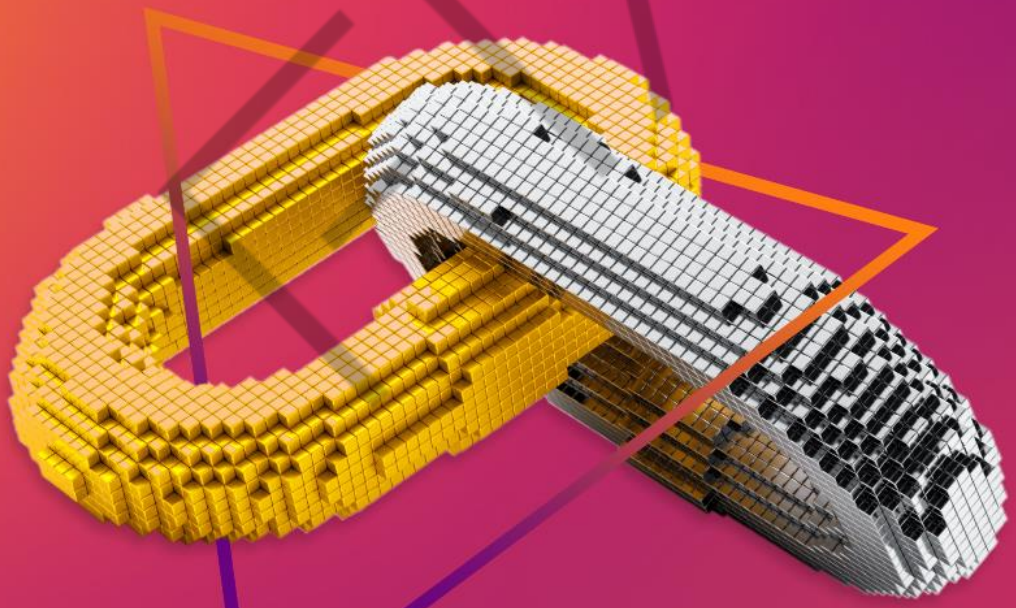
FIAP ON

BLOCKCHAIN ADVANCED

# BLOCKCHAIN, a Introdução

HENRIQUE POYATOS



01

## LISTA DE FIGURAS

## LISTA DE QUADROS

**SUMÁRIO**

# 1 *BLOCKCHAIN*, A INTRODUÇÃO

Muito se ouve falar sobre *blockchain*, especialmente o seu maior caso de sucesso, a criptomoeda conhecida como Bitcoin. No entanto, você sabe realmente como esta tecnologia funciona, que problemas ela se propõe a resolver e quais são seus benefícios em utilizá-lo? Falaremos sobre isso neste capítulo, venha conosco!

## 1.1 O problema da confiança

Do ponto de vista jurídico, uma transação é um negócio entre duas (ou mais) partes, pela qual os sujeitos de uma obrigação resolvem extingui-las mediante concessões recíprocas (GAGLIANO, 2006, p. 225), ou seja, as partes realizam ações visando quitar suas obrigações umas com as outras.

Ao ler a palavra “transação”, geralmente presumimos que se trata de uma transação financeira, como transferir dinheiro de uma pessoa a outra; porém, procure expandir o emprego dessa palavra, que pode ser utilizada para representar um processo de compra e venda, a contratação de um serviço, um reembolso de um plano de saúde, o pagamento de um prêmio de seguro em caso de sinistro automotivo, entre várias outras possibilidades.

Contudo, seres humanos não são plenamente confiáveis ou infalíveis: desde uma impossibilidade momentânea até nunca ter tido a intenção de cumprir suas obrigações com a outra parte, as transações podem não acontecer ou não se concluir por completo.

Como seres sociais, somos obrigados a colaborar uns com os outros o tempo todo; não dominamos todas as atividades e não possuímos todos os recursos para nossa subsistência e, por esta razão, dependemos uns dos outros. Um indivíduo que não colabora e não cumpre suas obrigações com os demais de seu grupo, tem sua reputação manchada e o estigma de alguém não-confiável provoca o afastamento automático do grupo, tornando-o um pária social. Isso acontece até hoje com alguns primatas e tem acontecido com seres humanos desde a época das cavernas.

No entanto, algo mudou substancialmente de vários séculos para cá: não vivemos mais em pequenos grupos com algumas dezenas de pessoas; muitos de

nós vivemos em metrópoles com milhões de habitantes. O mundo globalizado e a evolução dos meios computacionais e de comunicação providos pela Internet permitem transações internacionais e podemos fazer negócios com partes que estão literalmente do outro lado do mundo. Assim sendo, o que compelirá as partes a cumprir suas obrigações umas com as outras? Qual realmente é o impacto de me tornar alguém não-confiável na Nigéria ou na Austrália? Tendemos a cumprir nossas obrigações com nossas comunidades locais, mas não globais.

De forma a viabilizar transações entre duas partes que não se conhecem e, portanto, não confia uma na outra, existe o chamado **terceiro de confiança**. Trata-se de alguém que, por possuir a confiança das duas partes, **intermedia a transação e garante que estas irão cumprir suas obrigações**.

Algumas instituições se tornaram **terceiros de confiança por força de lei**, o que é chamado de **fé pública**. É o caso escrivães e servidores da Justiça, escrivães de polícia, oficiais de justiça, oficiais de registro civil, tabeliães, oficiais de registro de imóveis, funcionários públicos federais, entre outros. Quando um boletim de ocorrência é emitido por um escrivão de polícia, consideramos as informações contidas ali fidedignas; quando **um cartório atesta pela autenticidade de uma assinatura em um contrato, presumimos por fé pública que esta validação de identidade é confiável**.

Embora absolutamente necessário, existem alguns problemas no processo de confiança como ele é feito hoje. Em primeiro lugar, adiciona processos extras na transação entre as partes, tornando-a mais lenta e burocrática. No entanto, o grande problema da confiança é seu custo: quem atua como um terceiro de confiança vai cobrar para fazer este trabalho. Confiança custa caro!

Dependendo da transação que estamos realizando, o custo se torna alto, pois não temos um único intermediador garantindo a confiança, e sim vários: quando enviamos uma remessa de dinheiro internacionalmente pelos canais formais, temos várias instituições atuando como intermediárias (vide figura “Envio de dinheiro internacionalmente”). Empresas especializadas cobram, em média, 6,84% para transferência de remessas internacionais de dinheiro (THE WORLD BANK, 2019).

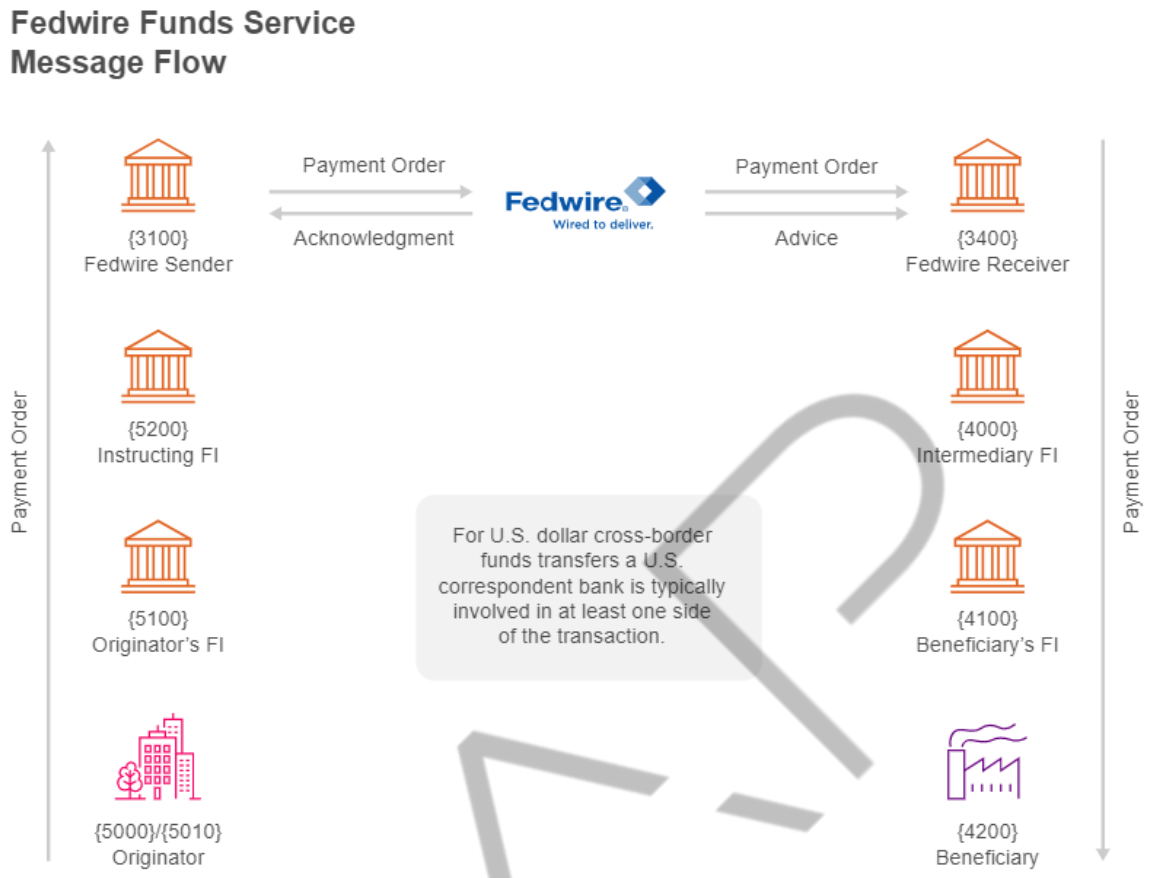



Figura 1.1 – Envio de dinheiro internacionalmente
Fonte: THE FEDERAL RESERVE (2017)

Por exemplo, se deseja transferir dinheiro para uma empresa estrangeira para pagá-la da forma tradicional, você dependerá do seu banco para informar ao banco (por meio de um ou mais bancos intermediários) que o dinheiro que você está enviando é legítimo. Pode levar alguns bons dias para que seu dinheiro chegue à conta deste intermediário. Por sua vez, a empresa estrangeira deve depender de seu banco para certificar essa legitimidade e cada etapa deste processo tem uma taxa; na verdade, você está pagando por "confiança" (WILLIAMS, 2019).

Vivemos em um mundo cada vez mais globalizado, cuja Internet atinge pontos do outro lado do globo em questão de milissegundos, que melhorou muito o fluxo de dados dentro e entre empresas e pessoas, mas não transformou a maneira como fazemos negócios. Isso ocorre porque a Internet foi projetada para mover informações - e não valor - de pessoa para pessoa (TAPSCOTT; TAPSCOTT, 2018). Há de se convir que a forma de se enviar dinheiro (ou mesmo outros ativos) não pode levar vários dias, ela precisa ser definitivamente repensada.

## 1.2 O livro-razão

Outro ponto importante em relação a transações é que estas precisam ser registradas para verificação posterior: se anos depois, uma das partes alegar que a outra não cumpriu sua parte na transação, é preciso verificar todos os registros efetuados na época para se determinar se a alegação é verdadeira ou falsa.

Transações financeiras, por sua vez, são registradas em um sistema conhecido como **livro-razão ou *ledger*** desde que foi inventado em 1494 pelo padre Luca Pacioli com o **objetivo de promover um balanço de ativos tangíveis e intangíveis, disponibilizando de forma ordenada e detalhada várias operações de crédito e débito e a composição de um balanço final**.

Vamos a um exemplo didático simples para demonstrar um livro-razão: imagine que André e Victor possuem 100 reais cada um. André resolve dar para Victor 50 reais, ficando com os 50 reais restantes, enquanto Victor agora possui 150 reais. O quadro “Exemplo de livro-razão” exemplifica como isso ficaria registrado.

| Evento | André | Victor |
|---|---|---|
| Saldos | 100 | 100 |
| Transferência de 50 | - 50 | + 50 |
| Saldos | 50 | 150 |

Quadro 1.1 – Exemplo de livro-razão
Fonte: Elaborado pelo autor (2019)

Em um sistema tradicional, a instituição bancária é o terceiro de confiança: em primeiro lugar, é ela quem faz a custódia dos 200 reais, o dinheiro não está nos bolsos de André e Victor, está todo com o banco; André comunica ao banco sua intenção de realizar uma transação cedendo 50 reais a Victor, e este terceiro de confiança registra a transação em seu livro-razão, comunicando a ambos de seu sucesso.

Figura 1.2 – Transação comercial envolvendo um terceiro de confiança
Fonte: Banco de imagens Shutterstock (2019)

Repare que, neste modelo, a **instituição bancária é a guardiã do livro-razão**, sendo a **única autorizada a realizar alterações nele**; se houver qualquer tipo de impasse futuro como, por exemplo, Victor alegar que jamais recebeu 50 reais de André, ambos podem recorrer à instituição bancária que exibirá a comprovação de que a transação realmente aconteceu. Contudo, para que este modelo todo funcione, **as partes envolvidas precisam confiar plenamente no intermediário**.

Conforme mencionado antes, confiança custa caro. A instituição bancária certamente vai cobrar pelos dois serviços prestados neste exemplo: a de realizar a **custódia da soma envolvida** (com todo o ônus implicado, como sofrer uma fraude ou ser furtado) e de **intermediar e promover a confiança das transações entre as partes**. Ou seja, falei que cada um possui 100 reais, provavelmente 90 reais seria mais acurado.

## 1.3 O livro-razão distribuído

Vamos propor algo mais inusitado: tirar o banco da jogada. A partir de agora, André e Victor cuidam de seu próprio dinheiro e cada um deles mantém seu próprio livro-razão, registrando as transações entre os dois.

Figura 1.3 – Cada parte controlando seu próprio livro-razão
Fonte: Banco de imagens Shutterstock (2019)

Claro que, neste momento, você deve estar pensando que isso não resolve o problema da confiança, pelo contrário, ele traz o problema de volta! No cenário proposto, uma parte deve confiar na outra, senão, nada feito. Por serem responsáveis cada um por seu livro-razão, se uma das partes resolver cometer uma fraude, basta realizar uma alteração estratégica em seu livro-razão e defender aquela mentira com unhas e dentes (realmente um cenário ficcional fantástico, nada parecido com os dias de hoje).

No quadro “Fraudes nos livros-razão de André e Victor” imaginamos um cenário extremamente pessimista, no qual um lado resolve passar a perna no outro: André resolve “passar uma borrachinha” na transferência que havia feito para Victor, voltando magicamente a ter cem reais, como lhe convém. Victor, por sua vez, conclui que para um número cinco virar um nove basta um risquinho no lugar certo, e a transferência de 50 reais passa a ser de 90.

| Livro-razão de André | | | Livro-razão de Victor | | |
|---|---|---|---|---|---|
| Evento | André | Victor | Evento | André | Victor |
| Saldos | 100 | 100 | Saldos | 100 | 100 |
| Transferência de 50 | - 50 | + 50 | Transferência de 90 | - 90 | + 90 |
| Saldos | 100 | 100 | Saldos | 10 | 190 |

Quadro 1.2 – Fraudes nos livros-razão de André e Victor
Fonte: Elaborado pelo autor (2019)

Abusando hoje das expressões de gente velha, o circo está armado, não é mesmo? André e Victor vão discutir sem fim um com o outro, afinal, é a palavra de um falsário contra o outro.

**Como resolver esse problema? Simples: colocando testemunhas nessa transação.** O livro-razão não será mais mantido apenas pelos envolvidos (André e Victor), vamos colocar várias pessoas registrando a mesma transação, com cópias idênticas do livro-razão. Assim, se um deles resolver adulterar algum registro, podemos comparar sua cópia com a de várias outras testemunhas, identificando e refutando a fraude.

Figura 1.4 – Outras partes comparando seus livros-razão
Fonte: Banco de imagens Shutterstock (2019)

Assim, podemos descartar os livros-razão discrepantes e fraudulentos, pois passa a valer o que está dizendo a maioria.

Talvez você já esteja se antecipando ao problema: Se André e Victor possuem apenas cinco testemunhas (como na figura “Outras partes comparando seus livros-razão”), basta que o fraudador convença três das testemunhas (de uma rede de sete membros) a alterar seus livros-razão da mesma forma que ele, corrompendo-os ao prometer a eles dividir os lucros do golpe. Sim, de fato isso pode ser um problema e tem até nome nesta literatura: ataque de 51%. **Sendo assim,**

**quanto mais membros esse sistema possuir, mais difícil de executar essa fraude se torna.**

Esse verdadeiro livro-razão distribuído permite registrar transações entre duas partes que não confiam uma na outra, suportados por uma rede de “testemunhas” (que passamos a chamar de validadores) cujos membros também não estão acima de qualquer suspeita, mas a maioria seguirá as regras estabelecidas, tornando a rede confiável. Pois este é o *modus operandi* básico do *Blockchain*, o qual Don Tapscott e Alex Tapscott (2018) gostam de chamar de “Protocolo da Confiança”.

## 1.4 Blockchain, o protocolo da confiança

A tecnologia *Blockchain* foi descrita pela primeira vez no *whitepaper* do Bitcoin de Satoshi Nakamoto (2008) como uma cadeira de blocos (e de assinaturas digitais) originalmente criada para rastrear o gasto dessa moeda digital, transação por transação. Nakamoto apoia sua invenção em trabalhos anteriores importantes, como de Back (2002), Merkle (1980) e Bayer, Haber e Stornetta (1993), tornando-se a primeira experiência bem-sucedida a resolver o problema do gasto duplo em uma rede descentralizada.

Contudo, o *whitepaper* de Nakamoto (2008) não utiliza o termo *blockchain* em momento algum, referindo-se à estrutura proposta como *chain of blocks* (cadeia de blocos). O termo seria usado pela primeira vez ainda em 2008 por Hal Finney, o número 2 do projeto Bitcoin, ao se referir à estrutura descrita por Nakamoto como *block chain*, ainda em duas palavras separadas (RICHBODO, 2017).

Além do problema do gasto duplo, o *blockchain* resolve outro grande problema descrito no exemplo da seção anterior: a alteração ou remoção de informações de um livro-razão. Em um registro feito em papel, a informação pode ser adulterada (ou o papel simplesmente substituído), eliminando os rastros de uma alteração. Com a digitalização de informações provida pela informática, o problema se intensificou, afinal, a arquitetura dos computadores foi concebida para que dados sejam alterados com facilidade. Como, então, efetuar registros de forma permanente e inalterável?

Para tal, o *blockchain* utiliza um engenhoso mecanismo dividindo a informação em blocos que são assinados digitalmente (de forma criptográfica) e encadeados, assim, para assinar um novo bloco, é preciso a assinatura do anterior. Alterar um bloco antigo faria com que a assinatura desste bloco mudasse, resultando na necessidade de alterar todos os blocos da cadeia.

Complicado por enquanto? Vamos fazer uma analogia: imagine que você queira guardar objetos e os armazene em caixas que, uma vez fechadas, são empilhadas, uma em cima da outra. Sempre que quiser guardar novos objetos, você lota uma nova caixa, fecha e a coloca no topo da pilha.

Agora imagine que você quer reorganizar ou remover objetos de uma delas, digamos que da segunda caixa: seria necessário tirar todas as caixas de cima dela, abrir, fazer as mudanças e recolocar as caixas na pilha novamente, na mesma ordem em que estavam (vide figura “Pilha de caixas como analogia ao *Blockchain*”).


Figura 1.5 – Pilha de caixas como analogia ao *Blockchain*
Fonte: Banco de imagens Shutterstock (2019)

Convenhamos, não há muito incentivo para fazer mudanças, certo? Vai dar um trabalho IMENSO realizar toda a operação; provavelmente você julgará mais

interessante deixar as coisas como estão. “Não preciso tanto assim do objeto da caixa dois”, você diria. Bem, o *blockchain* é como essa pilha de caixas, só que elas são transparentes: conseguimos ver todo o conteúdo dentro delas, mas não conseguimos alterá-los sem muito, muito trabalho envolvido. Quanto mais caixas, mais difícil essa alteração será; alterar o conteúdo da caixa dois com uma pilha contendo um milhão de caixas em cima tornará tal mudança virtualmente impossível.

> O Blockchain é uma tecnologia simples que, na sua forma mais básica, serve como um registro permanente e inalterável para quase qualquer tipo de informação que você gostaria de gravar. No entanto, essa simples tecnologia de contabilidade é uma plataforma ideal para a criação de todos os tipos de aplicativos inovadores e radicalmente novos (WILLIAMS, 2019, p. 35, tradução nossa)

Portanto, o *blockchain* pode ser definido como um livro-razão distribuído, engenhosamente arquitetado para armazenar informações de forma permanente e inalterável sem, para tal, precisar de uma autoridade central para isso; todo o processo é mantido por uma rede de participantes que seguem as mesmas regras e possuem o mesmo poder de decisão, coordenando seus esforços por meio de um consenso.

## 1.5 Tecnologias envolvidas

Conforme mencionado antes, a tecnologia do *Blockchain* é suportada por vários outros trabalhos anteriores e, porque não acrescentar, tecnologias que já existiam há algumas décadas. Vamos agora descrever a “trindade” tecnológica do *Blockchain*; sem eles, a tecnologia definitivamente não existiria.

### 1.5.1 Criptografia

Para a tecnologia do *Blockchain* e criptografia clássica utilizada, cifrar mensagens inteiras não é o carro-chefe, pois geralmente o conteúdo dos blocos contendo transações (ou quaisquer informações que quisermos preservar) são armazenados em texto puro, para facilitar a auditabilidade das informações ali contidas. Dúvidas sobre criptografia?

O que o *blockchain* utiliza em peso é um tipo específico de criptografia conhecida como função *hash* (ou *hashing*) na qual uma mensagem de qualquer tamanho é mapeada para uma mensagem de tamanho fixo, geralmente em hexadecimal.

Essa excelente propriedade torna a função *hash* muito útil para assinar digitalmente arquivos, documentos e, é claro, transações presentes em um bloco de *blockchain*, garantindo a identidade e autenticidade das transações armazenadas. Além disso, a função *hash* também é utilizada para assinar o bloco como um todo, "selando-o" para prevenir futuras alterações. Conforme mencionado antes, esse *hash* do bloco é propagado e utilizado como conteúdo do bloco seguinte, criando um encadeamento perfeito.

Figura 1.6 – Cadeia de peças de quebra-cabeça, o encaixe perfeito dos blocos de *blockchain*
Fonte: Banco de imagens Shutterstock (2019)

Ao observar a figura "Cadeia de peças de quebra-cabeça, o encaixe perfeito dos blocos de blockchain", digamos que haja uma alteração no conteúdo de um bloco já estabelecido anteriormente, a peça vermelha de nosso quebra-cabeça, e essa exigiria um novo processo de "selamento", gerando um *hash* completamente diferente. Esse, por sua vez, havia sido propagado para o bloco seguinte (peça roxa), que já não se encaixa perfeitamente na peça vermelha, precisando ser novamente assinada/selada com o novo *hash* anterior, e assim sucessivamente. Todas as peças azuis e verdes seguintes teriam que ser revalidadas.

É graças à função *hash* que um *blockchain* adquire suas propriedades de autenticidade e imutabilidade.

### 1.5.2 Redes ponto-a-ponto (*P2P networks*)

A maior quebra de paradigma da tecnologia *blockchain* é a descentralização do sistema, funcionando de forma distribuída. Contudo, a topologia predominante em redes de computadores é o modelo centralizado (vide figura “Topologia de rede centralizada”), da qual possuímos um servidor central que concentra as decisões e regras, e as máquinas cliente, que simplesmente obedecem ao nó central.

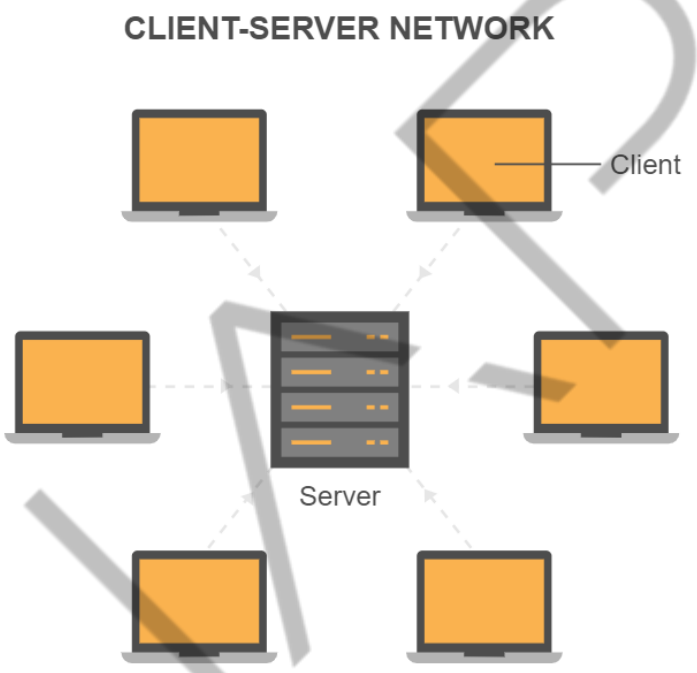



Figura 1.7 – Topologia de rede centralizada (ou cliente-servidor)
Fonte: Banco de imagens Shutterstock (2019)

É exatamente dessa maneira que a maioria dos sistemas presentes na Internet funcionam. Por mais que, graças ao *Cloud Computing*, não seja um único nó central, mas dezenas de nós, a verdade é que, se todos eles se tornarem indisponíveis de uma só vez, o sistema simplesmente sai do ar.

Embora existam vários exemplos para ilustrar este mecanismo, usaremos um em particular: O Napster. Já ouviu falar no Napster? Tratava-se de uma rede de compartilhamento de arquivos musicais em MP3 que surgiu em 1999 e se tornou uma febre mundial. Por permitir compartilhar arquivos protegidos por leis de direitos autorais, a empresa foi processada pela *Recording Industry Association of America* (RIAA). Em 2001, foi obrigada a desativar seus servidores (os nós centrais). No momento em que isso aconteceu, o sistema todo parou de funcionar.


Figura 1.8 – Usuário acessando o Napster
Fonte: Banco de imagens Shutterstock (2019)

Topologia com nós centrais não é a única possibilidade, entretanto: existem as redes de ponto-a-ponto, ou *peer-to-peer* (P2P) *networks*. Nessa modalidade, não há nós centrais, porque todos os membros da rede são servidores e clientes ao mesmo tempo. As requisições não passam necessariamente por nós que organizam e controlam os trabalhos, pois seus membros trocam dados diretamente e coordenam suas ações em consenso (vide figura “Topologia de rede centralizada”).

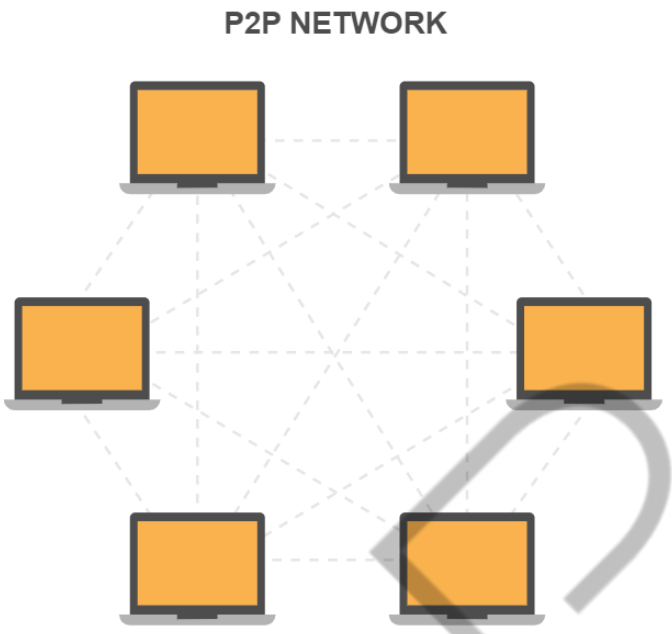



Figura 1.9 – Topologia de rede centralizada
Fonte: Banco de imagens Shutterstock (2019)

Repare que não há uma hierarquia definida nesste tipo de rede de computadores; todos são membros e seguem as regras igualitariamente. Quando o consenso é atingido por, digamos, um algoritmo de votação, todos os nós têm o mesmo direito a voto, cujo peso é o mesmo.

O maior exponente das redes ponto-a-ponto é o BitTorrent, utilizado para compartilhamento de músicas, séries de TV, filmes e jogos. Como a maioria dos arquivos compartilhados nesse sistema também é protegida por direitos autorais (e seu compartilhamento configura pirataria), não apenas a RIAA, mas várias gravadoras e estúdios de Hollywood já pediram o bloqueio do sistema na justiça. Contudo, BitTorrent não é uma empresa que possa ser processada. Além disso, não existem servidores centrais que pudessem ser bloqueados para inviabilizar o serviço; como uma Hidra, o ser mitológico com corpo de dragão e várias cabeças de serpente, quando você corta uma cabeça, duas nascem no lugar. O BitTorrent não pode ser parado e continua funcionando, décadas depois.

Por conta de sua natureza descentralizada, *blockchains* funcionam em redes ponto-a-ponto como a utilizada pelo BitTorrent.

### 1.5.3 Software livre e de código-fonte aberto

Retomando a questão do movimento do software, por que o código-fonte aberto é fundamental para a tecnologia *blockchain*? Além de ser um sistema menos vulnerável a falhas, permite que todos possam **auditar o *software*** e ter plena certeza de como ele funciona. Somente dessa maneira temos certeza de que todos na rede de *blockchain* estão sujeitos às mesmas regras, que não há nenhuma espécie de *backdoor* favorecendo este ou aquele grupo de usuários. Nesse cenário hipotético, o usuário de uma *backdoor* de *blockchain* não estaria sujeito às mesmas regras rigorosas que outros participantes, obtendo assim algum favorecimento indevido. O acesso integral ao código-fonte permite vistoriá-lo e ter certeza de que tais favorecimentos não existem.

Além disso, o software livre proporciona um ecossistema diverso. Por ter seu código-fonte disponível no GitHub (http://github.com/bitcoin), existem centenas de criptomoedas disponíveis atualmente que são derivações do código original do Bitcoin, cada uma com uma característica diferente (e outras são meros clones baratos, mas isso é assunto para outro capítulo).

## 1.6 Benefícios esperados

A implementação da tecnologia *Blockchain* pode resultar em uma série de benefícios na solução dos problemas. Vejamos a seguir alguns deles.

### 1.6.1 Descentralização de poder

A natureza descentralizada do *blockchain* promove um ecossistema equilibrado, com todos os participantes possuindo o mesmo poder que os demais. Por vezes, entidades centralizadoras exercem seu poder político ou econômico para defender seus interesses, o que acaba desequilibrando o ambiente de negócios. Em um blockchain, todos os participantes dividem o poder igualitariamente.

> [...] por distribuído, quero dizer que o sistema não tem autoridade central, ao contrário de quase todos os sistemas aos quais estamos acostumados, mas é executado em comunidade, com todos os participantes alcançando um consenso sobre as decisões. Em um

> sistema distribuído puro, não há hierarquia, nem presidente, nem pai, nem CEO. Quando todos os participantes são valorizados, as regras dos negócios, da criatividade e da sociedade mudam. (WILLIAMS, 2019, p. 234)

Para um exemplo mais tangível nessa área, saiba que moedas soberanas como o real brasileiro ou dólar americano são monopólios de seus governos, que reservam a si o direito de emissão da moeda. Quando convém aos seus interesses, governos aceleram a taxa de emissão de sua moeda e aumentam sua oferta no mercado, o que pode resultar em inflação e perda de poder de compra, prejudicando todos os outros participantes (empresas e cidadãos). No caso de uma criptomoeda como o Bitcoin, a taxa de emissão de novas criptomoedas é regulamentada e constante, não podendo ser alterada por um participante em específico. Nesse caso, não há como um membro de rede *blockchain* exercer seu poderio para impor seus interesses aos demais, o poder é compartilhado por todos.

> Ao ingressar, você se torna parte de um sistema que pode incluir centenas, milhares ou até milhões de pessoas e máquinas conectadas, todos vocês no mesmo campo de jogo, sem controle hierárquico. A natureza efêmera das cadeias esconde como elas podem conceder às pessoas um poder sem precedentes nos mercados de ideias, governança e finanças (WILLIAMS, 2019, p. 62).

### 1.6.2 Imutabilidade

Conforme mencionado anteriormente, a função *hash* provida pela criptomoeda moderna foi engenhosamente aplicada por Nakamoto (2008) para encadear os blocos de um *blockchain*, formando elos de uma corrente. Como já explicado antes, no exemplo da pilha de caixas ou nas peças do quebra-cabeça, o encadeamento de *hashes* concede à tecnologia a propriedade de imutabilidade, ou seja, as informações ali contidas são virtualmente permanentes e inapagáveis.

> A natureza imutável das transações em uma *blockchain* pode eliminar essa necessidade de intermediários e pagamentos, porque o dinheiro foi gravado indiscutivelmente como seu para gastar. Cada vez que é transferido, o novo proprietário é gravado. Você não pode "gastar o dobro" do seu dinheiro ou afirmar ter dinheiro que não possui. (WILLIAMS, 2019, p. 96)

Além da clara credibilidade para um sistema financeiro (afinal sua transação não vai sumir, ela está registrada para todo o sempre), a imutabilidade do *blockchain*

pode ser útil em diversas outras aplicações, praticamente qualquer coisa que queiramos registrar de forma indelével: direitos autorais, registros de compra e venda de imóveis, rastreio de bens em uma cadeia logística, ou seja, as possibilidades são inúmeras!

### 1.6.3 Auditabilidade

Um dos benefícios inegáveis da tecnologia *blockchain* é sua grande auditabilidade. Como as informações estão gravadas de forma permanente e sempre disponíveis, todas as transações podem ser auditadas, permitindo uma grande rastreabilidade de um ativo. Tentativas de fraude, movimentações suspeitas, tudo é registrado de forma inapagável.

### 1.6.4 Resistência a censura

Como pode ser observado no exemplo do Napster x BitTorrent, uma rede descentralizada ponto-a-ponto não pode ser bloqueada ou detida: seria centenas ou milhares de endereços de internet (o endereço IP) a serem bloqueados e, o maior problema, os participantes da rede podem mudar o tempo todo!

Redes descentralizadas se tornam resistentes à censura e, na prática, inviabilizam algum tipo de proibição ou reserva de mercado por parte de nações inteiras.

Países no mundo inteiro já compreenderam que as criptomoedas não podem ser paradas: segundo o COIN.DANCE (2019), apenas sete países no mundo inteiro (Peru, Argélia, Macedônia, Arábia Saudita, Afeganistão, Paquistão, Bangladesh e Vietnã) proíbem o uso de criptomoedas, enquanto os demais provavelmente já concluíram que é como “tapar o sol com uma peneira”.

### 1.6.5 Resiliência

Além da resistência à censura, podemos destacar a alta resiliência de um sistema utilizando tecnologia de *blockchain*: enquanto houver ao menos dois membros participantes, os blocos continuam a ser gerados e registrados e as

transações acontecerão. Não há nós centrais que possam ser atacados física ou ciberneticamente, retirando o sistema do ar.

Para se ter uma ideia, o *blockchain* do Bitcoin está há mais de dez anos em funcionamento sem interrupção, com uma taxa de disponibilidade (*uptime*) de 99,99%. Qual sistema tecnológico pode se gabar de uma marca tão incrível?

### 1.6.6 Múltiplas cópias de segurança

Quem vive a tecnológica sabe o quanto cópias de segurança (backups) são importantes. Todos os participantes de um *blockchain* que queiram realizar todas as ações disponíveis em um sistema como esse precisam ter uma cópia completa deste, tornando-se o que chamamos de *fullnode*, ou nó completo.

Estima-se que, no caso do Bitcoin, existam quase cem mil *fullnodes* (CANELLIS, 2019), cada um deles possuindo uma cópia completa de seu *blockchain*, ou seja, para as transações em Bitcoin sumirem da face da Terra, estas cem mil cópias teriam que ser apagadas. Provavelmente é o “banco de dados” com o maior número de backups da atualidade. Enquanto existirem *fullnodes*, as transações de todos existirão.

## 1.7 *Blockchain* é a “bala de prata”?

A importância do *blockchain* é respalda pela Gartner Inc, uma empresa global de consultoria e pesquisa que fornece informações, consultoria e ferramentas para empresas nas áreas de TI, finanças, RH, atendimento e suporte ao cliente, funções legais e de conformidade, marketing, vendas e cadeia de suprimentos, sendo uma das empresas mais respeitadas dests segmento.

Em seus relatórios, tornam-se populares os *hype cycles,* representações gráficas criadas pela empresa americana para representar a maturidade, adoção e aplicação social de tecnologias em específico. Para eles, toda tecnologia passa por:

- **Gatilho de inovação:** quando provas de conceito surgem e há uma publicidade positiva em torno da tecnologia, embora geralmente não haja produtos e a viabilidade comercial não é comprovada.

- **Pico das expectativas inflamadas:** o auge das expectativas, o *hype* é alcançado aqui.
- **Vale da desilusão:** quando o mercado “cai na real”, compreendendo as vantagens e finalmente enxergando as desvantagens do emprego da tecnologia, que deixa de ser a “bala de prata”.
- **Inclinação da iluminação:** é repensada a forma como a tecnologia pode ser útil para as empresas; novas provas de conceito e produtos surgem, startups que empregam a tecnologia começam a prosperar de maneira mais madura, enquanto as empresas mais conservadoras continuam neutras.
- **Platô da produtividade:** a tecnologia se estabelece de maneira sadia e madura; até mesmo as empresas mais conversadoras passam a investir na tecnologia, que se estabeleceu e veio para ficar.

Constando por anos nos *hype cycles* de tecnologias emergentes da Gartner, as tecnologias derivadas do *Blockchain* ganharam, em 2019, um *hype cycle* só seu, o que denota um grande interesse e estudo dessa respeitável consultoria no assunto. Segundo o Gartner (s.d.; 2019), em 2023 tecnologias de *blockchain* farão o rastreio de bens e serviços no valor de dois trilhões de dólares anuais. Contudo, as tecnologias do Blockchain ainda levarão de cinco a dez anos para promover um impacto a ponto de transformar o mercado e sua maturidade é prevista para 2025, quando a rede mundial de computadores deixa de ser a “Internet do Conteúdo” para se tornar a “Internet do Valor”.

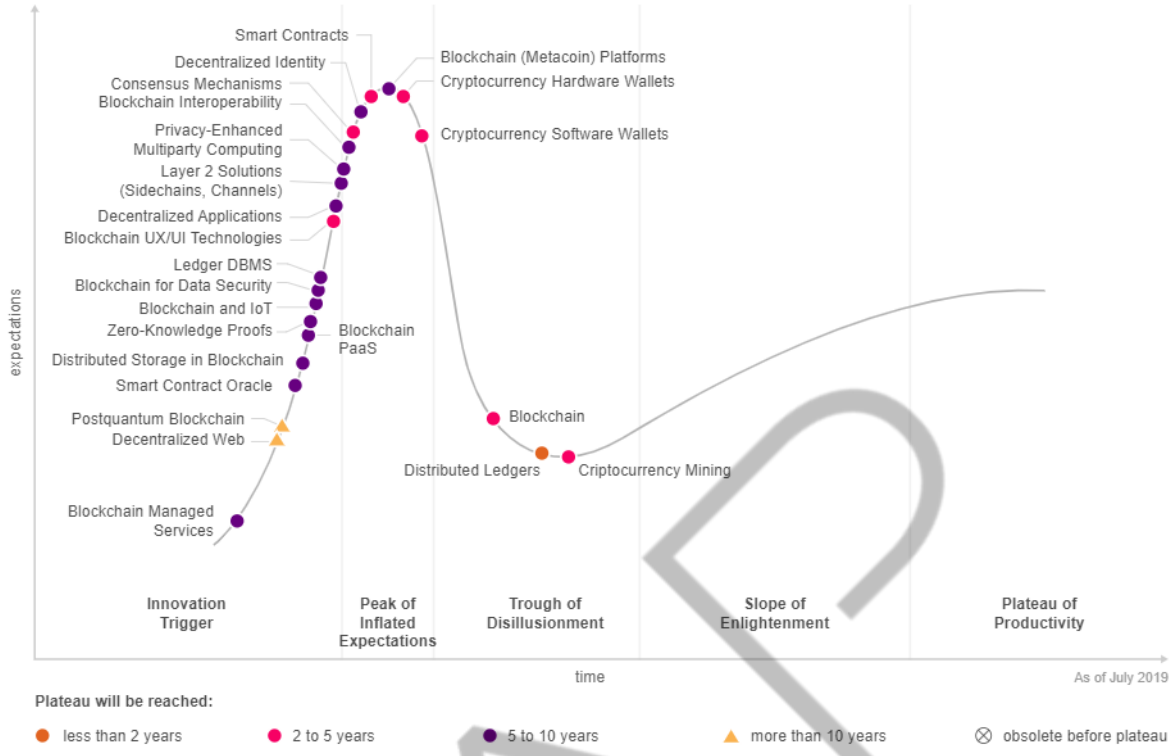



Figura 1.10 – Hype Cycle para tecnologia de Blockchain em 2019
Fonte: GARTNER (2019)

Respondendo à provocação no início desta seção, *Blockchain* é a bala de prata? Absolutamente não. A tecnologia deve ser aplicada apenas em situações nas quais informações devem ser armazenadas de maneira inalterável e intermediações queiram ser simplificadas ou eliminadas. Quaisquer outras necessidades que não tenham como objetivo esses dois fatores, a tecnologia não é recomendada, possivelmente contraindicada. Como podemos ver no gráfico do Gartner, rumamos para uma era além do *hype* tecnológico, quando o *blockchain* será empregado de maneira madura e responsável.

## 1.8 Conclusão

A tecnologia *Blockchain* possui um enorme potencial transformador e pode revolucionar tudo o que pensamos de sistemas confiáveis nos próximos anos. Contudo, conforme discutido neste capítulo, está longe de ser a solução para todos os problemas, além de ser uma tecnologia que deve atingir sua maturidade nos próximos anos.

É fundamental nos mantermos atualizados nas tecnologias emergentes da atualidade, sendo capazes de utilizar a tecnologia mais adequada na solução de problemas.

Discutirmos mais sobre aplicabilidade da tecnologia, seu funcionamento e implicações de segurança em capítulos vindouros. Até lá!

# REFERÊNCIAS

BACK, Adam. **Hashcash - a denial of service counter-measure.** 2002. Disponível em: <http://www.hashcash.org/papers/hashcash.pdf>. Acesso em: 18 nov. 2019.

BAYER, D.; HABER, S.; STORNETTA, W. S. **Improving the efficiency and reliability of digital time-stamping.** Sequences II: Methods in Communication, Security and Computer Science, páginas 329-334, 1993. Disponível em: <https://www.math.columbia.edu/~bayer/papers/Timestamp_BHS93.pdf>. Acesso em: 18 nov. 2019.

CANELLIS, David. **Bitcoin has nearly 100,000 nodes, but over 50% run vulnerable code.** 2019. Disponível em: <https://thenextweb.com/hardfork/2019/05/06/bitcoin-100000-nodes-vulnerable-cryptocurrency/>. Acesso em: 19 nov. 2019.

COIN.DANCE. **Bitcoin Legality by Country Summary.** 2019. Disponível em: < https://coin.dance/poli/legality>. Acesso em: 19 nov. 2019.

FREE SOFTWARE FOUNDATION. **General Public License (GPL) versão 3.** 2007. Disponível em: < https://www.gnu.org/licenses/gpl-3.0.en.html>. Acesso em: 18 nov. 2019.

GAGLIANO, Pablo Stolze. **Novo Curso de Direito Civil. Obrigações.** 6ª edição. São Paulo: Saraiva, 2006.

GARTNER. **Blockchain: What's Ahead?** Disponível em: <https://www.gartner.com/en/information-technology/insights/blockchain>. Acesso em: 19 nov. 2019.

GARTNER. **Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact.** 2019. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact>. Acesso em: 19 nov. 2019.

MERKLE, Ralph C. **Protocols for public key cryptosystems.** Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, páginas 122-133, 1980. Disponível em: <https://www.researchgate.net/profile/Ralph_Merkle/publication/220713913_Protocols_for_Public_Key_Cryptosystems/links/00b495384ecda07784000000/Protocols-for-Public-Key-Cryptosystems.pdf>. Acesso em: 18 nov. 2019.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 18 nov. 2019.

RICHBODO. **Usage of the word "blockchain".** 2017. Disponível em: < https://medium.com/@richbodo/common-use-of-the-word-blockchain-5b916cecef29>. Acesso em 18 nov. 2019.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.** 2a. Edição. New York: Portfolio/Penguin, 2018.

THE FEDERAL RESERVE. **Sending or Receiving International Wires via the Fedwire Funds Service.** 2017. Disponível em: <https://www.youtube.com/watch?v=GSd2gZ8-bzQ>. Acesso em: 11 nov. 2019.

THE WORLD BANK. **Remittances Prices Worldwide.** 2019. Disponível em: <https://remittanceprices.worldbank.org/en>. Acesso em: 11 nov. 2019.

WIKIMEDIA COMMONS. **How a hash function works.** 2014. Disponível em: <https://simple.wikipedia.org/wiki/Hash_function#/media/File:Hash_function.svg>. Acesso em 19 nov. 2019.

WIKIMEDIA COMMONS. **Um bastão reconstruído dos gregos antigos, a Cítala era utilizada para envio de mensagens secretas.** 2007. Disponível em: <https://pt.wikipedia.org/wiki/Criptografia#/media/Ficheiro:Skytala&EmptyStrip-Shaded.png>. Acesso em 19 nov. 2019.

WILLIAMS, Stephen P. **Blockchain: the next everything.** New York: Scribner, 2019.

## GLOSSÁRIO

| | |
|---|---|
| ***backdoor*** | É um método, geralmente secreto, de escapar de uma autenticação ou criptografia normais em um sistema computacional, um produto ou um dispositivo embarcado ganhando acesso indevido a ele. |
| **Gasto duplo (ou *double spending*)** | Gasto duplo é uma falha em potencial em mecanismos de dinheiro digital na qual uma única moeda (ou *token*) acaba sendo utilizada mais de uma vez. Diferentemente do dinheiro físico (que é único), um *token* digital pode ser falsificado ou duplicado, propriedades não desejáveis para ativos financeiros. |