

BITCOIN

PARA TODOS

Descubra o Poder do Ouro Digital



Felippe
Percigo



Índice

Estamos passando pela (R)evolução do dinheiro!.....	03
O começo	12
O básico do básico	16
Os 21 milhões de Bitcoins.....	25
Como funciona a mineração?	32
A sua Wallet	38
Como comprar Bitcoins	45
Posso pensar no BTC como investimento?	55
Bitcoin é uma bolha?	75
Regulação e leis	80



Estamos passando pela (R)evolução do dinheiro!





Eu sei, parece loucura falar em revolução ou evolução do dinheiro, parece exagero pensar que o dinheiro está mudando, mas a realidade é que depois de ler esse livro você nunca mais olhará para a sua carteira da mesma forma e, mais do que isso, você estará preparado(a) para se garantir em um período de mudanças e evoluções importantíssimas – que já estão acontecendo – no sistema financeiro mundial.

O que hoje são notas de papel que representam um valor monetário, ou aquele número em sua conta bancária que é usado quando você passa o seu cartão de “crédito ou débito”, já foi algo muito diferente e menos – digamos assim – desenvolvido ou moderno. A revolução do dinheiro não começou agora. Ele sempre evoluiu, mudou e se modernizou para o que temos hoje e para o que teremos em pouco tempo por meio do Bitcoin.





Você deve estar pensando: “O Felipe não está falando sério, o Bitcoin nem é dinheiro de verdade!”. Será mesmo? Que tal refletirmos rapidamente sobre a história do dinheiro, como passamos pelo ouro e acabamos com pedaços de papel dentro da carteira e qual a importância do Bitcoin nisso para ver se entramos em um acordo?

Antes de qualquer coisa se tornar realmente “dinheiro”, ele precisa ser adotado como um meio de troca, ou seja, as pessoas precisam usar determinado bem para trocar por algum outro bem de seu interesse. Para que algo se torne um meio de troca, ele precisa demonstrar ter alguma utilidade para as pessoas que o usarão.

Pode ser trazer certo tipo de conforto, comodidade ou até bem-estar. A conclusão é que um bem só pode ser considerado um meio de troca se ele já tem um valor como mercadoria, pelo seu uso e pelo benefício que traz. Esse é o teorema da regressão, base da primeira obra de Ludwig von Mises (“Teoria do Dinheiro e da Moeda Fiduciária”).

É possível que você tenha pensado no exemplo mais comum sobre o que acabamos de falar, o ouro. O metal foi escolhido como dinheiro há muito tempo, mas antes disso demonstrou seu valor de uso e utilidade. É um elemento escasso, de difícil acesso e, por isso, considerado nobre, digno de ser usado em uma troca comercial. O Bitcoin, vamos chamá-lo de BTC, não é diferente – aliás, tem muito a ver com o ouro –, pois passou



e ainda passa pela mesma regrinha tão bem explicada pelo teorema da regressão de von Mises. Ele encontrou valor em determinado período, ainda tem encontrado seu espaço, e não demorará para se tornar um meio de troca propriamente dito.

Na comparação que fizemos com o ouro, na descoberta desse metal, a sua utilidade era bem limitada, assim como o BTC hoje. O ouro era usado em enfeites, mas mesmo assim se tornou dinheiro. Se tornou um meio de troca, encontrando valor não apenas em sua utilidade anterior, mas valorizando-se conforme a sua utilidade monetária aumentava.





Em relação ao BTC, a primeira vez que ele foi considerado um meio de troca foi em maio de 2010, quando um homem chamado Laszlo Hanyecz comprou duas pizzas no valor de 10.000 BTC. Sim, isso mesmo! Provavelmente é a pizza mais cara da história! Atualmente, isso equivaleria a quase 100 milhões de dólares.

Você pode dizer: “Tá bom Felipe, mas você me falou que iria explicar como o dinheiro veio do ouro para o pedaço de papel de hoje...” Sim, vou falar sobre isso agora mesmo. A história nos revela que muitos bens funcionaram como meio de troca em determinado período. Tabaco, açúcar, sal, gado, pregos, cobre, grãos, especiarias e algumas outras coisas. Mas nenhum bem se destacou e teve igual importância quanto o ouro, como já falamos.

A característica comum a todas essas mercadorias, como destaca Fernando Ulrich – a quem admiro – em seu livro “Bitcoin, a moeda na era digital”, é a tangibilidade. Eles existem fisicamente, quimicamente e biologicamente.

Com o tempo, o sistema monetário precisou evoluir, surgindo então a custódia do ouro pelos ourives ou por instituições especializadas, conhecidas como bancos. A evolução aconteceu por uma questão de segurança – já que carregar ouro por aí começou a se tornar perigoso – e por uma questão de espaço físico e peso, já que caixas e mais caixas de ouro tem um peso muito grande.



As pessoas depositavam o ouro em um banco e recebiam em troca um certificado da quantidade de ouro armazenado. Assim, esses papéis começaram a circular por aí facilitando as trocas monetárias e financeiras. Em um determinado momento, os bancos tinham tanta credibilidade junto aos seus clientes, que estes resolveram se abster da responsabilidade de transferir o ouro físico (após a transação com os certificados) e deixaram esse trabalho com os próprios bancos.

Ou seja, o cliente apenas assinava um certificado de que estava transacionando certa quantidade de ouro com alguém, e o banco se responsabilizava em enviar a quantidade correspondente e realizar a transação, surgindo então os cheques e os depósitos bancários.





Nesta época, o cliente tinha uma cédula com um valor exatamente correspondente a quantidade de ouro depositada no banco, e isso chamamos de lastro. Tudo era 100% lastreado em ouro.

Chegou a hora em que os bancos começaram a perceber que nem todos os clientes exigiam o saque de ouro em espécie e preferiam ficar com a cédula que representava a quantia correspondente.

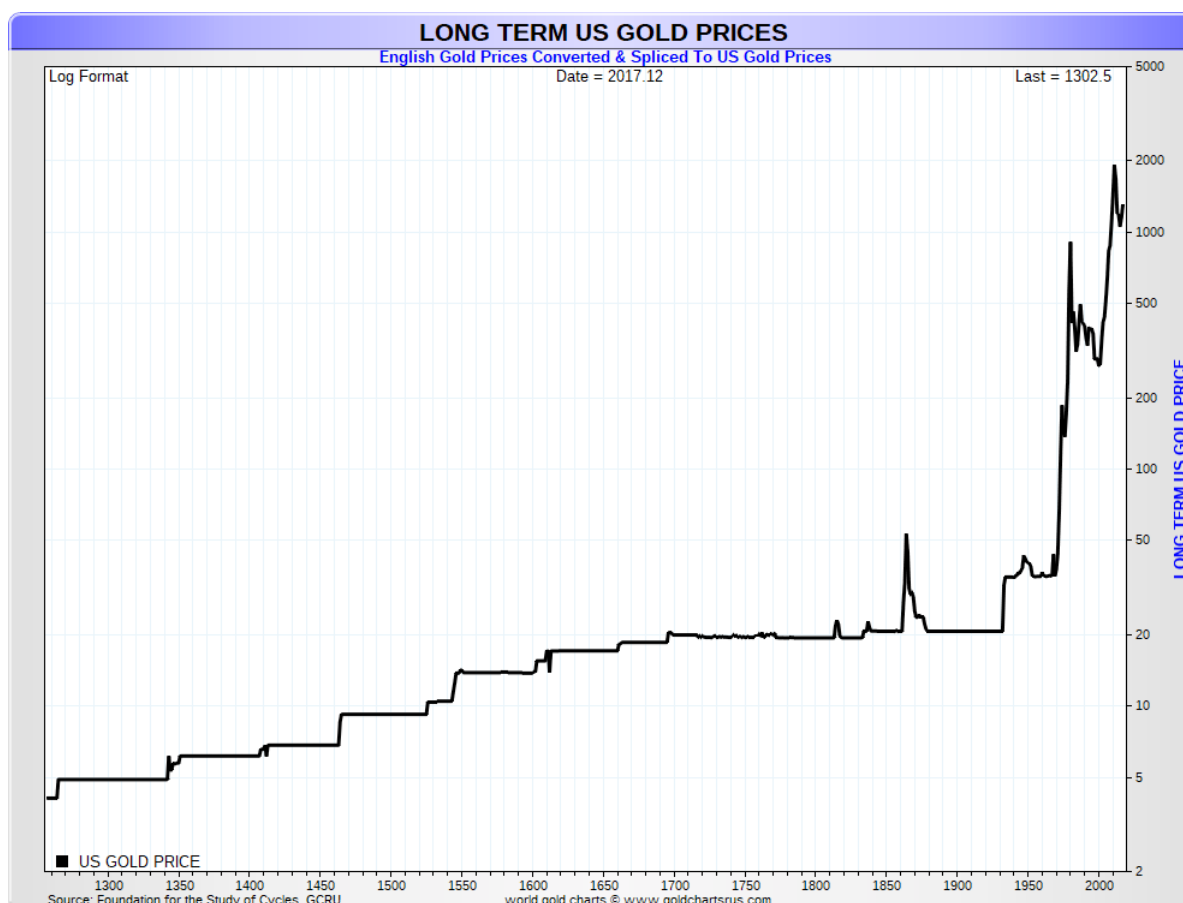
Assim, as instituições bancárias iniciaram um processo que dura até hoje: ficavam com apenas uma parte da reserva lastreada e emprestavam o restante para obter lucros maiores do que aqueles abrangendo apenas as taxas de transação.

Esse dinheiro emprestado que excedia o lastro do ouro passou a ser chamado de moeda escritural, que não existe no mundo material, só na contabilidade dos bancos. Então, na verdade, a moeda invisível, como o BTC é considerado, já passou a existir desde esse momento. Hoje em dia, a moeda escritural ainda existe, 100% digital, pois os bancos só possuem parte do dinheiro que rodam lastreados em notas físicas no Banco Central, que por sua vez não tem lastro nenhum em coisa alguma.

De acordo com Fernando Ulrich, a moeda escritural em circulação no Brasil é de 52% do valor total do dinheiro rodando por aí. Ou seja, mais da metade do dinheiro rodando em nosso país hoje é 100% digital e virtual.



Essa possibilidade liberou os bancos centrais para imprimirem notas de dinheiro à vontade, já que não existe lastro em ouro como exigência. Para você ter uma ideia, em 1971, o então presidente americano Richard Nixon, cancelou a conversão do dólar em ouro, acabando com as reservas de lastro ainda existentes. A consequência disso foi uma impressão desenfreada de dólares pelo FED (Banco Central Americano), acarretando na desvalorização do dinheiro e do poder de compra da população. Assim como mostra o gráfico a seguir:



Fonte: <https://sdbullion.com/gold-price-history>

Quanto mais notas impressas, mais dinheiro na mão das pessoas. E como as pessoas têm mais dinheiro em suas mãos, mais será



cobrado por serviços e produtos – isso se chama inflação. Os bancos centrais ao redor de todo mundo fazem isso e, quando acham necessário, imprimem mais notas. Sim, eles podem fazer isso.

Qual é o problema disso tudo e onde o BTC entra nessa história? O problema é que eu e você não podemos fazer nada para resolver isso, isto é, para evitar que o nosso dinheiro se desvalorize e que valha cada vez menos. Não conseguimos evitar que as coisas fiquem mais caras, não temos poder para isso. O sistema é centralizado e comandado pelos bancos centrais, e o BTC é antítese disso. É descentralizado e o poder está nas mãos dos donos de seus BTC's. A partir do momento que você compra o seu BTC, ele é seu e somente seu, ninguém tem nada com isso.

Com todas as suas propriedades, o BTC tem tecnologia robusta e características suficientes para ser considerado uma *commodity digital* escasso e valioso, ou seja, o “ouro digital,” como alguns gostam de chamar. Pode também ser considerado um investimento rentável, a longo prazo inclusive, e tem tudo para se tornar um meio de troca, dinheiro literalmente.

Se você está pronto(a) para entender mais sobre isso e participar da revolução do dinheiro que já está acontecendo, me acompanhe pelas próximas páginas. Você vai entender tudo que você precisa saber para participar disso de maneira correta e segura. Vamos lá?



O Começo





Se você não lembra, ao menos já deve ter ouvido bastante gente falar sobre a crise mundial de 2008, não é mesmo? Não estou aqui pra explicar sobre ela, não é meu objetivo e no Google você vai encontrar um monte de gente mostrando detalhadamente o que aconteceu. Mas em resumo, foi um verdadeiro caos!

Em um efeito dominó, bancos e instituições financeiras envolvidos nos “*swaps do subprime*” foram quebrando, deixando pessoas a ver navios, com todas as suas economias transformadas em pó, ou quase isso. Mas esse mesmo ano foi marcado pelo início de algo que impactaria o mundo do sistema bancário e financeiro: a publicação do White Paper do Bitcoin.

Esse White Paper é um documento simples, sem frescura, com a explicação de como o Bitcoin e a Blockchain, a tecnologia que sustenta o Bitcoin, funciona. A data exata do surgimento disso é 01 de Novembro de 2008 e o título é – “Bitcoin: A Peer-to-Peer Electronic Cash System” (Bitcoin: Um Sistema Monetário Peer-to-Peer) e foi escrito por Satoshi Nakamoto. O resumo desta apresentação dizia que o Bitcoin era uma versão pura de dinheiro eletrônico que permitiria pagamentos online com envio direto de uma parte para outra sem passar por uma instituição financeira.

Ou seja, em sua concepção, o BTC sempre teve o objetivo de ser um dinheiro virtual e que não precisa do controle de nenhuma instituição financeira, e que depende exclusiva e simplesmente das duas partes envolvidas em uma transação financeira, isto é, quem vai enviar e quem vai receber.



Em Janeiro de 2009 aconteceu a primeira transação de BTC's entre Satoshi Nakamoto e Hal Finney, talvez o primeiro entusiasta da moeda e que ajudou Satoshi no melhoramento do sistema. Você deve estar se perguntando: "Quem é esse tal de Satoshi Nakamoto?", a verdade é que ninguém sabe! Existem inúmeras teorias, a principal é de que ele não é necessariamente apenas uma pessoa, mas sim um grupo de desenvolvedores *cyberpunks* (anarcocapitalistas) que juntos teriam desenvolvido todo o sistema. Outra teoria dá a entender que o próprio Hal Finney poderia ser a pessoa atrás do pseudônimo, mas ninguém sabe com certeza. O fato é que tudo foi desenvolvido de tal forma, com estrutura tão bem desenhada e segura, que é difícil imaginar que uma pessoa pudesse fazer tudo sozinha.

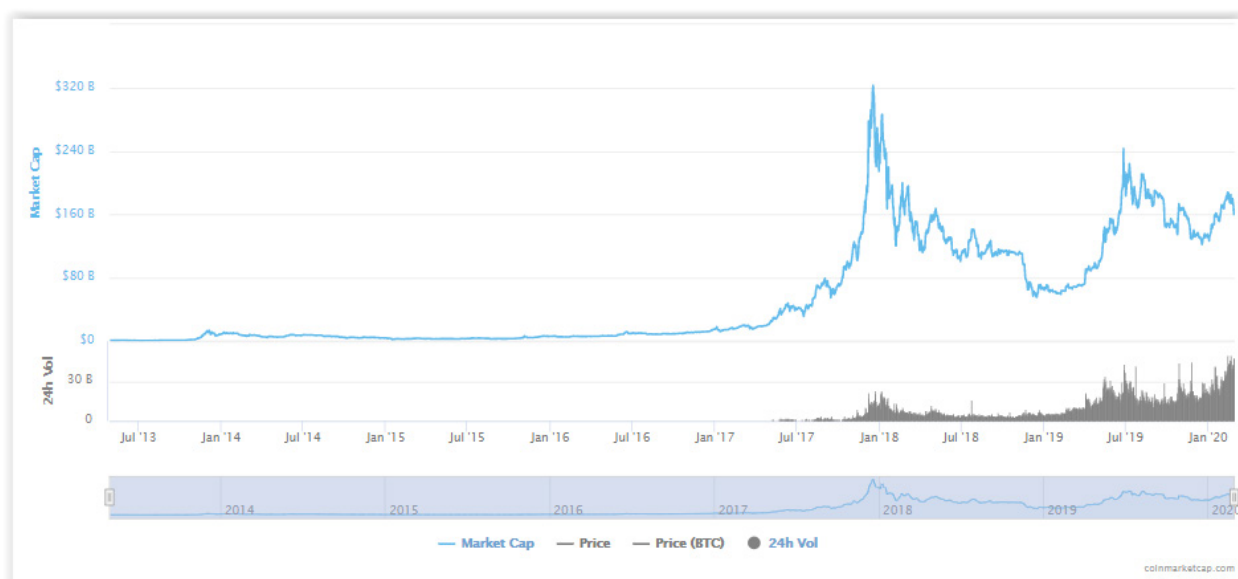
Obviamente que nesse início o BTC não era famoso e a sua fama se limitava apenas aos entusiastas, e o valor de mercado da moeda era de menos de centavos de dólar.





Opa, calma... Eu já sei o que você pensou – “Por que eu não sabia disso? Se eu tivesse colocado uma grana nessa época, hoje eu estaria bilionário(a)!”. Pois é, a grande maioria pensa isso, mas o tempo não volta e, sinceramente, se alguém te oferecesse esse investimento na época, a probabilidade era altíssima que você achasse que era só mais uma loucura de alguns nerds que ficavam o dia todo no computador.

Em Maio de 2010, como já citamos anteriormente, a primeira compra usando BTC foi realizada. Foi quando Laszlo Hanyecz comprou duas pizzas por 10.000BTC. Em Novembro de 2010, apenas dois anos depois de sua criação, o BTC atingiu a marca de um milhão de dólares de Market Cap – Capitalização do Mercado (a multiplicação entre o preço do ativo e a quantidade em circulação). O restante, caros leitores, é história. De 2010 para janeiro de 2020, ano em que estou escrevendo isso, o BTC já somou 131.850.847.000,00 bilhões de dólares, como mostra o gráfico a seguir:



Fonte: coinmarketcap.com



O básico do básico





Quero ir adiante e te explicar como toda essa lógica funciona na prática, desde a “mineração” até como comprar um BTC para você não ficar de fora desse mundo, e antes que eu prossiga, preciso te avisar uma coisa: se você está procurando um material que te explique em minuciosos detalhes de programação como todo esse sistema funciona, esse livro não é para você.

Aqui eu quero fazer com que o maior número de pessoas possíveis sejam inseridas na evolução do dinheiro e comecem a experimentar a liberdade que é ser dono do seu próprio dinheiro sem ter uma instituição financeira achando que pode mandar nele, além é claro de te ensinar algumas maneiras de lucrar com isso, já que a valorização do BTC em 2019 foi de 93%. Isso mesmo, se você tivesse investido R\$50.000 em BTC no início do ano passado, ao final você teria R\$96.500, de forma segura,





sem essa conversa bandida de pirâmide financeira que usa BTC como pretexto para cometer crime e roubar o seu dinheiro.

Ah, e já que estamos falando nisso, é importante lembrar: Bitcoin não é pirâmide financeira! Uma coisa não tem nada a ver com a outra. A moda hoje é que as pirâmides financeiras usem os criptoativos e as moedas digitais para enganarem você e roubarem o seu dinheiro.

Voltando ao assunto, como falamos, o BTC é uma moeda virtual e digital que é transferida de forma segura e criptografada, cuja transação é registrada e mantida em um livro-razão, suportado por um sistema chamado “Blockchain” e sustentado pela rede de computadores Peer-to-Peer (P2P).

É daqui que começamos a entender o básico!

O QUE É CRIPTOGRAFIA?

É o processo de converter qualquer dado ou informação em um código que é travado por uma chave única ou múltiplas chaves, usando algoritmos de computador prevenindo o sistema de ter as informações acessadas sem autorização. A chave única chamamos de “Private Key”. (BANSAL, 2018, p. 8)

Você talvez já deve ter visto isso, mas atualmente a maneira mais comum de um hacker prejudicar alguém é criptografando os



dados do computador do “hackedo.” Assim, ele pode extorquir a vítima pedindo dinheiro a ela para que então entregue as chaves de acesso.

A Private Key é a senha de acesso à carteira onde os seus BTC's estão alocados e precisa ser guardada pelo dono da carteira. Nós veremos isso mais para frente, mas te adiantando, ao comprar Bitcoins você os transferirá para uma carteira – que chamamos de wallet – e a Private Key é a senha de acesso dela.

No universo BTC, a criptografia vai criptografar a identidade das duas pessoas que estão transacionando a(s) moeda(s), a transação propriamente dita e as informações das wallets envolvidas nas transações.

O QUE É O LIVRO-RAZÃO?

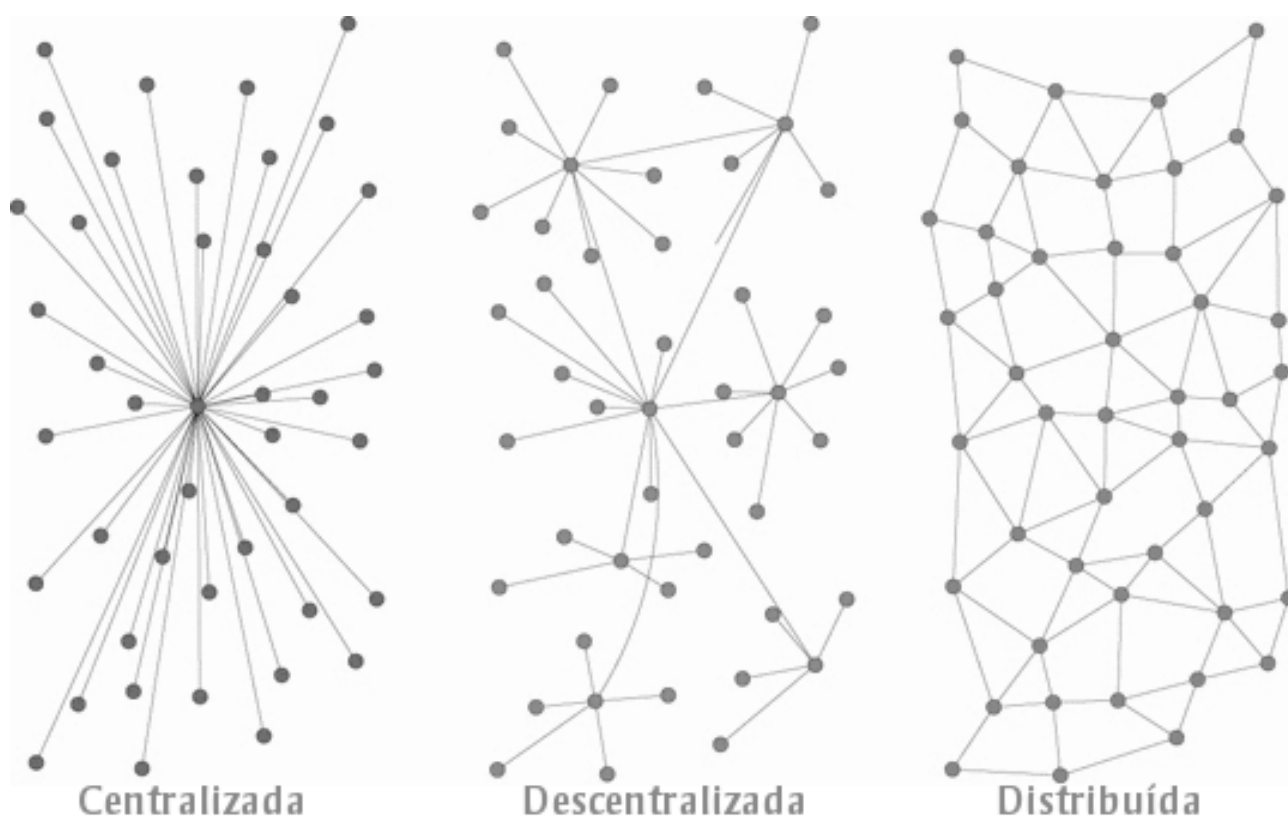
Esse termo é comum na área contábil e se refere ao livro onde estão citadas e registradas as transações e as contas de transação de um determinado negócio ou sistema. Todas as transações são registradas nesse livro.

No caso do BTC, esse livro é digital e sustentado por um sistema inteligentíssimo chamado Blockchain.



O QUE É BLOCKCHAIN?

A Blockchain (rede de blocos) é o funcionamento do livro-razão mantido por uma rede de computadores que são individualmente chamados de “nós”. Todos eles são conectados entre eles pela rede Blockchain, promovendo as trocas Peer-to-Peer (P2P) dentro do sistema e atualizados com as mesmas informações da rede. Pela rede ser composta por milhares de computadores, não é necessário um servidor central para o controle de tudo, e por isso não é necessária a centralização de controle de todas as transações. Por isso, chamamos a rede Blockchain de rede descentralizada:



Uma rede centralizada, como mostra a imagem acima, possui um “hub” central que detém todas as informações importantes



daquele sistema, e isso o torna extremamente frágil. Suponha que ocorra um ataque à rede centralizada. Todas as demais extremidades da rede tendem a sofrer e/ou deixar de existir porque a unidade central foi prejudicada. Enxergando tudo isso em nossa realidade, o sistema bancário atual é totalmente centralizado. Todos estão ligados em hubs centrais, e todos são prejudicados – na verdade eles não, mas os correntistas sim – em crises severas.

A rede descentralizada, por outro lado, possui vários “hubs” espalhados e caso algum desses “hubs” sofram algum tipo de ataque, ele não se estende para a rede toda, e o dano se limita apenas àquele hub.

Nas redes distribuídas, sempre que um ataque à rede é efetuado, ele é local e não se ramifica de forma alguma. A única forma de fazer com que o sistema todo sofra, é se a rede toda resolver se voltar contra ele mesmo, como um ataque autoimune.

Onde eu quero chegar com isso? Podemos dizer que o Bitcoin é uma rede de pagamentos descentralizada, por não ter nenhuma entidade ou instituição central para fragilizar o sistema, mas sua rede de verificação de transações, realizada pelos mineradores (vou falar sobre isso adiante, não se preocupe), funcionam de forma distribuída. Ou seja, o Bitcoin é descentralizado que utiliza uma rede distribuída.



Todas as transações que ocorrem dentro da Blockchain são ordenadas de forma cronológica e distribuídas em pacotes de arquivo de dados que chamamos de “blocos”. Um novo bloco de dados é formado a partir do momento que o último está cheio, pois cada um deles tem um tamanho predefinido de 1MB. O bloco posterior tem o hash (o código que identifica o bloco) do anterior, pois todos eles estão conectados entre eles, formando então uma rede de blocos.

Para você entender melhor o que é um hash, compare-o com um problema matemático difícil de ser resolvido, que apenas um computador pode resolver em segundos, talvez minutos.





Cada bloco precisa resolver o problema criptográfico do bloco anterior, e nenhum bloco é formado se o problema não for resolvido. Com isso em mente, nós podemos afirmar que a formação de um bloco exige trabalho, concorda?

Esse trabalho usará de processamento computacional, energia elétrica (os computadores estão ligados à energia) e tempo. Ou seja, cada bloco formado precisa provar o seu trabalho, a isso chamamos de “Proof of Work” (Prova de Trabalho).

No seu White Paper, Satoshi Nakamoto descreve isso de maneira simples. Ele descreve o sistema como uma rede de computadores P2P (Peer-to-Peer) e todos eles são elegíveis para achar a resposta do problema criptográfico. O primeiro “nó” (um conjunto de computadores que participaram daquele trabalho) a achar a resposta é recompensado com uma certa quantidade de Bitcoins. Ou seja, Bitcoins são dados como incentivo para o “nó” que é merecedor por completar a tarefa com sucesso.

A solução deste problema matemático e o trabalho computacional, energético e cronológico que ela gera se chama MINERAÇÃO. Vou falar sobre isso com mais detalhes mais para frente, mas pense junto comigo no ouro ou qualquer minério. A mineração deles exige trabalho, por parte do minerador ou da máquina, energia (elétrica ou não) e tempo. O princípio para o BTC é o mesmo.



A dificuldade de mineração, independente do número ou da capacidade de processamento dos computadores, sempre será ajustada pela rede para que o tempo de mineração (formação) de cada bloco seja de 10 minutos, ou 6 blocos por hora.

Se você está confuso(a), não se preocupe. Vou falar mais sobre tudo isso no decorrer deste livro. Como eu disse no título, o meu objetivo é que você entenda a lógica da revolução que você não pode ficar de fora.





Os 21 milhões de Bitcoins





Nessa altura do campeonato você já tem uma certa noção do que é Bitcoin e como essa “loucura” surgiu. Neste capítulo, quero aprofundar mais um pouco sobre o assunto.

Já sabemos que o Bitcoin é um dinheiro virtual, ou dinheiro eletrônico. Qualquer pessoa na posse de uma moeda dessas pode enviar dinheiro para qualquer lugar do mundo, a qualquer hora, sem precisar passar por validações de instituições bancárias ou uma autoridade central que manda em tudo. Em resumo, se você quiser enviar o seu Bitcoin para um amigo que está no Japão às 2 horas da manhã, você pode, e ele receberá quase que instantaneamente. Basta as duas partes terem uma wallet de onde as moedas vieram e para onde irão. A wallet é um endereço que mais se parece com um código de 34 caracteres, e todas as transações são registradas na Blockchain, como já mencionamos.





Existe um detalhe importantíssimo em meio a isso tudo e quero dedicar essa parte deste livro para te explicar. Você lembra que comparamos o Bitcoin com o ouro? O que vou te falar agora vai reiterar esse fato. Você precisa concordar comigo que a quantidade de ouro no planeta terra é limitada, certo? A quantidade de Bitcoins também é!

O número total de BTC's é de 21 milhões de moedas. Depois disso, mais nenhuma será minerada ou criada – vou explicar com mais detalhes sobre “mineração” depois. Eu suponho que algumas perguntas surgiram na sua cabeça, como por exemplo: “Quantos bitcoins já foram minerados até hoje?”; “E quando não for mais possível minerar BTC's, o que acontece?”; “Quer dizer que ele é um recurso escasso assim como o ouro?”. Vamos devagar e vou respondendo essas perguntas.





Satoshi Nakamoto estabeleceu o número limitado de moedas para evitar exatamente aquilo que teria sido um dos problemas para o seu surgimento: **inflação**. Lembra que a partir de um determinado momento, os governos poderiam imprimir o dinheiro que quisessem e assim fazer com que a moeda perdesse o seu valor? Com o número limitado de moedas isso não acontece.

O mais incrível é que o próprio sistema “controla” – aspas porque quem controla é um algoritmo matemático e não alguém ou algo – de duas formas diferentes. A primeira delas é que, como mencionamos, cada bloco formado na Blockchain demora aproximadamente 10 minutos para ser formado. Com o aumento do número de computadores minerando e validando as transações dentro do sistema e com a modernização da tecnologia dos processadores, o poder de processamento





umenta exponencialmente o que acarreta, logicamente, em um tempo menor para que o bloco seja formado, já que o tamanho dele sempre será de aproximadamente 1MB. Em outras palavras, se eu tiver um computador mais potente, ele processará 1MB muito mais rápido. Com isso, o algoritmo da Blockchain estabelece que quanto maior for a capacidade de processamento dos computadores, maior será a dificuldade de mineração, para que o tempo de formação de cada bloco se mantenha constante em 10 minutos. Em outras palavras, quanto mais BTC's são minerados, quanto mais computadores estiverem ligados na rede, quando mais BTC's surgirem, mais difícil será a mineração, maior será a exigência de poder de processamento, maior será a quantidade de energia elétrica despendida, mais caro será todo o processo e então mais lento será o surgimento de novas moedas.

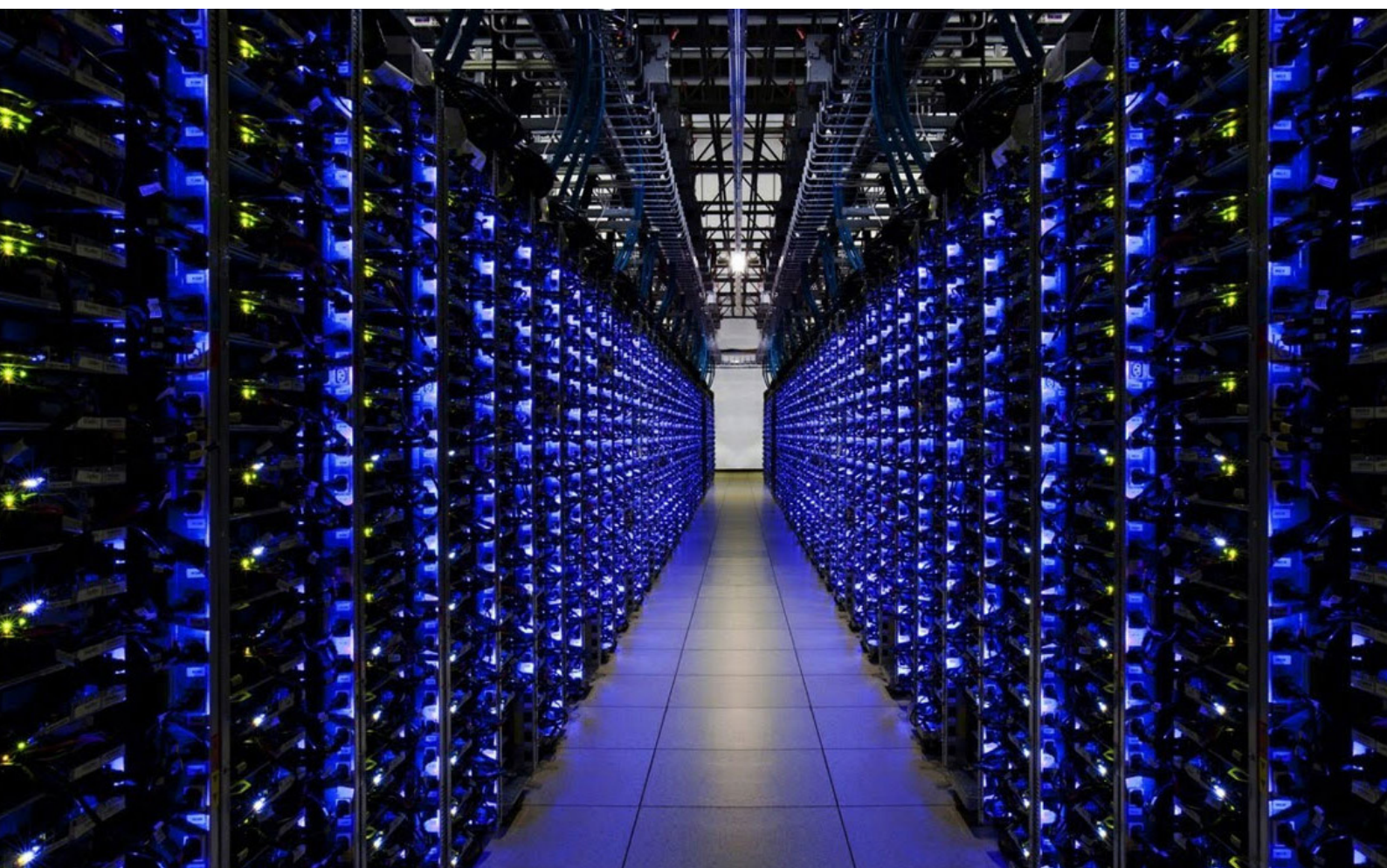
Com as palavras que usamos no capítulo anterior, a Prova de Trabalho para minerar um BTC será cada vez maior, ou seja, será necessário muito mais capacidade de processamento computacional e, conseqüentemente, muito mais energia elétrica para que um bloco seja formado sempre em 10 minutos.

No início, era possível minerar BTC's com um computador normal, desses que trabalhamos no nosso dia a dia. Atualmente isso é impossível. Eles não têm processadores capazes de fazer



isso. Para você ter uma ideia, hoje a energia elétrica gasta em mineração de BTC's supera a quantidade de energia elétrica necessária para abastecer a Nova Zelândia (BANSAL, 2018, p. 20).

Outro fator que controla o surgimento dos blocos é o que chamamos de “Halving”. Como mencionamos, a mineração gera aos computadores envolvidos na formação de cada bloco uma recompensa em BTC. Esta recompensa era de 50 BTC's por bloco em 2009, mas hoje ela já é bem menor porque o Halving acontece a cada 210.000 blocos formados. Se considerarmos os 10 minutos para formação de cada bloco, a cada quatro anos a recompensa da mineração cai pela metade. Como a mineração





gera custos, a partir do momento que a recompensa não se torna mais atrativa para alguns mineradores, os computadores são desligados, diminuindo a capacidade de processamento de todo o sistema de “nós”, aumentando a dificuldade de mineração dos blocos, diminuindo o surgimento de novos BTC's. Atualmente, a recompensa é de 12,5 BTC's por bloco, mas em junho de 2020 teremos outro halving que diminuirá esse número para 6,26 BTC's (<https://blockgeeks.com/guides/bitcoin-halving/>).

Hoje, mais 80% das moedas já foram mineradas, o que representa mais de 18 milhões de BTC's (<https://coinmarketcap.com>). Pelos cálculos, a data para chegarmos ao número de 21 milhões é o ano de 2140.





Como funciona a mineração?





O Bitcoin e o Blockchain não funcionam se não existir mineração. De forma mais técnica, a mineração dos BTC's trabalha na SHA256 (Secure Hash Algorithm), que é um tipo de criptografia que gera um resultado criptografado de 256 bits para a validação das transações dos blocos. Ela é parte fundamental para que todo o sistema se mantenha funcionando e moedas possam ser compradas e transacionadas. Por isso, ao desenvolver toda a sua ideia, Satoshi Nakamoto estabeleceu que o processamento de validação de todo ecossistema seria chamado de MINERAÇÃO, dando a entender que os “nós” responsáveis pela validação dos blocos merecem uma recompensa.

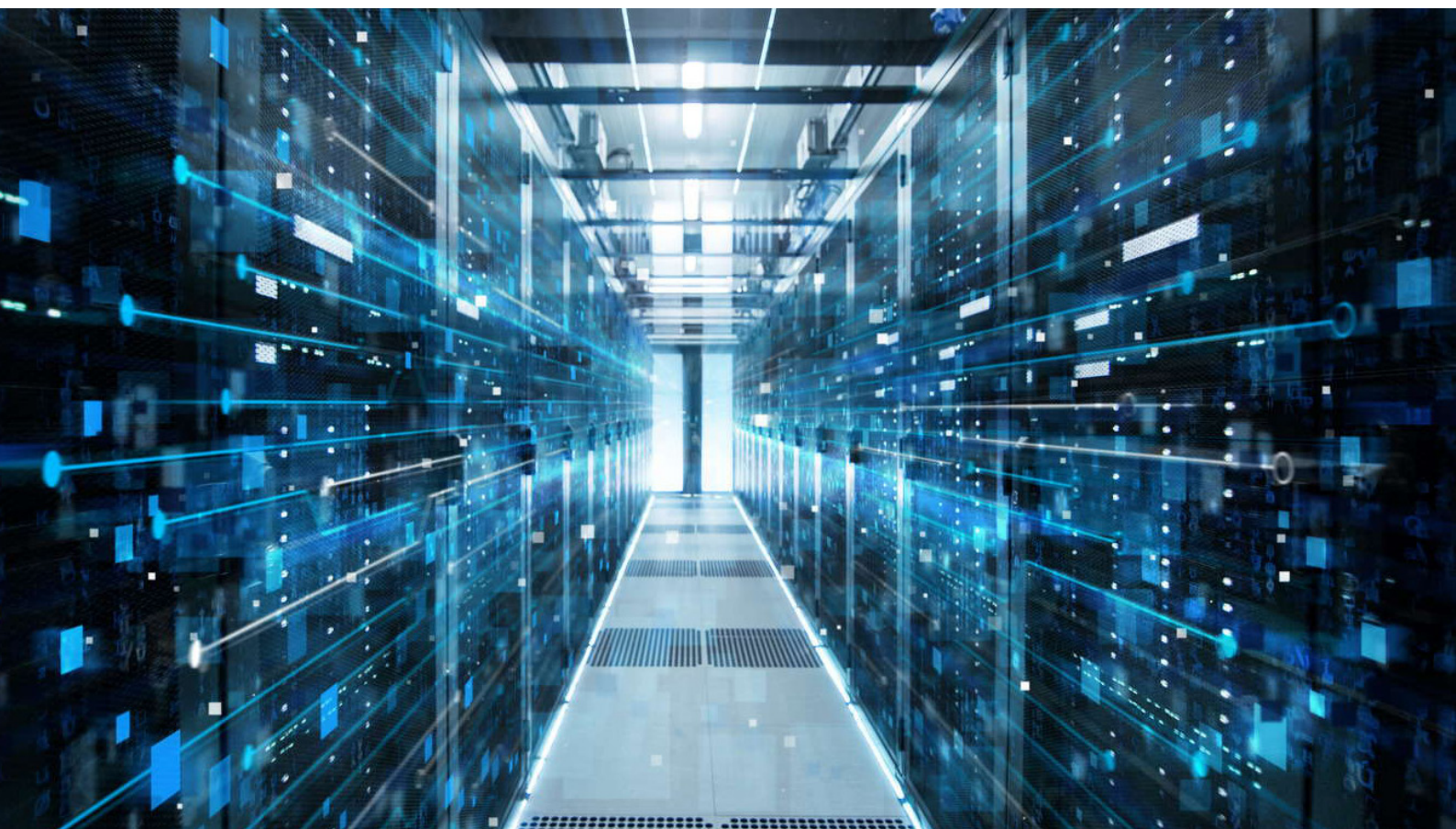
Como já mencionei, no início de tudo a mineração poderia ser realizada em computadores normais. Com o aumento do valor do BTC, grande parte dos mineradores começou a perceber que poderiam ganhar mais dinheiro se minerassem mais blocos. Claro, qualquer um de nós faria isso, já que a recompensa é proporcional ao número de blocos minerados. Quanto mais eles mineravam, mais blocos eram validados e, conseqüentemente, mais eles ganhavam.

Com isso, começaram a surgir empresas e mineradores desenvolvendo processadores cada vez mais potentes em busca de maior lucro. O que muitos não se atentaram é que com o aumento de capacidade de processamento, a mineração diminuiria sua recompensa, já que o tempo de formação de cada bloco deve ser constante e que existe um número máximo



de BTC's. Dessa forma, o processo de mineração passou a ser muito caro, não cobrindo os seus custos, fazendo com que muitas empresas com centenas de computadores fechassem as portas e se mantivessem no mercado apenas as grandes donas de patentes e grandes fábricas de processadores.

Não é tão simples minerar o bitcoin, especialmente em um país como o Brasil. O primeiro fator a ser levado em conta é o valor do computador. Se considerarmos que grande parte das máquinas à venda estão no exterior, paga-se impostos de importação e o fator câmbio é bem significativo. Além disso, o custo da energia elétrica no Brasil é mais caro do que em outros países e, como falamos, quanto mais processamento, maior é o consumo de energia elétrica. Ao falar que não era simples minerar em solo brasileiro, eu estava sendo modesto.





A verdade é que aqui dificilmente a recompensa da mineração cobrirá os seus custos e muitos mineradores fecharão as portas em poucos meses ao constatarem que seu investimento retornará em anos, ou nunca acontecerá.

Atualmente, uma das maiores mineradoras é a Bitmain, de Pequim, na China. Coincidentemente ou não, ela é a maior fabricante de máquinas mineradoras de todo mundo e especula-se que ela “seja dona” de 40% de toda a mineração do Bitcoin.

Certo, pausa no assunto para eu fazer uma confissão pra você. Eu já comprei essas máquinas e a experiência foi péssima. Ao chegar no Brasil, a mineração com elas já “não se pagava”, ou seja, demoraria anos para retornar o meu investimento. Sabe o que aconteceu? Nunca liguei essas máquinas! É ruim falar isso, mas às vezes é preciso errar para aprender uma grande lição.

Você talvez se pergunte: “Mas será que é tão caro mesmo?” Bom, vou te falar alguns números. Os computadores custavam por volta de US\$ 1.000,00 cada um. Além disso, como eles consumiam muita energia elétrica, tínhamos que fazer uma reforma elétrica no local onde as colocaríamos, o que nos custaria por volta de R\$ 20.000,00. Cada máquina consumia cerca de 900 kwh mensalmente, gerando um custo aproximado de R\$ 1.000,00 por máquina em um mês. No final das contas, o que a máquina minerava não pagava a conta de energia elétrica.



Como mencionei, a mineração gasta tanta energia, que a quantidade gasta para minerar o sistema atualmente poderia abastecer um país todo como a Nova Zelândia.

Com toda essa dificuldade, surgiram os chamados “*Mining Pools*”, que na tradução literal significa “Piscinas de Mineração”. Nesse caso, você pode comprar ou investir em uma espécie de cota para participar da mineração de alguma grande empresa que disponibiliza essa possibilidade no mercado. Com isso, você não precisa comprar uma máquina, fazer toda a instalação, ligar na energia elétrica, colocar para funcionar e torcer para dar certo.

A grande questão é que existem alguns problemas quando tratamos disso. O primeiro deles é que existem inúmeras Mining Pools que são fraudes ou golpes.





Ou seja, você acha que está comprando alguma cota, mas na realidade aquilo nem existe, ou não dá resultado algum. O segundo é que nem assim a mineração é rentável. Você pode até ganhar alguma “coisinha,” mas absolutamente nada significativo e, no final das contas, o seu investimento demorará anos para retornar ao seu bolso. Existem inúmeros investimentos mais rentáveis com muito menos riscos.

No final das contas, mineração é coisa pra gente grande que já está no mercado há um tempo, tem tecnologia proprietária e está em países onde o custo de energia elétrica é baixíssimo se comparado ao Brasil. Recomendo você investir em Bitcoins de outra forma, é isso que vou te mostrar.





A sua Wallet





Talvez você já tenha ouvido alguém falar: “Me passa sua wallet para enviar o Bitcoin”, “Na wallet do Satoshi tem muitos bitcoins”. Mas o que será que são wallets? A palavra Wallet, traduzindo para o português, significa Carteira, e ela tem as mesmas funções que as carteiras convencionais que nós temos para guardar dinheiro, mas nesse caso ela guarda bitcoins e de forma digital.

Neste capítulo vou falar quais são os tipos de carteiras existentes, quais são as suas principais características e, dessa forma, te ajudar a escolher a melhor wallet para você. As Bitcoin Wallets, carteiras virtuais de Bitcoin, são ferramentas criadas por empresas para que você acessar as chaves criptografadas que provam a posse das suas moedas, são formas de você acessar os seus bitcoins mediante o fornecimento das chaves privadas.

Quero te mostrar quais são os tipos mais conhecidos de Carteiras de Bitcoin. Veja:





WALLET DESKTOP



São carteiras virtuais instaladas no seu próprio computador, ou seja, as chaves privadas são armazenadas no disco rígido do seu computador, HD.

Esse tipo de carteira é segura pelo fato do seu computador estar normalmente em casa ou em lugares onde só você tem acesso. Uma das desvantagens é o fato de que, caso você perca o computador, você perderia o acesso aos bitcoins. Já vimos essa história acontecer no passado.

Existe uma história famosa sobre um rapaz que perdeu 5.000 bitcoins porque jogou o computador fora quando o bitcoin não valia praticamente nada.



WALLET HARDWARE



É uma carteira que funciona como um pendrive na qual o investidor armazena suas chaves. Uma das vantagens desse tipo de carteira é que você precisa ter o dispositivo para acessar os fundos e, como esses dispositivos normalmente são protegidos por senhas, você tem um aumento da segurança. A desvantagem é a falta de praticidade para acessar e configurar.

WALLET MOBILE

Provavelmente este é o tipo de carteira mais usada pelos usuários que estão começando ou que gostam de praticidade. Quem quer ter a possibilidade de enviar seus bitcoins a qualquer momento e em qualquer lugar, essa wallet é perfeita.



São aplicativos instalados no celular nos quais você cria uma carteira deixando as chaves privadas armazenadas dentro do aparelho. O ideal é que as chaves também sejam anotadas fora do celular em caso de perda do celular. Assim, ao comprar um celular novo, é possível fazer o backup da carteira usando as chaves anotadas.

Caso você tenha valores mais altos investidos, acima de 0.5 BTC, seria interessante partir para uma Wallet Hardware, porque querendo ou não, estamos falando de valores financeiros mais altos.

WALLET PAPER



Caso você seja aquela pessoa que acredita que a todo momento está sendo vigiado e que seu computador e celular não são



lugares confiáveis para armazenar nada, muito menos Bitcoins, essa wallet é feita para você.

Nesse tipo de carteira, você literalmente armazena seus Bitcoins dentro de uma folha de papel.

É um documento físico, que contém as chaves privadas e públicas. Sua grande vantagem é o fato de ser 100% offline, ou seja, ninguém terá acesso. O grande problema é que se você colocar fogo ou jogar o papel fora, não existirá meios de recuperar o Bitcoin.

“Bom, já entendi as formas de guardar meus bitcoins, agora quais os próximos passos que devo dar?” Quero mostrar como você faria a criação da sua primeira carteira.

Para isso, usarei o exemplo da Wallet Mobile, carteira de bitcoin de celular, pois é o tipo mais usado e mais simples de entender. Inclusive, esse foi o tipo de carteira que eu usei quando me inseri nesse universo.

Para começar, basta você ir para o Google Play ou App Store e baixar uma carteira do seu interesse. A que eu utilizei e é a mais comum e se chama *Blockchain.com*.



O passo a passo é bem simples de ser seguido.

- 1** Crie sua conta;
- 2** Crie um Pin;
- 3** Acesse o painel superior esquerdo e clique em “Fazer backup dos seus Bitcoins”;
- 4** Inicie o Backup. Nesta parte é muito importante que você anote estas palavras que vão ser geradas de forma extremamente segura. Estas palavras são o seu backup;
- 5** Pronto, sua carteira está criada e está pronta para receber bitcoin.

Para recebimento de Bitcoin, você pode ir no canto direito do aplicativo na parte de baixo e clicar em “Recieve”, que significa receber. Quando você clicar, irá aparecer um endereço cheio de números e letras, esta é sua chave pública, a responsável por receber o Bitcoin.

No próximo capítulo vamos aprender como comprar o bitcoin e enviar para esta carteira.



Como comprar Bitcoins





Após termos aprendido sobre diversos conceitos, acredito que chegou a hora de você começar a se expor a este ativo chamado Bitcoin. De forma simples e bem objetiva, quero exemplificar com um passo a passo como que você pode efetuar a compra de Bitcoin.

O passo “zero” é você achar uma corretora/exchange de confiança, uma corretora cuja reputação seja a melhor possível, impecável, de preferência.

No nosso exemplo, vou utilizar as telas modelo de uma corretora brasileira sem expor seu nome. Independente da corretora, os princípios deste capítulo são aplicáveis para qualquer corretora que você escolher.

Vou dividir este passo a passo em 3 partes, sendo elas:

- 1** Como abrir uma conta em uma corretora de Bitcoin;
- 2** Como depositar o dinheiro dentro da corretora e comprar o Bitcoin;
- 3** Como sacar o Bitcoin para sua wallet externa.



1. COMO ABRIR UMA CONTA EM UMA CORRETORA DE BITCOIN?



Para a criação de uma conta, para que seja possível comercializar os criptoativos, será necessário fazer um cadastro. Neste cadastro são pedidas algumas informações pessoais. Não se preocupe, se a corretora que você escolheu tem boa reputação é totalmente seguro fornecer essas informações. Elas são necessárias, para que o setor de Compliance da corretora avalie seus documentos e aprove sua conta. São procedimentos padrões para a sua segurança, mas também da corretora. Com esse procedimento, eles irão conferir se você existe de verdade ou se não é uma tentativa de fraude ou golpe.



A tela de cadastro é muito parecida para todas as corretoras, possivelmente elas se pareçam com esta dela:

CADASTRE-SE

Pessoa física | Pessoa jurídica

Nome completo

E-mail:

Senha:

Confirme sua senha:

CPF

Data de nascimento

Criar sua conta | Já é cliente?

Ao clicar em **Criar sua conta** você aceita os nossos [Termos e Condições](#) e [Política de Privacidade](#)

Uma vez feito o cadastro e confirmadas as suas informações, a sua conta provavelmente será liberada para que você faça o login. Feito o login, será necessário enviar a foto de alguns documentos, como sua identidade (RG ou CNH) e comprovante de endereço. Tudo isso ainda faz parte do procedimento de Compliance.



Se tudo estiver de acordo, sua conta será aprovada. Nesse momento, você pode avançar ao segundo passo: “carregar” a sua conta com REAIS para a compra do(s) seu(s) bitcoin(s).

2. COMO DEPOSITAR O DINHEIRO DENTRO DA CORRETORA E COMPRAR BITCOIN?

Com a sua conta na corretora aprovada e com dinheiro na sua conta bancária pronto para ser enviado para a corretora, o que você deve fazer agora é acessar o campo de depósito na sua corretora e selecionar a opção “reais”.

Aparecerá na sua tela a conta bancária da corretora para que o depósito para a corretora seja feito.

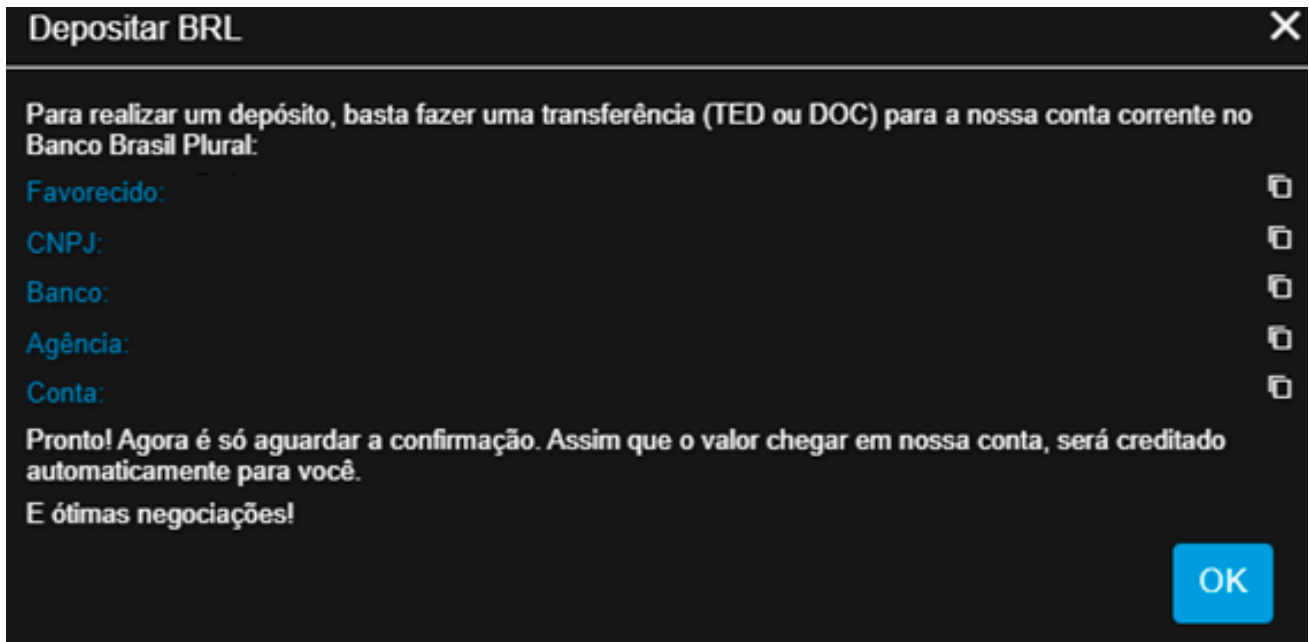
De forma automática, sempre que o depósito for feito, a corretora identificará que o dinheiro veio da sua conta bancária e liberará o saldo correspondente na sua conta da corretora.

Importante fazer um alerta para uma coisa: Sempre, absolutamente sempre, deposite o dinheiro da conta bancária em seu nome e CPF, não de outra pessoa.

Como o reconhecimento do depósito é feito de forma automática, caso o depósito seja feito em nome de outra pessoa, as informações conflitam e você vai ter um trabalho gigante para reverter isso.



A tela de depósito será parecida com esta:



Dinheiro na conta da corretora, saldo liberado para eu comprar Bitcoin. O que eu faço agora?

Primeiro você terá que ver o livro de ofertas, para saber o valor que estão cobrando pelos Bitcoins e se existem ordens de venda. A figura a seguir é um exemplo de livro de ofertas, no qual podemos ver o preço que estão cobrando por Bitcoin e o volume que estão comprando ou vendendo. As ordens em vermelho são ordens de venda, e as azuis são ordens de compra.

Analisando as ordens, podemos ver que posso comprar uma fração de Bitcoin ou um Bitcoin todo.



LIVRO DE OFERTAS	
Preço (BRL)	Volume (BTC)
34042.54	0.04650000
34039.78	2.60000000
34000.00	0.55748900
33997.00	0.00132071
33988.81	0.10000000
33971.57	0.01302039
33903.01	0.17478125
203.01 BRL spread	
33700.00	2.07723590
33641.17	0.56998597
33600.00	0.00004000
33500.01	0.10000000
33500.00	0.00216029
33495.00	0.03069085

Para colocar a ordem de compra e para que ela seja executada de forma rápida, utilize a “compra a mercado”, este é um tipo de ordem que não leva em consideração o preço da ordem executada. Ele comprará a quantidade que você quiser no preço em que o mercado está vendendo.

Sempre uso esse modelo de ordem para compras pequenas. Para compras maiores utilizo o tipo de ordem limite, que se resume em uma ordem na qual eu estipulo o valor que quero vender ou comprar o bitcoin. Assim, a ordem só será executada quando chegar ao meu preço.



Este é um tipo de formulário de envio de ordem de compra e venda:

The screenshot shows a dark-themed mobile application interface for placing an order. At the top, the word "ORDEM" is displayed. Below it, there are three buttons: "MARKET" (selected), "LIMIT", and "STOP". Underneath, there are two buttons: "COMPRAR" (highlighted in blue) and "VENDER". A section labeled "Quantidade compra" contains a text input field with the number "1" and a dropdown menu set to "BTC". Below this, a summary table shows: "Mercado: 33.880,00 BRL", "Ordem Total: ≈ 33.987,10 BRL", and "Taxas: ≈ 0,00250000 BTC". At the bottom, there is a large blue button labeled "CONFIRMAR ORDEM" and a link for "Ordens Avançadas".

Uma vez confirmada a ordem, você terá o seu saldo em reais debitado e aparecerá o valor em Bitcoin na sua conta.

Mesmo que a exchange tenha uma excelente reputação, nunca deixe seus bitcoins dentro dela.

De forma rápida, se você deixar, a corretora estará com a posse de suas chaves privadas e lembre-se que quem possui as chaves privadas, possui a carteira. Ou seja, nesse caso a corretora será dona da sua carteira.



3. COMO SACAR O BITCOIN PARA SUA WALLET EXTERNA?

Primeiramente, precisamos acessar o campo de saques e ir até as criptomoedas e selecionar o Bitcoin.

Quando você for sacar a criptomoeda, ele irá pedir um endereço de carteira para envio. Esse endereço é o endereço da “wallet” que você tem.

No capítulo anterior vimos quais tipos de wallets existem e, provavelmente, você escolheu uma e fez o “setup” dela. Caso você tenha feito, você poderá acessar essa “wallet” que você criou e pegar o endereço de recebimento e assim usá-lo na corretora para o envio das moedas.

O campo de envio da corretora deve se parecer com este:

Sacar BTC ✕

Informe o valor (saldo: 0,00379050, mínimo: 0.0004)

0,0 Valor total

Taxa: 0,00040000
Valor líquido: -0,00040000

Informe o endereço de destino

Ex: 3Jojx2v93oZbZRyXGvCP22t55ETxRpyaKf

O endereço de destino está correto.

A carteira deste endereço é de BTC.

✓ Você receberá um email para confirmar o saque.
✓ Após a confirmação do email, os dados são enviados para a blockchain e o processo segue por lá.
✓ As confirmações na rede blockchain podem levar de segundos a 1 hora.

Enviar



Uma vez solicitado o saque, você só precisa aguardar o envio das moedas feito pela corretora, vale lembrar também que muitas corretoras pedem para que seja feito uma autenticação via e-mail, apenas para confirmar se você realmente pediu o saque da corretora.

Não é tão difícil quanto parece. Na verdade, é quase intuitivo, se você tem alguma familiaridade com o seu celular, você vai tirar isso de letra.





Posso pensar no BTC como investimento?





Se eu pudesse estar aí com você pessoalmente te explicando isso, eu tentaria te convencer de todos os modos que esse é o capítulo mais importante deste livro. É decisivo, importante e “*game changer*”.

Esse capítulo é o pulo do gato. Garanto que se você entender o que vou te dizer, o seu modo de pensar investimentos vai mudar, especialmente quando falamos de moedas digitais. Para ficar mais fácil, vou dividir tudo em alguns tópicos e vou introduzindo alguns conceitos importantíssimos com calma.

Antes de qualquer coisa, não existiria momento mais propício para eu estar escrevendo isso. Hoje é dia 12 de março de 2020, e com toda certeza você se lembrará por alguns anos o que está acontecendo agora. Estamos no que, até o momento pelo menos, é o auge da crise causada pelo novo Coronavírus, uma gripe letal que está se alastrando no mundo rapidamente.

A bolsa de ações brasileira despencou mais de 20% e teve o seu segundo “circuit breaker” no intervalo de uma semana. Circuit Breaker é uma suspensão das negociações quando a queda é maior do que 10%. Com palavras simples – a bolsa parou duas vezes de trabalhar porque caiu mais de 10% em dois dias.

A OMS (Organização Mundial da Saúde) declarou que o Coronavírus, tecnicamente chamado de Covid-19, já é uma **pandemia** e muitos campeonatos esportivos como a NBA (liga



de basquete americana) e campeonato espanhol de futebol foram suspensos por tempo indeterminado. Outros eventos esportivos estão ocorrendo, mas sem presença do público e a Itália, país que passa pelo maior surto do vírus no momento na Europa, está com as fronteiras fechadas. Além de tudo isso, os EUA fecharam as suas fronteiras para todos os voos vindos da Europa.

Ainda não há vacina para a gripe causada pelo vírus, que se espalha rapidamente, e - “chute” meu - é uma questão de tempo para que outros eventos de ajuntamento sejam proibidos e suspensos.





Além disso, a Arábia Saudita, uma das maiores produtoras de petróleo do mundo declarou o aumento da sua produção. Esse aumento gera um pico na oferta de petróleo no mercado e, já que a demanda se mantém a mesma, o preço do barril do petróleo diminuiu. Diminuindo o preço, as empresas que possuem um custo de extração maior em outros países diminuem significativamente suas margens de lucro. Como estas empresas, algumas estatais, outras de capital aberto em bolsas de valores, têm milhares de acionistas, o seu valor na bolsa de valores diminuiu, gerando ainda mais caos para o que já estava caótico.

“Mas Felipe, por que estamos falando disso tudo?” Porque nesse capítulo falo sobre investimentos. Nesse cenário apocalíptico que acabei de descrever, muitos investidores despreparados e inconsequentes perderam muito, ou todo o seu dinheiro.

Quem não sabe investir, perde dinheiro. Isso é um fato! Isso faz a pergunta do título deste capítulo ser ainda mais importante. E a resposta dela ainda mais. A resposta é um sonoro “SIM!”, Bitcoin e outros criptoativos podem ser considerados investimentos incrivelmente rentáveis, proporcionalmente voláteis, mas seguros se tudo for feito da maneira correta.

Como falei no início deste livro, não estou aqui para te dar dicas para ficar milionário em pouco tempo. Meu objetivo é criar em



em você uma consciência de que é possível ganhar bastante dinheiro com criptoativos, mas que isso precisa ser feito de maneira segura – muito segura. Agora que estou onde eu preciso para eu começar a te explicar tudo que você precisa saber para investir de maneira correta e participar da revolução do dinheiro, vou avançar.

O CISNE NEGRO

Parece até loucura falar de cisnes para falar de investimentos, mas sinceramente, é um conceito que você precisa entender e que pouquíssimas pessoas entendem.

Quem inventou esse termo foi um cara chamado Nassim Nicholas Taleb. Ele é escritor, filósofo e estatístico, além de ser um megainvestidor nos EUA e participar de um fundo que *performa* muito bem ao longo de todos os seus anos.

O cenário que descrevemos no início do capítulo representa bem o que ele chama de Cisne Negro, um evento raro, improvável e muitas vezes catastrófico, que pega de surpresa os mais desavisados e inconsequentes, muito bem abordado em seu livro “A lógica do Cisne Negro”. Taleb usa esse conceito para provar que é impossível prever o futuro, embora muitos no mercado financeiro – ou até fora dele – tentem fazê-lo. Ninguém podia



prever o 11 de setembro e suas consequências, assim como ninguém poderia prever as consequências do novo Coronavírus. O conceito tem origem no fato de que no século XV os ingleses acreditavam existir apenas cisnes brancos, mas tudo mudou depois que um cisne negro foi avistado na Austrália.

Um exemplo muito bem-humorado usado por Taleb para descrever um “evento cisne negro” é o ciclo de vida de um peru de natal. Ao longo de todo ano, o peru é engordado, alimentado e cuidado para ter a maior quantidade de carne possível. Se analisarmos o peso do animal ao longo do ano, perceberemos que ele formará um gráfico crescente, extremamente otimista. Pois é, no final do ano o cisne negro acontece.

Aquilo que era um otimismo enorme, justamente no momento que o animal estava mais empolgado e com o cenário otimista de sua evolução anual, ele morre! Tudo aquilo que ele tinha conquistado foi perdido em questão de minutos. Um evento único determina o seu fim.

Se os nossos investimentos não forem feitos de maneira correta, corremos o mesmo risco. Um único evento pode nos levar à lona como um lutador, que com um soco sofre o nocaute.



O ANTIFRÁGIL



Já falamos de cisnes, agora vamos falar de uma palavra que nem existe no dicionário. Isso está ficando bom, não é? Não desista, tudo vai fazer sentido daqui a pouco!

Também criado por Nassim Taleb, esse conceito envolve o entendimento de que se necessita fugir de qualquer tipo de fragilidade.

Pense da seguinte forma, existem objetos extremamente frágeis, não é? Um exemplo que gosto de usar, e ele mesmo usa, são taças de cristal. São tão frágeis que para lavá-las precisamos ter cuidado dobrado para não as quebrar. Para o transporte delas precisamos protegê-las com o máximo cuidado.



Quando pensamos na antítese, no contrário de “frágil”, logo pensamos em um objeto que não quebra, concorda? Uma pedra, por exemplo. Não importa o que você faça com uma pedra, dificilmente ela quebrará ou sofrerá algum dano. A grande questão levantada por Taleb é que aquilo que pensamos ser o contrário de “frágil” não está correto. A pedra, segundo o nosso exemplo, pode ser considerada robusta, pode sofrer pancadas fortes, mas não se abala e não perde nada.

O grande problema levantado pelo autor em seu livro “Antifrágil” é que o robusto, embora seja melhor que frágil, permanece sempre da mesma forma, não muda, não cresce. E isso não é exatamente o contrário de “frágil” já que, neste caso, quando algum evento drástico acontece, o objeto se quebra.





Pensando nisso, ele estabelece que o contrário exato para aquilo que chamamos de fragilidade é a antifragilidade. Ao invés de quebrar como o frágil, e em vez de se manter como está o robusto, ao ser exposto a um evento prejudicial, o Antifrágil fica mais forte e cresce. Se usarmos o exemplo da taça de cristal, é como se a cada vez que submetêssemos uma taça a uma força que a quebraria, ela ficasse ainda mais forte.

Trazendo à tona o tema investimentos, Nassim Taleb ensina que quando um Antifrágil, aquela pessoa que investe levando em conta esse conceito, está diante de um Cisne Negro negativo, como o que descrevemos no início do capítulo, ele ganha em vez de se manter estável ou invés de quebrar.

Um Antifrágil prepara seus investimentos de forma que possa ganhar em todos os cenários possíveis, especialmente nos negativos. Aliás, se existe um momento no qual o Antifrágil realmente ganha, esse momento é no Cisne Negro negativo.

Por isso, Taleb usa uma figura muito interessante para descrever o conceito, a Hidra de Lerna. Segundo a mitologia grega, a Hidra era um animal com corpo de dragão e várias cabeças de cobra que ao ser atacada e ter uma de suas cabeças arrancadas, duas nasciam em seu lugar. Ou seja, a cada golpe que levava, a Hidra ficava mais forte.



Em resumo até aqui, eu quero que você perceba que existem eventos que estão fora do nosso controle e que podem dizimar nossos investimentos. Não ache que eu exagero. Em 2008, na última grande crise, quem estava investindo em bolsa perdeu pelo menos 40% do seu investimento. No caso de alguns, o evento os tirou do jogo.

Para lidar com esses eventos e, inclusive, lucrar com eles, é preciso estar Antifrágil, preparado para esses eventos, sem depender da sorte ou do acaso.

EFEITO LINDY



Existem algumas coisas que você precisa levar em conta para “entrar Antifrágil” no mercado. Uma delas é o efeito Lindy, um conceito muito simples e que pode mudar a sua forma de ver como o jogo funciona.



Esse conceito foi criado por Albert Goldman na década de 60 e dizia que a expectativa do futuro da carreira de um comediante na televisão americana era proporcional à metade de sua exposição no passado. Ele queria dizer que quanto mais tempo o comediante já estivesse trabalhando na televisão, mais tempo ele se manteria por lá. Se estivesse há 10 anos, a lógica era que ficaria mais cinco anos, pelo menos.

Apesar de Goldman ter inventado o conceito, foi Benoit Mandelbrot que o provou matematicamente, e ainda deu um “upgrade” na ideia. Mandelbrot concluiu que o futuro não dependia da metade da exposição ao passado, mas sim do tempo total de exposição. Ou seja, se algo já dura 10 anos, existe uma probabilidade altíssima disso durar mais 10 anos.

Apesar de não poder ser aplicado em tudo na vida, o conceito faz muito sentido na maioria das vezes, especialmente quando tratamos de investimento. Vou te dar um exemplo bem simples e você vai precisar concordar comigo.

Você acha que usaremos garfos para comer daqui a 50 anos? Seguindo a ideia do efeito Lindy, eu digo que sim. Garfos já servem como ferramentas para ingerir alimentos desde, pelo menos, o século XI.

Ou seja, a probabilidade é altíssima que o uso dure algo proporcional ao tempo que já usamos.



Entenda isso na área de investimentos e você evitará muita dor de cabeça mais para frente. Invista naquilo que já se provou no tempo, não em invenções mirabolantes que ainda não perduraram por um bom período de tempo.

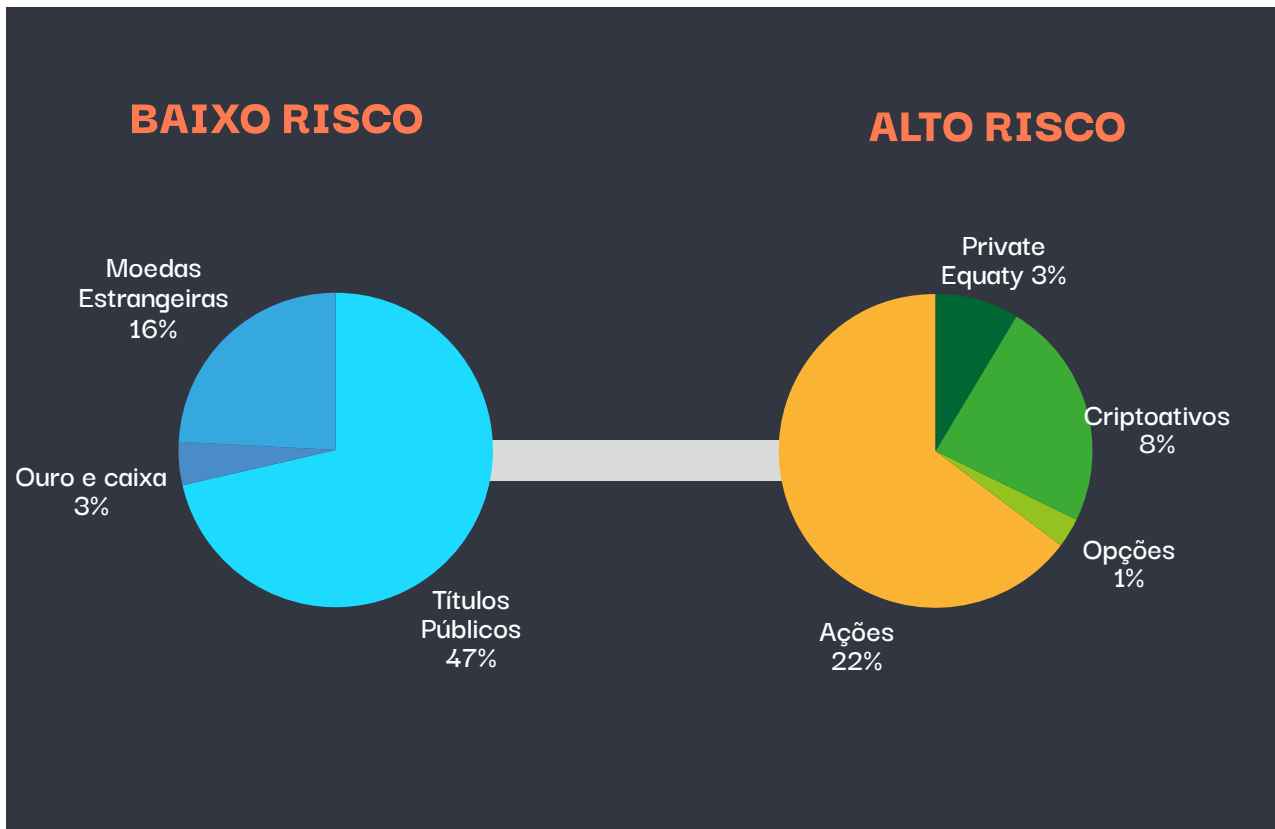
Você deve estar pensando: “O Bitcoin é muito novo, ele tem efeito Lindy?”. Chegarei lá!

ESTRATÉGIA BARBELL

Além de levar em conta o Efeito Lindy, ainda é necessário entender como distribuir os seus investimentos da maneira correta e Antifrágil. A estratégia barbell – que significa barra de supino, em inglês – é fácil de entender e tem a cara da Antifragilidade.

Não vou ficar enrolando, falando termos técnicos, mas em resumo, assim como uma barra de supino tem peso nos dois lados extremos da barra, os nossos investimentos devem estar alocados nos dois extremos: Alto Risco (Investimentos altamente agressivos) e Baixo Risco (Investimentos Extremamente Seguros). Fuja de investimentos de médio risco!

Como assim? Veja a imagem a seguir e você vai entender!



É simples, 65% a 80% do seu capital devem estar alocados no seu lado de Baixo Risco. Destes destaco os títulos de Renda Fixa, suas reservas de valor (ouro e caixa) e moedas estrangeiras fortes que te protegerão da desvalorização do Real.

No seu lado de Alto Risco, o restante do seu capital de investimento é alocado em alguns ativos – não precisa ser todos os que falarei – como as ações, os criptoativos, opções (derivativos) e Private Equity (participações em empresas).

Essa estratégia é segura e te ajudará a se proteger em casos de Cisnes Negros. Percebeu que os criptoativos fazem parte dos seus investimentos e onde eles se encaixam?

Você entende porque uma boa parte das pessoas que investem em criptoativos se decepcionam? Porque elas fazem errado. Colocam o dinheiro que não é para colocar e em uma



desvalorização abrupta causada pela alta volatilidade do ativo elas se decepcionam por perder dinheiro. A partir disso, passam a falar que Bitcoin é uma armadilha. Garanto, não é! Pelo contrário, o BTC tem se mostrado um ativo muito rentável e seguro!

BITCOIN JUNTO COM O OURO COMO RESERVA DE VALOR



Talvez eu nem devesse falar sobre isso neste livro, mas tenho a sensação de que preciso. Perceba que na parte de Baixo Risco da nossa estratégia Barbell citei ativos para nossa proteção contra Cisnes Negros negativos. Por exemplo, o dólar é a moeda mais forte de todo o mundo. Em uma crise, como a que estamos vivendo neste exato momento em que escrevo o livro, moedas mais fracas como o Real se desvalorizam muito, conseqüentemente o dólar fica muito mais caro. Se estiver bem posicionado, posso



proteger pelo menos parte da desvalorização gerada nos meus investimentos de Alto Risco (ações principalmente) que invariavelmente vão sofrer.

Ouro também é uma proteção contra o caos, por ser uma commodity, o que em caso de uma guerra, ou um cenário apocalíptico, é extremamente valioso. Não que você precise guardar ouro em casa, mas existem alguns índices atrelados ao preço do minério e você pode investir neles.

Alguns defendem, e de certa forma concordo, que o Bitcoin tem Efeito Lindy para poder ser comparado a uma reserva de valor, como o ouro. No mesmo cenário que imaginamos no caso do ouro, o Bitcoin seria uma solução para um caos generalizado nas moedas de todo o mundo.

Por exemplo, há pouco tempo a Argentina teve suas eleições e um novo presidente assumiu o comando. Como o novo presidente não era o que o mercado internacional desejava, com a já altíssima inflação existente e com a fuga do dólar dos investidores do país, o Peso, moeda argentina, desvalorizou-se abruptamente, causando um aumento significativo no dólar, a ponto do governo proibir a compra de dólares, já que as pessoas queriam proteger o seu patrimônio em alguma moeda que fosse forte.

Nesse cenário, comendo pelas beiradas, apareceu o Bitcoin como alternativa a essa proibição. Muitos argentinos começaram a investir em BTC's para proteger o seu dinheiro, o que levou



ao aumento de pelo menos 20% no valor do criptoativo. O que eu quero dizer com isso? O Bitcoin foi usado como reserva de valor para proteger os argentinos da desvalorização da moeda corrente no país.

ESTRATÉGIA BARBELL PARA OS CRIPTOATIVOS

Dê um *zoom* na parte de Alto Risco da nossa estratégia Barbell. Agora dê mais um *zoom* apenas na parte de Criptoativos. É possível imaginar uma estratégia Barbell apenas para as Criptomonedas, o que é muito inteligente.

Considere que os 65% a 80% do seu capital alocado em criptomonedas serão destinados para o extremo de Baixo Risco do Barbell que será investido apenas em Bitcoin. No universo dos criptoativos, O BTC é o que possui menor risco e maior efeito Lindy, porque já tem se provado no tempo.

Os seus 20% a 35% do capital investido em criptoativos você pode alocar na parte de Alto Risco da estratégia Barbell. Nesse caso, o investimento será em moedas que chamamos de ALTCOINS, um nome dado às *Alternative Coins*, moedas alternativas.

Vamos conversar mais especificamente sobre as Altcoins no próximo capítulo?



P.S: Só hoje, dia 12 de março de 2020, a bolsa caiu mais de 17% novamente, gerando mais dois circuit breakers. Está o caos, minha gente.

ENTENDENDO AS ALTERNATIVE COINS



Possivelmente você já ouviu o termo Altcoins e a explicação que lhe deram provavelmente foi da seguinte maneira: “São todas as moedas que não são o Bitcoin”, “São outros tipos de criptomoeda”, “Altcoins são scam’s”.

Primeiramente precisamos entender o conceito e perceberemos juntos que estas explicações estão certas até certo ponto, e por outro lado, tem respostas muito rasas, sem fundamento algum.



O termo *Alternative Coins* ou Altcoin, traduzindo do inglês, significa “Moeda Alternativa”, esse termo surgiu três anos depois da criação do Bitcoin (BTC), em 2011, quando foi criada a segunda criptomoeda, conhecida como Litecoin (LTC), uma versão melhorada do Bitcoin. Digo uma versão melhorada pelo fato de ela ter surgido a partir de um “Fork” (uma ramificação) do Bitcoin, as principais de suas características seriam a velocidade de transação mais rápida e custos de transferências mais baixos. Gosto de ressaltar que não foi sempre que o Bitcoin teve os custos de transações baixos, até meados de 2018 o seu custo de transação era fator de discussão em rodas de conversas de pessoas do universo Cripto.

Podemos então agora concordar com aquela primeira afirmação que foi feita, Altcoins são, de fato, todas as moedas que não são o Bitcoin, são protocolos que surgiram de algum FORK do Bitcoin (BTC) ou até mesmo de criações de protocolos diferentes, como é o caso da Ethereum (ETH).

A Ethereum foi um das criações que mais trouxe visibilidade para as criptomoedas, com sua própria Blockchain. Rodando em algoritmos diferentes do BTC, a Ethereum apresenta propriedades que estendem o uso de sua Blockchain para diversas aplicações na área da economia. A essas propriedades nós podemos chamar de Contratos Inteligentes, mais comumente conhecidas como Smart Contracts (na tradução em inglês).



No mundo já são mais de 5.200 criptomoedas existentes e listadas em algumas corretoras. As mais conhecidas delas são as que possuem mais aceitação do público em geral e maior aplicabilidade em diversos projetos. Em meados de 2017 vimos um *boom* na criação de Altcoins, e não era raro ver o surgimento de mais de 50 projetos de moedas e aplicações novos por dia.

O problema era que muitos se aproveitaram desse movimento e surgiram com projetos fraudulentos, nos quais apenas o fundador da moeda ganhava dinheiro. A isso chamamos de *scam*, termo em inglês que significa “golpe”, literalmente.

Vamos deixar isso de lado, hoje poucos projetos sérios e com reais aplicações vêm surgindo. Por isso, é importante fazermos a seguinte pergunta:

kriptoparahaber





















COMO EU POSSO IDENTIFICAR UM BOM PROJETO E INVESTIR EM UMA ALTCOIN COM SEGURANÇA?

Para sua segurança, procure as moedas que são mais bem classificadas no www.coinmarketcap.com. Fazendo isso, você vai minimizar suas chances de investir em projetos que vão acabar ficando com seu dinheiro e sumindo do mapa.

Tabela de Moedas mais bem classificadas:

#	Name	Market Cap	Price	Volume (24h)	
1	 Bitcoin	\$114.984.057.508	\$6.288,95	\$46.447.564.143	
2	 Ethereum	\$14.367.954.648	\$130,36	\$14.022.092.744	
3	 XRP	\$6.837.925.093	\$0,155965	\$2.117.307.445	4
4	 Tether	\$4.638.972.874	\$0,999269	\$57.590.484.734	4.
5	 Bitcoin Cash	\$3.969.619.681	\$216,37	\$4.268.586.598	
6	 Bitcoin SV	\$3.051.086.682	\$166,33	\$3.260.872.353	
7	 Litecoin	\$2.458.096.357	\$38,20	\$3.606.092.951	
8	 EOS	\$2.076.199.595	\$2,25	\$3.135.806.788	
9	 Binance Coin	\$1.845.434.228	\$11,86	\$339.276.220	
10	 Tezos	\$1.150.665.571	\$1,63	\$150.718.583	
11	 UNUS SED LEO	\$1.013.731.312	\$1,01	\$10.171.924	
12	 Stellar	\$785.415.198	\$0,038722	\$356.859.978	2
13	 Chainlink	\$752.189.185	\$2,15	\$360.663.734	
14	 Monero	\$748.484.675	\$42,78	\$130.411.770	
15	 TRON	\$746.256.456	\$0,011191	\$1.130.674.376	
16	 Cardano	\$744.762.697	\$0,028725	\$94.937.842	

Fonte: www.coinmarketcap.com.



Bitcoin é uma bolha?



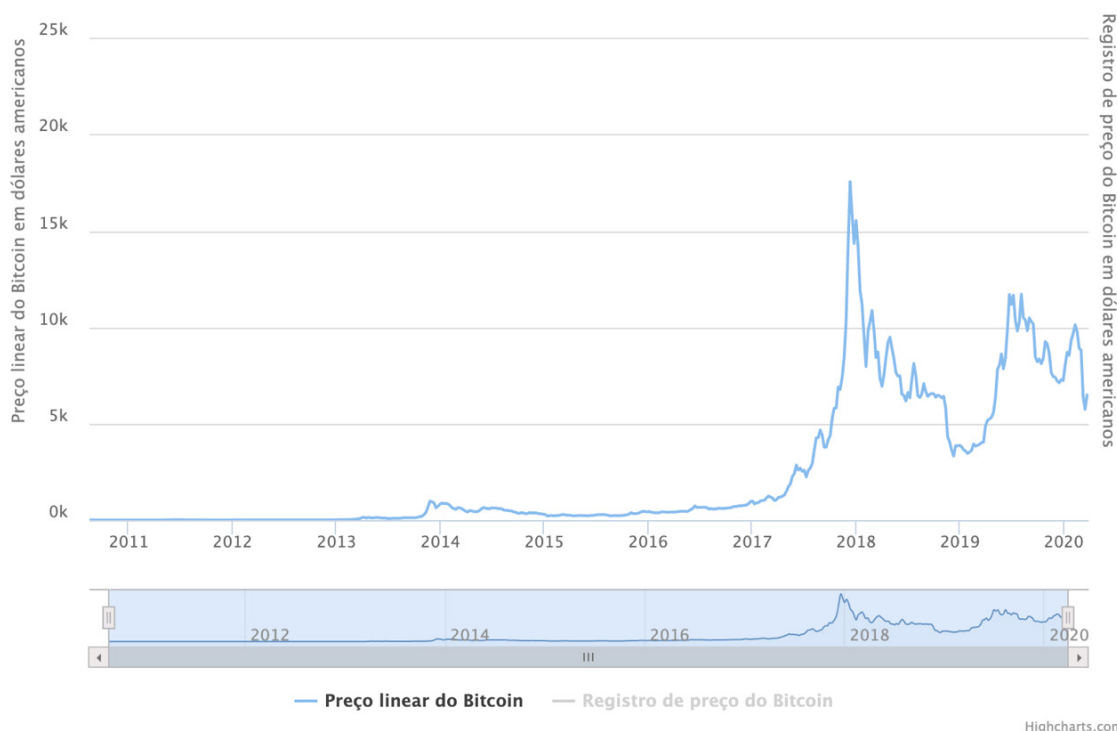


Escuto muito que o Bitcoin é uma bolha e que cedo ou tarde vai explodir e desaparecer. Não gosto de ser fatalista a esse ponto, mas acredito que é muito coerente levar em conta o fator especulativo e você precisa prestar muita atenção nisso que eu vou te falar. Preste atenção neste parágrafo para você nunca enganar a si mesmo.

O bitcoin não é uma bolha, mas se comporta como uma, assim como a maioria dos ativos financeiros listados em uma bolsa de valores tradicional. Apresentam períodos de bolha, que invariavelmente estouram em algum momento. Isso é normal, por isso não me preocupo com isso, basta se posicionar da maneira correta.

Ao longo da história do BTC percebemos “momentos bolha”. Em 2013 a moeda chegou a valer mais de mil dólares, mas “estourou” caindo para cerca de 200 dólares, patamar que se manteve até 2015.

No final de 2017 o bitcoin bateu a marca de US\$ 10.000, e chegou a ser vendida aqui no Brasil por quase R\$ 70.000,00. Em questão de um mês o valor já era metade disso.



(Fonte: <https://www.buybitcoinworldwide.com/pt-br/preco/>)

Embora esses momentos existam, chamar Bitcoin de bolha é muito exagerado. Ele tem se provado no tempo – tem apresentado o efeito Lindy a seu favor – e tem sobrevivido a épocas bem conturbadas. A questão toda é que o Bitcoin não tem necessariamente uma definição de identidade, e por isso é chamado de “bolha” e “engano” por muitos. O seu preço envolve muita especulação, e parte disso é culpa dessa falta de identidade. De qualquer forma, existem “forças” que levam o preço do Bitcoin a subir:

- ✔ **Investimentos Institucionais:** fundos de investimento e grandes investidores quando vão às compras elevam o preço do Bitcoin pela lei da oferta e demanda. Se existe demanda suficiente, aumenta-se o preço.



- ✓ **Especulação Natural:** o BTC é naturalmente especulativo. Ou seja, quanto mais procura existir, mais caro o ativo fica.
- ✓ **Crises políticas e econômicas:** como citei em um capítulo anterior, a Argentina é um belo exemplo disso. A partir do momento em que uma crise acontece em um país, muitas pessoas fugirão da moeda corrente e correrão para o BTC. Isso fará com que o preço aumente.

Assim como o BTC sobe de preço, ele também cai. Existem alguns motivos para isso acontecer:

- ✓ **Aumento de regulação:** veremos isso no próximo capítulo, mas a maioria dos países não tem nenhuma regulação para o BTC. A partir do momento que passa a existir, acontece a fuga de muitos investidores, causando diminuição do preço.
- ✓ **Imprevisibilidade:** esse fator faz com que as pessoas saiam dos seus investimentos em criptoativos. Muita oferta para pouca demanda gera preço mais baixo.
- ✓ **Diminuição da confiança:** muitos perdem a confiança nos criptoativos por conta da sua volatilidade e, por isso, retiram seus investimentos. Lembre-se apenas de uma coisa e nunca mais esqueça – volatilidade não é sinônimo de risco. Ou seja, não é porque um ativo é volátil é que ele se apresenta como arriscado.



- ✓ **Pirâmides Financeiras:** a perda da confiança nos criptoativos gerada pelas pirâmides financeiras faz com que pessoas saiam das suas posições de investimento em criptoativos.

Recomendo que você não se empolgue tanto com os períodos de alta ou se desespere com os períodos de baixa. Existem maneiras inteligentes e momentos corretos de liquidar os Bitcoins e colocar dinheiro no bolso.

Mas deixo aqui uma dica para o momento de entrar no mercado: se a mídia não especializada em investimentos e mercado financeiro estiver falando muito de Bitcoin e criptoativos, não compre! Você cairá na armadilha da manada. Normalmente nesses períodos o preço do ativo está muito alto e você corre o risco de perder dinheiro. Gosto da frase: “compre guarda chuvas em dia de sol, não em dia de chuva”.





Regulação e leis





Muito bem, agora que você já entendeu que esta moeda digital, pelo aspecto revolucionário que tem em si mesma, pode ser um ativo de investimento, você precisa perguntar a si mesmo: “Eu comprei Bitcoins, e agora, como declaro isto à Receita Federal?” O que pretendo neste capítulo é lhe dar subsídios sobre as instruções atualizadas até Março/2020, mas meu conselho é: Mantenha-se atualizado o máximo possível, pois pela dinâmica deste mercado e mudanças constantes, novas regras são implementadas constantemente.

Vou usar muito o termo “criptoativo”, o qual a receita através da instrução normativa define como: “representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira,





transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que podem ser utilizados como forma de investimento, instrumento de transferência de valores ou acesso à serviços, e que não constitui moeda de curso legal“. (art. 5º, inc.I,IN 1888/2019)

A Receita Federal do Brasil (‘Receita’ ou ‘RFB’), por meio da Instrução Normativa nº 1.888/2019, instituiu a obrigação de informar operações realizadas com criptoativos por pessoas físicas com domicílio fiscal no Brasil ou por meio de exchanges de criptoativos brasileiras (‘exchanges’ ou ‘corretoras’), obrigação esta que se iniciou em agosto de 2019.

Essas obrigações foram criadas para averiguar o ganho de capital nas transações com criptoativos e também para combater a lavagem de dinheiro e corrupção. Tanto pessoas físicas quanto pessoas jurídicas estão obrigadas a prestarem informações conforme artigo 6º da instrução.

E quando você é obrigado a informar à Receita Federal suas operações? Bem, tanto pessoas físicas quanto jurídicas devem relatar seu histórico de transações se ultrapassarem a quantia de R\$ 30.000,00 (Trinta mil reais) por mês, tendo o prazo de um mês para enviar o relatório.



As operações que deverão ser relatadas são as seguintes:

- ✓ Compra e Venda;
- ✓ Doação;
- ✓ Transferência e retirada de criptoativo para Exchange;
- ✓ Cessão temporária (Aluguel);
- ✓ Emissão;
- ✓ Ação em pagamento;
- ✓ Outras operações que impliquem transferência de criptoativos.





No relatório das operações deverá conter as seguintes informações:

- ✓ Data da operação;
- ✓ Tipo de operação;
- ✓ Titulares da operação (envolvidos na transferência);
- ✓ Quantidade negociada;
- ✓ Valor da operação;
- ✓ Valor de taxas de serviços.





E em relação aos titulares da operação, devem ser informados:

- ✓ Nome da Física ou Jurídica;
- ✓ Endereço;
- ✓ Domicílio Fiscal;
- ✓ Número do CPF para pessoa Física e CNPJ para pessoa jurídica;
- ✓ Demais informações cadastrais que forem solicitadas.

De acordo com art. 8º da Instrução Normativa 1.888/2019, as informações deverão ser feitas mensalmente no prazo de 01 (um) mês após o ocorrido das operações realizadas com criptoativos. Vamos supor que você fez uma transação no mês de fevereiro, então você terá até às 23h59min59s de 31 de março para fornecer todas as informações solicitadas.

Estas informações deverão ser encaminhadas à Receita Federal pelo sistema de coleta nacional disponível no Centro Virtual de Atendimento (e-CAC). Este é o link:

[Ato Declaratório Executivo COPES nº 1/2019:](#)

A Receita Federal também disponibiliza modelos de arquivos em excel para orientar os declarantes, que você encontrará **[neste link.](#)**



Um estudo prévio do Manual de Orientação destes modelos é recomendado, devido aos termos técnicos.

Para realizar estes envios você precisará de uma assinatura digital, realizada pelo certificado digital válido, emitido por entidade credenciada tipo Certisign ou Serasa.

A Instrução normativa 1.888/2019 em seu art. 10, estabelece punições para pessoa física ou jurídica que deixar de prestar informações a que estiver obrigada, conforme a seguir:





Infração: Prestação de informações fora do prazo (art. 10, inc. I)

Característica do Declarante	Pena
Pessoa jurídica em início de atividade, imune ou isenta, optante pelo Simples Nacional, ou que na última declaração apresentada tenha apurado o Imposto sobre a Renda da Pessoa Jurídica (IRPJ) com base no lucro presumido (alínea a)	R\$ 500,00 (quinhentos reais) por mês ou fração de mês
Pessoa jurídica não descrita na alínea a (alínea b)	R\$1.500,00 (mil e quinhentos reais) por mês ou fração de mês
Pessoa física (alínea c)	R\$ 100,00 (cem reais) por mês ou fração de mês



Infração: Prestação com informações inexatas, incompletas ou incorretas ou com omissão

Característica do Declarante	Pena
Pessoa jurídica (alínea a)	3% (três por cento) do valor da operação a que se refere a informação omitida, inexata, incorreta ou incompleta, não inferior a R\$ 100,00 (cem reais)
Pessoa física (alínea b)	1,5% (um inteiro e cinco décimos por cento) do valor da operação a que se refere a informação omitida, inexata, incorreta ou incompleta
Pessoa física (alínea c)	R\$ 100,00 (cem reais) por mês ou fração de mês



Infração: Não cumprimento a intimação da RFB para cumprir obrigação acessória ou para prestar esclarecimentos nos prazos estipulados pela autoridade fiscal (art. 10, inc. III)

Pena

**R\$ 500,00 (quinhentos reais)
por mês-calendário**



REFERÊNCIAS:

ULRICH, Fernando. Bitcoin: A Moeda na Era Digital, 1ª Edição, São Paulo: Instituto Ludwig Von Mises Brasil, 2014.

BANSAL, Gaurav. Bitcoin Basics: Logic and Magic of Digital Gold, 1a Edição, Chennai, Índia: Notion Prerss, 2018

CHAMPAGNE, Phil. The Book of Satoshi: The Collected Writings of Bitcoin Creator, 1a Edição, Estados Unidos: e53 Publishing LLC, 2014.

SWAN, Melanie. Blockchain: Blueprint for a New Economy, 1a Edição, Estados Unidos: O'Reilly, 2015.

ANTONPOULOS, Andreas M.. Mastering Bitcoin: Programming The Open Blockchain, 2a Edição, Estados Unidos: O'Reilly, 2017.

SCHWAB, Klaus. A Quarta Revolução Industrial, 1ª Edição, São Paulo: Edipro, 2016.

TALEB, Nassim Nicholas. Antifragil: Coisas que se beneficiam com o caos, 1ª Edição, São Paulo: Best Business, 2015

COLB. Manual Tributário para as Exchanges Brasileiras de Criptoativos: Comentários à Instrução Normativa nº 1.888/2019 da Receita Federal do Brasil