

ANDRÉ FRANCO    VINÍCIUS BAZAN

PREFÁCIO SAFIRI FELIX

# CRIPTO MOEDAS

MELHOR QUE DINHEIRO



EMPIRICUS

# CRIPTO MOEDAS

## MELHOR QUE DINHEIRO

ANDRÉ FRANCO      VINÍCIUS BAZAN

PREFÁCIO SAFIRI FELIX

# CRIPTO MOEDAS

## MELHOR QUE DINHEIRO

1<sup>a</sup> edição

São Paulo • 2018



Colaboração  
**SAFIRI FELIX**

Coordenação do Projeto  
**BRUNO MONTEIRO**

Edição  
**RAFAEL BRANDIMARTI**

Revisão  
**ERIKA SÁ, GABRIEL MIRANDA & SANDRA GUERREIRO**

Capa  
**FERNANDO BARRETO**

Diagramação  
**THALES MAIRESSE**

Projeto Gráfico  
**FERNANDO BARRETO, THALES MAIRESSE & THIAGO SOUZA**

#### DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

Franco, André

Criptomoedas: melhor que dinheiro [livro eletrônico] / André Franco, Vinícius Bazan; prefácio Safiri Felix. - São Paulo : Empiricus, 2018. 206 p.

Formato: PDF

ISBN: 978-85-92581-17-6

1. Moedas digitais 2. Criptografia 3. Bitcoin 4. Transferência eletrônica de fundos I. Bazan, Vinicius II. Felix, Safiri III. Título.

CDD-332.4

Índices para catálogo sistemático:

1. Moeda: Economia financeira 332.4

Empiricus, 2018  
Todos os direitos reservados

#### **Empiricus Research**

Pátio Victor Malzoni

Av. Brigadeiro Faria Lima, 3.477 – 10º andar

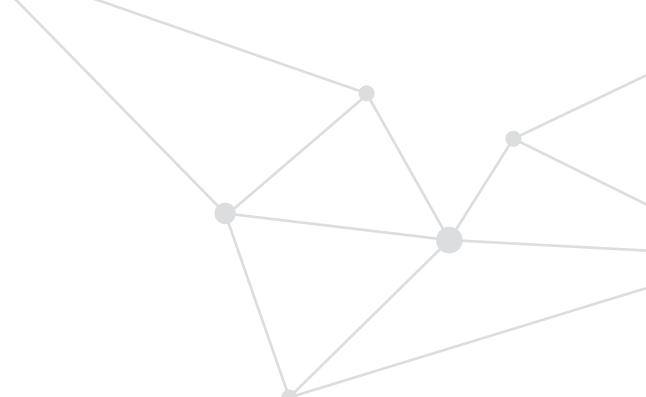
Itaim Bibi – São Paulo/SP | CEP 04538-133

[www.empiricus.com.br](http://www.empiricus.com.br)

*À Empírico,*

*que nos ensinou que o poder sobre o  
dinheiro pertence às pessoas comuns,  
não apenas aos engravatados.*





## *AGRADECIMENTOS*

Este livro é fruto de meses de estudo e esforço para traduzir nossa visão sobre o mercado de criptomoedas em algumas páginas. Apesar das incontáveis horas que dedicamos a ele, nada seria feito sem o apoio das demais pessoas que contribuíram para a realização deste trabalho. Portanto, queremos deixar aqui nosso mais sincero agradecimento àqueles que fizeram parte deste projeto.

Nosso muito obrigado à Empiricus por ter nos acolhido desde 2016, quando iniciamos uma conversa despretensiosa com o Rodolfo Amstalden. Ainda nos lembramos de nossa primeira reunião, em que o Rodolfo perguntou: “Como a gente pode ajudar vocês?”. Pedimos para usar o estúdio da empresa para gravar as aulas do curso online sobre educação financeira que havíamos planejado. Apesar de simples, aquele favor mudaria completamente o rumo de nossas carreiras. Somos muito gratos à Empiricus, em especial aos seus sócios-fundadores — Rodolfo Amstalden, Felipe Miranda e Caio Mesquita —, e a todos os seus colaboradores que, desde o início, fizeram de tudo para nos ajudar a alcançar os objetivos propostos.

Abaixo, expressamos nossos agradecimentos àqueles que colaboraram de forma direta para a elaboração deste livro:

Ao Safiri Felix, pela parceria, por ter entrado de cabeça conosco no projeto de elaborar publicações sobre investimento em criptomoedas e por ter trazido ensinamentos valiosos ao longo desse caminho; à Erika Sá e Sandra Guerreiro, que, junto com a equipe de Edição da Empiricus, nos ajudaram a estruturar o livro, organizar ideias e tornar tudo mais claro (sem vocês, ninguém entenderia o que estamos falando aqui); à Beatriz Nantes e Roberto Altenhofen, que foram indispensáveis na organização do projeto e na reflexão sobre como trazer para o leitor algo que o instigasse e fosse uma informação valiosa; à Olivia Alonso, da Inversa Publicações, cujos conteúdos sobre educação financeira nos fisgaram de vez e fizeram com que nos dedicássemos a ajudar investidores iniciantes em sua caminhada rumo à independência financeira; ao Frederico Rosas, o “monstro sagrado”, por todos os conselhos e conversas de bar, em que grandes ideias surgiram; ao Renzo Fedri e sua equipe de vídeo, que operam verdadeiros milagres e que nunca mediram esforços para produzir conteúdos que impactassem os espectadores de forma positiva; ao Bruno Monteiro, Fernando Barreto, Thales Mairesse, Thiago de Souza, Priscila Vieira, Raquel Kiss, Ricardo Tozo e Pedro Fogaça, que foram essenciais em diversos aspectos do projeto, desde a preparação até a produção gráfica, a confecção do livro e a organização operacional; e a todas as outras pessoas que, direta ou indiretamente, dedicaram horas dos seus dias para tornar este projeto possível.

E, é claro, por último, mas não menos importante, nosso muito obrigado ao lendário Satoshi Nakamoto, criador do Bitcoin, sem o qual este livro seria um conjunto de páginas em branco.

*“Tudo é óbvio depois que aconteceu.”*

NASSIM N. TALEB



# *SUMÁRIO*

13	<i>PREFÁCIO</i>
21	<i>INTRODUÇÃO POR QUE É MELHOR QUE DINHEIRO?</i>
31	<b>UMA BREVE HISTÓRIA DO SISTEMA FINANCEIRO</b>
45	<b>A REVOLUÇÃO — ESTRELANDO: O BITCOIN</b>
59	<b>O <i>HYPE</i> E A PERGUNTA: É BOLHA?</b>
77	<b>ANATOMIA DE UMA INOVAÇÃO</b>
97	<b>BLOCKCHAIN: A TECNOLOGIA DISRUPTIVA QUE VAI MUDAR O MUNDO</b>
113	<b>ALÉM DO DINHEIRO: O UNIVERSO DAS OUTRAS CRIPTOMOEDAS</b>
131	<b>GUIA PRÁTICO PARA INVESTIR EM CRIPTOMOEDAS PARTE 1 — COMO COMPRAR</b>
147	<b>GUIA PRÁTICO PARA INVESTIR EM CRIPTOMOEDAS PARTE 2 — ESTRATÉGIAS DE INVESTIMENTO</b>
169	<b>CONCLUSÃO OU O PRIMEIRO PASSO?</b>
177	<i>APÊNDICE</i> <b>COMO ME APAIXONEI DE VEZ PELAS CRIPTOMOEDAS: UMA VISÃO TÉCNICA SOBRE O BITCOIN</b>
197	<b>GLOSSÁRIO</b>
205	<b>REFERÊNCIAS</b>





## *PREFÁCIO*

*por Safiri Felix*

No começo de dezembro de 2011, sentado no sofá, tive meu primeiro contato com a tecnologia que mudaria a minha carreira. Enquanto zapeava os canais de televisão, me deparei com o programa Mod, na MTV Brasil, que falava sobre cultura pop, tecnologia e ciberativismo, apresentado pelo até então desconhecido Ronaldo Lemos, que mais tarde se tornaria colunista da Folha de S.Paulo e da GloboNews. Aquele episódio explicou rapidamente uma tecnologia que emergia e prometia ser disruptiva: o Bitcoin.

Pela primeira vez, eu ouvia sobre a moeda digital que circula pela internet, sem controle de nenhuma empresa ou governo, e conecta diretamente usuários, de forma muito parecida à dos aplicativos para baixar filmes e músicas que eu usava com frequência.

Aquilo despertou minha curiosidade, mas não a ponto de me fazer buscar mais informações sobre o assunto. Posso dizer que, naquele instante, não compreendi o quanto interessante era aquela

tecnologia, cujas características especiais a tornam diferente de qualquer outra. Quando começou um episódio de South Park na sequência, eu já havia praticamente esquecido o Bitcoin.

Curiosamente, essa história é parecida com a de muitas pessoas que se envolveram com moedas digitais. À primeira vista, o Bitcoin pode passar despercebido ou ser confundido com as manias especulativas que aparecem de tempos em tempos. De imediato, pouquíssimas pessoas conseguem entender os fundamentos essenciais dessa rede de pagamentos impossível de ser controlada e imune à censura.

Naquela época, um bitcoin custava algo em torno de US\$ 3 e era um experimento restrito a membros de fóruns de discussão online sobre software livre e criptografia, frequentados basicamente por anarquistas e libertários. Se uma pessoa tivesse me dito que aquilo um dia valeria mais de US\$ 100, dificilmente eu a teria levado a sério.

Desde muito cedo, tive acesso à tecnologia. Meu pai sempre teve um espírito *maker*, e um de seus *hobbies* era montar e desmontar computadores em casa. Lembro-me nitidamente do PC 286, com o monitor bege e a tela verde, que ficava na sala de casa, no início dos anos de 1990. Recordo-me de ter aberto a minha primeira conta de e-mail aos 14 anos e da incrível sensação de poder me comunicar instantaneamente com qualquer pessoa do mundo. Logo em seguida, veio a desilusão: não existia ainda nada muito divertido ou útil na internet. A rede era um ambiente primordialmente para estudos acadêmicos, frequentada por alguns poucos nerds.

Cresci sob a influência da incontrolável inflação brasileira dos anos de 1980 e 1990 e com a imagem de que economistas tinham superpoderes graças ao “milagre” do Plano Real.

Na hora de prestar vestibular, estudar Economia me pareceu um caminho interessante. Após quatro anos inesquecíveis no interior

de São Paulo, estudando na Unesp de Araraquara, passei um ano em Londres e trabalhei nas mais variadas ocupações enquanto aprimorava o meu inglês.

Foi então que aprendi na prática a importância de ter moeda forte. Com as poucas reservas acumuladas em libras dos trabalhos que tive na Inglaterra, consegui retornar ao Brasil com capital para investir em um momento em que o mercado de ações vivia um período de grande euforia. O ano de 2007 ficou marcado por uma série de IPOs (ofertas públicas iniciais de ações) na Bovespa, atual B3, pela descoberta das reservas do pré-sal e também pelas perspectivas otimistas de crescimento econômico.

Ao voltar a São Paulo, cursei Administração de Empresas no Mackenzie e iniciei minha carreira no mercado financeiro. Isso me levou naturalmente a desenvolver um interesse especial por renda variável. Estudei sobre os diversos produtos financeiros e tomei confiança para arriscar em minhas primeiras operações.

O ambiente de otimismo com a Bolsa era um prato cheio para ganhos de curto prazo, especialmente para quem operava também no mercado de opções, no qual centavos poderiam literalmente se multiplicar em questão de horas. Ganhar e, acima de tudo, perder dinheiro com ações e opções foi meu treinamento prático para identificar oportunidades e aproveitar assimetrias de preço.

Em 2013, depois de algumas lições aprendidas no mercado e das primeiras experiências como empreendedor, o Bitcoin cruzou novamente o meu caminho. Dessa vez, contudo, foi como se eu tivesse mergulhado de cabeça em uma piscina de fundo infinito. Não consegui mais voltar à superfície para buscar oxigênio. Decidi aprender a respirar embaixo d'água.

O preço do bitcoin havia ultrapassado a marca dos US\$ 100 e vários veículos de mídia publicaram reportagens sobre a moeda digital, com um conteúdo que poucas pessoas conseguiam entender.

Em poucos meses, a cotação ultrapassou os US\$ 1.200, e os primeiros analistas levantaram a questão: estamos diante de uma bolha?

Decidi me aprofundar no assunto e comprei minhas primeiras moedas em uma transação *peer-to-peer* (P2P)<sup>1</sup> com um usuário de um dos fóruns online de Bitcoin para brasileiros. Naquele momento, meu interesse era puramente especulativo. Os termos discutidos no fórum eram incompreensíveis e existia uma forte vinculação da moeda digital com o comércio ilegal na *deep web*.

No ano seguinte, eu já operava com frequência e meu entendimento sobre os fundamentos da tecnologia aumentava gradativamente. A escassez intrínseca e os incentivos econômicos por trás do protocolo do Bitcoin foram as propriedades que mais me chamaram atenção, assim como a possibilidade de criar um sistema monetário totalmente controlado por software.

Em abril de 2014, participei da primeira conferência brasileira de Bitcoin e conheci algumas pessoas com as quais havia começado a interagir pelo fórum de discussão no Facebook. À época, o grupo era formado majoritariamente por libertários, simpatizantes do Partido Pirata e alguns entusiastas da corrente de pensamento econômico da Escola Austríaca. Nesse período, começava a se formar a primeira onda de startups de Bitcoin no Brasil.

O mercado se concentrava no P2P e as primeiras corretoras tinham pouquíssima liquidez. Comecei a enxergar uma grande oportunidade de prover alternativas de liquidez no mercado brasileiro e de utilizar o Bitcoin como plataforma para serviços financeiros até então exclusivos aos bancos.

Em algumas semanas, a ideia tomou forma e eu me tornei um dos cofundadores da Coinverse, um serviço de compra e

---

1. Termo usado em arquitetura de redes de computadores que indica a ligação ponto a ponto. Também comumente usado para definir transações de valores que ocorrem sem um intermediário. No caso, uma compra/venda de bitcoin entre duas pessoas, sem utilizar uma corretora.

venda de bitcoin, que contava com o primeiro caixa eletrônico de criptomoedas da América Latina.

No fim de junho de 2014, pouco tempo antes do início da Copa do Mundo de futebol no Brasil, colocamos o caixa eletrônico em operação, apostando na divulgação dos benefícios e diferenciais do bitcoin em um mercado ainda incipiente.

Por causa do *frisson* provocado pela instalação de um caixa eletrônico de bitcoin em São Paulo, várias reportagens foram feitas e a repercussão em torno do lançamento me posicionou na comunidade brasileira como uma das referências no assunto.

Nesse período, fiz as primeiras palestras sobre Bitcoin. No início, para um público bem pequeno de profissionais ligados a startups. O momento era de pós-euforia com o rali de preços do ano anterior e, como a cotação havia passado todo o ano de 2014 bastante lateralizada, poucas pessoas realmente se interessavam pelo tema. As palestras acabavam se transformando em bate-papos informais entre os poucos entusiastas.

Comecei a realmente entender o senso de comunidade em torno das criptomoedas quando participei, no fim de 2014, de um painel na Conferência Latino-Americana de Bitcoin, que aconteceu no Rio de Janeiro. Naquele evento internacional, foi interessante notar o quanto globalizada era aquela comunidade e como, apesar das particularidades, todos ali partilhavam de valores comuns e planos ambiciosos de construir as bases para que a tecnologia pudesse transformar o mundo.

Em meados do ano seguinte, tive mais uma demonstração de que esse mercado é ultradinâmico. Recebemos uma oferta de compra da operação da Coinverse, que sequer tinha um ano de funcionamento. A oferta da coinBR era praticamente irrecusável e, em pouquíssimo tempo, saí de uma ideia que quase ninguém conseguia entender para gerenciar um processo de fusão.

Na coinBR, tive o desafio de integrar os serviços prestados pela Coinverse a uma das peças fundamentais para o mercado, mas que até hoje é pouco desenvolvida por aqui: a mineração de bitcoin. A proposta era sermos a primeira empresa latino-americana totalmente verticalizada, que possuísse uma planta de mineração de criptomoedas, uma casa de câmbio e uma plataforma de serviços de pagamento.

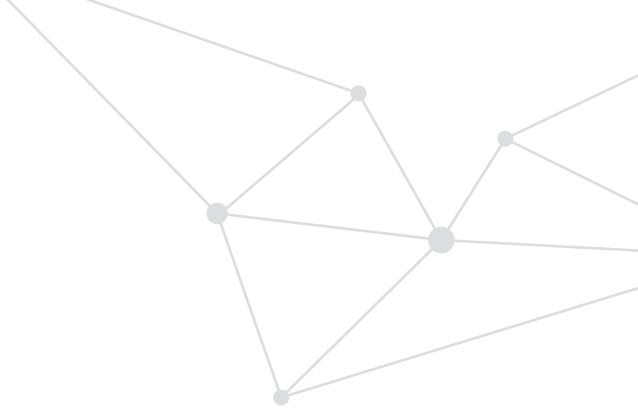
Tive a oportunidade de viajar o mundo, visitar dezenas de startups e conhecer outros empreendedores que estavam construindo as bases de acesso para que consumidores ao redor do mundo pudessem ter acesso às moedas digitais.

Participei das principais conferências sobre criptomoedas. Em Hong Kong, me surpreendi com o potencial do mercado asiático e conheci um pouco mais de perto a relação dos chineses com o Bitcoin. Em Nova York e Londres, onde o mercado estava muito mais profissionalizado, pude conversar com figuras conhecidas no meio, como Roger Ver, Andreas Antonopoulos, Vinny Lingham e Vitalik Buterin, que me apresentaram visões, muitas vezes conflitantes, sobre a relevância do fenômeno das moedas digitais e o potencial do mercado.

Essa jornada curta, porém intensa, me dá a convicção de que estamos na vanguarda de uma revolução que tem tudo para rever não apenas nossos investimentos, mas a forma como o mundo funciona. Estamos diante da “internet do dinheiro”, e não apenas do “dinheiro de internet”.







## *INTRODUÇÃO*

# **POR QUE É MELHOR QUE DINHEIRO?**

Se você pudesse voltar dez ou vinte anos no tempo e dizer para seu eu do passado quais seriam os grandes sucessos do mercado de hoje, o que você faria? Talvez você se aconselhasse a comprar ações do Facebook ou da Amazon. Ou pode ser que escolhesse se dar a dica para criar um site de buscas que pesquisasse qualquer coisa sobre qualquer assunto e desse a ele o nome de Google.

Além da triste realidade de que não podemos (ainda) voltar ao passado, é preciso reconhecer que um sucesso só se revela, de fato, *a posteriori*. Hoje é óbvio que o Facebook seria a maior rede social do mundo, que a Amazon seria uma varejista global ou que o Google saberia tudo sobre a sua vida.

Mas... e no passado? Definitivamente, não era óbvio. Apenas quem vislumbrou o potencial futuro e pagou para ver é que conseguiu de fato surfar o enorme crescimento dessas empresas. A questão central é que de forma alguma é simples identificar *a priori* um grande sucesso ou a próxima inovação. Contudo, é possível exercitarmos nossa mente para buscar indícios nas invenções atuais que ao menos revelem o potencial que carregam.

Realizamos esse exercício buscando pensar fora dos limites lineares. Nossa mente está programada para buscar e seguir padrões de forma incremental. Porém, algo disruptivo assume uma trajetória completamente oposta, de forma exponencial. Buscar pelas próximas inovações tem a ver com pensar além das trivialidades, procurando as reais assimetrias por trás de novos projetos, empresas e tecnologias. Esse é nosso mote de vida ou, pelo menos, aquele que assumimos nos últimos anos: ir atrás das inovações que dominarão o mercado no futuro e estudá-las a fundo.

Essa busca pela não linearidade se iniciou nos tempos de faculdade. Carregamos as ótimas lembranças do tempo de USP em São Carlos (das festas, inclusive) e daquela busca quase utópica por desenvolver uma invenção tecnológica que revolucionaria o mundo. Durante aqueles pouco mais de cinco anos de engenharia mecatrônica, procuramos entender o que poderia ser derivado da junção de mecânica, eletrônica e computação.

Entre um projeto e outro, alguns de sucesso, outros que fracassaram antes mesmo de serem colocados à prova, nós dois decidimos que seguiríamos carreira em alguma área que trouxesse a inovação em sua essência. Esta é a palavra que define a evolução do mundo: inovação. Uma sociedade que não inova, que se prende apenas àquilo que já funciona e está estabelecido, cria seu próprio caminho para a estagnação e o fracasso social e econômico.

Nosso mundo pede, constantemente, que busquemos soluções novas para problemas dos mais variados. E essas soluções não

só têm que ser novas como também precisam causar disruptão. Melhorias incrementais ajudam a manter o estado de crescimento orgânico, mas as grandes mudanças vêm a galope, em ritmo exponencial.

Você se lembra de quando deixou de enviar mensagens por SMS e passou a usar o WhatsApp? Ou de quando deixou de usar fax e passou a enviar documentos por e-mail? (Tudo bem que alguns leitores mais novos talvez nem saibam o que é um aparelho de fac-símile e outros ainda o usem para fins bastante específicos.) O ponto é que nem percebemos as mudanças chegando e, de repente, elas já aconteceram.

O que era óbvio até certo momento virou passado de uma hora para outra. Da mesma forma que hoje dirigimos nossos próprios carros, daqui a não muito tempo, você não vai nem se lembrar de que tinha que fazer aula em uma autoescola, passar por uma prova de direção e realizar uma baliza bem feita para poder dirigir, porque carros autônomos serão a forma convencional (e mais “normal”) de se deslocar de um lado para outro.

Indo mais a fundo, você pode até argumentar que os carros autônomos já existem e que se pode vislumbrar uma transição do tradicional para o autônomo. Contudo, lembre-se de que até alguns anos atrás um carro que anda sozinho era coisa de filmes de ficção científica, junto com os carros voadores.

Pois bem, repetidas vezes na história acreditamos que algo era improvável ou distante da realidade até que, sem perceber, uma enorme transição aconteceu e o que parecia imaginário virou o “novo normal”. Isso nada mais é que a natureza da inovação em ação e o processo natural de evolução tecnológica. Foi ela que nos saltou aos olhos desde cedo e fez com que nos apaixonássemos por tecnologia, que, na verdade, é apenas um meio. Nos apaixonamos, de fato, pelo que é possível criar por meio dela.

Com essa visão, passamos os últimos anos trabalhando com startups, desenvolvendo projetos de tecnologia e buscando inovar em diferentes áreas, da robótica à educação. Mas, se você pensa que o mercado financeiro surgiu no meio dessa história da mesma forma, se enganou. Nos aproximamos inicialmente do universo de investimentos durante a faculdade, quando achamos que o fato de conhecer o mundo dos números nos garantiria a competência necessária para lidarmos com o assunto. Não podíamos estar mais errados.

A verdade é que aquele papo de economia não entrava nas nossas cabeças de jeito nenhum. Aceitamos a realidade e decidimos estudar por conta própria, buscando algo que não falasse em “economês”. Foi aí que nos deparamos com as publicações da Empiricus e fomos fisgados de vez por esse tema. Por mais que os investimentos tratados nos conteúdos não tivessem nada de inovador em si, entendíamos que a forma de falar de finanças com a pessoa comum era uma inovação por si só. Definitivamente, era algo que faltava no Brasil. Um verdadeiro serviço de utilidade pública.

Nos meses que se seguiram, passamos a reunir o que aprendíamos sobre o mercado financeiro e a desenvolver nossos próprios conteúdos e materiais sobre investimentos. Demos início a cursos sobre o assunto na faculdade e, um ano depois, fundávamo o Investeaê, nosso projeto de educação financeira que ficou em operação até o fim de 2017. Mas algo ainda mais interessante viria paralelamente a essa jornada. Falo do elemento que ligou nossa paixão por inovação e tecnologia ao aprofundamento no universo do mercado financeiro. Você já deve ter um palpite, certo? Foi o Bitcoin.

No início, tudo parecia muito estranho e nebuloso. Coisa de hackers. Porém, conforme estudávamos mais sobre o assunto, ficava cada vez mais claro que era mais uma inovação que se colocava à nossa frente, assim como a internet na década de 1990 e os carros autônomos dos dias de hoje.

A cada nova referência que líamos, mais “comprados” ficávamos na ideia. Sem dúvida, a proposta de Satoshi Nakamoto, que deu início à criptoeconomia e abriu caminho para o surgimento de inúmeras outras criptomoedas, é uma completa revolução daquilo que conhecemos como sistema financeiro.

Assim, retomo a pergunta inicial, que se liga ao título deste livro: por que acreditamos que as criptomoedas são melhores que dinheiro? A resposta começa pelo sistema financeiro tradicional. Ele é dominado pelas grandes instituições financeiras, que centralizam o poder de decisão e o controle monetário. Ele seria ótimo se todos os seus movimentos fossem feitos de forma responsável e coordenada. O problema surge porque essas autoridades financeiras têm o direito de emitir moeda (leia-se imprimir dinheiro) da forma que bem entenderem, sem controle, deixando o resto da sociedade à mercê de suas decisões. Basta olhar para o tamanho da dívida global ou para a quantidade de dinheiro emitido pelos países para chegar à conclusão de que a conta não fecha. Logo, em vez de ter fé no sistema, por ele ser controlado pelas grandes instituições, na verdade, deveríamos temê-lo.

As crises recentes tentaram deixar lições de como não tratar a economia global, mas elas parecem não ter sido aprendidas, tampouco assimiladas. Sendo assim, como podemos viver confortavelmente em um mundo em que erros enormes são cometidos pelas autoridades do sistema financeiro e depois repetidos como se pudessem gerar resultados diferentes? Pois é. E os problemas não param por aí.

Há uma série deles que precisam e podem ser endereçados, e as criptomoedas são um meio capaz de resolver boa parte deles. Então, indagamos novamente, por que “melhor que dinheiro?”.

Por um lado, porque, como dito, as criptomoedas são capazes de resolver problemas atuais e tradicionais do dinheiro fiduciário, funcionando de forma mais eficiente e controlada. Por outro, porque elas podem, de fato, ser muito mais que dinheiro.

Ao longo deste livro, você entenderá como surgiram as criptomoedas, o que elas representam, por que temos tanta convicção em seu sucesso no longo prazo e quais são as outras classes de ativos nesse mercado que podem assumir papéis muito além do meramente financeiro.

O Bitcoin foi o protagonista dessa história, surgindo em meio ao cenário pós-crise de 2008, e deu o pontapé inicial para o surgimento de diversas outras abordagens tecnológicas envolvendo criptoativos que se propõem a trazer soluções para o mundo atual.

Apesar de essencialmente virtuais, esses ativos resolvem problemas reais, de pessoas reais, em um mundo real. Por isso, volto ao ponto dito anteriormente: a tecnologia é um meio. É o caminho pelo qual as criptomoedas foram estabelecidas, mas seu real potencial está nas aplicações que podem ser geradas por elas.

Entendemos as criptomoedas como uma classe totalmente nova de ativos, que precisa da sua própria classificação e do seu método de análise e estratégias, algo que discutiremos também ao longo deste livro.

Por mais que ainda haja muita gente tentando incluir o Bitcoin e os outros ativos desse mercado em uma classe já existente (moeda, commodity, etc.), acreditamos que seja necessário criar uma nova classificação, própria para as criptomoedas, que leve em conta todas as particularidades desse tipo de ativo. Vamos contar uma breve história do reino animal que nos ajuda a ilustrar uma situação parecida com a que os criptoativos se confrontam atualmente.

No século 18, a pele de um animal que ninguém conhecia chegou à Europa, vinda da Austrália. Os cientistas não conseguiam identificá-la e classificá-la dentro dos grupos já conhecidos. No início, achavam que se tratava de uma brincadeira dos colegas do outro lado do globo.

Mesmo depois de muitas trocas de informações entre os especialistas dos dois continentes, os europeus continuavam céticos, achando impossível existir uma espécie tão única, que pudesse reunir características de mamíferos, répteis e aves. Até que em dado momento o capitão John Hunter viu o animal com os próprios olhos e enviou um desenho para a Europa.

Parecia impossível haver um ser vivo como aquele, mas ele era real. Era a descoberta do ornitorrinco. A comunidade científica precisou aceitar que se tratava de algo real e que não se encaixava nas classificações vigentes.

Não deve ter sido nada fácil mudar aquilo em que acreditavam para incluir uma classe nova e estranha, que era desconhecida até então, mas foi, sobretudo, algo necessário.

Da mesma forma, o Bitcoin surgiu sem ser bem entendido pelo meio econômico. Sua presença no mercado e fluxo financeiro, entretanto, tornaram-se inegáveis.

Assim como ocorreu com o ornitorrinco, à medida que a comunidade global passar a entender o bitcoin junto com seus companheiros criptográficos, será necessária uma reformulação das classes de ativos, a fim de incluir as criptomoedas como algo novo. Obviamente, é difícil, a princípio, para o sistema financeiro aceitar essa mudança porque, como mencionado no início desta introdução, a mente humana é programada para pensar de forma linear e incremental.

Mas o bitcoin e as outras criptomoedas são inovações exponenciais. Esses ativos vêm surgindo para solucionar inúmeros problemas que vivemos hoje, começando pelos do meio financeiro, como, por exemplo, a dificuldade de fazer remessas de dinheiro entre países.

Para compreender as reais dificuldades da economia global e como elas podem ser, ao menos em parte, solucionadas por meio das criptomoedas, precisamos voltar alguns anos na história e entender um pouco melhor como funciona o sistema financeiro tradicional.

É justamente disso que tratará o primeiro capítulo, que inicia a jornada que aqui faremos juntos. Ao longo das páginas que você lerá, buscamos investigar o que, de fato, está por trás do sucesso das criptomoedas e como você poderá se beneficiar do processo de adoção delas para obter lucros formidáveis.

Estruturamos o livro de forma a discutir os problemas do sistema financeiro atual, evidenciar como o Bitcoin e os outros protocolos de ativos digitais surgiram como propostas tecnológicas que podem ajudar a resolver vários deles e porque esse ecossistema de moedas digitais não se limita apenas ao âmbito do dinheiro. Aliás, em vários momentos usaremos a terminologia “criptomoedas” no sentido mais amplo, dos ativos digitais, para denominar a classe de ativos com característica criptográfica como um todo. Para os leitores mais técnicos, temos um apêndice dedicado à parte da tecnologia do bitcoin, com detalhes sobre o funcionamento do protocolo.

Entendemos o surgimento das criptomoedas como uma inovação tecnológica que caminha para a adoção em larga escala. Desejamos mostrar ao leitor o que está por trás de cada novo projeto e quais são as formas de investir nesse mercado. Ao final da leitura, você perceberá que as criptomoedas são muito mais do que aquilo que a mídia divulga. Esperamos que você se apaixone por esse universo assim como nós nos apaixonamos.

Este pode ser um caminho sem volta. E, sinceramente, esperamos que seja.







# 1

## UMA BREVE HISTÓRIA DO SISTEMA FINANCEIRO

O sistema financeiro nunca foi perfeito, e isso não é segredo para quem entende que a economia mundial foi crescendo e encontrando crises de tempos em tempos. Mas, antes de falar sobre como ocorreu o seu desenvolvimento, precisamos entender sua definição.

O **sistema financeiro** é um conjunto de instituições, mercados e recursos de um determinado país, cuja principal finalidade é canalizar para os devedores a poupança gerada pelos credores.

Canalizar poupança de credores para devedores? Mas o que seria essa poupança? Explicando em poucas palavras, trata-se de recursos que são transferidos de quem os têm para quem necessita deles. Na verdade, podemos afirmar que a poupança ou os recursos são, basicamente, dinheiro. Isso mesmo: bufunfa, dindim, cascalho, mangos... e por aí vai.

O sistema financeiro só existe porque existe dinheiro, e o dinheiro só existe por uma necessidade das pessoas. Afinal, ninguém cria algo que não atenda a alguma necessidade. Por isso, antes de contarmos a história do sistema financeiro, começaremos falando daquilo que o sustenta: o dinheiro.

## UMA BREVÍSSIMA HISTÓRIA DO DINHEIRO

Sabe esse pedaço de papel que você carrega na carteira? Essa notinha azul, verde, amarela ou de qualquer cor que seja? Pois bem, ela é uma “farsa”. Não que sua nota seja falsificada e que isso implique algum crime. A verdade é que, em essência, todas as notas são uma farsa.

Caso você não ande com nada na carteira, pense naqueles números que aparecem na sua conta bancária. Eles são apenas números, ou seja, também são uma farsa. Boa parte desses algarismos nunca se transformará em cédulas, em dinheiro vivo. Em vez disso, ao longo da sua vida, provavelmente, você apenas verá esses números indo de uma conta para outra: de sua conta para a conta do dono do apartamento em que você mora de aluguel. Para a conta do amigo ao qual você fez um empréstimo. Para a conta da companhia de energia, da operadora de internet e para tantas outras. E tudo isso não passa de uma grande farsa com a qual nós todos compactuamos. Mas, por outro lado, essa foi a melhor invenção para chegarmos até o momento em que estamos, com uma sociedade com recursos financeiros mais abundantes. O dinheiro falso em sua carteira, na carteira de seus pais e na mão do ambulante foi o que possibilitou que a sociedade prosperasse.

São essas cédulas que permitem que eu consiga comer na padaria aqui ao lado de casa sem ter que trocar meus relatórios de recomendações de investimentos com o dono da padaria. E que

permitem que ele tenha café em pó no estoque sem ter que fazer pães para todos os trabalhadores da fazenda de café. Portanto, o dinheiro, da forma que o conhecemos hoje, faz com que o sistema não trave na primeira tentativa de troca, quando um dos lados quer algo e o outro não deseja o que aquele tem a lhe oferecer.

A concepção de dinheiro começa assim que nossos ancestrais conseguem produzir mais do que conseguem consumir e precisam de outros bens além daqueles que produzem ou têm. A história remonta à época em que o homem iniciou o plantio dos primeiros grãos, o que marcou o surgimento da agricultura. Por volta de 8.500 a.C., os habitantes do Crescente Fértil (região que hoje compreende partes do Egito, Israel, Turquia, Iraque e de outros países) começaram a agricultura rudimentar e passaram a se estabelecer em regiões, deixando a vida nômade para trás.

Em seguida, veio a domesticação dos animais e, com ela, a relativa abundância de recursos, se comparada a centenas de anos anteriores, quando o homem saía para caçar. Com os grãos da agricultura e a facilidade de abater os animais por estarem em cercados, os seres humanos tinham a estrutura perfeita para um comércio rudimentar e para o nascimento do dinheiro.

A principal moeda desse período eram os alimentos. Essa espécie de escambo fazia com que o dono dos animais pudesse comer os grãos do agricultor, e vice-versa. Naquele momento, não era necessário sair para encontrar frutas se você criava animais. Bastava ofertar um pedaço de carne em troca da produção de um agricultor.

Na teoria, a história parece muito bonita, com todos trocando bens e sendo felizes. Mas a verdade é que a agricultura trouxe também muita desigualdade para a região do Crescente Fértil. Os agricultores se tornaram latifundiários, e contratavam trabalhadores para fermentar vinhos, construir casas e assar pães, sempre os remunerando com comida.

Como quem era dono de grandes quantidades de terra “plantava” o próprio dinheiro, esses agricultores prosperaram por pagar aos trabalhadores braçais a quantidade de comida que bem entendessem. Para conter a revolta dos que estivessem insatisfeitos com o sistema, bastava manter um exército bem alimentado.

Com essa forma de economia estabelecida, os latifundiários que produzissem mais poderiam comer, beber e vestir melhor. Mas, para isso, precisariam pagar mais e mais sacos de alimentos por esses confortos. Imagine a dificuldade que seria carregar sacos e sacos de comida para trocar por mercadorias?

Isso não era nada prático e a solução para esse problema nos acompanha até hoje. Estou falando dos bancos, talvez não do modo como os conhecemos hoje, mas num modelo que servia para as necessidades da época. Foram os babilônios, povo que viveu também no Crescente Fértil, que há quatro mil anos criaram os primeiros bancos. Aquela região era uma metrópole para os padrões da época, tinha comércio, produção e bancos. Uma maravilha!

Voltando ao tema dos bancos babilônicos, estes funcionavam da seguinte forma: o latifundiário que gerava excedente de produção depositava os grãos nos silos do rei, os quais funcionavam como bancos. Então, confeccionava-se um tablete de argila no qual era escrita a quantidade depositada. Com isso, uma das primeiras cédulas foi criada.

Esse tablete de argila era mais parecido com uma moeda gigante do que com notas, mas servia ao propósito de dinheiro, pois garantia ao portador o acesso a uma certa quantidade de alimento. Já os “bancos do rei” eram a contraparte que garantia que a quantidade de alimento gravada no tablete era verdadeira. Eram esses bancos que conferiam segurança ao sistema da época.

Se você sabe como trabalha essa instituição que dá lucros enormes, faça chuva ou faça sol, deve imaginar exatamente o que vem

depois: os empréstimos. Os bancos passaram a emprestar tabletes de argila às pessoas que desejassesem em troca de juros no futuro. Por exemplo, dez dessas peças emprestadas deveriam ser devolvidas no futuro com o acréscimo de uma. Assim, quem tomasse emprestadas dez unidades dessas moedas, devolveria, lá na frente, 11 unidades.

Era o começo da estrutura financeira que perdura até hoje. Os bancos ficam com o dinheiro das pessoas e o emprestam para outras com juros. É exatamente esse modelo que faz com que nossa sociedade seja tão próspera atualmente, e com que viva à base de ciclos econômicos que passam por períodos de tempestades.

Essas tempestades, leia-se crises, podem ser locais, como a que vivemos recentemente no Brasil, ou podem ser mundiais, como a que vivemos em 2008, que começou nos EUA e se alastrou pelo mundo todo.

Mas será que as crises são uma “invenção” moderna?

Com toda a certeza não. Trata-se de um fenômeno cujo primeiro episódio de que se tem notícia aconteceu na Holanda, no século 17.

## O SISTEMA FINANCEIRO

Como vimos na definição do início do capítulo, o objetivo do sistema financeiro é fazer com que pessoas com sobra de recursos emprestem para quem não os têm. Por isso, ele funciona quase sempre como um intermediário entre as partes, tomando daqui e dando ali, mas sempre tirando um naco para si.

Quanto mais o sistema “toma de lá e dá cá”, mais nacos consegue para si próprio. É por esse motivo que, quanto mais dinheiro estiver circulando, melhor para as instituições financeiras, que

ganham nessa intermediação. E aí mora o perigo, pois a última grande crise mundial, que começou nos Estados Unidos, teve início pela ganância do sistema em sempre fazer mais e mais dinheiro e, com isso, emprestá-lo para quem não podia arcar com essas dívidas.

Mas, como eu disse, a crise imobiliária na terra do Tio Sam não foi a primeira nem será a última. Na verdade, estamos acostumados a ver por lá crises iniciadas por bolhas, ainda que não tenham sido os norte-americanos que iniciaram a “cultura” de bolhas do sistema. Quem de fato começou com essa história foram os holandeses, com algo aparentemente inofensivo: tulipas.

## ***SEMPER AUGUSTUS: A PRIMEIRA BOLHA***

Na Holanda do século 17, um botão de flor valia o mesmo que uma casa em Amsterdã. Sim, era possível comprar uma casa na capital holandesa com o mesmo valor que se comprava uma tulipa, mas não qualquer flor. Apenas um tipo específico valia tanto quanto uma residência na cidade portuária. Esse fato deu origem ao que podemos chamar de a primeira bolha econômica da história.

As primeiras tulipas plantadas na Holanda foram trazidas da Turquia e logo caíram no gosto dos holandeses mais endinheirados. Até aí, nada de novo. Tratava-se de um item relativamente raro que os mais abastados queriam ter como sinal de status.

Mas, se as tulipas, de forma geral, eram um artigo de luxo, a *Semper Augustus* era o suprassumo da beleza — e também do preço. Havia um vírus que algumas vezes contaminava as tulipas normais e as deixava com um aspecto diferenciado. As flores contaminadas perdiam parte das cores da pétala, o que as deixava com cores leitosas. Por serem raras, essas tulipas eram comercializadas por um preço mais alto em relação às outras.

A *Semper Augustus* era desejada por muitos, mas poucos podiam comprá-la. Seguindo a lei da oferta e da procura, seus preços decolaram, chegando a valores que dariam para comprar uma casa em Amsterdã. Com o encarecimento de um dos tipos de tulipa, o preço das outras foi naturalmente puxado para cima.

As tulipas se tornaram o mercado mais quente da época e passaram a chamar atenção de pessoas que não tinham nenhum interesse real em flores, mas queriam apenas aproveitar as grandes valorizações que o mercado apresentava. Apesar de não haver tulipas suficientes para serem comercializadas, as pessoas que desejavam tirar proveito das valorizações das flores arrumaram um jeito de vendê-las sem nem ao menos tê-las à mão. A solução encontrada por essas pessoas foi comprar dos floricultores papéis que garantissem uma tulipa no bulbo, antes mesmo do florescimento, para então revendê-los com algum lucro a terceiros.

Digamos, por exemplo, que uma tulipa valesse R\$ 1 mil depois de florescida. Você, um floricultor precisando de dinheiro, ainda não pode vender suas tulipas, pois elas estão dentro do bulbo. Então você topa vender por R\$ 800 um papel que garante uma tulipa assim que florescida. Para você, foi um ótimo negócio, pois rendeu dinheiro imediatamente sem que tivesse a mercadoria de fato. À pessoa que comprou a tulipa com 20% de desconto bastava esperar o florescimento para conseguir lucrar com a venda.

Mas eis que, na sequência, aparece alguém querendo comprar o mesmo título por R\$ 900, e a pessoa em posse do papel resolve vendê-lo. Sem sequer ter visto a cor da tulipa, ela vendeu um título e embolsou R\$ 100 de lucro. Se ela pudesse fazer isso com R\$ 8 mil, o lucro seria dez vezes maior. Talvez ela própria nem precisasse ter o dinheiro; bastaria tomar um empréstimo, comprar títulos de tulipa e depois revendê-los, pagando com juros o valor emprestado e ainda embolsando uma grana.

Esse tipo de comportamento foi o que fez saltar o preço das tulipas de forma estrondosa. A *Semper Augustus* subiu 300% e a tulipa do tipo Gouda (a mais comum), no mesmo período, teve um salto de 1.125%. A ganância dos investidores era voraz e os preços das tulipas não se sustentaram. Primeiro, porque não havia demanda o bastante de pessoas que realmente queriam as tulipas. Na verdade, as vendas de títulos eram sustentadas por especuladores que esperavam sempre vender seu papel por um valor mais alto do que haviam comprado.

Além disso, alguns floricultores venderam títulos sem o lastro da tulipa, e esse tipo de descoberta foi feita no auge da bolha, fazendo com que os preços derretessem rapidamente. Muitas pessoas perderam suas economias ao investir nessa empreitada, e é justamente isso que sempre acontece quando uma bolha estoura: alguém sai perdendo.

Ao longo da história, tivemos as mais diversas experiências com esse tipo de acontecimento. Ao que parece, as crises e as bolhas são algo inerente ao nosso sistema financeiro e não deixarão de existir tão cedo.

## DAS TULIPAS AO SUBPRIME

Quase na mesma época da tulipomania, outra bolha se formava na Inglaterra e na França. John Law, um escocês filho de banqueiro, em solo francês, fundou o que podemos chamar de Banco Central francês, responsável por emitir as notas do país, as quais eram garantidas pelo rei da França, Luís 15.

A propensão de Law aos jogos de azar, contudo, não era uma vantagem para quem ocupava um cargo tão importante na economia. Na verdade, foi sua ganância de ter cada vez mais dinheiro que ajudou a afundar a Europa em uma crise de extrema pobreza que culminaria na Revolução Francesa.

O filho de banqueiro, que logo se tornaria um dono de banco também, fez uma manobra ousada ao criar a Companhia do Mississippi. Essa empresa fazia negócios com a América do Norte, mais precisamente com a Louisiana, que se estendia desde o golfo do México até o Canadá. Ela tinha o monopólio da comercialização de todos os produtos que saíssem desse território da América do Norte garantido pelo rei Luís 15. Com isso, Law conseguia passar confiança aos investidores.

Posteriormente, as ações da Companhia do Mississippi foram vendidas em troca de títulos de dívidas do governo. Porém, esses títulos não valeriam nada se o governo não os pagasse. Diante desse cenário, Law fez aquilo que qualquer banqueiro adoraria fazer: imprimir dinheiro para pagar dívidas e financiar investimentos. Isso foi possível porque ele tinha o poder do Banco Central nas mãos e porque o dinheiro impresso gozava da confiança da população, já que se acreditava que havia lastro em metais preciosos.

Assim, Law imprimia dinheiro para financiar sua empreitada com a Companhia do Mississippi, pagar credores e distribuir dividendos aos acionistas. Como o dinheiro não tinha lastro, ele conseguia pagar dividendos anuais de 40% sem que a companhia nem ao menos apresentasse resultados reais. O banqueiro estava criando dinheiro do nada e, com a notícia de que uma empresa pagava tantos dividendos, o valor das ações da companhia subia com a expectativa de mais dividendos. Então, o Banco Central imprimia mais dinheiro e continuava pagando dividendos gordos para os acionistas.

Por fim, começou a haver questionamentos sobre se tanto dinheiro assim tinha, de fato, lastro em metais. A Coroa francesa acabou obrigada a admitir que não tinha mais lastro. Nesse momento, o cenário de hiperinflação já dominava a França. Em paralelo à crise francesa, a Inglaterra passava pelo mesmo problema.

Ao norte do Canal da Mancha, em solo inglês, a companhia dos Mares do Sul, guiada por outro John — John Blunt — também fez um esquema parecido ao trocar ações da Companhia por títulos de dívidas da Coroa. Na prática, quem trocasse esses títulos por ações ganhava um desconto no preço, o que fez os papéis da empresa bombarem nos primeiros períodos.

Em resumo, o esquema de John Blunt para lucrar era fazer o preço das ações subir artificialmente para ganhar tanto com a valorização dos papéis quanto no mercado de derivativos. E foi isso que fez o mercado entrar em colapso por lá. Um fato curioso sobre a história inglesa é que ela fez uma vítima muito ilustre: *sir* Isaac Newton perdeu na época o que hoje equivaleria a mais de R\$ 80 milhões em dinheiro.

Mas a história das bolhas não termina aí, apenas migra de território. Ela reaparece nos Estados Unidos, de modo grandioso, no começo da era da internet. Antes do estouro dessa bolha, bastava uma empresa ter “.com” no nome para conseguir arrecadar valores absurdos de investidores a *valuations* ridículos. O caso mais emblemático dessa insanidade das “ponto com” foi o Yahoo, que, um ano antes de a bolha estourar, valia US\$ 96 bilhões e proporcionava um lucro de apenas US\$ 61 milhões.

Mas essa insanidade foi colocada em xeque nos anos 2000, com o estouro da bolha das “ponto com”. Em 2002, a Nasdaq, bolsa de valores americana em que são negociadas empresas de tecnologia, tinha perdido US\$ 4 trilhões em valor. Depois dessa perda estrondosa, voltando ao mesmo patamar de valor de 1996, as empresas que conseguiram sobreviver deram a volta por cima, e algumas se tornaram líderes de mercado. É o caso da Amazon, que na época da crise era apenas uma vendedora de livros, e hoje é líder em e-commerce em vários países.

## **SUBPRIME**

Se a “bolha.com” sacudiu o mercado americano, a crise do *subprime* em 2008 sacudiu o mundo, causando uma onda de desemprego em vários países. Em resumo, a sua principal causa foi a concessão desenfreada de crédito imobiliário a quem não podia pagar por ele. O pior de tudo é que os bancos sabiam dos riscos de conceder empréstimos a pessoas que não tinham condições de pagar pelas casas que compravam e, por isso, vendiam os títulos de crédito imobiliário concedidos como investimentos para seus clientes.

Primeiro, as instituições financeiras procuravam emprestar para aqueles que poderiam honrar a dívida, pessoas com bons empregos e com algumas posses. Mas, à medida que se tornava mais difícil encontrar pessoas com esse perfil, os banqueiros decidiram recorrer a pessoas sem emprego fixo e com quase nenhum, ou nenhum, bem. Os empréstimos se destinavam principalmente à compra de casas, pois eram a segurança para quem emprestava de poder reaver o empréstimo por meio de um bem físico, a casa.

Caso o empréstimo não fosse honrado, a casa era tomada e revendida a outra pessoa. Parecia o negócio perfeito, já que os valores dos imóveis não paravam de subir; se uma casa fosse devolvida, facilmente era vendida por um valor acima do preço inicial. Isso começou a chamar atenção de pessoas que perceberam que poderiam financiar uma casa, revendê-la, pagar o empréstimo e ainda embolsar algum dinheiro.

Qualquer semelhança com as tulipas não é mera coincidência. Uma bolha estava, de fato, se formando.

Quem emprestava o dinheiro para essas pessoas? Os bancos? Sim e não. Eram os bancos porque, ao repassar o dinheiro às

pessoas que queriam comprar uma casa, os banqueiros pegavam esse dinheiro de outras pessoas, que queriam investir em títulos dessas dívidas. Não apenas de pessoas, mas também de fundos de investimentos e fundos de pensão.

O aval para comprar os títulos de dívida hipotecária vinha do selo que os títulos carregavam: “AAA”, o carimbo mais seguro das agências de classificação. Ao ver um “AAA”, as pessoas se sentiam seguras para investir, pois se tratava de um título quase impossível de não ser honrado. Por muito tempo, isso foi feito sistematicamente pelos bancos e demais instituições financeiras dos Estados Unidos. Até que a inadimplência se alastrou e os devedores simplesmente não conseguiam mais pagar o que deviam, e os credores, consequentemente, não conseguiam mais receber o que lhes era devido.

Toda essa crise tem um culpado central: o sistema financeiro como ele é. A falta de transparência do sistema permitiu que as agências de classificação elegessem títulos péssimos como sendo bons e que os bancos os vendessem para os desavisados. Por incrível que pareça, pouco antes da crise estourar, já havia questionamentos sobre o potencial enorme dos bancos de provocar o colapso das economias.

Uma saída seria dar às pessoas a posse e o controle de seu próprio dinheiro, para que não precisassem mais de instituições intermediando suas transações. Isso, que seria possível com a tecnologia, era o que buscava um pequeno grupo de indivíduos que trocava e-mails e ideias a partir de seus computadores.

Esse grupo de pessoas estava engajado em trazer uma solução para o sistema financeiro pouco transparente. Foram várias trocas de e-mails entre esses criptógrafos para que se propusesse uma solução viável de um sistema transparente de trocas financeiras que

não necessitasse de intermediário. E o desfecho, ou o início de tudo, foi um protocolo proposto por Satoshi Nakamoto. A proposição foi o **Bitcoin** e o **blockchain** e explico melhor o que é cada um nos próximos capítulos, mas primeiro vamos ao Bitcoin.





## A REVOLUÇÃO – ESTRELANDO: O BITCOIN

Em julho de 1944, delegados de 44 nações se reuniram no Mount Washington Hotel, em Bretton Woods, New Hampshire, para uma conferência que marcou a história mundial. Naquelas três semanas de encontro, foi firmado o acordo que estabelecia que moedas emitidas por um governo não poderiam ultrapassar o valor total de suas reservas em ouro.

Aquilo sustentava o lastro das moedas nacionais em relação a um ativo físico e esgotável. O acordo durou 27 anos, até que, em agosto de 1971, os EUA romperam o que foi estabelecido, passando a emitir dólares sem lastro em ouro.

A partir daí, o dólar passou a ser uma moeda fiduciária. O termo, apesar de esquisito, deriva de uma palavra bastante popular: fé. Logo, uma moeda ser fiduciária significa que você tem fé no governo que a emite.

O acontecimento desencadeou um movimento em que outras moedas nacionais deixaram de ser fixas e passaram também a ser emitidas com base nas definições de seus próprios governos. Desde então, vivemos em um mundo fiduciário.

Na realidade, o fato de as moedas nacionais terem deixado de possuir lastro em ouro não foi o pior problema. A questão central e mais preocupante, abordada no capítulo anterior, é que os governos passaram a não ter mais limites claros com relação ao dinheiro. Nesse modelo monetário, eles simplesmente podem imprimir cédulas e mais cédulas *ad infinitum*.

Daí surgem dois problemas:

1. A impressão de dinheiro, por vezes sem controle, pelos bancos centrais provoca destruição de valor ao invés de criação;
2. As pessoas comuns deixam de ter controle sobre o próprio dinheiro.

Os pontos 1 e 2 estão diretamente relacionados. Pare e abra sua carteira. Você provavelmente possui algumas cédulas ou moedas, e talvez tenha a impressão de que elas estão sob seu controle. Porém, por mais que as guarde consigo, você não pode controlar a forma como decisões do governo influenciarão seu valor.

Uma situação pior ainda acontece com o dinheiro no banco. O saldo que aparece na tela quando você consulta uma conta representa um valor que está ligado ao seu CPF, mas cujo controle está nas mãos da instituição financeira.

Ao longo das últimas décadas, foi possível perceber o impacto negativo da centralização de poder sobre o sistema financeiro. As grandes crises são prova disso e põem em xeque “a fé” nas instituições financeiras e o benefício de deixarmos todo o nosso patrimônio nas mãos de um órgão poderoso.

Foi com o objetivo de acabar com essa centralização do controle sobre o dinheiro que surgiu, em 2009, o protagonista da transformação — ou melhor, revolução — no sistema financeiro tradicional: o Bitcoin. Trataremos dos aspectos técnicos dessa revolução em capítulos posteriores. Neste momento, é importante entendermos como e de onde surgiu a primeira criptomoeda descentralizada.

A criação de uma moeda essencialmente digital já era tema de discussões e projetos bem antes do surgimento do bitcoin. As principais movimentações começaram na década de 1980, quando a criptografia passou a ser mais entendida e usada ao redor do mundo.

Na época, ainda havia o problema de essas moedas digitais serem controladas por um órgão central. Como consequência dessa centralização, elas se tornavam alvos fáceis para ataques de hackers. Além disso, persistia o problema da fé ou confiança em uma única instituição.

Com esses pontos em mente, em 2008, o misterioso sujeito (ou grupo) chamado Satoshi Nakamoto publicou um *paper* em que explicava as bases técnicas do Bitcoin. As primeiras palavras, logo no resumo inicial, dizem o seguinte:

*“Uma versão puramente peer-to-peer de dinheiro eletrônico possibilita que pagamentos online sejam enviados diretamente de uma pessoa a outra, sem precisar passar por uma instituição financeira.”*

Bingo! Um sistema puramente digital e não dependente de uma instituição financeira. Essa foi a proposta inicial do Bitcoin. Aquele *paper* definia as bases técnicas de um protocolo de transferência de dinheiro entre pessoas (por isso o *peer-to-peer*) e o bitcoin moeda é hoje apenas uma das aplicações possíveis desse protocolo.

O Bitcoin, portanto, inaugurou o universo das criptomoedas, isto é, das moedas digitais que usam criptografia para garantir a segurança das transações. A descentralização foi o elemento-chave para o sucesso da proposta. Duas pessoas poderiam trocar valores entre si sem precisar de um banco no meio do caminho. Na verdade, cada pessoa passaria a ser seu próprio banco.

Como retrato dessa versatilidade criada pelo Bitcoin, temos a emblemática história das duas pizzas mais caras do mundo. Desde janeiro de 2009, quando o bitcoin entrou em circulação, até maio de 2010, não havia um preço de referência para a moeda. A compra das duas pizzas veio para mudar esse cenário.

Em 22 de maio de 2010, um programador pagou 10.000 bitcoins a uma pizzaria por duas pizzas. Naquele momento, poderia parecer que a compra tinha saído “de graça”, afinal, o bitcoin valia muito pouco. Hoje, porém, essa quantia equivale a milhões de dólares.

A questão que surge para a maioria das pessoas que passaram a conhecer as criptomoedas há pouco tempo é: como e por que houve uma valorização dessa magnitude? Tenho certeza de que, ao final deste livro, você estará convencido do poder revolucionário das criptomoedas, e as valorizações expressivas que novas moedas tiveram ao longo dos anos soarão bastante normais e lógicas. Para tanto, é preciso entender o que está por trás das criptomoedas.

O que faz do bitcoin o protagonista da transformação no sistema financeiro é o fato de ele ter sido a primeira abordagem de criptomoeda a ganhar apoio da comunidade ao redor do mundo. Estamos falando de uma forma de dinheiro que não pode ser falsificada, que tem emissão controlada e que não está nas mãos de nenhum governo ou organização.

Parece um pouco anarquista? Sim e, de certa forma, é. Desde a década de 1990, já havia um movimento libertário que ficou conhecido como *cypherpunk*, que desenvolvia projetos envolvendo

criptografia, computação e matemática. O termo é a junção de “cypher”, que vem de criptografia, com “cyberpunks”, o grupo rebelde apaixonado por tecnologia.

O bitcoin apenas deu vida a um movimento que já existia há décadas. A criptomoeda inaugurou o que podemos chamar de criptoeconomia e é considerado por muitos como a internet do dinheiro, já que seu desenvolvimento guarda muitas similaridades com o surgimento da internet.

## **DA REVOLUÇÃO DA COMUNICAÇÃO À REVOLUÇÃO DO SISTEMA FINANCEIRO**

Você já parou para pensar no que a internet proporcionou às pessoas ao redor do mundo? Em um passado não muito distante, você teria que enviar uma carta pelo correio se quisesse que alguém em outro país recebesse informações de um documento. Se precisasse ligar para uma pessoa no exterior, pagaria tarifas altíssimas em uma chamada DDI.

Hoje, porém, você pode simplesmente enviar um e-mail ou ligar pelo Skype, FaceTime ou WhatsApp. É possível conectar-se em tempo real a qualquer pessoa, em qualquer lugar do mundo. Eu, que vivenciei pelo menos parte dessa evolução, fico maravilhado com os avanços obtidos e com a velocidade com que eles aconteceram.

Contudo, há algo ainda mais bonito nisso tudo, que não se limita à rapidez da comunicação. Estou falando da democratização da informação. Antes do surgimento da internet, apenas um jornalista ou escritor poderia publicar suas ideias para um grande público, por meio da mídia impressa. Hoje, com a internet cada vez mais acessível, qualquer pessoa, independentemente de sua formação, pode expor ideias na rede.

A internet, portanto, surgiu para derrubar barreiras. Atualmente, um número enorme de pessoas tem acesso a um computador e conexão à rede global. Dificilmente a internet é vista como item dispensável à sociedade.

Mas isso não foi sempre assim. A internet foi criada, inicialmente, para fins de comunicação entre militares e cientistas durante a Guerra Fria. Em seus primeiros anos, ela não era compreendida por todos e seus usos eram limitados. Levou algumas décadas para que a internet fosse utilizada em escala global por usuários comuns. Havia, inclusive, quem desacreditasse que ela pudesse se tornar importante.

De forma similar, o Bitcoin surgiu como uma inovação em um meio extremamente técnico. Como consequência, apenas um grupo restrito de pessoas compreendia o que o protocolo se propunha a resolver. Por isso, ele foi (e ainda é) desacreditado por quem não entendia, de fato, a tecnologia por trás da criptomoeda.

Apesar desses obstáculos, com o passar dos anos, o Bitcoin ganhou mais espaço e visibilidade no cenário mundial, em um movimento muito parecido com o da internet em seus primeiros anos. A palavra “bitcoin” dá nome tanto à **moeda** (grafia com inicial minúscula) quanto ao **protocolo** (grafia com inicial maiúscula). Este último nada mais é do que um conjunto de regras que define como os valores são transacionados.

Assim como a internet proporcionou a democratização da distribuição de informação ao redor do mundo, o Bitcoin, com sua capacidade de ampliar os canais de troca de valores entre pessoas, estabelece uma nova era e um novo conceito de dinheiro. Da mesma forma que a internet passou por um processo de adoção explosivo ao longo dos anos, as criptomoedas e, especialmente, o Bitcoin, têm tudo para repetir esse feito no sistema financeiro.

Portanto, reforço que estamos diante de uma inovação capaz de transformar todo o sistema em que vivemos. O motivo é simples: as criptomoedas resolvem problemas reais, de pessoas reais, em um mundo real. No mundo em que vivemos, ficar indiferente às criptomoedas simplesmente não é aceitável, e, para compreender o “universo cripto”, precisamos entender mais a fundo como funciona o Bitcoin.

## POR DENTRO DO BITCOIN

Já perdi a conta de quantas vezes comecei a explicar o que é o bitcoin para parentes e amigos. Em quase todas as ocasiões, acontecia algo parecido: a pessoa à minha frente estava toda animada para saber mais sobre o assunto, porém, quando eu dizia que o bitcoin não existe fisicamente e que não há um “dono” que o controle, a reação era mesma, uma cara de interrogação.

Entendo que o caráter abstrato do Bitcoin possa causar espanto ou desconfiança. Mas tomemos o seguinte exemplo: o seu cartão de crédito. Você saberia me dizer como funciona a tecnologia por trás dele? Ou alguma vez já viu alguma forma de dinheiro físico ligada ao seu cartão?

Pois é, seu cartão de crédito, apesar de ser um objeto físico, não passa de um pedaço de plástico que o coloca em contato com um saldo puramente digital. Ele simplesmente faz a ponte entre você e sua conta bancária (ou o crédito que você tem nela). Você não precisa entender a fundo a tecnologia da maquininha de cartão da padaria na frente da sua casa. Você simplesmente usa o cartão de crédito porque o resto da sociedade faz o mesmo.

Ou seja, existe um consenso de que aquele pedaço de plástico funciona como dinheiro. Por outro lado, talvez ainda não haja esse

tipo de consenso para o bitcoin e, por isso, muitas pessoas “travam” na hora de tentar compreendê-lo.

Se você é iniciante nesse tema, saiba que não é necessariamente preciso entender os detalhes técnicos do Bitcoin para usá-lo. Contudo, como sei que você não se daria por satisfeito com uma explicação simples, dedico as próximas linhas a entrarmos mais a fundo nesse parque de diversões tecnológico.

Como você já sabe, não existe um órgão central que controle o bitcoin. Todas as transações são feitas entre duas pessoas (daí a denominação *peer-to-peer*) e autenticadas em uma rede descentralizada. No fundo, o Bitcoin é um protocolo que estabelece um conjunto de regras que determinam como os valores são transferidos entre dois usuários.

As transações acontecem de maneira parecida à das transações bancárias, mas com a diferença de não serem “auditadas” apenas por um intermediário (o banco) e de serem mais rápidas e menos custosas. Se você já tentou transferir dinheiro do Brasil para outro país, sabe do que estou falando.

No caso do Bitcoin, em vez de termos um banco validando cada transação, os próprios usuários da rede são responsáveis por esse processo. A criptografia por trás do protocolo é o que garante a segurança.

Mais à frente no livro, explicarei em detalhes como isso ocorre. Por enquanto, um exemplo simples será mais do que suficiente.

Você já jogou Banco Imobiliário? No jogo, cada participante possui uma quantia de dinheiro e objetivos para cumprir. Imagine que dois amigos estejam jogando: Pedro e Antônio. Se Pedro quiser comprar uma casa que Antônio possui, ele separa o dinheiro correspondente e entrega a Antônio. A partir daí, Pedro terá a posse do imóvel.

Contudo, se Pedro dissesse que pagou pela casa, mas Antônio não tivesse recebido o dinheiro, este diria que a transação não aconteceu. Para organizar o jogo, Pedro e Antônio têm cada um seu caderninho, no qual anotam todas as movimentações de dinheiro. Como são amigos, um confia no outro, e o jogo flui sem maiores problemas.

Agora, imagine que mais dois amigos entrassem no jogo: Ana e Roberto. O fluxo continua o mesmo: se uma pessoa paga por algo, a outra precisa receber. Mas, em um dado momento, Pedro e Antônio poderiam bancar os espertões e fraudar uma transação. Pedro diria que pagou R\$ 100 a Antônio e este acusaria ter recebido o dinheiro, mesmo a transação não tendo ocorrido.

Se Ana e Roberto não estão atentos, esse pode ser o início de uma série de jogadas falsas que deixarão os dois amigos que iniciaram o jogo ricos à custa da falta de atenção dos novos jogadores. Para evitar que isso aconteça, Ana e Roberto decidem ter seus próprios cadernos, nos quais também anotarão todas as transações feitas.

Percebe o que ocorreu? Se todos passarem a anotar tudo, caso haja uma divergência nas anotações, eles saberão quando houver uma movimentação falsa de dinheiro. A rede do Bitcoin funciona de maneira parecida. Todos os participantes podem ter acesso a todas as transações que ocorrem, e mais de uma pessoa valida uma mesma operação.

A diferença é que, em vez de cada um ter seu próprio caderno ou planilha, todas as pessoas anotam as informações das transações em um único livro de registro, chamado blockchain. Ele nada mais é do que uma enorme planilha com todas as informações de transações desde o surgimento do Bitcoin.

Pense no blockchain como uma lista de todas as trocas de valores que já ocorreram entre dois usuários em toda a história do bitcoin. Ele sempre cresce em tamanho e tem esse nome pelo fato

de ser formado por uma cadeia (*chain*) de blocos (*blocks*), cada um contendo informações sobre as transações.

Todos os computadores de usuários conectados à rede do Bitcoin têm acesso ao blockchain e todas as transações são registradas simultaneamente em todos eles. Isso quer dizer que essas informações, vitais para o funcionamento e a segurança do sistema, não ficam em um único servidor, em um único local. Esse banco de dados é distribuído, descentralizado, dificultando qualquer tipo de ataque e fraude.

Voltando ao exemplo do Banco Imobiliário, é como se os jogadores registrassem as transações no blockchain, com todos eles podendo ter acesso aos registros e autenticando as transações como válidas. Na verdade, no caso do protocolo Bitcoin, você pode ter acesso ao blockchain e a todo o registro de transações, mas não precisa necessariamente fazer isso para usar e transferir a moeda. Também não é necessário conhecimento técnico ou de programação para a parte prática.

Os usuários — que de fato possuem computadores conectados à rede, que têm acesso ao blockchain e validam as transações — são chamados de **mineradores**. Essas pessoas “auditam” as movimentações financeiras. Se você deseja apenas comprar, usar e vender bitcoins, precisará de muito menos tecnologia. Um simples celular ou computador convencional já será suficiente, assim como seria para você movimentar dinheiro no seu internet banking.

Com isso, identificamos dois grupos importantes na rede Bitcoin: os **usuários** e os **mineradores**. No primeiro grupo estão pessoas como você e eu, que simplesmente desejam ter a posse desse dinheiro digital para trocar por mercadorias, serviços ou usar como investimento. No segundo, os mineradores garantem a validação das movimentações, resolvendo problemas matemáticos complexos (por conta da criptografia) e sendo remunerados por isso.

Ou seja, temos uma rede autossuficiente, que não necessita de nenhum banco ou organização para seu funcionamento. Os próprios usuários e mineradores fazem a gestão do sistema. A pergunta natural que surge é: isso tudo é seguro? Faz todo o sentido chegar a esse questionamento. Afinal, passamos nossas vidas acreditando que a segurança está na figura de bancos com cofres enormes.

Minha resposta simples e direta é: sim. Existem poucos sistemas tão seguros quanto os aplicados pelas criptomoedas. Estamos falando do uso da criptografia para evitar fraudes. Como toda transação é registrada em um bloco do blockchain, a cada novo bloco que é adicionado mais e mais esforço matemático precisaria ser empregado para reverter as transações. É por isso que se diz que quanto mais tempo se passa, mais o bitcoin se torna seguro.

Afinal, se você usa seu cartão de crédito ou faz TEDs (transferências) para movimentar dinheiro todos os dias é porque acredita que os sistemas por trás deles são seguros o suficiente para garantir que seu dinheiro não seja roubado ou perdido. Pois bem, o bitcoin é ainda mais seguro, e os usuários precisam apenas de acesso a formas práticas de tê-lo ou usá-lo.

Além disso, a emissão do bitcoin é controlada pelo próprio protocolo. Lembra-se dos mineradores? Seus computadores trabalham ininterruptamente para verificar a validade das transações e são recompensados pelo algoritmo do Bitcoin com novas unidades da moeda. É assim que são produzidos mais bitcoins. A cada quatro anos, porém, essa recompensa cai pela metade, em um processo chamado de *halving*. Até 2140, um total de 21 milhões de bitcoins terão sido minerados (criados) e o algoritmo automaticamente interromperá a produção.

Esse senso de escassez confere ainda mais valor ao bitcoin, uma vez que se sabe que é impossível gerar mais moeda indiscriminadamente, como um banco central faria com as moedas fiduciárias.

Essa escassez programada é o que leva o bitcoin a ser chamado por muitos de “ouro digital”.

Pensando na trajetória do ouro desde os séculos passados, é evidente que o valor do metal cresceu conforme ficou mais difícil encontrá-lo na natureza. Ou seja, escassez e aumento de valor estão diretamente relacionados. Um processo similar pode ser esperado para o bitcoin. Com a oferta diminuindo a cada quatro anos, se a demanda continuar constante ou, como é esperado, aumentar, seu valor crescerá junto.

Você está diante de uma das maiores inovações da história do sistema financeiro; talvez, da história da humanidade. O Bitcoin é o precursor de uma nova economia e, com ele, o universo das criptomoedas reserva um enorme potencial para o futuro.

Ficar indiferente a essa nova classe de ativos simplesmente não é uma opção. Por outro lado, compreendê-la e torná-la parte do seu dia a dia pode ser uma das melhores escolhas que você fará.







## O *HYPE* E A PERGUNTA: É BOLHA?

Se você nunca ouviu a palavra *hype* na sua vida, deve estar se perguntando o que diabos ela significa. Eu gostaria muito de responder exatamente assim: *hype* é *hype*, ora! Mas como a minha intenção neste livro é ser didático, tentarei defini-la e depois mostrarei um exemplo, que é minha forma preferida de explicá-la na prática. Na sequência, você entenderá porque ela tem tudo a ver com o mundo das criptomoedas.

Em um dicionário informal, a palavra estaria definida da seguinte forma:

***hype*: /hīp/**

**Substantivo:** estar extremamente empolgado com alguma coisa.

**Verbo:** promover ou fazer intensa publicidade de algo, geralmente exagerando sua importância ou seus benefícios.

Por essa definição, *hype* pode ter uma conotação pejorativa, já que pode significar apenas uma moda passageira, que não vai ser aceita em larga escala no caso de ser uma promoção exagerada. Mas a história do iPhone vai ajudar você a entender que essa palavra extrapola sua própria definição. E é por isso que gosto de explicá-la também com exemplos.

Basta voltarmos a 9 de janeiro de 2007, quando o primeiro iPhone foi anunciado. Um celular sem teclado e que custaria US\$ 500 foi ignorado como risco para o mercado de smartphones. Na verdade, Steve Ballmer, o então CEO da Microsoft, riu quando lhe perguntaram sobre o potencial do iPhone de ganhar mercado. Ele afirmou que um celular sem teclado não seria atrativo para os executivos que estavam acostumados com o teclado dos smartphones da época.

Como você pode perceber, ele estava completamente errado. Além de ganhar muito mercado nos anos seguintes, o teclado touchscreen ditou a tendência dali para a frente. Por isso, hoje o nosso padrão de celular é retangular, tem tela sensível ao toque e, se cair no chão, quebra. Tudo graças à inovação da Apple.

É por isso que essa história tem muito a ver com o *hype* que quero explicar para você. Pois, no começo da história desses smartphones, o touchscreen era exatamente isto: um *hype*. Quem desejava tê-los eram as pessoas que consomem inovação constantemente. E essa parcela do mercado é muito pequena, cerca de 2,5%. São essas pessoas que topam adquirir produtos não tão bons só para serem os primeiros a tê-los.

No capítulo seguinte, explico com mais detalhes de onde vem esse percentual e como ele ajuda a entender como algo sai do *hype* e vira inovação disruptiva de fato. Por enquanto, quero que você pense de forma bem simples. Uma coisa, para sair do *hype* e se consolidar de fato, tem que ser aceita e entendida por mais pessoas.

Falando ainda do iPhone, o primeiro modelo levou 74 dias para vender 1 milhão de unidades segundo a Apple. Já sete anos depois, o iPhone 6 e o iPhone 6 Plus levaram três dias para vender juntos 10 milhões de unidades. Isso comprova a evolução do *hype* para a aceitação geral. Na verdade, hoje o iPhone passou a ser consenso e se estabeleceu como o principal smartphone do mercado.

O caso do iPhone tem estreita ligação com o universo das criptomoedas, pois, para o bitcoin e outras tantas moedas se consolidarem, elas precisam sair do *hype* e ingressar no consenso. Se isso não acontecer, elas podem se tornar apenas tentativas fracassadas, que ficaram na história ou que foram suplantadas por tecnologias superiores.

Como exemplo disso, temos o *pager*, que foi uma tecnologia muito usada nos anos de 1970 e 1980 para comunicação instantânea, mas que perdeu espaço à medida que os celulares passaram a resolver o problema do envio de mensagens rápidas.

Além do uso da tecnologia para enviar pagamentos e fazer transações entre pessoas, as criptomoedas assumiram uma característica de investimento devido a sua forte valorização nos últimos anos. Então, além do questionamento sobre ultrapassar a barreira do *hype*, outra pergunta ronda a cabeça das pessoas quando o assunto é criptomoedas: será que tudo isso é uma enorme bolha?

Eu até poderia ser leviano, comparar o bitcoin com outras bolhas do passado e tirar alguma conclusão. Poderia traçar paralelos entre a tulipomania, a bolha das companhias de navegação francesa e inglesa e até com a “bolha ponto com”. No entanto, acho mais prudente tomar a visão de alguém que já escreve sobre o assunto, analisar as criptomoedas por essa perspectiva e tirar uma conclusão.

Para tanto, fui atrás do autor de *Boombustology: Spotting Financial Bubbles Before They Burst* (Boombustology: como detectar

bolhas financeiras antes que elas estourem, em tradução livre). Em seguida, apliquei sua teoria sobre as cinco lentes para identificar se algo é uma bolha ao Bitcoin, tanto para avaliar o momento atual quanto para ter uma visão do futuro.

Na verdade, o próprio autor, Vikram Mansharamani (ainda bem que estou escrevendo, e não falando), publicou um artigo avaliando se o bitcoin é ou não uma bolha. Apesar de respeitar o trabalho de Mansharamani, peço licença ao seu artigo, e também às suas conclusões, para apresentar minha própria visão e conclusões.

## **DEFINIÇÕES DE BOLHA: AS 5 LENTES DE VIKRAM MANSHARAMANI**

Vikram (prometo usar somente o primeiro nome do autor, para que você tenha uma leitura mais fácil) propõe a aplicação das cinco lentes para uma correta análise de uma potencial bolha.

São elas:

- Perspectiva microeconômica;
- Perspectiva macroeconômica;
- Psicologia — excesso de confiança;
- Incentivo governamental;
- Epidemiologia.

Em cada item da análise a seguir, iniciaremos com a visão do autor de *Boombustology*, traçaremos paralelos entre as últimas bolhas e, então, avaliaremos o bitcoin pela ótica atual e pela ótica futura.

Vamos nessa?

## PERSPECTIVA MICROECONÔMICA

Basicamente, nesse ponto, devemos avaliar a aplicação da lei da oferta e da demanda que rege boa parte das nossas relações econômicas em ecossistemas financeiros reduzidos. Só preciso que você lembre dessa lei que aprendeu em algum momento da sua vida. Ela diz, em linhas gerais, que quanto maior é a procura por um bem (demanda) maior será o seu preço (oferta). Da mesma forma, o caminho inverso funciona também: quando existe baixa procura por um produto, o preço dele tende a cair. Esse é o modelo simplificado, mas o modelo um pouco mais complexo é contemplado pela situação citada a seguir.

Por exemplo, se a padaria passar a vender pães mais caros, a consequência natural é as pessoas buscarem alternativas mais baratas e acabarem comprando em outras padarias. No entanto, se todas as padarias subirem os seus preços bem pouco, as pessoas podem reclamar, mas talvez ainda continuem comprando pães. Já se todas as padarias dobrarem o preço dos pães de um dia para o outro, além de as pessoas reclamarem, elas deixarão de comprar pães e procurarão alternativas, como bolachas ou biscoitos.

Claro que estou simplificando as coisas, mas a ideia por trás é esta: quanto mais o preço sobe, menos demanda você tem, especialmente com os preços subindo tão rápido como ocorre com as criptomoedas em geral. Mas o que geralmente vemos no preço do bitcoin é que, quanto mais ele sobe, mais atrai a atenção das pessoas e, consequentemente, um maior volume da moeda é transacionado.

Se usássemos essa lente para avaliar o comércio de tulipas na Holanda do século 17, a bolha que se formou na época seria facilmente identificável, já que, com um mercado tão pequeno, qualquer centena de pessoas que entrasse já causaria um grande salto no volume de títulos de tulipas comercializados. Ou seja, um

salto no preço que atraísse uma centena de pessoas já representaria uma quebra da lei da oferta e da demanda, o que mostraria uma tendência à formação de bolha.

Mas, hoje, nosso mercado é muitas vezes maior do que era o do século 17 na Holanda, portanto uma movimentação de centenas de pessoas não representa uma grande movimentação se olharmos de forma global. Por isso, apesar de o bitcoin atrair atenção pela grande valorização, ainda temos menos de 1% da população que tem acesso à internet investindo em bitcoin, segundo um estudo da Universidade de Cambridge.

Faço essa análise utilizando a população mundial porque qualquer análise sobre o bitcoin tem que ser global, já que, além de se propor a ser uma moeda global, ele é negociado no mundo todo. A tulipomania, por outro lado, deve ser analisada localmente, já que aconteceu apenas em solo holandês e que os títulos de tulipa eram negociados apenas por lá.

Ainda continuaremos nossa avaliação com as próximas lentes de Vikram, mas, pela ótica microeconômica, vemos que o bitcoin não pode ser uma bolha. Mas ele pode vir a ser, pois hoje ainda não temos a principal indústria financeira participando desse mercado como participa de outros, investindo em ações e títulos de dívida pública.

A maioria dos investidores de bitcoins e de outras criptomoedas é pessoa física. Ainda temos uma indústria de US\$ 30 trilhões não totalmente dentro desse mercado, pois, por enquanto, os fundos de investimentos não conseguem investir massivamente em criptomoedas. A partir do momento em que esses dois mercados se encontrarem definitivamente, poderemos ver a primeira lente de Vikram se confirmar no mercado de criptomoedas.

## PERSPECTIVA MACROECONÔMICA

A segunda lente do autor é um *zoom out* da primeira. Agora, vamos olhar para aspectos gerais, e não mais para os microssistemas individualmente. Por essa lente, é preciso analisar se existe alguma situação macroeconômica que ajude a elevar os preços das moedas. Para isso, devemos verificar se há a possibilidade de operação alavancada ou com margem de negociação.

Esses dois tipos de operação são muito comuns no mercado de renda variável e podem ser definidos, basicamente, como operações de compra e venda com mais dinheiro do que você realmente possui. Por exemplo, algumas poucas corretoras oferecem a possibilidade de você operar criptomoedas alavancado até cem vezes. Ou seja, se você possuir 1 bitcoin, é possível realizar compras e vendas como se portasse cem unidades do mesmo ativo. Essa condição ajudaria a sustentar altos preços e, se usada por muitos, poderia representar um risco de bolha.

Na época da tulipomania, não era possível fazer operações com alavancagem da forma como fazemos hoje, mas as pessoas podiam pegar empréstimos com bancos e com outras pessoas, o que, em essência, é uma forma de alavancagem. Assim, por essa segunda lente, as negociações de títulos de tulipa também dariam sinais de bolha.

Com as criptomoedas, a situação é diferente, pois apenas algumas corretoras oferecem a possibilidade de operar com alavancagem. Desse modo, enquanto no mercado de capitais atual a ampla maioria das corretoras oferece a oportunidade de negociar valores superiores aos que o cliente realmente possui, nas corretoras de criptomoedas isso não é tão comum.

Logo, pela segunda lente de Vikram, o bitcoin não apresenta características de bolha.

Contudo, assim como o mercado de capitais no início não oferecia muitas possibilidades de operações alavancadas, mas, com o seu desenvolvimento, foi popularizando esse tipo de operação, o mercado de criptomoedas pode seguir o mesmo caminho. Caso isso aconteça, poderemos ter características de formação de bolha pela lente macroeconômica.

## PSICOLOGIA – EXCESSO DE CONFIANÇA

O ser humano é mestre em ver apenas o que deseja que seja verdade. Por esse motivo, a terceira lente de Vikram faz todo o sentido para analisarmos uma bolha. O autor afirma que, em uma formação de bolha, as pessoas estão superconfiantes de que seus investimentos vão dar lucros, e todas as informações que chegam a elas apenas confirmam a sua visão.

Esse viés cognitivo é conhecido como “viés de confirmação” e leva as pessoas a aceitar apenas informações que confirmem seu ponto de vista e a ignorar as que vão contra suas ideias. Isso faz com que as pessoas, mesmo vendo o risco de bolha iminente, o desconsiderem, por acharem que “agora é diferente”, que não precisam se preocupar.

Na Holanda do século 17, vimos um excesso de confiança das pessoas, pautado no aumento contínuo e indefinido dos preços. Foi desconsiderado, contudo, o fato de não haver tantos compradores reais que fossem usar as tulipas para ornamentar uma casa ou um jardim. O que existia em demasia eram compradores que sempre esperavam vender as flores por preços maiores do que os que haviam pago. Não existiam nobres suficientes que pudesse pagar o preço de uma casa por uma *Semper Augustus*.

Sem dúvidas, conseguimos traçar um paralelo com bitcoins e outras criptomoedas. Vivemos uma fase de euforia, em que as pessoas compram bitcoins, principalmente, sem saber o que é e acreditando em sua valorização sem fim. Sinto que estamos realmente vivendo um momento de “agora é diferente”. Por isso, acho que a terceira lente de Vikram se aplica muito bem ao cenário atual do bitcoin e de outras criptomoedas. Estamos mergulhados em um excesso de confiança quanto à valorização ilimitada desses ativos.

Mais à frente, vamos discutir como podemos nos proteger do excesso de confiança de uma forma bem prática, mas antes precisamos saber como esse novo universo se sai quando examinado pela quarta e quinta lentes de Vikram.

## INCENTIVO GOVERNAMENTAL

Assim como na segunda lente, em que uma característica macroeconômica pode ser responsável por uma bolha, a quarta lente também diz respeito a uma influência externa. Os incentivos governamentais podem criar uma demanda artificial por algum bem. Esses incentivos podem vir na forma de isenção de impostos para pessoas físicas ou empresas, e também de compras diretas, por parte do governo, de um ativo específico, fazendo com que seu preço infla.

Além disso, o incentivo governamental pode se dar por meio do risco moral, que é quando existe a perspectiva de que, caso ocorra uma bolha ou crise em um setor, o governo mudará suas políticas e oferecerá socorro. Isso dá a sensação de segurança a diversos setores, o que propicia que se tome mais riscos que o habitual, com a confiança de que, se houver uma queda brusca em um setor, o governo será o paraquedas que vai salvá-lo.

Na bolha imobiliária dos Estados Unidos em 2008, havia incentivos do governo que estimulavam esse setor da economia. Além do que, é claro, havia a perspectiva de que o governo salvaria tanto o setor imobiliário quanto o setor financeiro se estes viessem a quebrar. Essa tendência foi confirmada no estouro da bolha, quando só um dos maiores bancos de investimento não foi salvo, o Lehman Brothers.

Ao olharmos para o universo de criptomoedas, vemos exatamente o contrário disso. O que existe é um desincentivo dos governos para que as pessoas utilizem bitcoin e outras moedas digitais. O fato de esses ativos estarem fora do controle de qualquer banco central assusta os reguladores e faz com que rejeitem a tecnologia e o seu uso. Como consequência desse desincentivo, os governos também não demonstram que estejam dispostos a socorrer as pessoas em caso de crise nesse mercado.

Por isso, não temos o risco moral no universo das moedas digitais, pois quem está investindo nele não tem a perspectiva de que algum órgão o socorra em caso de perdas substanciais. Como exemplo, podemos tomar o caso da Mt. Gox, uma corretora que alegou ter sido roubada grande parte dos bitcoins de clientes que estavam sob sua custódia.

Como a empresa tinha sede em Tóquio, no Japão, várias pessoas procuraram o auxílio da Agência de Serviços Financeiros do Japão, mas esta declarou que nada poderia fazer sobre o ocorrido. Esse evento corrobora o fato de que as moedas digitais não têm qualquer incentivo governamental e, portanto, pela quarta lente de Vikram, não apresentam característica de bolha.

Em um futuro próximo, não vejo os governos se aproximando desse universo a ponto de aceitá-lo amplamente e de posicionar-se para incentivá-lo ou socorrê-lo caso seja necessário. O que consigo ver é, gradativamente, alguns países passando a aceitar moedas digitais em circulação, enquanto outros as rejeitam. Já um incentivo

puro e real para adoção da tecnologia é um passo que não vejo sendo dado no curto prazo e, por isso, ainda não acredito que essa lente se torne verdadeira em um futuro próximo.

## EPIDEMIOLOGIA

Considero que a última lente de Vikram seja a mais fácil de se perceber quando está ocorrendo. Uma história que a ilustra é a de Joseph Kennedy, investidor de risco que saiu do mercado de ações pouco antes da Grande Depressão de 1929 por ter detectado uma epidemia de pessoas na Bolsa. Kennedy fez a constatação quando recebeu dicas de um engraxate sobre como investir. O episódio foi o gatilho para que ele percebesse que o mercado tinha se tornado popular demais e que essa popularização formava uma bolha em torno do mercado de ações.

Na mesma linha dessa “epidemia”, podemos analisar a crise imobiliária de 2008, na qual pessoas sem condições de pagar por um imóvel se alavancavam com duas ou mais casas por meio de hipotecas, na esperança de que os valores dos imóveis sempre subiriam.

Segundo a visão de Vikram, quando muitas pessoas estão participando de um mercado e especulando com ele, há um indício de formação de bolha. Talvez você tenha a percepção de que há muita gente falando e investindo em criptomoedas, mas a verdade é que, pelos mesmos motivos apresentados na primeira lente, posso afirmar que esse mercado ainda não chegou à maioria das pessoas.

Como disse na perspectiva microeconômica, menos de 1% das pessoas com acesso à internet possuem bitcoins e, se compararmos com qualquer mercado, o *market cap* das criptomoedas fica pequeno. Por exemplo, o mercado de moedas e cédulas mundial é de US\$ 5 trilhões. Se as moedas digitais se propõem a ser dinheiro

usado no dia a dia, ainda falta muito para se tornarem uma “epidemia”. Por isso, acredito que, pela quinta lente de Vikram, o bitcoin não apresenta características de bolha.

Porém, para o futuro, vale a mesma ressalva que fiz na primeira lente. Quando os fundos de investimentos, um mercado de US\$ 30 trilhões, conseguirem investir em massivamente criptomoedas, ocorrerá uma popularização imediata do ativo e, então, teremos um grau de epidemia grave. Por isso, a minha visão é que, em um futuro próximo, essa lente venha a ser positiva para as moedas digitais e que elas apresentem características de bolha.

## CONCLUSÃO: É OU NÃO É UMA BOLHA?

Aos leitores que esperavam por uma resposta direta e simples, sinto muito informar, mas terei que decepcioná-los. Posso até fazer uma checklist para saber se o nosso querido mercado de bitcoin passa pelas lentes de Vikram. Dessa forma, teríamos a seguinte configuração:

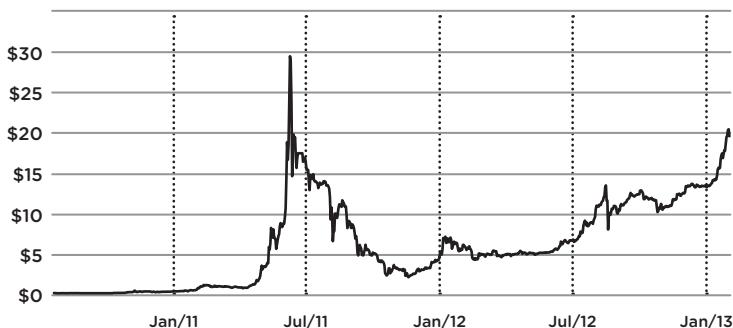
- ( ) Perspectiva microeconômica
- ( ) Perspectiva macroeconômica
- (✗) Psicologia — excesso de confiança
- ( ) Incentivo governamental
- ( ) Epidemiologia

Esses pontos bastariam para avaliarmos se algum ativo está sobrevalorizado e em processo de bolha? Talvez fossem suficientes se estivéssemos em Yale, em uma aula do professor Vikram. Levantar uma questão e discuti-la ajuda a estimular a troca de ideias entre alunos de uma classe e a enriquecer o repertório de todos. No entanto, estamos no mundo real e, para a maioria das pessoas, uma resposta satisfatória seria “sim” ou “não”.

Você que nos lê deve estar ansioso por uma resposta similar, mas eu não posso dá-la se realmente não consigo ter tal definição. Até porque a minha concepção é que o preço do bitcoin já enfrentou diversas bolhas ao longo do tempo. A verdade é que o problema não está na falta de respostas, mas, sim, na pergunta, que deveria ser outra: “por quantas ‘bolhas’ o bitcoin passou?”.

Se avaliarmos o preço do principal criptoativo, podemos entender como todo esse mercado se comporta. Tanto o preço do bitcoin como sua variação oferecem-nos uma visualização mais clara sobre o aspecto de bolha da criptomoeda.

Vamos analisar o primeiro desses movimentos que se tem documentado, o recorde de preço atingido pelo bitcoin em meados de 2011. Perceba que, nessa época, o preço atingiu um pico próximo de US\$ 30 e depois caiu abaixo dos US\$ 5. Apenas olhando o gráfico a seguir, é possível afirmar com alguma segurança que esse foi um comportamento claro de bolha. Os preços estavam inflados muito acima do valor real do ativo, e algum evento desencadeou a venda em massa, fazendo com que o preço sofresse uma perda de aproximadamente 90%. O episódio pode ser considerado o primeiro estouro de uma bolha do bitcoin.



Extraído de CoinDesk | <https://www.coindesk.com/>

Dois anos mais tarde, tivemos uma segunda ocorrência. Em fevereiro de 2013, o preço do bitcoin estava próximo dos US\$ 225 e teve uma queda vertiginosa de mais de 60%. Se tomarmos como referência os padrões do mercado financeiro tradicional, podemos afirmar que, nesse momento, ocorreu a segunda bolha dentro desse mercado, que só retomou seu preço anterior no fim do ano, em novembro.



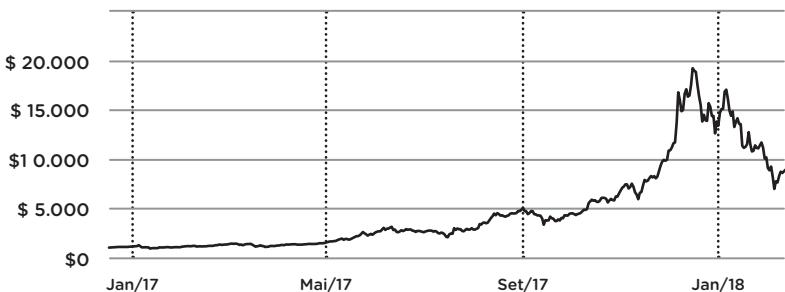
Extraído de CoinDesk | <https://www.coindesk.com/>

Em 2014, o preço do bitcoin passou por mais uma grande queda, repetindo os processos anteriores de desvalorização acelerada e posterior recuperação. Naquele ano, o preço ultrapassou a marca dos US\$ 1 mil e, logo na sequência, perdeu mais de 50% do valor e ficou abaixo dos US\$ 500. Como sempre, os detratores dessa tecnologia falaram em bolha, mas o preço se recuperou, como podemos constatar atualmente.



Extraído de CoinDesk | <https://www.coindesk.com/>

O preço do bitcoin continuou se fortalecendo durante mais de um ano até atingir o recorde anterior, de US\$ 1 mil. Então, recentemente, ele passou por mais uma correção, que assustou os investidores mais novos e fez os antigos respirarem mais fundo e se preparam para aguentar a queda. O preço, ao fim de 2017, atingiu a máxima histórica de aproximadamente US\$ 20 mil e, em cerca de um mês, foi abaixo dos US\$ 10 mil, gerando comentários de que a bolha havia estourado mais uma vez.



Extraído de CoinDesk | <https://www.coindesk.com/>

Esses não são os únicos casos, dentro da evolução do preço do bitcoin, que podemos chamar de “bolha”. Existem outros, em períodos menores e com oscilações até maiores. Basta analisar o gráfico da evolução dos preços em espaços de tempo diferentes para conseguir enxergar esse comportamento por toda a escalada de preço da moeda digital. Ao visualizar períodos mais curtos e mais longos, é possível vê-lo como fractais, movimentos dentro de movimentos, que compõem uma figura maior bem semelhante às suas menores partes. Ou seja, a primeira bolha se tornou apenas um trecho pequeno da segunda, e assim por diante.

Esses ciclos de altas e baixas têm ligação com a expectativa que as pessoas constroem em torno da utilidade do bitcoin. Essa expectativa por um suposto valor futuro faz com que o preço oscile

quando ela não encontra correspondência na realidade. Utilizando um exemplo simples, seria como se as pessoas acreditassem que o bitcoin pudesse substituir o dólar e passassem a comprá-lo com essa visão. Como consequência, os preços subiriam bastante, mas, à medida que o cenário esperado não se concretizasse, as pessoas começariam a vender suas posições e os preços cairiam.

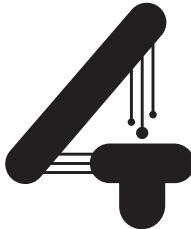
Seguindo a mesma lógica, podemos também analisar as grandes variações em que os preços se tornam cada vez mais altos. Nesse caso, seria como se as expectativas fossem se concretizando ao longo do tempo (o que estaria refletido nos preços crescentes), mas não na velocidade em que as pessoas desejavam e na qual apostaram, daí as quedas abruptas em determinados períodos. Portanto, as maiores variações de preços seriam apenas resultado das expectativas das pessoas com relação à tecnologia, e sua posterior desconstrução parcial, mas seguindo uma linha ascendente, porque o valor da tecnologia cresceria à medida que novos avanços fossem entregues.

Por tudo isso, acredito que a pergunta mais certa a se fazer é por quantas bolhas o bitcoin já passou. Sei que para a maioria dos investidores isso pode parecer um contrassenso. Contudo, se a grande massa chama essas oscilações de preço de 50% a 90% de “estouro da bolha”, então, esse ativo passou por diversas delas. No entanto, o ativo em si não deixou de existir; na verdade, a cada novo choque, ele saiu mais forte e foi buscar novas máximas de preço.

Isso evidencia uma característica muito admirada por investidores de risco: a antifragilidade. Descrito por Nassim Taleb, esse fenômeno diz respeito a investimentos ou objetos que se fortalecem ao serem submetidos a situações estressantes. Um exemplo mitológico é o da Hidra de Lerna, um ser de várias cabeças que, quando tinha uma delas cortada, logo produzia outras duas no lugar.

É desta forma que vemos esse mercado: toda vez que temos as “bolhas”, o bitcoin e os outros ativos voltam mais fortes e buscam novas máximas. Isso nos mostra que estamos falando de algo totalmente novo, com que nunca tivemos contato. Portanto, estamos tratando de uma inovação e devemos conduzir nossa análise de acordo. Com isso em mente, dedicaremos o capítulo seguinte para trazer essa visão.





## ANATOMIA DE UMA INOVAÇÃO

Ao longo do tempo em que eu estive imerso no universo das criptomoedas, os movimentos de valorização e desvalorização, algumas vezes de grande amplitude em um curto espaço de tempo, sempre chamaram atenção. A partir do momento que você compra seu primeiro bitcoin, uma porta é aberta e você entra em um ambiente no qual a volatilidade está sempre presente.

Se, de um lado, as grandes valorizações que diferentes criptomoedas obtiveram ao longo dos anos deixam muitas pessoas animadas e interessadas, por outro, inevitavelmente, levanta-se a discussão sobre bolhas e sobre a real validade dessas valorizações. Pelo que sempre ouvi de quem ainda não havia dado o primeiro passo para comprar criptomoedas, a preocupação quase sempre estava ligada ao desconforto com essa “incerteza” sobre o preço no futuro.

*“Mas por que valorizou tanto?”*

*“Ainda dá tempo de comprar?”*

*“Isso é realmente seguro?”*

*“Não é uma bolha?”*

Certamente faz sentido trazer essas perguntas à tona. Porém, acredito que essa não deva ser a barreira que impede novos investidores de ingressar no universo das criptomoedas. Este capítulo foi pensado exatamente para discutir esse ponto e reforçar nossa visão sobre o mercado. Antes de pensarmos em volatilidade, riscos e incertezas sobre o futuro, é essencial lembrarmos de um ponto: estamos no meio de um processo de inovação.

Isso significa que, diferente de um mercado tradicional que já existe há décadas e vive uma fase de maturidade, como o de títulos públicos ou o de ações, o mercado de ativos digitais está no meio de um processo de desenvolvimento, que certamente não é nem será linear. Contudo, nossa mente está acostumada a pensar de forma linear, incremental. Sendo assim, não é óbvio enxergar de cara o potencial da inovação ou aonde exatamente ela chegará.

Na verdade, os inovadores, aquelas pessoas que desenvolvem soluções disruptivas, nunca têm clareza sobre o futuro. Afinal, se tivessem, não criariam inovações, mas apenas novidades. Pense em grandes invenções que mudaram completamente a forma de nos relacionarmos com um determinado ambiente ou rotina. Antes de elas surgirem, estava claro que aquilo poderia ser usado da maneira como proposto? Obviamente, não.

Um bom exemplo disso é o iPhone. Sua primeira versão foi lançada em 2007 com uma proposta clara: unir as funcionalidades

do iPod às de um telefone móvel que permitisse a comunicação com a internet. Tudo isso com uma tela sensível ao toque. Já existiam outros celulares que buscavam implementar uma ou mais dessas funções. Porém, nenhum deles conseguiu o mesmo sucesso que o iPhone. O grande trunfo da Apple foi unir recursos que estavam espalhados em dispositivos diferentes e combiná-los em um telefone celular.

Entretanto, por mais que Steve Jobs e a equipe da Apple estivessem convictos de que o iPhone revolucionaria o mercado de telefonia móvel, houve opositores que defendiam que ele seria um fracasso. O principal deles talvez tenha sido o então CEO da Microsoft, Steve Ballmer. Quando questionado sobre o que achava do iPhone, ele riu e disse que, além de caro, o celular sequer possuía um teclado físico, o que era ruim para quem desejasse enviar e-mails. Ou seja, remover o teclado físico, que era o padrão dos dispositivos móveis até então, parecia um absurdo para Ballmer.

De fato, mudar o *status quo* não é uma tarefa simples. Na maioria dos casos, há grande oposição, simplesmente pelo fato de a mudança não ser óbvia ou linear. Novos produtos ou serviços disruptivos quebram barreiras que existem para então avançar para uma nova proposta de solução. Da mesma maneira que o iPhone teve opositores no início, as criptomoedas sempre encontraram quem desacreditasse de seu sucesso.

Do ponto de vista do sistema financeiro, as criptomoedas surgiram para revolucionar as estruturas tradicionais e trazer mudanças que até então não haviam sido realizadas, como a geração de valor, o aumento da segurança nas transações e a redução de fraudes com dinheiro fiduciário. Obviamente, dado que os projetos que existem nesse mercado são jovens, há inúmeras incertezas sobre o futuro de cada um deles.

Porém, para um investidor, não é a certeza de sucesso que estará em jogo na hora de decidir se esse é um mercado que merece seu capital, e sim a assimetria das criptomoedas e as propostas tecnológicas e de mercado dos protocolos a elas atrelados. Se não é possível ter certeza de nada no futuro, resta apenas investir em ativos que possuem muito mais potencial de retorno do que de perda.

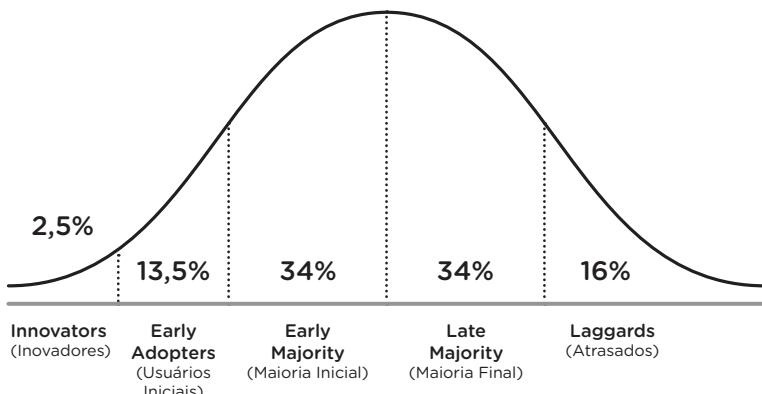
Apesar de essa relação parecer óbvia, pouquíssimas pessoas conseguem enxergá-la de fato, pois, novamente, a mente humana está acostumada a pensar de forma linear e as verdadeiras inovações, as verdadeiras assimetrias, não são lineares. Na verdade, a maioria delas é exponencial. Elas passam por um período inicial de crescimento moderado e, então, em um determinado ponto da virada, começam a crescer de forma exponencial.

Ainda neste capítulo, você verá que esse formato exponencial, no fim, se traduz em uma curva em forma de S, que resume o movimento de adoção de diversas inovações ao longo da história.

## OS 5 ESTÁGIOS DE UMA INOVAÇÃO

Em 1962, Everett M. Rogers, sociólogo e pesquisador da área de comunicação, publicou um livro chamado *Diffusion of Innovations*, no qual discutia sua teoria da difusão das inovações na sociedade. Rogers buscou padrões entre diferentes produtos ou serviços inovadores, de forma a criar um *framework* de avaliação. Ele segmentou o processo de adoção de uma inovação em cinco estágios. Basicamente, trata-se de cinco grupos de indivíduos, sequenciais, que passam a ter contato e a usar essa inovação ao longo do tempo.

Rogers dividiu os grupos conforme o gráfico a seguir:



Extraído de ROGERS, 2003.

Na extremidade esquerda se encontram os inovadores, o grupo de indivíduos mais aventureiros e que estão dispostos a testar novas ideias. É por meio dos inovadores, que formam uma parcela ínfima do total de usuários, que surgem as potenciais disruptões no mercado. São eles que estão expostos à maior parte dos riscos de uma invenção fracassar e que mergulham de cabeça em algo em que realmente acreditam, mesmo diante de um futuro totalmente opaco. Quando se trata de tecnologia, os inovadores são, na maioria das vezes, o público mais técnico, que propõe soluções de implementação para problemas complexos.

Na sequência, estão os *early adopters*, ou usuários iniciais, em tradução livre. São pessoas não diretamente envolvidas com a criação da potencial inovação, mas que, uma vez que tomam conhecimento da nova ideia, querem ter acesso a ela mesmo que não tenha sido testada ainda muito a fundo ou que seja desconhecida pela massa do mercado. Geralmente são pessoas que ficam vasculhando o mercado atrás de novas invenções.

Esses dois primeiros grupos formam uma minoria do mercado, cerca de 16%, segundo os estudos de Rogers. Porém, são eles os

responsáveis por levar uma inovação até a massa do mercado ou não. Caso vá para frente, a nova ideia chega até a maioria inicial (*early majority*), que representa uma fatia significativa do mercado. O processo de adoção continua, atingindo a maioria final (*late majority*) e, então, os atrasados (*laggards*). Esses últimos apenas adotam a inovação por falta de opção.

Com essa divisão em grupos, Rogers identificou cinco estágios pelos quais uma inovação passa no mercado. Indo mais além, existe uma barreira importantíssima formada entre os *early adopters* e a maioria inicial. Note que, quando uma inovação deixa de estar restrita a um grupo pequeno, formado pelos inovadores e *early adopters*, e passa para a primeira fatia de massa do mercado, o grau de adoção praticamente triplica. Essa barreira é o que Malcolm Gladwell chamou de ponto da virada, termo que deu nome a um de seus livros, *The Tipping Point*. Cruzar essa barreira significa levar a inovação à massa do mercado e destravar um processo de adoção mais amplo.

Para entender como esse ponto de virada pode ser atingido e de fato ultrapassado, é necessário compreender o que leva os primeiros 16% do mercado adotar a inovação. Se, por um lado, os inovadores toparam entrar nessa por enxergarem o potencial de uma invenção mesmo sem nada ainda criado, por outro, o que motiva os *early adopters* a entrarem na jogada?

Mais uma vez, o iPhone talvez responda a essa pergunta. O corpo técnico e de negócios da Apple propôs a nova abordagem do celular e acreditava fielmente em sua proposta. Convictos de que o iPhone poderia mudar a indústria de telefonia móvel, seus idealizadores dedicaram milhões de dólares ao seu desenvolvimento. Esses foram os inovadores, que apostaram o capital da empresa, arriscaram suas reputações e usaram seu tempo para desenvolver o dispositivo.

Depois que o produto foi anunciado em uma apresentação memorável de Steve Jobs, uma plateia enorme o ovacionou, louca para ter acesso ao mais novo produto da Apple. Essas mesmas pessoas formaram filas nas entradas das lojas da Apple, esperando horas até que as portas se abrissem e elas pudessem, enfim, comprar o iPhone. Elas poderiam ter esperado alguns dias ou a semana seguinte para fazer isso sem desconforto, sem passar horas e horas na porta de uma loja, mas não quiseram. Elas queriam ser as primeiras, mesmo que isso significasse comprar um iPhone ainda com alguns *bugs*. O risco valia a pena. Era uma simples relação de custo-benefício ou, como gostamos de chamar no mercado financeiro, de assimetria positiva. O que tinham a perder ali era pouco frente ao que ganhariam com a sensação de serem os primeiros a adquirirem o iPhone recém-lançado.

Se essas pessoas de fato gostassem do celular, elas certamente “evangelizariam” o resto do mercado para convencê-lo a ter um também. Foi o que fizeram. O iPhone virou um sucesso de vendas entre outros fatores graças à adesão do público inicial, que contagiou o restante do mercado que veio a comprá-lo. O iPhone, portanto, foi capaz de superar o ponto da virada e atingir a massa, tornando-se um dos aparelhos celulares mais importantes do mundo.

## COMO ULTRAPASSAR O PONTO DA VIRADA

No mesmo livro em que discute o ponto da virada, Gladwell descreve a Regra dos Eleitos, que explica quais são os três grupos de pessoas que tornam possível uma inovação cruzar essa barreira. Ele os divide em **Experts, Comunicadores e Vendedores**.

Os Experts são muitas vezes aqueles que propõem uma inovação e dão vida a ela, por meio da aplicação prática de seus

conhecimentos sobre um determinado tema. Normalmente, trata-se de indivíduos mais técnicos, com conhecimentos aprofundados sobre algo, mas que não são tão capazes de tornar a invenção viral.

O primeiro passo nesse sentido é dado pelos Comunicadores, indivíduos que têm boa capacidade de articulação e que conseguem conectar pessoas de forma fácil. Eles são agregadores que unem as pontas necessárias para uma inovação ser levada à frente. Na maioria das vezes, são os Comunicadores que articulam o time de inovadores que implementará a inovação. Além disso, por terem boa capacidade de comunicação, podem ser os responsáveis por levar a informação até o grupo dos *early adopters* de Rogers.

O trabalho conjunto de Experts e Comunicadores faz com que uma inovação seja proposta, prototipada, desenvolvida e apresentada para um grupo inicial de pessoas. Ao passo que os Comunicadores têm um poder de alcance maior, os Experts resguardam a credibilidade e a segurança das informações do projeto. Essa ótima combinação possibilita que as pessoas certas estejam em contato e que uma ideia seja levada à frente, tirada do papel.

Contudo, apenas esses dois grupos não são capazes de fazer uma inovação cruzar o ponto da virada e ser adotada em massa. A razão para isso, lembre-se, é que a mente humana pensa de forma linear e incremental. Desse modo, a massa do mercado é incapaz de enxergar através de uma inovação e, de cara, identificar seu potencial. Ela precisa ser convencida de que os benefícios da invenção são reais e de que vale a pena adotá-la para si. É nesse exato momento que entram em jogo os Vendedores. Eles são o terceiro elemento da Regra dos Eleitos, que possibilita que uma inovação de fato cruze o ponto da virada. Os Vendedores possuem uma capacidade única de retórica e persuasão e, assim, conseguem convencer a grande massa mesmo que, num primeiro momento, a inovação não seja óbvia para ela.

Experts, Comunicadores e Vendedores trabalham em conjunto para levar a inovação ao público geral. Se ela realmente resolver problemas da sociedade e passar a ser vista como necessária, então cruzará o ponto da virada e deixará de ser algo apenas embrionário ou restrito.

## ALGUMA SEMELHANÇA COM AS CRIPTOMOEDAS?

Quando se analisa a anatomia das inovações e todos os estágios pelos quais elas passam até chegar ao grande público, fica claro que as criptomoedas se enquadram nesse mesmo grupo. É inegável que a proposta do Bitcoin foi inovadora ao trazer descentralização e segurança ao ambiente das trocas financeiras. Da mesma maneira, surgiram outros projetos criptográficos, como o Ethereum, por exemplo, que buscam ir além do ambiente financeiro. O universo das criptomoedas é todo pautado em inovações em diversas frentes. Obviamente, nem todas elas são ou serão de fato relevantes, mas muitas das moedas resolvem problemas reais, de pessoas reais, em um mundo real, apesar de serem essencialmente digitais.

As semelhanças do processo de adoção das criptomoedas com a anatomia de uma inovação são evidentes. Retomando o exemplo do Bitcoin, um grupo de especialistas em criptografia e desenvolvimento de software foi responsável pela concepção da ideia e da implementação inicial. Em um primeiro momento, tudo era restrito a alguns poucos usuários de fóruns que interagiam entre si e se motivavam a agregar ao projeto, pois acreditavam na ideia, mesmo que ela nunca fosse para a frente.

Levou alguns anos até que isso realmente deixasse de ser limitado apenas à esfera técnica. Foi então que o assunto passou a se espalhar entre pessoas que não eram essencialmente técnicas,

mas eram fisgadas por ideias inovadoras. As primeiras pessoas que compraram bitcoin acreditando no seu potencial se colocaram em um risco muito mais elevado do que quem compra hoje, dado que o futuro da criptomoeda era totalmente opaco na época. O que havia era apenas a esperança de que aquela ideia, com o trabalho da comunidade desenvolvedora, ganhasse espaço.

É claro que, no meio do caminho, alguns eventos foram importantíssimos para fazer com que o Bitcoin ganhasse mais atenção e relevância. Alguns deles, inclusive, foram muito polêmicos, como o caso do Silk Road, site de venda de produtos ilegais que usava o bitcoin como meio de pagamento. Apesar disso, a moeda digital só sobreviveu por anos graças ao seu real potencial de transformação do sistema financeiro, e trouxe consigo a criação de várias outras criptomoedas com particularidades diferentes, que visavam melhorar o Bitcoin ou atacar um nicho específico.

As criptomoedas ganharam muito espaço na mídia e evoluem, a cada ano, em número de usuários e valor de mercado. Porém, até mesmo o bitcoin, o ativo digital mais representativo, parece estar logo atrás do seu ponto de virada. É quando uma inovação chega a esse ponto, que, aliás, demanda uma energia muito grande para ser superado, que a massa do mercado começa a tomar conhecimento dela. Antes que o ponto da virada seja realmente cruzado, parte do mercado começa a duvidar ou se opor. Evidência disso são as pessoas que acreditam que as criptomoedas são uma bolha, um esquema de pirâmide ou uma fraude. A maior causa dessa desconfiança é a falta de informação sobre o assunto ou a insegurança que algo novo traz às fatias mais conservadoras do mercado. De fato, os *laggards* da teoria de Rogers vão aceitar as criptomoedas apenas quando elas forem o único formato de pagamento disponível para uma determinada situação.

Apesar da oposição, natural em qualquer processo inovador, as criptomoedas possuem os elementos necessários para superar o ponto da virada. Entre os fatores que as levarão a cruzá-lo estão a entrada de investidores institucionais, por meio de fundos que permitam o investimento em criptomoedas ou empresas que empreguem esse tipo de tecnologia, a criação e disponibilização de plataformas mais amigáveis e simples de ser usadas por leigos, e a adoção, pelas instituições financeiras e governos, da tecnologia das criptomoedas.

Todos esses pontos contribuem para o que é chamado de efeito de rede, que é o efeito que um usuário tem sobre o valor de um certo produto. Veja o exemplo da rede de telefonia. Quanto mais pessoas passam a ter um telefone, mais ele passa a ter valor para quem o possui. Ou seja, trazer as criptomoedas para o grande público significa ativar esse efeito de rede e fazer com que elas passem, cada vez mais, a ter mais valor para quem as utiliza. Soma-se a isso um estudo que ficou conhecido como a Lei de Metcalfe, o qual, a partir do efeito de rede, diz que o valor de uma rede é proporcional ao quadrado do número de indivíduos que a usa. Em termos práticos, portanto, quanto mais adoção as criptomoedas ganham, mais seu valor aumenta no mercado, de forma exponencial.

A conclusão é que as criptomoedas parecem ter mostrado apenas a ponta do iceberg. Estamos logo atrás do ponto da virada. Até o momento, já foram obtidos ganhos muito elevados. Contudo, esse é apenas o início. Se as criptomoedas conseguirem ultrapassar o ponto da virada, criarão ainda muito mais valor para seus usuários. Os *early adopters*, obviamente, assumem mais risco ao entrar primeiro nesse universo, mas também terão um retorno muito mais elevado no caso de sua tese se confirmar. Quanto mais cedo se entra nesse mercado, mais assimétricos são os potenciais de retorno.

## OS GATILHOS PARA A ADOÇÃO EM MASSA

Até este momento, você entendeu qual é a anatomia de uma inovação e qual a sua semelhança com as criptomoedas. Voltando ao exemplo do livro de Gladwell, há três grupos responsáveis por fazer uma inovação cruzar o ponto da virada: os Experts, os Comunicadores e os Vendedores. Porém, não será apenas com base na ideia por trás de sua concepção que uma criptomoeda como o bitcoin alcançará a massa. Sem dúvida, esses três grupos de pessoas serão fundamentais para espalhar o conhecimento sobre esses ativos digitais. Contudo, uma investigação mais profunda revela quais são, de fato, os gatilhos que precisam ser acionados para esses três grupos de indivíduos entrarem em ação. A seguir, aponto três gatilhos principais.

### Gatilho #1 — Usabilidade

Lidar com criptomoedas não é algo tão simples. Sim, isso já foi muito mais complicado, quando o conhecimento e as ferramentas eram restritos ao grupo dos Experts. Porém, mesmo com os avanços obtidos nos últimos anos, ainda há uma distância que separa os usuários completamente leigos da utilização efetiva das criptomoedas no seu dia a dia.

A usabilidade está ligada principalmente às carteiras e às corretoras de criptomoedas. Nestas, as plataformas se parecem bastante com as de uma corretora de ativos tradicionais. Entretanto, o fato de não existir ainda um mercado unificado e a limitação de suporte para novos usuários fazem com que o processo de uso de uma corretora não seja para qualquer um. Sem dúvida, temos visto grandes avanços nesse sentido, e parece ser mais uma questão de tempo e desenvolvimento do que uma grande limitação do sistema.

No que diz respeito às carteiras, ou *wallets*, uma vasta gama de aplicações foi criada nos últimos anos. Se antes era preciso baixar um

programa complexo para computador e passar por muitas etapas, hoje é possível ter um aplicativo instalado no celular, que gerencia suas chaves (pública e privada) para que você tenha acesso prático às suas moedas. Contudo, as carteiras ainda estão em processo de evolução nos quesitos usabilidade e segurança. Normalmente esses dois fatores ficam em lados opostos de uma balança. Para ganhar em usabilidade, a carteira perde em segurança, e vice-versa. A questão da segurança é extremamente importante, visto que nesse mercado não existe um custodiante ou órgão garantidor. Você é seu próprio banco. Sendo assim, conforme os aplicativos evoluírem para permitir maior acesso dos usuários, ao mesmo tempo que conseguem transmitir segurança no armazenamento dos fundos, veremos uma escalada na adoção das criptomoedas.

## **Gatilho #2 — Instrumentos de varejo e acesso de investidores institucionais**

Por mais que existam corretoras nas quais qualquer pessoa física pode ter cadastro e negociar, ainda é necessário que esse mercado evolua para algo mais próximo ao que é o mercado de corretoras de ativos tradicionais. Para que possam ganhar escala, as plataformas de corretoras precisam seguir melhorando.

Hoje o investidor tem acesso à negociação de criptomoedas e algumas formas alternativas de investimento. Outros instrumentos de varejo precisam surgir para que o acesso a esse mercado seja ampliado. Estamos falando de fundos de investimento que possam se posicionar em criptomoedas e empresas que utilizem ou invistam em tecnologias desse meio, como o blockchain. Basta perceber que uma grande massa de investidores prefere aportar seu capital em fundos de investimentos de renda fixa, de ações, multimercado e outros em vez de ativamente comprar cada um desses ativos. Portanto, a criação de instrumentos de varejo, como fundos que permitam o acesso passivo a ativos do mercado de criptomoedas, é elemento essencial para a ampliação da adoção.

De outro lado, há o grupo dos investidores institucionais, que possuem capacidade limitada de exposição a esse mercado. Ampliar essa capacidade passa tanto pelo processo regulatório em curso nos diversos países quanto pela criação de instrumentos que funcionem como os fundos para pessoas físicas. Os investidores institucionais carregam uma verdadeira fortuna e uma simples migração de um pequeno percentual dela para o mercado de criptomoedas o levará a um patamar completamente diferente.

Esses dois gatilhos apresentados até aqui são essenciais para que o mercado de criptomoedas se desenvolva e ganhe capilaridade. Porém, o terceiro gatilho é um completo *game-changer*, capaz de mudar toda a história financeira.

### **Gatilho #3 — A fragilidade das moedas fiduciárias**

Como já foi discutido no capítulo 2, as moedas nacionais são frágeis pelo simples fato de dependerem de nossa fé nos governos. Cada governo detém sua máquina de impressão de dinheiro e pode fazê-lo como bem entender. Esse procedimento é o início de um processo de diluição da moeda, que causa destruição de valor, mas que não se limita a isso.

Você provavelmente se lembra da crise de 2008, quando a bolha imobiliária estourou nos EUA, causando o colapso de instituições financeiras como o Lehman Brothers. Essa crise resultou de uma superalavancagem do mercado imobiliário e de uma distribuição de crédito sem parâmetros. Naquela época, bastava ter o equivalente a um RG que você conseguia alugar um imóvel. Criaram-se instrumentos derivativos de derivativos, cujos *ratings* eram definidos sem base nenhuma. Quando essa bolha chegou ao seu limite, de repente, percebeu-se que não havia como honrar todos os compromissos e o sistema começou a colapsar.

Com isso, os bancos começaram a ruir. Primeiro foi o Bear Stearns, seguido por Fannie Mae e Freddie Mac. Logo após, vieram Lehman Brothers e AIG, como uma cadeia de dominós, um derrubando o outro. Bancos como Morgan Stanley, Goldman Sachs e J.P. Morgan estavam na fila e seriam os próximos, não fosse a intervenção do governo americano. Ele passou a injetar dinheiro para salvar as instituições e todo o sistema de um colapso total. Quando fez isso, introduziu na economia uma quantia enorme de dinheiro, que simplesmente destruiu valor para os cidadãos americanos e do resto do mundo.

Como sempre, quando algo assim acontece, o maior prejudicado é o povo, e não as instituições financeiras. Milhões de pessoas tiveram seus destinos mudados a partir daí. Muitos perderam casa, emprego ou outros bens do patrimônio. Enquanto isso, os peixes grandes dos bancos não tiveram sequer alteração nos seus bônus. Isso não só coloca em xeque o sistema financeiro como um todo, como também é um enorme sinal de alerta sobre a fragilidade das moedas nacionais fiduciárias, aquelas nas quais supostamente temos fé.

O sistema financeiro é capaz de aguentar uma certa pressão e, em 2008, esteve próximo do seu máximo. Seria um enorme engano acreditar que outra crise como essa não acontecerá de novo, apesar de os governos nacionais parecerem pensar que “agora será diferente”.

Se é inevitável que outro estouro aconteça nos próximos anos — e não muito distante de hoje —, como poderíamos proteger nosso capital? Parte da resposta está nas criptomoedas. Como elas não dependem de governos, estão imunes à destruição de valor gerada pelos bancos centrais. Por isso, funcionam como reserva de valor, principalmente para momentos de crise. Em um cenário em que tivéssemos uma crise tão grande ou maior do que a de 2008,

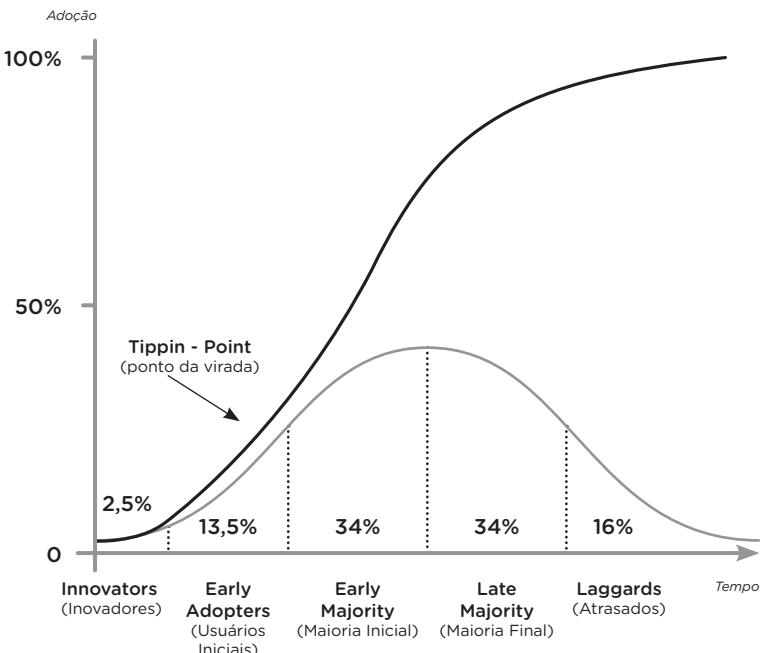
o bitcoin e as altcoins poderiam receber um volume gigantesco de aporte financeiro, que mudaria por completo o mercado de criptomoedas e o alçaria a um novo patamar de valor.

## AH... MAS EXISTE UMA BOLHA DENTRO DO PRÓPRIO MERCADO DE CRIPTOMOEDAS!

A discussão sobre a anatomia da inovação reforça a tese de que as criptomoedas ainda têm muito espaço a ganhar no mercado, porém não encerra completamente a especulação sobre a existência de uma bolha. O mercado desses ativos digitais tem, sim, uma evolução que se assemelha à de bolhas financeiras. Aquela a que mais se assemelha é a bolha ponto com ou bolha da internet. O grau especulativo no mercado de empresas de tecnologia era tão alto que a bolha simplesmente estourou no momento em que perceberam que o valor estava completamente descolado dos fundamentos.

Do lado das criptomoedas, existem algumas diferenças. É impossível, por exemplo, montar um modelo de fluxo de caixa tal qual o de uma empresa e avaliar o *valuation* de uma moeda digital. Existem abordagens nesse sentido, mas, no fim das contas, uma criptomoeda simplesmente não é uma empresa. Ela ganha valor conforme mais capital é direcionado para ela e quanto mais as pessoas a usam. Seu valor é formado ao longo do tempo, diferentemente de uma empresa, que possui, por exemplo, um valor patrimonial declarado contabilmente.

Quando se observa a evolução do bitcoin ao longo dos anos como moeda digital, seu movimento parece menos com o de uma bolha e mais com o de uma curva em S. Essa curva nada mais é que a síntese da anatomia da inovação, criada pelos cinco estágios propostos por Rogers. Se colocarmos em um gráfico como evolui o percentual de adoção de uma inovação ao longo do tempo, o resultado será algo assim:



Extraído de GLADWELL, 2009.

Ainda assim, poderia haver uma bolha no mercado de criptomoedas como um todo? Claro que sim. Apesar disso, vale lembrar que a bolha ponto com estourou e levou consigo as empresas que não eram representativas, e aquelas que realmente eram inovadoras e sólidas prosperaram nos anos à frente. Se uma bolha estourar no mercado de criptomoedas, as moedas que não fazem sentido ou que não possuem um grau de adoção elevado simplesmente deixarão de existir, enquanto as que são de fato representativas continuarão.

O ponto central, que diferencia essa possível bolha de uma crise global, é o fato de não haver um efeito em cascata que faça a economia mundial ruir, bem como a inexistência de um órgão central disposto a injetar dinheiro para sustentar o mercado.

O estouro dessa bolha seria mais como uma “limpeza” do mercado, eliminando as moedas que não são representativas e mantendo as que são embasadas em fundamentos e potenciais sólidos.

Havendo bolha ou não, é possível lucrar nesse mercado adotando estratégias adequadas, que discutiremos nos capítulos 7 e 8 e buscando os reais potenciais de inovação. Lembre-se de que estamos vivendo não só o nascimento de um novo mercado, mas também um completo processo de transformação digital no mundo, e que as criptomoedas possuem as características necessárias para surfar as próximas ondas da era digital.







## BLOCKCHAIN: A TECNOLOGIA DISRUPTIVA QUE VAI MUDAR O MUNDO

Até este ponto, você entendeu como a proposta do Bitcoin veio para transformar o sistema financeiro tradicional. Com o advento desse ativo digital, outras criptomoedas e criptoativos surgiram como derivações. No ano de 2017, registramos mais de mil ativos, entre moedas e tokens. De um lado, foram criadas diversas abordagens para as transações financeiras. De outro, aplicações da criptografia a outras esferas, como a de contratos inteligentes entre duas ou mais partes. Por trás de praticamente todos esses desenvolvimentos, está uma tecnologia inovadora e disruptiva: o **blockchain**.

Antes de entrarmos em mais detalhes sobre o que é e como funciona o blockchain, de forma simplificada, podemos entendê-lo como um registro de dados extremamente confiável. É ele que

garante que as transações feitas na rede do Bitcoin sejam seguras e impossíveis de se fraudar. O blockchain é uma ferramenta baseada em segurança de dados, que torna desnecessário haver um órgão central para o estabelecimento de confiança entre as partes.

Para que seja mais fácil visualizar seu real poder e aplicação, vamos considerar três exemplos práticos, situações do cotidiano que requerem registros de informações e que estão naturalmente sujeitas a falhas e fraudes.

### **Caso 1 — O funcionário que alterava o registro de caixa da loja e roubava o patrão**

Em uma cidade pequena do interior de São Paulo, uma loja de roupas funcionava de forma bastante simples. O dono controlava tanto o estoque quanto o caixa da empresa por meio de uma planilha no computador. O método havia sido adotado após muito tempo usando o registro em papel. Com a planilha eletrônica, cada compra era registrada como uma nova entrada. Inseria-se o valor pago pelo cliente, a forma de pagamento (dinheiro, cartão ou cheque) e o item comprado, para posterior baixa no estoque.

No fim de cada mês, o dono da loja verificava quantas vendas haviam sido feitas e qual era o faturamento. O dinheiro físico recebido ficava guardado no estabelecimento para ser depois depositado na “boca do caixa”. Os cheques também eram compensados no banco e os valores pagos com cartão de crédito ou débito eram recebidos de forma eletrônica, via transferência bancária.

O dono da loja tinha um funcionário que ficava no caixa e organizava os registros de vendas todos os dias, no fim da tarde. O funcionário era supostamente de confiança e devia entregar ao dono um pequeno relatório das entradas de dinheiro no negócio. Por confiar no funcionário, o dono nem sempre conferia à risca os

números, até que percebeu que havia algo estranho. O faturamento estava menor do que em meses anteriores, mesmo com as vendas em alta. Então, o proprietário da loja resolveu separar algum tempo para conferir as contas do estabelecimento. Ao ler o registro de vendas com cuidado, veio a surpresa: os valores anotados para algumas peças de roupa vendidas não condiziam com o valor que deveria ser cobrado. Mais estranho era que todos os registros alterados eram referentes a vendas com dinheiro em espécie. O dono da loja começou a suspeitar do funcionário e foi conferir as gravações da câmera de segurança, que ficava apontada para o caixa.

Ao analisar as imagens, percebeu imediatamente que estava sendo roubado. O funcionário recebia o valor correto em dinheiro, porém separava uma parte dele para si, enquanto lançava um valor menor no registro de vendas. Naquele momento, o dono perdeu toda a confiança que tinha no funcionário e ainda foi obrigado a arcar com um prejuízo de milhares de reais.

### **Como o blockchain poderia ajudar**

O blockchain nada mais é do que uma ferramenta de registro, assim como era a planilha usada na loja de roupas. Porém, no caso da loja, o funcionário podia incluir no sistema qualquer valor de venda, mesmo que fosse falso. Assim, não só o dono precisava confiar no funcionário (o agente central que organizava as contas e registros de transações da loja), como este podia incluir informações falsas no registro, pois ninguém iria “auditar” esses dados.

No caso do blockchain, temos uma forma de registro que funciona em uma rede distribuída de usuários. Tomando o blockchain do Bitcoin como exemplo, todos os membros da rede podem ter uma cópia desse registro e verificar as transações que são feitas. Assim, temos vários olhares direcionados para as movimentações financeiras. Para que uma transação seja efetivamente incluída no

registro, usuários “especiais”, os chamados mineradores, resolvem problemas matemáticos complexos para atestar a veracidade da transação, gastando, para isso, poder computacional e energia elétrica. Basicamente, os mineradores precisam provar o esforço despendido para que uma transação seja considerada verdadeira. Esse modelo é conhecido como Prova de Trabalho (*Proof-of-Work* ou PoW).

Além disso, outro problema que não existiria com o uso do blockchain — e, consequentemente, de uma criptomoeda — é a possibilidade de o funcionário receber o valor total de uma compra em espécie, mas repassar ao caixa somente uma parte. No blockchain do Bitcoin, todas as transações geram entradas e saídas que precisam condizer umas com as outras. Em termos práticos, isso quer dizer que, se o funcionário vendeu uma peça de roupa por R\$ 100, necessariamente R\$ 100 precisam ir para o registro de caixa da loja. Caso sejam registrados apenas R\$ 80, haverá informações que indicarão para onde foram os outros R\$ 20.

Há um outro possível problema para o dono da loja que seria facilmente contornado com o blockchain: os cheques sem fundo. Um cheque nada mais é do que um pedaço de papel em que se anota um saldo devido. Quando a pessoa que recebeu o cheque for compensá-lo no banco, o saldo devido será debitado da conta de quem pagou. Porém, esse sistema abre uma enorme brecha para a emissão de cheques sem fundo, já que quem recebe o cheque não consegue verificar instantaneamente se o pagante dispõe de fundos. Com o uso do blockchain, isso não ocorreria, pois todas as transações são anotadas e para cada uma delas é gerada uma saída, que indica se o valor envolvido foi gasto ou não. Assim, se fosse possível emitir um cheque de bitcoin por meio do blockchain, este verificaría o saldo e validaria a transferência, para então aceitá-la ou negá-la.

## **Caso 2 — As eleições para presidente que foram fraudadas**

No Brasil, já usamos há alguns anos um sistema digital de votação, com as famosas urnas eletrônicas. Esse foi um avanço em relação à grande maioria dos países do mundo, que ainda realizam as votações com cédulas de papel. Porém, em ambos os sistemas, sempre há especulações de fraude na contabilização de votos, pois cada um deles (papel ou urna eletrônica) é passível de alterações nos registros.

Tomemos como exemplo um país que realiza suas votações com cédulas de papel e no qual, em determinada eleição presidencial, tenha havido suspeitas de adulteração do resultado. Isso seria extremamente possível, dado que as cédulas de votação são preenchidas à mão pelas pessoas, depositadas em uma urna e, então, levadas aos centros de contabilização de votos. Estamos falando de um processo cheio de brechas para a fraude.

Levantada a suspeita de fraude na eleição, iniciou-se uma investigação em nível nacional e descobriu-se que havia um grupo de pessoas que adulterava a contabilização da votação, mudando o candidato que tinha recebido o voto. Com isso, votos que deveriam ter ido para um candidato, na realidade, foram contabilizados para outro, que acabou ganhando a eleição. Esse é um problema gravíssimo, que poderia acontecer mesmo com o uso de urnas eletrônicas, já que o sistema de votação pode ser hackeado e os registros, alterados.

### **Como o blockchain poderia ajudar**

Retomando o exemplo do blockchain do Bitcoin, esse sistema de registro utiliza técnicas de criptografia para garantir a segurança dos dados gravados em cada bloco da cadeia. Já entendemos, no caso anterior, que um valor é incluído no sistema por um agente,

chamado minerador, que realiza essa tarefa despendendo poder computacional e energia elétrica. Uma vez que a veracidade da informação foi atestada e tudo foi registrado no blockchain, o processo segue para os próximos blocos de informação, um após o outro. Imagine que o voto de um cidadão foi registrado em um determinado bloco desse blockchain. Cada novo voto vai sendo incluído em sequência e, a cada grupo de votos, um novo bloco é criado. Quanto mais blocos são adicionados à sequência, mais difícil fica de alterar a informação do voto, pois você tem que alterar toda a sequência de blocos até chegar àquele em que o voto foi registrado.

No caso do blockchain do Bitcoin, considera-se que, após seis blocos minerados, é impossível obter poder computacional suficiente para reverter a criptografia e alterar o registro dentro de um bloco. Certa vez, ouvi de Don Tapscott, fundador do Blockchain Research Institute, a seguinte definição, que ilustra bem o funcionamento dessa tecnologia: “O blockchain é uma cadeia sequencial de blocos de informação. A cada novo bloco inserido nessa cadeia, mais processada fica a informação e mais difícil é alterar ao bloco inicial. O blockchain é como um *nugget* de frango. Você pega o animal (informação original) e o processa várias e várias vezes até chegar no formato de um *nugget* (informação processada). Tentar reverter o processo é como tentar fazer o *nugget* voltar a ser um frango — o que, atualmente, é impossível.”.

Assim, o blockchain funciona como um sistema de armazenamento de dados que, quanto mais blocos são incluídos na sequência com o tempo, mais robusto se torna e mais difícil é reverter o processo para alterar a informação original. Ou seja, quanto mais tempo passa, mais seguro ele fica. No exemplo das eleições, se os votos fossem registrados no blockchain, teríamos certeza de que os dados originais não seriam adulterados por ninguém e, quanto mais tempo passasse da eleição, mais segurança teríamos sobre os dados das votações.

### **Caso 3 — A empreiteira que não respeitava prazos, muito menos a lei**

Agora imagine a seguinte situação: uma empreiteira é contratada para realizar uma obra estatal. O contrato inicial diz que a obra seria entregue completa em três anos, com diversos entregáveis menores durante esse período. Ao fim do primeiro ano, a obra já está atrasada, e uma nova avaliação conclui que a finalização se dará, na verdade, em três anos e meio. Ao fim do segundo, ocorre mais um atraso. O tempo total é jogado para quatro anos e dois meses. E por aí vai, até que a obra é concluída em seis anos, não em três. Além disso, o orçamento inicial de R\$ 2 bilhões foi alterado diversas vezes, e a obra acabou custando R\$ 5 bilhões para os cofres públicos. Notou alguma semelhança com a realidade?

Não bastasse o atraso na entrega e o superfaturamento, após dois anos do término da obra, descobre-se que a empreiteira havia desviado dinheiro e feito um “caixa dois”. Uma investigação é instaurada para o caso, porém deve levar anos para ser concluída e provavelmente nenhuma atitude concreta será tomada. Tanto a empreiteira quanto um grupo de políticos haviam desviado verba da obra, e a população, que deveria ser beneficiária da construção, acabou arcando com o prejuízo financeiro.

Infelizmente, isso não é incomum no Brasil, pois os registros dos entregáveis realizados e dos valores pagos podem ser facilmente adulterados. Porém, com o uso dos chamados contratos inteligentes — funcionalidade desenvolvida no blockchain do Ethereum —, isso poderia ser mitigado.

### **Como o blockchain poderia ajudar**

No início do capítulo, mencionamos a criação de diversos tipos de criptomoedas e criptoativos. A grande maioria deles utiliza um

blockchain para a realização de transações, e cada um tem suas particularidades. O Ethereum, que funciona como um computador descentralizado capaz de rodar inúmeros tipos de aplicações, implementou em seu blockchain os chamados contratos inteligentes (*smart contracts*). Por meio deles, são estabelecidas as partes envolvidas, as cláusulas de realização e detalhes de como a ação final (o pagamento, nesse caso) deve ser tomada.

Para o exemplo da empreiteira, o contrato de trabalho poderia ser feito via contrato inteligente, no qual os entregáveis estariam bem definidos. Apenas mediante a conclusão deles o pagamento seria realizado. Além disso, seria possível estabelecer cláusulas de atraso, em que a empreiteira estaria obrigada a pagar multas em caso de adiamento na entrega do projeto. Desse modo, ela seria penalizada se não cumprisse o prazo inicial de três anos.

Talvez você imagine que a obra poderia atrasar por uma causa natural — devido a fortes chuvas durante o período de verão, por exemplo —, e não por manipulação ou má-fé. Para essas situações, a empreiteira poderia estabelecer um contrato inteligente com uma seguradora, que prestaria o serviço de seguro da entrega da obra em caso de interrupção por causas naturais.

Indo além, o pagamento só seria liberado para a empreiteira após a entrega completa do projeto ou após entregas parciais. Como os pagamentos seriam gerenciados pelo contrato inteligente e registrados no blockchain, o desvio de verba se tornaria impossível. A obra também não seria superfaturada, já que o valor inicial seria respeitado por contrato e os atrasos gerariam penalidades.

Os contratos inteligentes podem ser configurados de diversas formas. Assim, é possível estabelecer várias entradas e várias saídas para o projeto e realizar toda a atividade dentro de um ambiente controlado e seguro. O blockchain e suas aplicações extrapolam o

âmbito financeiro e podem ser usados como solução para inúmeros problemas de fraude, adulteração e falsificação que existem hoje na sociedade.

## OS PRINCÍPIOS DO BLOCKCHAIN

Ao longo das últimas décadas, a criptografia tem sido muito utilizada em aplicações de segurança. Sempre houve a preocupação, nas mais diversas áreas, com a integridade da informação transmitida ou armazenada — engana-se quem acha que isso é coisa recente. Em 1918, o engenheiro alemão Arthur Scherbius patenteou um equipamento conhecido como máquina Enigma, um dispositivo que utilizava a criptografia para codificar mensagens. A máquina foi desenvolvida para uso comercial, para permitir que organizações ao redor do mundo enviassem e recebessem informações de forma segura. Isso ocorreu quase um século antes da concepção do Bitcoin. Porém, foi com a criação do blockchain e o estabelecimento do protocolo de transações ponto a ponto (*peer-to-peer* ou P2P) que um novo salto foi dado.

O blockchain que conhecemos e utilizamos hoje veio da concepção de Satoshi Nakamoto para o protocolo Bitcoin. A ideia central era criar um livro contábil extremamente seguro e que mantivesse algum nível de privacidade sobre as informações de transação. Isso estava em consonância com a proposta do manifesto *cryptopunk*:

*“A privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é a mesma coisa que segredo. Um assunto privado é algo que não se quer que o mundo inteiro conheça, mas um assunto secreto é algo que não se quer que ninguém conheça. A privacidade é o poder de revelar-se seletivamente ao mundo.”*

*Cypherpunk* é uma expressão que une dois termos: “*cypher*” (um algoritmo para fazer criptografia e decodificação) e “*cyberpunks*” (os rebeldes aficionados por tecnologia e adeptos da cultura *do-it-yourself* ou “faça você mesmo”). O movimento *cypherpunk* se iniciou em 1992, na Califórnia, a partir de uma comunidade de matemáticos, criptoanarquistas e hackers. Sua ideia central, carregada de pensamentos libertários, era desenvolver programas de computador que estabelecessem ambientes seguros de troca de informação, experimentação e respeito às liberdades individuais. Antes mesmo do surgimento do Bitcoin, já se buscava criar sistemas de pagamento que colocassem a questão da privacidade e da resistência à censura no centro de tudo. No entanto, nenhum desses projetos havia conseguido, efetivamente, implementar a proposta, por não conseguir resolver questões técnicas e econômicas que permitissem a adoção em larga escala.

O blockchain foi um dos elementos fundamentais para que o Bitcoin superasse as dificuldades encontradas até então pelos outros projetos do movimento *cypherpunk*. Ele armazena todos os dados de todas as transações realizadas, porém não associa a elas a identidade do usuário. Essa foi a primeira abordagem das criptomoedas com relação à tão sonhada privacidade.

O blockchain utiliza uma infraestrutura de chaves criptográficas para realizar as transações. Trata-se de um par de chaves, uma pública (à qual todos os participantes da rede podem ter acesso) e uma privada (à qual somente o detentor da criptomoeda deve ter acesso). A chave pública é usada para gerar um endereço público para as transações, algo semelhante ao conjunto agência e conta-corrente do seu banco. Esse endereço público possibilita que o usuário receba transações de valor, bastando para isso divulgá-lo a quem desejar.

Na concepção original do Bitcoin, não seria possível ligar um endereço público diretamente a uma identidade, e de fato

isso não é possível. Porém, na prática, o blockchain do Bitcoin não é 100% privado, já que os registros de transações são abertos a todos os participantes da rede e, com algumas contas e a triangulação de dados, é possível descobrir quem originou a transação, ligando, assim, um endereço público a uma identidade. Nos últimos anos, têm surgido outras criptomoedas que usam blockchains alternativos para garantir total privacidade nas transações. Mas a privacidade em si acaba sendo mais uma característica adicional do blockchain, pois seu real diferencial está na segurança de dados.

Existem alguns princípios básicos que foram aplicados pela tecnologia do blockchain. Em seu livro *Blockchain Revolution*, Don Tapscott define sete princípios do projeto da economia blockchain. Aqui, vamos focar em cinco, que são fundamentais para o funcionamento de uma rede como a do Bitcoin.

## 1. Segurança

O blockchain permite que as informações de transações sejam armazenadas de forma segura, sendo impossível alterá-las uma vez que tenham sido incluídas na cadeia e a informação tiver sido processada. Com isso, temos um sistema mais robusto do que os dos bancos ou das instituições financeiras — como as empresas de cartão de crédito —, nas quais os registros estão sujeitos a ataques e adulterações por parte de hackers.

## 2. Privacidade

Como discutido anteriormente, existe um certo grau de privacidade na transferência de dados, no sentido de que um endereço público não pode ser ligado de imediato a uma determinada identidade. Existem outras criptomoedas, além do bitcoin, que focam em algoritmos e estruturas de dados para garantir total privacidade nas transações.

### **3. Incentivo à participação na rede**

Se não há um órgão central para validar as transações, isso precisa ser feito pelos diversos participantes da rede. É aí que entram os mineradores. Esses são indivíduos que despendem poder computacional para realizar operações matemáticas complexas e resolver problemas do algoritmo, que resultam na validação das transações. Porém o minerador não faz tudo isso de graça. Ele recebe um incentivo para participar da rede. No modelo mais comum de mineração, o *Proof-of-Work*, o minerador apresenta uma prova do trabalho realizado para validar uma transação e é remunerado por isso com novas moedas. No caso do Bitcoin, a remuneração começou com 50 bitcoins por bloco em 2008 e, desde então, tem caído pela metade a cada quatro anos. Atualmente, cada bloco minerado resulta em uma remuneração de 12,5 bitcoins. Esse valor será válido até o ano de 2020, quando cairá pela metade mais uma vez.

### **4. Inclusão**

O blockchain permite a inclusão econômica e democratiza o acesso aos serviços financeiros. Enquanto a transferência bancária entre dois países — por exemplo, o envio de US\$ 1 mil do Brasil para os Estados Unidos — é um processo moroso e caro, com o blockchain não há barreiras para as transações de valor. Enviar uma fração de bitcoin de um usuário em São Paulo para um no Rio de Janeiro envolve o mesmo trabalho e custo que enviá-la de São Paulo para Taiwan. Assim, indivíduos que não possuem conta em banco ou não teriam condições de fazer remessas internacionais periódicas têm uma nova forma de enviar dinheiro pelo mundo. O blockchain torna as criptomoedas ativos sem fronteiras.

## 5. Descentralização

No blockchain, o poder está distribuído. Não há um órgão central que regule como as transações são realizadas, muito menos que tenha poder para tomar decisões sozinho. Cada participante da rede — isto é, cada minerador — tem sua parcela de poder.

A descentralização não apenas constrói um sistema democrático como faz com que a rede não tenha um ponto central de poder sujeito a ataques. O blockchain não tem um servidor central que possa ser hackeado, pois esse “servidor” está distribuído entre os mineradores. Ao tirar o controle das mãos de um só governo ou corporação, busca-se evitar que ocorram novos colapsos financeiros como o de 2008. Na época, um dos grandes propulsores da crise financeira global foi a concentração de dinheiro e de poder nas mãos dos grandes bancos. Eles é que definiam como o dinheiro circularia e tomavam as decisões sobre a economia. Ironia ou não, mesmo com o colapso total ao redor do mundo, os bônus dos banqueiros não sofreram alteração. Algo precisava ser feito, e foi.

O Bitcoin surgiu logo após a crise de 2008, com a proposta de descentralizar o poder financeiro. Em seu bloco gênese, o primeiro da cadeia, consta a seguinte frase: “*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*” (“Chanceler à beira do segundo resgate dos bancos”, em tradução livre). Essa é a manchete de uma edição do jornal britânico “The Times”, que anunciava os efeitos pós-crise global. Claramente, a instabilidade financeira mundial motivou Satoshi Nakamoto a criar uma solução que não mantivesse nas mãos de poucos órgãos o poder sobre a vida financeira de milhões de cidadãos.

Esses cinco princípios definem como funciona o blockchain. A aplicação inicial, com o Bitcoin, foi financeira. Porém essa tecnologia pode ser usada para uma infinidade de situações, desde registros de

transações bancárias até redes sociais de música, em que um artista é remunerado automaticamente quando um usuário escuta uma música sua. Satoshi Nakamoto propôs o Bitcoin como um sistema de dinheiro eletrônico ponto a ponto, mas não faltam aplicações além desse escopo, tanto é que há mais de mil criptoativos sendo negociados atualmente.

O blockchain é, portanto, uma plataforma que permite o desenvolvimento de qualquer aplicação que use uma planilha de registro. Sua segurança e versatilidade têm feito grandes inovações virem à tona e são capazes de alçar a economia global a um novo patamar nas próximas décadas.







## ALÉM DO DINHEIRO: O UNIVERSO DAS OUTRAS CRIPTOMOEDAS

O estádio de futebol Cícero Pompeu de Toledo, mais conhecido como Morumbi, é um local que já foi palco de diversas partidas importantes: final da Copa Libertadores da América, final do campeonato paulista e de outros clássicos, como São Paulo e Corinthians. Sua importância se deve também ao fato de ele ser o segundo estádio com maior capacidade do país, só perdendo para o Maracanã.

Além das partidas de futebol, o Cícero Pompeu recebe vários shows internacionais, de bandas como U2, Bon Jovi, Black Eyed Peas e muitas outras. No local, acontecem apresentações para todos os gostos musicais, mas esse não é meu ponto para o presente capítulo. Afinal, este livro fala sobre criptomoedas, e não sobre construções que abrigam partidas de futebol e megashows. E eu sequer torço para o São Paulo para ficar aqui falando sobre o estádio do time.

No entanto, o Morumbi tem tudo a ver com o que você viu no capítulo anterior e com o que vai ver neste. O estádio é a melhor analogia para o blockchain e as possibilidades que essa tecnologia abriu, que vão muito além do dinheiro digital, como o bitcoin. Basta olharmos para como tudo começou, com a primeira moeda totalmente digital, e compararmos com o projeto do estádio.

De forma bem resumida, o Cícero Pompeu de Toledo foi pensado para ser a casa do São Paulo Futebol Clube e abrigar os jogos do time. Mas, por ser tão bem estruturado e ter capacidade para mais de 70 mil pessoas, o estádio acabou se tornando também um espaço para apresentações de bandas e cantores que atraem multidões. Isso mostra que, apesar de o Morumbi ter sido construído com o propósito de abrigar partidas de futebol, posteriormente, outras possibilidades foram encontradas para o local, que não haviam sido previstas antes.

A semelhança com a história das criptomoedas e do blockchain é evidente. O bitcoin surgiu com a proposta de ser um dinheiro apenas digital, mas a tecnologia que o sustenta permite diversas aplicações. Lembra-se de que no capítulo anterior falamos sobre como a tecnologia do blockchain é disruptiva e, além de ser o livro razão do Bitcoin, abre muitas outras possibilidades?

Pois é exatamente isto que vamos ver agora, como a disruptão causada pelo blockchain criou uma classe de ativos totalmente nova, que vai muito além das criptomoedas. Esses ativos, ou criptoativos, representam toda a classe de investimentos que envolve criptocommodities (criptomercadorias), criptotokens e também as criptomoedas. Nas próximas linhas, trarei definições e exemplos para cada um desses nomes para que fique claro o que representam.

## CRIPTOATIVOS

Criptocommodities

Criptotokens

Criptomoedas

## **DEFININDO O QUE SÃO CRIPTOATIVOS, CRIPTOCOMMODITIES, CRIPTOTOKENS E CRIPTOMOEDAS**

Como a figura demonstra, criptoativo é um nome que engloba todas as outras três classes de ativos. Essa nomenclatura permite fazer referência a todos os ativos do universo cripto com uma única palavra, sem o perigo de errarmos a denominação. Na classificação dos seres vivos podemos nos referir aos animais e às plantas de uma maneira genérica, chamando-os simplesmente de “seres vivos”. Também podemos nos referir a cachorros, gatos e humanos chamando-os apenas de “animais”. Neste momento do livro, essa é a melhor analogia para a palavra “criptoativo”, pois ela tem a capacidade englobar todas as classes que existem e que vão existir no universo cripto. Da mesma forma, se novas espécies de animais forem catalogadas, ainda poderemos nos referir a elas como “animais”.

Agora, vamos deixar a biologia de lado e vamos mergulhar em cada uma dessas classes, trazendo suas definições e exemplos.

### **CRIPTOCOMMODITIES (CRIPTOMERCADORIAS)**

Essas novas nomenclaturas foram inspiradas em classificações já existentes no mercado financeiro. De forma bem simples, apenas foi acrescentado o prefixo cripto para fazer referência a esse novo universo que surgiu com o *white paper* de Satoshi Nakamoto. Por isso, para entender o que é uma criptocommodity, devemos buscar a definição do que seria uma commodity ou mercadoria. Essas palavras se referem a matérias-primas como carvão, óleo, trigo, leite, arroz. Todas elas são usadas na produção de bens industrializados, seja como fonte de energia ou submetidas ao beneficiamento até estarem prontas para o consumo.

Desse modo, as criptocommodities seriam matérias-primas, servindo como combustível ou sendo beneficiadas e então consumidas. No entanto, até o momento, o conceito de commodity é aplicado no universo cripto apenas como combustível. Assim como no mundo digital, as commodities são apenas alicerces que geram outros produtos. Por exemplo, imagine os recursos que temos hoje no meio digital, como internet banda larga, capacidade de armazenamento e poder de computação. Todos eles são commodities digitais, matérias-primas para gerar outros produtos, também digitais, os quais podemos chamar de produtos acabados. Esses produtos finais são os jogos digitais, redes sociais e outros programas de computador. Perceba também que, à medida que novos processos vão sendo descobertos, é possível fazer novos produtos com a mesma matéria-prima, como no caso do leite, que só pode ser matéria-prima para o queijo quando se entende o processo para essa transformação.

Da mesma forma, podemos ver isso acontecendo com as criptocommodities, que em um momento podem estar servindo de matéria-prima para alguma aplicação, mas em alguns anos servirão para outras funções, inimagináveis no momento anterior. Isso depende apenas da evolução das tecnologias que estão inseridas no universo dos criptoativos. Além disso, no mundo digital, as commodities são meios de troca para se obter o que de fato é desejado. Da mesma forma que, se alguém quiser fazer um queijo, precisará obter leite para produzir o bem final, se uma pessoa deseja criar um programa de computador, ela precisará obrigatoriamente escrever linhas de código em alguma linguagem de programação.

O Ethereum, cujo criptoativo ether possui o segundo maior valor de mercado, tem a proposta de ser uma plataforma na qual os pagamentos são feitos por criptocommodities. Na verdade, ele é mais bem definido como uma imensa plataforma descentralizada, capaz de executar inúmeras aplicações mediante o pagamento

em ether, sua commodity interna. Se ainda não ficou claro para você o que exatamente é o Ethereum, fique tranquilo, porque nas próximas linhas vamos apresentar uma analogia que deve fazer você entender como ele funciona.

## ETHEREUM: UMA APPLE SEM DONO

Em maio de 2017, a Apple foi a primeira empresa do mundo a ultrapassar US\$ 800 bilhões em valor de mercado. Isso se deveu à ótima qualidade de seus produtos, tanto do design quanto do poder dos softwares. A fama da empresa foi construída principalmente por iPhones e MacBooks. Se esses produtos fossem apenas bonitos, a Apple seria reconhecida somente pelo design; mas é seu sistema operacional que faz com que eles sejam muito admirados.

Tanto o iOS, sistema operacional do iPhone, quanto o macOS, sistema operacional do MacBook, são referências em softwares. É nesse ponto que quero focar por ora, pois podemos traçar um paralelo entre ele e a rede do Ethereum. Isso porque a Apple não criou todos os aplicativos que funcionam no iPhone. O iOS é apenas uma plataforma na qual os desenvolvedores criam aplicações, utilizando os recursos fornecidos com um determinado objetivo.

Além dos recursos de programação que o iOS oferece, os dados coletados por sensores do iPhone também podem ser usados em determinadas aplicações. Por exemplo, o GPS do iPhone pode ser usado para saber a localização do usuário e, a partir dessa informação, sugerir um restaurante próximo que seja do interesse da pessoa. Essa tomada de decisão sobre a sugestão a ser dada é feita por um algoritmo que avalia os gostos do usuário, fornecidos previamente. Além disso, o aplicativo analisa quais estabelecimentos mais próximos podem ser uma boa sugestão e envia uma notificação ao celular com uma proposta.

Nesse processo simplificado, o iOS, o GPS e o poder de processamento do iPhone formam, em conjunto, uma plataforma que possibilita que o aplicativo de sugestão de restaurantes funcione. Mas perceba que a empresa que desenvolveu o aplicativo não precisou criar um celular do zero ou um sistema operacional como o iOS para poder sugerir um restaurante para o usuário. Ela apenas usou recursos já disponíveis, assim como qualquer outro aplicativo pode usar. Para o aplicativo ficar disponível na App Store, a empresa paga uma taxa para a Apple. Desse modo, ela pode usar a plataforma e ter acesso a recursos que se encontram no iPhone.

Da mesma forma que essa cadeia funciona na plataforma disponibilizada pela Apple, o Ethereum pretende funcionar para toda e qualquer aplicação. Mas com um diferencial: não é a Ethereum Foundation, empresa que criou o Ethereum, que recebe todos os pagamentos pelas aplicações ou detém todo o poder que a plataforma ambiciona. Na verdade, como a proposta do Ethereum é ser descentralizada, qualquer um pode ser remunerado por emprestar poder computacional à rede.

A ideia é bem simples e permite que qualquer pessoa faça parte da rede como um prestador de serviço ou como um usuário. Por exemplo, imagine que alguém possua uma planilha de Excel com diversas fórmulas, milhares de linhas e colunas e que exija um processamento de dados que o computador da pessoa não suporte. Consequentemente, todas as vezes que a planilha tenta executar uma fórmula, o computador trava e tem que ser reiniciado.

Uma primeira solução seria comprar um computador com maior capacidade de processamento. Mas se a pessoa pretende executar a aplicação poucas vezes, seria extremamente custoso comprar uma máquina apenas para um uso pontual. Esse é um dos tipos de problema que a rede Ethereum poderá resolver quando estiver funcionando plenamente. Nesse caso, a pessoa poderia usar o poder computacional de outros computadores espalhados

pelo mundo para processar as contas da planilha mediante um pagamento em ether.

Poderia acontecer também o caminho inverso, a pessoa que desejasse receber pagamentos pelo uso do poder de processamento de seu computador poderia emprestar sua máquina para aplicações de outros usuários da rede. Esse seria um processamento *on-demand*, em que não é preciso ter o ativo físico para usá-lo, bastando apenas acessá-lo quando for necessário mediante um pagamento.

Mas esse conceito não é algo que o Ethereum trouxe. Ele já existe há algum tempo e tem se estendido cada vez mais a outros mercados. Empresas como Airbnb e Uber já entenderam que é possível fazer o compartilhamento de recursos, e da mesma forma você pode ser um consumidor ou um prestador de serviços.

Por enquanto, a rede não chegou ao ponto de funcionar para aplicações como a que citei acima. Apenas os *smart contracts* foram implantados com sucesso e, mesmo assim, já provocaram uma disruptão no meio. Esses contratos inteligentes permitem fazer contratos entre duas partes, por meio de programação, sem a necessidade de haver um intermediário para garantir que o dispositivo seja executado. Na verdade, a programação consiste em uma série de condições que autorizam ou não a realização de algo.

Talvez pareça um pouco abstrato, mas você pode entender o contrato como uma aposta em que uma pessoa não confia na outra. Seria necessário existir um intermediário que ficasse com o dinheiro das duas pessoas e, a depender do resultado, passasse o valor para uma das partes. Ou seja, existiria alguém apenas para decidir quem foi o ganhador. Mas, se a aposta fosse feita por meio de um *smart contract*, a decisão seria tomada por uma série de condições criadas digitalmente, por meio de um programa de computador, sem a necessidade de um indivíduo para validar a aposta e o prêmio.

Apesar de um *smart contract* poder ser usado dessa forma, o emprego que tem chamado mais atenção, e que também tem sido o mais comum, é outro. Por meio das estruturas de contratos inteligentes, é possível criar tokens que são entregues aos usuários mediante pagamento em ether.

De maneira bem resumida, essa funcionalidade da rede Ethereum permite que uma pessoa crie criptotokens, entregues em troca de alguma contribuição em ether. Isso é possível graças à estrutura dos contratos inteligentes, que possibilitam a execução de uma tarefa de troca sem intervenção humana. E é nesse ponto que chegamos à segunda designação dentro de criptoativos: os criptotokens.

## CRIPTOTOKENS

Para apresentar o que é criptocommodity, recorri à comparação com uma commodity de fato. Quero proceder da mesma forma com a explicação do que é um criptotoken. No entanto, a definição de token é de certa maneira mais ampla, e pode envolver desde um símbolo ou representação até um dispositivo de segurança. Portanto, precisamos do conceito que vai nos levar a entender o que são criptotokens.

Devemos recorrer ao significado mais antigo de um token, que é basicamente o de uma ficha que representa alguma quantia em dinheiro. Sim, tão simples quanto uma ficha de uma quermesse, que você compra com dinheiro para poder adquirir os produtos vendidos nas barracas. Esse exemplo se encaixa muito bem no nosso contexto, pois os criptotokens podem servir como fichas que só são aceitas em determinados lugares, assim como ocorre com as fichas de uma quermesse. Como você deve saber, uma ficha da

quermesse de uma paróquia não vale na outra, e vice-versa. Um criptotoken pode funcionar da mesma forma, só valendo como meio de troca no seu próprio ecossistema.

Ainda podemos usar o exemplo da quermesse para entender como esse modelo de criptoativo funciona. Basta imaginar que você queira realizar uma quermesse e não tenha os recursos para comprar os alimentos, montar as barracas e contratar pessoas. A solução mais fácil e mais usual é pedir doações, tanto de materiais quanto de mão de obra. Mas há uma alternativa para isso: vender previamente as fichas. Dessa maneira, você conseguiria o dinheiro para realizar a quermesse sem precisar pedir ajuda. As pessoas ajudariam a fazer o evento não por meio de doações, mas comprando aquilo que já comprariam quando as barracas estivessem de pé.

Você poderia fazer até melhor. Uma outra forma de atrair as pessoas seria oferecer um desconto no valor das fichas para quem as comprasse antes da quermesse estar garantida. Esse modelo seria muito justo e as pessoas se sentiriam incentivadas a comprar antes. Você poderia dar um desconto de 10%, de modo que quem comprasse dez fichas pagasse apenas nove e tivesse uma vantagem frente a quem deixasse para comprar apenas quando o evento estivesse acontecendo.

Essa é uma das formas de funcionamento do criptotoken, como ficha, em que ele representa uma quantidade de dinheiro, mas é usado apenas dentro de um ecossistema. No entanto, a venda dos criptotokens não ocorre como no exemplo da quermesse, de modo presencial e com fichas de verdade. Em primeiro lugar, porque estamos falando de um ativo essencialmente digital; em segundo, porque não seria escalável vendê-los como se faz com fichas.

A solução, nesse caso, é aplicar o conceito de contratos inteligentes para que a troca entre dinheiro e token seja feita de maneira digital e sem necessitar de uma terceira parte que garanta a

execução da operação. Por isso, a maioria dos criptotokens é criada utilizando o blockchain do Ethereum, o que dispensa a criação de uma plataforma do zero.

Esse tipo de criptotoken é conhecido também como utility token e tem a função de servir como dinheiro dentro de um ecossistema, como no caso da ficha que não teria valor fora do local. Mas as possibilidades para os tokens digitais não se esgotam no utility token. Outro modelo também muito usado é o equity token.

Para entender essa modalidade, mudaremos um pouco o exemplo da quermesse. Agora você não vai vender fichas que serão usadas para comprar alimentos quando o evento estiver acontecendo. No novo exemplo, você venderá tokens que dão direito aos lucros quando o dia acabar. Isso significa que, em vez das fichas representarem dinheiro, elas representam parte da quermesse. Os compradores dos tokens terão direito de colher os lucros do evento com você, como se fossem sócios. Seria o mesmo que vender partes de uma empresa para pessoas que, quando os lucros fossem atingidos, teriam direito a uma parte proporcional ao quanto contribuíram.

Esse modelo se assemelha muito ao que acontece já na Bolsa de Valores quando uma empresa faz um IPO (*Initial Public Offering* ou Oferta Pública Inicial) e capta recursos de investidores de todos os tipos, que passam a ser seus sócios. Por essa semelhança com o mercado tradicional, esse modelo tem sido alvo de críticas por parte dos reguladores no mundo todo e, por isso, ainda não está claro se o mercado aceitará a modalidade como legítima.

Além dos criptotokens, existe a última modalidade de criptoativos, que é a mais conhecida e, por esse motivo, é um dos focos principais do livro. Quando o bitcoin surgiu, visava ser uma moeda mundial que não dependesse de governos ou bancos. Com objetivos semelhantes, surgiram outras criptomoedas, que trouxeram inovações e diferenciais, o que as torna complementares ao bitcoin ou até capazes de substituí-lo um dia.

## **CRİPTOMOEDAS**

Para mantermos a linha mestra das definições que nos acompanharam até aqui, precisamos de algumas sentenças para definir o que é uma criptomoeda antes de continuarmos a última parte do capítulo. Acredito que você já deva estar habituado com o conceito de moeda e, mesmo que não esteja, consegue entender intuitivamente para que uma moeda serve. Ela é essencialmente um meio que facilita a troca de bens entre pessoas. As criptomoedas se propõem a fazer o mesmo, só que de forma digital.

Apesar de o conceito de criptomoeda estar mais claro hoje para as pessoas que conhecem o bitcoin, Satoshi Nakamoto não deve ter tido a real noção da disruptão que estava causando no mundo. Os primeiros criptógrafos que tiveram acesso a seu *white paper* elogiaram a iniciativa e disseram que aquilo poderia dar certo. Como todo o conteúdo tecnológico era de código aberto, qualquer um poderia criar uma cópia do bitcoin e chamar de outro nome.

Várias dessas tentativas não foram para a frente porque não traziam nenhum diferencial como criptomoedas, mas as que trouxeram foram ganhando destaque e notoriedade na comunidade. Um exemplo é o litecoin, que usa o mesmo código que o bitcoin, mas traz inovações que apontam para um futuro promissor.

### **Litecoin**

O litecoin foi criado em 2011 por Charlie Lee, ex-funcionário da Google. Ele foi responsável por diversas contribuições técnicas ao protocolo do bitcoin, e, desde então, sua reputação cresceu na comunidade de criptógrafos. Por ter construído uma imagem de quem consegue aglutinar diversos interesses da comunidade, já se suspeitou que Lee fosse Satoshi Nakamoto, mas ele nega ser o criador do bitcoin.

Já quando o assunto é litecoin, podemos considerá-lo como o dono, o que traz uma característica interessante de liderança que o bitcoin não possui. Foi com essa influência que Lee conseguiu implementar diversas melhorias no código, que fizeram com que o litecoin ganhasse espaço e valor de mercado. Além disso, a proposta da criptomoeda é ser complementar àquela criada por Satoshi e servir como uma rede de pagamentos mais eficientes, mas com três diferenças principais:

- A rede do litecoin pretende processar blocos quatro vezes mais rápido do que a rede do bitcoin, que os processa a cada dez minutos;
- Enquanto o bitcoin tem emissão máxima de 21 milhões de unidades, serão produzidos até 84 milhões de litecoins, o que torna a moeda menos escassa;
- A mineração de litecoin é mais barata e, portanto, mais acessível, já que utiliza o método *scrypt* em seu algoritmo.

Devido a essas características, o litecoin é visto como uma rede complementar. Da mesma maneira que algumas pessoas gostam de afirmar que o bitcoin é o ouro digital, o projeto de Charlie Lee pode facilmente ser considerado a prata digital, por ser menos escasso e por ter uma mineração mais barata.

Assim como o litecoin pretende ser melhor do que o bitcoin em alguns quesitos, outras criptomoedas propõem-se a resolver outros tipos de problemas, como o do anonimato completo. Afinal, em seu artigo original, Nakamoto dedica toda uma seção à discussão do anonimato que as transações com bitcoin proporcionam.

No entanto, o entendimento que se tem hoje sobre o blockchain mostra que as transações são “pseudoanônimas”. Digo isso com base no fato de que elas são abertas para que qualquer um possa ver de qual endereço partiu e valor e para qual foi. Apenas com o endereço, não é possível saber quem está envolvido, mas, sabendo quem é seu dono, é possível rastrear por onde o dinheiro está circulando.

De certa forma, isso é bom, porque evita que o bitcoin seja usado facilmente para a lavagem de dinheiro, mas incomoda algumas pessoas da comunidade cripto que acreditam que o anonimato completo tenha que ser uma opção. Foi pensando nessas pessoas que não apenas uma, mas três moedas digitais foram criadas com o intuito de ter esse tipo de característica.

### **A batalha pelo anonimato: dash, monero e zcash**

Essas três criptomoedas nasceram com a intenção de serem meios de pagamento como o bitcoin, mas, ao contrário de seu predecessor, elas se propuseram a fazer transações totalmente anônimas.

Criada por Evan Duffield, a Dash foi lançada inicialmente como Darkcoin, mas, como você pode imaginar, com esse nome ela só atraia a atenção do mercado negro, da *deep web* e afins. Então, buscando se posicionar de uma forma menos negativa, a Darkcoin passou por um *rebranding* e passou a se chamar Digital Cash ou Dash.

Para atrair os mineradores no início, 1,9 milhão de dash foram mineradas nas primeiras 24 horas. Se compararmos com o suprimento atual total, o incentivo para quem minerou dash nas primeiras horas foi substancial, considerando os preços de hoje. Isso mostra uma visão de Duffield para atrair mineradores logo de início e começar a gerar efeito de rede, que é tão necessário nesse ecossistema.

Depois do passado sombrio como Darkcoin, a Dash passou a se posicionar como um meio de pagamento, o Digital Cash. A empresa por trás da criptomoeda pretende ter um sistema tão eficiente e rápido quanto uma transação com cartão de crédito. Quanto à questão do anonimato, a equipe realinhou seu objetivo de longo prazo e passou a considerá-la uma característica essencial para o projeto nos próximos anos, mas não mais aquilo que a define.

Foi conversando com um dos integrantes do time que consegui extrair essa visão de que o anonimato faz parte da solução de pagamento, mas não é a principal característica. Afinal, para quem se propõe a ser um meio de pagamento tão rápido quanto o cartão de crédito, velocidade é primordial e anonimato é necessário. Ninguém quer as informações de suas transações expostas a qualquer um.

Outra criptomoeda que surgiu no mesmo ano que a dash, a monero, nasceu como a moeda da *deep web*, e pretende continuar sendo. Em 8 de abril de 2014, uma postagem no bitcointalk.org falava sobre uma nova moeda, chamada bitmonero, que usava o CryptoNote e tinha uma política mais justa de distribuição se comparada com a sua predecessora, a bytecoin. Essa criptomoeda introduziu o conceito de CryptoNote, que hoje é uma das principais características da monero. Ela deu origem a bitmonero e cometeu o erro de ir ao mercado apenas quando estava quase completamente minerada. Em torno de 80% de todas as bytecoins já estavam nas mãos de algumas pessoas quando o mercado ficou sabendo da existência da moeda.

Como mencionei com relação à dash, o sucesso de um criptoativo depende da criação de um efeito de rede, algo que a predecessora da monero não conseguiu fazer, porque não privilegiou novos entrantes com o incentivo à mineração.

O CryptoNote é a principal inovação da monero e, em linhas gerais, ela mantém o total anonimato de quem transfere valores por meio da sua rede. Diferentemente da tecnologia do bitcoin, que oferece apenas anonimato parcial, com o CryptoNote, nenhuma transação é rastreável.

Por último, temos a mais recente de todas as criptomoedas, que tem a equipe de criptógrafos mais respeitada pela comunidade: o zcash.

A moeda foi criada em outubro de 2016 por Zooko Wilcox, e utiliza como mecanismo de validação das transações a tecnologia zk-SNARK, sigla para “zero-knowledge Succinct Non-Interactive Argument of Knowledge”. Graças às normas matemáticas aplicadas pelas zk-SNARKs, o blockchain da zcash é capaz de manter um livro contábil de saldos seguro que não revela a nenhum outro usuário o saldo dos endereços.

O minerador que processa as transações é capaz de validar os blocos sem revelar nenhuma informação dos envolvidos. A validação se dá por meio de parâmetros públicos gerados pelo protocolo. Esses parâmetros são números com uma estrutura criptográfica muito específica, conhecida por todas as partes envolvidas no sistema.

Na rede do zcash, os participantes asseguram as transações, com vários agentes gerando “fragmentos” do par de chaves pública/privada. Depois, cada participante destrói seu fragmento da chave privada, criando uma espécie de “lixo criptográfico”. A partir da “reciclagem” desses fragmentos, os agentes reconstituem a chave pública, estabelecendo o parâmetro público de validação para a transação.

Pode parecer complicado, mas é o que garante ao zcash características únicas de anonimato. Isso chamou a atenção de Edward Snowden, ex-agente da NSA, que afirmou que essa criptomoeda é a mais avançada tecnicamente e a única com uma equipe de criptografia com profissionais experientes.

É exatamente de uma boa equipe que um projeto que envolve criptoativos precisa para dar certo, já que as ideias e conceitos iniciais mudam ao longo do amadurecimento, tanto da equipe quanto do ecossistema. Por isso, o comum é vermos milhares de criptoativos surgindo, mas apenas uma pequena parcela dando certo. Nem todas as equipes são boas e capazes de levar o projeto a ser o que se propõe.

Com isso, chegamos ao fim deste capítulo, que começou falando do Morumbi e terminou com a mais alta tecnologia de transações criptografadas. Depois de tantas teorias e analogias sobre o tema, podemos prosseguir para a parte mais prática do assunto. Afinal, é muito bom entender todos esses ativos, mas, se não soubermos como adquiri-los, o valor gerado por eles vai sempre ficar com outro e todas essas informações servirão apenas para conversas de bar.

Portanto, dedicamos o próximo capítulo a explicar como comprar suas primeiras criptomoedas. E, no capítulo 8, falaremos um pouco sobre nossas estratégias para selecionar os melhores criptoativos, aqueles com maior potencial de valorização.







É

# GUIA PRÁTICO PARA INVESTIR EM CRIPTOMOEDAS

## *PARTE 1 – COMO COMPRAR*

A esta altura do livro você deve entender que as criptomoedas representam uma revolução para a nossa sociedade. As possibilidades que suas transações totalmente seguras e rápidas abrem são muitas e vão além daquilo que podemos imaginar agora. Assim como no início da internet você não poderia imaginar uma empresa como a Google ou o Facebook, na era das criptomoedas não é possível prever quais serão as grandes empresas que se erguerão por meio dessa tecnologia.

Outra revolução passa pelo blockchain, pois a partir dele teremos outras disruptões sendo criadas, que também não podem ser imaginadas hoje ainda. Por isso, considero este um período

similar ao de 1994, quando surgiu a internet. No entanto, se no começo da internet a maioria das pessoas não podia aproveitar para lucrar com aquele mercado, quando o assunto é criptoativos, isso já é possível.

Digo isso porque, no início da internet, tirar proveito como investidor só era possível se você tivesse muito dinheiro para apostar em uma dúzia de startups promissoras. Mas quando o assunto é aproveitar o novo universo de criptoativos, a questão é bem mais simples. Não é necessário ter tanto dinheiro quanto para investir em startups. Basta que você tenha conta em corretoras especializadas em criptoativos para poder comprar diversos deles. A proposta deste capítulo é exatamente mostrar como é simples começar a investir.

De forma bem resumida, se você nunca comprou nenhum criptoativo, o fluxo para realizar a sua primeira compra no Brasil envolve os seguintes passos: abrir conta em uma exchange (corretora especializada em criptoativos); enviar documentação para validar a conta; depositar algum dinheiro na sua conta na exchange; criar uma ordem de compra de bitcoins e esperar a ordem ser atendida por outra parte que esteja vendendo. Assim que a operação for executada, você verá seu saldo em bitcoins na exchange.

Esse fluxo serve para você comprar alguns poucos criptoativos negociados no Brasil, como litecoin, bitcoin, ethereum e bcash. Para adquirir outros, é necessário ter conta em exchanges com um portfólio maior de ativos. No Brasil, as principais dão suporte a poucas criptomoedas e criptocommodities. Por isso, para conseguir comprar os demais ativos, você precisará abrir conta em corretoras estrangeiras.

No entanto, por estarmos falando de itens digitais, não é necessário que você tenha conta em um banco no exterior para mandar recursos para fora do país e depois depositar na exchange estrangeira. Basta transferir bitcoins ou qualquer outro ativo digital

para sua conta na corretora estrangeira e você já estará apto para negociar outros criptoativos. Esse é um resumo do processo de como comprar mais do que um criptoativo. A seguir, detalharemos para você cada um dos passos citados acima e, ao final, faremos nossas considerações sobre armazenamento com segurança.

## PASSO A PASSO PARA ABRIR CONTA EM UMA CORRETORA

Como já foi mencionado, as corretoras de bitcoins e outros ativos digitais relacionados são conhecidas como exchanges, um nome que veio de fora e se tornou usual. Optamos por nos referir a essas corretoras especializadas tanto com o nome em inglês quanto com o nome em português por acreditarmos que as duas formas sejam amplamente usadas no país.

O primeiro passo para ter conta em uma exchange é realizar um registro na plataforma. No Brasil, temos duas principais corretoras: o Mercado Bitcoin e a Foxbit. São elas que operam os principais volumes. O fluxo é bem parecido para ambas, como descrito abaixo:

1. Entre na página *mercadobitcoin.com.br* ou *foxbit.com.br*;
2. Coloque e-mail e CPF válido e escolha uma senha para sua conta. Um link de confirmação será enviado para a caixa de entrada do seu e-mail;
3. Clique no link para validar sua conta;
4. Entre na página da exchange para preencher o cadastro. Neste passo, a depender da corretora, será necessário preencher dados como CPF, RG e endereço, além de criar uma senha interna para validar compras e vendas na plataforma. Será necessário também enviar fotos de documentos e uma foto do seu rosto. Este é o momento em que a empresa precisa colher

o máximo de informações sobre você, para cumprir duas regras muito comuns no mercado financeiro, o KYC (Know Your Client) e o AML (Anti Money Laundering), que visa evitar problemas como a lavagem de dinheiro;

5. Depois de completado o passo acima, é necessário esperar pela aprovação dos seus documentos. Dependendo da exchange, já será possível fazer depósitos em dinheiro para comprar seus primeiros ativos digitais. Mas é preciso consultar as políticas de compra da empresa;

6. Depois da aprovação, você já pode depositar na conta da corretora para comprar dentro da plataforma. Nesta etapa existem diferenças entre as empresas também. Algumas pedem que você envie uma foto sua ao lado de uma placa em que esteja escrito “quero comprar bitcoins”. Pode parecer estranho, a princípio, mas a medida evita que uma outra pessoa compre em seu nome. Não se assuste caso algum pedido nesses moldes seja feito a você. Além disso, pode ser que as corretoras cobrem uma taxa para você efetuar depósitos. Então, fique atento.

Depois de finalizar a criação da sua conta na exchange, é hora de comprar os primeiros bitcoins. Lembre-se de que você precisa ter saldo em reais na corretora para realizar a compra. Mas, antes de entrar nessa questão, vamos lembrar como é formado o preço do bitcoin. Não temos um preço único, nem mesmo no Brasil. Cada corretora forma o preço de acordo com o valor da última transação realizada dentro da sua plataforma, e essas empresas não são integradas entre si. Existem esforços para realizar essa integração e acreditamos que isso vai acontecer em breve, tanto local como mundialmente.

Por enquanto, o preço do bitcoin dentro das plataformas funciona da seguinte maneira: de um lado, existem compradores tentando comprar pelo preço mais baixo possível, de outro,

vendedores tentando vender pelo preço mais alto possível. Quando há pelo menos um comprador e um vendedor que entram em acordo sobre o preço, uma transação é realizada e o preço do bitcoin é dado. Como não existe integração entre as corretoras, o livro com as ordens de compra e venda é único para cada plataforma. Isso significa que uma ordem de compra ou venda dentro da plataforma de uma corretora não pode ser atendida por um vendedor em outra.

Existem dois modelos de ordem compra: **a mercado** ou **a preço escolhido**.

Quando a ordem é a mercado, ela é executada imediatamente, desde de que haja pelo menos um vendedor disponível. Nesse modelo de ordem, a transação é executada com o menor preço possível no momento, o que corresponde a realizar a compra com o preço mais baixo que foi postado no livro de vendas. Para a ordem de venda, a lógica é a mesma, mas a ordem é executada no maior valor possível. Como mencionamos, o vendedor quer vender pelo maior preço, enquanto o comprador quer comprar pelo menor preço.

COMPRA			VENDA			Acumulado	Taxas
Comprador	Quantidade	Preço	Preço	Quantidade	Vendedor		
Pavo_901037	฿ 0,26316454	R\$ 36.499,99	R\$ 36.500,00	฿ 0,32373122	Bull_901516		
Sapo_903154	฿ 0,02741692	R\$ 36.473,82	R\$ 36.899,99	฿ 0,27548208	Pulpo_901439		
Zebra_900185	฿ 0,22200000	R\$ 36.425,00	R\$ 36.900,00	฿ 0,00136270	Puma_899874		
Drac_901588	฿ 0,00041184	R\$ 36.421,08	R\$ 36.999,98	฿ 0,02728867	Bison_901700		
Hyena_899013	฿ 0,01479667	R\$ 36.402,02	R\$ 37.000,00	฿ 0,02000000	Ostra_899869		
Raven_901636	฿ 0,01373550	R\$ 36.402,01	R\$ 37100,00	฿ 0,00269541	Pombo_902138		
Puma_899874	฿ 0,00137362	R\$ 36.400,00	R\$ 37100,00	฿ 0,11491831	Gato_901932		
Hippo_901165	฿ 0,01373626	R\$ 36.400,00	R\$ 37101,00	฿ 0,02000000	Ostra_899869		
Owl_902652	฿ 0,00110000	R\$ 36.400,00	R\$ 37199,99	฿ 0,11491830	Viper_900222		
Drac_901588	฿ 0,00033029	R\$ 36.331,08	R\$ 37.300,01	฿ 0,00392825	Puma_899874		
Gos_899014	฿ 0,26955007	R\$ 36.330,01	R\$ 37.500,00	฿ 0,00690494	Peru_902713		
Whale_901385	฿ 0,02738783	R\$ 36.330,00	R\$ 37.500,00	฿ 0,00056524	Orca_900594		
Wal_901141	฿ 0,30784992	R\$ 36.315,00	R\$ 37.500,00	฿ 0,01335538	Bull_901744		
Pavo_900977	฿ 0,01100000	R\$ 36.305,00	R\$ 37.650,00	฿ 0,00146082	Orca_900594		
Galo_901823	฿ 0,05509186	R\$ 36.303,00	R\$ 37.670,00	฿ 0,00039819	Swan_901865		
Orca_902253	฿ 0,00646000	R\$ 36.302,50	R\$ 37799,00	฿ 0,07936717	Llop_900981		

Extraído de Foxbit | <https://foxbit.com.br/>

## Ordens de Compra

QUANTIDADE	PREÇO (R\$)
0,91575	36901,00000
0,10955	36900,00000
0,17730	36850,00000
0,02700	36801,00000
0,01469	36800,00000
0,01000	36799,67000
0,08477	36790,00000
0,00913	36780,00000
0,02764	36714,00001
0,00395	36714,00000
0,50000	36701,00000
0,05799	36700,00000
0,01500	36651,35000
0,01250	36650,00000
0,11605	36600,00000
0,01277	36599,99999
0,00136	36550,01000
0,17169	36550,00000
0,00100	36505,00000

## Ordens de Venda

QUANTIDADE	PREÇO (R\$)
0,06614	36999,99999
3,58781	37000,00000
0,02725	37088,01000
0,06000	37100,00000
0,00500	37190,00000
0,01971	37249,93000
0,04985	37249,94000
0,00500	37287,99000
0,00550	37288,00000
0,09367	37299,00000
0,00963	37399,99000
0,22807	37399,99998
0,00620	37400,00000
0,06979	37495,00000
0,05233	37498,00000
0,03247	37499,00000
1,30845	37500,00000
0,00899	37690,00000
0,01161	37699,90000

Extraído de Mercado Bitcoin | <https://www.mercadobitcoin.com.br/>

Diferentemente do que ocorre na ordem a mercado, no segundo modelo, a preço escolhido, é possível escolher o preço. Nesse modelo, você escolhe o quanto quer pagar por unidade do ativo e sua ordem só é executada se aparecer um vendedor oferecendo

pelo preço que você colocou. De forma bem didática, na compra a mercado, é como se você estivesse em uma feira livre decidido a comprar um maço de alface e só estivesse procurando o preço mais baixo para realizar a compra. No caso da ordem a preço fixo, você decidiu comprar alface, mas só se estiver com o preço exato que você estabeleceu previamente.

Diferentemente do exemplo da alface, para fazer a compra dos bitcoins, é necessário pagar taxas para as corretoras, e elas são bem salgadas. Todas as corretoras cobram taxas percentuais sobre as ordens de compra e de venda. As taxas variam, mas ficam em torno de 0,5% dependendo do tipo de ordem. Por exemplo, em algumas corretoras, para incentivar que exista um grande volume de ordens postadas, tanto de compra como de venda, taxas menores são cobradas de quem põe a ordem. Já para quem atende a ordem, o executor, as taxas são maiores. Isso incentiva as pessoas a postarem suas ordens, e não a aceitar uma que já foi postada. Dessa forma, o mercado dentro da corretora ganha muita liquidez, por possuir várias ordens abertas. Além desse modelo de taxa, existem os que não fazem distinção entre quem coloca a ordem e quem a atende. Nesse caso, as corretoras cobram, em média, 0,5% de quem posta a ordem e o mesmo valor do executor.

De todo modo, acreditamos que as taxas são muito altas e devem, em um futuro próximo, ser convertidas em valores fixos, ou em valores máximos, caso as cobranças continuem sendo percentuais. As corretoras tradicionais também trabalhavam, inicialmente, com taxa percentual, mas, à medida que foram surgindo novos concorrentes, esse modelo foi mudando para a corretagem a preço fixo. Então, estabeleceu-se um novo padrão, nas grandes corretoras, de cobrança de um valor fixo por ordem, tanto de quem posta a ordem quanto de quem a executa. O mercado de criptomoedas deve seguir o mesmo caminho. O investidor só tem a ganhar com esse movimento em direção ao que as grandes corretoras já fazem no mercado tradicional.

Voltando ao nosso fluxo de compra, depois de adquirir os seus primeiros bitcoins, talvez você ache que o processo não é complicado e decida comprar outros criptoativos. No entanto, o processo de compra que descrevemos é válido apenas para as exchanges brasileiras, que negociam pouquíssimas variedades de ativos.

Para ter acesso a uma gama maior de criptoativos, será necessário abrir conta em uma corretora estrangeira. O processo é semelhante ao feito no Brasil, com a diferença de que você não precisa ter uma conta-corrente em um banco estrangeiro para transferir recursos para a corretora, pois tudo é feito por meio de criptoativos.

Agora, vamos ao passo a passo para abrir uma conta em exchange estrangeira:

1. Entre na página da corretora estrangeira. Existem milhares delas — Bittrex, Kraken e Coinbase são alguns exemplos —, por isso, é interessante buscar informações sobre a segurança de cada uma. Como não existe custo para abrir uma conta, é aconselhável que você tenha conta em mais de uma;
2. Crie uma conta com e-mail válido e escolha uma senha de acesso. Um link para confirmação do cadastro será enviado para o seu e-mail;
3. Entre no seu e-mail e clique no link para validar sua conta;
4. Entre na sua conta e busque por “wallet” para encontrar sua carteira com o saldo e também o endereço para o qual você enviará seus bitcoins.

Ao encontrar sua carteira de bitcoins, procure algum indicativo de depósito e, então, será fornecido um endereço para o qual você enviará os seus bitcoins. Esse endereço é uma sequência de caracteres no seguinte formato: `1BXbUcNf9wDvobx7wCF6cTQNonLMYLtjhA`. Basta copiar o endereço e colar no local indicado na sua corretora para enviar seus ativos digitais.

Após enviar seu saldo para a exchange estrangeira, é hora de comprar. Nesse quesito, cada plataforma é diferente, portanto, nosso conselho para quem está começando é não comprar grandes quantias em plataformas com as quais não tenha familiaridade. A forma ideal de começar é adquirir poucas quantias e ir se familiarizando com a plataforma, tanto com a parte operacional quanto com as taxas.

De modo geral, as exchanges estrangeiras funcionam de forma parecida com as brasileiras, ou seja, você pode colocar uma ordem a mercado ou a valor escolhido. A lógica é a mesma apresentada acima, com taxas cobradas de quem compra e de quem vende. A diferença é que, como o mercado estrangeiro é mais maduro do que o brasileiro, as taxas cobradas no exterior são menores e as plataformas têm mais liquidez, pois possuem um volume maior de negociação.

Esse é o caminho mais comum para quem deseja comprar criptoativos que não são negociados no país. Ao comprar esses ativos digitais, a maioria das pessoas os deixa em custódia da corretora. Isso, porém, apresenta um risco que às vezes é mal calculado. As exchanges sofrem ataques constantes de hackers, já que possuem um saldo grande em suas carteiras que as torna um alvo muito atraente. Por essa razão, não aconselhamos deixar grandes quantias em contas nas corretoras, nem estrangeiras, nem nacionais.

Pensamos que a maneira mais segura de armazenar os seus ativos digitais seja consigo mesmo. Mas o que é possível armazenar consigo mesmo são as chaves privadas que dão acesso ao blockchain com o saldo dos criptoativos. Não existe uma forma de guardar os ativos digitais de fato, apenas as chaves privadas, que são sequências de caracteres similares aos endereços de que falamos acima:  
`L1sq97KRQzf77tRJTsJqm2ByDvdEBpwoaPbaG1kVXpkJqWUGDKj8.`

Existem diversas formas de armazenar essas chaves, que variam em questão de segurança, usabilidade e praticidade. A maneira mais prática e com boa usabilidade é deixar em uma exchange. Contudo, nessa opção, a segurança não é das melhores, pelos motivos que apresentamos. Além disso, você não tem acesso a sua chave privada, e terceiriza essa função para a empresa.

## OUTRAS FORMAS DE ARMAZENAMENTO

O local onde se armazena as chaves privadas é conhecido como wallet ou carteira. Na verdade, seria mais preciso chamá-lo de chaveiro, já que ele permite o armazenamento de chaves privadas, e não de saldos de fato, como foi explicado no capítulo sobre o blockchain. Mas, por uma questão de simplicidade e entendimento de quem está iniciando, o mercado decidiu chamar esses locais de carteiras.

Existem diversos tipos de wallets para armazenar chaves privadas. As mais conhecidas são as software wallets, que são aplicativos em celulares, ou sites que se conectam com o blockchain. Existem milhares delas e como não é trivial uma carteira servir para vários criptoativos, existem carteiras específicas para cada um. Claro que também existem multi-wallets, que armazenam mais de um tipo de ativo digital, mas a maioria das carteiras digitais serve apenas para um ativo. No segmento multi-wallets, as mais conhecidas e utilizadas são a Jaxx e a Coinomi.

Em contraste com as software wallets, existem também as hardware wallets, que são basicamente dispositivos bem parecidos com pendrives, nos quais é possível armazenar suas chaves privadas. Os modelos de hardware para armazenamento mais conhecidos e usados são a Trezor e a Ledger.



Trezor e Ledger Nano S  
(imagens retiradas dos sites das empresas)

Esses dispositivos têm o tamanho de pendrives e são o modo mais seguro que temos para armazenar as chaves privadas. As duas hardwallets mais usadas são bem intuitivas, tanto na inicialização como na utilização. Ao conectá-las ao seu computador, as instruções que se seguem são as mesmas de qualquer programa. A grande diferença é que, no momento da inicialização, é mostrada uma sequência de 12 a 24 palavras, conhecida como *seed*, que você deve anotar em um papel e guardar. Essas palavras são capazes de gerar suas chaves privadas, no caso de você perder sua hardwallet ou de ela se danificar.

Essa recuperação só é possível porque uma wallet física não armazena o seu saldo, mas apenas a sequência de caracteres que permite a você o acesso ao blockchain, que é onde o saldo realmente se encontra. É essa sequência de caracteres que realmente importa, pois basta que você a tenha para ter acesso à sua conta. Por isso, algumas pessoas decidem anotar essa sequência de caracteres em um papel e com isso constituir o que chamamos de paper wallet.

Dessa forma, a chave privada fica anotada em uma folha de papel que pode ser deixada em um cofre, como uma cédula ou um

título ao portador, já que quem a possuir pode ter acesso ao seu saldo na carteira. Esse modo de armazenamento é o mais barato, pois requer apenas papel e caneta, mas também é a maneira mais sujeita a extravio. Afinal, se as pessoas perdem documentos, chaves de casa e cédulas de dinheiro, porque não perderiam um pedaço de papel?

Mesmo com o modo mais profissional de se fazer uma paper wallet, via [bitcoinpapewallet.com](http://bitcoinpapewallet.com), as chances de perda continuam as mesmas, já que a chave privada ficará armazenada apenas em um pedaço de papel. Por isso, consideramos a paper wallet um modelo de armazenagem problemático, tendo em vista o tipo de cuidado que demanda. Aliás, além desse problema, tem algo de paradoxal em armazenar um ativo essencialmente digital em uma folha de papel.

E se esse modelo não é à prova de erro humano, imagine armazenar a sua chave privada inteira na sua cabeça? É exatamente este o conceito por trás da brain wallet: guardar a sequência de caracteres na sua memória. Quem está há mais tempo no meio dos criptoativos defende que esse é o único meio de se proteger de hackers ou de roubo, mas com certeza não protege você do esquecimento. Guardar uma sequência de caracteres sem lógica beira o impossível e, por isso, existe uma alternativa mais “fácil” para a brain wallet. No caso mais acessível, as pessoas memorizam apenas as palavras que reconstroem a chave privada. Mas são de 12 a 24 palavras para memorizar, o que não confere trivialidade a nenhuma das alternativas. Dessa forma, acredito que ninguém deva recorrer a esse tipo de armazenagem de chaves. Até porque esse modo é o mais complicado e só é adotado por pessoas muito preocupadas em serem hackeadas ou por aqueles que gostam de exibir suas habilidades de memorização.

## O PARADOXO DA GAVETA DE MEIAS

Lembra quando falei sobre a questão paradoxal de armazenar algo totalmente digital em um pedaço de papel? Pois esse paradoxo percorre todo o mundo de criptoativos, basta relembrar para que toda essa inovação foi criada a princípio. Essa tecnologia foi desenvolvida para devolver às pessoas o controle do seu próprio dinheiro, em uma clara oposição ao controle exercido pelos bancos.

Perceba o rumo que isso toma: um ativo totalmente digital, com o qual se tem todo o controle do seu saldo e das chaves privadas, e ninguém mais precisa armazenar nada para você. Por outro lado, isso traz grandes responsabilidades, pois, agora, suas chaves precisam ser colocadas em um local seguro, do seu controle. E, por incrível que pareça, o que acontece, no fim das contas, é que uma quantidade de pessoas considerável anota suas chaves privadas ou suas palavras de reconstituição em um pedaço de papel que colocam em uma gaveta; muitas vezes, na gaveta de meias. Isso porque acreditam que a única forma de se proteger de hackers é deixando tudo offline, constituindo, assim, o paradoxo da gaveta de meias.

Esse é exatamente um dos problemas que os bancos resolveram no passado. Eles armazenavam os recursos das pessoas em segurança, para que elas não corressem o risco de ser furtadas por deixarem dinheiro em gavetas ou debaixo de colchões. Visualizando esse paradoxo, é possível que em um futuro próximo vão existir mecanismos ou empresas para evitar que as pessoas tenham que guardar suas chaves privadas consigo mesmas de modo tão arcaico quanto se fazia nos séculos passados com dinheiro em espécie. Mas, por enquanto, guardar as suas chaves privadas totalmente offline parece, de fato, ser a opção mais segura.

Depois de aprender como adquirir seus primeiros criptoativos e também como comprar qualquer ativo digital em outras corretores, o ideal é que você tenha uma boa estratégia de investimento. Do contrário, em vez de investidor, você será apenas um apostador. Por isso, reservamos o próximo capítulo para discutir a nossa estratégia na hora de selecionar outros criptoativos. Nas páginas que seguem, você entenderá como analisar os diferentes ativos por uma ótica que consideramos a mais consistente na hora de montar um portfólio de ativos digitais.





A faint, abstract network diagram consisting of several grey dots connected by thin grey lines, forming a complex web-like structure.

# GUIA PRÁTICO PARA INVESTIR EM CRIPTOMOEDAS

## *PARTE 2 – ESTRATÉGIAS DE INVESTIMENTO*

Alguns anos atrás, possuir criptomoedas era algo feito apenas por aficionados em tecnologia ou por pessoas de espírito muito libertário. De fato, essa nova classe de ativos surgiu com o advento do Bitcoin e, por vários anos, seu conhecimento ficou restrito a poucos *early adopters*, que acreditavam na proposta estabelecida por Satoshi Nakamoto. Na verdade, no início nem era possível chamar os detentores de moedas digitais de investidores. Eram mais entusiastas do blockchain e da descentralização que queriam participar daquela possível revolução do sistema financeiro. Hoje, percebemos que eles estavam certos e assistimos à consolidação

da iniciativa como uma nova classe de ativos que deve fazer parte de qualquer portfólio de investimentos diversificado.

Por mais que ainda haja muitas pessoas do mercado financeiro que considerem a compra de criptomoedas uma mera aposta, nós enxergamos isso como um investimento. É claro que existem vários riscos associados: a volatilidade tende a ser alta e sempre presente e pode ser que daqui a um tempo ninguém mais fale em bitcoin. Porém, essas características não se diferenciam em nada de outros tipos de investimento de alto risco, como é o caso enfrentado pelas startups. Um investidor-anjo, por exemplo, aporta capital em uma empresa nascente por enxergar seu potencial de desenvolvimento. Por mais que existam planos de negócio, muitas vezes, não existe caixa entrando e saindo de forma constante para que possamos realizar um modelo de fluxo de caixa descontado. Contudo, isso não é problema; é, na verdade, a alma do negócio. Um investidor-anjo analisa o potencial da startup de implementar com sucesso sua proposta e ganhar mercado nos anos que seguem. Se isso der certo, ganhos incalculáveis o esperam. Se der errado, a perda é limitada ao valor investido. Além disso, esse investidor não aporta capital em apenas uma empresa, mas sim em um conjunto variado, de forma a diversificar as possibilidades e mitigar maiores riscos de perda.

Com as criptomoedas, o processo funciona de forma similar. Escolhemos aquelas que vão fazer parte da nossa carteira, baseados na proposta tecnológica apresentada e no potencial de sucesso que podemos vislumbrar. Além disso, diversificar em mais de uma proposta ajuda a expor seu portfólio a diferentes possibilidades. Neste capítulo, vamos discutir mais a fundo como enxergamos o universo das criptomoedas e como nossa estratégia de investimento se desenvolve. Para isso, voltaremos aos mercados tradicionais.

Um investidor que busca retornos acima da média precisa adotar um método que seja igualmente acima da média. Uma das melhores formas de se fazer isso é por meio da montagem de uma

carteira diversificada de investimentos. Ao dar esse passo, você está assumindo graus de risco distintos, aportando seu dinheiro em ativos que possuem gatilhos e potenciais de valorização diferentes. O ponto central é que cada um deles carrega sua própria parcela de risco. Aliás, esse é o ponto inicial: entender que todo investimento possui risco, mesmo que seja um extremamente conservador.

Pense nos títulos do governo, que são considerados o tipo de investimento mais seguro do país. Ainda assim, existe o risco de o país se tornar incapaz de pagar sua dívida. Nesse caso, o governo poderia imprimir mais dinheiro para honrar os títulos, mas isso gera aumento da inflação e, consequentemente, seu dinheiro se desvaloriza. Por outro lado, pense agora no mercado de ações. O preço de uma ação está diretamente ligado ao sentimento que o mercado tem sobre aquela empresa. A avaliação tradicional se baseia na projeção de resultados futuros da companhia, que podem simplesmente não se concretizar. Uma ação ora está bem cotada, ora pode vir a zero. Se formos além, para o mercado imobiliário: está ligado a ativos físicos que são tradicionalmente geradores de renda para seus proprietários. Em um momento de crise, com menos indivíduos dispostos a alugar um determinado imóvel, o proprietário sofrerá com a vacância e passará alguns meses sem obter a renda passiva.

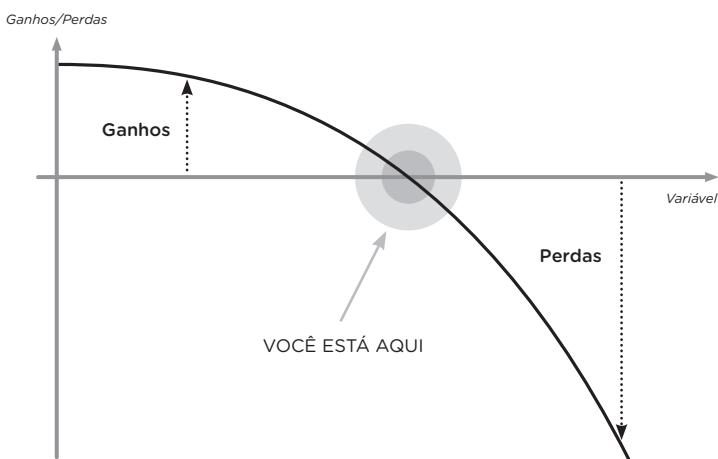
Ou seja, qualquer tipo de investimento carrega consigo uma parcela de risco. Alguns mais, outros menos. E cada risco contém um potencial de retorno associado. A questão central na hora de decidir pela inclusão (ou não) de um investimento na sua carteira passa pela seguinte pergunta: quão positivamente assimétrico ele é? Apesar de a expressão ser feia, significa nada mais que seu custo-benefício é interessante. Quando discutimos assimetria de um investimento, estamos olhando para qual é o tamanho da perda potencial versus qual é o ganho que pode ser obtido. Um investimento negativamente assimétrico é aquele cujo potencial

de retorno é limitado e o de perda é maior ou até ilimitado. Em contrapartida, um investimento positivamente assimétrico é aquele no qual as perdas são limitadas, mas os ganhos são potencialmente maiores ou ilimitados.

#### POSITIVAMENTE ASSIMÉTRICO



#### NEGATIVAMENTE ASSIMÉTRICO



Dados extraídos de TALEB, 2014.

No caso das criptomoedas, temos um investimento com enorme assimetria positiva. Dado que o máximo que se pode perder é o próprio valor investido e o potencial de ganho é praticamente infinito — não existe um limite preestabelecido de quanto uma criptomoeda pode valer —, esse é um jogo que definitivamente vale a pena jogar. Isso vai, também, em linha com o racional da *barbell strategy*, defendida por Nassim Taleb. Seu portfólio deve ter, de um lado, uma boa parcela em investimentos ultrasseguros, como títulos públicos e, de outro, um pouco de investimentos altamente arrojados. Não queremos apenas riscos medianos. Sendo assim, as criptomoedas e criptoativos são um elemento perfeito para compor a parte arriscada do seu portfólio. Seguindo o racional dessa estratégia, é prudente alocar uma fatia pequena nesse tipo de ativo, evitando passar dos 5% da sua carteira.

O jogo fica ainda mais interessante quando entendemos que as criptomoedas compõem uma classe totalmente nova de ativos. No artigo “*Bitcoin: Ringing the Bell for a New Asset Class*”<sup>1</sup>, Chris Burniske, da Ark Invest e Adam White, da Coinbase, defendem que o bitcoin capitanou o movimento de criação de uma nova classe de ativos. A discussão gira em torno de como as moedas digitais devem ser classificadas e, ao longo da publicação, fica claro que é necessário se criar uma nova definição para enquadrá-las no mercado financeiro.

Em linhas gerais, uma classe de ativos possui quatro peculiaridades próprias: investibilidade, características político-econômicas, independência de preço e perfil de risco-retorno. Se identificamos, de modo único, esses quatro itens para um grupo de ativos, podemos enquadrá-lo em uma nova classe. Para o estudo, o bitcoin foi usado como representante da classe de ativos criptográficos. O ponto mais interessante destacado pelos autores

---

1. BURNISKE, Chris e WHITE, Adam, *Bitcoin: Ringing the Bell for a New Asset Class*, [https://research.ark-invest.com/hubfs/\\_Download\\_Files\\_ARK-Invest/White\\_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf](https://research.ark-invest.com/hubfs/_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf) (acessado em 12 de janeiro de 2018).

é a baixa correlação da moeda com os representantes das outras classes de ativos. De forma simplificada, o coeficiente de correção é um coeficiente que indica a relação entre a movimentação dos preços de dois ativos. Esse valor varia entre -1 e 1. Se for igual a -1, isso significa que sempre que um ativo sobe, o outro cai, enquanto 1 significa que ambos os ativos sempre andam na mesma direção. Se um sobe, o outro também sobe, e vice-versa. Um coeficiente de correlação igual a 0 indica que os ativos não dependem linearmente um do outro.

No estudo de Burniske e White, o bitcoin foi comparado com ativos tradicionais, sendo eles S&P 500, títulos do tesouro americano, ouro, mercado imobiliário americano, petróleo e moedas de países emergentes. Quando analisamos a história recente do bitcoin, desde o início de sua negociação no mercado, é possível verificar que, dentre os coeficientes de correlação calculados entre todos esses, o do bitcoin é o mais baixo. De fato, ele se aproxima de 0. A correlação média do bitcoin com todos os outros ativos em questão foi de -0.03. Isso indica que não só as criptomoedas se enquadram em uma nova classe de ativos, como faz todo sentido serem incluídas em um portfólio tradicional. Afinal, se buscamos diversificação entre diferentes ativos, claramente temos um que é completamente distinto dos demais e atende ao perfil de risco-retorno desejado para a parte arriscada do portfólio. É claro que, dado que o Bitcoin existe há poucos anos, é difícil avaliar qualquer tipo de histórico. Sendo assim, é necessário seguir acompanhando os movimentos do mercado de criptomoedas como um todo pelos anos à frente, mas, certamente, temos uma classe de ativos digna de atenção.

Entrando no assunto central deste capítulo, é necessário ter uma estratégia bem definida para investir em criptomoedas. O objetivo aqui é discorrer sobre nossa estratégia pessoal e como você pode aplicá-la. Quando falamos em adquirir criptomoedas, precisamos pensar em três frentes: 1) o que comprar?; 2) quando comprar?;

e 3) por quanto comprar? Saber responder a essas perguntas é essencial para obter um portfólio bem-sucedido. Vamos entrar em detalhes sobre cada uma delas a seguir.

## O QUE EU COMPRO?

Semanalmente, recebemos centenas de e-mails de pessoas que desejam investir em criptomoedas. A pergunta que mais se repete é: “o que eu compro agora?”. Esse questionamento faz todo sentido, afinal, o mercado de criptomoedas está em expansão e em 2017 bateu a marca de mais de mil ativos diferentes. Para responder à pergunta “o que comprar?”, é necessário antes se perguntar “por que eu quero comprar?”. Existem três tipos de estratégias em que focamos e que definem o que decidimos comprar em cada momento: buy-and-hold, apostas e trading.

### BUY-AND-HOLD

Trazemos o buy-and-hold do universo das ações. A estratégia consiste em comprar um ativo e mantê-lo por tempo indeterminado em carteira, buscando capturar potenciais de longo prazo. Quando selecionamos uma ação via análise fundamentalista, estamos interessados nos fundamentos por trás da empresa que são capazes de fazê-la gerar ótimos lucros para seus acionistas ao longo dos anos. No limite, esperamos nos casar com a empresa, comprando suas ações para nunca vendê-las. Afinal, se a companhia é boa, quero ser sócio dela e ela me traz bons retornos, por que eu iria me desfazer dela?

Com essa ideia em mente, podemos aplicar o buy-and-hold para moedas de maior solidez. Por solidez, nos referimos a ativos que possuam ampla adoção no mercado de criptomoedas

e que possibilitem, de forma única, resolver problemas de seus usuários. É difícil pensar em longo prazo para esse mercado da mesma forma que pensamos para o mercado tradicional. Contudo, é possível imaginar fazer investimentos que não tenham necessariamente uma data de venda preestabelecida. Para definir, portanto, quais são as moedas e os ativos que podem ser incluídos em um grupo de buy-and-hold, precisamos ir mais a fundo em suas definições.

Antes disso, temos que fazer um parêntese técnico: todo criptoativo é constituído de um protocolo. O bitcoin, por exemplo, é a moeda do protocolo Bitcoin. O ether é o token do protocolo Ethereum. E assim por diante. Da mesma forma, com o advento da internet nos anos de 1990, empresas de tecnologia surgiram baseadas em protocolos. Os protocolos TCP/IP e HTTP são bons exemplos que possibilitam a troca de informações em rede. Em cima deles, surgiram empresas, que funcionam como aplicações desses protocolos. Veja o caso do Google. Ele é uma aplicação que utiliza o protocolo de comunicação da internet para entregar ao usuário um produto final: a busca de palavras-chave. Pois bem, a era online nos mostrou que, na maioria dos casos, a aplicação do protocolo agrupa mais valor que o próprio protocolo. Google, Facebook, Twitter e afins conseguem monetizar seus modelos de negócio em um nível muito superior no qual o protocolo em si conseguiria monetizar.

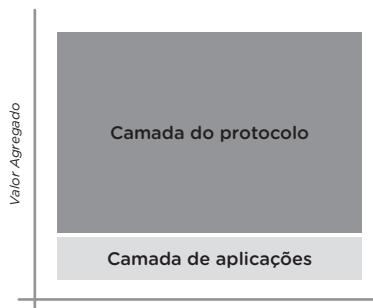
#### PROTOCOLOS WEB



Extraído de <http://www.usv.com/blog/fat-protocols>

Para o mercado de criptomoedas, entretanto, essa relação parece se inverter. Quando falamos em ativos ligados ao blockchain, vemos maior valor agregado pelo protocolo-base e menor valor agregado pela aplicação acima dele. O caso do Ethereum é emblemático: com centenas de tokens derivados, via ICOs (as Initial Coin Offerings) e utilizando sua estrutura para funcionar, o protocolo e seu token (o ether) agregam valor de mercado muito superior ao das aplicações separadamente. A isso damos o nome de protocolos gordos (*fat protocols*<sup>2</sup>, na definição em inglês, cunhada por Joel Monegro).

#### FAT PROTOCOLS — BLOCKCHAIN



Extraído de <http://www.usv.com/blog/fat-protocols>

Isso é explicado pelo fato de que o sucesso de uma aplicação tende a refletir em seu protocolo-base, transferindo seu valor para ele. Por exemplo, uma aplicação bem-sucedida baseada no protocolo do Ethereum tende a trazer mais atenção e especulação sobre o próprio Ethereum, refletindo no preço do ether. De fato, no ano de 2017, com o boom dos ICOs, tokens criados a partir da rede do Ethereum, uma enxurrada de dinheiro fluiu para o ativo do protocolo-base, fazendo com que sua capitalização de mercado chegasse a dezenas de bilhões de dólares.

<sup>2</sup>. MONEGRO, Joel, *Fat Protocols*, <http://www.usv.com/blog/fat-protocols> (acessado em 12 de janeiro de 2018).

Com isso em mente, faz sentido aplicar a estratégia de buy-and-hold para ativos de protocolos gordos, pois é a partir deles que devem surgir outras criptomoedas e criptoativos. Além disso, ao decidir por comprar uma criptomoeda para um prazo mais longo, outros pontos importantes precisam ser levados em consideração:

- **Equipe técnica**

Da mesma forma que ao avaliar as ações de uma empresa nos preocupamos em conhecer sua gestão e sua operação, entender a qualidade da equipe desenvolvedora de uma criptomoeda é essencial. Com tantos tokens surgindo nesse mercado, não são raros os casos de projetos que carecem de desenvolvedores ou até mesmo que não passam de puro marketing. No caso do Bitcoin, por exemplo, temos um código aberto que conta com a atenção de centenas de desenvolvedores ao redor do mundo. O fato de ser o maior e o mais antigo protocolo do mercado de criptomoedas faz com que muitas das melhores mentes estejam focadas em desenvolver as melhores soluções para ele.

- **Tempo de vida e comunidade**

Como se trata de software, quanto mais novo é o projeto, mais incertezas tendemos a ter, uma vez que incorporamos aos riscos a adoção do ativo pela comunidade e a própria solidez da equipe por trás do projeto. Sendo assim, nossa estratégia de buy-and-hold se baseia em ativos que possuam maior tempo de rede ativa, pelo menos de três a seis meses. Quando damos esse tempo à rede de se desenvolver e operar, conseguimos avaliar o real comprometimento da equipe de desenvolvedores, acompanhar a formação de comunidade, esperar falhas iniciais de projeto serem corrigidas e, até mesmo, garantir que não se trata de um *scam* ou esquema fraudulento.

## • Volume e liquidez

Outro ponto muito importante é verificar se o ativo possui boa liquidez. Em outras palavras, não é interessante fazer um investimento do qual não se pode desfazer quando desejar. Por mais que compremos esse ativo para o longo prazo, é imprescindível que tenhamos essa janela para sair da posição quando necessário. Afinal de contas, a análise pode mudar no meio do caminho ou podemos ter imprevistos. Além disso, se dividirmos nosso portfólio de criptomoedas nos três tipos de estratégia mencionados anteriormente, destinaremos a maior parte para buy-and-hold. Portanto, será a fatia mais significativa e que merece atenção à liquidez. Paralelamente, é preciso verificar o volume do ativo que é negociado diariamente. Ele está diretamente ligado à liquidez. Ativos com baixo volume são mais fáceis de ser manipulados e também dificultam a negociação de valores maiores ou por um número maior de investidores. Dado que o valor de uma criptomoeda está intimamente ligado ao número de usuários, um baixo volume atua como uma barreira para a adoção por parte de novos investidores.

## • Plataformas e usabilidade

Por último, um ponto crucial para a decisão de adicionar uma criptomoeda ao seu portfólio: a qualidade e quantidade das plataformas e carteiras que dão suporte a ela. Em linhas gerais, costumamos excluir, em nossa análise, ativos que não sejam negociados em corretoras conhecidas e que não possuam carteiras com boa usabilidade. Essa é uma medida conservadora, sim, mas lembre-se de que estamos falando de buy-and-hold. Sendo assim, inicialmente verificamos quais corretoras negociam a criptomoeda em questão. Poucas corretoras negociando-a geralmente significa também baixo volume e pouca liquidez. Depois, é importante olhar a concentração de volume negociado em cada corretora. Se, por exemplo, um ativo é negociado apenas em três corretoras e uma

delas concentra 80% do volume, você corre um risco inerente de contraparte. Isso quer dizer que, se a corretora tiver um problema, digamos de insolvência ou se for invadida por hackers, o impacto no mercado daquela criptomoeda especificamente será maior.

Junto a isso, a usabilidade é extremamente importante. Alguns ativos não possuem carteiras que funcionem para celular ou sejam facilmente executadas em um computador. Para tal, demanda-se um maior conhecimento técnico, o que mais uma vez limita a adoção por mais investidores e dificulta a parte operacional de armazenamento. Sendo assim, é interessante focar em criptomoedas que sejam amplamente negociadas pelo mundo e tenham suporte por várias carteiras diferentes, especialmente pelas hardware wallets.

A primeira estratégia, portanto, de comprar e manter a moeda pelo longo prazo, deve ser a parte principal do seu portfólio de criptomoedas. A partir daí é que abrimos espaço para outras duas estratégias, que têm o potencial de amplificar a valorização do portfólio.

## APOSTAS

Pegue quase tudo o que foi dito na estratégia anterior e inverta. Aqui, o grau especulativo é muito maior. Contudo, é possível obter retornos incríveis. Na discussão sobre os protocolos gordos, afirmamos que a maior parte do valor está concentrada nos protocolos-base dos criptoativos. De fato, quando olhamos a geração de valor nesse mercado, é isso que observamos. Porém, não podemos negar que nem tudo é valor. Muito se baseia puramente no preço. Os movimentos especulativos em torno de moedas virtuais

nascentes são prova disso. Nessa fatia do portfólio, portanto, buscamos ativos que de alguma forma não respeitem todos os filtros de buy-and-hold, mas que ainda assim apresentam potencial interessante e assimetria convidativa. Aqui entram as aplicações em cima de protocolos. Um token derivado do Ethereum que proponha soluções únicas para problemas usuais, por exemplo, faz parte da fatia de apostas.

Como o próprio nome diz, ao investir nesses ativos, estamos apostando no seu sucesso futuro, com muito menos histórico para avaliá-lo. Nesse grupo, entram criptomoedas nascentes, ICOs ou outras moedas de menor valor de mercado e menor liquidez. Basicamente, quando compramos bitcoin ou ether, que são ativos para buy-and-hold, temos meses ou anos de histórico de desenvolvimento, um planejamento do que pode ser implementado no futuro e dados suficientes para avaliar o ativo. Já quando falamos de uma moeda ou token que acabou de surgir, focamos em sua proposta de inovação e apostamos na sua adoção futura em larga escala, mesmo que ainda haja coisas a serem provadas. Além disso, como aqui há espaço para as aplicações derivadas de protocolos, podemos ter exposição a novas tecnologias, como por exemplo ativos que apliquem o blockchain para solucionar problemas de mercados tradicionais, além do sistema financeiro.

De certa forma, então, aceitamos correr ainda mais risco, muitas vezes abrindo mão de boas plataformas ou de usabilidade, para capturar retornos potenciais maiores. Duas coisas, porém, precisam sempre ficar claras: 1) não podemos abandonar a análise da proposta tecnológica e da equipe técnica envolvida no projeto; e 2) essa fatia do seu portfólio de criptomoedas deve ser menor que a de buy-and-hold.

## TRADING

Para esta terceira estratégia, pouco importa o tipo de ativo. Estamos interessados em fluxo de dinheiro para encontrar oportunidades de curto prazo. Um trader pode simplesmente encontrar pontos de compra e venda de um ativo olhando seu gráfico, sem nem saber de qual ativo se trata. As informações vêm da análise técnica. Para tal, precisamos apenas refinar nosso espectro de criptomoedas negociáveis por volume/liquidez e plataforma. Optar por fazer trading de criptomoedas pode ser uma forma de amplificar os retornos da sua carteira, pois esse mercado possui bastante volatilidade e oferece, quase diariamente, oportunidades de operação para o curto prazo.

Contudo, é importante também salientar que é necessário experiência e controle emocional para suportar as variações. Inevitavelmente, um trader passa horas e horas analisando gráficos em um computador e precisa de monitoramento constante dos ativos para não perder o momento de compra ou venda. Muitas corretoras de criptomoedas oferecem plataformas de boa qualidade. Nelas, você já tem acesso aos gráficos das moedas, em algumas pode até mesmo adicionar indicadores a eles para refinar a análise e pode acompanhar o livro de ofertas em tempo real. Se você é trader, poderá aproveitar as ótimas oportunidades que esse mercado oferece. Se não for, pode buscar a ajuda de um profissional experiente para operar.

Com essas três estratégias delineadas, basta escolher quais você deseja implementar para seu portfólio. Como comentamos anteriormente, é importante que você responda para si mesmo a pergunta: “por que eu quero comprar criptomoedas?”. Se o seu objetivo é participar da revolução financeira que elas estão trazendo à tona, a estratégia de buy-and-hold é a ideal e ganhos espetaculares podem ser obtidos. Se você pretende apenas capturar

movimentos de médio prazo com projetos inovadores, a estratégia de apostas será interessante. Já se seu objetivo for lucrar no curto prazo, inclusive com o objetivo de potencializar os retornos da sua carteira de criptomoedas, fazer trading será uma boa opção. Definido o que comprar e qual estratégia seguir, é necessário saber quando comprar cada ativo.

## QUANDO EU COMPRO?

Vamos de trás para a frente aqui, passando pelas três estratégias definidas anteriormente. Quando falamos em trading, o momento de compra e venda é definido pelos sinais encontrados nos gráficos, via análise técnica (vale lembrar que o objetivo deste livro não é explicar as bases teóricas desse tipo de análise). Porém, em linhas gerais, na análise técnica, identificamos padrões de comportamento dos preços, bem como tendências e movimentos característicos de um determinado ativo. Assim, buscamos comprar um ativo quando identificamos que ele tem potencial de se valorizar no curto prazo. Por exemplo, se analisamos o gráfico do bitcoin em um determinado momento e verificamos que seu preço vem se comportando em uma tendência de alta e, além disso, outros indicadores da análise confirmam esse movimento, podemos optar pela compra. Confirmado o movimento de alta do preço, vendemos o ativo quando atingirmos o objetivo desejado de lucro.

Agora, se estivermos falando da fatia de apostas do seu portfólio de criptomoedas, muitas vezes o momento ideal de compra é quando esse ativo estreia no mercado, por meio de um ICO, por exemplo. Para criptomoedas que já estão sendo negociadas há algum tempo, a preocupação será menor com o momento exato de compra e maior com a investigação do projeto e do seu potencial futuro, como descrito na seção “O que eu compro?”, para então

proceder com a compra. Para projetos nascentes, dificilmente acertaremos o *timing*, ou seja, o momento exato de compra. Portanto, já que se trata de uma aposta, é preferível que o ativo passe pelo seu crivo inicial e, uma vez que você decidir investir nele, compre e o esqueça por algum tempo. Desenvolvimentos de projeto inevitavelmente levam tempo, e não será de uma hora para a outra que a moeda, o token ou o ativo irá se valorizar.

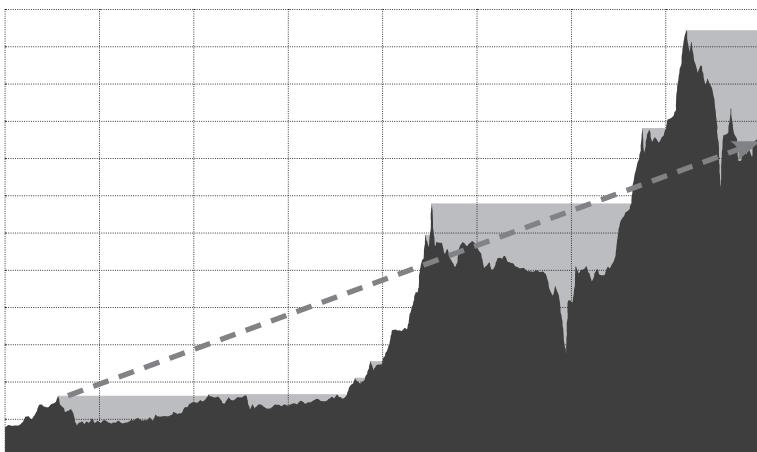
Por último, o caso mais importante. Quando falamos da estratégia de buy-and-hold, há basicamente três formas de definirmos o momento de compra. Nesse caso, como estamos comprando ativo para o longo prazo, é possível que você venha a fazer mais de uma compra ao longo do tempo, conforme reajusta sua posição.

## 1. Aporte único

Essa é a forma mais simples de alocação: compre uma vez, para adicionar uma determinada criptomoeda ao seu portfólio. Ela faz muito sentido para quem deseja comprar bitcoin ou altcoins para o longo prazo, focando na valorização do ativo nos próximos anos e no aumento da diversificação de seu portfólio, combinando com ativos tradicionais. Essa é a estratégia mais prática e que permite ao investidor possuir criptomoedas sem precisar ficar movimentando a carteira a todo momento. Se você acredita no potencial de valorização de uma ou mais moedas digitais para os próximos anos, pode fazer um aporte que seja coerente com suas outras alocações e então seguir com a estratégia de buy-and-hold.

Existe um ponto importante para se levar em conta e ele vale para qualquer estratégia de médio ou longo prazo, mas, sobretudo, para uma estratégia de buy-and-hold com aporte único. Estou falando do conceito de *market drawdown*, que basicamente se refere aos períodos em que o preço de um ativo está abaixo do seu último pico.

É importante saber se manter estável em períodos como esse, pois nossa mente tende a entendê-los como momentos de perda, principalmente se um ativo cai logo depois de você tê-lo comprado. Os períodos de *market drawdown* muitas vezes levam investidores menos experientes a venderem o ativo por acharem que poderiam melhorar seus retornos “partindo para a próxima”. Entretanto, veja a linha reta no gráfico abaixo, destacadamente crescente. Ela indica o movimento de longo prazo do ativo e é a ela que devemos nos ater. Se estamos comprando uma criptomoeda para o longo prazo, especialmente se fizermos isso via um aporte único, então é importante focar na sua tendência de longo prazo, e não nos movimentos de curto prazo. Isso ajuda a evitar vendas precipitadas.



## 2. Compras graduais fixas

Se você pretende fazer mais de um aporte em uma determinada criptomoeda, esta segunda estratégia será interessante. A estratégia de compras graduais fixas é também conhecida como DCA (*dollar-cost averaging*). Por meio dela, você reserva um valor fixo mensal para investir. Essa abordagem funciona bem para quem possui seus

fundos para investir mensalmente, especialmente se você não tem, de início, o valor total que deseja destinar para criptomoedas. Com compras graduais fixas, você terá um preço médio de compra da criptomoeda. Em um *bull market* (mercado em tendência de alta), essa estratégia resulta em um preço médio mais elevado do que o aporte único no início. Porém, nunca somos capazes de prever o futuro. Mesmo que enxerguemos uma tendência de alta para um determinando ativo no longo prazo, a volatilidade traz janelas de oportunidades em períodos de baixa. Isso nos conecta à terceira forma de aquisição.

### **3. Custo médio de aquisição**

Esta abordagem basicamente combina as duas primeiras. Você faz um aporte inicial e aproveita janelas de queda no preço para fazer novos aportes e reduzir o preço médio de compra. O mercado de criptomoedas é muito volátil e sensível a notícias. Assim, existirão momentos em que veremos quedas no preço, puxadas por acontecimentos ao redor do mundo, mas, eventualmente, a tendência em um prazo maior permanecerá inalterada. Nesse caso, você pode aproveitar para comprar com “desconto” e reduzir o preço médio de aquisição. Gostamos desta estratégia também por outro motivo: ela força você a pensar, previamente, a que preços mais baixos você faria novas entradas e, assim, acaba indiretamente se preparando psicologicamente para períodos de baixa.

## **POR QUANTO EU COMPRO?**

Essa talvez seja a pergunta mais difícil de respondermos em um livro. Afinal, decidir até qual preço devemos comprar um ativo depende de uma análise momentânea dele. Sendo assim, inevitavelmente a pergunta “por quanto comprar?” se conecta à

anterior, “quando comprar?”. Se, por exemplo, seu objetivo é o buy-and-hold, importa mais comprá-lo de fato do que se se está pagando o melhor preço possível por ele. Basicamente, pagamos o preço que vale o ativo no momento que identificamos ser o melhor para a compra.

Apesar dessa resposta vaga, há um ponto que é interessante observarmos aqui e que certamente ajudará a definir se vale a pena pagar um certo preço por uma criptomoeda em questão. Desde a criação do bitcoin, ele reina como dominante do mercado de criptomoedas. É o ativo de maior valor de mercado e, de uma forma ou de outra, muitos outros seguem seus movimentos. É bastante comum ver outras moedas virtuais se valorizando quando o bitcoin se valoriza, e vice-versa. Isso é provocado pela dominância que o bitcoin exerce, em termos de valor de mercado, no universo das criptomoedas como um todo, além do fato de ele ser a moeda-base para a compra da maioria dos outros ativos. Dessa forma, uma maneira interessante de olhar para o mercado é usar o bitcoin como uma referência e buscar ativos que possam se valorizar mais do que ele. Em linhas gerais, você pode se fazer a seguinte pergunta: “quais ativos eu compro para que valha mais a pena ter uma cesta diversificada de criptomoedas do que manter meu dinheiro só em bitcoin?”.

A partir daí, uma forma de definir se vale a pena comprar determinada altcoin é olhando para ela em relação ao bitcoin. É possível encontrar na internet gráficos que mostrem os preços na cotação altcoin/bitcoin. Ou seja, em vez, por exemplo, de olhar para o gráfico do preço do litecoin em dólares, pode-se observar o gráfico de preço do litecoin em bitcoin. Caso, para um certo período, esse gráfico indique que a altcoin está em movimento de alta, isso quer dizer que ela está se valorizando mais que o bitcoin ou se desvalorizando menos que ele. Sendo assim, ao olhar para essa cotação em relação ao bitcoin, é possível identificar se a altcoin tem

potencial, no médio prazo, de se valorizar mais do que o bitcoin, maximizando seu lucro. Já se a resposta for negativa, talvez não seja o melhor momento de comprar a moeda em questão.

No fim, a forma mais prática de definir por quanto comprar uma determinada criptomoeda é sabendo quando não comprá-la. Aqui vale a máxima de Warren Buffett: “compre ao som dos canhões e venda ao som dos violinos”. Busque comprar em momentos de baixa do mercado, quando oportunidades se abrem, e não em momentos de pico dos preços e euforia, quando temos indicativos de que o ativo continuará subindo.

## COLOCANDO A ESTRATÉGIA EM PRÁTICA

Neste capítulo, investigamos a fundo as diferentes estratégias de compra de criptomoedas. Isso, associado ao capítulo anterior, mais operacional, será um ótimo guia para sua vida de investidor em criptomoedas. Aqui estão as ferramentas de que você precisa. Agora mãos à obra!

O objetivo dessas estratégias de investimento é buscar adicionar as criptomoedas a um portfólio tradicional de forma a maximizar seus retornos. Por isso, vale sempre reforçar que um investidor com uma carteira equilibrada deve evitar expor mais do que 5% do seu patrimônio em criptomoedas. Por via de regra, invista um valor que não o prejudicará se você perdê-lo completamente. As criptomoedas, sem dúvida, são um instrumento maravilhoso para quem busca retornos acima da média e deseja acelerar o processo de construção de riqueza, mas deve-se lidar com elas com a devida diligência.

Dentro de nossa estratégia de investimento, buscamos destinar a maior parte do aporte em criptomoedas para aquelas

mais representativas em termos de valor de mercado. Além disso, diversificamos o investimento em mais de um ativo como forma de estarmos expostos a diferentes potenciais de valorização, por meio de ativos com propostas distintas.

Falamos aqui sobre o que, quando e por quanto comprar os ativos. Porém, quando o foco é o médio ou o longo prazo, tenha sempre em mente que é mais importante comprar um ativo de qualidade do que buscar acertar o momento exato de sua compra.





## CONCLUSÃO OU O PRIMEIRO PASSO?

Quando vejo a palavra “conclusão” em um livro que estou lendo, sempre espero considerações que me mostrem alguma ideia que eu já tenha extraído, mas que também apontem outras que eu sequer notei. Naturalmente, pretendemos fazer o mesmo aqui, mas com uma diferença. É meio incoerente dizer que este é um capítulo de “conclusão”, pois o livro inteiro é apenas um ponto de partida para o mundo dos criptoativos, e não o fim.

Por outro lado, se você queria um pontapé para iniciar seus investimentos no mundo das criptomoedas, aqui se encerra o seu primeiro passo. Já falamos isso ao longo dos capítulos anteriores, mas reforçamos que, enquanto as pessoas não pararem para entender do que se trata toda essa revolução, vão comprar pelo *hype*, e não pelo fundamento. E se os investidores colocam seu dinheiro em algo que não compreendem totalmente, estão no caminho para o insucesso na vida de investidor.

Por esse motivo, neste livro, procuramos mostrar por que consideramos as criptomoedas melhores do que o dinheiro logo na introdução. Claro que, à medida que você lia o livro, espero que essa visão tenha se sedimentado pelos mais diversos motivos, seja por ter percebido que o sistema financeiro tem muitos erros intrínsecos e, por isso, as criptomoedas são melhores do que dinheiro, seja por ter enxergado o potencial que a tecnologia do blockchain pode destravar. Você pode também ter notado que investir em cripto pode tirar todo o poder de uma indústria trilionária e devolvê-lo para as pessoas; e isso, sim, seria a revolução.

Na verdade, foi com essa proposta que Satoshi Nakamoto lançou seu *white paper*, mas isso você já deve saber a essa altura do livro. Foi em meio à crise do subprime nos Estados Unidos que nasceu o bitcoin e ninguém poderia imaginar uma evolução tão exponencial de lá para cá. Foi isso que assustou a todos no mercado financeiro e fez o principal questionamento de todos surgir à medida que o preço dessa criptomoeda crescia: “Será que tudo isso não é apenas uma bolha?”. De certa forma, o questionamento é válido se olharmos para as tecnologias dos criptoativos apenas como investimento. Por outro lado, sabemos que não podemos encaixá-los em uma classe de ativos já existente, pois eles são tão diferentes do que temos atualmente, que merecem uma classe totalmente nova para comportá-los.

Esse foi o caso do ornitorrinco, que mencionamos no início do livro. As primeiras pessoas de fora do continente natural do animal que receberam as imagens da espécie não acreditaram no que viram e, em um primeiro momento, acharam que se tratava de uma brincadeira. Só depois de convencidos da existência da criatura tentaram enquadrá-lo na categoria de ave ou mamífero. Mas essa não é uma atitude restrita aos cientistas. O ser humano, de maneira geral, sempre quer colocar as inovações

em taxonomias já existentes, como se as classificações fossem verdades imutáveis que permitissem compreender todos os tipos de novidades que aparecem.

Assim como as primeiras documentações do ornitorrinco foram confundidas pelos especialistas que entendiam do reino animal com uma brincadeira, os analistas de investimento não deram muita atenção quando ouviram falar do bitcoin. Para eles, aquilo parecia algo que um bando de nerds havia inventado para se divertir, e não teria valor algum. Depois que viram que a invenção poderia ter alguma serventia no mercado financeiro, tentaram enquadrá-la nas categorias de investimento com que estavam acostumados a trabalhar, como moeda, reserva de valor ou ações.

Bem sabemos que não é possível categorizar uma nova classe ativos como se fosse uma já existente. É exatamente por não se enquadrarem em nenhuma definição preexistente que não podemos avaliar os criptoativos como simplesmente um investimento e acreditar que são uma bolha, dada sua valorização expressiva.

Se pensarmos em bens de consumo que passaram a existir em um determinado período da história e foram ocupando as casas quase que completamente pelo mundo, poderíamos entendê-los como uma bolha, mas, por serem bens, não são vistos dessa forma. Por exemplo, atualmente existem mais celulares do que pessoas no Brasil, e não conheço muitos teóricos que afirmam que a produção dos aparelhos é uma bolha. Afinal, trata-se de um bem que as pessoas sempre procuram, dadas suas amplas utilidades.

Nossa maior crença sobre as criptomoedas é esta: elas são inovações que precisam de maturação para destravarem todo seu potencial; uma vez que isso acontecer, e que houver também uma melhoria de sua usabilidade, o caminho estará livre para uma ampla aceitação e apreciação maior de valor.

Foi isso o que ocorreu com a indústria de celulares, que teve uma aceitação tão grande que, de 2002 a 2010, dobrou de tamanho a cada dois anos. O mais impressionante é que os especialistas da época previram crescimentos abaixo de 20% para cada biênio desde 2002.

Realmente, o ser humano não estava (nem está) preparado para enxergar o crescimento exponencial que as novas tecnologias tendem a ter em um curto espaço de tempo. O homem é capaz apenas de projetar curvas lineares e prever crescimento incremental; o avanço exponencial não é contemplado por nosso cérebro.

É exatamente por isso que a evolução de valor do mercado de cripto causa, à grande maioria, estranheza e medo de formação de bolha. Por outro lado, mostramos que não devemos confundir a anatomia de uma bolha com a de uma inovação, algo que tem sido feito com relação aos criptoativos. E acreditamos fortemente nisso porque nos debruçamos sobre o que é a tecnologia por trás da maioria dos criptoativos e percebemos o poder que tem a disruptão do blockchain.

Foi por essa razão que dedicamos duas partes do livro a falar sobre essa tecnologia. A primeira, o capítulo 5, foi bem mais leve e objetiva, com o simples intuito de transmitir com exemplos e da maneira mais fácil possível a revolução que a nova tecnologia trouxe. O segundo momento em que falaremos sobre o blockchain é no apêndice à frente, no qual nos dedicamos a ir mais a fundo nas questões técnicas sobre essa inovação.

Acreditamos que, por sermos engenheiros de formação, gostamos de saber sobre a tecnologia em si, e não nos contentamos com uma descrição superficial. Como sabemos que isso não agrada a todos os leitores, decidimos deixar os aspectos técnicos em uma seção separada. Mesmo que você não seja uma pessoa que ame a parte tecnológica das coisas que o cercam, recomendamos que

leia pelo menos a primeira página do apêndice. Caso a leitura seja técnica demais, tudo bem. Ao menos você tentou.

Quando falamos sobre o universo dos outros criptoativos, trouxemos algumas definições que colhemos ao longo de pesquisas sobre o assunto, o que exigiu bastante dedicação. Como não existem definições consagradas para os ativos que abordamos, apenas optamos pelas mais coerentes e consistentes, comparando com tudo o que encontramos espalhado em livros e na internet. Além disso, selecionar o que falar nesta seção do livro foi desafiador, dada a velocidade com que o mercado se movimenta e as mudanças que acontecem da noite para o dia, literalmente — já que esse é um mercado que não para. Procuramos nos ater aos ativos que apresentaram mais consistência ao longo dos anos e que têm mais tempo de estrada.

Ainda assim, não há garantia de que tais ativos perdurarão para sempre. Esse universo muda cada vez mais rápido, e não nos assustaria ver criptoativos novos tomando o lugar dos que mencionamos, em questão de meses após seu surgimento. Pois como dissemos, acreditamos na visão exponencial e, dessa forma, qualquer ativo novo que traga uma disruptão maior ainda pode, sim, tomar a frente de outros consagrados até o momento. Por termos essa visão, e sempre tentarmos incuti-la na cabeça das pessoas, recomendamos que este livro não seja o fim da sua jornada nesse novo universo de ativos, mas apenas o primeiro passo. Grande parte da visão que temos agora para o futuro dos criptoativos deve mudar bastante a cada três meses, simplesmente porque o mundo em que vivemos está se transformando cada vez mais rápido. Além disso, um mercado que funciona 24 horas por dia tem ciclos bem mais ágeis do que aqueles a que estamos acostumados.

Nossa intenção com este livro é convencer todos leitores que de certa forma criaram uma fobia pelo assunto, por qualquer que seja o motivo, a parar por um momento e analisá-lo de forma não trivial.

Melhor ainda, a avaliar o tema de maneira estritamente racional, analisando todos os lados do prisma, desde as posições daqueles que afirmam ser uma bolha até a ótica dos mais entusiastas, como nós. Só olhando a questão de maneira mais racional podemos tirar conclusões mais seguras sobre o que fazer. E, a partir do momento em que essa decisão estiver mais sedimentada, você poderá tomar uma ação mais congruente e segura.

Foi por isso que dedicamos dois capítulos do livro à parte prática, um sobre como comprar seus primeiros criptoativos e outro sobre a estratégia para melhor selecioná-los. Dessa forma, acreditamos que tudo de que você precisa para dar o pontapé inicial na sua vida de criptoinvestidor tenha sido explorado até o momento.

É extremamente satisfatório falar sobre o assunto para quem está começando, pois, quando buscamos saber mais sobre as criptomoedas, sempre fomos bem recebidos pela comunidade. É claro que nem sempre as experiências foram positivas, porque muitos fatos são realmente complicados e exigiram tempo e um pouco de neurônios gastos. Com essas dificuldades em mente, sempre tomamos muito cuidado ao apresentar conceitos complexos neste livro, explicando-os da maneira mais simples possível, mas sempre evitando ser superficiais.

Ver esse mercado evoluindo à medida que escrevíamos esta obra foi uma experiência única e conclusiva sobre a velocidade com que ele se movimenta. Se no começo do livro tínhamos uma ideia de como se comportava o mundo cripto, ao fim, estamos com outra cabeça. É dessa forma que espero que você termine sua leitura: com uma ideia diferente da que tinha antes de ler as primeiras linhas. Se conseguimos que você mudasse ou expandisse de alguma forma seu pensamento sobre essa nova classe de ativos, consideramos nosso trabalho bem-feito. Principalmente porque o que queremos neste momento é que você entre nesse universo.

**FIM**

SERÁ?



## *APÊNDICE*

# **COMO ME APAIXONEI DE VEZ PELAS CRIPTOMOEDAS: UMA VISÃO TÉCNICA SOBRE O BITCOIN**

Quando decidimos como seria esta obra, o conteúdo e os tópicos abordados, queríamos escrever algo diferente dos outros livros existentes sobre criptomoedas. A grande maioria deles é bastante técnica, no sentido de entrar em detalhes a respeito do desenvolvimento tecnológico. Sem dúvidas, existem grandes obras de referência por aí. Mas desejávamos ir por outro lado, com um livro que falasse mais sobre a evolução do dinheiro ao longo do tempo e sobre como processos de inovação semelhantes ao que ocorre com o universo das criptomoedas podem mudar completamente o mundo em que vivemos.

Acredito que, de alguma forma, conseguimos alcançar esse objetivo. É claro que é difícil deixar de lado todos os pormenores técnicos, afinal, eles são imprescindíveis em alguns momentos. Agora, sim, neste apêndice, mergulharemos nesses tópicos. Discutiremos o funcionamento das criptomoedas, tomando por base o protocolo Bitcoin.

Esta seção foi pensada para os leitores que desejam entender mais a fundo o que está de fato por trás das criptomoedas. Confesso que foi quando comecei a estudar com esse nível maior de profundidade tecnológica que realmente comprei a ideia. Tenho certeza de que, se você gosta de ler e aprender sobre tecnologia, especialmente software, vai se apaixonar ainda mais pelos ativos criptográficos e ficará convencido de que eles vieram para mudar o sistema financeiro global.

Lembro-me de quando ouvi falar sobre o protocolo Bitcoin pela primeira vez. Entendia que era uma tecnologia que tinha uma moeda essencialmente digital, sem fronteiras, e que se falava muito sobre a tal descentralização. Aquilo, porém, não era tão claro para mim. Tudo se esclareceu quando fui apresentado à tecnologia do blockchain.

Já discorremos bastante sobre esse sistema de registro no capítulo 5. Agora, vamos olhar mais detalhadamente para seu funcionamento e o que, de fato, são os blocos dessa cadeia. Aqui também entenderemos em mais detalhes como funcionam outros mecanismos da tecnologia do Bitcoin, investigando aspectos mais técnicos.

A principal referência utilizada por nós foi o livro *Mastering Bitcoin — Programming the Open Blockchain*, de Andreas M. Antonopoulos. Trata-se de uma das maiores referências de programação voltada para o blockchain do Bitcoin que existe. Alguns exemplos utilizados neste apêndice foram adaptados de lá. Aproveitamos para deixar aqui nosso agradecimento a Antonopoulos pela grande obra criada.

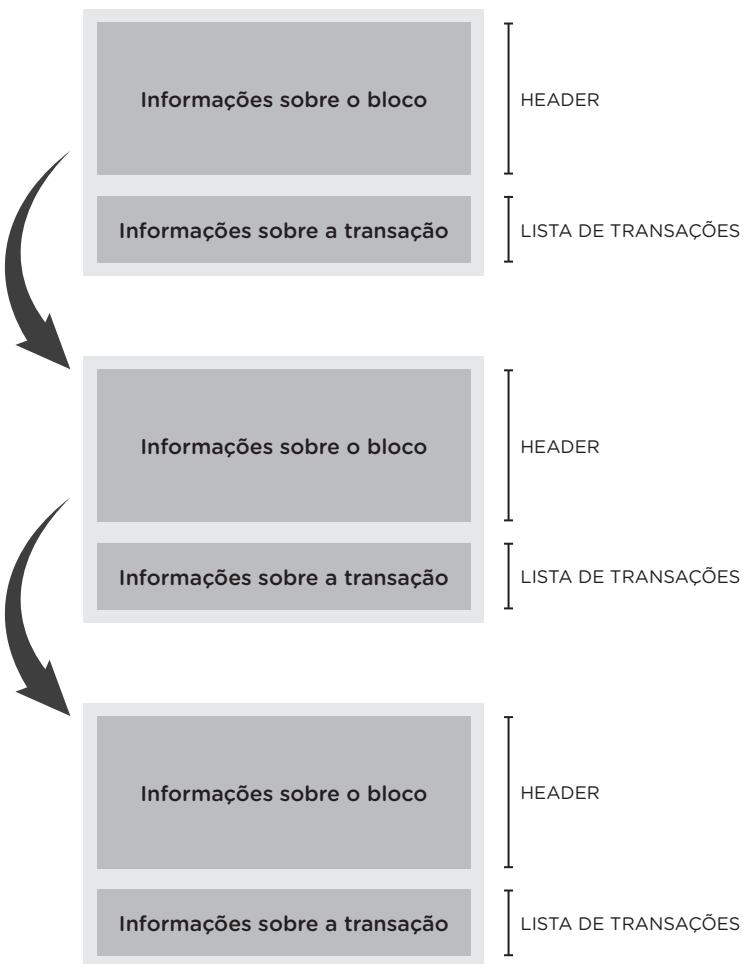
## POR DENTRO DO BLOCKCHAIN

O blockchain nada mais é do que uma estrutura de registro. O termo “blockchain”, na verdade, não aparece no *white paper* original do Bitcoin, publicado por Satoshi Nakamoto. O autor cita uma série de blocos encadeados que formam o registro histórico de movimentações. Um bloco contém informações sobre um número de transações que foram efetuadas na rede do Bitcoin. Além disso, cada bloco é ligado ao bloco anterior, formando assim uma cadeia de blocos, daí derivando a denominação blockchain.

Cada bloco é identificado por um hash, que é simplesmente uma mensagem criptografada. O protocolo Bitcoin utiliza criptografia para garantir a segurança de suas transações, um algoritmo chamado “função hash criptográfica”. Esse algoritmo é responsável por transformar uma certa mensagem em uma sequência criptografada de caracteres. Ele é considerado uma função de apenas uma via, o que significa que é capaz de criptografar a mensagem, mas é impossível, para um usuário qualquer, reverter a mensagem criptografada para a mensagem original, a menos que se use força bruta para testar todas as combinações de palavras possíveis. Entenda o hash como uma impressão digital do bloco, que é usada para encadeá-lo aos demais. Um bloco, portanto, terá seu próprio hash e será ligado ao bloco anterior referenciando o hash desse bloco-pai. Essa sequência continua até que se chegue ao primeiro bloco da sequência do blockchain, chamado Bloco Gênesis.

Um bloco armazena centenas de transações que ocorrem na rede do Bitcoin. Quem faz todo esse trabalho de capturar as transações que ocorrem e incluí-las em um bloco é o minerador. Falaremos mais sobre ele à frente. Um bloco possui, basicamente, duas partes: um header (cabeçalho) e a lista de transações. O header funciona como um grupo de dados identificadores. Nele fica armazenado o hash do bloco em questão (uma impressão digital

que funciona como identidade) e o hash do bloco anterior, seu pai. Calcular o hash depende da aplicação de um algoritmo de criptografia. Portanto, poder computacional é dispendido para essa atividade.



Dados extraídos de ANTONOPOULOS, 2017.

Como o hash de um bloco é calculado a partir das informações daquele que o antecede, uma mudança no hash do bloco-pai também resulta em uma mudança no do bloco-filho. Isso, por sua vez, resultará em uma mudança no bloco-neto, o próximo na sequência, e assim por diante. Dessa maneira, cria-se um efeito cascata.

Para alterar um bloco do blockchain, é necessário alterar todos os outros na sequência. Quando há vários blocos à frente, o poder computacional requerido para alterar o bloco em questão e todos os seguintes é tão grande que essa alteração se torna simplesmente inviável. Sendo assim, quanto mais tempo passa, mais difícil é modificar o que está registrado no blockchain.

Por convenção, considera-se que, quando seis blocos são adicionados à frente de um certo bloco, é impossível, dada a tecnologia hoje existente, reverter todos os cálculos para fraudá-lo. O blockchain é, portanto, uma estrutura de dados extremamente segura, que fica melhor com o passar do tempo.

Podemos entender o blockchain como uma pilha de blocos de concreto, um colocado em cima do outro. Você pode até ter força para mover um ou dois no topo da pilha, mas, conforme mais blocos de concreto são adicionados em cima, mais difícil fica movê-los, até chegar um ponto em que você simplesmente não terá força suficiente para tirá-lo do lugar. Ele estará consolidado na pilha, imóvel.

## **COMO FUNCIONAM AS TRANSAÇÕES**

O bitcoin é um instrumento que carrega valor consigo, seja em seu emprego como reserva de valor, seja como meio de pagamento. De uma forma ou de outra, as transações são elementos essenciais para o funcionamento da rede. O protocolo Bitcoin só é utilizado pelas pessoas se elas são capazes de mover quantias de dinheiro

entre si, sob a forma da criptomoeda bitcoin. A tecnologia do Bitcoin foi desenvolvida para permitir que essas transações ocorram de maneira segura, e o blockchain funciona como uma cadeia de blocos que armazena os registros dessas operações. Agora, precisamos entender como, de fato, elas funcionam.

Vamos começar com um exemplo. Roberto, que adquiriu recentemente suas primeiras frações de bitcoin, exatamente 0,005 BTC, por meio de uma corretora especializada, deseja enviá-las para sua carteira digital, ou wallet. Ele precisará fazer uma transação. Para isso, no painel da corretora, ele escolherá a opção de enviar bitcoin para um endereço externo, na qual poderá digitar o endereço da sua carteira ou escanear um código QR que contenha essa informação. Em linhas gerais, portanto, Roberto precisa escolher: 1) quanto enviar; e 2) para onde enviar. Uma vez configurada a transação, ele verá que uma taxa será incluída, que é a taxa de mineração, paga aos mineradores para garantir a propagação e a validade da transação.

Ao confirmar o envio dos 0,005 BTC, a chave privada da carteira em que o valor se encontra – nesse caso, a carteira da corretora – será usada para assinar a transação, e a rede Bitcoin será notificada de que a transferência do valor para o novo endereço foi autorizada. Após alguns minutos, a transação é registrada como “não confirmada”. Isso significa que ela foi enviada para a rede de nós do Bitcoin com sucesso, mas ainda não houve quem a incluísse no blockchain, em um determinado bloco. Para verificar o status da transação, Roberto pode usar sites que fazem buscas no blockchain, como os apresentados a seguir:

- Blockchain.info (<https://blockchain.info>)
- BlockCypher Explorer (<https://live.blockcypher.com>)
- Bitcoin Block Explorer (<https://blockexplorer.com>)

Basta utilizar o endereço público da carteira que vai receber o valor ou o hash da transação para fazer a busca. Em nosso exemplo, Roberto digitou o endereço da carteira que recebeu os 0,005 BTC no blockchain.info e encontrou a operação, como mostra a figura abaixo:

### Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary	Transactions
Address 1Htb532rSekommL1DAUssuzicrwpthbRp	No. Transactions 1
Hash 160 b943aa9b8edd36605069cc0d35b67e3bfa7bef4	Total Received 0.005 BTC
Tools Related Tags - Unspent Outputs	Final Balance 0.005 BTC

Request Payment      Donation Button

**Transactions (Oldest First)**

Transaction ID	Date
cfcf02d1ea919a8944a5c70fcff5b307763060e1bb83009a914f18858f9ea84	2018-01-07 18:20:38
3KBJNsZtQAFUawGkeAY8xGvFAKJMgtZCt	→ 1Htb532rSekommL1DAUssuzicrwpthbRp 0.005 BTC

Filter ▾

Unconfirmed Transaction | 0.005 BTC

Extraído de <https://blockchain.info>

Antes de entendermos o processo de confirmação da transação, que é papel dos mineradores, vamos entrar em mais detalhes sobre o funcionamento das transações em si. Uma transação tem entradas (inputs) e saídas (outputs). Inputs são valores que estão saindo de uma determinada carteira, enquanto outputs estão indo para outros endereços. Um ponto importante a se destacar é que a soma das entradas difere da soma das saídas em vista do valor pago aos mineradores como taxa de transação. Por exemplo, no caso de Roberto, a entrada foi de 0,0052 BTC, enquanto a saída foi de 0,005 BTC. A diferença, 0,0002 BTC, diz respeito ao valor pago de taxa.

Conforme transações são feitas na rede do Bitcoin, uma saída se conecta a uma entrada, criando um encadeamento de transações. Retomando o exemplo de Roberto, a entrada é o valor sacado da corretora e a saída é o valor recebido em sua carteira. Se ele decidir usar parte desse valor (0,003 BTC) para pagar o jantar em um restaurante que aceita bitcoin, gerará uma nova transação,

que usará a saída da operação anterior como entrada. Ao mesmo tempo, uma nova saída será criada, a qual corresponderá ao valor enviado para a carteira do restaurante, e assim por diante. A figura a seguir ilustra esse processo.

#### TRANSAÇÃO 1

Entrada: 0,0052 BTC

Saída: 0,005 BTC (spent)

Taxas de transação: 0,0002 BTC

#### TRANSAÇÃO 2

Entrada: 0,005 BTC

Saída restaurante: 0,003 BTC (unspent)

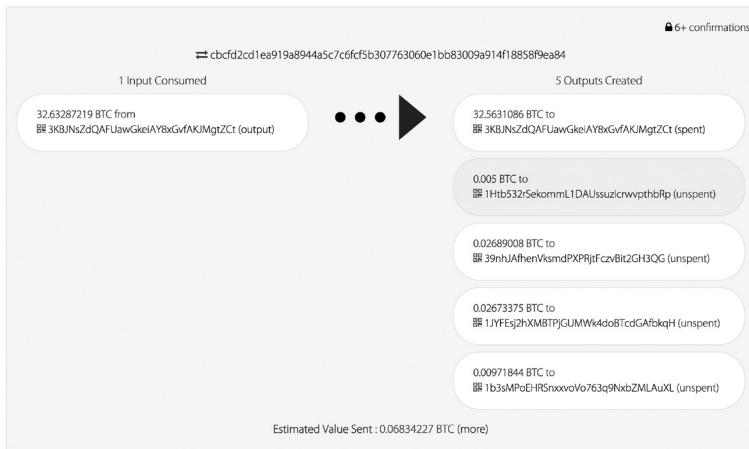
Taxas de transação: 0,0002 BTC

Além da concatenação das transações, há duas coisas importantes para extraímos do exemplo: o troco e o estado de cada saída. Começando pelo primeiro, ao fazer uma transferência de valor de uma carteira para outra, todo o saldo precisa ser movido. Porém, se ele não for totalmente utilizado na transação, o restante volta como troco, como acontece quando você paga por um produto que custa menos do que o montante que tem à mão. A parte devida vai para o receptor e o restante é devolvido a você como troco.

Vejamos o caso da Transação 2. Roberto tinha inicialmente 0,005 BTC na carteira e precisou pagar uma conta de 0,003 BTC no restaurante. Como o valor pago é menor do que o disponível na carteira, o restante, descontada a taxa de transferência, volta para sua carteira (0,0018 BTC). Quanto ao estado de cada saída, temos duas possibilidades: gasto (spent) e não gasto (unspent). A primeira indica que aquele valor que existia em carteira já foi usado em uma nova transação, enquanto “não gasto” significa que o valor chegou à carteira e não foi movimentado ainda.

Voltando à transação em que Roberto solicitou o saque de 0,005 BTC de sua corretora, ao buscar pela operação no BlockCypher Explorer, ele encontrou o seguinte resultado:

#### 1 Transaction



Extraído de <https://live.blockcypher.com>

A imagem mostra que o endereço da corretora no momento do saque continha 32.63287219 BTC (input) e cinco saídas (outputs) foram geradas, sendo a primeira o troco e as outras quatro, pedidos de saque, incluindo o de Roberto, de 0,005 BTC. Note também que o troco está marcado como spent, pois novos saques já foram realizados da mesma carteira, fazendo com que o saldo fosse utilizado. Por outro lado, as quatro outras saídas geradas permanecem unspent, já que seus donos ainda não utilizaram os valores em novas transações. Por último, no canto superior direito da imagem, observe que já ocorreram mais de seis confirmações na rede. Portanto, essa transação pode ser considerada impossível de ser revertida.

Uma vez que uma transação é realizada, como no caso do saque que Roberto fez de sua corretora para sua carteira, ela é registrada na rede, para que os mineradores possam tomar conhecimento e, assim, algum deles a inclua no blockchain, validando-a. Dado que

a rede do Bitcoin é *peer-to-peer*, os usuários estão interconectados e uma informação como essa é facilmente propagada. Em linhas gerais, os dispositivos eletrônicos conectados à rede são chamados de “nós” (*Bitcoin nodes*) e conversam entre si por meio do protocolo Bitcoin. A informação sobre a operação de Roberto pode ser propagada pela rede fazendo-se uso da internet. Quando um nó recebe uma transação nova, ele a propaga para o restante dos nós, a fim de que todos tenham conhecimento dela.

## O DIA A DIA DOS MINERADORES

Como você já sabe, o Bitcoin surgiu como uma resposta à concentração do poder monetário nas mãos de grandes instituições financeiras globais. A descentralização talvez tenha sido a proposta mais genial de Satoshi Nakamoto. Ela cria uma rede de incentivos que permite haver confiança no processo de validação das transações, sem a necessidade de uma autoridade central.

Para que isso seja possível, os mineradores são um elemento crucial. São eles os responsáveis por autenticar cada nova transação e construir o registro do blockchain. Muitas pessoas acreditam que o principal papel dos mineradores é criar novas moedas de bitcoin. Essa é uma visão equivocada, uma vez que a criação de novas moedas é apenas o modelo de incentivo para os mineradores continuarem operando. Seu papel, de fato, é garantir o funcionamento da rede pela inclusão de novas transações em blocos, formando o próprio blockchain.

No processo de mineração mais conhecido, o Proof-of-Work (PoW), o que ocorre é uma incansável busca pela solução de um problema matemático complexo. O minerador, portanto, procura incluir novas transações em um bloco e encontrar uma solução matemática que o valide para ser adicionado à cadeia de blocos já existente. Todos os mineradores competem ao mesmo tempo por

essa solução, e aquele que primeiro encontrá-la é recompensado com as taxas de mineração e os novos bitcoins criados.

Antonopoulos utiliza um ótimo exemplo ilustrativo em seu livro. Segundo ele, o processo de mineração é como um enorme jogo de sudoku, com inúmeras linhas e colunas, em que todos os mineradores disputam entre si para encontrar a solução. Toda vez que alguém encontra uma solução, o jogo é “resetado” e uma nova busca é iniciada. Esse processo normalmente ocorre a cada dez minutos. Esse sudoku é um problema baseado em um hash criptográfico, assimetricamente difícil de resolver e fácil de verificar, com a dificuldade podendo ser ajustada.

O processo de mineração (PoW) ocorre da seguinte forma: conforme novas transações são geradas e enviadas à rede, cada nó as recebe e adiciona a uma pool temporária. As transações são consideradas não verificadas nesse caso, até que sejam de fato incluídas em um bloco válido. Então, cada minerador constrói um novo bloco que contenha essas transações, o hash do bloco anterior (o bloco-pai) e uma transação especial, que contém o pagamento da recompensa para seu próprio endereço. A partir daí, começa o processo de PoW para o novo bloco, em busca de sua solução. Se ela for encontrada, o bloco, bem como as transações contidas nele (incluindo a da recompensa), será considerado como válido e será inserido na sequência do blockchain.

Analizando mais detalhadamente os processos de mineração, observamos que ele funciona da seguinte forma: o hardware do minerador trabalha para encontrar uma solução para o algoritmo de PoW que faz com que o bloco seja válido. Isso significa encontrar um hash que seja válido para o bloco em questão. Para calcular o hash, é utilizada a função hash criptográfica SHA-256. Uma função como essa toma uma frase de qualquer tamanho e a transforma em uma sequência de caracteres de tamanho único. Cada frase gerará um hash completamente diferente. O resultado, portanto, é único.

Quando for minerar um novo bloco, o minerador terá um *target* (objetivo), que é uma sequência hexadecimal no formato de um hash. Como a sequência é hexadecimal, ela representa um número inteiro. Assim, o processo de mineração consiste em calcular a função hash criptográfica, repetidamente, para entradas aleatórias, até que a solução encontrada seja um número menor do que o target. Ser menor do que o target significa que existe um espectro menor de soluções possíveis. Conforme o tempo passa, a dificuldade pode ser ajustada, simplesmente elevando o target.

Esse ajuste se baseia na capacidade computacional empregada pelos mineradores ao longo do tempo, o chamado *hashrate*. Ele nada mais é que a taxa de hashes que são calculados pelos mineradores em um certo período de tempo. É de se esperar que, conforme o poder de processamento dos computadores aumenta, mais cálculos de hash por segundo podem ser feitos. Portanto, a dificuldade precisa ser ajustada ao longo do tempo para que a rede continue evoluindo de forma saudável.

Voltando para o processo de mineração, o minerador, portanto, precisará testar repetidamente vários cálculos até que encontre uma solução válida para o hash do bloco. Nesse momento, todos os outros nós (dispositivos) recebem esse novo bloco, o que invicia seu trabalho já realizado e faz com que precisem iniciá-lo novamente. Assim, apenas um minerador pode encontrar a solução por vez e receber a recompensa. Ela é reajustada pela metade a cada quatro anos, e atualmente é de 12,5 bitcoins. O próximo reajuste, conhecido como *halving*, será em 2020.

Apesar de, à primeira vista, a recompensa da mineração parecer interessante, é importante lembrar que é praticamente impossível um minerador, sozinho, receber o montante completo. Isso acontece porque, na verdade, os mineradores trabalham em grupos, conhecidos como *pools de mineração*, e somam esforços para encontrar novos blocos. Sendo assim, uma vez que a máquina mineradora de

um participante desse grupo encontra a solução, a recompensa é dividida proporcionalmente com todos os outros.

Esse trabalho constante dos mineradores, de verificar soluções e receber recompensas por isso, é o que confere ao Bitcoin a característica de descentralização, pois não há um órgão central único validando as transações e emitindo novas moedas. Além disso, como todos os nós da rede podem ter acesso a todo o histórico do blockchain, eles podem “auditar” o trabalho realizado pelos demais e garantir que não haja fraudes. O processo de mineração tradicional é chamado Proof-of-Work (Prova de Trabalho) justamente porque, para incluir um novo bloco no blockchain, é necessário provar o esforço computacional despendido para resolver o problema criptográfico.

Como dito anteriormente, a quantidade de bitcoins produzidos a cada novo bloco encontrado cai com o tempo, fazendo com que a moeda se torne cada vez mais escassa ao longo dos anos, até que, aproximadamente em 2140, toda a produção seja encerrada, após atingir 21 milhões de moedas produzidas. Na verdade, em 2032, mais de 99% dos bitcoins já terão sido minerados.

Como explicamos, a renda do minerador advém de uma combinação de novos bitcoins criados e taxas de mineração pagas pelos usuários para realizarem transações. Conforme o tempo passar, a remuneração por novos bitcoins ficará menor, enquanto a por taxas se tornará predominante. Sendo assim, a rede deverá se ajustar no longo prazo para que a atividade mineradora continue sendo viável. Lembre-se de que, para realizar o esforço computacional necessário para a mineração, o minerador precisa gastar energia elétrica, bem como investir em equipamentos e manutenção. Ou seja, estamos falando de um processo que precisa ter seus custos e ganhos balanceados ao longo do tempo.

## FORKS: A DIVISÃO (OU NÃO) DA REDE

Dissemos, até agora, que o bitcoin funciona de forma descentralizada. Para isso, é necessário haver consenso entre os participantes da rede, e que todos concordem com o conjunto de regras utilizado e mantenham a colaboração para continuar validando as transações. Mas o que ocorre quando nem todos concordam com as mesmas coisas? O protocolo do bitcoin, ou de qualquer outra criptomoeda, é um projeto em constante evolução e mudanças precisam ser feitas periodicamente. Porém, quando temos uma rede que funciona de forma descentralizada, as decisões precisam ser tomadas por consenso para definir os próximos passos do projeto. Só que, como sabemos que nem sempre haverá consenso, é necessária uma solução para esse caso também. É aí que entra a discussão sobre os *forks*.

Um fork é a divisão de um software em duas versões. A tradução de fork para o português (“bifurcação”) remete exatamente ao que acontece com um software como um protocolo criptográfico. Um protocolo pode se dividir, criando uma nova versão derivada dele e mantendo a cadeia original. Essa nova versão é considerada um *hard fork* da versão original. Ou seja, um hard fork ocorre quando parte da rede decide operar sob outro conjunto de regras de consenso. Com isso, decide-se criar uma derivação do protocolo original e as duas cadeias passam a se desenvolver de forma independente. Exemplo disso é o hard fork que criou o Bitcoin Cash. Um grupo de desenvolvedores não entrou em consenso sobre o formato segundo o qual o Bitcoin deveria continuar sendo desenvolvido e resolveu criar uma versão alternativa do software, com características próprias.

Contudo, nem sempre um fork resultará em uma completa divisão da rede. Existe, de fato, o *soft fork*, que é uma atualização do protocolo sem a derivação em uma segunda cadeia. Um soft fork é uma mudança nas regras de consenso que não altera

a compatibilidade da cadeia de blocos que será criada com a já existente. Sendo assim, cada fork que ocorre na rede de uma determinada criptomoeda deve ser analisado separadamente. E, para entender as diferenças entre as versões anterior e atual ou entre a versão original e a derivada, é necessário entrar em aspectos técnicos de software.

Do ponto de vista prático, para um detentor de criptomoedas, um hard fork resulta na criação de uma nova moeda que copiará todo o histórico do blockchain da moeda original. Seu protocolo também preservará a estrutura de chaves pública e privada preexistente e copiará esses valores em seu blockchain. Portanto, se você possuir, por exemplo, bitcoin em uma carteira com acesso às suas chaves privadas antes de um hard fork, poderá usar as mesmas chaves privadas para acessar o saldo da nova moeda, que foi replicado de modo idêntico no novo blockchain.

Em vista da similaridade de estrutura dos dois blockchains (o antigo e o novo), é necessário ter atenção ao realizar transferências, pois as estruturas de endereço de ambas as redes serão semelhantes, e enviar uma moeda para um endereço de outra derivada dela (por exemplo, enviar uma moeda da rede antiga para um endereço da rede nova) pode resultar em perda permanente do valor. Além disso, é importante, como medida de segurança, evitar expor sua chave privada a terceiros, a menos que seja para sincronizá-la com uma carteira que dê suporte à nova moeda e que seja confiável.

## **SEGURANÇA E ARMAZENAMENTO: CONTROLE DAS CHAVES**

No universo das criptomoedas, não há um custodiante ou órgão que defina qual moeda pertence a quem. Isso quer dizer que um bitcoin que você possua, por exemplo, não está ligado ao seu nome, à sua identidade. Na realidade, um saldo em bitcoins está ligado à

chave privada relacionada a ele. Qualquer pessoa que possua acesso à chave privada terá acesso também ao saldo a ela correspondente. Entenda o “armazenamento” do bitcoin (para outras criptomoedas acontece de forma similar) como um cofre que possui uma chave. Porém não há nenhuma identificação nesse cofre que o ligue a você. Ele não está em um banco, nem ligado a nenhuma identidade. Existe apenas uma chave capaz de abrir a porta do cofre e, se você a possui, passa a ser o dono do conteúdo (no caso, dos bitcoins).

Chamamos essa “chave do cofre” de chave privada. Ela é a chave usada para assinar as transações no blockchain ou, se preferir, é sua senha para confirmar transações. Entender o funcionamento do par chave pública/chave privada é essencial para entender como funciona a “posse” de bitcoins. Como disse, uma chave privada é uma senha. Trata-se de uma sequência de números, em formato hexadecimal, com 64 caracteres, ou seja, 256 bits. Você pode, aliás, criar sua própria chave privada, escolhendo 256 números entre 0 e 1 aleatoriamente e formando uma sequência de bits. Porém, as wallets e os programas especializados em criação de chaves privadas usam métodos mais robustos de seleção de números randômicos.

Como a chave privada é utilizada para atribuir “posse” às moedas a ela relacionada, é extremamente importante que seja mantida em segredo e não compartilhada com ninguém. Por meio da chave privada, gera-se uma chave pública. Essa, sim, pode ser divulgada, e é usada para construir o endereço público utilizado para receber transações.

Antonopoulos explica em seu livro como funciona o processo de geração da chave pública a partir da chave privada e do endereço público a partir da chave pública. Trata-se de uma sequência de funções de apenas uma via, que funcionam como um alçapão: é possível ir em um sentido, mas não no contrário. À chave privada, gerada randomicamente, é aplicada uma função criptográfica elíptica (função de apenas uma via) para gerar a chave pública.

À chave pública, por sua vez, aplica-se uma função hash criptográfica (também de uma via, como aquela explicada na seção sobre blockchain deste apêndice), que gerará um endereço público. O esquema a seguir mostra como são gerados as chaves e o endereço.



Extraído de ANTONOPOULOS, 2017.

Assim, a partir de uma chave privada é possível derivar um endereço público, mas, sabendo o endereço público, é impossível reconstruir a chave privada. É aqui, de fato, que reside o poder da criptografia no bitcoin.

Para transacionar valores na rede do bitcoin, portanto, é necessário ter a posse do par de chaves pública e privada. Para guardar esse par, utiliza-se um software de wallet. A denominação *wallet* traz consigo uma conotação errada, pois faz parecer que os fundos em si estão armazenados na carteira. Na realidade, a wallet é um chaveiro, pois guarda apenas o par de chaves pública e privada e, com ele, consegue acessar seus fundos no blockchain, exibi-los na tela e assinar transações para que você seja capaz de movimentar os fundos de um endereço para outro.

Lembre-se de que as chaves privadas garantem acesso aos seus bitcoins. A posse das chaves privadas é essencial para ter total controle sobre seu dinheiro. Por isso, sempre que tiver um valor elevado, procure utilizar métodos seguros de armazenamento de suas chaves privadas, especialmente por meio de hardware wallets, carteiras físicas que podem ficar desconectadas da internet e constituem o que chamamos de cold storage (em contraposição às carteiras via aplicativos, que permanecem conectadas à internet).

## ENTENDENDO AS OUTRAS CRIPTOMOEDAS

Neste apêndice, utilizamos o Bitcoin como exemplo para explicar os detalhes técnicos que são essenciais para entender o funcionamento de uma criptomoeda. Os outros protocolos, de certa forma, derivaram da concepção original do Bitcoin. Porém, com tantas variações existentes, diversos caminhos foram trilhados e surgiram propostas das mais variadas. Para entender como funciona uma outra criptomoeda, é importante entender seus detalhes técnicos, analisando os aspectos discutidos aqui. Os modelos criptográficos, as regras de consenso e a tecnologia envolvida podem variar, mas a essência permanece similar.

Espero que essa visão geral sobre o Bitcoin ajude os leitores a gostarem ainda mais das criptomoedas, bem como os motive a continuar estudando outros protocolos e outras abordagens de ativos criptográficos.





# GLOSSÁRIO

**Alavancagem:** endividamento para conseguir investir mais do que se tem, com o objetivo de apurar maiores lucros.

**Alocação:** destinação de verbas a determinados investimentos.

**Altcoin:** termo que se refere a todas as moedas, menos o bitcoin.

**Ativo:** termo usado para descrever bens, tais como propriedades ou investimentos.

**Ativo criptográfico:** ativo digital criado a partir de estruturas criptográficas.

**Ativo digital:** ativo que existe de maneira digital, mas que pode ter como referência um ativo físico.

**Ativo físico:** ativo que existe como matéria física, como é o caso de um apartamento ou uma casa.

**Ativos tradicionais:** ativos já consolidados no mercado, negociados há mais de décadas pelas corretoras.

**Bailout:** injeção de capital em uma entidade para evitar que esta venha a falir e para permitir que possa honrar seus compromissos.

**Bitcoin:** protocolo de transferência de dinheiro eletrônico ponto a ponto, criado por Satoshi Nakamoto. Quando grafado com inicial maiúscula, o termo “Bitcoin” se refere ao protocolo. Quando grafado com inicial minúscula, bitcoin, faz referência à criptomoeda que é transacionada dentro da rede.

**Blockchain:** tecnologia que sustenta todo o protocolo Bitcoin e registra todas as transações efetuadas na rede. Também é utilizada como base para diversos outros criptoativos.

**Blocos:** elementos constituintes do blockchain. Um bloco consiste em um conjunto de informações estruturadas que reúne detalhes, principalmente sobre as transações realizadas na rede de uma determinada criptomoeda.

**Blocos minerados:** blocos que já foram “validados” pelos mineradores.

**Bolha (ou bolha econômica):** efeito de supervalorização de um ativo, que ultrapassa seu valor justo.

**BTC:** código que designa o bitcoin, similar aos tickers de ações de empresas.

**Bull market:** mercado com tendência de alta.

**Buy-and-hold:** estratégia de investimento em que um ativo é comprado e mantido em carteira por tempo indeterminado.

**Carteira:** local no qual se armazenam as chaves públicas e privadas que dão acesso aos saldos em criptomoedas. A mesma coisa que *wallet*.

**Chave privada:** sequência alfanumérica que permite acessar e controlar o saldo em criptomoeda a ela associado. Dada sua função, não deve ser compartilhada. É usada para gerar a chave pública.

**Chave pública:** sequência alfanumérica derivada da chave privada, e que, diferentemente desta, pode ser exposta e divulgada. É usada para gerar o endereço público de uma carteira.

**Commodities digitais:** recursos digitais que servem para criar ou chegar a produtos digitais finais.

**Commodity:** bem em estado mais bruto, com pouco acabamento ou beneficiamento.

**Corretora:** empresa responsável por intermediar a compra e venda de ativos. No contexto de criptoativos, a mesma coisa que *exchange*.

**Criptoativos:** todos os ativos em que, de alguma forma, é utilizada criptografia, seja para sua criação, seja para seu uso.

**Criptocommodities:** commodities digitais criadas com o emprego de criptografia.

**Criptoconomia:** economia que surgiu com o advento dos cripto-ativos.

**Criptografia:** estudo dos princípios e técnicas usados para transformar uma informação legível em ilegível, a não ser para quem detém a chave capaz de decifrá-la.

**Criptomoedas:** classe de ativos digitais das moedas criptografadas, como o bitcoin e o litecoin.

**Criptotokens:** tokens digitais que utilizam a criptografia em suas redes de distribuição.

**Custodiante:** empresa ou pessoa que detém a posse de algum bem e é responsável por sua segurança.

**Deep web:** camada mais profunda da internet que está fora do alcance de qualquer regulação e serve a propósitos ilegais em boa parte dos casos.

**Dinheiro fiduciário:** dinheiro cujo valor depende da confiança ou fé que nele é depositada.

**Early adopters:** usuários que adotam uma inovação muito antes da maioria das pessoas.

**Equity token:** token que, assim como uma ação, representa uma parte de uma empresa.

**Ether:** criptocommodity que funciona dentro da rede Ethereum.

**Ethereum:** plataforma cujo objetivo é ser um imenso computador descentralizado que permita processar qualquer aplicação na rede.

**Exchange:** ver *corretora*.

**Fork:** bifurcação ou separação de uma rede.

**Função hash criptográfica:** algoritmo computacional capaz de criptografar uma mensagem.

**Halving:** característica inerente ao código do bitcoin, de acordo com a qual a quantidade de bitcoins produzida cai pela metade a cada quatro anos.

**Hard fork:** fork que gera uma nova versão de uma rede, derivada da original.

**Hard wallets:** carteira que armazena em um dispositivo físico parecido com um pendrive as chaves privadas de um determinado criptoativo.

**Hash:** mensagem criptografada que é produto da aplicação de uma função hash criptográfica a uma mensagem (sequência de caracteres).

**Hashrate:** poder de processamento das máquinas de mineração.

**ICO (Initial Coin Offering):** processo de oferta pública em que uma nova moeda, token ou ativo é oferecido a investidores.

**Lastro:** garantia implícita de um ativo.

**Liquidex:** capacidade que um ativo tem de ser convertido em dinheiro.

**Market cap:** estimativa de valor de um ativo feita a partir da soma do valor de suas pequenas partes que estão no mercado.

**Market drawdown:** período em que o mercado se encontra em baixa em relação ao momento anterior recente.

**Mineração:** atividade realizada pelos mineradores para validar as transações que ocorrem na rede de uma criptomoeda. Como recompensa, geram novas moedas.

**Mineradores:** agentes do ecossistema do Bitcoin responsáveis por validar as transações que ocorrem na rede da criptomoeda em troca

de uma remuneração. Outros protocolos também utilizam a figura do minerador.

**Moedas digitais:** moedas ou ativos que existem apenas no formato digital.

**Multiwallet:** carteira que armazena as chaves privadas de vários criptoativos em apenas um local.

**Paper wallet:** carteira que permite guardar as chaves privadas em uma impressão em papel.

**Peer-to-peer:** formato de rede descentralizado, em que todos os pontos podem se comunicar entre si.

**Pools de mineração:** locais virtuais em que vários mineradores se juntam para compartilhar hashrate e conseguir minerar criptomoedas.

**Portfólio:** conjunto de ativos que fazem parte de uma carteira de investimento.

**PoW (Proof-of-Work):** modelo de consenso em que o minerador precisa despender poder computacional para chegar à solução de um problema matemático que valida um bloco de transações com criptomoedas. Em português, Prova de Trabalho.

**Protocolo (criptográfico):** conjunto de informações e regras que regem um modelo criptográfico.

**Protocolo Bitcoin:** conjunto de regras e princípios que regem a rede do bitcoin.

**Protocolo-base:** conjunto de regras e princípios que originam uma aplicação técnica.

**Satoshi Nakamoto:** responsável por propor o Bitcoin como sistema ponto a ponto de pagamentos com dinheiro eletrônico.

**Smart contract:** contrato inteligente que funciona sem a necessidade de um intermediário que garanta seu cumprimento.

**Soft fork:** fork executado com consenso, mantendo apenas uma rede e aplicando a ela as atualizações propostas.

**Soft wallet:** carteira que armazena as chaves privadas de um determinado criptoativo em um software, como um aplicativo em um dispositivo.

**Token:** representação, em forma de ficha, de uma quantia em dinheiro.

**Trader:** indivíduo que realiza tradings.

**Trading:** operação de compra ou de venda de ativos que visa obter lucros no curto prazo.

**Utility token:** token utilizado como uma representação de dinheiro em um ecossistema.

**Wallet:** ver *carteira*.

**White paper:** no mercado de ativos digitais, documento padrão para apresentar um criptoativo.

**Zk-SNARK:** sigla de *zero-knowledge Succinct Non-Interactive Argument of Knowledge*. Tecnologia utilizada para conferir privacidade às transações de algumas criptomoedas existentes.





## *REFERÊNCIAS*

ANTONOPOULOS, Andreas M. *Mastering Bitcoin: programming the open blockchain*. 2nd ed. Sebastopol: O'Reilly Media, 2017.

BURNISKE, Chris; TATAR, Jack. *Cryptoassets: the innovative investor's guide to Bitcoin and beyond*. New York: McGraw-Hill Professional, 2017.

BURNISKE, Chris; WHITE, Adam. *Bitcoin: ringing the bell for a new asset class*, 2017. Disponível em: <[https://research.ark-invest.com/hubfs/1\\_Download\\_Files\\_ARK-Invest/White\\_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf](https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf)>. Acesso em: 12 jan. 2018.

FERGUSON, Niall. *A ascensão do dinheiro*. 2ª ed. São Paulo: Crítica, 2017.

GEEST, Yuri Van; ISMAIL, Salim; MALONE, Michael S. *Organizações exponenciais*. São Paulo: Hsm Editora, 2015.

GLADWELL, Malcolm. *O ponto da virada*. Rio de Janeiro: Sextante, 2009.

MANSARAMANI, Vikram. *Boombustology: spotting financial bubbles before they burst*. Hoboken: John Wiley Trade, 2011.

NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer electronic cash system*. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 12 jan. 2018.

RICKARDS, James. *A grande queda: como aumentar o seu patrimônio no colapso por vir*. São Paulo: Empiricus Research, 2015.

ROGERS, Everett M. *Diffusion of innovations*. 5th ed. New York: Free Pass, 2003.

TALEB, Nassim N. *Antifrágil: coisas que se beneficiam com o caos*. 1ª ed. Rio de Janeiro: Best Business, 2014.

TAPSCOTT, Alex; TAPSCOTT, Don. *Blockchain revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo*. São Paulo: SENAI-SP Editora, 2016.

VERSIGNASSI, Alexandre. *Crash: uma breve história da Economia — da Grécia Antiga ao século XXI*. 2ª ed. São Paulo: Leya, 2015.

## MELHOR QUE DINHEIRO?

Entendemos o surgimento das criptomoedas como uma inovação tecnológica que caminha para a adoção em larga escala. Nossa intuito é mostrar ao leitor o que está por trás de cada novo projeto e quais são as formas de investir nesse mercado.

Ao longo deste livro, você entenderá como surgiram as criptomoedas, o que elas representam, por que temos tanta convicção em seu sucesso no longo prazo e quais são as outras classes de ativos nesse mercado que podem assumir papéis muito além do meramente financeiro.

Ao fim da leitura, você perceberá que as criptomoedas são muito mais do que aquilo que a mídia divulga.

Este pode ser um caminho sem volta. E, sinceramente, esperamos que seja.

