# ÍNDICE

# CAPÍTULO 1

## A ORIGEM OBSCURA DA BITCOIN, E PORQUE ELA É IMPORTANTE.

A Bitcoin nasceu em novembro de 2008. Para nos situarmos no contexto económico e social da altura, devemos recordar que em 2008 vivíamos uma das maiores crises de que há memória no mundo ocidental, sobretudo nos Estados Unidos. A crise do Subprime ameaçava fazer ruir todo o sistema financeiro. A queda do banco americano Lehman Brothers em setembro de 2008, foi a pedra de toque que provocou um efeito dominó, fazendo cair um banco após outro. A maior falência de sempre da história dos Estados Unidos veio gerar um nervosismo descontrolado nos mercados financeiros, que ultrapassou em muito o impacto que o banco tinha. Passados 3 dias, o caso da AIG despoletou uma sequência de ajudas do estado. A multinacional de seguros beneficiou de 85 biliões de dólares para ser salva da falência. Mas foram 85 biliões que se vieram a tornar 180 biliões de dólares em pouco tempo, e que acabaram por tornar a AIG numa empresa do estado. Mais tarde o governo justificou que quis salvar a AIG porque a sua falência levaria à falência de todo o sistema bancário ocidental (incluindo bancos europeus.) Também na Europa o contágio era evidente: Alemanha, França, Austria, Holanda e Itália, injetaram biliões de euros na economia para cobrir as perdas sofridas pelos bancos, seguradoras e empresas de investimento.

O criador da Bitcoin é conhecido pelo nome de Satoshi Nakamoto. Mas até hoje, a sua verdadeira identidade permanece um mistério. Ninguém sabe quem era Satoshi Nakamoto, nem se ele tinha alguma relação com o mercado financeiro. Mas é incrível a coincidência de o nascimento da Bitcoin ser quase simultâneo com o descrédito generalizado que abalou o sistema financeiro, bem como os impactos que as moedas como o dólar e o euro geraram em todo mundo.

Enquanto o sistema financeiro mundial colapsava, Satoshi Nakamoto, teoricamente um jovem japonês, inventava no seu quarto estudantil, uma solução para o nascimento de uma nova moeda revolucionária. Uma moeda que sonhava mudar o mundo. Uma moeda que os bancos e governos fossem incapazes de manipular ou falsear o seu valor. Uma moeda global, que não precisava de um banco sequer para ser transacionada. Uma moeda que não existia em papel. Puramente digital, e mais do que isso, uma moeda baseada na matemática e na criptografia. Assim nasceu a Bitcoin. A primeira criptomoeda a conseguir implementar-se.

A ideia de criar moedas digitais, já não era novidade. Antes da Bitcoin existiram outros projetos. Mas nenhuma tinha triunfado. E o motivo principal para terem falhado foi a incapacidade de resolverem um problema muito específico. Um problema matemático que permitisse evitar que uma moeda fosse gasta mais do que uma vez. E acima de tudo, conseguir fazê-lo de forma descentralizada. De modo resumido, o que Satoshi conseguiu resolver, foi uma forma de impedir a cópia ou duplicação de uma coisa digital. Ao resolver o *Byzantine General's Problem*, Satoshi conseguiu criar uma revolução digital que promete mudar o mundo. Falaremos mais em detalhe sobre descentralização e *Byzantine General's Problem*.

Satoshi publicou o seu *white-paper* em novembro de 2008, anunciando que tinha resolvido o problema. Os objetivos da sua moeda eram claros:

- Criar o primeiro sistema de criptomoeda que resolvesse o problema da descentralização da moeda.
- Eliminar a possibilidade de alguma pessoa ou instituição exercer poder sobre a mesma.
- Tornar as pessoas mais autónomas relativamente ao seu dinheiro.

Satoshi visou criar dinheiro eletrónico, *peer-to-peer*, que permitisse fazer pagamentos *online* de uma entidade para outra, sem ter que passar por uma instituição financeira ou outro intermediário nesse processo. Na sua ótica, uma troca financeira deveria precisar apenas de 2 intervenientes: um que paga e um que recebe. Segundo as suas próprias palavras: A existência de uma "terceira parte", um mediador financeiro, torna forçosamente as transferências mais caras, limitando o valor mínimo para uma transação se realizar; impediria a generalização de transferências de valores casuais e tornaria o processo de transferências demorado e ineficiente.

**"Eliminar o intermediário é algo que só traz vantagens para qualquer processo de otimização. Principalmente se isso mantiver ou aumentar a segurança."**

A promessa era fascinante e o *white-paper* de Satoshi Nakamoto explicava exatamente como o iria conseguir fazer. O mundo da criptografia teve pouco tempo para se pasmar com a teoria de Satoshi.

Em janeiro de 2009 (3 meses depois) Satoshi Nakamoto lançava o software sobre o qual correria a sua moeda. E os milhares de fóruns de discussão sobre criptografia e criptomoeda onde milhares de pessoas conversavam ativamente todos os dias passava a ter um tema em comum. A Bitcoin, acabara de nascer.

# O MISTERIOSO DESAPARECIMENTO DE SATOSHI NAKAMOTO E PORQUE ISSO É IMPORTANTE.

No final de 2008, Nakamoto publicava o seu *white-paper*. No início de 2009 Satoshi trabalhou com outros programadores e colocou o seu sistema imediatamente em teste. Era bastante ativo como programador: lançou o seu software; participava ativamente em fóruns; enviava emails, e trocava opiniões com programadores e *developers* de outros projetos. Cypherpunk e outros fóruns viam frequentemente Satoshi escrever sobre este tema. Mas tudo isso mudou em 2011, quando Nakamoto simplesmente desapareceu. Terminaram os emails, os fóruns, os contactos. De um dia para o outro, Satoshi excluiu o seu email da página oficial da Bitcoin e nunca mais o mundo soube nada sobre ele. Ninguém sabe ao certo quem era Satoshi Nakamoto. Nunca nenhum dos colaboradores de Satoshi Nakamoto o conhecera pessoalmente. Nunca ninguém tinha estado com ele fisicamente numa sala ou numa reunião por Skype. Nunca ninguém vira uma foto de Satoshi até ao dia em que ele decidiu desaparecer. De um dia para o outro, elegeu Gavin Anderson como *project leader* e simplesmente retirou o seu nome e contacto dos websites. Ninguém sabe se Satoshi era um homem, uma mulher ou um grupo de pessoas. Teorias mais conspiratórias dizem que Satoshi pode inclusivamente ser um governo, o FBI, ou outra organização secreta.

**De um dia para o outro, Satoshi excluiu o seu email da página oficial da Bitcoin e nunca mais o mundo soube nada sobre ele. Ninguém sabe ao certo quem era Satoshi Nakamoto.**

Também se suspeita que Nakamoto era um pseudónimo de outros programadores como Nick Szabo (anteriormente envolvido noutros projetos de moedas digitais que não chegaram a triunfar), Dorian Satoshi Nakamoto (um físico experiente de origem nipónica que trabalhou como engenheiro de sistemas em projetos secretos da defesa e engenheiro informático para empresas de

tecnologia), Hal Finney (um ex-programador de jogos de consola e o receptor da primeira transferência executada com Bitcoin). As histórias e razões de cada um deles davam um filme de Hollywood. Mais ainda, quando Dorian Satoshi e Hal Finney viveram na mesma vila por mais de 10 anos.

Quem quer que seja Nakamoto, ele não virou as costas de mãos vazias. Estão identificadas as carteiras digitais que lhe pertenciam e portanto sabe-se que possuirá cerca de 1 milhão de Bitcoins, que ao valor de hoje totalizam cerca de 12 mil milhões de euros. Com este valor, Satoshi Nakamoto apareceu entre os 50 homens mais ricos do mundo. Mais concretamente no 44º lugar.

## PORQUE TERÁ DESAPARECIDO O INVENTOR DA BITCOIN?

Relativamente ao motivo do seu desaparecimento, existem diferentes teorias.

Há quem defenda  que ele quis deixar a Bitcoin crescer por si própria, após verificar que o seu trabalho tinha terminado. Acreditando que a sua presença seria mais prejudicial do que benéfica para o sucesso da sua moeda, Satoshi terá optado por afastar-se e manter o anonimato, possivelmente por não valorizar a fama em detrimento da sua privacidade.

Outra teoria é que Satoshi viu o arranque da Bitcoin e simplesmente decidiu abandonar o projeto e "fugir" com as suas moedas aproveitando o seu anonimato.

Para todos os efeitos, a verdade é que Satoshi Nakamoto não era apenas um programador genial. Era também alguém que media muito bem cada um dos seus passos e planeava-os ao mais ínfimo detalhe. Não será por acaso, que até hoje as várias agências de informação americanas como FBI, CIA, NSA, nunca conseguiram seguir o seu rasto com sucesso.

O facto de ter permanecido sempre anónimo, leva-me a crer que este desaparecimento já fazia parte do seu plano desde o primeiro dia. Talvez porque já conseguisse prever que dar a cara por uma criptomoeda poderia ter consequências más quer para a moeda quer para o líder da mesma.

## LIDERAR UMA CRIPTOMOEDA: DAR A CARA TEM UM PREÇO.

No passado dia 22 de dezembro de 2017, Charlie Lee, criador da Litecoin (umas das 5 moedas mais populares e mais transacionadas) anunciou que acabara de vender ou doar a totalidade das suas moedas.

Ao contrário de Satoshi Nakamoto, Charlie Lee, criador da Litecoin, é bem conhecido no mundo das criptomoedas, principalmente pelos seus frequentes *posts* no tweeter e nos media sociais, onde emite as suas opiniões acerca das criptomoedas e principalmente da Litecoin. As opiniões dividem-se. E enquanto uns acham que Charlie Lee é apenas um apaixonado por criptomoedas, outros, suspeitam que Charlie Lee tem vindo a usar a sua posição privilegiada para influenciar a cotação da moeda com as suas declarações e lucrar com as variações positivas e negativas da mesma. Acusações de *inside trading* têm feito "manchetes" nos fóruns e blogues de criptomoedas. A sua enorme carteira de criptomoedas, associada ao facto de ele ser também o CEO da Litecoin, geravam um inegável conflito de interesses.

Cansado das acusações, após o seu *tweet* sobre a possível "quebra súbita" de valor da Litecoin no próximo ano, Charlie Lee anunciou que acabara de vender toda a sua carteira de Litecoin.

Terminou o seu *tweet* com uma provocação enigmática: "Satoshi Nakamoto, é a tua vez..."

Certamente uma alegação ao facto de Nakamoto possuir mais de 1 milhão de Bitcoins até hoje.

No entanto, Nakamoto aparentemente soube afastar-se no momento certo para que a sua presença não prejudicasse a confiança na moeda.

Apesar de ter dito que se absteve de comentar os preços da Litecoin diretamente, Charlie Lee reconheceu que os seus tweets foram criticados e considerados manipulação de preço. Prontamente Lee admite que a sua posição representa um conflito de interesses  e por isso, este desfecho.

# O QUE É A BITCOIN?

A Bitcoin é uma versão de dinheiro eletrónico, puramente *peer-to-peer*, que permite fazer pagamentos *online* de uma parte para outra parte, sem passar por uma instituição financeira ou nenhum outro intermediário.

Mas vamos decompor esta frase em cada um dos conceitos para que fique bem claro.

## DINHEIRO ELETRÓNICO

Já todos estamos familiarizados com o dinheiro eletrónico. Hoje, quando fazemos um pagamento com um cartão de crédito ou débito, estamos a usar dinheiro eletrónico. Nós não entregamos notas nem moedas ao comerciante quando pagamos com o nosso cartão. O nosso pagamento é simplesmente uma instrução para que uma certa quantia a pagar seja deduzida ao número que temos na nossa conta bancária, e seja depois somada ao número que o comerciante tem na sua conta. Neste processo de pagamento não há envolvimento de dinheiro propriamente dito. Há apenas movimentação de números nos saldos das contas dos seus intervenientes. Portanto o conceito de dinheiro eletrónico já nos é familiar. Lidamos todos os dias com esta "desmaterialização" do dinheiro e, inclusivamente, já sabemos que o dinheiro físico (notas e moedas) irá desaparecer nos próximos anos.

Outras formas de dinheiro eletrónico ou dinheiro digital mais populares são por exemplo: Paypal, MBway, Revolut, ou outros sistemas bancários ou das chamadas *FinTech* (empresas tecnológicas que se movimentam na área financeira). Mas todas estas interagem sempre com entidades licenciadas por alguém, para transacionar moedas emitidas pelos estados. Como o Euro ou o Dólar.

## PAGAMENTO *ONLINE*

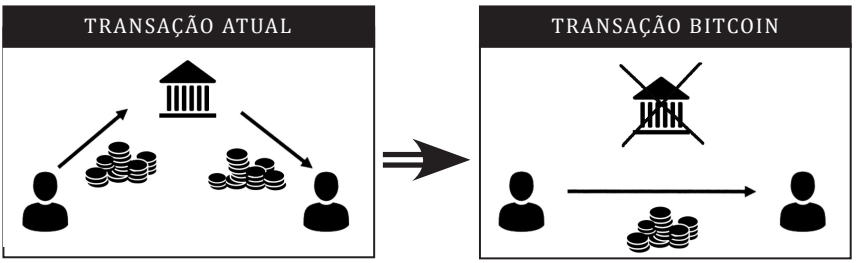
Os pagamentos *online*, também não são nada de novo para a grande maioria das pessoas. Quando acedemos ao homebanking e

fazemos alguma transferência, ou quando pagamos a nossa conta de eletricidade através de Entidade, Referência e Valor, estamos a proceder a um pagamento *online*. Quando compramos alguma coisa num site como o Ebay, Amazon, Alibaba, etc,... Estamos a fazer um pagamento *online*. É comum, é cada vez mais popular e cada vez mais pessoas em todo mundo usam formas de pagamento *online*.

**Resta-nos então explicar a parte revolucionária da Bitcoin:** o facto de excluir uma "terceira entidade" de representar qualquer papel numa transação monetária. Sejam elas governos, bancos ou outras instituições financeiras que autorizem ou desempenhem algum papel nesta transferência de valor.

Nos exemplos anteriores, as transações só são possíveis através de bancos ou instituições financeiras. E a razão de existência dessas instituições é precisamente servir de intermediário nas transações. Claro que, como sabemos, para que nos prestem esse serviço cobram-nos uma taxa. Se por uma questão de perspetiva decidirmos esquecer todas as outras fontes de rendimento dos bancos que surgiram muitos e muitos anos após a sua criação, fica claro que o sustento "primário" de um banco, foi cobrar pelo seu serviço de intermediário. Um intermediário que para além de processar na prática as nossas transferências, assegurava que eram feitas de forma segura, e que eram verdadeiras.

A Bitcoin distingue-se das restantes formas de dinheiro por ter sido a primeira a criar um sistema de confiança no qual não é necessário um interveniente entre quem paga e quem recebe. É puramente *peer-to-peer*, ou se preferirmos: "de uma carteira para outra". De um indivíduo diretamente para outro, sem precisar de passar pelas mãos de nenhuma outra entidade.



E este é o momento em que você vai fazer as perguntas mais pertinentes: "Mas como é que isso é possível?" ou "Mas como é que eu sei que não vou ser enganado?"

"Como pode uma pessoa normal, sem conhecimentos financeiros ou informáticos, transferir dinheiro para qualquer outra pessoa no mundo sem usar um banco?" "Como pode o mundo financeiro funcionar sem intermediários?"

É difícil explicar o conceito e mostrar o tremendo impacto da Bitcoin sobre o mundo sem antes falar um pouco da história da moeda. Mas pense nisto: A verdade é que, na origem do dinheiro, não esteve sempre subjacente a ideia de que tinha que existir um intermediário entre um pagador e um recebedor. Esse conceito veio mais tarde, e revelou-se tão apetecível para esse intermediário, que cada vez se tem criado maior distância entre pagador e recebedor.

No entanto, com a Bitcoin, esse apetecível e lucrativo lugar de intermediário ou "middleman" é completamente eliminado. Em lugar dele, inseriu-se um sistema de confiança, chamado *blockchain*. Um sistema que não é controlado por nenhuma entidade em particular, mas sim pela totalidade de pessoas envolvidas na rede. Explicarei mais à frente o que é a *blockchain* e as bases do seu funcionamento, mas neste momento o importante é solidificar o conceito de que a capacidade de efetuar um pagamento não está nas mãos de nenhum banco, nenhum intermediário nem nenhuma entidade. O pagador e o recebedor, são suficientes e não precisam de despender de nenhum valor para que algum terceiro a faça por si. Neste aspeto, funciona como um pagamento em dinheiro físico (moedas ou notas).

**Quando pagamos em dinheiro físico, também não precisamos de uma terceira entidade a garantir essa transferência de valor. Quando muito precisamos de olhar para as notas e moedas para perceber se têm as marcas de água e características que as distinguem de notas ou moedas falsas.**

No caso da Bitcoin, podemos dizer que a *blockchain* é a tecnologia que nos permite verificar as marcas de água das transferências *peer-to-peer* (transferências de Carteira para Carteira). É claro que um banco também faz isso. Mas para quê pagar esse serviço se o seu dinheiro pode ser "inteligente"? A Bitcoin tem a incrível característica de ser idónea e descentralizada. Desprovida de qualquer interesse na transferência em si. O que torna o seu banco completamente obsoleto no que diz respeito à função de transferir ou guardar o seu dinheiro. Não tem limites horários para executar transferências, elas são tremendamente mais rápidas, e funcionam 24 horas por dia 365 dias por ano.

Mas falámos de descentralização e este é um dos conceitos fundamentais da Bitcoin. Um sistema de pagamentos descentralizado significa que ele é processado por uma rede *blockchain*. Uma rede de computadores, e não um computador centralizado numa instituição financeira que tem completo poder sobre o nosso dinheiro. Um banco, não só tem o poder de realizar transferências, como adquire o poder de saber toda a informação sobre tudo o que os seus clientes fazem. Nos dias de hoje, damos algumas instituições como garantidas, sem sequer nos questionarmos do poder que adquirem sobre nós. E depois só em momentos extremos é que nos lembramos de que fomos nós quem colocou esse poder na mão de terceiros. Fomos nós que assinámos o contrato de várias páginas com letrinhas muito pequeninas. E cujas alíneas em momentos de crise nos reserva quase sempre, surpresas muito desagradáveis. Um pouco mais à frente vou falar de alguns casos em que os bancos inclusive se negaram a executar transferências ordenadas pelos seus clientes. Para perceber o desafio é necessário pensar a nível global. Pense nos países de terceiro mundo e na forma como são geridas as suas finanças. E se isto não o choca, certamente que se recordará do que começou a acontecer recentemente nalgumas falências de bancos mundiais (e também portugueses) onde os clientes foram vítimas de elegantes esquemas multinacionais para passarem o seu prejuízo aos seus clientes e ainda tirar proveito disso.

No sistema descentralizado da *blockchain*, as transferências são executadas por milhões de computadores espalhados pelo

mundo, que validam simultaneamente transferências em "blocos" de criptografia. Nenhum computador sabe que transferência está a validar e há sempre mais do que um computador a validar cada transferência, fazendo com que assim, se construa um sistema de segurança. Explicarei o sistema de confiança mais à frente, quando falarmos da *blockchain*. Mas resumidamente, podemos dizer que uns computadores vigiam o trabalho de outros computadores e que desta forma validam verdades.

Não é errado dizer que com a Bitcoin cada pessoa tenderá a ter a capacidade para transformar-se num banco. Com autonomia para administrar o seu dinheiro e nunca perder controlo sobre o mesmo. Sem ter que pagar comissões ou taxas sobre ele para o manter disponível em qualquer parte do mundo e a qualquer hora. Sem perder a sua privacidade. E poderá entregar o seu dinheiro diretamente a quem entender sem ter que prestar contas relativamente ao que faz com algo que é seu. Para fazer uma transferência de Bitcoin para qualquer pessoa em qualquer parte do mundo, basta inserir o endereço da carteira do seu destinatário, e enviar. Passados minutos, a sua Bitcoin chega ao destinatário. Tal como acontece hoje com um email.

## A PRIVACIDADE

O tema da privacidade não deve ser confundido com anonimato ou criminalidade. A privacidade é um direito de cidadania, que tem vindo a ser violado todos os dias por grande parte das empresas no mundo moderno. A preocupação com a privacidade é algo que a nossa geração começa a identificar, mas que será um dos mais graves desafios das próximas gerações. Por enquanto, você só se preocupa com a pessoa que lhe telefona para o telemóvel a qualquer hora do dia e sabe o seu nome sem que você nunca lhe tenha dado. Sabe também outras informações que não revela saber nesse primeiro momento. Mas nos dias de hoje, acredite quando lhe digo que várias empresas de quem você nunca foi sequer cliente, sabem mais sobre si do que a maioria dos seus melhores amigos.

**Acredite quando lhe digo que várias empresas de quem você nunca foi sequer cliente, sabem mais sobre si do que a maioria dos seus melhores amigos.**

Vamos falar um pouco sobre privacidade. Esta preocupação existiu na origem da criação da Bitcoin. Mas desde já é importante referir que privacidade não significa crime ou ilegalidade. A privacidade é um direito do cidadão, do qual ele não deve prescindir, sob risco de poder vir a sofrer consequências graves na sua vida.

No modelo de privacidade tradicional dos bancos, a privacidade é mantida limitando o acesso à informação que existe nos seus servidores. Mas internamente essa informação está relativamente disponível para o banco e todos os funcionários do banco dependendo do seu nível de acesso. Além do que, apenas o facto de a informação estar fisicamente alojada em servidores centrais, significa que a informação é passível de ser extraída por alguém que deseje obtê-la. Seja por *hacking* ou outro método.

**É oportuno, até pelas recentes polémicas entre Facebook e Cambridge Analytica, referir que a privacidade será cada vez mais um problema entre as pessoas conscientes do perigo que ela representa.**

No modelo de privacidade da Bitcoin, o acesso à informação quebra-se noutro momento cadeia. Cada pessoa tem uma carteira que tem um endereço público e as carteiras são visíveis. Toda a gente pode ver que a carteira A envia uma transferência para a carteira B no valor de X. Mas a carteira A e B são um código de números e letras que não dizem nada sobre as partes envolvidas. Por comparação, é semelhante a estarmos a observar as transações do mercado bolsista: conseguimos assistir em direto às compras e vendas de ações porque são públicas. Mas não se divulgam publicamente as partes envolvidas.

# A MOEDA NA NATUREZA

Vivemos uma época em que o dinheiro e o seu funcionamento é algo quase intrínseco à nossa existência. Quando cada um de nós nasceu, já existia dinheiro. E portanto levantam-se poucas questões sobre a forma como ele nasceu, por quem foi criado, como é gerido e quem decide. Olhamos para a moeda, da mesma forma que olhamos para o sol quando ele nasce: aceitamos que existe e que foi criado da forma mais harmoniosa possível. Aceitamos que a forma como existe hoje é a mesma forma como vai existir amanhã. E que "não temos que nos preocupar com isso. Isso é para os economistas e gestores." Apenas as pessoas ligadas às áreas de gestão e economia têm algum entendimento da forma como funciona a massa monetária, e mesmo esses conhecimentos são muitas vezes passados de forma abstrata e apressada no seu curriculum académico.

Esta lacuna tem sido extremamente danosa para as pessoas de um modo geral. As crises que temos vivido, e que continuaremos a viver nos próximos anos, têm grande parte da sua origem neste massificado desconhecimento do funcionamento do dinheiro. Nascem também do aproveitamento ambicioso de quem compreende a moeda e a usa em seu proveito próprio.

É muito provável que Satoshi Nakamoto tenha partido deste pensamento quando criou a Bitcoin. O momento em que a Bitcoin nasce é de facto oportuno. Estamos em pleno ano de 2009, quando a crise do Subprime começava a provocar as primeiras falências e o sistema económico mundial ameaçava ruir por completo. Estamos numa década em que o mundo vive uma guerra cambial intensa, com os maiores governos e conglomerados económicos a digladiarem-se por valorizações e desvalorizações cambiais propositadas para provocar uma expansão económica de outro modo inalcançável. Vivemos um momento em que os indicadores económicos são mais importantes do que o verdadeiro valor daquilo que os produz. Vivemos num mercado em que se provocam aumentos de exportações com desvalorização de moeda, para se conseguir manipular preços e ser mais competitivo face à concorrência.

Surge então algo diferente: uma moeda não governamental,

cujo valor não pode ser manipulado por nenhuma entidade, e que é global, descentralizada, anónima e rápida na sua circulação.

Satoshi não teve um golpe de sorte. Sabia o que procurava alcançar. E quem souber um pouco sobre a história da moeda entenderá que o plano de Satoshi é genial.

Vamos então voltar uns séculos atrás.

## MOEDA E GOVERNO SÃO DUAS NOÇÕES DISTINTAS

A moeda não nasce por uma necessidade governamental. A moeda nasce por uma necessidade de mercado. Ela vem simplificar e ultrapassar a dificuldade da troca direta de bens. Sem moeda, o homem trocava batata por cebolas; pimentos por tomate, cereais por carne, e por aí diante. Inclusive, trocaria trabalho por roupa, pão, ou outro bem que necessitasse.

Inicialmente a troca era realizada sem uma referência de valor. Um pescador que pescasse mais peixe do que consumia, trocaria o seu excedente de peixe, por carne, cereais ou qualquer outro bem, sem uma necessidade imediata de quantificar. Não havia uma necessidade de quantificar detalhadamente um bem, porque simplesmente trocávamos um que fosse dispensável, por um que desejávamos ter. Se pensarmos bem, uma criança antes de aprender a trabalhar com moeda, também troca um brinquedo mais caro por um brinquedo mais barato sem que isso seja uma preocupação. Troca-o apenas porque tem um desejo maior pelo outro brinquedo independentemente do seu "valor relativo".

Mas com o tempo e a perceção da escassez de cada bem veio instalar a complexidade nas trocas diretas. E com ela, a necessidade de criar equivalências. A melhor forma de resolver o sistema complexo de equivalências foi criar uma unidade contábil. Uma unidade à qual todos os outros bens pudessem ser comparados. Assim nascia a época da moeda-mercadoria. Alguns bens foram sendo usados em certas zonas geográficas como “moeda” generalizada. O gado, o Sal (pela sua raridade, elevada procura e praticidade de transporte e durabilidade.) Mercadores e comerciantes usavam os seus sacos de sal para pagar mercadorias diversas que trouxessem para outra parte do mundo. A própria

palavra "salário" vem do latim *salarium*, que significa "pagamento com sal". A palavra salário tem como origem o termo *salarium argentum*, que consistia na utilização do sal para o pagamento de serviços prestados, na Roma Antiga.

E com o tempo, foi crescendo a vontade de encontrar o bem mais adequado para ser a unidade de comparação.

Existiam no entanto algumas condições já percecionadas: Não podia ser um bem perecível. Tomemos por exemplo que escolheríamos as cebolas para serem a nossa moeda: hoje receberíamos cebolas em troca do nosso trabalho. Mas se não as consumíssemos em pouco tempo, elas apodreceriam e o nosso trabalho perderia o seu valor. Tinha que ser um bem durável. Resistente. Que não se degradasse com o tempo, ou pelo menos não se degradasse num prazo previsivelmente longo. Também não poderia ser algo facilmente disponível. Se escolhêssemos por exemplo um punhado de erva para ser a nossa moeda, seria fácil de colher erva em qualquer campo e usá-lo para trocar por alimentos ou roupa. Ou mesmo por algum bem muito mais raro ou que implicasse o trabalho de outra pessoa. Se fôssemos pagar em punhados de erva a alguém, porque haveria esse alguém de trabalhar para nós em lugar de ir ele próprio apanhar um punhado de erva?

Assim se reuniram dois conceitos necessários: Ser duradouro e ser raro.

E foi muito cedo que o homem entendeu estes conceitos. Ao longo dos milénios, existiram vários bens que serviram de moeda: conchas raras, pedras preciosas, metais, entre outros. O ouro foi o mais comum e também aquele que se instituiu mais tarde, não só como referência de valor mas também como reserva de valor para praticamente todas as moedas no mundo.

Mas é importante voltarmos a distanciar a origem da moeda de qualquer sistema político, governo ou país. Pode parecer chocante, mas mesmo  entre os animais, existem dinâmicas monetárias. Os macacos trocam bens entre si a valorizam bens raros ou especialmente belos. Há registos de animais trocarem conchas raras por favores (estudos do Comparative Cognition Laboratory na Universidade de Yale revelam detalhes curiosos). O uso da moeda e a sua utilidade são e sempre foram independentes de bancos ou governos

ou entidades centrais que as gerem. A moeda é também um conceito "orgânico". Em épocas de escassez de moeda eleita, a sociedade procura outras formas de se organizar. Nas prisões por exemplo, os cigarros funcionam muitas vezes como moeda. Mais uma vez porque se trata de um bem raro no seu ambiente. Que também é desejado e portanto com um valor intrínseco alto dada a diferença entre a sua procura e a sua disponibilidade.

A maior parte dos países possui um padrão monetário específico. Uma moeda reconhecida oficialmente, e cuja emissão é monopólio do estado. A esta capacidade chamamos de política monetária. Moedas como o Euro ou o Dólar, extravasam até esse conceito de moeda nacional, na medida em que são adotados por vários países. (sendo o dólar uma moeda quase global pois estende-se a outros países.)

## A MOEDA COMO CONCEITO ABSTRATO

A moeda, é um conceito abstrato. A moeda ganha um determinado significado sempre que de um certo grupo de indivíduos, atribui um valor a um bem. E apenas o tem enquanto todas as pessoas continuarem a concordar que esse valor existe.

Repare que por muito popular que você seja, se escrever num guardanapo que ele vale 200 euros, terá certamente alguma dificuldade em pagar um jantar com ele. Mas no entanto, todos sabemos que se pagarmos com uma nota de 200 euros, ela será aceite. Porquê? Ela não é apenas um pedaço de papel com um número escrito? O que a distingue então?

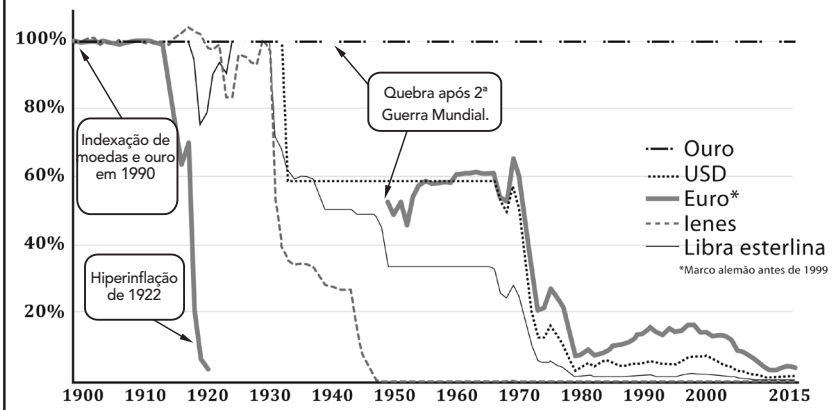
Simples: contém nela alguns elementos que a identificam como “verdadeira” e portanto conseguimos validar que ela pertence à quantidade de notas que o governo emitiu (e que não se trata de uma imitação). Sabemos que por isso, o governo garante o seu valor, dando o seu aval. Vemos então aqui um novo papel na moeda: o governo entra como agente credibilizador de uma moeda. Uma figura importante no valor da moeda nos nossos dias.

## UM CAMINHO SEM REGRESSO

Como falámos há pouco, o ouro, pela sua raridade e características únicas entre os metais, tornou-se uma referência global em termos de valor. Em pouco tempo os reis e imperadores começaram a cunhar as suas moedas, a maioria das vezes com o seu rosto, sinal do seu aval perante o valor da sua moeda. Temos portanto o pontapé de saída para os governadores começarem a emitir moeda.

As moedas de ouro tinham um determinado valor intrínseco, na medida em que o ouro tem um valor já sustentado. E assim sendo, uma moeda com uma certa quantidade de ouro, valeria por referência essa quantidade. Independentemente do governo que a cunhasse. Mas rapidamente a dimensão do poder do rei o do imperador que a cunhasse começou a ter também um valor por si só. Até porque dada a raridade do ouro, os governadores começaram a decidir que colocariam menores quantidades de ouro nas suas moedas. Porque o seu valor abstrato (ao serem moedas cunhadas e asseguradas por um rei ou imperador) não precisavam de conter tanto ouro. O seu aval tinha muito valor. Neste momento da história, iniciou-se um caminho sem regresso… o caminho da desvalorização material da moeda, para uma valorização abstrata. Cada vez mais distante de um valor intrínseco. Desde então, a evolução teve sempre uma única direção: porque haveria um rei, imperador ou governo, de "gastar" ouro para imprimir moeda, se em troca disso poderia dar o seu aval? Não era muito mais conveniente guardar o seu ouro a 7 chaves nos seus cofres, e imprimir metais mais baratos sem ter que incluir ouro no material das moedas? Afinal de contas, a cunhagem da sua cara na moeda, era aval mais que suficiente!

**MOEDAS EM TERMOS DE OURO**




## A DANÇA DAS EQUIVALÊNCIAS

Até há pouco mais de 300 anos, se um cliente chegasse ao banco e pedisse toda a sua moeda em ouro, o banco era obrigado a entregar-lhe. Mas não passariam muitos anos até novos desenvolvimentos voltarem a ditar o caminho da moeda como reserva de valor. No século XIX, as grandes potências mundiais entraram em acordo para definir uma equivalência fixa da sua moeda em comparação com o ouro. Desta forma, o sistema cambial era fixo: todas as grandes moedas do mundo estavam comparadas no seu valor com o ouro. Estipulando assim também uma relação de umas moedas para outras. Operando neste regime, cada banco central era obrigado a manter uma reserva de ouro que refletia as suas necessidades comerciais. Sem entrar em grandes pormenores, Londres era o centro financeiro mundial deste sistema, e cada país era obrigado a manter uma quantidade de ouro cuja referência era o valor da sua moeda. Desvalorização obrigava a exportação de ouro, valorização obrigaria a aquisição de ouro.

Este acordo, manteve-se até 1914, início da 1ª guerra mundial. Existia uma relação direta entre o valor da moeda e a quantidade de ouro possuída por um governo emissor de moeda.

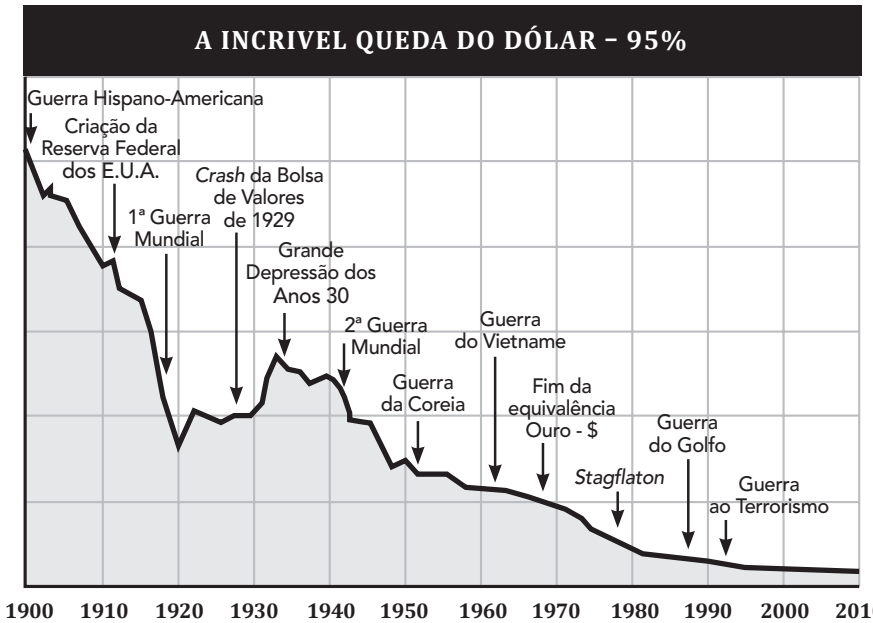
Portanto, para emitirmos moeda, era necessário possuirmos uma grande quantidade de ouro, por forma a fazer face ao seu valor real. A libra era a moeda de referência.

**Até 1914 existia uma relação direta entre o valor da moeda e a quantidade de ouro possuída por um governo emissor de moeda. Após 1914, o sistema ruiu.**

Até que finalmente, em 1944, (finais da 2ª guerra mundial), num Hotel na pequena cidade de Bretton Woods, New Hampshire, nos Estados Unidos da América, 730 delegados dos 44 países líderes mundiais dos Aliados reuniram para decidir o futuro da moeda. Foram 21 dias de reuniões e negociações, onde a Rússia chegou a participar, embora tenha abandonado as reuniões antes de assinar. Nesta conferência, criou-se todo um sistema monetário internacional, e dela nasceram instituições como o FMI (fundo monetário internacional) ou o Banco Mundial.

Os Estados Unidos, proprietários de ⅔ de todo o ouro mundial, insistiam num sistema semelhante ao anterior, mas desta feita, com uma paridade de todas as moedas com o ouro e o dólar americano. E assim nasceu o sistema Bretton Woods. Em 1945, quando o suficiente número de países ratificou o acordo, ele entrou em vigor. O mundo tinha um novo sistema cambial, e os EUA eram o centro do mundo no que diz respeito a política monetária.

A 15 de agosto de 1971, os Estados Unidos terminavam o acordo, pondo fim à paridade entre o dólar e o ouro. Esta medida conhecida como o choque de Nixon, veio pôr um fim ao acordo Bretoon Woods, e tornar o dólar uma moeda Fiat. A consequência foi que muitas moedas tornaram-se moedas fixas relativamente ao dólar. Outras, tornaram-se moedas flutuantes. Mas esta foi a última vez que uma moeda teve qualquer relação com um bem tangível e real. O dólar, moeda forte mundial, acabava de deixar de ter qualquer valor intrínseco ou qualquer equivalência a um bem com um valor concreto.




**Quando os dólares compram apenas 5% do que costumavam comprar, ter 1 milhão de dólares já não significa ser rico.**

A realidade é que Fiat Currency é apenas um nome pomposo para a anarquia do sistema cambial que vivemos desde então. Recentemente li num jornal conceituado uma jornalista referir-se a Fiat Currency como moedas que são garantidas por ouro. Não são. São precisamente o oposto. Fiat vem diretamente do latim e significa algo que é "ordenado por alguém autoritariamente." Algo que é definido por decreto de alguém que tem o poder para o fazer. Não existe portanto nada que garanta valor por trás do dólar. Não existem reservas de ouro totais ou parciais que garantam nada. Existem entidades que visam controlar as disparidades, e os regimes monetários tendem a concertar-se em torno de 3 grandes moedas mundiais: o dólar, o yuan e o euro. Há uma total ausência de paridades.

Perguntam os estudiosos da moeda: existirá de facto uma necessidade de um sistema de paridade formal ou um sistema monetário internacional?

# FIAT, QUE VALOR TEM AFINAL A MOEDA DOS NOSSOS DIAS?

Um dos principais ataques à credibilidade da Bitcoin é que ela não tem valor. Que é uma bolha. "Ela não tem qualquer valor intrínseco!" Aqui está uma novidade para si: Nenhuma moeda dos nossos dias tem um valor intrínseco ou qualquer equivalência parcial a um valor intrínseco.

As moedas Fiat (como o Euro, Dólar e todas as moedas governamentais), não têm qualquer ligação a um sistema de reservas físicas em ouro ou qualquer outra equivalência. A definição Fiat money (usada frequentemente em todos os jornais de economia) significa precisamente isso: Moeda sem valor intrínseco. Arriscam-se todos os dias a valer zero devido à hiperinflação. Porque o seu valor é atribuído por um governo e imposto por regulação. Mas se o povo perder a confiança numa moeda, por exemplo no dólar, o dinheiro deixa de ter qualquer valor. É um conceito difícil de colocar em perspetiva. Muita gente tende a torcer o nariz e balbuciar algo como "isso não é bem assim". Alguns vão rir-se, outros vão dizer que você anda a ver muitos filmes ou a ler muitas teorias da conspiração. Mas experimente perguntar a um venezuelano se ele também se ri perante esta possibilidade… Pergunte-lhe o que valem os seus bolívares na crise que se está a viver neste exato momento na Venezuela. Experimente dizer a um homem que poupou bolívares ao longo de toda a sua vida, que o seu dinheiro não vale nada. E que não pode comprar comida para pôr na mesa e alimentar os seus filhos. O que fez ele diferente do que você faria? Confiou na moeda do governo, presumindo que estava a guardar um valor real. Mas você não confia no seu também? Que culpa tem esse homem sobre as decisões que o seu governo toma relativamente à política monetária? Que controlo teve sobre a forma de poder prevenir-se desta catástrofe?

Pense: Que controlo tem você se lhe acontecer o mesmo?

As moedas Fiat são pura fé. Isto é muito diferente do ouro. O ouro historicamente tem sido usado como decoração, joalharia, fabrico de aparelhos eletrónicos, componentes para computadores, e até componentes para veículos espaciais.

Antes os governos emitiam moedas a partir de bens com valor, como ouro ou prata. Depois garantiam uma equivalência a esses mesmos bens. Mas as moedas Fiat têm zero valor. Tal como a mal afamada Bitcoin. E se quisermos ser meticulosos, uma Bitcoin custa muito mais dinheiro a fazer do que uma nota de papel. Pelo que assim sendo, o seu valor intrínseco deverá ser muito maior. Mas não é o valor intrínseco que define o valor de uma moeda. Certo? Nunca aceite argumentos que não se aplicam de forma transversal.

## PARA QUE SERVE UMA MOEDA FIAT?

Uma moeda Fiat tem a vantagem de servir o seu governo nas suas necessidades económicas: Reserva de valor, unidade contábil e facilidade nas trocas. Como as moedas Fiat não têm raridade nem estão fixadas a nada que o tenha, os governos têm muito maior poder e controlo sobre as economias. As variáveis como crédito, oferta, liquidez, taxa de juro, e velocidade do dinheiro, passam a ser controladas de forma simples. Muitas pessoas acreditaram que este controlo era positivo porque anulava as possibilidades de termos uma crise como a do Subprime, em 2008. Mas aparentemente isso não é verdade. A crise aconteceu e destruiu a vida de milhares de pessoas.

Quando as moedas tinham equivalência ao ouro, o seu valor "real" estava anexado a um bem que tinha "raridade". O ouro é raro na natureza e como tal tende a ter um valor estável. A Bitcoin, beneficia da mesma raridade (uma vez que a quantidade total de moedas está definida desde a sua criação). As moedas Fiat não são limitadas, e por isso criam mais oportunidades para se criarem bolhas, visto que a sua oferta é ilimitada. Mas não vamos entrar só pelo caminho dos males das Fiat currencies. Afinal de contas, este é um livro sobre a Bitcoin.

# AS DIFERENÇAS ENTRE A BITCOIN E AS MOEDAS FIAT

Agora que já sabemos algumas coisas sobre ambas as moedas, podemos fazer um quadro de comparação entre a Bitcoin e as nossas moedas correntes como o Euro ou o Dólar.

| EURO | BITCOIN |
|---|---|
| Reserva de valor ilimitada pode imprimir-se mais a qualquer momento. | Reserva de valor limitada. Existe um limite máximo de 21 milhões de Bitcoins no mundo. |
| Valor da moeda influênciado por interesses de entidades concretas – governos e bancos. | Moeda democrática – ninguém detém o seu controlo absoluto. Todos os intervenientes são iguais. |
| Transferências caras e que necessitam de uma terceira parte para as processarem: bancos. | Transferências baratas e diretas de individuo para individuo. (sem intermediários) |
| Processo de transferências lento e burocrático. 48 horas ou mais, para transferências internacionais. Apenas 5 dias por semana.. | Transferências instantâneas – velocidade da rede de *blockchain* que as processa. 24 horas por dia, 7 dias por semana. |

# CAPÍTULO 2

## AS PRIMEIRAS COISAS QUE TEM QUE SABER ANTES DE INVESTIR EM BITCOIN

Muita gente acha difícil entender as criptomoedas ou a Bitcoin. É muito importante entender a filosofia do dinheiro. Em outubro de 2008 Satoshi Nakamoto (um pseudónimo de alguém que permanece anónimo até hoje) publicou um *white-paper* e disse: "Eu acho que resolvi um problema inultrapassável na ciência. Acho que é possível duas pessoas trocarem dinheiro diretamente na internet sem a interveniência de um intermediário. Escrevi um *white-paper* e implementei informaticamente."

E em nove páginas, Satoshi Nakamoto previu o que se iria passar-se nos próximos 10 anos. Ele criou o software e convidou pessoas a participar nele. Bitcoin é sofware. Instala-se no seu computador. Corre no seu CPU. A Bitcoin é uma aplicação que exige bastantes recursos neste momento. Ela corre num computador, ou num telemóvel. Precisa de uma conexão à internet. Quando corre o seu programa, ele liga-se à internet, e liga-se a outras pessoas na internet. Ninguém sabe a quem o software se liga nem com quem troca informação. Mas liga-se a milhares de outros computadores no mundo. Não precisamos de entendê-lo para que funcione. A isto chama-se uma rede *peer-to-peer*. Juntos, os computadores criam uma rede que serve para trocar e propagar transferências,

que contêm a informação de transferência de valor, bem como a autorização para o fazer. Ninguém controla esta rede. Ninguém consegue perceber ou influenciar o que acontece.

Esta rede começou a 3 de janeiro de 2009. E nesse dia, o mundo mudou. Pela primeira vez na história do dinheiro, na história das instituições, na história da sociedade… foi criado um sistema de confiança. Um sistema que transmite dinheiro em *streaming*. Onde quer que haja internet, há possibilidade de haver Bitcoin. A Bitcoin é diferente de qualquer outra forma de dinheiro que alguma vez existiu.

## A BITCOIN NÃO TEM EXISTÊNCIA FÍSICA. MAS... AS OUTRAS MOEDAS TÊM?

Ao longo dos anos, como pudemos constatar no capítulo 1, o caminho tem sido o de tornar o dinheiro abstrato. O dinheiro deixou de ser algo com valor intrínseco, como a comida ou outros bens inicialmente usados como moeda. Passou a ser algo que representa uma coisa com valor. Como aconteceu com o ouro. A ideia de usar o ouro foi o de poder ter dinheiro que pudesse ser trocado por algo que tem um valor intrínseco. Algo que pode ser usado amanhã, em troca de coisas com valor.

Esta promessa de valor futuro, é a essência do dinheiro. Mesmo quando o dinheiro era um papel ou moeda com uma equivalência em ouro, que podia ser trocada a qualquer momento num banco.

Então o que procuramos no dinheiro é algo abstrato, imutável, inimitável, eterno, e que mantém o seu valor. Algo que promete manter o seu valor no futuro. Ao longo do tempo, o dinheiro tem vindo a desmaterializar-se e a distanciar-se cada vez mais dos verdadeiros bens com valor intrínseco.

Hoje, não nos é estranho este conceito. Mas se recuássemos no tempo e disséssemos a alguém pela primeira vez: "não te vou dar arroz pelo teu trabalho. Mas não te preocupes porque vou dar-te aqui um pedacinho deste minério que se chama ouro, que tu podes ir quando quiseres ao mercado e trocar por arroz". Provavelmente a reação iria ser: “eu sempre recebi arroz pelo meu

trabalho. Acho que prefiro continuar a receber arroz pelo meu trabalho."

Cem anos mais tarde, as pessoas passaram a acreditar que o ouro tinha valor. A coisinha brilhante que era um minério, já servia como pagamento. E o problema seria quando lhe quiséssemos dar um pedaço de papel. "Obrigado pelo papel… mas seria possível pagar-me antes com aquela coisinha brilhante que é o ouro?"

O mundo foi mudando. Hoje dizem-nos: "Sabes que mais? Não vais receber arroz, nem uma coisinha brilhante que é o ouro, não vais receber o papel nem sequer a moeda. Tu vais olhar para números numa página de internet, e lá vais poder ler qual é a quantia que recebeste. Mas não te preocupes! Não podes tocar, não podes ver, mas aquilo é o teu dinheiro."

**O que procuramos no dinheiro é algo abstrato, imutável, inimitável, eterno, e que mantém o seu valor. Algo que promete manter o seu valor no futuro.**

Esta caraterística do dinheiro que temos hoje, é exatamente igual à Bitcoin em termos de existência física. Não podemos tocar numa Bitcoin. Não podemos vê-la. Mas isso não quer dizer que ela não seja dinheiro. É dinheiro digital. A grande diferença da Bitcoin, é que quando olhamos para os números que ela representa no ecrã, ela não está entregue a alguém com a capacidade para a reter contra nossa vontade. Não é guardado por um governo ou banco, por uma empresa privada ou pública. A Bitcoin é guardada em criptografia, simultaneamente em todos os computadores de uma rede espalhados pelo mundo. Não pode ser apagada. Não pode ser desviada. Não pode ser cancelada ou retida ou congelada. Em todo lado do mundo a Bitcoin está disponível. A sua emissão e o seu valor, não são controlados por ninguém em particular. Só o seu proprietário pode autorizar qualquer operação sobre o seu dinheiro.

Numa aplicação no nosso telemóvel, podemos aceder à nossa Bitcoin, ver o nosso saldo, transferir para outro endereço, escolher quantias, etc… Nem sequer precisamos de registar a

nossa Bitcoin com uma correspondência a uma identidade. Ela é anónima.

Não partilho da mesma opinião de alguns escritores que se dedicam à Bitcoin, quando afirmam que a ideia da fisicalidade da Bitcoin é uma das coisas que faz as pessoas desconfiarem da Bitcoin. A fisicalidade é de facto inexistente na Bitcoin. Mas essa ausência de forma física já não é uma novidade nos dias que correm. Já estamos num mundo digital há muitos anos, e diariamente todos manejamos bens sem fisicalidade, sem que isso nos faça duvidar da existência dessas mesmas coisas. Ou sem que nos faça duvidar da legitimidade ou legalidade dessas coisas. Tomemos para exemplo o correio eletrónico (ou email). Alguém duvida de que um email substitui uma caixa de correio normal? Quantos emails enviamos todos os dias?

Um jornal eletrónico, um livro em formato ebook, uma loja *online*, ou mesmo um perfil no facebook, linked in, etc…

Há milhares de empresas que já usam centros de atendimento que são *bots*. São máquinas! Programas de software, com os quais trocamos mensagens escritas para nos ajudarem a resolver problemas. A desmaterialização não é minimamente estranha para nós.

Já ninguém (ou quase ninguém) se preocupa ou perde tempo a pensar que o seu dinheiro não tem existência física. Claro que temos moedas e notas. Mas o facto de muitas das nossas transferências de valor serem feitas através de pagamentos *online* nos websites dos nossos bancos, ou em smartphones com aplicações para o mesmo efeito, ou feitos através de cartões de débito e crédito, já não nos faz pensar duas vezes no aspeto físico do dinheiro. Mas então, vamos tentar ser um pouco racionais. Quando pensamos que a Bitcoin não tem existência física, porque nos faz tanta confusão que ela tenha um valor também? Afinal de contas se o nosso dinheiro também não tem existência física no dia a dia, que diferença faz?

Simples. Existe uma noção (embora errada) de que o nosso dinheiro físico está completamente disponível, à mão de semear, ao primeiro gesto que fizermos para o pedir ao nosso banco. Essa

ideia, de que o banco tem o nosso dinheiro disponível, e de que aquele número que nos mostra num pequeno ecrã representa algo que é real e materializável, é uma completa ilusão. É uma confortável ilusão da qual devíamos sair rapidamente antes que ela se transforme num pesadelo.

**Se acredita que o seu dinheiro existe verdadeiramente e está guardado no banco à sua disposição para o dia que queira ir levantá-lo, está muito enganado.**

Se todos os portugueses forem ao banco levantar o seu dinheiro, perceberão a gravidade. Podemos até querer acreditar que nunca acontecerá nada de grave no nosso país... ou na europa. Mesmo sabendo que só passaram 3 anos desde que tivemos um caso gravíssimo na Grécia. Mas quando pensamos em Bitcoin (uma moeda global) temos que pensar na utilidade mundial desta moeda. Nessa perspetiva, vamos perguntar a um Venezuelano se consegue levantar o seu dinheiro da conta bancária. Vamos perguntar a um Cipriota o que aconteceu ao seu dinheiro investido em obrigações quando o Chipre decidiu fazer um Haircut. Será que merecemos ver as poupanças de uma vida inteira à disposição de uma entidade que nos vai dizer a nós "quanto desse dinheiro" vamos ter depois de o governo e os bancos corrigirem as suas borradas? Quanto desse dinheiro podemos levantar nos próximos dias, meses ou anos? Porque a verdade é que podem desvalorizá-lo tanto quanto lhes seja conveniente para ocultar a má gestão e as decisões económicas suicidas que vem feito ao longo dos anos.

O problema das pessoas quando criticam a desmaterialização da Bitcoin, não é o facto de não lhe poderem tocar. Elas sabem que não tocam de forma diferente no seu salário quando ele é depositado numa conta bancária. O problema das pessoas é acharem que podem confiar no banco quando vêm os números no ecrã, enquanto não confiam nos mesmo números do ecrã quando não vêm uma entidade a "tomar conta do seu dinheiro".

# O QUE PRECISA PARA TER BITCOIN

A Bitcoin é um sistema 100% democrático. Para ter Bitcoin, basta saber fazer meia dúzia de coisas básicas, ao alcance de qualquer pessoa que consiga clicar num mouse. São necessárias coisas simples como: fazer download de um ficheiro ou decorar uma *password*. E acredite: esta parte da password é a mais difícil.

Para ter Bitcoin não temos que qualificar para rigorosamente mais nada. Não temos que preencher uma identidade, uma morada, uma profissão número de contribuinte, cidadão ou passaporte. Não temos que ter nenhuma acreditação. Não precisamos de nenhum aval de nenhuma entidade. Ninguém precisa de nos autorizar. Basta existirmos e termos um acesso à internet para passamos a poder possuir Bitcoin. Isto é diferente de qualquer outro sistema monetário que alguma vez existiu.

Não existe censura. Repare que hoje é impensável a censura ao direito de expressão nos países desenvolvidos. No entanto, aceitamos a censura relativamente a poderes para gerir e aplicar dinheiro. A Bitcoin faz essa revolução no dinheiro. Toda a gente pode fazer tudo o que quiser com o seu dinheiro, sem ser censurada e sem que alguém consiga controlar ou limitar as escolhas dos outros.

Hoje, não existe liberdade no dinheiro, porque até agora, a única forma de controlar a legitimidade no dinheiro, era através de instituições que validassem a legitimidade. Mas o que vemos hoje por todo o mundo, é que as instituições estão a falhar. O sistema está a falhar. As organizações estão a falhar. As regras são contornadas e estão cada vez mais desadequadas da realidade. Esses grupos de pessoas, instituições e organizações com responsabilidades e capacidades para regulamentar, têm-se servido deste sistema de regras para escalar os seus próprios interesses. O que presenciamos sistematicamente, são essas entidades a contornarem as regras e as responsabilidades sempre que possível, por forma a corromper o sistema em benefício próprio. Não temos que presumir que isto aconteça por maldade. Mas se é possível fazê-lo e se é reincidente, o que devemos concluir é que o sistema simplesmente não funciona. A ironia é que o sistema precisa de um outro sistema que o regule e controle a si

próprio. Esta forma de organização é incomportável. Não tem fim. Gastaremos os nossos recursos a inventar fiscais de fiscais cuja função é fiscalizar!

**Presenciamos sistematicamente as entidades a contornarem as regras em benefício próprio.**

A Bitcoin conseguiu ultrapassar isto, criando um sistema de confiança baseado na criptografia e computação matemática. Representa um sistema monetário que está para além do controlo e manipulação de qualquer entidade ou governo ou instituição. Sem fronteiras ou barreiras.

## COMO COMPRAR BITCOIN

Há várias formas de obter Bitcoin. Pode comprar a uma pessoa ou pode comprar a um *exchange*. Mas para comprar Bitcoin com dinheiro Fiat (euros, dólares ou outra moeda comum) terá sempre que comprar de uma destas formas.

### COMPRAR BITCOIN A UMA PESSOA

Vamos começar por explicar a compra "pessoa para pessoa". Esta compra pode ser feita virtualmente ou fisicamente.

O cenário mais simples é, por exemplo, dirigir-se fisicamente a um amigo ou a alguém que sabe que tem Bitcoin, e propor-lhe a compra. Fixado um preço de referência (há vários *exchanges* que dão a cotação do preço da Bitcoin em euros), basta entregar a essa pessoa o endereço da sua carteira de Bitcoin (a sua chave pública) num pedaço de papel, e ele poderá enviar-lhe Bitcoin, colocando o seu endereço de carteira como destinatário e enviando da carteira dele para a sua. Em troca, entregará a quantia em euros conforme a cotação acordada entre os dois. É tão simples como qualquer outra compra. Você entrega dinheiro e recebe Bitcoin na sua carteira digital.

O mesmo cenário "pessoa para pessoa" pode ser feito de forma semi virtual. Existe por exemplo o website: **www.localbitcoins.com**, onde pessoas que querem vender Bitcoins colocam o seu local possível de encontro, e o seu valor de venda. Desta forma, pode pesquisar se há alguém perto de si que esteja disposto a vender Bitcoin. O processo daí em diante é igual, sendo que a localbitoins.com dá alguma segurança. Basicamente o website funciona como uma plataforma de encontro entre compradores e vendedores, e providencia proteção ao comprador e ao vendedor, servindo de intermediário e de depositário das criptomoedas durante o processo de compra e de pagamento.

Esta forma é simples, no entanto é provavelmente mais dispendiosa do que as outras, dado que vai pagar um preço possivelmente superior ao dos *exchanges*. Trata-se no entanto de um mercado quase direto entre um comprador e um vendedor. Um pouco como o Olx ou Ebay.

## COMPRAR BITCOIN NUM *EXCHANGE*

Um *exchange* é um local virtual, onde as pessoas podem comprar e vender, a um preço de mercado acordado. Tal como acontece no mercado de ações ou de futuros. Existem pessoas a tentar comprar, pessoas a tentar vender, e através dessa vontade, alcança-se o que é conhecido por descoberta de preço. Que é basicamente o preço de mercado: o preço no qual a curva da procura e a curva da oferta se cruzam. É bastante eficiente para todos os participantes do mercado.

O *exchange* cria um ambiente de utilizador facilitado e eficiente para permitir aos utilizadores comprar e vender Bitcoin.

É necessário criar um perfil de utilizador, e depois estamos aptos para fazer a nossa compra.

O *exchange* é um prestador de serviços. E portanto, fica com uma percentagem do negócio. Pode ser 0,1% ou pode ser 1% ou mais. Tenha sempre o cuidado de validar todas as condições do *exchange* antes de executar a sua compra.

Para começar a fazer *trading*, precisa de criar o seu perfil. Alguns deles pedem bastante informação pessoal, especialmente se vai comprar Bitcoin com moeda Fiat (euros).

Para comprar com euros ou dólares, tem na maioria dos *exchanges* 2 alternativas: usar o seu cartão de crédito, ou usar a sua conta bancária executando uma transferência SEPA para a conta bancária do *exchange*. De uma forma simples, podemos dizer que se optar por comprar com o seu cartão de crédito tem um limite baixo em termos de quantidades que consegue comprar (independentemente do limite do seu cartão). Se pretende fazer uma compra maior (alguns milhares de euros) terá que usar a sua conta bancária e fazer uma transferência SEPA. Também em termos de velocidade de todo o processo são diferentes: o seu cartão de crédito permite uma compra rápida. Por transferência bancária levará sempre 2 dias até chegar ao banco do *exchange*, e depois será então processada a compra.

Em ambos os casos, o seu perfil de utilizador também poderá limitar a sua compra ou o limite máximo de Bitcoin que consegue comprar de cada vez. Normalmente os seus limites aumentam conforme fornece mais informação pessoal. Entre a informação pedida nos *exchanges*, começa a ser usual pedirem: carta de condução/BI ou passaporte. E comprovativo de morada de alguma das suas contas pessoais.

Não se preocupe. Este processo pode parecer complexo mas a maioria dos *exchanges* tem um website fácil e intuitivo, e a maioria das instruções vão aparecendo à medida que vão sendo necessárias. O step by step até chegar à sua compra é bastante fácil, e a informação é normalmente completada com emails a cada passo, que o ajudam a perceber em que passo está e o que falta para conseguir comprar as suas Bitcoins (ou vender).

Alguns dos *exchanges* populares são por exemplo:

Coinbase – uma ótima forma de começar. É tecnicamente um *exchange*, simples, direto, embora tenha taxas um pouco altas face a alguma concorrência. Mas é definitivamente o mais conhecido e o mais mainstream no que diz respeito a *exchanges*.

Bitfinex, Blockchain.info, Binance, Kraken, GDax, também fazem um bom trabalho. Destacando-se o blockchain.info por ser muito semelhante ao Coinbase e o Bitfinex por ser um verdadeiro *exchange*, com todas as capacidades inclusive fazer "short" a Bitcoin. O Binance é provavelmente o meu *exchange* favorito, e parece-me ser o mais capacitado para crescer neste momento,

quer em volume quer em agilidade e adaptação ao mercado. Pessoalmente, acho o Binance e o GDax os mais agradáveis e eficiente para quem quer fazer *trading*.

Explore um pouco os sites destes e outros *exchanges* que encontre e veja qual ou quais os que lhe parecem mais intuitivos e adequados ao seu nível de conhecimento. Alguns deles inclusivamente já têm o site em português.

Entenda uma coisa: um exchange é uma plataforma de conversão entre moeda Fiat e criptomoeda. E como tal, necessita de regular-se pelas regras impostas pelos bancos e governos para que possa trabalhar de forma legal no seu país de origem. Nem todos os *exchanges* exigem a mesma informação. Mas os protocolos de KYC e ALM são provavelmente aplicados na maioria dos *exchanges* atuais. No entanto, esta condição, é uma condição para a conversão de moeda. Ela não é uma característica das criptomoedas nem é uma realidade aplicável a quem lida com criptomoedas.

## *EXCHANGES* E CHAVES PRIVADAS

A minha opinião é de que os *exchanges* são um conector de entrada e saída entre moeda Fiat e criptomoeda. Pessoalmente, não considero que guardar moedas nos *exchanges* seja a forma mais segura de as manter. Dependendo dos *exchanges*, a segurança é por vezes sofrível e muitas das vezes você não tem acesso às suas chaves privadas na sua carteira do *exchange*. Sabe o que isso quer dizer, certo?

**Se não tem a sua chave privada,
as suas critpomoedas são tão suas quanto
o dinheiro que está no banco.**

Se o seu *exchange* lhe der a possibilidade de extrair e guardar a sua chave privada, a propriedade das criptomoedas é verdadeiramente sua. Se o seu *exchange* não tem essa opção, você não é um verdadeiro proprietário de criptomoedas. É o seu exchange