FIAP ON

ENSINO A DISTÂNCIA

SOLUÇÕES TECNOLÓGICAS EMERGENTES

BITCOIN & BLOCKCHAIN

Henrique Poyatos

CAPÍTULO 2

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

2 BITCOIN & BLOCKCHAIN

2.1 A Revolução do dinheiro

Você certamente já ouviu falar em Bitcoin. Talvez tenha ouvido dizer que se trata de um dinheiro virtual utilizado por hackers que invadem e sequestram as máquinas das empresas e pedem um resgate (o chamado *Ransomware*), ou talvez tenha ouvido que o utilizam na *Deep Web* para negócios ilícitos, ou alguém lhe disse ganhar muito dinheiro com sua alta de preço ou minerando bitcoins. Quem sabe você talvez já tenha "googlado" procurando por bitcoins, e achou esse assunto muito complicado. Bem, tudo isso de que você já ouviu falar está meio certo, mas também meio errado; o bitcoin é algo que vai muito além disso.

O bitcoin é a mais fascinante experiência financeira já criada na história da humanidade, e lhe explicamos o porquê.

A necessidade de algo que atue como marcador de valor para trocas de bens e serviços remete a milênios. No começo, foram utilizados elementos que possuíam um valor intrínseco, como grãos, sementes (como a do cacau) ou sal: eles podiam ser usados para trocas ou mesmo utilizados. Posteriormente, foram utilizados elementos que eram raros e escassos, como é o caso do ouro. Por sua dificuldade ao ser transportado, rapidamente foram cunhadas moedas, que eram atestadas por um rei (e posteriormente governos) e representavam a promessa de troca. Assim sendo, duas pessoas que não se conheciam e, portanto, não confiavam uma na outra, poderiam efetuar trocas, pois ambas atribuíam à moeda algo de valor, mesmo que ela não possuísse um valor intrínseco. Esses dois negociantes sabiam que outras pessoas confiavam na mesma moeda, e ela se transformava, portanto, em uma promessa para a troca futura.

Figura 2.1 – Dinheiro usado na troca por bens e serviços
Fonte: Banco de imagens Shutterstock (2017)

Se, antigamente, títulos de valor eram representantes de um bem preciso como ouro ou prata, ou seja, eram lastreados, o papel-moeda atual é estabelecido por um reinado, governo ou nação, que atesta seu valor e chamamos isso de moeda fiduciária. É o caso do real, dólar ou euro: o valor do dinheiro é baseado na confiança que temos na instituição que o emite.

O grande problema das moedas fiduciárias é justamente o fato de terem instituições centrais que as controlam: se essas instituições (ou nações) perdem sua fé pública, a moeda por elas controlada também perde seu valor. Passamos por isso no Brasil, após diversas trocas de moeda e assistimos a reprises desse filme em outros países, com uma frequência incômoda. Além disso, tais nações controlam a moeda e, se isso estiver dentro de seus interesses, podem emitir mais dinheiro, resultando invariavelmente em um processo de inflação e perda do poder de compra por parte da população.

O sistema financeiro moderno precisa, portanto, de nações que emitam o dinheiro e lhe atribuam valor (e cidadãos que acreditem nesse valor) e instituições bancárias que assumam pelo menos duas funções importantes: guardem nosso dinheiro para nós (pois custodiar o próprio dinheiro é um processo muito caro) e garantam a confiança na transferência de valores de uma pessoa para outra, especialmente neste mundo tecnológico no qual o dinheiro em raras ocasiões é materializado, ou seja, se torna papel-moeda.

E se eu lhe disser que a mera existência do bitcoin desafia essa lógica?

2.2 O que é o bitcoin?

O bitcoin não é uma moeda em sua definição clássica, isso porque não foi emitido por nenhum reino ou nação: trata-se da primeira vez que o próprio povo "cunhou uma moeda". Seu nascimento data de menos de uma década, em 31 de outubro de 2008, Satoshi Nakamoto publicou, em uma lista on-line de criptografia, um *paper* cujo título é (em tradução livre): "Bitcoin: o sistema de dinheiro eletrônico *peer-to-peer*". Ele propunha um experimento tecnológico, financeiro e bancário: uma moeda totalmente digital, que não pudesse ser duplicada (ou gasta duas vezes), em um sistema descentralizado de confiança, ou seja, não exigiria uma entidade central para emitir o dinheiro e validar as transações.

A proposta ousada de não haver uma entidade central resolveria duas questões importantes: primeiro, não haveria uma entidade central que, mediante ao seu próprio interesse, pudesse emitir mais dinheiro e inflacionar o mercado, o sistema de Satoshi deveria emitir as moedas regularmente (a cada dez minutos) em uma taxa constante. Na verdade, a cada quatro anos, essa taxa cairia pela metade sistematicamente, simulando uma escassez artificial, característica fundamental em uma moeda.

Além disso, não haveria uma entidade central que pudesse ser atacada ou ter sua confiança abalada: por ser baseado em uma rede P2P, sem servidores centrais como acontece com uma rede Tor ou no Bittorren, o sistema não pode ser derrubado.

Poucos meses depois, às 18h15 de 3 de janeiro de 2009, a primeira transação no chamado bloco gênese do bitcoin foi registrada em seu blockchain.

A transação acompanhava a seguinte mensagem: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*". A alusão à manchete do jornal britânico *The Times* é uma clara crítica ao caos financeiro da época, quando o mundo passava por uma crise econômica mundial.

Figura 2.2 – O “B” cifrado que se tornou o símbolo do Bitcoin.
Fonte: Fortune (2017)

O bitcoin é, portanto, um ativo financeiro que funciona como uma moeda, transacionado em uma rede descentralizada, utilizando um software de código fonte-aberto. Outra denominação comum para o bitcoin é ser uma criptomoeda, que é uma moeda protegida por criptografia.

2.3 Como ele funciona?

Para se utilizar os bitcoins, é necessário criar carteiras virtuais com softwares específicos para isso. Essas carteiras, por sua vez, são ligadas à rede bitcoin e, toda vez que uma quantia de bitcoins é transferida de uma carteira a outra, a transação deve ser registrada em um bloco de transações que, quando validado, é ligado a uma corrente de blocos que é batizada de blockchain. Trata-se de um imenso livro-razão, que registra todas as transações de bitcoin da história, de sua primeira em 2009 até a última. É como se houvesse um extrato bancário universal, registrando todas as remessas de dinheiro que vão de um lado a outro, e qualquer pessoa no mundo pudesse olhar.

Figura 2.3 – Analogia ao blockchain, um livro-razão com todas as transações de uma criptomoeda
Fonte: Banco de imagens Shutterstock (2017)

Agora, como esses blocos são validados?

Eles, por sua vez, são validados por mineradores, que são máquinas do tipo servidores que, a cada dez minutos, participam de uma espécie de “corrida”. É proposto a eles a solução de um problema matemático complexo, que deve empregar um grande poder computacional para resolvê-lo. A esse problema, é dado o nome de prova de trabalho (*proof of work*). Por se tratar de uma corrida, a cada dez minutos um único minerador acha a resposta para esse problema primeiro, e se torna o descobridor do bloco.

Ao vencedor, é dado o direito de escolher quais transações da rede serão validadas nesse bloco, que possui um limite. O bloco é registrado no final da corrente e é dado ao minerador uma recompensa em bitcoins. É por essa razão que esse papel é chamado de “minerador”, ele “minera” novos bitcoins a cada bloco descoberto.

Esse prêmio, no início da rede era de 50 bitcoins. Ou seja, 50 bitcoins eram minerados a cada dez minutos. No entanto, a cada quatro anos, essa recompensa cai pela metade: caiu em 2012 para 25 bitcoins por bloco, em 2015 caiu para 12,5 bitcoins, depois caiu para 6,25 depois e assim sucessivamente, e estimamos que em 140 anos o último bitcoin será minerado. Por ter uma taxa de geração constante, estima-se que, em vez da inflação observada em moedas fiduciárias pela sua emissão desenfreada, o que se observa é uma deflação por sua escassez artificial, característica essencial para qualquer tipo de moeda.

Embora não sejam recompensados, os outros mineradores que “perderam a corrida” precisam validar o problema matemático, registrar e validar o bloco descoberto pelo vencedor, pois, afinal, é uma corrente: não se pode partir para o bloco seguinte sem passar por todos os elos dessa corrente. Assim, milhares de mineradores validam o mesmo bloco e, portanto, o mesmo conjunto de transações.

Diferente do sistema bancário tradicional, no qual temos a confiança baseada em entidade central (um banco), validando uma transferência bancária de um correntista para outro, no caso do sistema de bitcoin temos o que chamamos de confiança descentralizada baseada em consenso, pois temos várias entidades que, empregando muito poder computacional (e, portanto, gastando dinheiro), validam as mesmas “transações bancárias”, garantindo a confiança no sistema.

O saldo das pessoas em bitcoins é, portanto, o total de adições ou subtrações que tenham como destinatário ou remetente a carteira virtual do usuário. O bitcoin não é, portanto, um arquivo digital que possa ser duplicado e gasto duas vezes (fraude financeira conhecida como *double spending*).

Cada minerador possui uma cópia completa do blockchain em sua máquina, garantindo que esses registros não possam ser perdidos. Graças ao sistema em corrente, se um único bloco fosse adulterado de alguma forma, toda a cadeia de blocos dali por diante precisaria ser revalidada, gerando uma cadeia totalmente divergente, que seria rejeitada pelos outros mineradores. Por essa razão, é virtualmente impossível adulterar o blockchain, tornando-o inviolável.

2.4 Como adquirir bitcoins?

Um assunto importante em relação ao bitcoin é como adquiri-lo, afinal, você provavelmente não recebe seu salário em bitcoins, embora isso esteja se tornando cada vez mais comum, especialmente para profissionais que trabalham no Brasil, prestando serviço diretamente a empresas fora de nosso país.

Você pode adquirir bitcoins de qualquer pessoa que possua bitcoins e esteja interessada em vendê-los em troca de uma moeda fiduciária, como o real, dólar ou euro. No entanto, com o objetivo de aproximar compradores de vendedores, foram criadas as *exchanges*.

Exchanges são empresas que fazem o papel de uma casa de câmbio no ecossistema do bitcoin, permitindo que possamos “transformar” reais em bitcoin. A diferença em relação às casas de câmbio é que as *exchanges* não vendem bitcoins diretamente. Elas atuam como intermediárias, anunciando a venda de bitcoins de outras pessoas e, por essa razão, elas atuam de forma muito semelhante a uma bolsa de valores.

O valor de um bitcoin é totalmente regido por sua oferta e procura e, como em qualquer ativo financeiro, altamente influenciado pela confiança que as pessoas depositam nele. Por ser algo muito novo, seu valor é altamente volátil, e pode variar em centenas de reais em um único dia. Por essa razão, recomenda-se cautela caso você se interesse em trabalhar com esse ativo. Conforme um maior número de pessoas comece a se interessar por ele, adquiri-lo e aceitá-lo, mais estável seu preço se tornará. É um fato que seu valor hoje flutua menos do que flutuava no passado.

Em território nacional, um dos exemplos que temos de *exchange* é a Foxbit (http://www.foxbit.com.br/), e uma que tem ganhado muito destaque internacional é a polonesa Poloniex (http://www.poloniex.com/), especialmente pela possibilidade de comerciar outras moedas digitais.

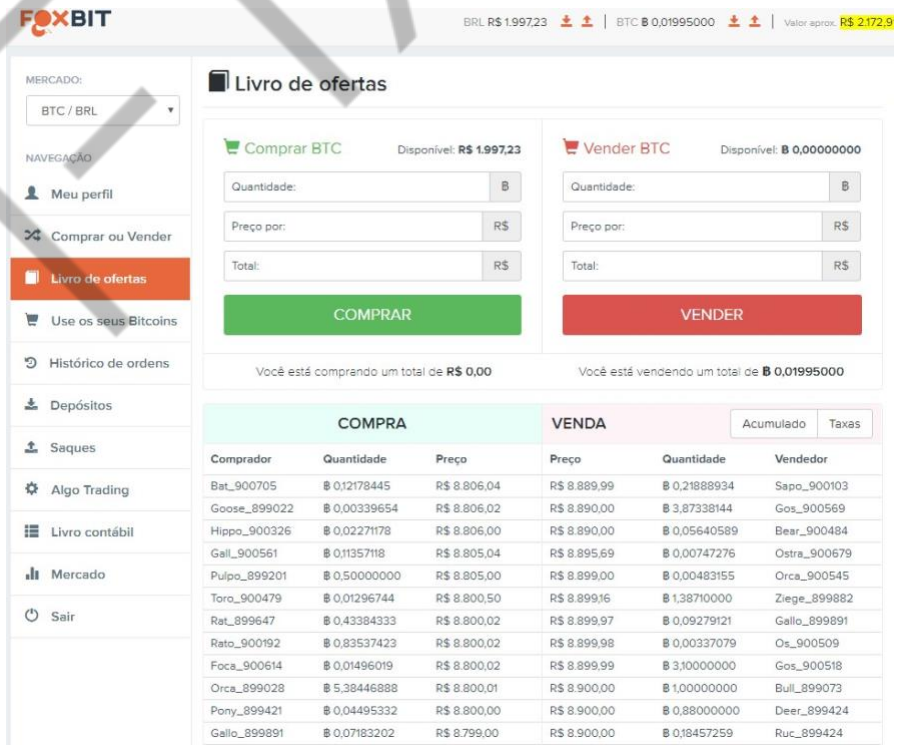

Figura 2.4 – Tela de ofertas em bitcoin da *exchange* brasileira Foxbit
Fonte: Elaborado pelo autor (2017)

Figura 2.5 – Tela da *exchange* polonesa Poloniex
Fonte: Elaborado pelo autor (2017)

Como uma única unidade de bitcoin possui um valor muito alto para ser adquirida por inteiro ou mesmo gastá-la por completo, é possível comprar frações de bitcoins até a sua oitava casa decimal, conhecida como “satoshi”, em homenagem ao criador do bitcoin, Satoshi Nakamoto. Um satoshi é a menor quantidade do sistema, representando 0,00000001 bitcoin, ou um centésimo de milionésimo de um bitcoin.

2.5 Como armazenar bitcoins?

O armazenamento desse ativo é outro assunto da extrema importância. Uma grande diferença do bitcoin em relação a outros ativos é a possibilidade de fazer a custódia dele com baixo ou nenhum custo, afinal, estocar ouro ou dinheiro em espécie em casa requer um alto investimento para evitar furto ou acidentes e é exatamente por essa razão que confiamos em instituições bancárias.

Como sabemos, grandes concentrações de dinheiro despertam a cobiça; assim como bancos são constantes alvos de furtos físicos ou tentativas de invasão, *exchanges* também se tornam alvos de hackers, assim sendo, manter seus bitcoins dentro da exchange é algo que as próprias empresas desaconselham. Se a Exchange for invadida, há um grande risco de não conseguir honrar os saques de seus clientes, como já aconteceu no passado com a *exchange* japonesa Mt Gox.

Além disso, por serem empresas reais sediadas em seus países, elas são obrigadas a cumprir leis e eventuais sanções.

Para dar um **exemplo**, por um breve período, o governo chinês impôs limites para os saques em *exchanges* chinesas, causando um transtorno aos seus clientes.

Por tudo que foi abordado aqui, o melhor lugar para seus bitcoins ficarem é com você mesmo.

O sistema do bitcoin permite a criação de carteiras virtuais que armazenam o ativo de maneira prática e segura e é algo que podemos fazer de maneira totalmente gratuita.

A criação de uma carteira segue o modelo de criptografia de chave público-privada, uma tecnologia que existe há décadas. O processo consiste em gerar duas chaves de segurança, uma pública e outra privada. Como o nome indica, uma dessas chaves é pública e deve ser divulgada para o maior número de pessoas possível, enquanto a outra deve ser mantida de forma secreta e segura.

Um **exemplo** para ficar claro: Alice gera seu par de chaves e Bob também gera o seu par de chaves, pública e privada. Alice e Bob trocam suas chaves públicas, divulgando essas chaves um para o outro.

Quando Alice precisa mandar uma mensagem cifrada para Bob, ela assina sua mensagem com sua chave privada e a chave pública de Bob, já que a mensagem tem a ele como destinatário. Para decifrar a mensagem enviada por Alice, Bob utiliza sua chave privada e a chave pública de Alice, revelando o conteúdo da mensagem.

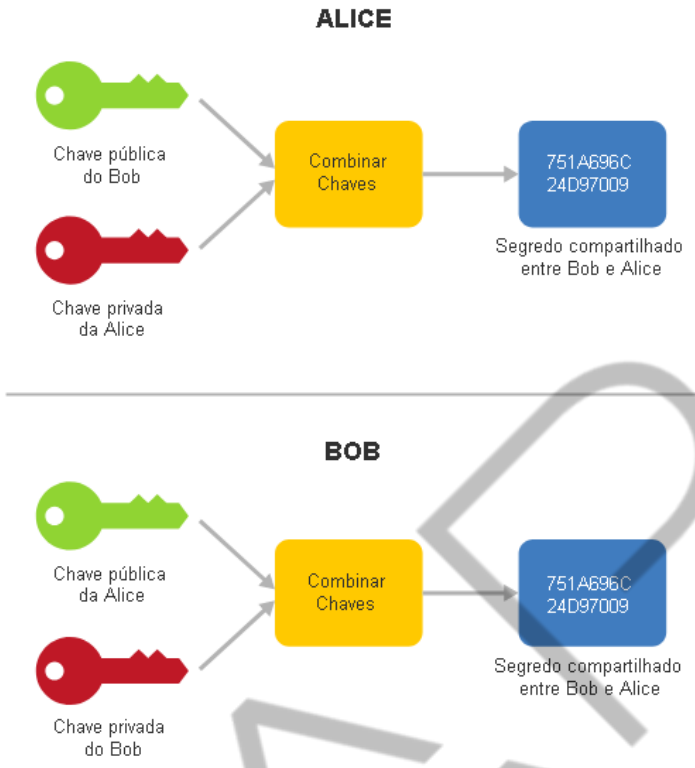

Figura 2.6 – Exemplo de criptografia em chave público-privada
Fonte: Elaborado pelo autor (2017)

Curiosamente, Alice é incapaz de decifrar a própria mensagem: apenas Bob com a combinação de chaves mencionada (sua privada e a pública dela) consegue fazer isso.

Pois bem, o sistema de carteiras presente no bitcoin utiliza o mesmo conceito: quando criamos uma carteira virtual (ou *wallet*), são geradas uma chave pública e uma chave privada. A chave pública é conhecida como o endereço da carteira virtual e, por ser uma sequência de alfanuméricos (letras, números e símbolos) relativamente extensa, geralmente é divulgada por meio de um QRCode. Para efeito de demonstração, “1CU3qXYCwbHC4A7vNcW9d5rdmGCs7KC9EH” é a chave pública/endereço de uma carteira real. A Figura 2.7 é a representação desse alfanumérico em QRCode:

Figura 2.7 – Endereço de uma carteira virtual em formato QRCode
Fonte: Elaborado pelo autor (2017)

Para movimentar os valores contidos nessa carteira ou *wallet*, deve-se utilizar a chave privada, que faz par com a chave pública. As transações de transferências de bitcoin são, portanto, assinadas com a chave privada da carteira, e a chave pública (ou endereço) da carteira de destino, e tais movimentações ficam registradas no blockchain de forma pública e para todo o sempre.

A segurança de uma carteira reside na complexidade da frase-senha utilizada na geração do par de chaves. Todas as regras de segurança em relação a senhas são aplicáveis aqui: não utilizar palavras presentes em qualquer idioma, intercalar com números, símbolos, letras maiúsculas e minúsculas, e quanto mais extensa, melhor.

2.5.1 Carteiras via software

Em geral, os softwares utilizados na geração das carteiras utilizam 12 palavras do idioma inglês (conhecidas como *seed*, ou semente) e a frase-senha mencionada. Em posse desses dois itens, uma carteira que estivesse configurada em um computador ou smartphone perdidos poderia ser recuperada.

Diferente de um sistema bancário, em que posso me dirigir a uma agência de meu banco ao perder ou esquecer minha senha, uma carteira tradicional de bitcoin sem sua senha estará perdida para todo o sempre; o dono da carteira é, literalmente, o único a conhecer sua senha e é aí que reside a segurança do sistema e o conceito de custódia própria.

Exceções existem, como é o caso da carteira web/smartphone da empresa Coinbase. No entanto, a Coinbase disponibiliza a seus usuários um login e senha para seu sistema e fica com o par de chaves das carteiras ali geradas, sendo assim, a praticidade nesse caso corresponde ao risco de se compartilhar o par de chaves com terceiros.

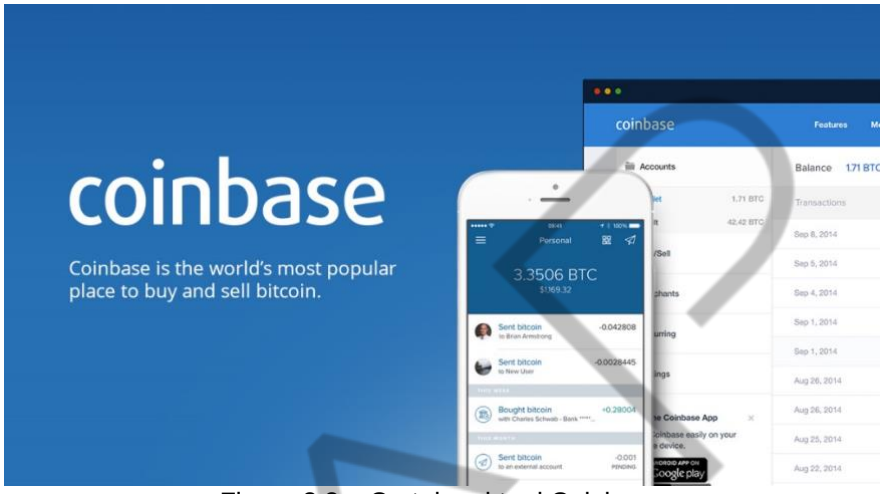

Figura 2.8 – Carteira virtual Coinbase
Fonte: Coinbase.com (2017)

Outros softwares de carteira, como é o caso da carteira da Electrum, são mais recomendados, pois o par de chaves é gerado e conhecido apenas pelo dono da carteira:

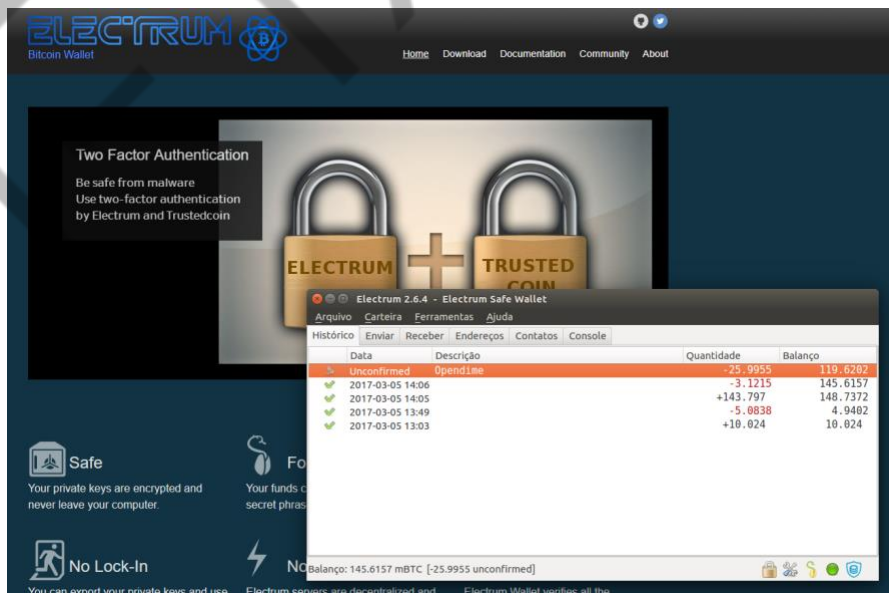

Figura 2.9 – Carteira virtual Electrum
Fonte: Elaborado pelo autor (2017)

Por ser possível gerar quantas carteiras quisermos sem qualquer tipo de custo, é aconselhável criar várias delas com senhas diferentes, minimizando o

prejuízo caso a senha seja perdida ou descoberta por um terceiro. Nesse caso, a máxima “Não coloque todos os ovos em uma mesma cesta” é totalmente aplicável.

2.5.2 Carteiras via hardware

Existe a possibilidade de ser utilizada uma carteira gerada via hardware (*hardware wallet*). Trata-se, costumeiramente, de um dispositivo semelhante a um *pendrive*, desenvolvido especificamente para esse fim. Essa abordagem é interessante, pois o hardware pode gerar e armazenar, de forma muito prática, uma senha extremamente complexa, aumentando muito o nível de segurança. O risco reside, no entanto, nas possibilidades de perda, furto ou dano do dispositivo, portanto, cópias de segurança são sempre aconselháveis.

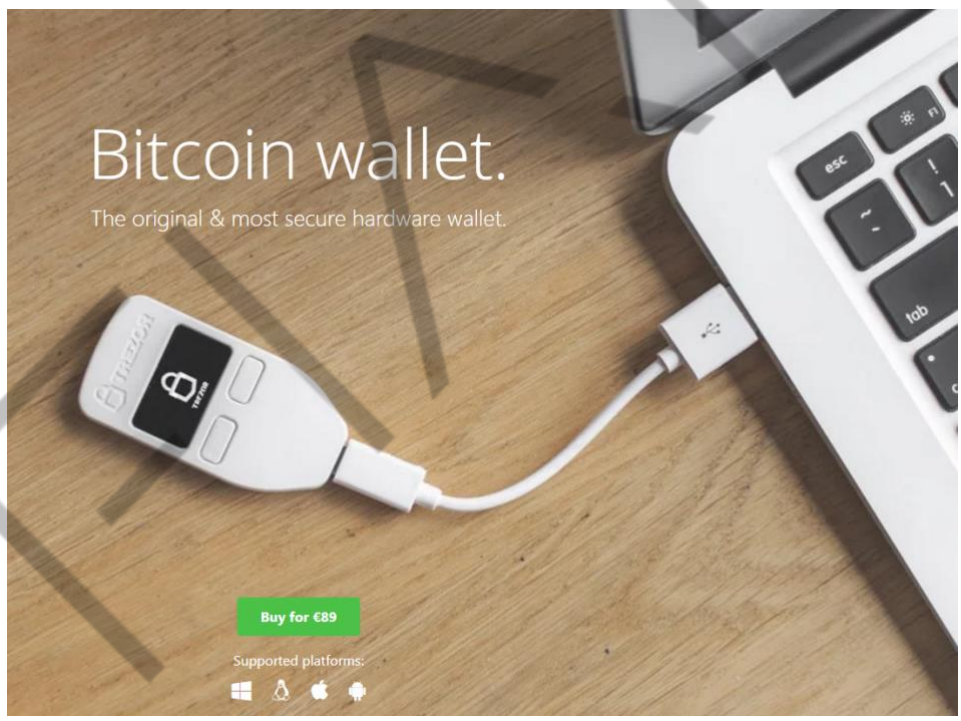

Figura 2.10 – A *hardware wallet* Trezor.io
Fonte: Trezor.io (2017)

Outros dispositivos estão sendo criados com outras finalidades. A empresa Opendime criou o que eles chamam de “*Stick wallet*”: um pendrive de baixíssimo custo, criado para transferência física entre duas pessoas. O dispositivo tem o funcionamento similar a um cofre de moeda “porquinho”, pois, para movimentar os bitcoins contidos em sua carteira, o pendrive precisa ser fisicamente violado, revelando assim a chave privada gerada automaticamente:

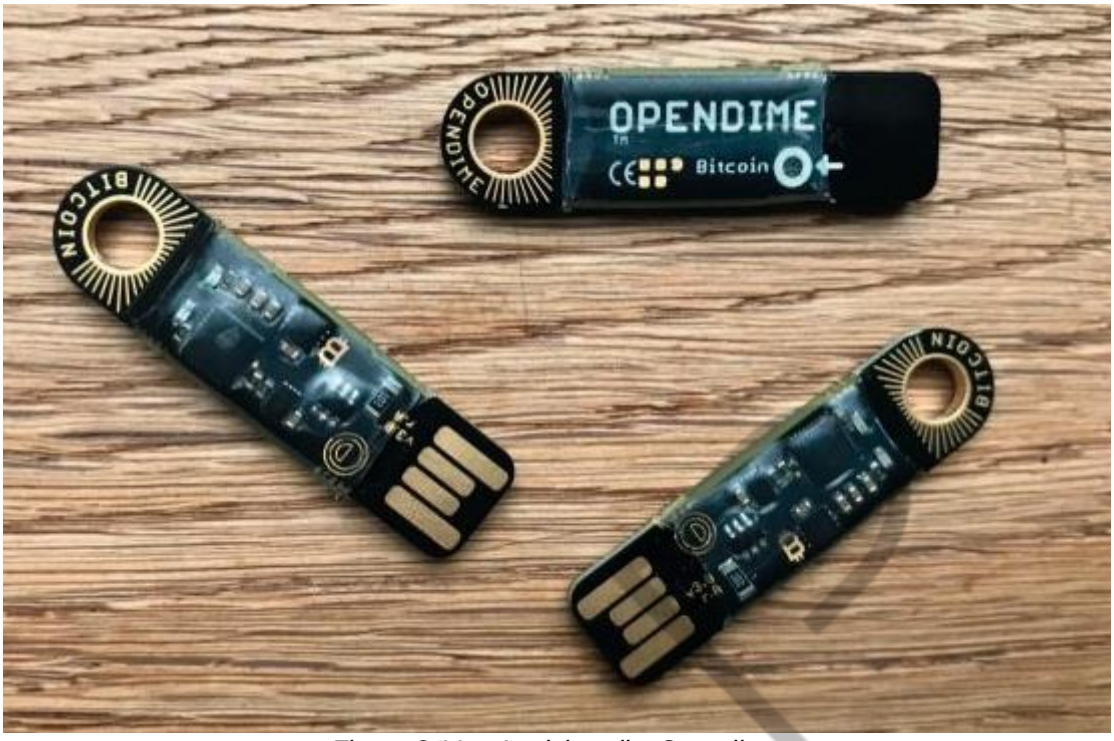

Figura 2.11 – A *stick wallet* Opendime
Fonte: Opendime.com (2017)

2.5.3 Carteiras de papel

Há quem prefira, ainda, armazenar bitcoins em um formato de “papel-moeda”, nas chamadas carteiras de papel (*paper wallets*). Nesse formato, a chave pública (endereço de carteira) e chave privada (senha) são impressas em um papel. A chave privada, costumeiramente, é oculta pela dobra de papel. Tal formato também é bastante utilizado na transferência física de valor entre dois indivíduos. Repare que, na Figura 2.12, o “papel-moeda” está protegido por um plástico do tipo *ziplock*, o que parece ser uma boa ideia.

Figura 2.12 – Carteira de bitcoin em formato de papel (*paper wallet*)
Fonte: BitcoinPaperWallet.com (2017)

2.5.4 Carteiras frias

O cúmulo da segurança, no entanto, são as pessoas ou empresas que usam um tipo de carteira conhecida como carteira fria (ou *cold wallet*). Nessa modalidade, o par de chaves é criado por uma máquina que não está e jamais será conectada à internet. Assim, a chave privada não pode ser descoberta por uma invasão ao equipamento, uma vez que ela está fora da rede.

Cada transação é realizada por outro equipamento ligado à internet e a rede de bitcoin, e cada uma delas é exportada em arquivo e transferida para o equipamento off-line via pendrive, cuja única responsabilidade é assinar/autorizar as transações.

Trata-se de uma abordagem utilizada por algumas empresas cujo volume de movimentação financeira é muito alto e, nesse caso, segurança nunca é demais.

2.6 Como gastar bitcoins?

Se a proposta do bitcoin é atuar como uma espécie de moeda, um fator fundamental é que terceiros vejam seu valor e o aceitem em troca de produtos ou serviços. Assim sendo, como podemos gastar os bitcoins?

2.6.1 Doações

Instituições sem fins lucrativos no mundo todo têm aceitado bitcoins como meio para receber suas doações, como a Wikimedia Foundation, mantenedora da enciclopédia Wikipedia explica no endereço https://wikimediafoundation.org/wiki/Ways_to_Give/pt, ou o Greenpeace, que criou uma postagem específica sobre o assunto que pode ser encontrada no endereço http://www.greenpeace.org/usa/greenpeace-now-accepting-bitcoin-donations/, e explica o que é bitcoin.

2.6.2 Comprando jogos na Steam!

Uma das principais plataformas de compra e venda de jogos do mundo, a Steam, da empresa Valve, aceita bitcoins como forma de pagamento na aquisição de jogos e outros itens vendidos pela empresa.

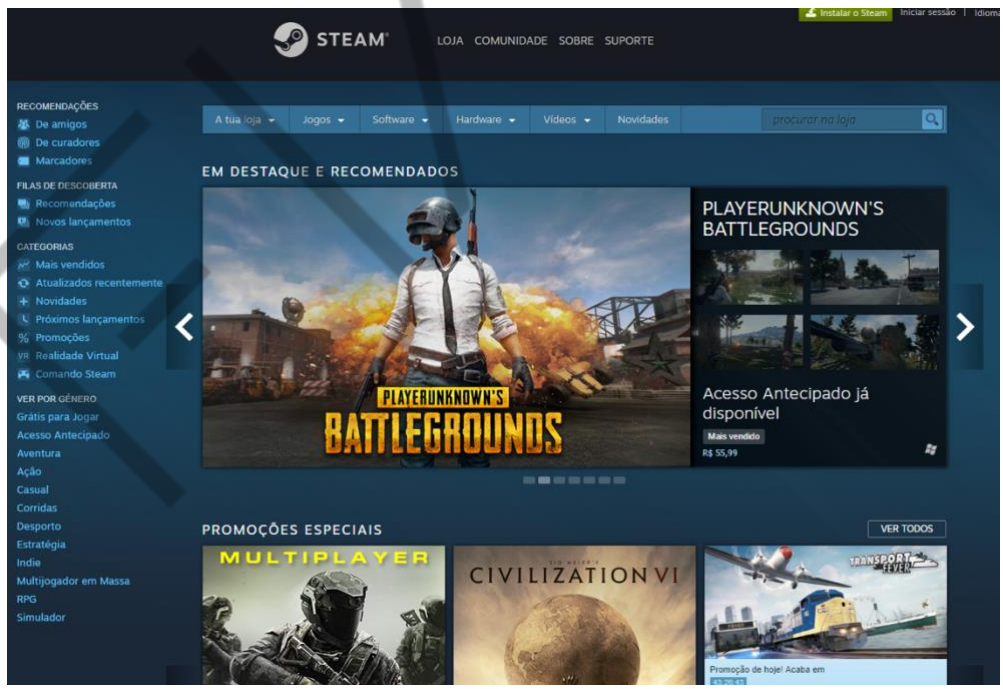

Figura 2.13 – Site da Steam, que aceita bitcoins como forma de pagamento
Fonte: store.steampowered.com (2017)

2.6.3 Comprando cartões de presente

O site Gyft.com permite a compra de cartões de presente de mais de duzentas lojas, entre elas, Starbucks, iTunes Store, eBay, BestBuy, Nike, entre várias outras. Os cartões podem ser adquiridos em bitcoins, e possuem seus valores em dólares. Na sequência, basta trocá-los nesses estabelecimentos por produtos a sua escolha.

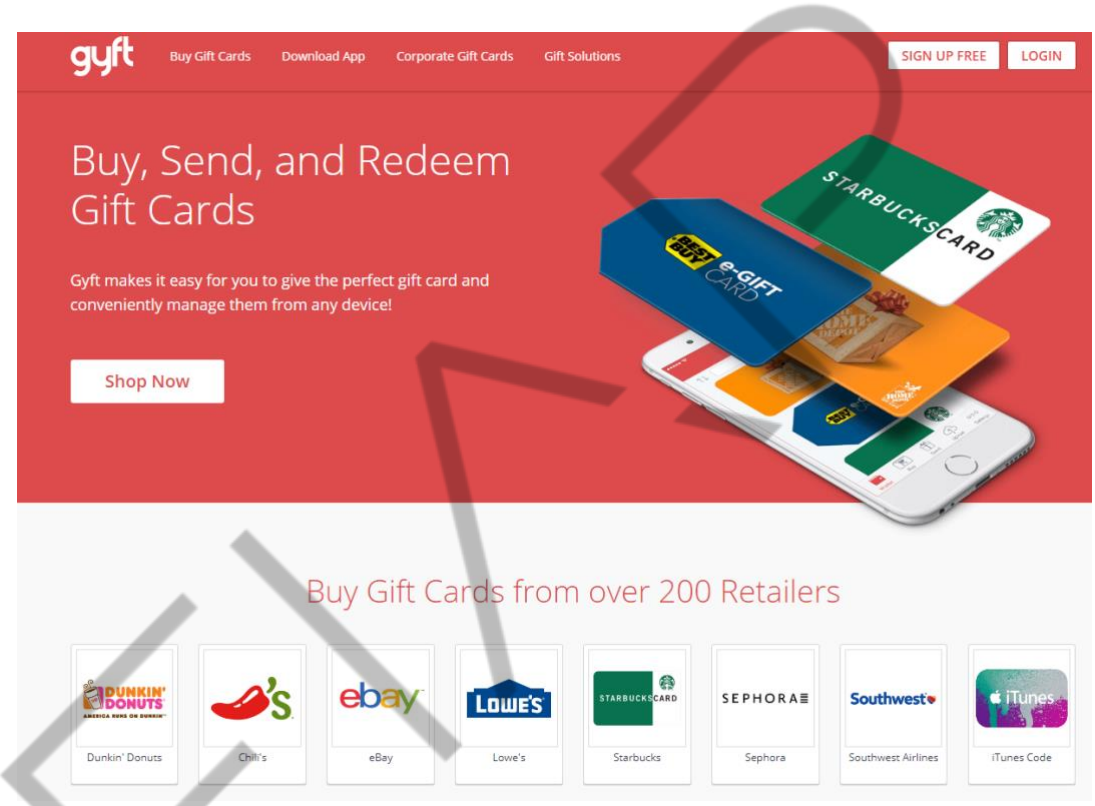

Figura 2.14 – Site Gyft.com
Fonte: Gyft.com (2017)

2.6.4. Carregando cartões pré-pagos e gastando onde quiser

A empresa Advcash.com possui um cartão de crédito na modalidade pré-paga, ou seja, você o carrega antes de usar. A carga pode ser feita em bitcoins e é imediatamente convertida em dólares ou euros e pode ser utilizada como forma de pagamento em qualquer estabelecimento do mundo que aceite Mastercard.

Figura 2.15 – Advcash, o cartão de bandeira Mastercard que pode ser carregado com bitcoins
Fonte: Advcash.com (2017)

Recentemente, a empresa Acesso (https://www.acessocard.com.br/), que oferece o mesmo serviço de cartão de crédito pré-pago Mastercard no Brasil, também passou a aceitar bitcoins como forma de realizar a carga de seus cartões.

2.6.5. Qualquer e-commerce pode aceitar bitcoins

Qualquer loja de comércio eletrônico possui meios de receber em bitcoins facilmente. A empresa brasileira Bit.One atua como um Gateway de pagamento, a exemplo de empresas como PayPal e PagSeguro, com um diferencial: ela permite que o cliente pague as compras com bitcoin e o lojista pode resgatar o valor convertido em reais.

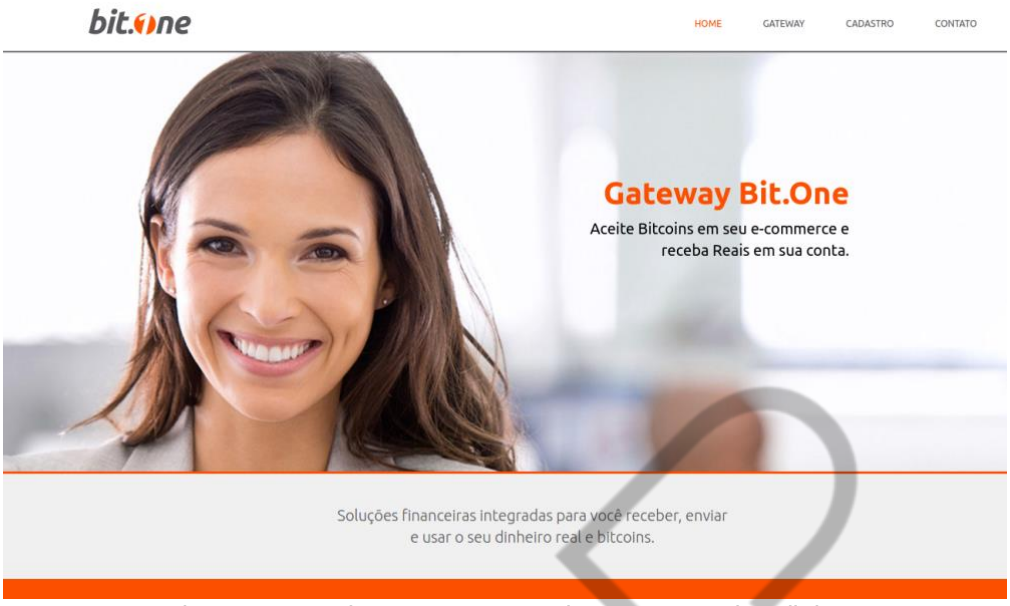

Figura 2.16 – Bit.one, o gateway de pagamento brasileiro
Fonte: bit.one (2017)

2.7 Outras aplicações para o blockchain

Graças ao grande poder computacional envolvido e o sistema de consenso criado para o seu funcionamento, o blockchain do bitcoin tem uma característica única: ele é virtualmente impossível de ser apagado ou adulterado, tornando-se o livro-razão distribuído mais confiável do mundo.

Embora seu uso primordial seja o registro de transações entre carteiras de bitcoin, qualquer tipo de informação, desde que não seja grande demais, pode ser registrado por ele para sempre e, portanto, já está realizando uma série de outras aplicações.

2.7.1 Registro de obras com direitos autorais

Por ser “inadulterável”, o blockchain pode ser utilizado para registro e posterior comprovação de direitos autorais, fornecendo uma prova de autenticidade para criações, ideias, contratos, obras literárias, entre outros.

A *startup* brasileira OriginalMy oferece esse serviço, que funciona de maneira muito simples: cria-se um documento em formato pdf, arquivo de áudio ou vídeo documentando a informação a ser protegida. Na prática, qualquer arquivo digital

pode ser registrado. Ao realizar o *upload* no site da empresa, é gerado um *hash* a partir desse arquivo, que é uma sequência alfanumérica única: um único bit alterado no documento original resultaria em uma geração de *hash* completamente diferente. Ao efetuar o pagamento do serviço, a empresa registra esse *hash* em um bloco do blockchain, que pode ser verificado publicamente.

Figura 2.17 – Original My, *startup* brasileira que presta serviço de prova legal de autenticidade
Fonte: Original My (2017)

2.7.2 Grupos de ajuda mútua

A formação de grupos de ajuda mútua como alternativa ao seguro é uma prática estabelecida em todo o mundo, especialmente em países menos desenvolvidos. As pessoas formam grupos e cada membro contribui com uma soma em dinheiro, formando um fundo de emergência que pode ser acionado em caso de avaria ou furto dos bens que estão acordados.

No entanto, operacionalizar e garantir a segurança do grupo é uma tarefa trabalhosa, e a *startup* brasileira Mutual Life promete resolver o problema. Eles atuam como administradores do grupo, com o intuito de garantir a segurança do valor financeiro de fundo criado. O dinheiro é transformado em bitcoins e armazenado em uma carteira e só pode ser desbloqueado pelo voto da maioria do grupo.

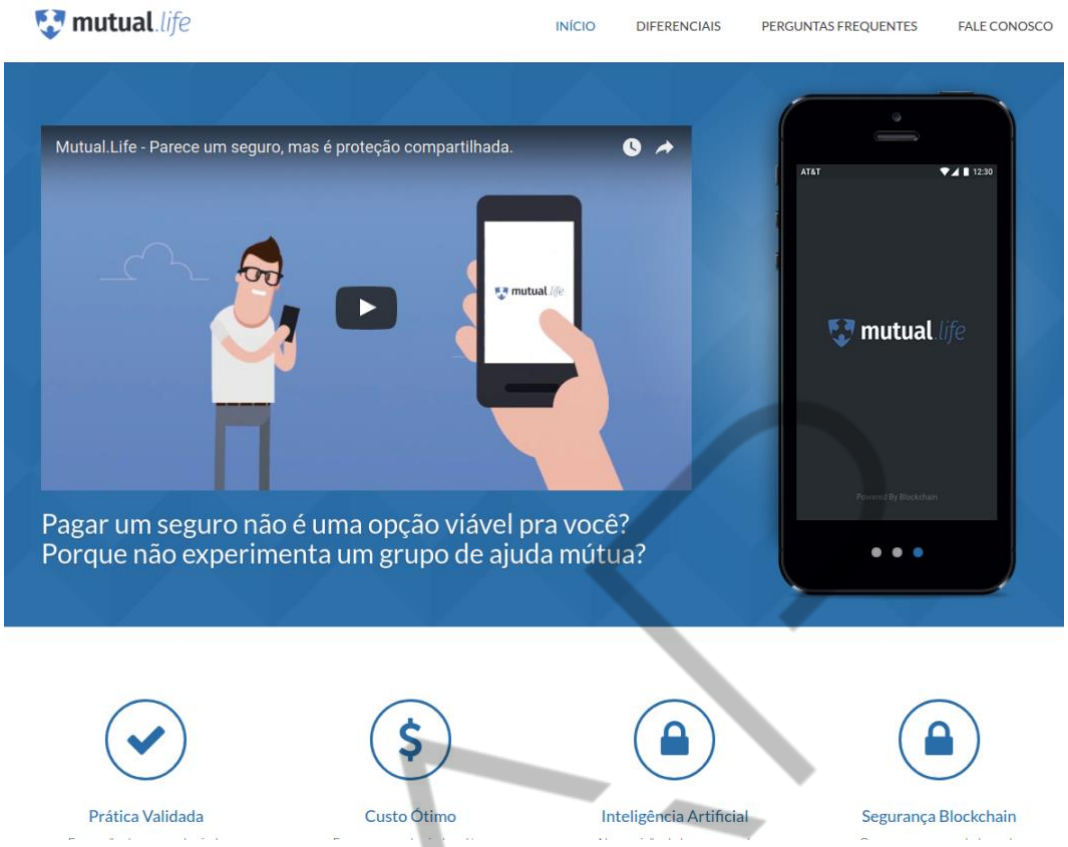

Figura 2.18 – Mutual.Life, serviço de proteção compartilhada
Fonte: Mutual Life (2017)

2.7.3 Segurança logística

A empresa Blockverify fornece um serviço que envolve a identificação de produtos de alto valor, como produtos farmacêuticos, diamantes ou eletrônicos, registrando-os no blockchain do bitcoin. A prática torna a cadeia de suprimentos mais transparente, coibindo práticas como adulteração e falsificação de produtos.

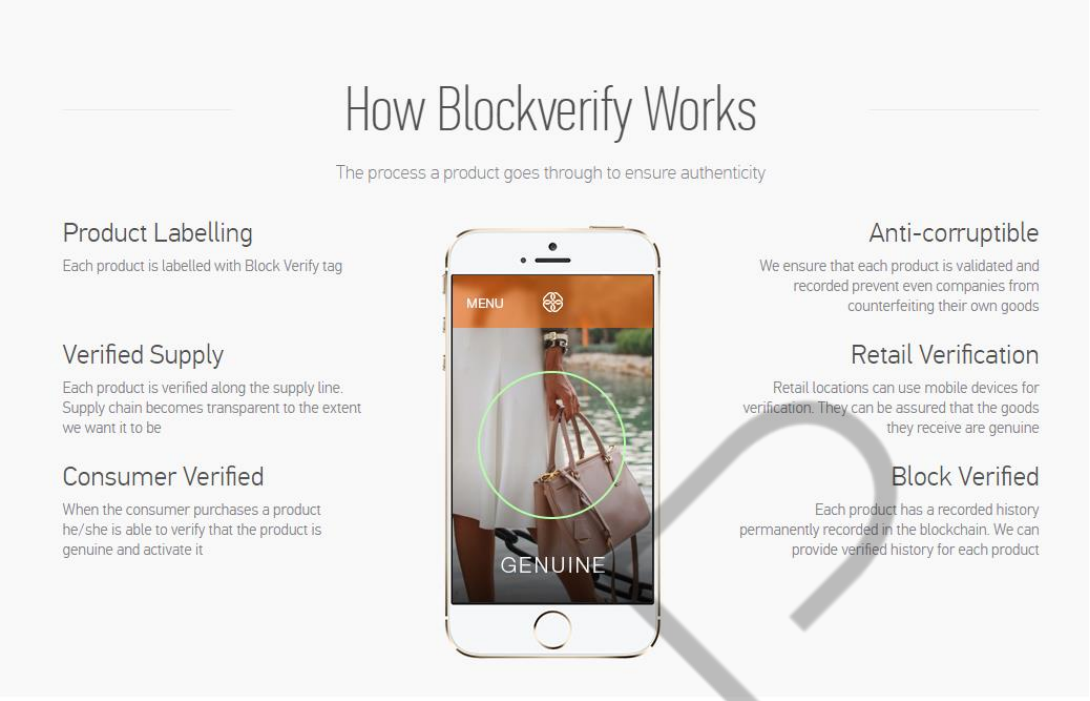

Figura 2.19 – Blockverify, garantindo autenticidade de produtos em uma cadeia logística
Fonte: Blockverify (2017)

2.7.4 Registros imobiliários

Segundo Chavez-Dreyfuss (2016), em uma reportagem para a Reuters, a Suécia está conduzindo testes para colocar o sistema de registro imobiliário do país no blockchain. A iniciativa, que envolve cartórios de registros de imóveis e instituições bancárias, visa aumentar a segurança e a transparência de todas as partes interessadas envolvidas na transação.

Projetos similares estão acontecendo em outros países, como Honduras e Geórgia. A característica de inviolabilidade do blockchain mitiga o risco de fraude tão comum nesse tipo de transação financeira.

2.7.5 Compensação de boletos

Embora enxerguem o bitcoin com desconfiança, os principais bancos brasileiros têm estudado com entusiasmo seu blockchain. Diversas aplicações estão sendo estudadas em seus laboratórios, sendo a mais proeminente delas o “Aceite de boleto de proposta”, um projeto que reúne Banco do Brasil, Bradesco, CIP, Itaú e Santander.

O projeto consiste na criação de um blockchain privado e controlado pelas instituições financeiras com o objetivo de registrar a criação e compensação de boletos bancários. Além de redução de custos e fraudes, a implementação de tecnologia permitiria reduzir o tempo de validação do pagamento de um boleto de alguns dias para poucas horas.

2.8 Outras criptomoedas

Há quase uma década em funcionamento, a rede de bitcoins provou sua viabilidade e não demorou a aparecerem outras criptomoedas, cada uma com suas próprias variações e diferenciais.

O **litecoin**, por exemplo, é uma criptomoeda que tem como um de seus diferenciais o tempo de confirmação da transação, bem mais rápido que do bitcoin (que, conforme abordado, leva, no mínimo, dez minutos). Além disso, foi projetado para ter quatro vezes maior volume de moedas do que o bitcoin. Tais características levam muitos a especular que, no futuro, o bitcoin será reservado para transferências de maior valor (pela demora na confirmação e taxas cobradas) e criptomoedas, como o litecoin, serão utilizadas para pequenas transações, como pagar um café.

Ripple tem ganhado certo destaque; ela tem recebido muito apoio de instituições bancárias, e seu ecossistema de validação prevê não somente o uso de sua moeda, o ripple, mas de moedas fiduciárias como o real, dólar ou euro, ou até mesmo o bitcoin. Por essa razão, ela é considerada pelos seus próprios criadores um complemento ao bitcoin, e não um concorrente.

Outras criptomoedas, como o **Dash**, apostam em transações com mais privacidade, além de um ecossistema que prevê incentivos não somente aos seus mineradores, mas também aos usuários do tipo *fullnodes*, que acabam atuando como auditores da rede.

Figura 2.20 – Altcoins e suas milhares opções
Fonte: Google Imagens (2017)

No entanto, quando falamos em valor de mercado, a segunda criptomoeda em relevância é o **Ethereum**. Seu sistema prevê os contratos inteligentes (ou *Smart Contracts*) como grande diferencial, assunto que veremos a seguir.

Concluindo, existem milhares de moedas alternativas ao bitcoin (também conhecidas como *alt coins*), cada uma delas com uma particularidade ou objetivo diferente; é importante que fiquemos atentos, pois uma moeda pode ser criada com o propósito único de especulação de mercado, enriquecendo seu criador.

As dez primeiras criptomoedas da Tabela 2.1 possuem seu valor de mercado e seu propósito bem estabelecidos. Entretanto, é seguro afirmar que nenhuma delas possui o poder computacional e, portanto, a robustez presente no sistema de validação de consenso do bitcoin.

Tabela 2.1 – As 10 melhores criptomoedas em valor de mercado

Criptomoeda	Valor de mercado	Preço	Qtde em circulação
Bitcoin	US$ 92.653.638.726,00	US$ 5566,02	16.646.300 BTC
Ethereum	US$ 28.396.170.361,00	US$ 297,91	95.318.589 ETH
Ripple	US$ 7.794.005.567,00	US$ 0,202276	38.531.538.922 XRP
Bitcoin Cash	US$ 5.498.655.927,00	US$ 329,00	16.713.088 BCH
Litecoin	US$ 2.959.385.122,00	US$ 55,28	53.533.107 LTC
Dash	US$ 2.212.306.300,00	US$ 289,46	7.642.900 DASH
NEM	US$ 1.849.050.000,00	US$ 0,205450	8.999.999.999 XEM
NEO	US$ 1.463.780.000,00	US$ 29,28	50.000.000 NEO
BitConnect	US$ 1.440.894.091,00	US$ 197,42	7.298.623 BCC
Monero	US$ 1.389.397.734,00	US$ 91,01	15.266.228 XMR

Fonte: Coinmarketcap.com (2017)

2.9 O futuro da moeda

Muito é especulado sobre o futuro do bitcoin. Algumas pessoas, provavelmente por desconhecimento no assunto ou por temê-lo, são ávidas em decretar o seu fim, especialmente economistas de velha guarda. O site Bitcoin Obituaries (https://99bitcoins.com/bitcoinobituaries/) se diverte com tais previsões, registrando, até outubro de 2017, a morte da criptomoeda 179 vezes. Algo que “morreu e ressuscitou” mais de uma centena e meia de vezes mostra resiliência e merece nossa atenção.

As previsões apresentadas aqui são baseadas em discussões atuais e iniciativas interessantes, sendo, portanto, menos levianas do que decretar sua morte. Como todo exercício de futurologia, possui uma certa probabilidade de não se concretizar.

2.9.1 Sidechains

Quando nos referimos ao ecossistema do bitcoin, que vale bilhões de dólares, todas as melhorias propostas precisam ser largamente debatidas, exaustivamente testadas, sendo implementadas em consenso e de forma gradativa. O sistema em funcionamento possui um equilíbrio delicado e nenhuma melhoria pode ferir os seus diferenciais, em especial, sua característica de descentralização.

Muitas melhorias são debatidas com o intuito de garantir um tempo de resposta “saudável” para as transações, afinal de contas, se uma transferência de bitcoin levar muitas horas ou até alguns dias para ser validada como padrão, o sistema se torna insustentável.

Desde o chamado SegWit até os debates envolvendo o aumento do tamanho de bloco (“cabendo”, assim, mais transações) estão em curso, entretanto, boa parte dos usuários e especialistas defende que o protocolo do bitcoin e sua corrente de blocos precisa se manter estável e... simples. Assim sendo, conforme novas necessidades vão surgindo, novas correntes (ou *chains*) começam a rodar ligadas à corrente principal, e a essas correntes interrelacionadas damos o nome de *sidechains*.

Para dar um **exemplo**, o protocolo de comunicação da internet é o IP, *Internet Protocol*. Por ser muito simples, um protocolo específico para sua transmissão foi criado (TCP), atuando em conjunto a ele, formando o TCP/IP. Cada serviço de internet tem sua complexidade e particularidade, sendo necessário criar protocolos que o suportem, como o HTTP, FTP, entre vários, que são transmitidos por cima do TCP/IP, que mantém a sua simplicidade.

É exatamente o que se prevê para a rede bitcoin: o blockchain atual manterá as características que possui, e novos blockchains serão criados para novas necessidades, mantendo um contato, de tempos em tempos, com a cadeia de bloco principal.

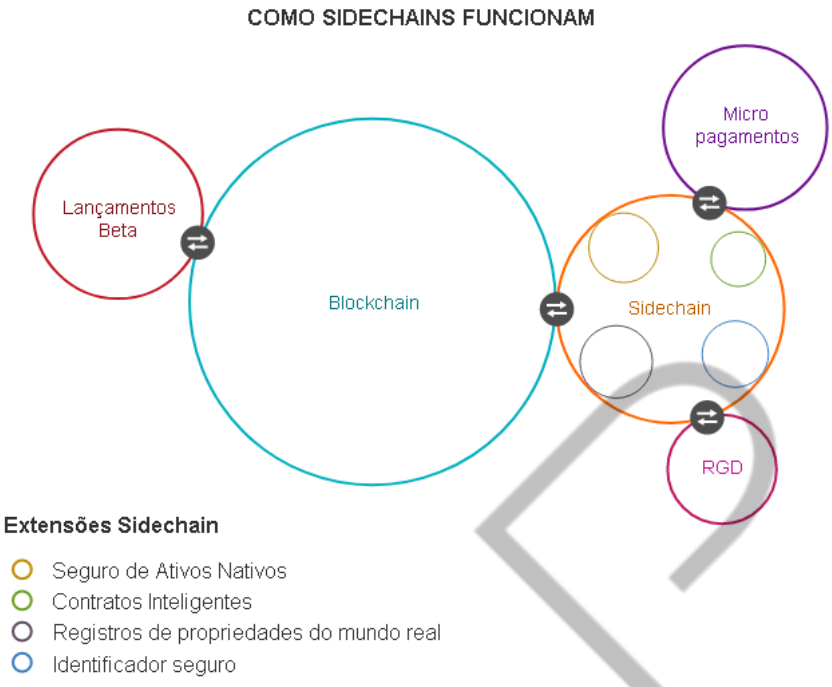

Figura 2.21 – Sidechains
Fonte: HIGGINS (2014)

2.9.2 *Smart contracts*

O que desponta como horizonte para o bitcoin é, certamente, os contratos inteligentes (*smart contracts*). Implementados no Ethereum, a tecnologia prevê contratos autoliquidáveis e autogerenciáveis. O projeto RSK Ginger (http://www.rsk.co/) é um forte candidato à implementação de *smart contracts* no bitcoin, por meio de uma sidechain.

Realidade na rede Ethereum, você se pergunta, o que são, de fato, smart contracts?

Vamos a um **exemplo**: imagine que Alice, em uma conversa com Bob, acredita que a cotação do dólar ultrapassará a barreira dos quatro reais até o fim de 2017. Bob discorda, dizendo que Alice não poderia estar mais enganada. Ambos, então, resolvem fazer uma aposta: mediante uma soma em dinheiro de cada uma das partes, estabelecem que, se a qualquer momento, até 31 de dezembro de 2017, a cotação passar de quatro reais por um dólar, Alice vence a aposta e fica com o bolão, caso contrário, se o ano-novo passar e isso não se concretizar, Bob vence.

Antes dos *smart contracts*, Alice e Bob teriam que recorrer a um terceiro, alguém digno de confiança de ambos, que pudesse custodiar a quantia e liquidasse a aposta, sob as condições estabelecidas. Pois bem, isso não é mais necessário: é possível redigir um contrato inteligente, com o endereço das carteiras de Alice e Bob e sua própria, que irá reter o valor durante a vigência do contrato. As condições são redigidas com uma linguagem de programação e, o contrato pode, até mesmo, verificar a cotação de dólar sozinho. Que tal ele consultar o site do *Valor Econômico*? Talvez outra cotação, como do Yahoo! Finance? Não importa: o contrato verifica a condição diariamente e, se a cotação >= 4 reais, envia dinheiro para Alice. Se a cotação < 4 reais e ano > 2017, envia para Bob. Fascinante, não é mesmo?

A aplicabilidade dos *smart contracts* não precisa ficar restrita à frivolidade das apostas. Contratos de aluguel, compra e venda de bens e serviços, praticamente qualquer coisa que peça um contrato para ser redigido pode se transformar em um contrato inteligente.

A empresa Slock.it (https://slock.it/) aposta nesse futuro inteligente. Um de seus produtos é uma fechadura eletrônica baseada em duas tecnologias emergentes: o IoT e os *smarts contracts*.

Figura 2.22 – A fechadura da Slock.it
Fonte: coincheck.com (2017)

Imagine que você tem um salão de festas o qual deseja alugar por diária. Estabelece um preço, começa a anunciar, instala uma fechadura como essa e resolve se mudar para a Austrália. Cristiane encontra seu anúncio, gosta das fotos

do salão e o reserva para o sábado, depositando, em criptomoedas, um valor como caução.

Sexta à noite, Cristiane chega até a porta do salão com seu smartphone. A fechadura inteligente verifica a reserva, a quantia depositada como caução e, sabendo da presença de Cristiane à sua frente, abre a fechadura. A festa acontece normalmente durante o sábado e, ao final do dia, a feliz locatária fecha a porta, paga pela diária e encerra o negócio. A fechadura fecha a porta, verifica o valor da diária e devolve o valor depositado como caução.

Maria, que faz a limpeza do salão, aparece no domingo, e ela também possui um smartphone. A fechadura abre a porta, Maria faz o serviço e sai do salão, avisando à fechadura que o serviço está completo. A fechadura tranca a porta e deposita automaticamente o valor do serviço de Maria, enquanto você continua na Austrália. Você teve que fazer ALGUMA COISA durante o contrato de aluguel? Provavelmente estava pegando uma onda em Surfer's Paradise Beach.

2.10 Conclusões

Apesar de economistas desconfiados e previsões apocalípticas, é seguro afirmar que o bitcoin, assim como a tecnologia de criptomoedas, veio para ficar. Quais dessas moedas permanecerão e quais irão sumir é uma incógnita. No entanto, após oito anos em funcionamento, o bitcoin se tornou uma rede de proporções monstruosas, com um grau de segurança e confiabilidade inéditos. Sua criação e seu funcionamento desafiam a própria definição de moeda e representam uma quebra de paradigmas, vislumbrando um futuro no qual possamos custodiar o próprio dinheiro e efetuar pagamentos reduzindo o grande número de intermediários que existe hoje, de uma forma transparente, segura e rápida.

A implementação de contratos inteligentes desenha um futuro digno de romances de ficção científica, enquanto outras aplicações representam o potencial imenso de inovação: está muito longe do objetivo deste capítulo incentivá-lo a comprar bitcoins ou outras criptomoedas, e sim expandir os horizontes, sobretudo aqueles que envolvem essa tecnologia e o que pode ser feito a respeito dela.

Esperamos que esse objetivo tenha sido cumprido!

REFERÊNCIAS

7COMM. **Bancos brasileiros puxam fio da meada do blockchain com projetos antifraudes, smart contracts e boletos.** 2017. Disponível em: <https://www.7comm.com.br/blog/2017/06/bancos-brasileiros-puxam-fio-da-meada-do-blockchain-com-projetos-antifraudes-smart-contracts-e-boletos/>. Acesso em: 12 ago. 2017.

ANTONOPOULOS, Andreas. **Mastering Bitcoin:** Unlocking Digital Cryptocurrencies. Sebastopol: O'Reilly Media, 2016.

CHAVEZ-DREYFUSS, Gertrude. **Sweden tests blockchain technology for land registry.** 2016. Disponível em: <http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV>. Acesso em: 12 ago. 2017.

HIGGINS, STAN. **Sidechains White Paper Imagines New Future for Digital Currency Development.** 2014. Disponível em: <https://www.coindesk.com/sidechains-white-paper-ecosystem-reboot/>. Acesso em: 14 ago. 2017

POPPER, Nathaniel. **Digital Gold:** Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money. Nova York: Harper Paperbacks, 2016.

PRESCOTT, Roberta. **Banco do Brasil testa blockchain para aceite de boletos de propostas.** 2017. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=45384&sid=148>. Acesso em: 12 ago. 2017.

ULRICH, Fernando. **Bitcoin — a moeda na era digital.** 1. ed. São Paulo: Instituto Ludwig von Mises Brasil, 2014.