Drescher (2017).

Necessária para criar um meio confiável de identificação, autenticação e autorização que assegure a segurança dos dados, a criptografia pode ser classificada, de acordo com Vallim (2019), em chave simétrica e chave assimétrica.

A **chave simétrica** faz uso da mesma chave para cifragem e decifragem da mensagem, conforme ilustra a Figura 2.

**Figura 2.** Chave simétrica.
**Fonte:** Adaptada de Drescher (2017).

Dessa forma, algoritmos simétricos podem ser considerados mais simples e com processamento mais rápido se comparados a algoritmos assimétricos. Quando se trata de grandes volumes de dados, utilizar chave simétrica pode ser vantajoso. No entanto, esse método apresenta algumas vulnerabilidades no processo de comunicação de senha, justamente na parte que a torna mais eficiente, pois todos os envolvidos na transação devem conhecer a mesma chave. Assim, não é possível identificar o criador da mensagem, o que torna mais fácil que uma alteração maliciosa feita por um terceiro que conheça a chave ocorra sem ser percebida.

Já a **chave assimétrica** faz uso de duas chaves, uma utilizada para cifrar e outra para decifrar, como se pode observar na Figura 3. A parte superior da ilustração apresenta a criptografia, e a parte inferior, a descriptografia. O texto cifrado em preto só poderá ser decifrado com o texto em branco e vice-versa.

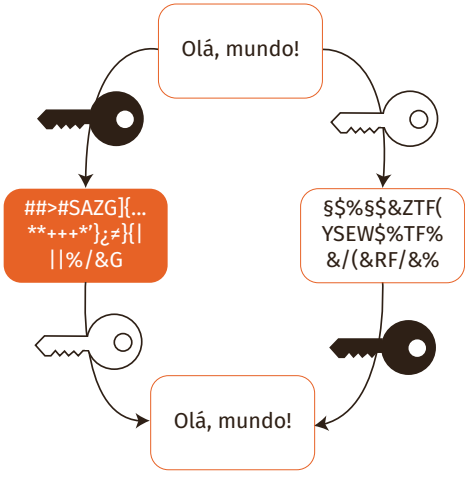


**Figura 3.** Chave assimétrica.
**Fonte:** Adaptada de Drescher (2017).

A chave utilizada para cifrar a mensagem é privada, secreta, sendo conhecida somente pelo criador da mensagem. Já a chave para decifrar a mensagem é pública, ou seja, é conhecida por todos. Entretanto, ambas as chaves são geradas de modo simultâneo por um algoritmo e são correlatas. Dessa forma, apenas o destinatário conseguirá acessar o conteúdo da mensagem, garantindo sua autoria. A desvantagem da chave assimétrica é que ela exige mais processamento que a chave simétrica, mas com a garantia de que a confidencialidade e a autenticidade das mensagens estejam protegidas.

Mas, afinal, qual é a relação entre *blockchain* e criptografia? Como a *blockchain* funciona como um modelo de rede ponto a ponto descentralizado, não existe apenas um nó. Além disso, esses nós não precisam confiar uns nos outros. Por isso, a *blockchain* deve garantir proteções adequadas para informações de transações que ocorrem em canais não seguros, enquanto mantém a integridade da transação. Assim, a criptografia é essencial para que a *blockchain* consiga, ao mesmo tempo, proteger as informações de transações e sua privacidade e assegurar a consistência dos dados.

A criptografia é utilizada em diversos lugares para fornecer segurança a uma rede *blockchain*, baseando-se em três conceitos básicos: *hashing*, chaves e assinaturas digitais. O *hash* é uma impressão digital única usada para verificar se as informações não foram alteradas, sem que seja necessário vê-las. As chaves, por sua vez, são usadas combinando-se públicas e privadas para criptografar e descriptografar as mensagens. Já a assinatura digital é um cálculo matemático utilizado para comprovar a autenticidade de uma mensagem ou de um documento digital (MOUGAYAR, 2016).

Mougayar (2016) afirma que, no contexto da *blockchain*, a criptografia é baseada na hegemonia público/privado, ou seja, há visibilidade pública, mas inspeção privada. Como analogia, você pode pensar em seu endereço residencial, que, embora possa ser publicado (isto é, tornado público), não fornece informações sobre o interior da sua residência. Sendo assim, você só poderá acessá-lo se tiver a chave privada, e, como esse endereço foi reivindicado como seu, ninguém mais poderá se apropriar dele.

A *blockchain* utiliza a criptografia de chave assimétrica, com o objetivo de identificar contas e autorizar transações, conforme define Drescher (2017).

- Identificação de contas: a *blockchain* precisa identificar usuários ou contas de usuários, com o intuito de manter o mapeamento entre proprietário e propriedade, e, para isso, utiliza uma abordagem público-privada. Como os números das contas na *blockchain* são chaves criptográficas públicas, os dados das transações fazem uso de chaves

públicas para identificar as contas que estão envolvidas na transferência de propriedade. Assim, as contas de usuários têm um endereço conhecido publicamente, e todos podem enviar mensagens para ele.

- Autorização de transações: os dados das transações devem conter uma informação que comprove que o proprietário da conta que transfere a propriedade realmente concorda com essa transação. Ou seja, o fluxo de informações implícito nesse acordo inicia com o proprietário da conta, que faz a transferência da propriedade e deve chegar a todos que realizam a inspeção dos dados da transação. Quando transfere a propriedade, o proprietário da conta cria um texto cifrado com sua chave cifrada e todos que tiverem sua chave criptográfica pública podem verificar essa prova de concordância.

O processo de criptografia envolve o uso de códigos matemáticos avançados para armazenar e transmitir valores de dados de forma segura. Com isso, é possível garantir que somente os usuários aos quais as transações ou os dados se destinam consigam obtê-los, lê-los e processá-los.

Na próxima seção, serão apresentadas as principais ferramentas utilizadas para garantir a integridade das informações na *blockchain*.

## Integração entre criptografia e *blockchain*

A *blockchain* é um banco de dados distribuído, em que são permitidas transações diretas sem que seja necessária a atuação de um mediador autorizado. A criptografia *blockchain* encapsula transações na forma de blocos, de modo que esses blocos sejam vinculados por meio do *hash* criptográfico, formando uma cadeia de blocos protegidos.

A seguir, vamos apresentar, baseando-se em Gayoso Martínez, Hernández-Álvarez e Hernández Encinas (2020) e Raikwar, Gligoroski e Kralevska (2019), os principais conceitos criptográficos utilizados para que a integridade das informações seja garantida na *blockchain*.

### Funções *hash*

Funções *hash* são funções capazes de transformar qualquer bloco de dados binários em outro bloco binário com tamanho fixo. O resultado dessa transformação é o chamado *hash*, ou *digest*. Observe os exemplos apresentados na Figura 4.

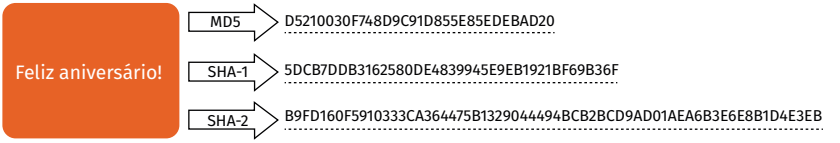


**Figura 4.** Exemplos de *hash*.

A Figura 4 mostra a transformação da frase "Feliz aniversário!" nas principais funções *hash*, detalhadas a seguir.

- MD5 (Message Digest 5): gera *hashes* de 128 bits e parou de ser utilizada quando foram publicadas algumas vulnerabilidades nela encontradas.
- SHA-1 (Secure Hash Algorithm-1): gera *hashes* de 160 bits e, embora apresente algumas colisões, ainda é utilizada.
- SHA-2 (Secure Hash Algorithm-2): a família de funções SHA-2 inclui funções SHA-224, SHA-256, SHA-384 e SHA-512, que fornecem *hashes* de 224, 256, 384 e 512 bits, respectivamente. As funções *hash* mais utilizadas na *blockchain* são SHA-256.

Na *blockchain*, as funções criptográficas de *hash* podem ser usadas para:

- resolver quebra-cabeças criptográficos, ou seja, a prova de trabalho (PoW, do inglês *proof of work*) em *bitcoin*;
- gerar endereços para chaves públicas e privadas;
- reduzir o tamanho de endereços públicos;
- resumir mensagens em assinaturas.

## *Saiba mais*

A PoW serve para evitar comportamentos indesejados em uma rede, como ataques de negação de serviço (DoS, do inglês *denial of service*). Trata-se de um protocolo que funciona exigindo que o cliente execute ações, geralmente operações computacionais complexas (como o *captcha*, por exemplo). Assim que a ação é executada, ela é verificada pela rede. Se o desempenho do cliente for aprovado, os acessos solicitados por ele serão permitidos.

A Figura 5 mostra a estrutura básica de uma *blockchain*. Como ela é uma maneira de encapsular transações em forma de blocos, é por meio de *hash* criptográfico que esses blocos são vinculados, formando uma cadeia de blocos. Cada bloco tem um *hash* exclusivo, ou seja, sempre único e responsável por identificar um bloco e todo o seu conteúdo. Dessa forma, quando um bloco é criado, qualquer mudança ocorrida dentro dele fará com que o *hash* também mude.

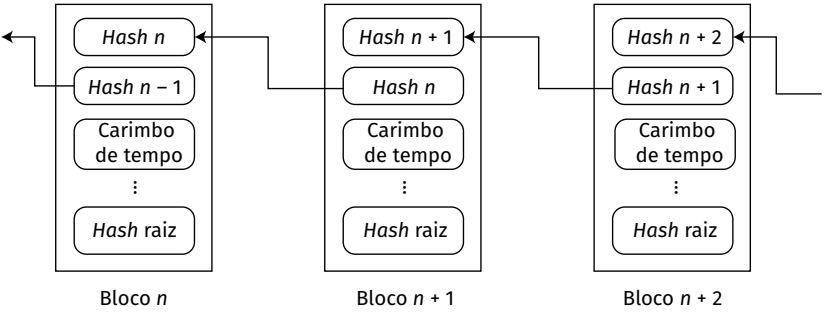


**Figura 5.** Estrutura básica de uma *blockchain*.
**Fonte:** Adaptada de Mohamed (2020).

## Assinaturas digitais

Assim como a assinatura manuscrita, a assinatura digital visa a garantir a autoria de um documento a fim de evitar falsificações, podendo ser realizada mediante um certificado digital. Esse pode ser considerado o protocolo criptográfico mais utilizado atualmente.

Uma assinatura digital é um esquema matemático baseado em criptografia de chave pública, que produz códigos curtos, chamados "assinaturas de mensagens digitais", pelo uso de uma chave privada. Assim, essas assinaturas são verificáveis usando-se a chave pública correspondente.

Na *blockchain*, usa-se o esquema de assinatura para assinar transações, com o objetivo de autenticar o remetente e garantir a integridade da transação. A Figura 6 apresenta um exemplo do processo de criação de uma transação ou de um bloco assinado digitalmente por um usuário (signatário) da *blockchain*, utilizando sua chave privada.

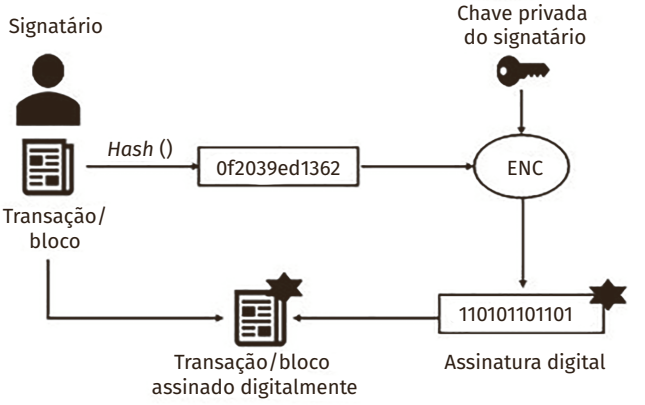


**Figura 6.** Processo de assinatura de transação/bloco.
**Fonte:** Adaptada de Raikwar, Gligoroski e Kralevska (2019).

A Figura 7 ilustra como os outros nós (verificador) da *blockchain* verificam a autenticidade da assinatura utilizando a chave pública do signatário.

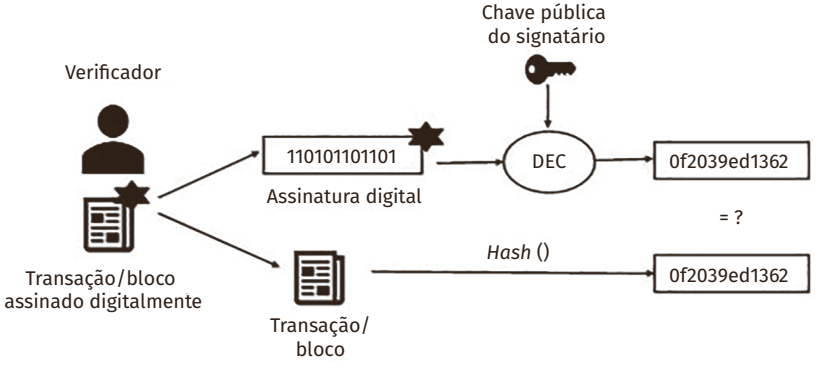


**Figura 7.** Verificação de assinatura da transação/bloco.
**Fonte:** Adaptada de Raikwar, Gligoroski e Kralevska (2019).

Conheça a seguir os diferentes métodos de assinatura utilizados na *blockchain* para adicionar recursos como privacidade, anonimato e desvinculação.

- Assinatura múltipla: uma única mensagem é assinada por um grupo de usuários.
- Assinatura cega: signatários e autores das transações são partes diferentes, fornecendo anonimato e desvinculação.
- Assinatura de anel: uma assinatura é criada por qualquer membro de um grupo, preservando a identidade do signatário individual.
- Assinatura de limite: quando *n* partes recebem uma parte da chave secreta, permitindo a criação da assinatura *t* sobre qualquer mensagem.

Na próxima seção, vamos apresentar exemplos de aplicação da criptografia em *blockchain*.

## Criptografia aplicada a *blockchain*

Nas seções anteriores, você pôde compreender o que é *blockchain*, criptografia e os principais conceitos criptográficos usados nessa integração. Para facilitar o entendimento da aplicação da criptografia nesse processo, a seguir vamos exemplificar o funcionamento da *blockchain*.

As criptomoedas estão em alta, sendo hoje usadas em diversas transações. Seu próprio nome nos indica que se trata de moedas digitais protegidas por criptografia, o que torna quase impossível sua falsificação. Baseadas na tecnologia *blockchain*, as criptomoedas são sistemas que permitem a realização segura de pagamentos *on-line*, dispondo de diversos algoritmos de criptografia e técnicas criptográficas que protegem essas entradas.

Uma das criptomoedas mais populares é o *bitcoin*, que foi a primeira criptomoeda baseada em *blockchain*. Chaves assimétricas e assinaturas digitais são responsáveis por definir a propriedade de um *bitcoin*. O endereço *bitcoin* usado como receptor na transferência de propriedade é criado por uma chave pública, que é criada a partir de uma chave privada. Normalmente essas chaves são criadas por *software* específico, chamados, de forma genérica, de *wallets* (carteiras), que não dependem nem do protocolo *bitcoin*, nem da internet. Sendo assim, não é necessário que as chaves sejam armazenadas na rede, e, então, a segurança *bitcoin* depende de como os usuários protegem suas chaves privadas.

A Figura 8 mostra genericamente como um endereço *bitcoin* é gerado. Como se pode observar, primeiramente é gerada uma chave privada, que só pode ser vista pelo proprietário. A partir dela, ocorre a transformação algorítmica, gerando a chave pública. Esta, então, por meio das funções *hash*, geram o endereço do *bitcoin*, que é público, ou seja, pode ser visto por todos. Convém salientar que um *bitcoin* não armazena moedas digitais, como se pode ver, mas, sim, as chaves que permitem seu uso.

**Figura 8.** Endereço *bitcoin*.

Veja na Figura 9 um exemplo do funcionamento da *blockchain* e da integração com as demais tecnologias, inclusive a criptografia.

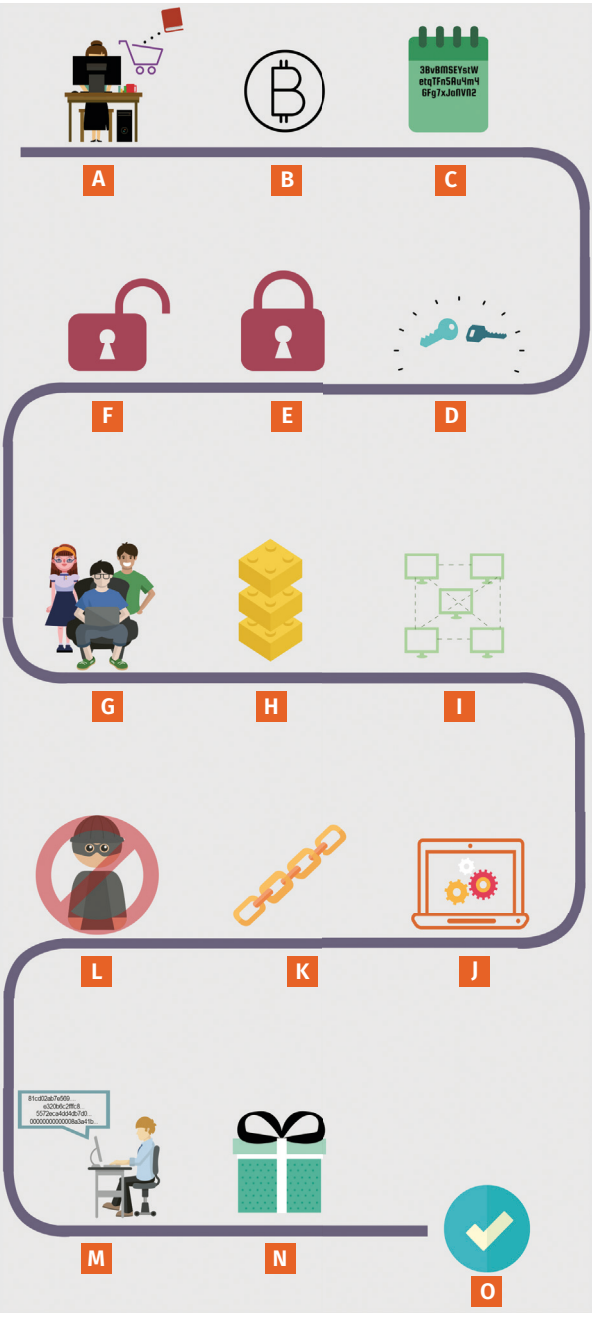


**Figura 9.** Exemplo de funcionamento *blockchain*.
**Fonte:** Adaptada de Al-Housni (2019).

A seguir são descritas as etapas de uma transação de *bitcoin*, ilustradas na Figura 9.

a) A usuária está realizando uma compra *on-line*, e a loja em questão aceita pagamento em *bitcoin*.
b) A usuária, que já tem uma carteira *bitcoin*, escolhe usar essa criptomoeda como forma de pagamento pelo produto desejado.
c) A loja envia à usuária seu endereço *bitcoin* (uma cadeia de 26 a 35 caracteres).
d) Os endereços costumam ser diferentes para cada transação, de modo a garantir a privacidade. Um endereço está vinculado a uma chave privada e a uma chave pública.
e) A usuária envia o pagamento para o endereço da loja. Ela assina a transação com a chave privada de seu próprio endereço (criada para essa determinada transação) e adiciona sua própria chave pública à transação.
f) Assim que é iniciada, a transação se propaga ponto a ponto em uma rede distribuída para todos os participantes. Com a chave pública, qualquer pessoa pode verificar a transação.
g) Os mineiros entram em jogo para garantir a autenticidade e a validação das transações, já que não existe uma autoridade central para esses fins. Assim, a transação é transmitida na forma de mensagem digital utilizando algoritmo criptográfico, e os mineiros validam as transações por meio da rede de trabalho. Essa autenticação ocorre mediante assinatura digital, que prova a propriedade do documento.
h) Após a verificação das transações, elas são registradas em blocos. A *blockchain* é a realização de um livro-razão público.
i) A *blockchain* é compartilhada em tempo real nos computadores dos mineiros e armazena o registro de todas as transações de *bitcoin* confirmadas.
j) Os computadores dos mineiros criam *hashes* criptográficos (sequências de letras e números) para armazenar uma transação na *blockchain*.
k) Todos os blocos são ligados entre si, e cada um deles contém os *hashes* dos blocos anteriores e atuais e, ainda, um "nonce" (um número aleatório).
l) A cada 10 minutos, é criado um novo bloco. Isso significa que, se um bloco gravado fosse modificado, seria necessário modificar todos os blocos seguintes, o que é quase impossível.

m) Um *hash* deve seguir um determinado parâmetro (iniciando com vários zeros). Assim, muitos *hashes* são gerados por parte dos mineiros até que seja encontrado um bem-sucedido.
n) O mineiro que encontra o *hash* correto é recompensado com *bitcoins*.
o) Por fim, a transação é concluída com sucesso e adicionada ao livro-razão. Seu saldo é atualizado na carteira *bitcoin*.

Com esse exemplo, é possível compreender todo o processo da *blockchain* e identificar onde a criptografia e as funções criptográficas se encaixam nessa questão, sendo elas indispensáveis para garantir a segurança dessa tecnologia. Cada vez mais as *blockchains* estão ganhando espaço no mercado, não apenas em moedas criptográficas, mas também em diversas outras áreas, o que se deve à segurança que esse banco de dados distribuído garante.

## Referências

AL-HOUSNI, N. *An exploratory study in blockchain technology*. 2019. 88 f. Dissertação (Mestrado) — School of Computer Science, University of Manchester, Manchester, 2019.

AUMASSON, J. P. *Serious cryptography*: a practical introduction to modern encryption. San Francisco: No Starch Press, 2018.

BASHIR, I. *Mastering blockchain*: deeper insights into decentralization, cryptography, bitcoin, and popular blockchain frameworks. Birmingham: Packt Publishing, 2017.

DRESCHER, D. *Blockchain basics*: a non-technical introduction in 25 steps. Frankfurt: Apress, 2017.

GAYOSO MARTÍNEZ, V.; HERNÁNDEZ-ÁLVAREZ, L.; HERNÁNDEZ ENCINAS, L. Analysis of the cryptographic tools for blockchain and bitcoin. *Mathematics*, v. 8, n. 131, 2020.

GUPTA, M. *Blockchan for dummies*: IBM limited edition. Hoboken: John Wiley & Sons, 2017.

MOHAMED, K. S. *New frontiers in cryptography*: quantum, blockchain, lightweight, chaotic and DNA. Cham: Springer, 2020.

MOUGAYAR, W. *The business blockchain*: promise, practice, and application of the next internet technology. New Jersey: John Wiley & Sons, 2016.

RAIKWAR, M.; GLIGOROSKI, D.; KRALEVSKA, K. Sok of used cryptography in blockchain. *IEEE Access*, v. 7, p. 148550-148575, 2019.

VALLIM, A. P. A. *Forense computacional e criptografia*. São Paulo: Senac, 2019.

# Curvas elípticas aplicadas a *blockchain*

*José Eugênio de Mira*

**OBJETIVOS DE APRENDIZAGEM**

- Conceituar curvas elípticas com *blockchain*.
- Integrar curvas elípticas com *blockchain*.
- Apresentar exemplos de curvas elípticas com *blockchain*.

## Introdução

Em tecnologia, algumas soluções são tão fantásticas, que à primeira vista podem parecer uma espécie de mágica. Sistemas criptográficos complexos permitem a codificação de informações sensíveis, como dados médicos e informações bancárias, que são enviadas de um lado ao outro do globo por meio de conexões que na maioria das vezes não são seguras. Isso é possível graças a processos matemáticos reversíveis, que, utilizando processamento computacional pesado, convertem esses dados em sequências que não podem ser revertidas sem determinadas informações privadas, as chaves.

Na *blockchain*, o uso de chaves privadas é o que protege as informações que são adicionadas como registros em um determinado endereço. Dessa maneira, o endereço, que é público, pode receber registros, mas, para enviar tais registros para outro endereço, é preciso utilizar a chave privada associada a esse endereço. Aqui você vai conhecer o processo de criação dessa chave,

com a matemática envolvida no processo e na sua irreversibilidade, graças ao uso da criptografia de curva elíptica (ECC, do inglês *elliptic curve cryptography*).

Neste capítulo, você poderá compreender melhor a importância das curvas elípticas para a criptografia de chave pública e, consequentemente, para a *blockchain*. Também vamos descrever como as características únicas dessa curva algébrica são utilizadas para criar chaves menores e tão seguras quanto as geradas por algoritmos como o RSA. Por fim, você vai ver como essas curvas são usadas para gerar as chaves privadas a partir dos endereços da *blockchain*.

## Conceituando ECC: chave e endereço

Um dos dados pessoais mais solicitados em formulários é o endereço, que será usado, por exemplo, para o envio de correspondências, quando necessário. Mesmo tendo o seu endereço revelado nessas situações, as pessoas ainda têm a segurança de suas residências garantida por portas e/ou portões protegidos por uma fechadura, que só pode ser aberta por uma chave específica. Da mesma maneira, quando uma transação é realizada em uma *blockchain*, usa-se um endereço, que é público e permite que *tokens* sejam enviados e alterações sejam feitas na *blockchain* pelo proprietário do endereço. A fim de impedir que qualquer pessoa realize essas alterações, é requerida uma chave, de modo que apenas o proprietário do endereço possa ter acesso a ele. Essa tecnologia é chamada "criptografia de chave pública", ou "criptografia assimétrica", em que uma parte da criptografia é o endereço, que é público, e a outra é a chave, que é privada.

A principal característica desse tipo de criptografia é que a chave privada é utilizada para realizar o processo de descriptografia, mas não é necessária no processo criptográfico. Como analogia, podemos pensar em nossas caixas de correspondência. Qualquer pessoa que conhecer nosso endereço poderá enviar algo para elas, mas, para a retirada das correspondências, será preciso utilizar a chave (Figura 1). Trata-se de um processo de via única, obtido por meio da matemática.

Qualquer um pode enviar para seu endereço, pois ele é público.

Porém, sua caixa de correio é protegida por uma chave.

Embora todos possam entregar, apenas quem tem a chave pode receber.

**Figura 1.** Uma caixa de correio é pública, mas é segura.

## Chave pública e chave privada

Algoritmos de chave pública utilizam operações matemáticas complexas e reversíveis, desde que uma parte dos elementos da equação seja conhecida. Whitfield Diffie e Martin Hellman foram os primeiros a propor um sistema eficiente de uso de chaves públicas para resolver o problema de distribuição de chaves. Inspirados por eles, Ronald Rivest, Adi Shamir e Len Adleman, professores do MIT, criaram então o algoritmo RSA (ZOCHIO, 2016).

A segurança do RSA depende da dificuldade para fatorar números grandes e dos números primos escolhidos para a criação das chaves, que também devem ser grandes, utilizando as propriedades da aritmética modular. A forma mais óbvia de atacar o RSA é encontrar um método de fatoração rápido que consiga descobrir os fatores primos do número usado como chave, o que, com a computação tradicional, ainda é algo extremamente complexo.

Já o algoritmo El Gamal, desenvolvido pelo criptógrafo Taher Elgamal (1985), utiliza igualmente a propriedade do logaritmo discreto para permitir o envio de um texto ilegível através de um canal inseguro, com uma adição interessante: o uso de um nonce (acrônimo para *number used once*, ou, em português, número usado uma vez). Isso porque o algoritmo El Gamal publica uma parte da chave, e apenas uma parte é mantida secreta. Para isso, o El Gamal usa alguns números específicos:

- $p$ é um número primo relativamente longo;
- $g$ é um inteiro relativamente primo de $n$, sua raiz primitiva, que, elevado a algum número $n$, vai produzir o número $p$, sendo, dessa forma, conhecido como "gerador".

Para compreendermos esse processo matemático, vamos pegar como exemplo uma troca de mensagens entre Lucas e Adélia. Acompanhe a seguir.

1. **Lucas gera a chave pública e a chave privada:** Luke escolhe um número muito grande $q$ e um grupo cíclico $Fq$. Do grupo cíclico $Fq$, ele escolhe qualquer elemento $g$ e um elemento $a$ tal que o mínimo divisor comum (mdc) $(a, q) = 1$. Em seguida, ele calcula $h = ga$. Lucas publica $F$, $h = ga$, $q$ e $g$ como sua chave pública e mantém $a$ como chave privada. Observe que, mesmo tendo sido publicados os itens do cálculo, quem receber a chave pública não terá todos os elementos.
2. **Adélia criptografa os dados usando a chave pública de Lucas:** Adélia seleciona um elemento $k$ do grupo cíclico $F$ de modo que o mdc $(k, q) = 1$. Lembre-se que ela tem acesso ao valor de $q$. Em seguida, ela calcula $p = gk$ e $s = hk = gak$, e multiplica $s$ com $M$, que é a mensagem a ser enviada. Feito isso, ela envia para Lucas $(p, M * s) = (gk, M * s)$.
3. **Agora Lucas pode descriptografar a mensagem:** Lucas calcula $s_1 = pa = gak$. Ele divide $M * s$ por $s_1$ para obter $M$ como $s = s_1$, revertendo o processo.

Essa propriedade é importante porque permite o cálculo do módulo (mod), mas não o cálculo do número ao qual $p$ é elevado. Assim, ao publicar a chave pública, o emissor omite a informação do expoente, que é sua chave privada. Dessa maneira, a mensagem original ($M$) é criptografada multiplicando-se $gak$ por ela. Para remover a máscara, uma pista é fornecida na forma de $gk$. A menos que alguém conheça $a$, ele não será capaz de recuperar $M$. Isso ocorre porque é difícil encontrar o logaritmo discreto em um grupo cíclico, e simplesmente conhecer $ga$ e $gk$ não é bom o suficiente para calcular $gak$.

## *Fique atento*

A segurança do sistema de chave pública e chave privada reside na dificuldade computacional de se calcular o valor de $a$ sabendo-se apenas os valores dos elementos $g$ e $p$. Quando $g$ e $p$ são muito longos, essa resolução se torna inviável, o que em matemática é chamado "problema do logaritmo discreto" (PLD).

## PLD e a integração de curvas elípticas na *blockchain*

Embora eficiente, a proposta de uso de módulo para a geração de chaves públicas e privadas tem um problema intrínseco, que é a capacidade computacional necessária para esse processo. Mesmo atualmente, o uso do RSA na criptografia de grandes blocos de dados poderia ser inviável. Durante a década de 1980, no entanto, Neal Koblitz (1987) e Victor Miller (1986) apresentaram, de forma independente, uma solução elegante para esse problema, utilizando a trigonometria em vez da álgebra como ponto de partida para um sistema criptográfico baseado em pontos em um gráfico de curvas elípticas. O sistema, além de tão seguro quanto o método RSA, permite a criação de chaves privadas menores.

De fato, parte do sucesso da *blockchain* e, consequentemente, do *bitcoin* e das demais criptomoedas se deve à possibilidade de uso dessa chave, que pode ser armazenada em forma de um código QR, ou mesmo por meio de um conjunto de palavras, as *seeds*. Assim, o sistema mantém a segurança, mas com a possibilidade de se obter a chave a partir de um processo computacional mais limitado, e com uma largura de chave menor.

A segurança desse método, conforme Lara e Oliveira (2007, documento *on-line*), "[...] está, mais uma vez, baseada no PLD. Esse criptossistema exige uma chave de comprimento consideravelmente menor que a chave usada em alguns clássicos da criptografia assimétrica, tais como o RSA, no entanto com segurança equivalente". A aplicação do conceito de curvas elípticas para a geração de chaves baseia-se no lugar onde determinados pontos estarão em um gráfico cartesiano, e, a partir daí, é possível saber a posição de um terceiro ponto.

Uma das propriedades singulares de uma curva elíptica, ainda segundo Lara e Oliveira (2007), consiste no fato de que os pontos que a compõem formam uma estrutura de grupo. Assim, uma curva elíptica é formada por dois pontos que satisfazem a equação $y^2 = x^3 + ax + b$ e mais um ponto no infinito.

### *Saiba mais*

Parte fundamental da segurança da *blockchain*, usada para a negociação de milhões de dólares, baseia-se na inviolabilidade da sua chave privada e no seu tamanho, que é relativamente curto dada a sua importância. Essas chaves privadas são normalmente armazenadas de três formas, apresentadas a seguir.

- Nas chamadas *paper wallets*, ou carteiras de papel, a chave é um código QR impresso, que, ao ser lido por um aplicativo de carteira (*wallet*), permite ao proprietário a obtenção imediata do controle do endereço e dos seus valores (registros).
- Nas carteiras de *node* completo, ou *wallets* baseadas em *hardware*, essa chave é um arquivo de 256 bits, armazenado na raiz do dispositivo ou em uma pasta protegida. Têm-se tornado comuns as notícias de pessoas que perdem esses dispositivos e, com a atual alta no valor de algumas criptomoedas, tentam recuperá-las.
- Outra forma de se guardar uma chave, sendo essa maneira considerada a mais segura, é por meio da memorização de uma *seed*, ou seja, uma semente geradora, ou um conjunto de palavras específicas que, ao ser utilizado em um *node* ou uma *wallet*, é convertido em chave privada. A vantagem desse sistema é que ele é à prova de furto, pois está apenas na mente do dono da chave. A principal desvantagem é que, uma vez esquecido, será impossível recuperá-lo.

## Campos finitos e segurança

Existem basicamente duas maneiras de se quebrar um sistema criptográfico baseado em um problema matemático, como são as curvas elípticas que usamos na *blockchain*: algoritmos específicos e algoritmos de uso geral. Algoritmos específicos são aqueles desenvolvidos para se resolver uma situação matemática conhecida, como é o caso das curvas supersingulares e anômalas. Já os algoritmos de uso genérico, como se pode esperar, têm um tempo de execução muito maior quando comparados com os de uso específico e, no nosso caso, não são eficientes. Isso porque o tempo que um algoritmo desses levaria para solucionar o problema é tão grande, que é inviável, pois apresenta tempo polinomial, ou seja, seu tempo de execução varia em função do tamanho da entrada. Em ciência da computação, chamamos isso de "complexidade de tempo".

Para a resolução do PLD original, como o usado no RSA, a chave, para ser segura, deve ter pelo menos 1.024 bits de comprimento. Porém, o algoritmo mais utilizado para esse tipo de resolução, o Pollard-ρ (lê-se "pollard-rho") (KUHN; STRUIK, 2001), tem tempo de execução maior quando se trata do PLD baseado em curvas elípticas. As chaves de 160 bits já são seguras dessa forma, mas, ainda assim, na *blockchain* utilizamos chaves de 256 bits. Como poderíamos esperar, algoritmos simétricos exigem chaves muito menores. Podemos ver a relação entre os algoritmos simétricos, a ECC e o RSA no Quadro 1.

**Quadro 1.** Tamanho das chaves em bits

| Modelo de criptografia | | | |
|---|---|---|---|
| **Simétrico** | **ECC** | **RSA** | **Razão ECC:RSA** |
| 80 | 163 | 1.024 | 1:6 |
| 128 | 256 | 3.072 | 1:12 |
| 192 | 384 | 7.680 | 1:20 |
| 256 | 512 | 15.360 | 1:30 |

**Fonte:** Adaptado de Lara e Oliveira (2007).

## Utilizando curvas elípticas na *blockchain*

O conceito de confiança em documentos digitais baseia-se na premissa de cálculos matemáticos tão grandes e complexos, que somente quem estiver de posse de todos os dados originais poderia prever exatamente seu resultado. Assim, ao usar o PLD, é possível que um cálculo realizado previamente com um determinado número e seu módulo forneça um resultado que pode ser obtido utilizando-se uma parte dos números usados nesse cálculo. Esse é o princípio por trás dos algoritmos de chave pública e chave privada, como o RSA e o El Gamal, e na *blockchain* ele é utilizado para garantir o acesso aos blocos de dados e permitir registros.

Além disso, a função de *hash* é utilizada no processo de criação das cadeias que compõem a *blockchain*, garantindo a irreversibilidade do processo de criação. O *hash* é uma validação utilizada no processo de geração do *bitcoin*, uma criptomoeda gerada a partir da criação do processo de mineração, que é o nome dado à criação das chaves públicas e privadas que vão garantir o acesso à escrita no bloco. Diferentemente do RSA, no entanto, a *blockchain* utiliza um sistema de chaves públicas e privadas baseadas em uma função que se aproveita das propriedades da teoria das curvas elípticas. Uma curva elíptica é, por definição, uma curva algébrica não linear, o que significa que ela não tem pontas agudas (cúspides) ou intersecções. Geradas a partir de uma função matemática, elas têm propriedades de multiplicação e de soma, de forma que uma reta traçada sobre essa curva fará intersecções com ela em pontos específicos. Observe na Figura 2 uma curva elíptica gerada a partir da função $y^2 = x^3 - 3x + 7$.

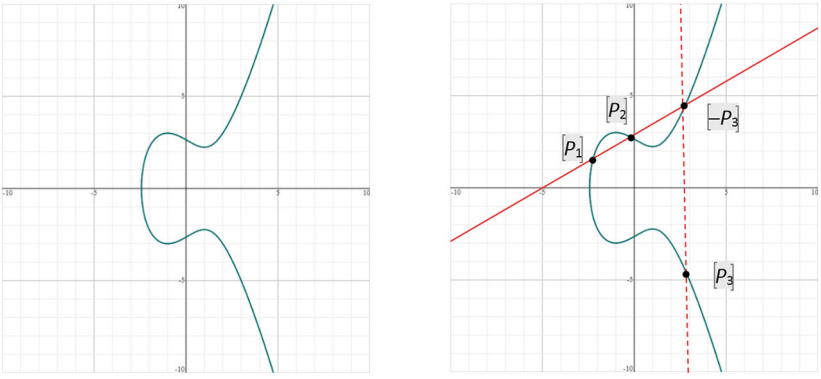


**Figura 2.** Curva elíptica de uma função.

Os pontos traçados na reta $P_1$ e $P_2$, desde que não tenham o mesmo valor em x, determinam o próximo ponto, chamado de $-P_3$. Uma reta paralela ao eixo y define o ponto $P_3$, onde $P_1 + P_2 = P_3$. Qualquer ponto nesse gráfico pode ser definido como uma soma de *P*, onde $kP = P + P + P$ (repetido por *k* vezes). Um sistema de chave pública e privada baseada nas curvas elípticas gera um gráfico de pontos, em que as informações sobre as intersecções desses pontos não são conhecidas, mas a função o é (TERADA, 2008). Dessa maneira, é possível utilizar a propriedade de reversibilidade da operação em sentido único. A chave privada é, portanto, um número de forma imprevisível, e a chave pública é obtida a partir dela e da multiplicação do chamado "ponto base". Esse algoritmo é conhecido como "algoritmo de assinatura digital de curvas elípticas" (ECDSA, do inglês *elliptic curve digital signature algorithm*), e é o sistema criptográfico de chave pública por trás da proteção dos dados armazenados na *blockchain* (RYKWALDER, 2020). Uma transação, ou seja, a movimentação de valores por meio da cadeia da *blockchain*, só é possível para quem tem a chave privada desse bloco. Já a chave pública é utilizada como endereço para o envio de valores por meio do bloco.

## Assinatura e verificação

O ECDSA funciona em dois modos diferentes: um modo de verificação e outro de assinatura. Para a transferência dos dados, ele funciona fazendo a verificação, analisando um endereço e enviando para ele os registros (fundos). Porém, para permitir que os fundos saiam de um endereço, ele funciona realizando

uma verificação da assinatura, ou seja, analisando se a assinatura utilizada realmente foi gerada a partir daquele endereço, ou, em linguagem algébrica, se aquele ponto específico realmente está presente naquela curva elíptica gerada de acordo com os pontos anteriores. Como aprendemos anteriormente, em um sistema de criptografia de chave pública, conhecer o elemento gerador é suficiente para saber sua validade, mas somente quem conhece todos os valores pode ter acesso à assinatura.

### *Exemplo*

Suponha que temos de calcular seis pontos em um gráfico de curva elíptica. A forma mais fácil de fazer isso seria $P + P + P + P + P + P$, correto? Porém, do ponto de vista computacional, a maneira mais fácil é simplificar essas operações. Assim, usando as propriedades algébricas, podemos dizer que $n * P + r * P = (n * r) * P$. Desse modo, calculamos que $P + P = 2 * P$ e que $2 * P + 2 * P = 4 * P$ e $2 * P + 4 * P = 6 * P$, em apenas seis operações.

Parece simples, não? No entanto, a curva elíptica utilizada na *blockchain* usa um valor de *x* que é um número randômico de até 256 bits de comprimento, cujo valor máximo é 115792089237316195423570985008687907853269984665640564039457584007913129639935, aproximadamente 1.1579 × 1077. Para calcular o ponto no gráfico, faremos até 510 adições de pontos. Isso porque, além de computar a série, também teremos de calcular a expansão binária de *x*, o que chegará no máximo a 256 elementos. Ou seja, nunca teremos de adicionar mais do que 256 pontos nessa etapa, o que nos deixa com um máximo de 255 + 255 operações, isto é, 510.

No ECDSA, o algoritmo usa algumas variáveis fundamentais para obter a assinatura e o processo reverso:

- *r* e *s* representam a assinatura;
- *z* representa o *hash* da mensagem que se deseja assinar — como na *blockchain* do *bitcoin* usamos uma chave que tem o mesmo tamanho do *hash N* (gerado por meio do SHA256), *z* tem sempre o mesmo tamanho de *N* (no caso, 256 bits);
- *k* é um número randômico, que, no caso das *paper wallets*, é gerado por meio de um movimento aleatório do *mouse*, por exemplo;
- $d_a$ e $Q_A$ são, respectivamente, o número da chave privada e o número da chave pública.

As curvas elípticas usadas na *blockchain* do *bitcoin*, do *ethereum* e de outras criptomoedas famosas são chamadas de "secp256k1", e a sua equação corresponde a $y^2 = x^3 + 7$. No *white paper* que descreve o *bitcoin*, não existe uma razão específica para que essa seja a curva utilizada. Embora continuemos aqui empregando o nome "curva", como vamos aplicar isso em uma estrutura de campos finitos, essa equação será transformada de maneira que todos os pontos estejam distribuídos dentro de uma mesma matriz (os tais campos finitos), conforme explica Rykwalder (2020), um dos mais proeminentes desenvolvedores e conhecidos colaboradores da área de criptomoedas e *blockchains*. Isso garante que o maior número primo utilizado como gerador seja menor que 2 elevados a 256. A partir daí, a curva elíptica passará a se parecer com um jogo de campos minados, com pontos distribuídos de forma quase aleatória. Mas, na verdade, esses pontos ainda obedecem à lógica da curva, e, portanto, podemos traçar uma reta entre eles, assim como fizemos anteriormente (Figura 3).

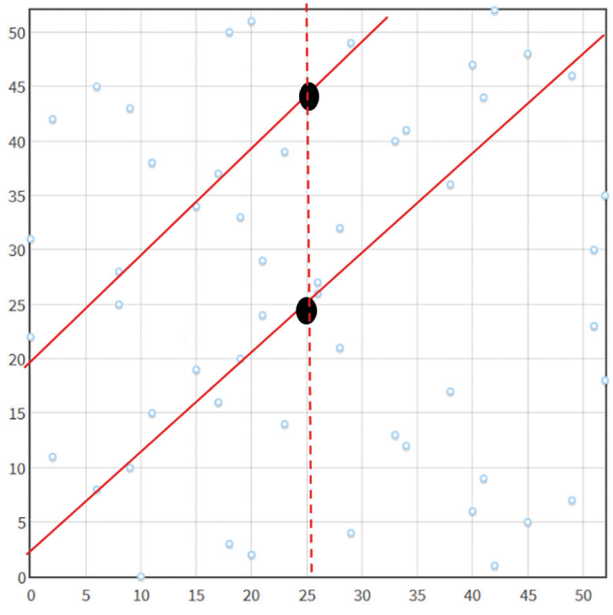


**Figura 3.** Exemplo de uma curva elíptica traçada em um gráfico finito de módulo 55.

O algoritmo de assinatura calcula o par $r$ e $s$ a partir de $d_a$ e $z$. A partir daí, ele obtém o grupo da curva $n$ e gera um nonce $k$ de forma randômica e segura. Esse número não pode ser reutilizado, e não é o mesmo nonce usado no processo de mineração.

Calcula-se $(x, y) = k * G$, onde $G$ é o gerador da curva. Então, calcula-se $r = x \bmod n$. Se for igual a 0, começa-se com um novo número $k$ randômico. Por fim, calcula-se $s = k^{-1}(z + r * d_a) \bmod n$.

Para o cálculo da verificação, não usamos a chave pública $d_a$, mas garante-se que os pares $r$ e $s$ e $Q_A$ e $z$ sejam consistentes. Calcula-se $u_1 = z * s - 1^{-1}$ e $u_2 = r * s^{-1} \bmod n$, e, depois, calcula-se $(x, y) = u_1 * G + u_2 * Q_A$ e verifica-se se isso não é igual a um ponto no infinito, o que significaria que os dois pontos não estão na mesma curva. Após essa verificação, se $r = x \bmod n$, então a assinatura é válida e a transação é efetivada. Caso contrário, a assinatura é inválida. Lembre-se que esse processo não é como uma senha, que é utilizada toda vez que se usa o aplicativo, e sim um acesso permanente, que fornece o controle de todos os valores (registros) em um determinado endereço da *blockchain*. Tanto esse endereço quanto a chave privada são imutáveis, e, então, uma vez comprometidos, não podem ser recuperados.

Embora a explicação seja extensa, a lógica por trás disso é simples. Como temos um número muito longo sobre o qual muitas operações são feitas, a partir do resultado dessas operações e de alguns elementos conseguimos saber se a equação está correta, mas não conseguimos saber qual é o valor de todos os elementos da equação. Quando se fala que o número $3 + x = n$ e que $n$ dividido por 2 tem resto 0, pode-se afirmar com certeza que $x$ é um número inteiro e ímpar, mas não se pode dizer qual é o seu valor. Da mesma maneira, quando se fala que $3 + x' = n * 2$ e que $n$ vale 5, pode-se afirmar que o resto é 0 e que $x'$ é igual a 7. O que temos, na prática, são equações com elementos inteligentemente escolhidos para que, dependendo de qual seja o elemento dessa equação a que temos acesso, podemos ou não conhecer o resto da equação e/ou seus valores.

Neste capítulo, você pôde compreender que os criptossistemas baseados em ECC são extremamente seguros, uma vez que a capacidade computacional de que dispomos atualmente está longe de ser suficiente para quebrá-los. Além disso, pudemos verificar que as transferências de valores de forma irreversível e transparente por meio de uma rede descentralizada de *software* que utiliza um algoritmo de verificação não é nenhuma magia; trata-se de pura matemática aplicada.

# Referências

ELGAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, v. 31, n. 4, p. 469-472, Jul. 1985.

KOBLITZ, N. Elliptic curve cryptosystems. *Mathematics of Computacion*, v. 48, n. 177, p. 203-209, 1987.

KUHN, F.; STRUIK, R. Extensions of pollard's rho algorithm for computing multiple discrete logarithms. *In*: ANNUAL INTERNATIONAL WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY, 8th, 2001, Toronto. *Revised papers*. London: International Workshop on Selected Areas in Cryptography, 2001. p. 212–229.

LARA, P. C. S.; OLIVEIRA, F. B. Curvas elípticas: aplicação em criptografia assimétrica. *In*: REUNIÃO ANUAL DA SBPC, 59., 2007; JORNADA NACIONAL DE INICIAÇÃO CIENTÍFICA, 14., 2007, Belém. *Anais* [...]. São Paulo: SBPC, 2007. Disponível em: https://www.lncc.br/~borges/doc/Curvas%20Elipticas%20-%20Aplicacao%20em%20Criptografia%20Assimetrica.pdf. Acesso em: 27 nov. 2021.

MILLER, V. S. Use of elliptic curves in cryptography. *In*: WILLIAMS, H.C. (ed.). *Advances in cryptology*: CRYPTO '85: lecture notes in computer science. Berlin: Springer, 1986. v. 218, p. 417-426.

RYKWALDER, E. A matemática por trás do Bitcoin: CoinDesk. *Bitcoin on Air*, 2020. Disponível em: https://pt.bitcoinonair.com/math-behind-bitcoin. Acesso em: 27 nov. 2021.

TERADA, R. *Segurança de dados*: criptografia em redes. 2. ed. São Paulo: Blucher, 2008.

ZOCHIO, M. F. *Introdução à criptografia*. São Paulo: Novatec, 2016.

# Leituras recomendadas

KNUTSON, H. What is the math behind elliptic curve cryptography? *Hackernoon.com*, 2018. Disponível em: https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3. Acesso em: 27 nov. 2021.

STALLINGS, W. *Criptografia e segurança de redes*. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

## *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

# Funções *hash* aplicadas a *blockchain*

*Thaís Bison*

**OBJETIVOS DE APRENDIZAGEM**

- Conceituar funções *hash* com *blockchain*.
- Integrar funções *hash* com *blockchain*.
- Apresentar exemplos de funções *hash* com *blockchain*.

## Introdução

Nos últimos anos, muito tem-se ouvido sobre criptomoedas e a sua tecnologia *blockchain*. Em suma, a *blockchain* dispõe de uma arquitetura segura, estruturada por meio de blocos criptográficos, registro de *data* e metadados no geral. Inicialmente, essa tecnologia foi aplicada ao setor financeiro, trazendo um novo sistema de investimento e negócio, as criptomoedas, por meio do *bitcoin*. Com o passar dos anos, outras soluções foram surgindo, como a Ethereum, na qual, por meio de *smart contracts*, permitiu-se a criação de ferramentas para diversos tipos de negócios.

Neste capítulo, você vai estudar o conceito da *blockchain* e das *hashes*, utilizadas nessas tecnologias, aprendendo a integração entre as duas e exemplos de onde são utilizadas.

# Conceito

## *Blockchain*

A *blockchain* é uma cadeia de registros imutáveis, públicos e distribuídos:

- **cadeia** porque os registros estão cuidadosamente encadeados uns aos outros por meio de chaves públicas, entradas e saídas;
- **imutáveis** porque, uma vez que o registro é inserido na cadeia, ele não pode mais ser alterado.
- **públicos** porque a única condição necessária para que um cidadão tenha acesso aos registros do *blockchain* é que ele acesse a internet.
- **distribuídos** porque essa cadeia de registro não está armazenada em um único servidor central, ao contrário, está replicada em milhões de máquinas distribuídas pelo mundo todo, e nenhuma empresa ou indivíduo pode reivindicar a propriedade desses registros.

A *blockchain* está estruturada na forma de blocos encadeados. Cada bloco tem uma área de transações e uma área de cabeçalho (Figura 1).

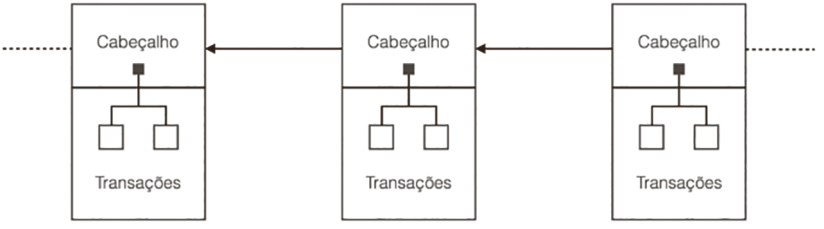


**Figura 1.** Cadeia de blocos da *blockchain*.
**Fonte:** Adaptada de Okupski (2014).

Na área de transações estão todas as transações coletadas por aquele bloco. Na área de cabeçalho se encontram a *hash* do cabeçalho do bloco anterior e a raiz da árvore de Merkle das transações presentes no campo de transações. Dessa forma, cada bloco está ligado ao bloco anterior, formando uma cadeia de blocos, e cada transação está representada no cabeçalho por meio da raiz da árvore de Merkle em que foi coletada (NARAYANAN *et al.*, 2016).

É interessante notar que a propriedade de imutabilidade da *blockchain* e boa parte de sua segurança derivam-se da estrutura encadeada dos blocos. Como cada bloco contém em seu cabeçalho a *hash* do cabeçalho do bloco anterior, para se alterar um bloco da cadeia é necessário alterar todos os blocos posteriores, o que exige uma capacidade de processamento absurda, uma vez que novos blocos estão sendo constantemente adicionados por outros nós. A utilização da árvore de Merkle permite detectar as mudanças nas transações, uma vez que qualquer alteração nas transações do bloco resulta em uma alteração na raiz da árvore de Merkle inserida no cabeçalho do bloco. Assim, a dificuldade para se alterar um registro da *blockchain* cresce à medida que novos nós são adicionados à rede (OKUPSKI, 2014).

Não apenas os blocos estão encadeados na *blockchain*, mas também as transações. O Quadro 1 apresenta os campos que compõem uma transação.

**Quadro 1.** Descrição dos campos de uma transação

| Campo | Descrição |
|---|---|
| Metadados | Informações da transação como ID e tamanho. |
| Entradas | Vetor com informações de cada entrada da transação. |
| Saídas | Vetor com informações de cada saída da transação. |

**Fonte:** Adaptado de Okupski (2014).

O campo Metadados reúne informações gerais da transação, como o tamanho da transação em bytes, a quantidade de entradas e saídas, a versão do protocolo e o ID da transação, obtido a partir do cálculo de sua *hash* SHA256.

O campo Entradas apresenta uma lista numerada de entradas dessa transação. Cada entrada de uma transação deve fazer referência à saída de outra. Logo, nesse campo há uma lista de IDs de outros registros e o respectivo número da saída. Essas saídas devem ser computadas como entradas nessa transação. Ainda no campo entrada, são adicionadas uma assinatura digital e uma chave pública, responsáveis por confirmar que aquela transação está autorizada a utilizar as saídas indicadas no campo Entradas.

O campo Saída apresenta uma lista numerada de saídas que devem ser utilizadas como entradas de transações futuras. Esse campo contém, ainda, uma *hash* de chave pública que tem informações que condicionam a utilização dessas saídas por outra transação.

A assinatura digital faz uso da chave privada para criptografar (assinar) uma mensagem e da chave pública para verificar a assinatura. Dessa maneira, ao inserir uma chave pública na saída da transação (ou sua *hash*), apenas o portador da chave privada correspondente estará autorizado a utilizar aquela saída. No processo de validação da transação, a chave pública informada no campo Entrada é comparada com a chave pública previamente inserida na saída. Caso elas sejam diferentes, a transação é considerada inválida e não é propagada para os demais nós da rede. Caso elas sejam iguais, a assinatura informada no campo Entrada é verificada com a chave pública previamente confirmada. Se a assinatura for autêntica, ou seja, se a decriptação com a chave pública revelar a *hash* dos dados da transação, então a transação é validada, replicada para os demais nós da rede e coletada em bloco para mineração. Caso contrário, a transação é descartada.

Quando a transação é validada, ela está pronta para ser coletada por um bloco e passar pelo processo de mineração. Um nó minerador da rede coleta as transações que deseja inserir na *blockchain* dentre todas as transações validadas recebidas, calcula a raiz da árvore de Merkle e passa a executar o algoritmo de prova de trabalho. Uma prova de trabalho é um desafio criptográfico utilizado para garantir que um nó realizou uma certa quantidade de trabalho. O *bitcoin*, em particular, utiliza uma prova de trabalho baseada no modelo de Adam Back (NAKAMOTO, 2008); outras aplicações da *blockchain* utilizam variações desse modelo, mas que tenham os mesmos dois princípios:

- garantir que o nó realizou uma quantidade predefinida de processamento; e
- garantir que a prova entregue é objetivamente verificável.

Tipicamente, uma prova de trabalho é um processo probabilístico, e a probabilidade de sucesso depende da dificuldade estabelecida.

No *bitcoin*, por exemplo, a prova de trabalho é encontrar um valor chamado *nonce* cujo duplo *hash* SHA256 com a raiz de Merkle seja igual ou menor que um parâmetro T. A busca por esse valor é feita por tentativa e erro. Quanto menor o parâmetro T, menor será a probabilidade de sucesso e mais difícil será conseguir realizar a prova de trabalho. Quanto maior o parâmetro T, maior será a probabilidade e mais fácil será encontrar um *nonce* válido. O protocolo do *bitcoin* ajusta o parâmetro T automaticamente a cada 2016 blocos para garantir que as provas de trabalho e, consequentemente, a mineração de um

bloco aconteçam, em média, a cada 10 minutos. Outras *blockchains* ajustam esse parâmetro para que a mineração aconteça em intervalos menores, como, por exemplo, de alguns segundos.

Quando a prova de trabalho é vencida, o nó pode avisar a toda rede que resolveu o desafio e inserir o bloco validado na cadeia de blocos. Ao realizar essa operação, o minerador recebe como recompensa uma quantia na unidade de valor utilizada pela *blockchain*, além da diferença entre o valor de entrada e saída das transações, caso exista.

Quando um bloco é validado, ele é imediatamente publicado na rede para todos os nós adjacentes por meio de uma rede p2p (é utilizado TCP na camada de transporte). Cada um desses nós recebe o novo bloco, verifica se, de fato, se trata de um bloco ainda não recebido (cada bloco tem a sua numeração incremental, também chamada de altura do bloco), adiciona o bloco à sua cópia da *blockchain* e replica aos nós adjacentes. O processo repete-se por toda a rede a fim de que haja consenso entre os nós da rede quanto ao estado da cadeia de blocos.

Caso aconteça de dois nós realizarem a prova de trabalho com uma diferença de tempo pequena, eles propagarão blocos de mesma altura na rede, gerando o que é chamado de corrida de blocos. O protocolo resolve essa questão da seguinte maneira: o maior segmento da cadeia de blocos é o segmento válido — isso é chamado de regra da maior cadeia (*longest chain rule*). Dessa forma, cada nó adiciona blocos recém-criados à cadeia de maior altura até que uma bifurcação da cadeia se torne maior e a outra sequência de blocos seja abandonada, gerando os chamados blocos órfãos. No fim, existe apenas uma cadeia que liga o último bloco validado de volta até o primeiro bloco da cadeia. No caso da *blockchain* do *bitcoin*, esse primeiro bloco é chamado de bloco gênesis.

## Função *hash*

Uma função *hash* é uma função matemática com as seguintes propriedades:

- a entrada pode ser qualquer sequência de caracteres de qualquer tamanho;
- a saída é uma sequência de caracteres de tamanho fixo;
- sua eficiência é computável, ou seja, o tempo de execução da função para uma entrada de n caracteres deve ser O(n).

Essas propriedades definem uma função *hash* de maneira geral, suficientes para construir uma tabela *hash*. No entanto, há mais duas propriedades normalmente desejadas em uma função *hash*, ou propriedades que caracterizam uma função *hash* criptográfica (NARAYANAN *et al.*, 2016). São elas:

- ser resistente a colisões;
- ser antirreversão.

Uma colisão acontece quando duas ou mais entradas diferentes produzem a mesmo *hash* de saída (Figura 2).

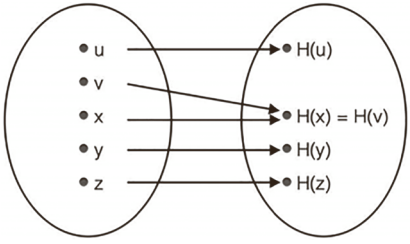


**Figura 2.** Colisão em uma função *hash*.
**Fonte:** Adaptada de Narayanan *et al*. (2016).

Ser resistente a colisões significa que a probabilidade de duas entradas produzirem a mesmo *hash* deve ser pequena. Não se pode afirmar a impossibilidade da ocorrência de colisão, uma vez que o domínio dessa função é composto de todas as sequências de caracteres possíveis; e a imagem, pelo conjunto de sequência de caracteres de um tamanho fixo. Se o domínio da função é um conjunto infinito e a imagem é um conjunto finito, as colisões são inevitáveis.

No entanto, boas funções de *hash* apresentam baixíssimas probabilidade de colisão. Na prática, é quase impossível a ocorrência de uma colisão natural. A resistência a colisão permite a utilização da *hash* como síntese de mensagem. Por exemplo, para verificar que um arquivo baixado de um servidor na nuvem corresponde ao arquivo desejado, basta fazer a comparação de seus *hashes* em vez de comparar todo o arquivo (NARAYANAN *et al.*, 2016).

Ser antirreversão significa que não é possível obter a mensagem de entrada *x* a partir do *hash* h(*x*). Essa característica é alcançada fazendo com que a probabilidade dos *hashes* na saída da função obedeçam a uma distribuição uniforme. Na prática, isto significa que não é possível correlacionar caracteres na entrada e na saída da função apenas observando a frequência com que eles aparecem (NARAYANAN *et al.*, 2016).

Uma das principais utilizações da função *hash* na tecnologia *blockchain* é na construção de árvores de Merkle — árvores binárias de *hash*. A árvore é construída das folhas para a raiz, realizando a *hash* por pares. Quando há um número ímpar de folhas, a última folha é duplicada e *hasheada* consigo mesma. Essa estrutura permite uma rápida verificação das entradas iniciais da função e reduz em uma única *hash* a representação de todas as entradas (a raiz da árvore de Merkle, ou *Merkle root*).

A aplicação principal da função *hash* é a garantia de integridade de uma mensagem. Em geral, o emissor de uma mensagem calcula o seu *hash* e o insere no final da mensagem. O receptor recalcula a *hash* da mensagem recebida e compara o resultado obtido com a *hash* recebida. Se as *hashes* forem diferentes, há garantia de que a mensagem recebida é diferente da mensagem enviada. Se as *hashes* forem iguais, há uma probabilidade muito alta de a mensagem recebida ser igual à mensagem enviada. Assim, qualquer alteração na mensagem pode ser detectada pelo recálculo e pela comparação da *hash*, o que garante a integridade da mensagem.

Existem diferentes funções *hash*, mas o *bitcoin* e maioria das moedas criptográficas usam a função *hash* SHA256, que resulta em 256 bits. O algoritmo seguro de *hash* (*secure hash algorithm* [SHA]) foi desenvolvido pela Agência de Segurança Nacional (National Security Agency [NSA]) dos EUA.

De acordo com Ishmaev (2017), uma função *hash* é essencialmente uma função matemática que, dada uma entrada de dados de qualquer tamanho, produz uma saída de tamanho limitado que pode ser computável com eficiência (em um período de tempo razoável). A função *hash* tem várias propriedades importantes, e três delas, listadas a seguir, são particularmente úteis para as implementações de *blockchain*s.

- Primeiro, a função *hash* é **resistente à colisão**, o que significa que duas entradas distintas não produzem a mesma saída. Na prática, isso significa que a função *hash* pode ser usada como um resumo de mensagem, uma ferramenta para verificar se uma cópia de uma mensagem é idêntica ao original.

- A segunda propriedade é a **ocultação**, o que significa que dada apenas a saída, ninguém pode inferir o valor da entrada. Essa propriedade se traduz na aplicação de um compromisso de ligação, semelhante a colocar uma mensagem em um envelope e se comprometer com seu conteúdo sem revelá-lo. Depois que a mensagem é colocada no envelope, não é possível mudar de ideia e alterar seu conteúdo.
- A terceira propriedade é a **facilidade de quebra-cabeça**, o que significa que a função *hash* pode ser apresentada na forma de um quebra-cabeça matemático, no qual tentamos diferentes entradas para uma determinada função *hash* para obter uma saída com um valor predeterminado.

A primeira e a segunda propriedades das funções *hash* são empregadas para construir estruturas de dados complexas usando estruturas de dados simples (ponteiros de *hash* como blocos de construção). A facilidade de quebra-cabeças não é um requisito necessário para uma estrutura de dados em si, mas é necessária para a *blockchain*. Um ponteiro é uma estrutura de dados e funciona, essencialmente, como uma referência que indica onde as informações são armazenadas, semelhante ao código em um catálogo de biblioteca. O ponteiro de *hash*, por sua vez, é uma referência complementada com um breve resumo das informações a que se refere (útil para verificação). Usando ponteiros de *hash*, é possível construir uma estrutura de dados em forma de *blockchain*, formando uma cadeia de blocos que representa essa estrutura.

## Funções *hash* com *blockchain*

Visualizar a *blockchain* como um componente de *software* nos ajuda a entender os importantes impactos arquitetônicos sobre o desempenho e a qualidade de atributos como segurança, privacidade, escalabilidade e sustentabilidade. Como componente, a *blockchain* possui propriedades e limitações exclusivas. *Blockchains* são componentes de *software* complexos e baseados em rede, que podem fornecer armazenamento de dados, serviços de computação e serviços de comunicação (XU *et al.*, 2017).

### Criptografia

Para a segurança em sistemas distribuídos é fundamental o uso de técnicas de criptografia. A criptografia apoia fortemente a *blockchain* para cumprir os requisitos de segurança do sistema e das aplicações. Dentre os recursos mais utilizados, destacam-se as funções *hash* e as assinaturas digitais (GREVE *et al.*, 2018).

## Árvore de Merkle

Uma árvore Merkle (Figura 3) é uma árvore de *hashes* construída de baixo para cima que permite a verificação eficiente da integridade dos dados. Cada nó folha é uma *hash* de dados (por exemplo, transações), e cada nó não folha é uma *hash* de seus nós filhos, culminando no nó superior (ou seja, a *hash* raiz, ou a raiz Merkle). Essa estrutura de dados otimiza o armazenamento e a verificação de dados em uma *blockchain*. O armazenamento de dados é otimizado porque apenas as *hashes* precisam ser salvas, e a *hash* raiz é a impressão digital de todo o conjunto de dados. Já a verificação de dados é otimizada porque apenas uma pequena parte da árvore precisa ser percorrida a fim de verificar onde as alterações ocorreram (POPOVIC *et al.*, 2020).

A *hash* raiz é a impressão digital de todo o conjunto de dados, fazendo parte do cabeçalho do bloco na *blockchain*. Outro componente do mesmo cabeçalho do bloco é a *hash* do bloco anterior. Essa é uma estrutura de dados única, em que os blocos estão encadeados, sendo uma das características dos recursos da *blockchain* que a torna inviolável. Isso ocorre porque uma mudança nos dados causaria uma mudança na *hash* do bloco, tornando-a incompatível com o cabeçalho do próximo bloco. Portanto, um adversário que deseja alterar o estado de um determinado bloco precisaria alterar todos os blocos.

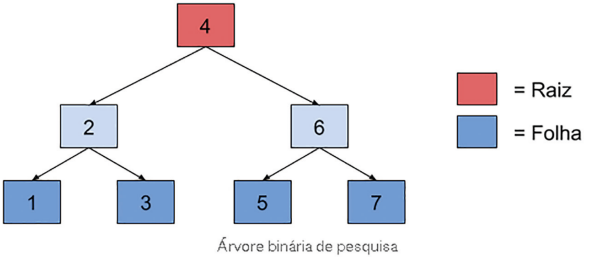


**Figura 3.** Árvore de Merkle.
**Fonte:** Seffrin (2019, documento *on-line*).

## Consenso — problema do gasto duplo

O consenso em computação distribuída é uma forma mais sofisticada da realização do sistema distribuído. Em um sistema de computação distribuída típico, um ou mais clientes emitem solicitações de operações para um con-

sórcio de servidores, que fornece serviço de computação correto e oportuno em resposta às solicitações, apesar de alguns servidores poderem falhar. Em comparação com a computação distribuída tradicional, uma rede *blockchain* permite que cada participante possa ser um cliente (para emitir transações) e um servidor (para validar e finalizar transações). Os dados do livro de registros subjacente à estrutura da *blockchain* são o alvo do consenso e consistem em blocos ordenados cronologicamente e encadeados por *hash*. Cada bloco contém um pacote de transações, sendo que as transações válidas em toda a *blockchain* devem ser consistentes entre si, ou seja, deve-se evitar gasto duplo ou excessivo (XIAO *et al*., 2020).

Na lógica econômica das criptomoedas, existe uma associação ao problema do gasto duplo, que representa um desafio de contabilidade e prestação de contas que as criptomoedas tentam superar de maneira eficaz. Esse problema é uma falha em potencial em uma criptomoeda ou outro esquema de dinheiro digital em que o mesmo *token* pode ser gasto mais de uma vez. Isso é possível porque um *token* digital consiste em um arquivo digital que pode ser duplicado ou falsificado (CHOHAN, 2017).

## Algoritmo *proof of work* (prova de trabalho)

O *proof of work* (PoW) é o algoritmo mais conhecido e implementado, sendo utilizado primeiro na rede *bitcoin*. Com a ajuda desse protocolo de consenso, o *bitcoin* se tornou o primeiro sistema de moeda digital a resistir a ataques de gasto duplo em um sistema descentralizado ponto a ponto de uma rede de pouca confiança. Esse protocolo é a chave por trás do *bitcoin* e de muitas outras criptomoedas estabelecidas, como *ethereum* e *litecoin* (XIAO *et al*., 2020).

No algoritmo PoW, a geração de blocos na *blockchain* requer encontrar uma pré-imagem para uma função *hash* para que o resultado da *hash* satisfaça uma meta de dificuldade definida, que é ajustada dinamicamente para manter um intervalo médio de geração de blocos. Também qualquer transação ou bloqueio gerado deve ser anunciado imediatamente e transmitido para todos nós da rede. Um bloco ou transação precisa ser validado antes de ser transmitido para os nós da rede ou anexado a *blockchain*. A validação inclui verificar o gasto duplo e a validade da prova de trabalho no cabeçalho do bloco. No PoW, considera-se a cadeia mais longa para representar a rede de consenso, que deve ser aceita por qualquer nó (também chamado de minerador) que participa dessa rede. A mineração deve sempre estender a cadeia mais longa (XIAO *et al*., 2020).

Nessa abordagem, o algoritmo PoW funciona como uma competição em termos de computação, em que os mineradores competem para resolver um problema criptográfico que consiste em encontrar um valor que, concatenado junto com outros dados do bloco (por exemplo, dados das transações, *timestamps* e *hash* do bloco anterior), é passado como entrada para uma função *hash* (por exemplo, SHA-256, *ethash* e *equihash*), a qual tenta encontrar um número aleatório chamado "*nonce*" que vai sendo incrementado até satisfazer as condições para resolver a função *hash* do próximo bloco. Quando as condições são satisfeitas, um novo bloco é minerado. Na geração de um bloco, os mineradores podem reivindicar uma certa quantidade de novos *tokens* e taxas coletadas de todas as transações incluídas, na forma de uma transação para si mesmo como recompensa pelo trabalho realizado (XIAO *et al.*, 2020).

## Algoritmo *proof of stake*

O *proof of stake* (PoS) se origina da comunidade *bitcoin* como uma alternativa eficiente em termos de energia à mineração do PoW. Em termos mais simples, é uma participação que se refere às moedas ou aos *tokens* da rede de propriedade de um participante que podem ser investidos no processo de consenso da *blockchain*. Do ponto de vista da segurança, o PoS aproveita a propriedade do *token* para mitigação de ataques Sybil (ameaça ao sistema em que tentam assumir o controle da rede criando múltiplas contas). Comparado a um minerador do PoW, cuja chance de gerar um bloco é proporcional ao seu poder de computação de força bruta, a chance de gerar um bloco para um minerador no PoS é proporcional ao seu valor de participação na rede (XIAO *et al.*, 2020).

Do ponto de vista econômico, o PoS move o custo de oportunidade de um minerador de fora do sistema (desperdício de poder de computação e eletricidade) para dentro do sistema (perda de capital e ganho de investimento). Devido à falta real de mineração, muitas vezes nos referimos a um minerador no PoS como um validador, ou uma parte interessada pela grande semelhança do PoS com o investimento em mercados capitais (XIAO *et al.*, 2020).

As principais variações do PoS seguem a estrutura do consenso do PoW, em que a comunicação ocorre por mensagens. Existem as regras de validação de bloqueio, as regras de cadeia mais longa e finalidade probabilística. Ao contrário do PoW, um minerador do PoS pode tentar resolver o quebra-cabeça da *hash* apenas uma vez por ciclo de tentativas. Com isso, a dificuldade do quebra-cabeça diminui com o valor da participação do validador. O número de tentativas para resolver o problema do quebra-cabeça da *hash* pode ser

significativamente reduzido se o valor da participação do minerador for alto. Portanto, o PoS evita a competição de força bruta que ocorreria se PoW fosse usado. Dessa forma, é alcançada uma significativa redução do uso de energia.

## Exemplos de funções *hash* com *blockchain*

Por serem rápidas, eficientes, exclusivas e econômicas em termos de computação, as funções de *hash* são amplamente usadas na tecnologia *blockchain*. O uso de funções *hash* aliadas a outras tecnologias, como a criptografia, tornam a *blockchain* ou outros algoritmos muito seguros, privados e até anônimos.

De todos os usos das funções *hash* na *blockchain*, os casos a seguir podem ser destacados.

### Criação de endereço (carteira de endereços)

Os endereços das carteiras de criptomoedas são uma representação segura das chaves públicas da carteira. As chaves públicas geralmente são muito longas e complexas. É por esse motivo que *blockchains* usam funções *hash* para originar um endereço mais curto. Esse processo é usado repetidamente para reduzir o endereço e adicionar uma camada extra de segurança.

No *bitcoin*, o processo de criação de um endereço de carteira usa funções *hash* RIPEMD-160 e SHA-256. Ambas são usadas para melhorar a segurança do processo e torná-las únicas e irrepetíveis.

### Processo de mineração

O processo de mineração é outro estágio importante da tecnologia *blockchain* em que as funções de *hash* são usadas. No *bitcoin*, a mineração faz uso intensivo do cálculo de *hash* SHA-256 distribuído em cada um dos seus nós. Os mineradores são responsáveis pelo cálculo de milhões de *hashes* para criar novos blocos de *bitcoin*. O processo também é utilizado para verificar as transações que são feitas na rede.

Embora o processo de cálculo de *hashes* seja muito rápido, seu uso intensivo dificulta drasticamente o processo. Isso leva os mineradores a usar alto poder de computação para resolver quebra-cabeças de *bitcoin*.

## Contratos inteligentes (*smart contracts*)

Essa é outra área em que as funções de *hash* são muito usadas. *blockchains* como *bitcoin*, *ethereum*, *neo* e *tron* fazem uso de contratos inteligentes para promover diferentes aplicações. Esses aplicativos são gerenciados por um contrato público entre as partes. No entanto, muitos desses dados são muito sensíveis ou simplesmente contêm muita informação para ser armazenada em uma *blockchain*. Portanto, a melhor maneira de resolver esses cenários é por meio de funções *hash*. Dessa maneira, o contrato inteiro é público, mas as informações vinculadas ou que você deseja manter em sigilo não são publicadas. Esses dados podem incluir nomes, endereços, endereços de carteira, dados de participantes de terceiros, ou seja: informações privilegiadas e apenas de interesse entre as partes.

As *hashes* também são usadas para versão de contratos. Isto é, um contrato público possui uma *hash* exclusiva, fornecida pelo que o contrato estabelece. Se o contrato for modificado, o contrato anterior é encerrado e um novo é gerado com uma nova *hash*. Dessa forma, a *hash* determina o contrato correto a ser usado num aplicativo descentralizado, facilitando o seu controle. Outro uso de *hashes* em contratos inteligentes é para marcar suas validade e autenticidade. Um exemplo pode ser um contrato feito para a venda de uma casa com um pagamento feito em criptomoedas. A conclusão do contrato e sua *hash* serão testemunhas inalteráveis da venda feita entre as partes.

# Referências

CHOHAN, U. W. The double spending problem and cryptocurrencies. *SSRN*, n. 1, p. 1–8, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174. Acesso em: 6 out. 2021.

GREVE, F. *et al.* Blockchain e a revolução do consenso sob demanda. *In*: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 2018, Porto Alegre. *Anais eletrônicos* [...]. Disponível em: http://143.54.25.88/index.php/sbrcminicursos/article/view/1770/1743. Acesso em: 6 out. 2021.

ISHMAEV, G. Blockchain technology as an institution of property. *Metaphilosophy*, v. 48, n. 5, p. 666-686, 2017.

NARAYANAN, A. *et al. Bitcoin and cryptocurrency technologies*: a comprehensive introduction. New Jersey: Princeton University Press, 2016.

NAKAMOTO, S. *Bitcoin*: um sistema de dinheiro eletrônico peer-to-peer. 2021. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf. Acesso em: 8 out. 2021.

POPOVIC, D. *et al.* Understanding blockchain for insurance use cases. *British Actuarial Journal*, v. 25, n. 1, p. 1-13, 2020.

OKUPSKI, K. *Bitcoin developer reference*. 2014. Disponível em: https://www.lopp.net/pdf/Bitcoin_Developer_Reference.pdf. Acesso em: 6 out. 2021.

SEFFRIN, H. *Descomplicando o Bitcoin*: árvores de merkle. 2019. Disponível em: https://medium.com/fs-dev/descomplicando-o-bitcoin-%C3%A1rvores-de-merkle--3a1b53fa4fd9. Acesso em: 6 out. 2021.

XIAO, Y. *et al.* A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys Tutorials*, v. 22, n. 2, p. 1432–1465, 2020.

XU, X. *et al.* A taxonomy of blockchain-based systems for architecture design. *In*: IEEE INTERNATIONAL CONFERENCE ON SOFTWARE ARCHITECTURE, 2017, New York. *Anais eletrônicos* [...]. Disponível em: http://pautasso.info/biblio-pdf/blockchain-icsa2017.pdf. Acesso em: 6 out. 2021.

## *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

# Redes P2P aplicadas a *blockchain*

*Thaís Bison*

**OBJETIVOS DE APRENDIZAGEM**

- Conceituar redes P2P com *blockchain*.
- Integrar redes P2P com *blockchain*.
- Apresentar exemplos de redes P2P com *blockchain*.

## Introdução

A tecnologia *blockchain* teve início com a introdução do *bitcoin*, para evitar a duplicidade de transações. Pouco tempo se passou e a referida tecnologia expandiu seus horizontes, podendo ser implementada em diversas frentes. Com ela, é possível guardar os mais diversos tipos de informações de forma segura, imutável e com privacidade, evitando corrupção de dados. Trata-se de uma modalidade de registro distribuído entre diversos dispositivos conectados que armazenam espécies de registros com estampa de tempo e assinatura digital.

Neste capítulo, você vai estudar os conceitos de *blockchain* e redes P2P e a interação entre essas duas tecnologias em alguns exemplos de implementações.

## Conceitos básicos

A *blockchain* é uma base distribuída de dados que mantém uma lista encadeada de registros (conhecidos como blocos) e que funciona sobre uma arquitetura *peer-to-peer* (P2P, ou ponto a ponto). A tecnologia *blockchain* diz respeito a uma rede de blocos encadeados e seguros que requerem uma validação digital. Assim, cada bloco subsequente contém a validação ou assinatura digital do bloco anterior somado ao seu conteúdo ou sua informação.

A *blockchain*, conforme descrito por Nakamoto ([200-?]), é uma solução para viabilizar uma rede de transações financeiras de moedas virtuais, a exemplo do *bitcoin* (NAKAMOTO, [200-?]). O *bitcoin* é uma criptomoeda, pois tem sua existência fundamentada em conceitos criptográficos, como funções *hash*. A *blockchain* está fundamentada em uma rede distribuída, e oferece visibilidade às transações efetuadas. Não há um agente centralizador na arquitetura, e sem um mediador central, as relações de confiança são executadas colaborativamente pelos usuários.

Para que essa base distribuída funcione da maneira proposta, a lista encadeada de blocos conta com funções criptográficas de mão única (assinatura *hash*), registro do tempo da criação ou modificação (*timestamp*), assinatura digital do autor, rede descentralizada P2P e mecanismo de geração de um novo bloco da *blockchain*. Todos esses mecanismos garantem à arquitetura a robustez necessária e a prevenção contra fraudes e adulterações indevidas.

Com as funções criptográficas de mão única (*hash*), fica permitida a operação em um sentido, mas é completamente inviável realizá-la no sentido oposto. Dada uma entrada, obtém-se uma saída única. Entradas diferentes produzem diferentes saídas. Com valores de saída, não é possível calcular valores de entrada, mesmo conhecendo de antemão o algoritmo da função. A finalidade dessas funções é tornar inviável e improvável qualquer alteração nos valores registrados na *blockchain*.

A alteração de um registro implica num novo valor de *hash* para ele, alteração no *hash* do próximo registro, e assim subsequentemente, pois os registros estão encadeados (NAKAMOTO, [200-?]).

O *hash* garante a assinatura de um determinado bloco. A criação de um novo bloco que contém o *hash* anterior cria um selo digital que é passível de verificação e sinaliza qualquer alteração. Tais informações ficam relacionadas no *ledger* como um livro-razão, uma espécie de livro contábil. Quando se armazena a *hash* ou impressão digital de um ativo, ao invés de armazenar o ativo digital em si, o anonimato é garantido, bem como a privacidade.

Vejamos agora como é a estrutura da *blockchain*. Um bloco possui um cabeçalho, que inclui o conjunto de regras para a validação que o bloco

deve seguir, apontando sua versão; o valor do *hash* de 256 bits, que indica qual é o bloco anterior, chamado *parent block hash*; o valor de *hash*, que se refere a todas as transações daquele bloco, denominado *merkle root hash*; o *timestamp*; um alvo de *hash* compacto (*nBits*); e *nonce*, um campo de 4 bytes e aumenta para cada *hash*.

O corpo do bloco é formado por um contador de transações e pelas respectivas transações. O máximo de transações que um bloco comporta depende de seu tamanho e da dimensão de cada transação. A tecnologia *blockchain* usa criptografia assimétrica para validar cada transação em um ambiente não confiável.

O registro de tempo da transação (*timestamp*) tem o objetivo de armazenar o elemento temporal de alteração na *blockchain*, evitando fraudes ligadas a adulteração de data/hora nas transações. O principal objetivo desse registro distribuído é fornecer um grau de segurança mais avançado àquelas informações, haja vista que há a necessidade de anuência de todos os dispositivos conectados sobre os registros armazenados. Assim, todas as transações são avalizadas pelo consenso da maioria dos participantes da *blockchain* (Figura 1).

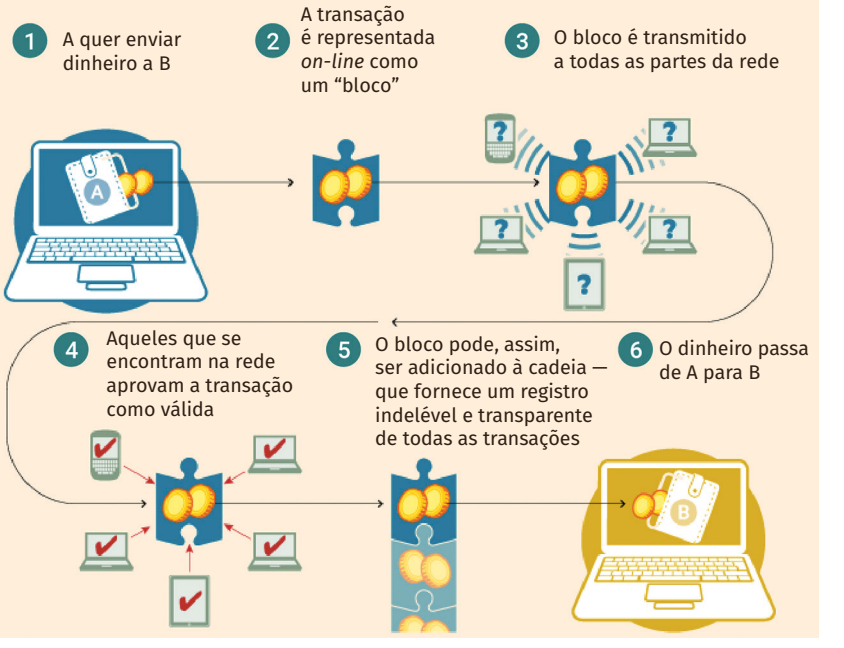


**Figura 1.** Funcionamento da tecnologia *blockchain*.
**Fonte:** Adaptada de IHODL (2017).

*Blockchain*, que significa literalmente cadeia de blocos, funciona com blocos de registros que operam por meio de rede descentralizada. Cada bloco possui uma gama de registros de acontecimentos, que, assim como o bloco, seguem uma ordem cronológica de armazenamento. Para a realização desse acontecimento, ou seja, a troca de informação entre usuários, é utilizada criptografia assimétrica de assinatura digital, que garante aspectos de segurança à transação ocorrida. Cada bloco possui um número de identificação, obtido a partir do resumo desse bloco, denominado função *hash*, e, além disso, possui em seus metadados o *hash* do bloco anterior, assegurando que nenhum bloco será alterado, preservando as informações contidas nele.

A estrutura da *blockchain* tem, nesse sentido, os seguintes pilares fundamentais.

- Segurança: sua estrutura garante aqueles que, segundo Stalling (2015), são os mais importantes princípios de segurança de computadores: integridade, confidencialidade e disponibilidade.
- Arquitetura descentralizada: os registros não estão armazenados em um servidor, sendo distribuídos entre diversas máquinas.
- Integridade dos dados: devido ao encadeamento de cada bloco adicionado ao *hash* do bloco anterior, qualquer tentativa de modificação de um bloco mudará a estrutura dos demais blocos.
- Imutabilidade: por ter uma estrutura ordenada de forma cronológica, nenhum dado adicionado pode ser apagado ou alterado do seu bloco, tornando-se também um histórico temporal de tudo que foi realizado.

Analisando algumas definições sobre a tecnologia em si, Antonopoulos (2014) define *blockchain* conforme a sua estrutura de funcionamento, entendendo-a como uma lista de blocos de transações que se ligam entre si de forma ordenada e cronológica, de modo que um bloco se refira ao seu anterior.

Outras definições interessantes aparecem com Mougayar (2017), que define *blockchain* de acordo com suas capacidades técnicas, corporativas e legais.

- Técnica: é uma base de dados *back-end*, que funciona por meio de registros distribuídos e que possibilitam a realização de inspeções abertamente.
- Coorporativa: rede de troca de fatos entre partes que dispensa a assistência de intermediários.
- Legal: funciona como um mecanismo de validação, não exigindo apoio de intermediários.

A rede P2P é um tipo de rede de computadores que vai na contramão do que é proposto em uma rede de modelo tradicional do tipo cliente/servidor (Figura 2), em que os servidores têm o papel de disponibilizar serviços e os usuários atuam somente como beneficiários.

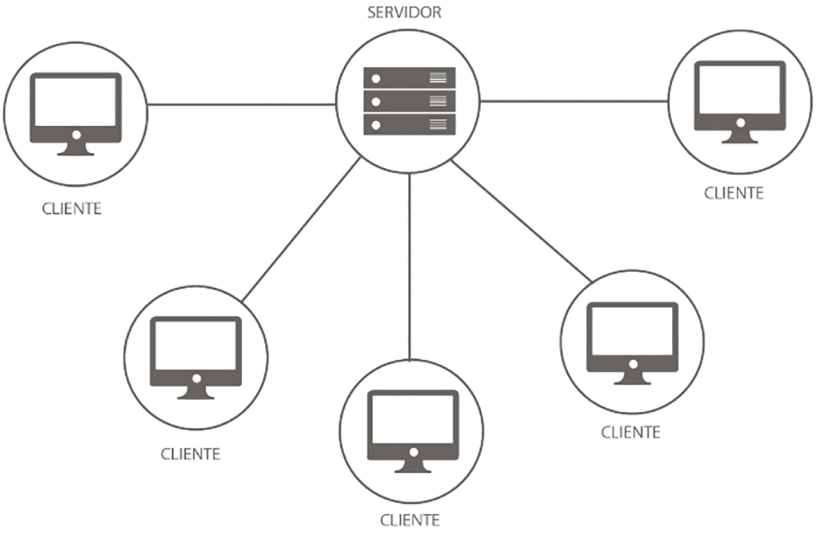


**Figura 2.** Rede do tipo cliente/servidor.
**Fonte:** Adaptada de Wang, Aslam e Zou (2010).

Na *blockchain*, sua mais fundamental característica está na descentralização, o que faz com que cada nó (*peer*) desempenhe funções como cliente e também servidor (LOPES, 2014). Esse tipo de rede não depende de uma organização central ou de hierarquia, fazendo com que todos os usuários integrantes, com direitos de acesso adequados, tenham a mesma capacidade e responsabilidade (Figura 3). Por ser descentralizado, todos os usuários possuem uma cópia da base de dados, o que garante uma maior segurança contra eventuais invasões ou perda de dados. Outro benefício é a garantia da disponibilidade do sistema: mesmo que algum nó por acaso não esteja funcionando, os demais nós mantêm o sistema em operação (KAMIENSKI *et al*., 2005).

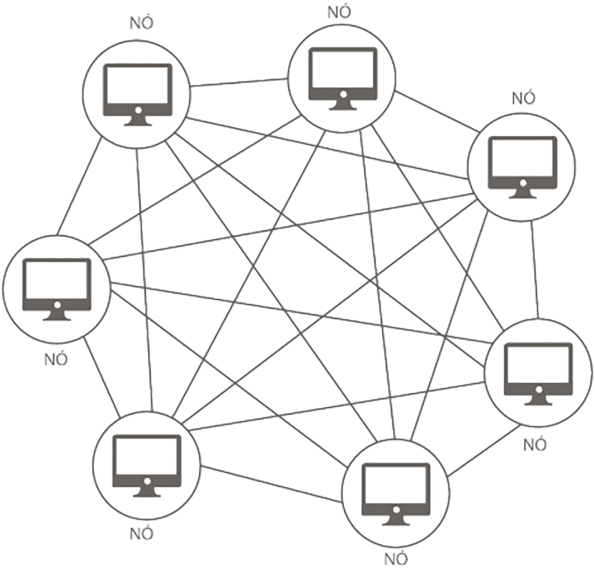


**Figura 3.** Modelo de rede P2P.
**Fonte:** Adaptada de Wang, Aslam e Zou (2010).

A rede P2P possibilita que os nós (*peers*) avaliem as informações da *blockchain* e aceitem ou rejeitem, por maioria, as alterações realizadas. Essa é a implementação da relação de confiança descentralizada.

Nota-se que são inúmeras as aplicações e vantagens na utilização da tecnologia *blockchain*, dentre as quais podemos destacar a eliminação do terceiro intermediário na realização de transações, haja vista que com a *blockchain*, as partes envolvidas podem realizar a troca sem intermediários que supervisionam o evento, diminuindo os riscos de inadimplemento das partes. Outra vantagem de destaque é a qualidade dos dados e informações, pois a autenticidade das transações é verificada quando há o fechamento de cada bloco. Na hipótese da transação não se concretizar, ela não será adicionada a determinado bloco. Conclui-se que as informações contidas em cada bloco e ao longo da *blockchain* são consistentes, datadas e verossímeis, o que garante alto grau de qualidade dos dados.

Outro ponto relevante versa sobre a durabilidade e a confiabilidade dessa tecnologia, considerando-se que a rede é descentralizada, seguindo a concepção P2P, de modo que a *blockchain* não tem um ponto central. Quando houver uma falha no sistema, ou mesmo se for hackeado, a descentralização

auxilia na proteção do sistema, devido à fala de um ponto central. Cada nó possui uma cópia dos dados, o que impede que eles se percam.

A integridade do processo é mais uma vantagem do sistema de *blockchain*. Os usuários têm a garantia de que as transações serão efetuadas de acordo com os termos propostos, caso contrário o evento não será validado.

## Integração de redes P2P com *blockchain*

Nos estágios iniciais do *bitcoin*, Nakamoto ([200-?], documento *on-line*) a definiu como "um sistema P2P de dinheiro eletrônico". O *bitcoin* foi criado como uma forma digital de dinheiro. Pode ser transferido de um usuário para outro através de uma rede P2P, que gerencia um livro contábil (*ledger*) distribuído, chamada *blockchain*.

Nesse contexto, a arquitetura P2P inerente à tecnologia *blockchain* é o que permite que o *bitcoin* e outras criptomoedas sejam transferidos em todo o mundo, sem a necessidade de intermediários nem de um servidor central. Além disso, qualquer usuário pode estabelecer um nó do *bitcoin* participando do processo de verificação e validação de blocos. Portanto, não há bancos processando ou registrando transações na rede *bitcoin*. Em vez disso, a *blockchain* atua como um livro contábil digital que registra publicamente todas as atividades. Basicamente, cada nó mantém uma cópia da *blockchain* e a compara com outros nós para garantir que os dados sejam válidos. A rede rejeita rapidamente qualquer atividade maliciosa ou inconsistência de dados.

No contexto das *blockchains* de criptomoedas, os nós podem assumir várias funções diferentes. Os nós completos (*full nodes*), por exemplo, são os que fornecem segurança à rede, verificando as transações com base nas regras de consenso do sistema. Cada nó completo mantém uma cópia completa e atualizada da *blockchain*, permitindo que participem do trabalho coletivo de verificação do verdadeiro estado do livro contábil distribuído. Vale ressaltar, no entanto, que nem todos os nós completos de validação são mineradores.

Apesar da *blockchain* surgir no contexto de criptomoedas (como o *bitcoin*), sua aplicação não está restrita a transações financeiras. Outras áreas têm utilizado o conceito de redes P2P e bases de dados distribuídas em cadeia de confiança como incremento para suas aplicações, como armazenamento de dados, distribuição de mídias, gerência de contratos, administração de propriedade material ou intelectual, votação eletrônica e participação colaborativa do cidadão nos governos, entidades ou federações descentralizadas.

## *Saiba mais*

Após o surgimento do *bitcoin* e da primeira *blockchain* associada, outras arquiteturas de *blockchain* estão sendo desenvolvidas e utilizadas, como o Ethereum, criado como uma plataforma P2P para executar aplicações descentralizadas sobre *blockchain*, especialmente *smart contracts* (WOOD, [200-?]). É uma rede distribuída que se propõe a corrigir muitos dos problemas encontrados na *blockchain* do *bitcoin* (especialmente com relação à mineração e ao tempo de validação). Para se utilizar essa plataforma, é necessário adquirir a criptomoeda criada para esse fim, chamada *ether*, cujo valor de mercado está atrás somente do *bitcoin*.

Segundo Braga ([2017?]), uma aplicação da *blockchain* é composta por três camadas (Figura 4): a primeira é o sistema distribuído, equivalente à estrutura básica, responsável pela implementação da rede P2P e suas funcionalidades necessárias, como método de consenso, armazenamento da rede e protocolos de comunicação ponto a ponto. Na segunda, tem-se os serviços de apoio e infraestrutura, normalmente associados à camada de plataforma, responsável pelo desenvolvimento de aplicações de segurança, como criptografia, segurança dos dados, disponibilidade dos nós na rede, gestão de identidade, etc. Por fim, na terceira temos uma camada de aplicação, que é formada pela lógica de negócios e contratos inteligentes que assegura a implementação.

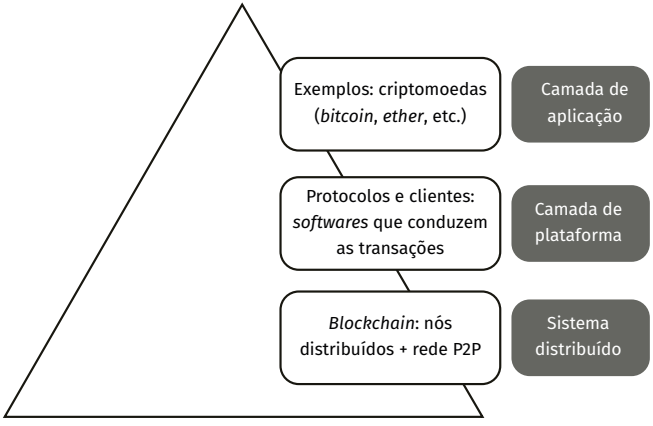


**Figura 4.** Camadas tecnológicas da *blockchain*.
**Fonte:** Adaptada de Braga ([2017?]).

A arquitetura P2P de *blockchains* oferece muitos benefícios. Dentre os mais importantes, está o fato das redes P2P oferecerem mais segurança do que a arquitetura tradicional de cliente/servidor. A distribuição de *blockchains* em grande número de nós os torna praticamente imunes a ataques Denial of Service (DoS), que prejudicam muitos sistemas.

Da mesma forma, como a maioria dos nós deve estabelecer um consenso antes que os dados sejam adicionados à *blockchain*, é quase impossível que um invasor altere os dados. A alteração de dados é ainda mais improvável para grandes redes, como a do *bitcoin*. *Blockchains* menores são mais suscetíveis a ataques, porque uma pessoa ou grupo pode eventualmente obter controle sobre a maioria dos nós. Como resultado, a rede P2P distribuída, combinada com um requisito de consenso majoritário, oferece às *blockchains* um grau relativamente alto de resistência a agentes maliciosos.

Além da segurança, o uso da arquitetura P2P em *blockchains* de criptomoedas também proporciona resistência à censura de autoridades centrais. Diferentemente de contas bancárias-padrão, as carteiras de criptomoedas não podem ser congeladas ou sofrer qualquer interferência do governo. Essa resistência também se estende às ações de censura por parte de plataformas privadas de pagamento e provedoras de conteúdo em geral.

Apesar das muitas vantagens, a utilização de redes P2P em *blockchains* também apresenta algumas limitações. Como os livros contábeis (*ledgers*) distribuídos devem ser atualizados em todos os nós e não em um servidor central, a inclusão de transações à *blockchain* requer muito poder computacional. Apesar de fornecer mais segurança, esse sistema possui baixa eficiência, o que é um dos principais obstáculos quando se trata de escalabilidade e adoção em massa.

Outra potencial limitação está relacionada a ataques que podem surgir durante eventos de *hard fork*. Como a maioria das *blockchains* é descentralizada e de código aberto, grupos de nós podem copiar e modificar o código e se separar da cadeia principal para formar uma nova rede paralela.

Seja como for, além de sua utilidade na tecnologia *blockchain*, os sistemas P2P também podem atender às necessidades de outras aplicações de computação distribuída, desde redes de compartilhamento de arquivos até plataformas de negociação de energia.

### *Saiba mais*

O chamado *phishing* é um golpe baseado na "pesca" de informações de usuários, e é feito a partir da clonagem de *sites* e aplicativos, onde são simuladas páginas e plataformas de instituições oficiais. No caso das criptomoedas, normalmente são criadas páginas quase idênticas às de *exchanges* legítimas, e a partir daí os investidores são induzidos e acabam entregando seus dados, e logo depois tendo suas carteiras esvaziadas.

## Exemplos de redes P2P com *blockchain*

Apesar de hoje mais conhecido, o surgimento da *blockchain* se deu a partir de uma aplicação chamada *bitcoin*. Percebendo que essa tecnologia poderia ser separada da moeda e utilizada em diversos tipos de cooperações, nasceu o interesse exclusivo pela *blockchain*. O *bitcoin* é uma moeda digital que funciona de modo descentralizado (P2P) e sem a necessidade de um intermediador ou autoridade central, como um banco (ULRICH, 2014).

Para entender com mais clareza o que é o princípio do *bitcoin*, e consequentemente da *blockchain*, é preciso voltar a 2008, ano em que foi publicada a pesquisa "Bitcoin: A peer-to-peer eletronic cash system". Nessa pesquisa, o autor, que se utiliza do pseudônimo Satoshi Nakamoto, apresenta os princípios e explica o funcionamento da nova moeda digital desenvolvida por ele. Nessa ocasião, tem-se a primeira aplicação conhecida da tecnologia *blockchain*, caracterizando, assim, seu surgimento. Em resumo, além de fornecer as informações conceituais já apresentadas anteriormente, a pesquisa de Nakamoto ([200-?]) discorre sobre os seguintes pontos:

- o *bitcoin* é definido como uma versão de dinheiro eletrônico que permite pagamentos *on-line* de uma parte para outra sem intermediadores;
- com o uso da tecnologia *blockchain*, deixa de ser necessário o envolvimento de terceiros, como bancos, para impedir a realização de gastos duplos;

## *Fique atento*

A solução do **problema do gasto duplo** é uma das grandes façanhas da tecnologia *blockchain* no ramo financeiro. Esse problema surge com o advento da internet e do meio digital, em que parece difícil replicar a escassez de certos bens que encontramos no mundo físico. Para dar um exemplo, quando seu amigo lhe empresta um disco de vinil, o objeto agora está com você e não está mais com ele. Porém, se ele lhe transferir o arquivo desse mesmo disco pela internet em formato MP3, o disco agora está em sua posse, mas o amigo ainda dispõe dele no seu computador. Pois esse era um enorme problema em se tratando de moeda virtual, e, até o desenvolvimento da *blockchain*, intermediários, como instituições bancárias, precisavam ser envolvidos em transações financeiras *on-line* para assegurar que um valor monetário tinha deixado uma conta e ido para outra, sem pairar nas duas ao mesmo tempo, como acontece com outros itens digitais (AMETRANO, 2020; BUDISH, 2018).

Mais recentemente, essa tecnologia de atribuição de escassez e unicidade a certos itens de mídia vem sendo aplicada no mundo das artes com as *non-fungible tokens* (NFTs), obras digitais não intercambiáveis que chegam a ser leiloadas por dezenas de milhões de dólares (A EXTRAORDINÁRIA..., 2021).

- como solução ao problema dos gastos duplos, é proposto o uso de uma rede P2P;
- tal rede registra as transações com uma marca temporal, criptografa-as em uma cadeia contínua baseada em um modelo de prova de trabalho, criando um registro único e que não pode ser alterado, caso não seja realizada uma outra prova de trabalho;
- a cadeia mais longa serve não somente como uma comprovação de eventos testemunhados, mas também como comprovação da existência de um poder computacional por trás dos registros, o que garante maior segurança.

Em relação ao funcionamento do *bitcoin*, pode-se comparar sua facilidade de realizar uma transação à facilidade de enviar um *e-mail*. Para se registrar na rede, basta realizar o *download* do programa e criar uma carteira *on-line* em um *site* especializado. Com o registro realizado, o usuário possui duas chaves: uma privada, utilizada para autenticar transações, e uma pública, parar funcionar como localizador de transações. Ambas estão disponíveis nessa carteira. No *bitcoin*, para o usuário realizar uma transação, é preciso usar a chave pública do favorecido. Essa chave funciona como uma espécie de endereço da carteira. A autenticação dessa transação é realizada por meio da chave privada, funcionando como um tipo de senha validadora. Após a

realização da transação, como prova de veracidade do processo ambas as chaves públicas (do fornecedor e do favorecido) ficam disponíveis ao público.

Desse modo, há um maior controle sobre as fraudes e duplicações de moedas. A partir do *bitcoin*, que instaurou o modelo básico de *blockchain* e criptomoeda, surgiram outros negócios, como os listados a seguir.

- Ethereum: considerada uma evolução do *bitcoin*, essa plataforma foi proposta em 2013 e lançada em 2015. Foi criada para funcionar no âmbito de contratos inteligentes. Tais contratos são executados por meio de uma moeda própria denominada *ether*. Hoje é uma das plataformas mais utilizadas em projetos-piloto, tendo sido adotada em iniciativas desenvolvidas por empresas como Microsoft e Santander.
- Hyperledger: plataforma criada para ambientes empresariais. Seu funcionamento, apesar de ser de código aberto, ocorre por meio de um P2P privado. Suas aplicações são variadas, sendo menos voltadas para o uso de criptomoedas. Promove aplicações baseadas em contratos inteligentes. Atualmente, sua gestão é realizada pela Linux Foundation e possui 81 membros.

Com essas iniciativas pioneiras que hoje servem como base para diversos aprofundamentos, outras entidades de âmbito público e privado também voltaram os olhos para explorar essa possibilidade. Ademais, existem variadas pesquisas de outros setores da sociedade que também propõem a utilização de *blockchain*, em aplicações que passam pelo setor automotivo, elétrico, varejo, saúde e assistência médica, e até por cidades, prédios e residências inteligentes. A seguir, vamos examinar algumas dessas iniciativas.

## Cadeia de suprimentos

Processos realizados desde o plantio ou extração da matéria-prima até a chegada do produto ao consumidor lidam na maioria das vezes com informações obscuras. Algumas empresas, em sua maioria do ramo da alimentação, já disponibilizam para seus clientes dados sobre toda a cadeia de processos que cada produto percorreu, muitas vezes mencionando datas, horas e até condições. Apesar de já se parecer um problema solucionado, em que somente se espera a disposição das empresas para sua adoção, tais processos ainda não são confiáveis o suficiente para realizar ações automáticas de forma concreta. Com a utilização da *blockchain*, alguns desses problemas seriam

solucionados, principalmente quanto ao controle de acesso e disponibilização das informações entre os atores responsáveis pelos processos. Tudo isso funcionaria de modo continuo, em tempo real, e os dados ficariam armazenados de forma segura, simples e mais eficiente do que sob métodos habituais.

## Telecomunicações

Com investimento das principais operadoras mundiais, atualmente a aplicação de *blockchain* em telecomunicações já é uma realidade. Seus usos estão em grande parte voltados para a utilização de contratos inteligentes que, por exemplo, poderiam trazer serviços como implementações de bases de dados para autenticação de usuários em *roaming*, pagamentos e autenticação em *wi-fi* público, autenticação entre dispositivos, aplicativos e organização. Com isso, almeja-se reduzir os custos e ofertar serviços digitais a preços mais competitivos.

## Ciência

Duas plataformas pioneiras, e ainda em fase de testes, se destacam quando ao uso de *blockchain* na área de ciências: Pluto e Sciencerоot. Observando suas funções, é possível notar bastante similaridade, e ambas se propõem a oferecer um sistema de colaboração e publicação científica, sob um funcionamento similar a uma rede social. Os cientistas ganham um espaço de publicação de suas descobertas científicas e de todos os dados de pesquisa, que ficam disponíveis livremente para uso de terceiros, o que facilita uma análise mais precisa dos dados e a reprodução de cada pesquisa. Todas as publicações ainda são avaliadas pelos próprios membros das plataformas. Há ainda a possibilidade de comentar e avaliar as publicações de outros cientistas. O cientista e o avaliador recebem recompensas pelos seus trabalhos, o que atribui um aspecto de gamificação e essas plataformas.

Vejamos ainda outras aplicações vantajosas com a implementação de *blockchain*:

- Criação de *marketplaces* distribuídos e autônomos — um *marketplace* é como um *shopping* virtual, que reúne diversas marcas e lojas em um só lugar. Assim, a *blockchain* garante a transferência de ativos de forma segura, privada, autorregulada e com celeridade, proporcionando flexibilidade ao caixa e gerenciamento de ativos.

- Transações comerciais facilitadas — com a aplicação dessa tecnologia, o gerenciamento de gastos torna-se mais fácil, tendo em vista que permite que as empresas criem uma rede autônoma de fornecedores e parceiros, automatizando os contratos e acompanhando toda a cadeia de suprimentos. Ademais, com a redução de interações humanas, a *blockchain* reduz os erros de transação ou falta de informações, implementando agilidade entre as partes.
- Administração e garantia de registros privados descentralizados: cada registro é criptografado individualmente e requer uma chave de acesso personalizada, o que garante dados com total segurança, inclusive em instituições educacionais e nas empresas no setor de recursos humanos, sem a preocupação com a possibilidade de falsificação.
- Acompanhamento da procedência de produtos e materiais — a *blockchain* pode assegurar a qualidade e a segurança de determinado produto e o rastreamento de seus insumos.

A tecnologia *blockchain* é mais conhecida por dar suporte ao *bitcoin*, mas apresenta diversas outras aplicações nos dias atuais. Essa tecnologia representa um registro distribuído e permanente entre as partes envolvidas, o que demonstra uma medida de segurança baseada na descentralização das informações, principalmente voltada para o mercado financeiro. Sua abrangência se expandiu para a guarda de qualquer tipo de documento.

Uma das grandes vantagens da utilização da *blockchain* é a globalização, pois não há interferência de fatores externos como dados, capital ou mesmo o governo. Sua tecnologia reside na guarda dos registros de transações, principalmente transações econômicas, num bloco com um número de identificação, conhecido como *hash*. Quando o bloco está cheio, ele é selado com a *hash*, determinando que as transações daquele bloco são válidas e imodificáveis, iniciando-se assim um novo bloco.

## Referências

A EXTRAORDINÁRIA venda em leilão por R$ 382 milhões de uma obra de arte que não existe na vida real. *BBC News*, 12 mar. 2021. Disponível em: https://www.bbc.com/portuguese/geral-56371789. Acesso em: 9 set. 2021.

AMETRANO, F. M. The Cryptocurrency Frontier in Monetary Engineering. *SSRN*, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2508296. Acesso em: 9 set. 2021.

ANTONOPOULOS, A. M. *Mastering bitcoin*: unlocking digital cryptocurrencies. Sebastopol: O'Reilly, 2014.

BRAGA, A. M. *Tecnologia Blockchain*: fundamentos, tecnologias de segurança e desenvolvimento de software. Campinas: CPQD, [2017?]. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINAL.pdf. Acesso em: 9 set. 2021.

BUDISH, E. *The economic limits of bitcoin and the blockchain*. Cambridge: National Bureau of Economic Research, 2018. Disponível em: https://www.nber.org/papers/w24717. Acesso em: 9 set. 2021.

IHODL. *Guia de Blockchain para principiantes*. [*S. l.*: *s. n.*], 2017. Disponível em: https://pt.ihodl.com/topic/crypto/tutorials/. Acesso em: 9 set. 2021.

KAMIENSKI, C. *et al*. Colaboração na internet e a tecnologia peer-to-peer. *In*: CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 25., 2005, São Leopoldo, Rio Grande do Sul. *Anais [...]* São Leopoldo: [*s. n.*], 2005. Disponível em: http://www.lbd.dcc.ufmg.br/colecoes/jai/2005/004.pdf. Acesso em: 9 set. 2021.

LOPES, A. D. da M. *VoIP em redes peer-to-peer*. 2014. 110 f. Dissertação (Mestrado em engenharia de comunicações) — Universidade do Minho, Braga, 2014. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/35186/1/Disserta%C3%A7%C3%A3o_Ant%C3%B3nio%20D.%20da%20M.%20Lopes_2014.pdf. Acesso em: 5 ago. 2021.

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

NAKAMOTO, S. *Bitcoin*: a peer-to-peer eletronic cash system. [*S. l.*: *s. n.*, 200-?]. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 9 set. 2021.

STALLING, W. *Criptografia e segurança de redes*: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

ULRICH, F. *Bitcoin*: a moeda na era digital. São Paulo: Instituto Ludwig Von Misses Brasil, 2014.

WANG, P.; ASLAM, B.; ZOU, C. C. Peer-to-peer botnets. *In*: STAVROULAKIS, P.; STAMP, M. (org.). *Handbook of information and communication security*. Springer: Berlin, 2010. Disponível em: http://cs.ucf.edu/~czou/research/P2PBotnets-bookChapter.pdf. Acesso em: 9 set. 2021.

WOOD, G. *Ethereum*: a secure decentralised generalised transaction. [*S. l.*: *s. n.*, 200-?]. Disponível em: https://gavwood.com/paper.pdf. Acesso em: 9 set. 2021.

## *Fique atento*

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

editora
papervest

Publicação da Papervest Editora
Av. Marechal Floriano, 947 - CEP: 88503-190
Fone: (49) 3225-4114 - Lages / SC
www.unifacvest.edu.br