



Diploma Bitcoin

Educação Financeira para a Era do Bitcoin

Manual do Aluno
Versão Portuguesa | 2025

O Meu Primeiro Bitcoin criou este projeto e disponibilizou-o gratuitamente sob uma licença **Creative Commons**.

Este projeto está licenciado sob
Creative Commons
Attribution-ShareAlike
4.0 International (CC BY-SA 4.0)



Diploma Bitcoin

Educação Financeira para a Era do Bitcoin

Manual do Aluno

Versão Portuguesa | 2025

 **O meu
Primeiro
Bitcoin**
PORTUGAL

Para doar



`bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zkzd54sgmv3yxr34dw8dqm9pzsd`

A história do Diploma Bitcoin

Não há nada mais poderoso do que uma ideia que surge na altura certa.

A história do Diploma Bitcoin teve início em El Salvador, com a graduação de uma primeira turma de 38 alunos em junho de 2022 – este foi o primeiro Diploma Bitcoin a acontecer numa escola de ensino público, em todo o mundo.

Custa a crer que aconteceu há menos de três anos.

O crescimento desde então tem sido extraordinário, com milhares de alunos de todo o país a obterem o Diploma Bitcoin. No entanto, o crescimento mais empolgante e inspirador veio de outros. O manual é de código aberto, e uma coleção incrivelmente diversa de educadores de Bitcoin adotou o material, tanto em El Salvador como além-fronteiras.

O Ministério da Educação de El Salvador utilizou-o como material principal para o seu próprio Diploma Bitcoin e, em 2024, juntámo-nos ao Bitcoin Beach para formar mais de 400 professores de escolas públicas, capacitando-os a ensinar o curso nas suas escolas.

Um dos nossos objetivos iniciais era transmitir conhecimentos a uma nação e demonstrar que a educação relativa ao Bitcoin é uma ferramenta com benefícios em grande escala. Este sonho está agora cada vez mais próximo.

O foco é El Salvador; a missão é o mundo inteiro.

Em março de 2023, fundámos a Rede Internacional de Nós de Educadores de Bitcoin, exigindo que todos os nós concordassem com alguns princípios fundamentais: a educação deve ser independente, imparcial, liderada pela comunidade, exclusivamente sobre bitcoin, de alta qualidade e centrada no empoderamento. Esta rede, agora autónoma, já traduziu o material educativo para mais de oito idiomas e ensinou o Diploma Bitcoin no Canadá, Estados Unidos, México, Guatemala, Honduras, Costa Rica, Cuba, República Dominicana, Haiti, Colômbia, Suriname, Peru, Brasil, Argentina, Irlanda, Reino Unido, Portugal, Geórgia, Gana, Nigéria, Uganda, Quénia, Zâmbia, Zimbabué, África do Sul, Afeganistão, Bangladesh, Índia, Hong Kong, Indonésia e Austrália. A rede acolhe novos nós todos os meses e, como o material é de código aberto, não é necessário pedir permissão para o utilizar. Muitos outros indivíduos provavelmente já o fizeram completamente por conta própria.

Trata-se de um movimento global e descentralizado.

A educação Bitcoin independente, imparcial e liderada pela comunidade vai mudar o mundo. Já o fez.

Por um mundo melhor,

A equipa O Meu Primeiro Bitcoin - 2025

Índice

Capítulo #1: Porque é que precisamos de dinheiro?

1.0 Introdução	01
1.1 Apresentamos o Satoshi	01
Atividade: Cinco perguntas relacionadas com o dinheiro	01
1.2 Debate de turma: Porque é que precisamos de dinheiro?	04

Capítulo #2: O que é o dinheiro?

2.0 Introdução	07
Atividade: Debate de turma - O que é o dinheiro?	07
2.1 Definição de dinheiro	07
2.2 Função do dinheiro	09
2.3 Propriedades do dinheiro	10
2.4 Tipos de dinheiro	13
2.5 A psicologia do dinheiro: escassez, preferência temporal e escolhas	14
Atividade: Preferência temporal	16

Capítulo #3: A história do dinheiro

3.0 Introdução	21
Atividade: Jogo das trocas diretas	21
3.1 Evolução desde a troca direta até às moedas modernas	23
3.1.1 Inconvenientes das primeiras formas de dinheiro	23
3.1.2 Desenvolvimento da cunhagem de moedas e do papel-moeda	24
3.1.3 Transição de dinheiro forte para dinheiro frágil	25
3.1.4 Do papel para o plástico	27
3.2 Moedas digitais	28

Capítulo #4: O que são moedas fiduciárias e quem as controla?

4.0 Introdução	31
4.1 História resumida do dinheiro fiduciário	31
4.2 O sistema fiduciário	34
4.2.1 Um sistema monetário obrigatório	34

4.2.2 Reservas mínimas obrigatórias: um sistema sustentado pela dívida	35
Atividade - Reservas mínimas obrigatórias	38
4.2.3 Quem controla o sistema fiduciário e que benefícios têm?	39
4.3 Moedas digitais do banco central: O futuro do dinheiro fiduciário	41

Capítulo #5: A criação de soluções, com base nos problemas

5.0 Introdução ao problema	45
5.1 Redução do poder de compra	45
5.1.1 A inflação monetária e o seu efeito no poder de compra	45
Atividade - Os efeitos da inflação - Uma atividade de leilão	46
5.2 O peso da dívida global e a desigualdade social	47
5.2.1 Impacto nos cidadãos - Perda de poder de compra	47
5.2.2 Impacto na sociedade - Aumento da desigualdade na distribuição da riqueza	52
Atividade - Consequências do sistema fiduciário	53
5.2.3 O peso da dívida global	54
5.3 Os Cypherpunks e a procura de uma moeda descentralizada	55
5.3.1 Os Cypherpunks	56
5.3.2 Sistemas centralizados e descentralizados	57
5.3.3 História resumida das moedas digitais	59

Capítulo #6: Introdução ao Bitcoin

6.0 Satoshi Nakamoto e a criação do Bitcoin	63
6.1 Como funciona o Bitcoin?	65
6.1.1 O mecanismo de consenso Nakamoto	65
6.1.2 Os intervenientes	67
Atividade - Obtenção de consenso numa rede ponto a ponto	69
6.2 O Bitcoin como moeda digital forte	71
6.2.1 Introdução	71
6.2.2 Características do Bitcoin	72
Atividade - Debate de turma - Será o bitcoin uma moeda forte?	76
6.2.3 Adoção da responsabilidade pessoal	76

Capítulo #7: Como usar o Bitcoin

7.0 Introdução	81
7.1 Adquirir e transferir bitcoin	81
7.1.1 Ponto a ponto: presencial	81
7.1.2 Ponto a ponto: online	82
7.1.3 Corretoras centralizadas	82
7.2 Uma introdução às carteiras Bitcoin	83
7.2.1 Carteiras custodiais e não custodiais	83
7.2.2 Diferentes tipos de carteiras Bitcoin	85
7.2.3 Código aberto e código fechado	86
Atividade - Avaliação de turma de carteiras Bitcoin	87
7.3 Configurar uma carteira móvel Bitcoin	87
Atividade - Configurar/recuperar uma Carteira Bitcoin	87
7.4 Receber e enviar transações	89
Atividade - Transações Bitcoin em ação	91
7.5 Poupar em bitcoin	93
7.6 Não confies, verifica	94

Capítulo #8: Rede Lightning: Usar bitcoin no dia a dia

8.0 Introdução	97
Atividade -vê o vídeo “Bitcoin Lightning Network Explained: How it Actually Works”	98
8.1 A rede Lightning	98
8.2 Diferentes tipos de Carteiras Lightning	100
8.2.1 Carteiras custodiais e não-custodiais	100
8.2.2 Código aberto e código fechado	100
8.3 Configurar uma Carteira de Bitcoin Lightning	100
8.4 Receber e envir transações Lightning	102
Atividade - Corrida de estafetas com a carteira Lightning	106
8.5 Comprar café e mercearias com bitcoin	107
8.5.1 Online: Plug-ins de pagamento - Comércio eletrónico	108
8.5.2 Presencialmente: Encontra um comerciante na tua área de residência	109
8.5.3 Ferramentas de transição: vales, cartões de oferta e cartões de pagamento	110
8.5.4 Economias circulares e o bitcoin como meio de troca	110

Capítulo #9: Uma Introdução ao lado técnico do Bitcoin

9.0 Introdução	115
Atividade - veja o vídeo “How Bitcoin Works Under the Hood”	115
9.1 Chaves públicas e privadas: Segurança com base na criptografia	116
9.1.1 Criptografia de chave privada e criptografia de chave pública	116
9.1.2 Explicação de hashing (dispersão)	119
Atividade - Gerar hash (valor de dispersão) SHA256	121
9.2 O modelo UTXO	122
9.3 Uma análise mais detalhada dos nós e mineradores do Bitcoin	125
9.3.1 O que é um nó do Bitcoin e como posso criar o meu próprio nó?	125
Atividade - Vê o vídeo sobre os Nós do Bitcoin	126
9.3.2 O que é um Minerador do Bitcoin e como funciona a mineração?	126
9.4 O que é a <i>mempool</i> (memória de transações)	132
Atividade - <i>Mempool</i>	134
9.5 O processo completo das transações Bitcoin	135

Capítulo #10: Porquê o Bitcoin?

10.0 Introdução	139
Atividade - Como seria um futuro Bitcoin?	139
10.1 O que são Moedas Digitais do Banco Central (CBDC) e quem as controla?	140
10.2 A filosofia do Bitcoin	141
Atividade - Debate de turma – Será que temos o direito de controlar o nosso próprio dinheiro?	141
10.3 Os benefícios do Bitcoin	142
10.4 Um futuro capacitado	143
Atividade - Debate de turma – Em que medida mudaste a tua perspetiva?	144

Recursos Adicionais	147
Conceitos principais de cada capítulo	149
Glossário	153

Diploma Bitcoin

*Um curso transformador de dez semanas,
através de uma educação independente,
imparcial, de qualidade e gratuita*

Antes de estudar o [Bitcoin](#), é essencial que comprehendas bem os princípios básicos do dinheiro, bem como a sua história e o sistema financeiro atual. Se compreenderes estes conceitos, tens uma boa base para compreender a natureza única e disruptiva do [Bitcoin](#). Quando conheceres melhor a evolução do dinheiro, conseguirás compreender melhor o potencial e as limitações do sistema financeiro atual, bem como a abordagem do Bitcoin aos mesmos. Sem esta base, poderá ser difícil entender por completo a importância e o possível impacto do Bitcoin. Confia no processo de aprendizagem e mantém-te focado, pois a recompensa de um melhor entendimento e consciência desta área inovadora valerá muito a pena.

Capítulo #1

Porque é que precisamos de dinheiro?

1.0 Introdução

1.1 Apresentamos o Satoshi

Atividade: Cinco perguntas relacionadas com o dinheiro

1.2 Debate de turma: Porque é que precisamos de dinheiro?

Manual do Aluno

Versão Portuguesa | 2025

Porque é que precisamos de dinheiro?

1.0 Introdução

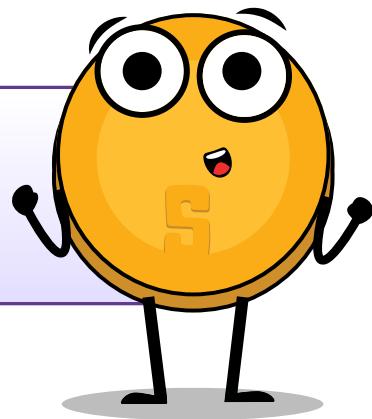
O dinheiro é um dos maiores instrumentos de liberdade que o Homem já inventou.

Friedrich Hayek

Bem-vindo ao Diploma Bitcoin. Neste capítulo, vamos abordar uma questão fundamental – o motivo pelo qual o dinheiro é essencial nas nossas vidas. Vamos estudar a natureza do dinheiro e as suas várias formas, com o objetivo de obter uma melhor compreensão do seu significado. O dinheiro é algo que usamos quase todos os dias. Mas será que compreendemos o que é o dinheiro e o que o torna indispensável? Porque é que os nossos pais e família trocam o seu tempo por dinheiro? Porque é que algumas pessoas têm mais dinheiro do que outras? Porque é que o dinheiro é diferente noutras países? Porque é que não podemos criar mais dinheiro, quando precisamos?

1.1 Apresentamos o Satoshi

Olá! Eu sou o Satoshi, um assistente interativo, e vou ajudar-te em cada etapa do Diploma Bitcoin. Vou dar-te recursos e dicas úteis, para que possas analisar mais detalhadamente os principais conceitos aqui presentes.



Atividade: Vamos dar início a este capítulo com as cinco perguntas que se seguem:

Pensa em utilizações práticas, como a aquisição de bens essenciais (p. ex. comida) e de outras coisas que desejas. Tenta elaborar os teus exemplos, com um bom equilíbrio entre criatividade e realismo.

Capítulo #1

Porque é que precisamos de dinheiro?

O que é o dinheiro?

Porque é que precisamos de dinheiro?

Quem controla o dinheiro?

O que dá valor ao dinheiro?

Capítulo #1

Que dúvidas tens sobre o dinheiro? Escreve aqui a tua questão para partilhar com a turma.

Conversa com o resto da turma, partilha e compara listas, para determinar as cinco maiores razões pelas quais precisamos de dinheiro. Identifica as opiniões mais comuns na tua turma. Reflete sobre as tuas opiniões individuais que não foram incluídas na lista, mas que também devem ser tidas em conta. Anota essas informações adicionais.

1.2 Debate de turma: Porque é que precisamos de dinheiro?

A turma será dividida em grupos e deverá:

- ◆ Partilhar e debater as respostas às primeiras quatro questões. Escrever as respostas favoritas.
- ◆ Partilhar as suas respostas à ultima questão e votar na melhor questão colocada por um aluno. Anotar o resultado.
- ◆ A turma deverá rever essas respostas e perguntas no final do Diploma Bitcoin.

Agora que comprehedes melhor o motivo pelo qual o dinheiro é necessário, os próximos capítulos vão abordar o que constitui o dinheiro, a sua evolução ao longo do tempo, quem o influencia e a forma de dinheiro mais recente que existe. Guarda estas listas, para consultar mais tarde e estabelecer ligações entre as tuas percepções e a evolução da criação do dinheiro, bem como a definição do mesmo e a sua utilização ao longo da História.

Capítulo #2

O que é o dinheiro?

2.0 Introdução

Atividade: Debate de turma - O que é o dinheiro?

2.1 Definição de dinheiro

2.2 Função do dinheiro

2.3 Propriedades do dinheiro

2.4 Tipos de dinheiro

2.5 A psicologia do dinheiro: escassez, preferência temporal e escolhas

Atividade: Preferência temporal

Manual do Aluno

Versão Portuguesa | 2025

O que é o dinheiro?

2.0 Introdução

O dinheiro é uma garantia de que, mais tarde, conseguiremos obter o que queremos. Embora não precisemos de nada neste momento, o dinheiro garante a possibilidade de satisfazer um novo desejo, quando o mesmo surgir.

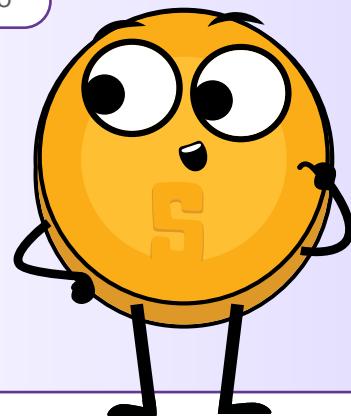
Aristóteles

Para compreender melhor as razões pelas quais precisamos de dinheiro, este capítulo aborda a questão principal: O que é o dinheiro? Vamos começar com uma atividade de debate em grupo.

Atividade: Debate de turma - "O que é o dinheiro?"

- 💡 Não comes já a guloseima que está em cima da tua mesa.
- 💡 Quem estaria disposto a trocar a sua guloseima por uma moeda de 1 euro?
- 💡 Agora, mantém a mão no ar, se também estiveres disposto a trocar a tua guloseima por uma nota de 1 unidade monetária do jogo Monopólio
- 💡 Porquê?
- 💡 O que é que torna uma moeda tão desejável e outra completamente inútil?
- 💡 O que dá *valor* ao dinheiro?
- 💡 De onde vem o dinheiro e quem decide quanto dinheiro se deve imprimir?
- 💡 Porque não imprimir mais dinheiro e distribuí-lo igualmente por todos?

A única diferença entre estas duas notas é a crença de que uma tem mais valor do que a outra.



2.1 Definição de dinheiro

Já alguma vez pensaste no que é o dinheiro? Já questionaste sequer o que é que torna o dinheiro... dinheiro? A maioria das pessoas sabe usá-lo, mas poucas entendem de onde vem ou como funciona. Essencialmente, o dinheiro é uma forma de trocar bens e serviços. Representa o valor dessas coisas de uma forma que facilita o comércio. O dinheiro pode ter várias formas, tais como notas de papel, moedas metálicas e pagamentos eletrónicos. Geralmente, são os governos ou outras autoridades que emitem e controlam o dinheiro. Mas o dinheiro é muito mais do que um meio de troca físico ou digital. É uma espécie de linguagem universal, que nos permite fazer transações com pessoas de todo o mundo, mesmo que não falemos a mesma língua, nem tenhamos a mesma cultura. Por exemplo, podemos estar do outro lado do mundo e, ainda assim, falar a língua do dinheiro, ao colocar um produto no balcão e ao pagar pelo mesmo com a moeda local ou com um cartão de crédito.

Capítulo #2



O dinheiro é uma espécie de contrato social, que nos permite fazer transações, sem ter de recorrer a trocas diretas e sem ter de encontrar alguém que procura exatamente o que temos para oferecer. Se um grupo de pessoas começasse a aceitar chocolate como pagamento pela maioria dos bens e serviços, o chocolate tornar-se-ia dinheiro (embora, tendo em conta que, em certas partes do mundo, acabaria por derreter, podemos considerá-lo uma má forma de dinheiro).

O economista francês Jean-Baptiste Say afirmou: "Numa troca, o dinheiro desempenha unicamente uma função momentânea; e, quando se conclui a transação, chegamos sempre à conclusão de que se trocou um tipo de mercadoria por outro."

Por outras palavras, o dinheiro, por si só, não tem a capacidade de satisfazer os desejos das pessoas. É apenas uma ferramenta que nos permite trocar uma mercadoria por outra.



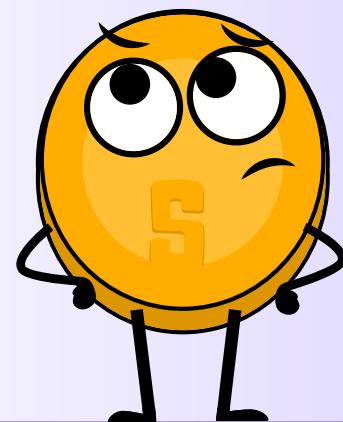
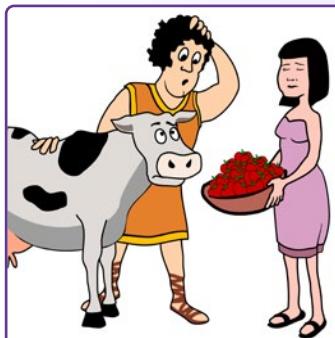
Transação é uma troca ou transferência de bens e serviços. É uma forma de fazer trocas de valor entre duas ou mais partes.

Existem muitos tipos diferentes de transações, desde trocas simples (como comprar uma sanduíche num café) a transações financeiras mais complexas (como comprar uma casa ou investir em ações e obrigações). As transações podem ser feitas presencialmente, por telefone, online ou através de outros meios, e podem ter inúmeras partes envolvidas, incluindo indivíduos, empresas e instituições financeiras.

Sem dinheiro, quanto fácil ou possível seria esta transação?

Trocarias uma vaca por 1 000 000 de morangos?

Ou seriam 600 000 morangos? E se fossem 50 000?





Vê este pequeno vídeo!



O dinheiro **É** o valor **ATRAVÉS** do qual trocamos bens e serviços. O dinheiro **NÃO É** o valor **PELO** qual os bens são trocados.

Resumindo, o dinheiro:

Facilita o comércio, porque todos o aceitam como pagamento final. Permite-nos medir o valor de diferentes bens e serviços e compará-los uns com os outros. Em seguida, vamos analisar a função do dinheiro.

O que é o dinheiro?

2.2 Função do dinheiro

Na compra e venda de bens e serviços, o dinheiro é o interveniente principal. O dinheiro desempenha várias funções importantes no mundo, tais como:



Reserva de valor

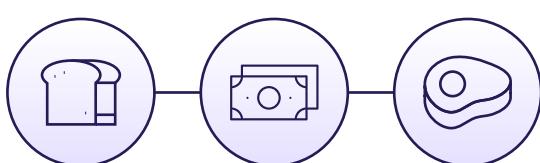
O dinheiro deve manter o seu valor ao longo do tempo, o que o torna útil como forma de poupar e investir o valor do trabalho humano. Isto permite que as pessoas usem o dinheiro para planear o futuro e para emprestar dinheiro ou contrair empréstimos. Por isso, da próxima vez que estiveres a poupar dinheiro para alguma ocasião especial, lembra-te de que o dinheiro é mais do que apenas uma forma de pagar as coisas – é uma ferramenta que te ajuda a planear e a investir no teu futuro.

Qual é a tua reserva de valor?		BTC (USD)	Ouro (USD)	USD (EUR)
	14 de Março, 2019	\$3 846	\$1 293	0,8817€
	14 de Março, 2020	\$5 258	\$1 529	0,90056€
	Ganho/Perda	+36,71%	+18,25%	+2,14%



Meio de Troca

Se tiveres dinheiro, não precisas de encontrar alguém que queira exatamente o que tens para oferecer. Em vez disso, podes usar o dinheiro para comprar e vender o que quiseres. Isto torna as transações e o comércio muito mais convenientes e eficientes.



Unidade de Conta

O dinheiro representa um padrão universal de valor, que nos permite expressar e comparar o preço de diferentes bens e serviços. Isto permite-nos ter um mercado mais eficiente e transparente, onde as pessoas podem tomar decisões informadas sobre aquilo que querem comprar e vender.

Unidade de Conta
Os consumidores reconhecem o valor de algo quando lhe é atribuído um preço (valor monetário).

29,00€ 350,00€



Capítulo #2

Pensa assim: se quiseres comprar um carro novo, consegues comparar preços de diferentes concessionários e tomar uma decisão informada sobre qual será a melhor compra, com base nos preços dos carros em euros. Sem uma unidade de conta, terias de experimentar outra forma de comparar os valores de dois carros, como, por exemplo, o número de vacas que valem ou o tempo que demorou o seu fabrico.

São estas três funções que permitem que as economias se tornem complexas e dinâmicas. Sem dinheiro, seria muito mais difícil comprar e vender bens e serviços, e a nossa economia seria muito menos desenvolvida.

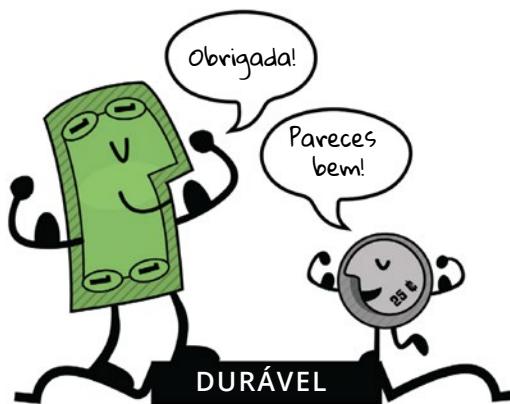
Exercício de turma: Que função do dinheiro é demonstrada neste exemplo?

- 💡 O Ivo decidiu poupar uma parte dos seus rendimentos semanais para comprar um cão.
- 💡 O Fábio compra duas fatias de pizza por 8,30€ no Ray's Pizza.
- 💡 O Benjamim não consegue decidir se quer gastar 75€ em bilhetes para um concerto ou 95€ num passeio de esqui.

2.3 Propriedades do dinheiro

Ao longo do tempo, as pessoas acabaram por perceber que o dinheiro deve ter determinadas qualidades, para ser eficaz como meio de troca. Estas características incluem durabilidade, divisibilidade, portabilidade, aceitabilidade, escassez e fungibilidade.

💡 **A durabilidade** refere-se à resistência do dinheiro à deterioração física e à sua capacidade de durar muito tempo. Esta característica faz com que o dinheiro possa circular na economia num estado aceitável e reconhecível. O ouro é um material durável, que consegue resistir ao desgaste, o que faz do mesmo um bom exemplo da durabilidade característica do dinheiro.

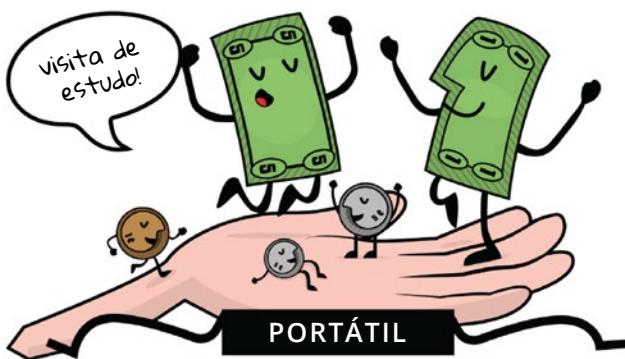


💡 **A divisibilidade** refere-se à capacidade do dinheiro de ser dividido em unidades mais pequenas, para que as pessoas o possam usar para fazer compras de diferentes montantes. As notas de papel podem ser facilmente divididas em denominações mais pequenas, pelo que são um bom exemplo da divisibilidade característica do dinheiro.



O que é o dinheiro?

 **A portabilidade** refere-se à facilidade com que o dinheiro pode ser transportado e movido de um lado para o outro. Isto permite às pessoas usar o dinheiro para comprar e vender bens e serviços sem dificuldade. Os cartões de crédito são portáteis, visto que podem ser facilmente transportados numa carteira ou mala, e é por isso que são um bom exemplo da portabilidade característica do dinheiro.



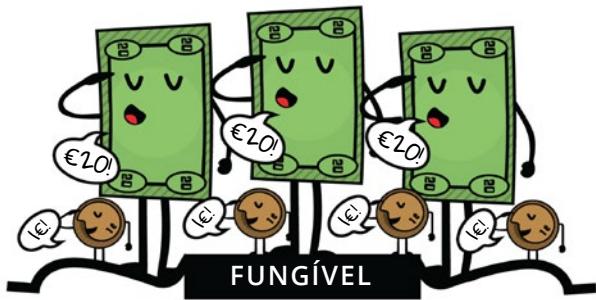
 **A aceitabilidade** refere-se à aceitação generalizada do dinheiro como forma de pagamento, para que as pessoas o possam usar para comprar e vender bens e serviços com confiança. O dólar americano é amplamente aceite como forma de pagamento, razão pela qual é um bom exemplo da aceitabilidade característica do dinheiro.



 **A escassez** refere-se à oferta limitada do dinheiro, que ajuda a manter o seu valor e a evitar que tenhamos de gastar mais dinheiro para comprar a mesma quantidade de bens. Os selos colecionáveis, especialmente os raros e valiosos, podem ser uma boa forma de dinheiro, pois são escassos e podem valorizar ao longo do tempo. Os colecionadores de selos utilizam muito os seus selos como forma de investir a sua riqueza e diversificar o seu portfólio.



 **A fungibilidade** refere-se à permutabilidade do dinheiro, que faz com que uma unidade de dinheiro seja equivalente a outra unidade do mesmo valor. O dinheiro deve ser uniforme. As moedas de cobre são uniformes em tamanho e peso, o que faz das mesmas um bom exemplo da uniformidade característica do dinheiro. Um centímo é sempre um centímo.



Em geral, são estas características que tornam o dinheiro uma ferramenta útil e eficaz, para facilitar as trocas e o comércio, e que são essenciais para o desenvolvimento e estabilidade das economias.

Exercício de turma:

Cada ativo tem propriedades diferentes e desempenha as funções de dinheiro em diferentes medidas. Em última análise, é a sociedade que escolhe o ativo que é utilizado como dinheiro, com base em fatores como a estabilidade, a escassez, a divisibilidade, a transferibilidade e a sua aceitação como meio de troca.

Para avaliar a capacidade de cada objeto de satisfazer os requisitos específicos do dinheiro, podes classificar cada objeto numa escala de **1 a 5** para cada característica. Ao somar as pontuações de cada objeto, conseguimos determinar qual será o mais adequado como forma de dinheiro.

[**0 = Péssimo; 3 = Razoável; 5 = Excelente**]

* Não preenças a coluna do Bitcoin; voltaremos à mesma mais tarde.

Utiliza as seguintes questões para determinar se os diferentes objetos da tabela possuem as características do dinheiro.

-  **Durabilidade:** Será que este dinheiro consegue resistir ao desgaste ao longo do tempo?
-  **Portabilidade:** Será que este dinheiro pode ser facilmente transportado e utilizado em diferentes locais?
-  **Fungibilidade:** Será que se pode trocar este dinheiro com outras formas de dinheiro?
-  **Aceitabilidade:** Será que este dinheiro é amplamente aceite como forma de pagamento?
-  **Escassez:** Será este dinheiro escasso e não muito abundante?
-  **Divisibilidade:** Será que este dinheiro pode ser dividido em unidades menores, para fazer transações?

Características de bom dinheiro	Vacas	Cigarros	Diamantes	Euros	Bitcoin
Durável					
Portátil					
Fungível					
Aceite					
Escasso					
Divisível					
Total					

O que é o dinheiro?

2.4 Tipos de dinheiro

Podemos dividir o dinheiro em duas categorias principais: físico e digital.
O dinheiro físico inclui:

- Moeda fiduciária, ou seja, as notas de papel e moedas emitidas pelos governos e aceites como meio de troca.
- Moeda representativa, que representa uma determinada quantidade de uma mercadoria física e que pode ser trocada pela mesma.
- Moeda-mercadoria, que é um objeto físico com valor intrínseco e amplamente aceite como meio de troca. Por exemplo, o ouro e a prata.

Nem todo o dinheiro é igual!

Moeda-mercadoria
Objetos como a pólvora já serviram como moeda-mercadoria.

Moeda Representativa
Moeda representativa, como este certificado de prata, podia ser trocado por prata.

Moeda Fiduciária
Hoje em dia, as notas da Reserva Federal são moeda fiduciária, decretada pelo governo federal como uma forma aceitável de pagar dívidas.

Moedas Digitais, por outro lado, podem ser usadas para transações online e incluem moedas eletrónicas, stablecoins e criptomoedas.

Moedas Eletrónicas, são versões digitais do dinheiro convencional, como dólares ou euros, e podem ser usadas para comprar e vender coisas online através de **sistemas de pagamento** digitais.



As redes de pagamento são a infraestrutura que permite a transferência de moedas eletrónicas e outros ativos digitais de um local para outro. No entanto, no sistema financeiro tradicional, há sempre um intermediário, como um banco ou instituição financeira, que cobra uma taxa e tem autoridade para aceitar, cancelar, reverter ou adiar transações.

No sistema financeiro intermediado, os principais tipos de redes de pagamentos digitais incluem redes de cartões (que facilitam a transferência de fundos entre instituições financeiras e comerciantes, quando um cliente usa um cartão de débito ou crédito para fazer uma compra) e carteiras digitais (contas online que permitem aos utilizadores guardar e gerir as suas moedas eletrónicas e fazer pagamentos, através da transferência de fundos da sua conta para a conta do destinatário).



Capítulo #2



Moedas Digitais do Banco Central (CBDC)

São versões digitais da moeda fiduciária de um país, que são emitidas e apoiadas pelo banco central e intermediadas pelo governo.



Stablecoins

São moedas digitais concebidas para manter um valor estável, em relação a um ativo como o dólar americano.



Criptomoedas

São um tipo de moeda digital. Algumas criptomoedas são descentralizadas e regidas por regras, enquanto outras são centralizadas e controladas por um pequeno grupo de pessoas.

Em última análise, uma moeda que opera sem intermediários é mais eficiente e benéfica para a sociedade, pois impede que alguns indivíduos controlem a massa monetária e concentrem o seu poder. No entanto, ao longo da História, nunca foi fácil criar uma moeda que facilitasse transações seguras, sem depender da confiança entre as partes envolvidas. Para tal, deve conceber-se uma moeda que funcione como a internet, onde o controlo é distribuído entre todos e ninguém ao mesmo tempo. Isto requer um acordo entre todas as partes, incluindo a renúncia ao controlo da parte que detém o poder, em prol de um bem maior.

2.5 A psicologia do dinheiro: escassez, preferência temporal e escolhas

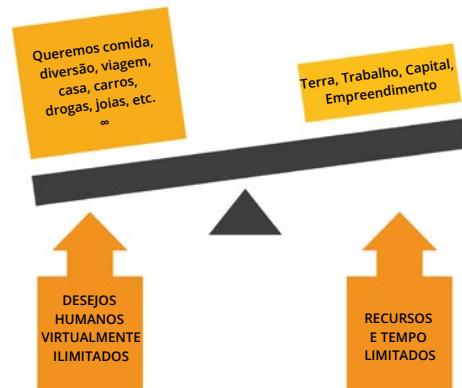
Imagina que estás perdido num deserto e que tens apenas uma garrafa de água. Tens muita sede e precisas desesperadamente de beber alguma coisa, mas também sabes que vais precisar de água para sobreviver, até encontrar mais. Este é um exemplo clássico de escassez – tens apenas uma quantidade limitada de um recurso (água) e tens de decidir como vais usá-lo. Nesta situação, podes decidir racioná-la e bebê-la aos poucos, durante um período mais longo, para que dure o máximo possível.

O que é o dinheiro?



A escassez força-nos a pesar os prós e os contras da forma como usamos os nossos recursos e a fazer escolhas.

Alternativamente, podes optar por beber toda a água que conseguires de uma só vez saciando a tua sede momentaneamente, no entanto este reforço de hidratação e energia pode não ser suficiente para conseguires encontrar mais água no futuro. Independentemente do que decidas fazer, és confrontado com uma escolha difícil. Neste caso, a escolha é entre saciar a sede imediata e guardar a água para mais tarde. Este conceito de escassez não se aplica apenas à água, mas também a todos os outros tipos de recursos. Quer se trate de dinheiro, tempo ou até mesmo amor e atenção, somos constantemente confrontados com decisões de como distribuir os nossos recursos limitados.



Existem dois tipos de escassez: escassez artificial e escassez natural.

- A escassez artificial, também conhecida como escassez centralizada, inclui coisas como malas de marca de edição limitada, cartas de coleção raras e obras de arte originais. Estes objetos podem ser facilmente copiados ou falsificados.
- A escassez natural, também conhecida como escassez descentralizada, inclui coisas como sal, conchas e metais preciosos como o ouro. Estes objetos são mais difíceis de copiar ou falsificar. A principal diferença entre os dois é o controlo.

A escassez centralizada é controlada por uma única entidade, como uma empresa ou governo, enquanto a escassez descentralizada não é controlada por ninguém. Um exemplo de escassez centralizada que afeta desproporcionalmente os pobres é o controlo de recursos essenciais como a água potável. Nalgumas regiões, o acesso à água potável é gerido por empresas privadas ou entidades governamentais, que podem limitar a sua distribuição e causar uma escassez deste bem essencial. Este controlo centralizado pode resultar em aumentos de preços ou num acesso desigual à água potável, o que tende a afetar muito mais as comunidades mais pobres. O acesso limitado à água potável não só afeta a sua saúde e bem-estar, como também perpetua a pobreza, pois as pessoas veem-se forçadas a pagar preços mais altos pela água ou a viajar longas distâncias para a obter.

A escassez afeta as nossas decisões. Se compreendermos isto, podemos melhorar a nossa tomada de decisões. Muitas vezes, temos de escolher entre ganhos imediatos e benefícios a longo prazo, e estas escolhas moldam o caminho que percorremos para alcançar os nossos objetivos.



Preferência temporal refere-se à ideia de que as pessoas tendem a preferir obter algo AGORA, em vez de mais tarde.





Capítulo #2

Um exemplo de preferência temporal:

Imagina que podes escolher entre receber 100 € hoje ou 110 € daqui a um ano. Se tiveres uma preferência temporal alta, tendes a optar por receber os 100 € hoje, porque dás mais valor aos 100 € agora do que aos benefícios de esperar um ano para receber mais 10 €. Por outro lado, se tiveres uma preferência temporal baixa, vais preferir esperar por uma recompensa maior, pois estás mais focado no planeamento a longo prazo e menos interessado na gratificação imediata.

Atividade - Preferência temporal

Preferência temporal alta contra preferência temporal baixa.

- 1 Ouve a explicação do professor em relação às opções de rebuçados à escolha.
- 2 Decide se pretendes receber um rebuçado ou marshmallow mais pequeno agora ou esperar até ao final da aula e receber dois rebuçados ou um maior e melhor.
- 3 Toma uma decisão final e informa o professor da tua escolha. Recebe o teu rebuçado de imediato ou no final da aula, com base na tua decisão.
- 4 Participa num debate de turma sobre esta atividade, para refletir sobre o teu processo de tomada de decisão e conceito de preferência temporal.

Conclusão e debate:

- 💡 Que fatores influenciaram a tua decisão de obter o rebuçado agora ou de esperar e obter uma recompensa maior mais tarde?
- 💡 Como te sentes em relação à tua decisão, agora que a atividade terminou?
- 💡 Consegues pensar em exemplos do dia a dia, em que uma preferência temporal alta pode ser prejudicial e em que uma preferência temporal baixa pode ser benéfica?
- 💡 Quais são algumas das possíveis consequências de priorizar uma preferência temporal alta, em vez de uma baixa?

No contexto do exemplo do deserto, isto significa que podes ter uma maior tendência para beber a água toda de imediato, mesmo que isso signifique que não terás água para beber mais tarde. Isto porque a sede que tens neste momento é mais premente do que a possível sede que poderás ter no futuro.

Por outro lado, se optares por racionar a água e bebê-la aos poucos, estás a demonstrar uma preferência temporal mais baixa. Isto significa que estás disposto a esperar para matar a sede e a aumentar a tua probabilidade de sobreviver. O conceito de custo de oportunidade está intimamente relacionado com a noção de escassez e preferência temporal.

O que é o dinheiro?



O custo de oportunidade refere-se ao “valor” da opção alternativa da qual abdicas, ao tomar uma decisão. Todas as decisões envolvem compromissos.

Escolha de hoje



Comprar um batido de morango por 7 €

Agora



Gastar 7 € de outra forma

Mais Tard



Beneficiar por poupar regularmente 7 €

Digamos que decides rationar a água e bebê-la aos poucos. Como resultado, tens a energia e a hidratação de que precisas para procurar mais água. Enquanto procuras, encontrares um cato com uma pequena quantidade de água. Não é muita, mas é suficiente para saciar a sede naquele momento. Se tivesses decidido beber a água toda de uma só vez, talvez não tivesses tido energia para procurar mais água e encontrar o cato.

Neste caso, o custo de oportunidade de beber a água toda de uma vez seria a oportunidade de encontrar o cato e de obter mais hidratação.

Este exemplo demonstra que o custo de oportunidade não implica apenas que abdiquemos de uma das opções disponíveis naquele momento, mas também das possíveis oportunidades futuras que podemos ganhar ou perder, como resultado das nossas escolhas.

A nossa vontade de abdicar de uma recompensa maior no futuro, em troca de uma recompensa menor imediata é influenciada pela nossa preferência temporal, ou o quanto valorizamos a gratificação imediata, em comparação com o planeamento a longo prazo.

Neste capítulo, abordámos o conceito fundamental do dinheiro. Aprendemos a definição do dinheiro, as suas funções e propriedades, bem como os diferentes tipos de dinheiro que existem. A compreensão da psicologia do dinheiro foi um aspeto muito importante do nosso debate, ao focarmo-nos em conceitos como a escassez, a preferência temporal e as escolhas. Estes conhecimentos dão-nos uma base para compreender a natureza complexa do dinheiro e o papel que o mesmo desempenha nas nossas vidas. No próximo capítulo, vamos abordar a história do dinheiro e a evolução do mesmo ao longo do tempo.

Capítulo #3

A história do dinheiro

3.0 Introdução

Atividade: Jogo das trocas diretas

3.1 Evolução desde a troca direta até às moedas modernas

3.1.1 Inconvenientes das primeiras formas de dinheiro

3.1.2 Desenvolvimento da cunhagem de moedas e do papel-moeda

3.1.3 Transição de dinheiro forte para dinheiro frágil

3.1.4 Do papel para o plástico

3.2 Moedas digitais

Manual do Aluno

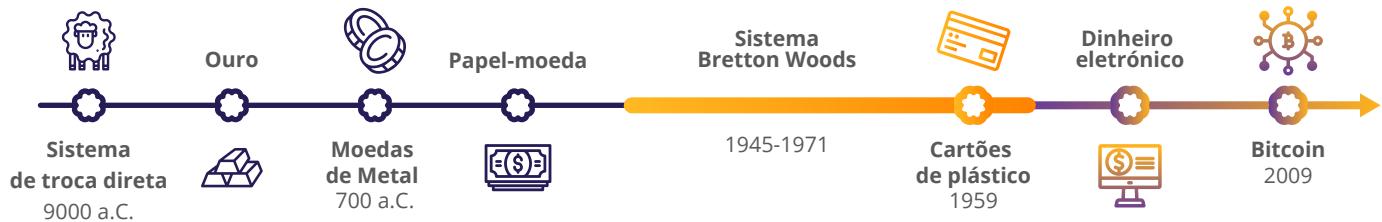
Versão Portuguesa | 2025

A história do dinheiro

3.0 Introdução

A evolução do dinheiro não foi um processo intencional. Foi o próprio mercado que deu origem ao dinheiro. Não foi criado por governos. Surgiu ao longo do tempo, de forma espontânea.

Murray Rothbard



Imagina um período da História no qual as pessoas não tinham as moedas e notas de papel que usamos hoje. Naquela época, tinham uma forma única de fazer transações – por meio de objetos como conchas ou de metais preciosos como o ouro, que eram um tipo de moeda especial. Pode parecer estranho, mas era o dinheiro que eles usavam, algo cujo valor era reconhecido por todos. Neste capítulo, vamos embarcar numa viagem no tempo, para testemunhar em primeira mão a evolução do dinheiro. Vamos descobrir as suas origens e ver como o mesmo mudou e se adaptou, ao longo da História.

Exercício de aula: Jogo das trocas diretas

O teu professor deu-te um pequeno papel. A tua intenção é trocar os teus pertences pelo teu objetivo, num jogo que retrata o comércio ao longo da História. Escreve o teu nome na parte superior do papel em letra pequena e legível.



Ronda #1: Troca direta

Estamos no ano 6000 a.C. Escusado será dizer que o dinheiro que hoje conhecemos ainda não foi inventado. Estamos na Mesopotâmia e usam a **troca direta** para trocar bens e serviços uns com os outros.

Muitas empresas ainda aceitam pagamentos não monetários pelos seus serviços. E os governos consideram estas transações de troca direta equivalentes a transações monetárias, para fins de declaração de impostos.



Corta a folha de papel pelo tracejado. A tua intenção é trocar os teus pertences as vezes que forem necessárias, até atingires o teu objetivo inicial. Não é permitido alterar o teu objetivo inicial. Tens 5 minutos para completar este exercício.

 Quando os teus novos pertences corresponderem ao teu objetivo inicial, regressa ao teu lugar.
Quando acabar o tempo, volta para o teu lugar, mesmo que não tenhas encontrado ninguém para fazer a troca.



Levanta a mão, se conseguiste obter o que querias com apenas uma transação. Duas? Três?

Responde às seguintes questões de forma sucinta, mas completa.

1. Porque é que alguns alunos encontraram alguém para negociar e outros não?

2. Quais são os benefícios da troca direta?

3. Com base no exercício que acabaste de fazer, quais são as desvantagens de utilizar a troca direta?

Ronda #2: Moeda-mercadoria

Avancemos no tempo até ao século XIV a.C. Estamos na costa ocidental africana. A troca direta tornou-se entediante e ineficiente. Já evoluímos como civilização e passámos a usar a **moeda-mercadoria**.

Dos búzios às moedas



1300 a.C.



1000 a.C.



687 a.C.



CURIOSIDADE

Os búzios foram aceites como moeda legal, em algumas partes de África, até ao século XX.

1300 a.C.

Os búzios eram a forma de pagamento predominante na maior parte da Ásia, África, Oceânia e algumas partes da Europa.

1000 a.C.

A dinastia ocidental chinesa Zhou começou a usar moedas de metal.

687 a.C.

O rei Alíates da Lídia (que é hoje a Turquia) encomendou as primeiras moedas de metal cunhadas no mundo ocidental

Estas primeiras moedas eram ovais, feitas de "eletro" (uma liga de ouro e prata) e tinham um desenho apenas num dos lados.

A história do dinheiro

O teu professor deu-te um macarrão (ou uma imagem de um macarrão). Para fins de simplicidade, vamos assumir que o preço de cada bem é um macarrão.

Terás, mais uma vez, de tentar obter o teu objetivo. Porém, a nossa espécie já é mais inteligente e encontrou uma forma de resolver determinados problemas.

- 💡 Porque é que consideramos o macarrão uma moeda-mercadoria?
 - 💡 Como passámos a conseguir os nossos objetivos?
 - 💡 Será que a fase do macarrão foi mais fácil?
 - 💡 Porque achas que o dinheiro veio substituir as mercadorias?
 - 💡 Em que medida é a moeda-mercadoria mais eficiente do que a troca direta?
 - 💡 Quais são as desvantagens de usar macarrão como dinheiro?
 - 💡 O que achas que aconteceu, quando os espanhóis começaram a trazer carregamentos enormes de macarrão para a tua comunidade e a levar ouro e prata das Américas para Espanha?
-
-
-
-

3.1 Evolução desde a troca direta até às moedas modernas

3.1.1 Inconvenientes das primeiras formas de dinheiro



Assiste a este pequeno vídeo para saber mais acerca das “Origens da Troca”, na série “A História do Papel-Moeda”.

Nas economias de troca direta, as pessoas fazem transações entre si, com base no valor relativo dos bens e serviços que têm para oferecer. As economias de troca direta são ineficientes e podem ser difíceis de gerir, especialmente em sociedades complexas.

Em qualquer sistema de troca direta, é necessária uma situação de **dupla coincidência** de vontades, visto que as pessoas têm sempre de encontrar alguém que tenha o que elas querem, mas que também queira o que elas têm para oferecer.



Imagine a situação:

- ◆ O José quer trocar a sua banana pelo coco da Ana.
- ◆ Mas a Ana só aceita trocar o seu coco pela manga da Inês.
- ◆ E a Inês só troca a sua manga pela banana do José.
- ◆ Sem uma dupla coincidência de vontades, eles estão presos num ciclo interminável de trocas de fruta.
- ◆ O José sugere que troquem os seus frutos por um refrigerante bem fresquinho, mas percebem que estão numa ilha remota e que não há refrigerantes.
- ◆ Decidem, então, sentar-se na praia e comer os seus frutos em silêncio.

Este é o segundo episódio, chamado "Mais do que Noodles", da série "A História do Papel-Moeda".



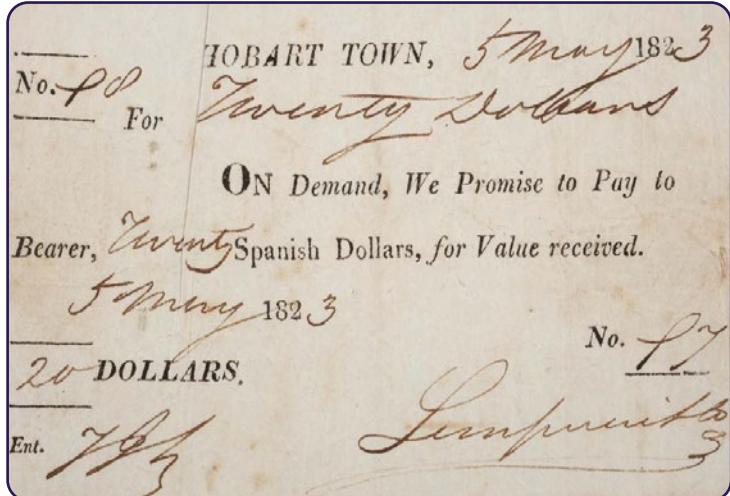
3.1.2 Desenvolvimento da cunhagem de moedas e do papel-moeda

À medida que a comunidade onde vives se torna mais envolvida no comércio, começa a perceber as limitações de usar a troca direta e outras formas de transação não monetárias. Eis que decidem adotar a utilização de moedas metálicas como forma de dinheiro.



Uma **moeda-mercadoria** é dinheiro feito de metais valiosos, como o ouro e a prata. Ao longo da História, estes metais sempre foram usados como reserva de valor, meio de troca e, num passado muito distante, também como unidade de conta.

A história do dinheiro



uma forma de moeda conveniente e fácil de trocar. São representativos do ouro e de outros metais valiosos, e podem ser convertidos nesses metais, como eram entre o século XVII e o século XIX. Isto permite ter uma forma de dinheiro mais portátil e fácil de transferir, enquanto se conserva o valor e a segurança dos metais preciosos.

No entanto, quando se começa a usar moedas metálicas com mais frequência, descobrem-se algumas desvantagens. Em grandes transações, podem ser pesadas e inconvenientes de transportar. Começa também a notar-se que algumas pessoas estão a aproveitam do sistema, ao derreter as moedas existentes e criar novas moedas com uma mistura de metais mais baratos, o que faz com que os preços aumentem e diminui a confiança no sistema.

Numa tentativa de resolver estes problemas, a tua comunidade começa a usar recibos de papel como forma de dinheiro. Estes recibos de papel, que têm origem na China antiga, são

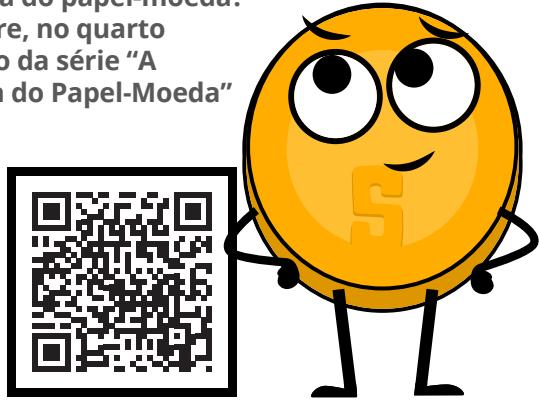


3.1.3 Transição de dinheiro forte para dinheiro frágil

Avancemos no tempo até ao século XVII, na Suécia. Por esta altura, já estás completamente dependente dos bancos para armazenar os teus bens valiosos. No entanto, começas a notar algo de estranho na conduta destes banqueiros. Ao que parece, estão a emitir mais recibos de papel do que a quantidade de ouro que têm armazenado, o que lhes permite criar mais dinheiro do que quele que conseguem converter. Esta prática sorrateira permite aos banqueiros lucrar com a diferença entre o valor dos recibos de papel e o valor do ouro dos seus clientes que têm guardado.



O que acontece, quando tentas colocar em prática a doutrina do papel-moeda? Descobre, no quarto episódio da série "A História do Papel-Moeda"



Apercebes-te também que isto marca uma enorme mudança na forma como se lida com o dinheiro. Estás a testemunhar a transição de um sistema de dinheiro forte (dinheiro conversível em metais preciosos) para um sistema de dinheiro frágil (moedas fiduciárias que não representam bens físicos). Esta transição não aconteceu do dia para a noite. Foi um processo gradual influenciado por vários fatores. A Revolução Industrial, com a sua produção e urbanização em massa, teve uma certa influência, bem como o desenvolvimento de sistemas financeiros avançados, como bancos e mercados de ações. O surgimento de bancos centrais e outras autoridades monetárias contribuiu para a centralização (ou controlo) do dinheiro, o que levou à emissão de moedas fiduciárias para apoiar o crescimento económico.

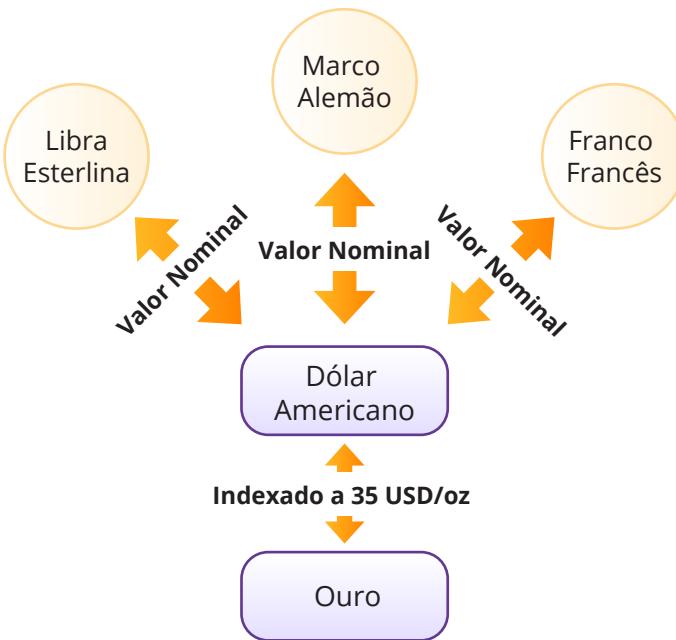


No entanto, também começas a ver as **desvantagens desta centralização**, incluindo o consumo irresponsável, o **aumento das dívidas** e a manipulação dos cidadãos por meio de incentivos económicos.

Até à Primeira Guerra Mundial, era possível converteres o teu papel-moeda numa quantidade pré-estabelecida de ouro. Mas as duas guerras mundiais e a crise económica de 1929 puseram fim a isso. Em 1944, foi assinado o acordo de Bretton Woods, que estabeleceu o dólar americano como a moeda de reserva mundial e fixou o valor do dólar americano ao preço do ouro, a uma taxa de 35 dólares por onça. As moedas de outros países estavam fixadas ao dólar, o que ajudava a estabilizar os mercados financeiros internacionais.

Sistema Bretton Woods

(1945 - 1972)



Infelizmente, este sistema começou a desmoronar no final dos anos 60, o que resultou no Choque Nixon de 1971, no qual o governo dos Estados Unidos suspendeu a conversibilidade do dólar em ouro. Este acontecimento marcou o fim do padrão ouro e deu início a um mundo movido pela criação e acumulação de dívida.

No teu dia a dia, começas a notar que o valor do dinheiro já não é tão estável como costumava ser. Com uma régua flexível, é difícil medir o comprimento de uma mesa com precisão. Pois, quando vivemos num mundo fiduciário, onde o valor do dinheiro está sujeito à imprevisibilidade de quem está no poder, também se torna difícil medir com precisão o valor dos bens e serviços. Sentimos confusão e desconforto, quando nos adaptamos a um mundo onde o valor do dinheiro já não está associado a um bem físico como o ouro.

A história do dinheiro

É visível o impacto desta mudança na economia global, pelo que começas a questionar a estabilidade e a fiabilidade das moedas fiduciárias. Apercebes-te de que, no mundo em que vivemos, o dólar já não tem um valor fixo e consistente, como tinha quando estava fixado ao ouro. Pelo contrário, fica sujeito a flutuações. Isto dificulta a utilização do dólar como unidade de conta, visto que o seu valor é afetado por vários fatores, incluindo a inflação (aumento dos preços), as taxas de juro, o estado da economia do país, eventos políticos, a especulação do mercado e a sua procura no comércio internacional. São tempos confusos e imprevisíveis, quando tentas lidar com o valor em constante mudança do dólar e com o impacto do mesmo no teu dia a dia.

Apesar dos esforços para melhorar a qualidade de vida, através de sistemas monetários modernos, de um aumento da eficiência, de um maior acesso à informação e de uma melhor comunicação, o nível de vida da maioria das pessoas começa a piorar, devido a:

- ◆ O abuso da centralização
- ◆ O aumento dos preços
- ◆ Salários reais estagnados
- ◆ Moedas enfraquecidas
- ◆ A necessidade de gastar mais dinheiro para obter menos coisas

Isto traz dificuldades a quem tem menos recursos económicos, que pode ter um acesso limitado à educação, ao crédito, a recursos, a redes sociais e à representação política. Tudo isto são possíveis desvantagens, relativamente à capacidade destas pessoas de vencer na vida.

Como resultado, parece que os ricos continuam a enriquecer e que os pobres estão cada vez mais pobres.

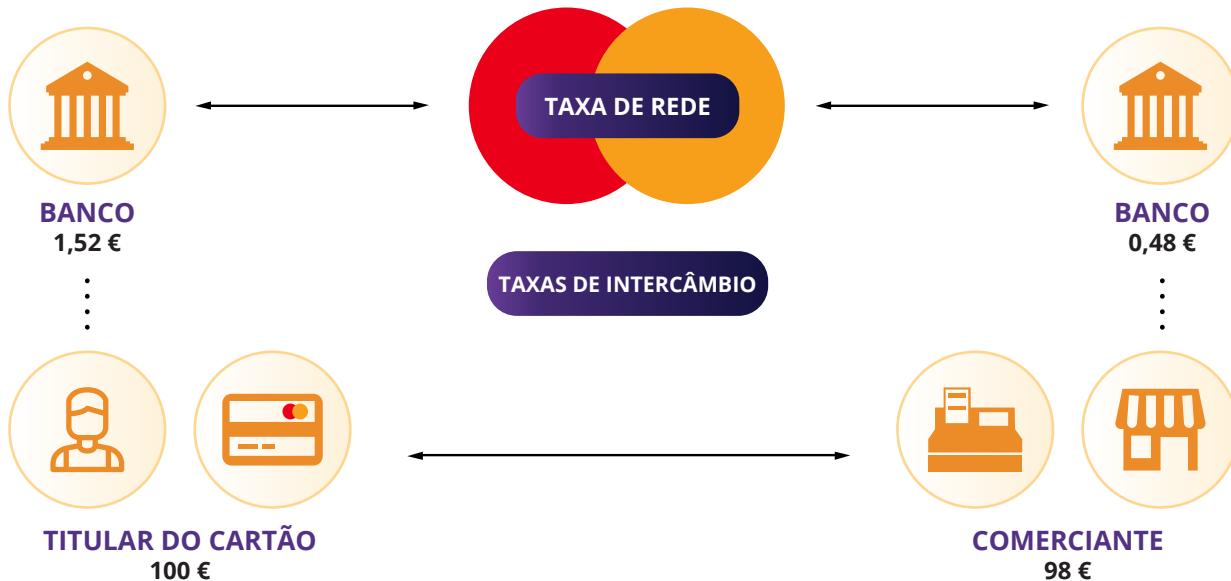


3.1.4 Do papel para o plástico

A forma como fazemos pagamentos evoluiu muito, desde a introdução do primeiro cartão de crédito, na década de 1950. Agora, basta passar um bocado de plástico numa máquina para comprarmos o que quisermos, quando quisermos, sem complicações. Foi como abrir um mundo de possibilidades infinitas e enormes expectativas... julgávamos nós. Mal sabíamos que a nossa dependência do crédito teria repercussões graves – como o aumento do custo geral dos bens e os incentivos a uma economia destinada ao fracasso.



Capítulo #3



À medida que a tecnologia evolui, o mesmo acontece com a forma como lidamos com o dinheiro. A internet torna-se um dos principais intervenientes no mundo financeiro, à medida que os serviços bancários online e websites de comércio eletrónico nos permitem gerir e gastar o nosso dinheiro inteiramente online.

A ascensão do dinheiro digital marca a enorme mudança que se seguiu nesta evolução, ao trazer novas possibilidades e ao mudar a forma como fazemos transações financeiras.

3.2 Moedas digitais

As moedas digitais, ao contrário das tradicionais, existem apenas em formato eletrónico. São armazenadas e transferidas por meio de computadores e de softwares especiais.

As moedas digitais permitem-nos enviar o nosso dinheiro através da internet. Tal como um e-mail nos permite enviar mensagens instantaneamente e sem custos de envio, as moedas digitais permitem-nos enviar e receber valor instantaneamente e com um custo muito reduzido.

As moedas que utilizamos atualmente estão a tornar-se cada vez mais digitais. Apenas uma pequena percentagem da massa monetária atual existe na forma de moedas metálicas e notas de papel. Os bancos e serviços bancários disponibilizam aos seus utilizadores aplicações para trocar dinheiro de forma fácil, através da internet. Mas de onde vem o dinheiro?

Neste capítulo, testemunhamos a transição de dinheiro forte, que representava o ouro, para dinheiro frágil na forma de papel e, agora, na forma de moedas fiduciárias digitais. No próximo capítulo, vamos abordar o funcionamento do atual sistema monetário fiduciário e como o mesmo surgiu.

Capítulo #4

O que são moedas fiduciárias e quem as controla?

4.0 Introdução

4.1 História resumida do dinheiro fiduciário

4.2 O sistema fiduciário

4.2.1 Um sistema monetário obrigatório

4.2.2 Reservas mínimas obrigatórias: um sistema sustentado pela dívida

Atividade - Reservas mínimas obrigatórias

4.2.3 Quem controla o sistema fiduciário e que benefícios têm?

4.3 Moedas digitais do banco central: O futuro do dinheiro fiduciário

Manual do Aluno

Versão Portuguesa | 2025

O que são moedas fiduciárias e quem as controla?

4.0 Introdução

A história da humanidade é a história da desvalorização do dinheiro.

Milton Friedman

No capítulo anterior, vimos como o dinheiro evoluiu ao longo do tempo e como o nosso sistema monetário fez a transição de um dinheiro forte para um dinheiro frágil, o que moldou o mundo em que vivemos hoje. Este capítulo aborda mais detalhadamente a forma como esses desenvolvimentos originaram o sistema fiduciário atual, bem como o funcionamento desse mesmo sistema.

Afinal de contas, em que consiste este sistema fiduciário e como é que o mesmo surgiu?

Para respondermos a esta pergunta, temos de começar por focar a nossa atenção no dólar americano, a atual moeda de reserva mundial, que desempenha um papel dominante no mundo atual. Direta ou indiretamente, todos os países sentem o impacto das decisões que envolvem o dólar americano. Para compreenderes o funcionamento do sistema fiduciário do teu país, é essencial que entendas a ligação entre o mesmo e o local onde surgiu o sistema fiduciário – os Estados Unidos da América.

4.1 História resumida do dinheiro fiduciário

1815-1933	1913	1933	1934	1944	1971	1980
O padrão ouro	Criação de um banco central chamado Reserva Federal	Decreto Presidencial 6102. Todos os cidadãos foram obrigados a entregar o seu ouro a uma taxa de câmbio de 20,67 dólares americanos por onça.	Lei da reserva de ouro. Roubou o património do povo, ao desvalorizar o dólar em 40%, para 35 dólares por onça de ouro.	Acordo de Bretton Woods: O dólar americano tornou-se a moeda de reserva mundial dominante	O Choque Nixon, que deu origem ao sistema fiduciário, ao acabar com a conversibilidade do dólar americano em ouro.	O valor do ouro era 35 USD por onça em 1970, e aumentou para 870 USD por onça até 1980, o que causou uma desvalorização do dinheiro das pessoas em 96%, num período de apenas 10 anos.

Cronologia Visual

No século XIX, houve civilizações em todo o mundo que prosperaram, com base num padrão de dinheiro forte, que utilizavam metais preciosos como o ouro e a prata, devido à sua escassez, durabilidade e reconhecimento. À medida que o comércio mundial se desenvolveu, tornou-se difícil transportar grandes quantidades de metais, o que levou ao surgimento de armazéns de ouro e prata. Estes armazéns guardavam os metais valiosos das pessoas em segurança e davam certificados de papel conversíveis em quantidades específicas de ouro ou prata.



Capítulo #4

Quando depositavam o seu dinheiro, as pessoas recebiam, em troca, certificados de papel com uma correspondência direta à quantidade exata de ouro ou prata que armazenaram. Esta correspondência direta entre os certificados de papel e uma moeda-mercadoria tangível marcou o surgimento das entidades que agora conhecemos como bancos.



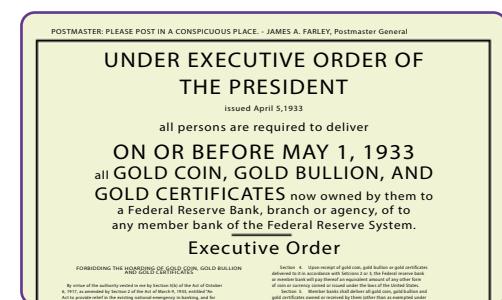
Inicialmente, os bancos tinham o objetivo de salvaguardar o dinheiro dos clientes. Porém, mais tarde, envolveram-se em práticas de empréstimo arriscadas, ao emitir certificados que correspondiam a um ouro que não tinham. Esta prática acarretava o risco de corridas ao banco, caso muitos clientes quisessem converter o seu dinheiro ao mesmo tempo. Para lidar com esse risco, os bancos colaboraram com os governos, para estabelecer

um sistema que legalizasse o reemprestimo. Em 1913, criaram a Reserva Federal, um banco central responsável pela emissão de novos certificados de papel e pelo resgate de bancos em situação de insolvência. Os governos, a nível mundial, reconheceram o valor do ouro e da prata, o que levou a conflitos e guerras pelo controlo dos mesmos. Nos anos que antecederam a Segunda Guerra Mundial, líderes como Lenine, Estaline, Churchill, Roosevelt, Mussolini e Hitler apreenderam ouro com propósitos estratégicos.



No início da década de 1930, nos Estados Unidos, deu-se uma mudança na conversibilidade do dinheiro em bens físicos. Naquela época, as pessoas costumavam ter uma grande parte da sua riqueza na forma de ouro. No entanto, em 1933, o Presidente Roosevelt emitiu o Decreto Presidencial 6102, que exigiu que todos os cidadãos entregassem o seu ouro. Não se tratou de uma troca voluntária – as pessoas foram obrigadas a entregar o seu ouro. Quem recusasse seria gravemente penalizado.

O governo definiu a taxa de câmbio de 20,67 USD por onça de ouro. Isto significava que, por cada onça de ouro que uma pessoa tinha, receberia certificados de papel que equivaliam a 20,67 dólares. As pessoas tiveram de aceitar estes dólares de papel, na esperança de que, um dia, pudessem voltar a trocá-los por ouro.

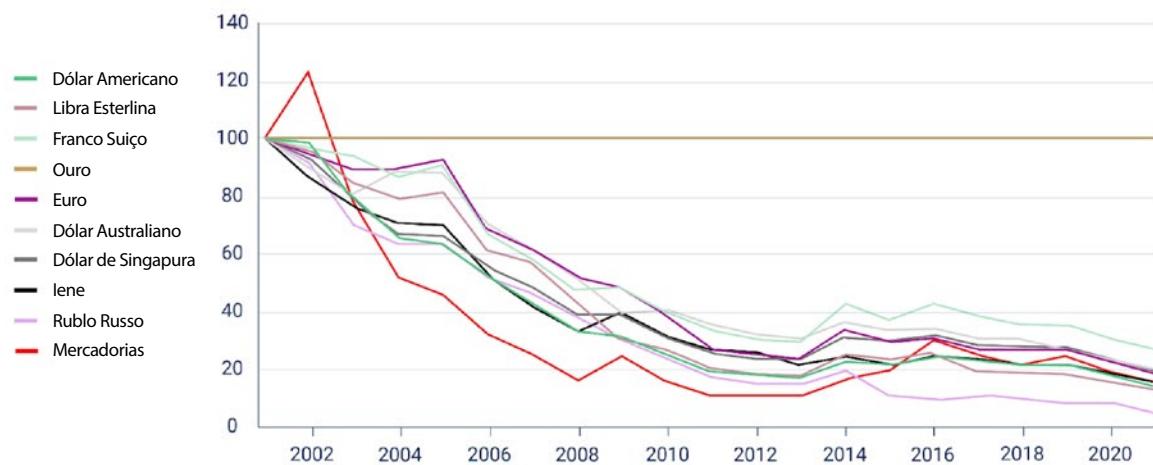


O que são moedas fiduciárias e quem as controla?

Em 1934, a lei da reserva de ouro permitiu às pessoas trocar novamente os seus dólares de papel por ouro. Porém, havia um problema. O governo desvalorizou propositadamente os dólares de papel, ao aumentar a taxa de câmbio para 35 dólares por onça de ouro. Esta desvalorização afetou pessoas trabalhadoras das classes média e baixa, pois significava que as suas poupanças, outrora mais valiosas, passavam a valer menos, devido à desvalorização dos dólares de papel.

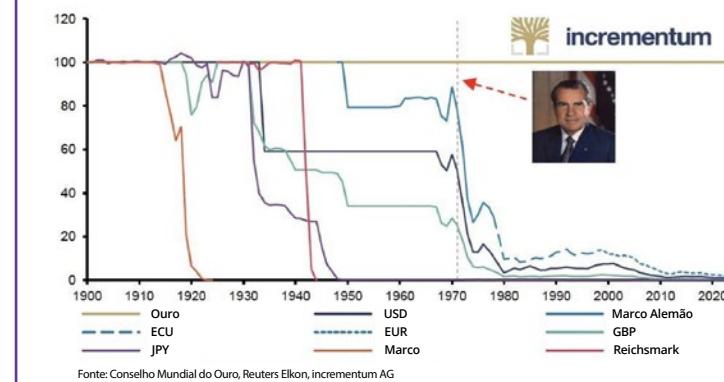
Após a Segunda Guerra Mundial, o acordo de Bretton Woods de 1944 estabeleceu o dólar americano como moeda de reserva mundial, conversível em ouro. No entanto, esta correspondência entre o dólar americano e o ouro deixou de existir em 1971, quando o Presidente Nixon acabou com a conversibilidade do dólar americano em ouro. Este acontecimento marcou uma enorme mudança e levou à adoção de um sistema de dinheiro fiduciário, onde o valor da moeda não corresponde a bens físicos como o ouro, mas sim à confiança das pessoas que a usam. Visto que os governos e os bancos centrais retiveram a maior parte do ouro das pessoas, o ouro valorizou bastante e chegou a atingir os 870 dólares por onça em 1980.

Valor do dólar americano em onças de ouro



Concluindo, a história da transição da sociedade humana de um padrão de dinheiro forte para um padrão de dinheiro frágil (fiduciário) é também a história em que os governos e bancos apreenderam os metais preciosos dos seus cidadãos. O verdadeiro dinheiro acabou nos bolsos dos governos e bancos, e as pessoas acabaram com papéis cujo valor vem unicamente dos governos que exigem a sua utilização.

Ouro e várias moedas medidas em ouro, 1900-2023



Fonte: Conselho Mundial do Ouro, Reuters Elkon, incrementum AG



Capítulo #4

4.2 O sistema fiduciário



O problema fundamental das moedas convencionais é o nível de confiança necessário para que funcionem. Temos de acreditar que o banco central não vai desvalorizar a moeda, embora a história das moedas fiduciárias esteja repleta de abusos dessa mesma confiança.

Satoshi Nakamoto



A humanidade deixou de ter um dinheiro forte controlado pelas massas e passou a ter um dinheiro frágil controlado pelas elites. Mas como é que este sistema funciona, exatamente?

4.2.1 Um sistema monetário obrigatório

O Sistema Fiduciário distingue-se pela sua natureza obrigatória, imposta às pessoas por meio de leis de curso legal. O termo "Fiat" (fiduciário), derivado do latim, significa "por lei" e representa uma ordem emitida pelas autoridades.

Ao contrário do dinheiro que é conversível em bens tangíveis como o ouro, o dinheiro fiduciário não tem essa capacidade. Em vez disso, a sua utilização é obrigatória por lei. As moedas que usamos diariamente, como dólares, euros, libras, yuans, pesos e outras, enquadram-se na categoria de dinheiro fiduciário.

Lei de curso legal: Uma lei que obriga todos os cidadãos a aceitar uma determinada moeda.



O valor do dinheiro fiduciário baseia-se na crença de que pode ser trocado por bens e serviços e na ilusão de que irá reter o seu valor ao longo do tempo. Podemos comparar o dinheiro fiduciário a um bilhete para um concerto; o seu valor não está no próprio bilhete de papel, mas sim na garantia de que a banda (o governo e respetivo banco central) vai proporcionar um ótimo espetáculo (oferecer estabilidade económica).

Vantagens do dinheiro fiduciário

- 💡 **Facilidade de utilização:** O dinheiro fiduciário é conveniente para transações do dia a dia.
- 💡 **Custos e riscos mais baixos:** O dinheiro fiduciário não requer grandes medidas de segurança, como é o caso do ouro, o que o torna mais barato e seguro.

Desvantagens do dinheiro fiduciário

- 💡 **Risco de inflação:** Os preços podem aumentar continuamente e causar inflação, incluindo ocorrências históricas de hiperinflação.
- 💡 **Controlo e manipulação centralizados:** O sistema pode ser influenciado e manipulado por pequenos grupos, o que leva à censura e à apreensão.
- 💡 **Riscos associados à contraparte:** Se o governo passar por dificuldades, a moeda pode desvalorizar.
- 💡 **Potencial de abuso:** É possível abusar do sistema, o que resulta em corrupção e perda de confiança.

O que são moedas fiduciárias e quem as controla?

Moeda-mercadoria e moeda fiduciária: Imagina a diferença

Lembra-te que, antes de surgirem as moedas fiduciárias, os governos produziam moedas feitas de uma matéria-prima física valiosa, escassa e difícil de obter, como o ouro ou a prata, ou imprimiam papel-moeda conversível numa determinada quantidade de uma matéria-prima física. Era um sistema baseado na conversibilidade em matérias-primas.

Por outro lado, o sistema fiduciário é mais parecido com o dinheiro do jogo Monopólio. No sistema fiduciário, o dinheiro consiste em papéis impressos pelo banco central, e as políticas governamentais influenciam diretamente o seu valor. O governo e os Bancos Centrais são basicamente os “banqueiros do jogo Monopólio”, que controlam o funcionamento do jogo, o que cada um recebe e o valor das coisas. Por outras palavras, o governo promete fazer uma boa gestão do sistema monetário.

Concluindo, as moedas fiduciárias só têm valor porque o governo exige a sua utilização; o dinheiro fiduciário, por si só, não tem qualquer utilidade.

Resumindo, o sistema fiduciário é um jogo de confiança, no qual o valor do nosso dinheiro baseia-se nas promessas dos governantes. E aos cidadãos, só resta esperar que o seu governo aja em benefício de todos. Em seguida, vamos ver como os bancos criam dinheiro, quem está envolvido nesse processo e o impacto que a criação de dinheiro tem na economia.

4.2.2 Reservas mínimas obrigatórias: sistema sustentado pela dívida



Ainda bem que o povo deste país não comprehende o nosso sistema bancário e monetário, pois acho que, se comprehendessem, haveria uma revolução ainda hoje.

Henry Ford



O sistema de reservas mínimas obrigatórias é uma parte fundamental do sistema fiduciário, que permite aos bancos emprestar uma grande parte dos depósitos dos seus clientes. Já alguma vez questionaste por que razão os bancos oferecem tantos serviços aos seus clientes? Pode parecer generosidade, mas é importante lembrar que os bancos são empresas e que o seu principal objetivo é obter lucro. Mas como é que lucram, se estão a dar dinheiro, quando concedem empréstimos?

Para além de receberem juros sobre os depósitos, os bancos têm outros rendimentos, incluindo:

- ✿ Juros sobre os empréstimos que concedem
- ✿ Taxas cobradas por serviços como a utilização de caixas multibanco e manutenções de contas
- ✿ Rendimentos provenientes de investimentos, como a compra e venda de títulos ou investimentos imobiliários
- ✿ Retenção de uma percentagem dos empréstimos em reserva e utilização do resto em investimentos ou empréstimos
- ✿ Juros pagos sobre depósitos e taxas cobradas em contas à ordem e contas poupança



Bancos pedem dinheiro emprestado aos depositantes a uma taxa de juro (digamos 5%)



Emprestam esse dinheiro aos mutuários a uma taxa de juro mais alta (digamos 9%)



Os bancos pagam juros com base nos juros recebidos pelos empréstimos ($9\% - 5\% = 4\%$) e mantêm o restante como seu lucro.



Capítulo #4

Quando um banco recebe um depósito, só precisa de reter uma fração do mesmo (reserva mínima), e pode emprestar o resto. Por exemplo, se depositar 100 €, com uma reserva mínima de 10%, o banco pode emprestar 90 € e reservar apenas 10 €. O mutuário deposita 90 € noutro banco, o que permite que o ciclo continue. Apesar do depósito inicial de 100 €, a quantia total na economia é agora de 271 €, que parecem surgir do nada – um fenómeno conhecido como efeito multiplicador.

Este processo dá origem a um sistema monetário sustentado pela dívida, tendo em conta que os bancos criam mais dinheiro com cada empréstimo, o que aumenta a massa monetária geral. Com a continuação do sistema de reservas mínimas obrigatórias, a dívida total na economia aumenta, o que contribui para a inflação. Este sistema depende de um ciclo contínuo de criação de dinheiro. Através de empréstimos, que é como um fornecimento constante de drogas a um toxicodependente. No entanto, se os bancos emprestarem mais dinheiro do que o que têm reservado e todos os depositantes resolverem levantar o seu dinheiro ao mesmo tempo, os bancos podem entrar em situação de insolvência.

Numa situação destas, o banco central intervém como mutuante de último recurso, para enviar aos bancos dinheiro novo, a fim de evitar insolvências. Para isso, o banco central readquire ativos ou injeta dinheiro diretamente nas contas dos bancos. Essencialmente, os bancos são resgatados, através da injeção constante de dinheiro novo por parte dos bancos centrais. Este sistema sustentado pela dívida e sistematicamente resgatado pelo banco central resulta em ciclos de expansão e recessão.

Imagina que tens um amigo que, por acaso, é banqueiro. Chamemos-lhe João.

O João adora bicicletas e quer pedir a tua bicicleta emprestada, pois quer visitar vários sítios. Ele convence-te a emprestar-lhe a tua bicicleta e, quando menos esperas, o João começa a prometer a mesma bicicleta a muitos outros amigos ao mesmo tempo. Com a tua bicicleta que te pediu emprestada, o João consegue criar bicicletas imaginárias e começa a emprestá-las a amigos. Cada um dos amigos dele pensa que poderá dar uma voltinha sempre que quiser. Mas eis o problema – só existe uma bicicleta! Todas as outras são imaginárias e não passam de promessas.

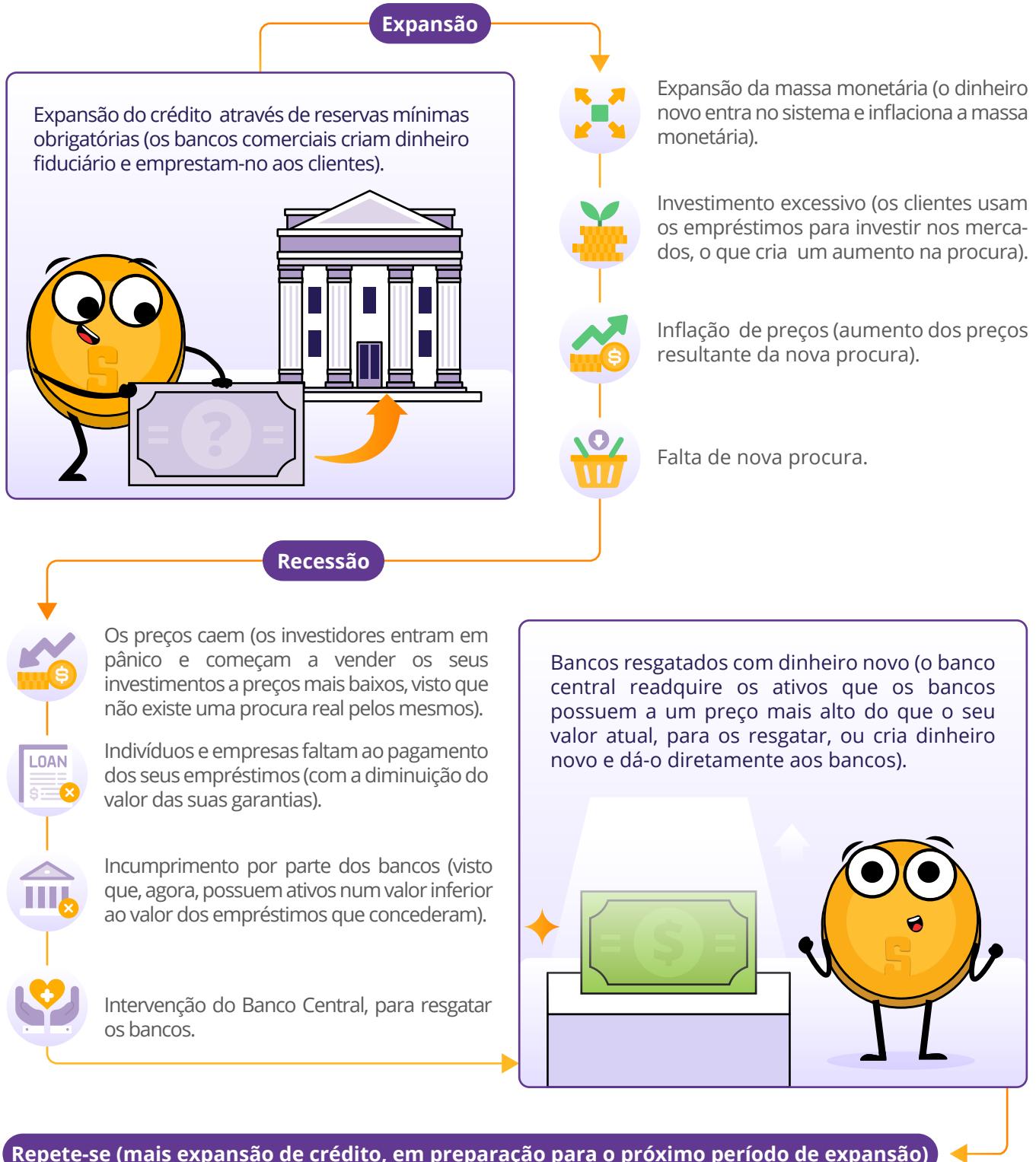
Eis o que acontece: À medida que circulam mais bicicletas imaginárias, ficam todos muito felizes, pelo menos no início. Porque, no início, ninguém usa a bicicleta ao mesmo tempo. Não parece haver problema. Parece haver uma abundância de bicicletas para todos. Depois, todos os amigos começam a fazer mais planos e a pensar em todos os lugares que vão visitar com as suas bicicletas.

Mas é aqui que a magia começa a perder o efeito. Certo dia, todos decidem que é o dia perfeito para um passeio de bicicleta. Aparecem todos à porta do João, entusiasmados para dar uma voltinha nas suas bicicletas imaginárias. Mas eis que a verdade vem ao de cima – só existe uma bicicleta. A desilusão instala-se e, de repente, o valor das viagens prometidas diminui.

O mundo dos empréstimos com reservas mínimas obrigatórias funciona de forma semelhante. Os bancos emprestam mais dinheiro do que o que realmente têm e, durante algum tempo, todos desfrutam dos benefícios. Entra mais dinheiro em circulação e o mesmo não parece ter fim à vista. Mas, se muitas pessoas tentarem levantar o seu dinheiro ao mesmo tempo, descobre-se a verdade: não existe dinheiro suficiente para cumprir todas as promessas.

Esta situação afeta o bem comum e o património de todos os envolvidos. A abundância prometida transforma-se num esquema fraudulento. As bicicletas imaginárias perdem o valor que lhes é atribuído, quando todos querem dar uma volta. Tal como o valor do dinheiro na economia pode diminuir, quando todos tentam levantar o dinheiro que lhes pertence. Quando isso acontece, as pessoas descobrem que o dinheiro que têm no banco, na verdade, não existe. Isto causa pânico, insolvências bancárias e até mesmo o colapso de economias inteiras. Até agora, foram sempre os mesmos a lidar com as consequências desses colapsos: as classes baixas e médias do mundo.

O que são moedas fiduciárias e quem as controla?



Atividade: Reservas mínimas obrigatórias

No exercício seguinte, vamos aprender como o sistema de reservas mínimas obrigatórias pode levar à desvalorização da moeda, à inflação e a uma redução do poder de compra. Vamos utilizar um exemplo simplificado, que envolve seis participantes (um dos quais será o banco) e um rácio de reserva que ainda é muito utilizado atualmente: 10%.

- ✿ "A" acabou de ganhar 100 000 € na lotaria e deposita-os no banco ("B"). Com um rácio de reserva de 10%, "B" tem de manter 10 000 € no seu cofre e pode emprestar os restantes 90 000 €.
- ✿ "C" pede um empréstimo a "B" no valor máximo (90 000 €) e usa-o para comprar uma casa a "D".
- ✿ "D" deposita os 90 000 € que recebeu de "C" no banco ("B"). A quantia total de depósitos no banco passou a ser de 190 000 €.
- ✿ "E" pede um empréstimo a "B", e o banco empresta 90% do novo depósito, que é 81 000 €.
- ✿ "E" usa o empréstimo de 81 000 € para comprar uma peça de arte a "F", que, em seguida, deposita o dinheiro no banco ("B"). O total de depósitos registados passa a 271 000 €.

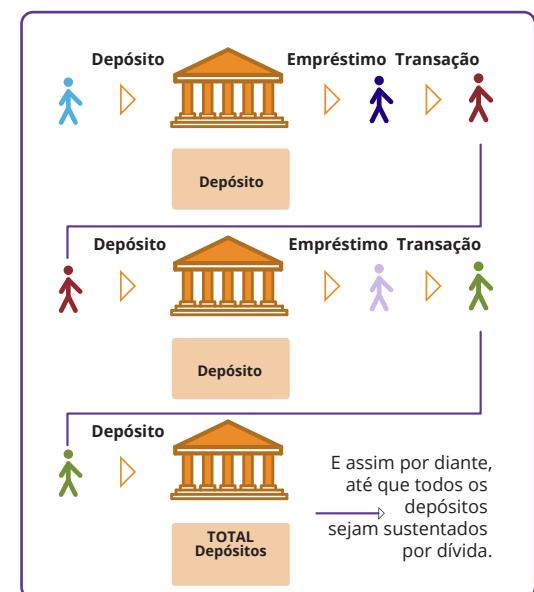
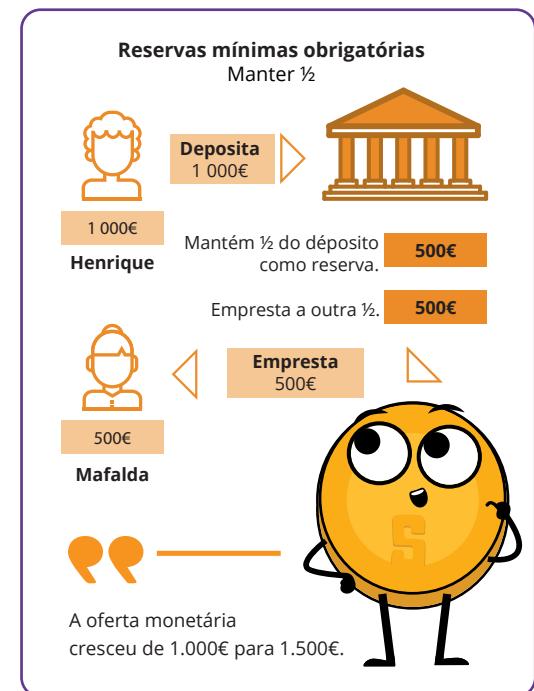
Neste cenário, o depósito inicial de 100 000 € resultou num total de 271 000 € em depósitos, após circular na economia.

Se o rácio de reserva fosse reduzido para 1%, a quantia criada seria muitíssimo superior ($100\ 000\ € / 0,01 = 10\ 000\ 000\ €$). No exemplo deste exercício, quanto dinheiro seria, de facto, criado com esses 100 000 €, se o dinheiro continuasse a circular na economia?

É de salientar que, desde 2020, a Reserva Federal (o Banco Central dos EUA) reduziu os rácios das reservas mínimas obrigatórias para zero por cento, com o propósito de estimular a economia.

Precisamos dos seguintes voluntários:

- A = Depositante (Vencedor da Loteria) (Azul Claro)
- B = Caixa do Banco (Banco)
- C = Devedor #1 (Azul Escuro)
- D = Proprietário de Imóvel/Depositante (Vermelho)
- E = Devedor #2 (Roxo Claro)
- F = Proprietário de Galeria de Arte/Depositante (Verde)



O que são moedas fiduciárias e quem as controla?

4.2.3 Quem controla o sistema fiduciário e que benefícios têm?

Existem quatro intervenientes principais: o governo, os ricos, o setor financeiro e o banco central. Em conjunto, todos eles controlam o sistema fiduciário.

O governo: O governo é uma espécie de diretor do espetáculo fiduciário. Juntamente com a cobrança de impostos, é financiado através de novas dívidas (obrigações) emitidas pelo Ministério das Finanças. Quando não há procura suficiente para estas obrigações, qualquer dívida restante é comprada pelo banco central. Isto significa que podem continuar a realizar as suas atividades e a perseguir os seus interesses, sem precisar da aprovação do povo. É como receber um cartão de crédito, sem se preocupar em pagar logo a dívida. Isto pode parecer benéfico para o governo, mas tem um custo para todas as outras pessoas.

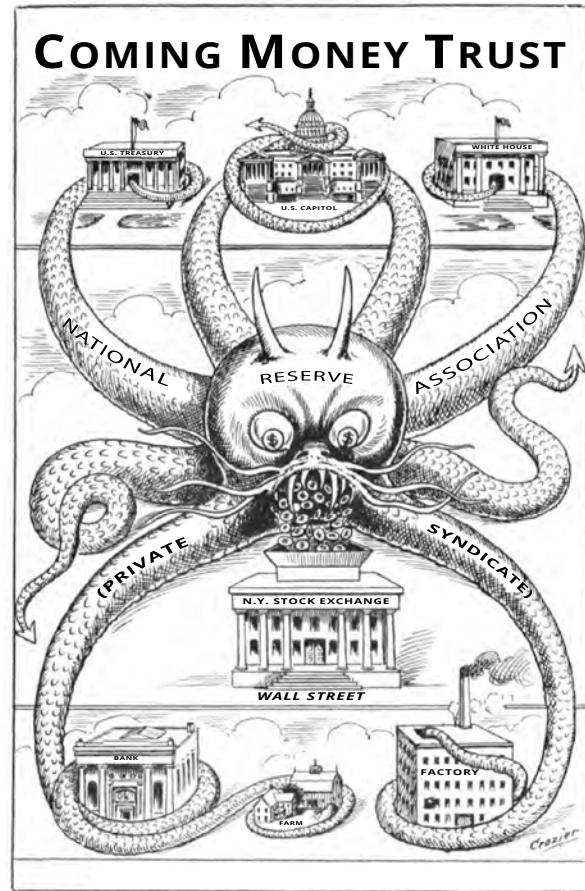
Ricos: Os ricos beneficiam muito com o sistema fiduciário. Ao conseguir acumular mais dívidas, podem investir em ativos como matérias-primas, imóveis e ações, para gerar mais riqueza, praticamente sem esforço nenhum.

Setor Financeiro: Os bancos e outras instituições financeiras não controlam diretamente o sistema fiduciário, mas beneficiam muito do mesmo. Sem qualquer responsabilização, podem continuar e acelerar o processo de criação de dinheiro, através de empréstimos com reservas mínimas obrigatórias, por forma a aumentar o seu lucro. Os bancos são praticamente isentos de consequências, pois são resgatados com dinheiro fiduciário novo, para evitar que o sistema inteiro entre em colapso.

Banco Central: O banco central é quem dá as ordens e, supostamente, controla o crescimento da massa monetária. Mas há um pormenor importante – o banco central também está sujeito às leis do governo, pelo que serve os interesses do mesmo. É como um marionetista a ser controlado por outro marionetista. Pode parecer que o banco central é a entidade responsável, mas está apenas a servir indiretamente o interesse do governo em imprimir dinheiro do nada, sempre que precisa.

Os benefícios que têm: Estes grupos beneficiam de várias formas, ao criar uma complexa rede de controlo. O governo obtém fundos sem consequências imediatas, os ricos e os bancos ganham dinheiro sem esforço, e o banco central faz com que o espetáculo continue. Entretanto, o resto da população sente as consequências, pois enfrenta dificuldades à medida que o sistema se desenvolve.

No final, os marionetistas do sistema fiduciário criam um sistema onde alguns beneficiam muito, mas onde a maioria se sente injustiçada na posição onde se encontra.



THE OCTOPUS - "ALDRICH PLAN"

O papel dos bancos centrais

Os bancos centrais moldam discretamente o funcionamento de uma economia. A sua função oficial é garantir estabilidade e integridade e “manter tudo estável”, mas os seus métodos revelam um lado mais misterioso.

Os bancos centrais trabalham em estreita colaboração com os governos e influenciam as políticas monetárias, por forma a utilizar ferramentas como as taxas de juro para controlar a massa monetária. Em tempos de crise, imprimem dinheiro do nada e injetam-no na economia, através dos bancos comerciais, para dar a impressão de que está tudo bem.

Eles não se limitam a monitorizar o sistema; os bancos centrais regulam os bancos comerciais, ditam as regras do jogo e intervêm para ajudar os bancos em situação de insolvência (como credores de último recurso). Esta rede de controlo dos bancos centrais, embora pareça protetora, torna a economia e os bancos ainda mais dependentes deles.

Para compreender todo o sistema financeiro, é fundamental que entendamos de onde vêm biliões de euros em estímulos e quem decide como distribuí-los. Os governos utilizam várias ferramentas para gerir a massa monetária, em determinadas alturas.

Os bancos centrais e os governos podem usar instrumentos de política monetária e orçamental para influenciar a massa monetária e a economia. Por exemplo, a Reserva Federal dos Estados Unidos (Fed) utiliza políticas monetárias para ajustar as taxas de juros, por forma a influenciar a quantia de dinheiro em circulação. As políticas orçamentais, por outro lado, envolvem o uso de políticas fiscais e de despesa para influenciar a atividade económica.

Política Monetária **Taxas Ideais**

Desemprego inferior a
6,5%



2% - 3%
Aumento anual do Produto Interno Bruto (PIB)



Taxa de inflação subjacente
2,0% - 2,5%



Política Orçamental **Expansionista**

Visa aumentar os gastos do consumidor e o investimento empresarial, por forma a aumentar a procura agregada e o crescimento económico.



Aumentar a despesa do governo

VS

Política Orçamental **Contracionista**

Visa diminuir os gastos dos consumidores e o investimento das empresas, para abrandar o crescimento económico insustentável e prevenir ou reduzir uma inflação alta.



Aumentar os impostos

O que são moedas fiduciárias e quem as controla?

As políticas cambiais, os choques de oferta e os controlos de preços são instrumentos adicionais, para regular a massa monetária e influenciar o comércio e a economia. Embora estas políticas tenham o objetivo de estabilizar os preços e controlar a inflação, estas intervenções causam, muitas vezes, ciclos de expansão e recessão, que dificultam a vida a todos os que usam a moeda controlada.

Exemplo: a expressão “demasiado grande para falir” refere-se a instituições financeiras que são tão grandes e interligadas que uma possível insolvência das mesmas teria repercussões catastróficas em todo o sistema financeiro. Durante a crise financeira de 2008, muitos grandes bancos foram considerados demasiado grandes para falir, o que levou o governo dos EUA a intervir e a resgatá-los, para evitar o seu colapso.

Um dos exemplos mais proeminentes de uma instituição demasiado grande para falir, durante a crise financeira, foi o banco de investimento Lehman Brothers. Quando o Lehman Brothers declarou falência em setembro de 2008, desencadeou um efeito dominó de acontecimentos, incluindo o quase colapso da gigante seguradora AIG e uma enorme queda no mercado de ações. O governo dos Estados Unidos teve de intervir e resgatar outras grandes instituições financeiras, para evitar um caos maior e para salvaguardar a economia em geral.

Para entenderes as limitações dos sistemas monetários fiduciários e centralizados, é essencial que comprehendas o funcionamento destas políticas. Se não entenderes o problema, não vais reconhecer a solução. Agora que abordámos o funcionamento do sistema fiduciário no passado e no presente, vamos ver o que nos reserva o futuro das moedas fiduciárias: Moedas Digitais do Banco Central (ou CBDC).

4.3 Moedas digitais do banco central: O futuro do dinheiro fiduciário

As Moedas Digitais do Banco Central (CBDC) são a próxima fase das moedas fiduciárias. Ao contrário da combinação de notas, moedas e pagamentos digitais, as CBDC são formas completamente digitais de moedas fiduciárias, emitidas por governos e controladas pelos bancos centrais.

Imagina a moeda que utilizas todos os dias, mas sem qualquer presença física – sem moedas a chocalhar no bolso, nem notas para dobrar e desdobrar. O que diferencia as CBDC é o elevado nível de controlo e monitorização que oferecem aos governos e aos bancos centrais. Com as CBDC, as autoridades ganham uma visibilidade sem precedentes sobre as transações financeiras, o que facilita a monitorização e regulação do fluxo de dinheiro.

Os governos e os bancos centrais podem ajustar instantaneamente a forma e a oferta das CBDC, manipular as taxas de juro e implementar instrumentos de política monetária e orçamental com maior precisão. Essencialmente, as CBDC oferecem às autoridades meios mais eficientes para influenciar e gerir a sua moeda fiduciária.

Embora as CBDC pareçam o futuro do dinheiro fiduciário, o atual sistema monetário mundial já opera com base num puro padrão fiduciário. As moedas fiduciárias já não têm correspondência ao ouro, o que resulta numa enorme expansão da massa monetária, praticamente sem restrições.

Agora que comprehendas melhor o funcionamento do sistema fiduciário, está na altura de desvendarmos as consequências do mesmo no Capítulo 5.

Capítulo #5

A criação de soluções, com base nos problemas

5.0 Introdução ao problema

5.1 Redução do poder de compra

5.1.1 A inflação monetária e o seu efeito no poder de compra

Atividade - Os efeitos da inflação - Uma atividade de leilão

5.2 O peso da dívida global e a desigualdade social

5.2.1 Impacto nos cidadãos - Perda de poder de compra

5.2.2 Impacto na sociedade - Aumento da desigualdade na distribuição da riqueza

Atividade - Consequências do sistema fiduciário

5.2.3 O peso da dívida global

5.3 Os Cypherpunks e a procura de uma moeda descentralizada

5.3.1 Os Cypherpunks

5.3.2 Sistemas centralizados e descentralizados

5.3.3 História resumida das moedas digitais

A criação de soluções, com base nos problemas

5.0 Introdução ao problema



Quem controlar o volume de dinheiro no nosso país tem o controlo absoluto de toda a indústria e comércio... Quando percebemos que todo o sistema é fácil de manipular, de uma forma ou de outra, por alguns homens poderosos que estão no topo, não precisamos que nos digam como surgem os períodos de inflação e de crise.

James A. Garfield, Presidente dos Estados Unidos



No Capítulo 4, aprendeste que o mundo financeiro está dependente de um sistema que pode não ser tão robusto como parece. O sistema fiduciário, sustentado pela constante impressão de papel-moeda, parece ser mais vantajoso para alguns do que para a maioria.

Este capítulo revela o impacto que o sistema fiduciário tem nos cidadãos e na sociedade. Por fim, vamos descobrir a história de um grupo de indivíduos, que detetou os problemas e, discretamente, tentou encontrar uma solução capaz de mudar o futuro da sociedade humana.

5.1 Redução do poder de compra

5.1.1 A inflação monetária e o seu efeito no poder de compra

A inflação monetária é o aumento da massa monetária dentro de uma economia, o que afeta diretamente o cidadão comum, pois reduz o seu poder de compra. O ciclo da inflação de preços começa em alturas em que existe mais dinheiro em circulação. Isto aumenta a procura de bens e serviços, o que faz com que os preços aumentem.

Imaginemos um pequeno grupo de amigos – o Alexandre, o Roberto e o Charlie – cada um com um euro na mão. E há uma garrafa de água à venda. A situação inicial é simples: três pessoas com um total de três euros e uma garrafa de água. Agora, imaginemos que alguém (digamos que é o governo local) decide dar a cada amigo mais um euro. Agora, em conjunto, têm seis euros. Com mais dinheiro no bolso, todos eles querem comprar aquela garrafa de água. Visto que todos querem a mesma garrafa, começam a fazer licitações uns contra os outros.

O aumento da procura, causada pela quantia adicional, fá-los oferecer valores acima do preço inicial da garrafa de água. No final, as licitações fazem com que o preço da garrafa de água suba. Esta situação reflete uma redução do poder de compra deles. Apesar de terem mais dinheiro, não conseguem comprar tantas garrafas de água como antes, o que demonstra o impacto da inflação no valor do seu dinheiro.

Neste exemplo, este grupo de amigos testemunhou uma redução do seu poder de compra, porque estavam a usar uma forma de dinheiro que foi influenciada por fatores externos, como a quantia adicional introduzida pelo governo. A falta de controlo sobre a massa monetária, em conjunto com o aumento da procura, levou a um aumento dos preços, o que faz com que seja mais difícil, para estes amigos, comprar a mesma quantidade de bens com a quantia adicional que têm.

Isto demonstra que o poder de compra deste grupo de amigos foi afetado por fatores que estavam fora do seu controlo e salienta a importância de compreender e questionar os sistemas que influenciam o valor do nosso dinheiro.

Agora, vamos ver como isto se aplica à vida real.



Capítulo #5

Atividade: Os efeitos da inflação – Uma atividade de leilão

Objetivo: Compreender o conceito de inflação e como o mesmo afeta os preços dos bens e serviços numa economia.

Definições:

 Massa monetária: quantia total em circulação dentro de uma economia, num determinado momento. Isto inclui:

- As formas físicas da moeda, tais como moedas e notas
- Contas-correntes
- Contas poupança
- Contas no Mercado Monetário
- Pequenos depósitos a prazo (como certificados de depósito) inferiores a 100 000 €

 Leilão: Uma venda pública, na qual são vendidos bens ou propriedades a quem fizer a melhor oferta.

Exercício de turma. Segue as instruções abaixo:

1. O professor vai distribuir, de forma aleatória, uma determinada quantia em dinheiro de Monopólio. Isto representa a massa monetária numa sociedade.
2. Anota a massa monetária total na tabela que te foi dada.
3. O professor vai leiloar um chocolate aos alunos. Para ganhares o chocolate, terás de fazer a melhor oferta com o dinheiro de Monopólio que tens. Regista a oferta vencedora ao lado da massa monetária.
4. Agora, o professor vai adicionar uma grande quantia de dinheiro de Monopólio à massa monetária. Isto representa um aumento da massa monetária de uma economia. Mais tarde, vais aprender como se aumenta e reduz a massa monetária numa economia.



Muitas vezes, as sociedades podem ser imprevisíveis e injustas, como exemplificado pela simulação em que um professor dá, aleatoriamente, uma quantia significativa a apenas alguns alunos. Isto assemelha-se a situações da vida real, onde pode haver uma distribuição desigual de recursos e oportunidades, destacando a aleatoriedade e injustiça inerentes em muitas situações.

5. O professor vai leiloar um segundo chocolate aos alunos, utilizando o mesmo processo. Regista a oferta vencedora na tabela, ao lado da massa monetária.
6. O professor vai repetir o leilão uma terceira vez.

A criação de soluções, com base nos problemas

Ronda	Massa Monetária	Oferta Vencedora
1		
2		
3		

Conclusão:

1. De que forma é que o aumento da massa monetária afetou as ofertas vencedoras dos chocolates?
2. Qual é a relação entre o aumento da massa monetária e a inflação?
3. Que importância tem a massa monetária na vida real?
4. Quando se injeta mais dinheiro na economia, o que achas que acontece aos preços dos bens e serviços? Será essa alteração nos preços temporária ou permanente. Porqué? A longo prazo, que impacto terão essas alterações de preços nos cidadãos de uma sociedade?

5.2 O peso da dívida global e a desigualdade social

5.2.1 Impacto nos Cidadãos – Perda de poder de compra

O Jaime é estudante universitário e vive num pequeno apartamento. Trabalha a tempo parcial num café, para pagar as contas e propinas. Assim que começou a viver sozinho, o Jaime aprendeu a gerir o seu próprio livro-razão.



Um **livro-razão** é um registo detalhado de todas as tuas transações monetárias. Quer se trate de rendimentos ou despesas, um livro-razão ajuda-te a monitorizar tudo.

No início de 2023, ele orçamentou 10 000 € para pagar as contas durante o ano todo, incluindo rendas, alimentação e outras necessidades. Estas foram as suas transações em janeiro de 2023:



Capítulo #5

Data	Descrição	Valor	Tipo	Saldo
01/01/2023	Saldo Inicial			1 600 €
01/01/2023	Renda de Janeiro	800 €	Débito	800 €
05/01/2023	Supermercado	100 €	Débito	700 €
15/01/2023	Salário do trabalho a tempo parcial	500 €	Crédito	1 200 €
20/01/2023	Gasolina para o carro	350 €	Débito	850 €
30/01/2023	Manuais Escolares	150 €	Débito	700 €

Este livro-razão mostra que o saldo inicial do Jaime era 1 600 €, dos quais ele **gastou** (um **débito**) 800 € para pagar a renda mensal. Depois, **gastou** 100 € no supermercado e recebeu uma renumeração de 500 € (um **crédito**) pelo seu trabalho a tempo parcial, o que aumentou o seu saldo para 1 200 €. Depois, **gastou** dinheiro em combustível e manuais escolares, o que reduziu o seu saldo para 700 € no final do mês.

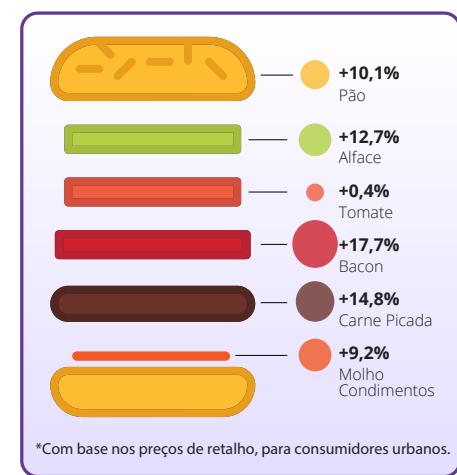
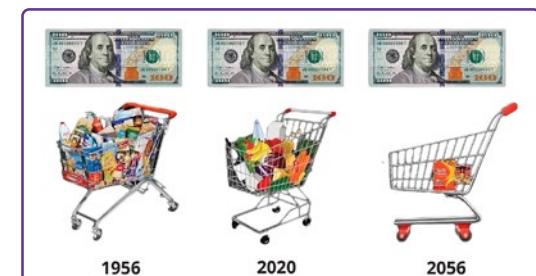
Um ano mais tarde, o Jaime foi almoçar com o seu avô, com quem partilhou os detalhes do seu orçamento para 2024. O Jaime repara que o seu orçamento já não chega para pagar tudo e que o seu custo de vida aumentou bastante no último ano. O Jaime tem dificuldade em entender o que causou esta mudança, ao que o seu avô lhe mostra a seguinte imagem.

O Jaime não acredita no que vê. Foi assim que descobriu que o custo dos bens e serviços aumenta drasticamente com o tempo, o que causa uma diminuição no seu poder de compra.

O seu avô diz: "Em 1956, eu era apenas um jovem a entrar no mundo do trabalho. Lembro-me que costumava ganhar 380 € por mês, a trabalhar numa fábrica. Pode não parecer muito, mas era um salário razoável naquela altura. Aliás, consegui poupar dinheiro suficiente para comprar a minha própria casa nos subúrbios."

O avô continua a sua explicação: "Os preços das coisas eram muito diferentes no século passado. Por exemplo, em 2020, 30 chocolates Hershey's custavam 26,14 €. Mas, se voltarmos atrás no tempo até 1913, o preço da mesma quantidade de chocolate Hershey's era apenas 1,00 €."

Esta enorme diferença de preços destaca a evolução do poder de compra ao longo do tempo e demonstra o quanto essa evolução foi influenciada pela inflação ao longo dos anos.

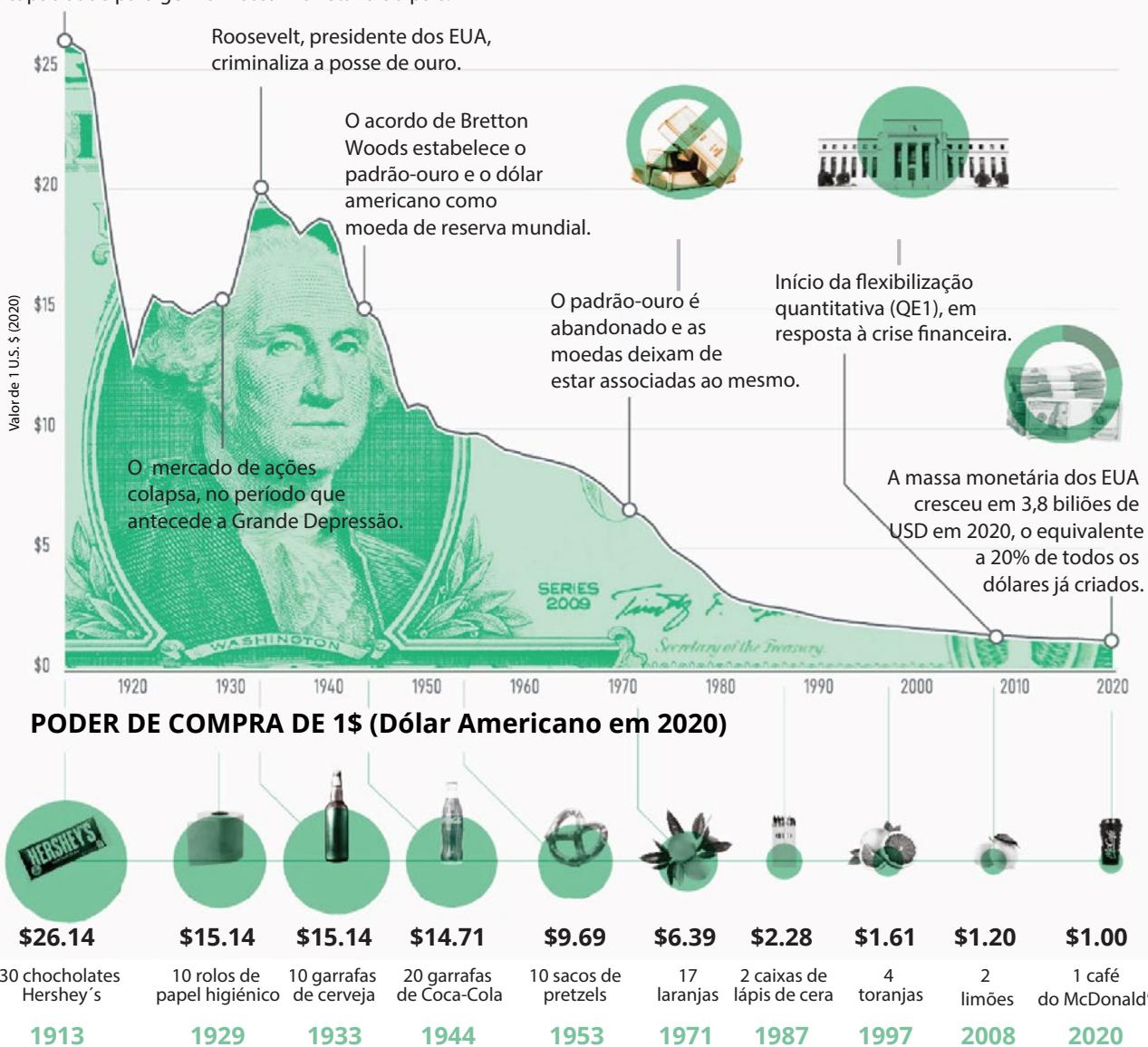


A criação de soluções, com base nos problemas

O Valor de um dólar

Poder de compra do dólar Americano

A Lei da Reserva Federal cria um banco central com capacidade para gerir a massa monetária do país.



Jaime: "O quê? Isso é de loucos. Nem imagino o quanto baixa a minha renda seria naquela altura, em comparação com o que é agora."

Avô: "Sim, a tua renda seria muito mais barata naquela altura. Eu tenho outro exemplo: na altura, 1,00 € dava para comprar cerca de 10 sacos de pretzels. Em 2020, paguei 9,69 € pela mesma coisa. Imagina quanto custarão 10 sacos de pretzels hoje."

Capítulo #5



Jaime: "Uau! Isso é muito interessante, avô. Como é que isto te afetou a ti, quando eras mais novo? "

Avô: "Oh, Jaime... quando eu era jovem, era tudo muito mais barato. Um pão só custava 0,18 €, e conseguia comprar um bidão de gasolina por apenas 0,29 euros. É incrível o quanto o custo de vida aumentou."

Após a conversa com o seu avô, o Jaime foi para casa e voltou a analisar o livro-razão. Percebeu de imediato que terá de orçamentar mais 1 000 € para 2024, para conseguir comprar a mesma quantidade de bens e serviços que comprou no ano anterior. Isto significa que o seu poder de compra diminuiu em 1 000 €, visto que passa a ter de gastar mais dinheiro para comprar os mesmos bens e serviços. Embora o salário do Jaime só aumente ligeiramente, os seus custos de vida aumentam bastante a cada ano que passa.

A tabela que se segue mostra as despesas do Jaime no primeiro ano e no segundo ano, bem como o aumento percentual dos preços.

Para conseguir manter o seu nível de vida, o Jaime terá de trabalhar mais horas por semana, por forma a receber mais 1 000 €.

Com base nas informações do Instituto de Estatísticas do Trabalho dos Estados Unidos, os preços atuais são cerca de 30 vezes mais altos do que em 1913. Isto significa que, atualmente, com um dólar, só consegue comprar cerca de 3% daquilo que conseguia comprar em 1913.

Item	Custo Ano #1	Custo Ano #2	% Aumento
Renda	4 000 €	4 500 €	12,5%
Supermercado	2 000 €	2 300 €	15%
Necessidades	4 000 €	4 200 €	5%
Total	10 000 €	11 000 €	10%

Por exemplo, se alguém desse ao Jaime a opção de viajar no tempo e receber 100 € em 1913 ou esperar até 2023 e receber apenas 3,00 €, seria como escolher entre carrinhos cheios de compras naquela altura e meia dúzia de coisas hoje. Esta enorme diferença de preços mostra o quanto diminuiu o poder de compra do dinheiro ao longo dos anos.

1938 CUSTO DE VIDA

DESPESAS COMUNS

Casa Nova	3.900,00 USD
Rendimento Médio	1.731,00 USD por ano
Carro Novo	860,00 USD
Renda Média	27,00 USD por mês
Propina para Harvard	420,00 USD por ano
Bilhete de Cinema	0,25 USD cada
Gasolina	0,10 USD por galão
Carimbo Postal dos EUA	0,03 USD cada

ALIMENTOS

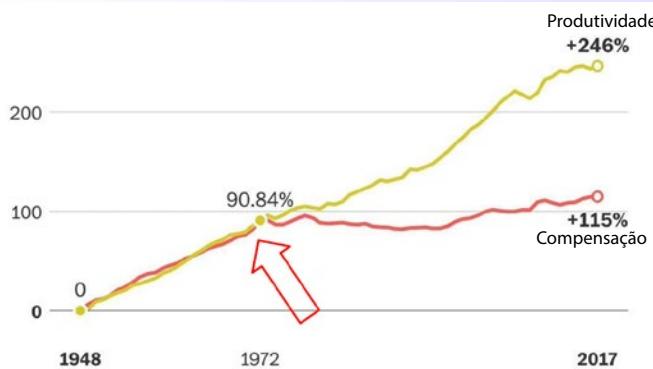
Açúcar Granulado	0,59 USD por 10 libras
Leite - Vitamin D	0,50 USD por galão
Bacon	0,39 USD por libra
Café Moído	0,32 USD por libra
Ovos	0,18 USD cada dúzia

(Com base na imagem original)

A criação de soluções, com base nos problemas

Se compararmos os salários, o Jaime ganha muito mais num ano do que o seu avô alguma vez ganhou. No entanto, o dinheiro que o avô do Jaime tinha valia muito mais e dava para comprar muito mais coisas naquela altura.

Crescimento na Produtividade e na Remuneração Horária (1948-2017)



NOTA: A remuneração inclui salários e benefícios para trabalhadores de produção e não supervisores.

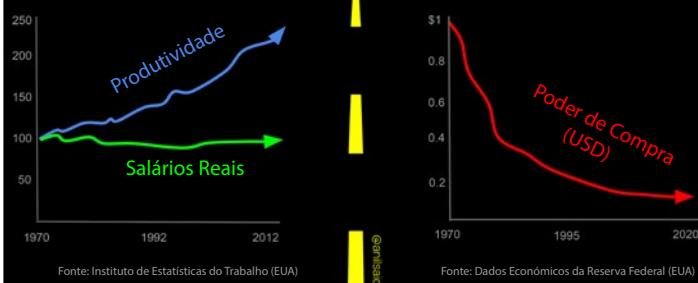
No mundo em que vivemos hoje, o enorme impacto da inflação faz com que as pessoas não se sintam motivadas a poupar dinheiro.

Pelo contrário, a maioria opta por gastar o seu dinheiro de imediato, tendo em conta que o valor do mesmo diminui muito rapidamente. Esta perspetiva pessimista tem um impacto negativo na capacidade das pessoas de planejar o seu futuro.

Como vimos no gráfico, o aumento geral dos salários permanece estagnado, quando se tem em conta a inflação. Isto significa que os aumentos dos salários das pessoas não estão a acompanhar a taxa de desvalorização do seu dinheiro, apesar de se trabalhar mais.

O exemplo do Jaime é apenas um entre muitos. No mundo fiduciário, os governos criam dinheiro do nada com bastante frequência, a fim de promover os seus próprios interesses, embora sejam os cidadãos de todo o mundo que lidam com as consequências. Os preços das nossas compras do dia a dia aumentam todos os anos, desde o pão até à habitação; desde as compras de supermercado até às viagens de férias. Enquanto os ricos lucram com a inflação, por possuírem ativos, o cidadão comum vê o dinheiro que lhe custa a ganhar a perder valor. O resultado? Existem pessoas e famílias no mundo inteiro a passar dificuldades, devido à redução do seu poder de compra.

O caminho para a Sujeição



Pessoas de todo o mundo acabam por ter mais empregos e trabalhar mais horas, apenas para manter o seu nível de vida. É como correr numa passadeira cada vez mais rápido, mas nunca sair do mesmo sítio. O sistema fiduciário faz com que as pessoas sintam que estão numa infundável corrida contra o aumento dos preços.

Muitas pessoas, numa tentativa de fazer face ao aumento dos preços, recorrem à dívida, que é como usar um penso rápido num golpe muito fundo. As pessoas contraem empréstimos ou tomam decisões impulsivas, apenas para sobreviver. O dinheiro fácil torna-se uma necessidade, e as pessoas acabam num ciclo onde a sobrevivência de hoje tem prioridade sobre o planeamento do futuro.

O sistema fiduciário, com a constante criação de dinheiro, afeta a psicologia da humanidade. Incute uma preferência temporal alta – um foco em ganhos a curto prazo, em vez do planeamento a longo prazo. Como solução rápida para um alívio imediato, os cidadãos do mundo fiduciário tendem a priorizar os benefícios a curto prazo. É um instinto de sobrevivência, que cria um ciclo de dependência, onde as pessoas procuram qualquer forma de obter dinheiro rápido, mesmo que não seja sustentável ou viável a longo prazo.

Essencialmente, o impacto do sistema fiduciário dificulta a vida a todos os cidadãos a nível global. No sistema fiduciário, os preços sobem, os salários estagnam, e a luta pela sobrevivência torna-se uma batalha diária. Enquanto certos grupos se tornam mais ricos, a maioria dos cidadãos do mundo permanece dependente de um sistema que os torna cada vez mais pobres.

5.2.2 Impacto na Sociedade - Aumento da desigualdade na distribuição da riqueza

Numa sociedade com dinheiro forte, a tomada de decisões financeiras do governo depende da aprovação do povo. No entanto, no sistema fiduciário, os governos podem contrair dívida de forma ilimitada, à custa dos seus cidadãos.

O poder de imprimir dinheiro conforme se deseja leva, muitas vezes, a uma centralização política. O sistema fiduciário permite que os governos acumulem dívidas enormes, enquanto tomam decisões que os beneficiam a eles, em vez da maioria. Graças a este fenómeno, as superpotências mundiais, como os Estados Unidos, ganham uma vantagem competitiva. Podem imprimir dinheiro sem fim, para financiar os seus planos, incluindo guerras. Esta capacidade permite que estas nações dominantes controlem, influenciem e se envolvam em conflitos geopolíticos, o que cria um desequilíbrio de poder global. As guerras e as principais iniciativas para controlar os outros tornam-se financeiramente viáveis para as superpotências, enquanto outros sem a mesma flexibilidade financeira enfrentam limitações.

No sistema fiduciário, a riqueza não é distribuída uniformemente. Pelo contrário, tende a concentrar-se nas mãos de pequenos grupos. Este fenómeno é como jogar um jogo de Monopólio, onde alguns jogadores possuem quase todos os hotéis e propriedades, enquanto a maioria luta para sobreviver. O sistema fiduciário tornou-se uma ferramenta usada por certos grupos para acumular riqueza. A impressão de dinheiro permite que os governos, em estreita colaboração com os bancos centrais, injetem mais dinheiro na economia, e os destinatários deste dinheiro novo são aqueles que já têm uma riqueza e estatuto privilegiados – entidades e indivíduos poderosos. Estes grupos beneficiam do dinheiro novo antes de o seu impacto negativo (como a redução do poder de compra) se começar a manifestar na economia.

A criação de soluções, com base nos problemas

A desigualdade na distribuição da riqueza não se trata apenas do que se tem ou não tem; trata-se de uma supressão da mobilidade económica. Quem tem origens menos privilegiadas tem cada vez mais dificuldade em melhorar o seu estatuto económico. É como entrar numa corrida com uma mochila pesada às costas. Com políticas que só favorecem e enriquecem as elites, o crescente fosso entre os ricos e os pobres causa problemas a todos. Isto dificulta a vida ao cidadão comum, o que resulta em agitação social, falta de confiança nas instituições e no desmoronamento de comunidades, como se fossem castelos de cartas. A instabilidade do sistema fiduciário manifesta-se na incerteza económica, agitação política e repercussões globais, à medida que o mundo ocidental enfrenta uma crise económica.

Isto é um fenómeno global, que afeta tanto as sociedades em nações desenvolvidas como as dos países em desenvolvimento. Os ricos, que geralmente operam a uma escala transnacional, usam o sistema financeiro global a seu favor, o que alarga ainda mais o fosso entre as classes alta e baixa.

No sistema fiduciário, contrair dívida tornou-se uma norma para a humanidade. Os governos, instituições, empresas e indivíduos de todo o mundo encontram-se imersos num mar de dívida.



A mudança de mentalidade que tornou a dívida aceitável deriva da forma como o sistema fiduciário foi concebido. Ao longo das últimas décadas as entidades têm conseguido contrair dívidas substanciais de forma cada vez mais fácil. Quanto ao cidadão comum, a dívida é, muitas vezes, uma questão de necessidade, face ao aumento dos preços e do custo de vida.

O consumismo – constante impulso para comprar e consumir – leva as pessoas a comprar mais do que precisam, o que causa um consumo excessivo e desperdício. Até pode parecer que as compras nunca acabam, mas o custo real vai para além do preço e afeta a saúde mental e o bem-estar das pessoas.

Torna-se evidente que o sistema fiduciário não é apenas um mecanismo económico. É também um sistema capaz de transformar toda a sociedade humana. Entre a concentração de poder, a dinâmica global, desigualdades na distribuição da riqueza e normas sociais, o sistema fiduciário influencia diretamente a forma como as nações operam e a vida do cidadão comum.

Atividade: Consequências do Sistema Fiduciário

- 1.** Existem outras consequências para os indivíduos e sociedade em geral, resultantes do sistema fiduciário?
- 2.** Quais são as consequências do sistema fiduciário no teu país? O que aconteceu ao longo da História, e como é que esses acontecimentos afetaram as pessoas do teu país?
 - a.** Exemplos pessoais – sessão interativa

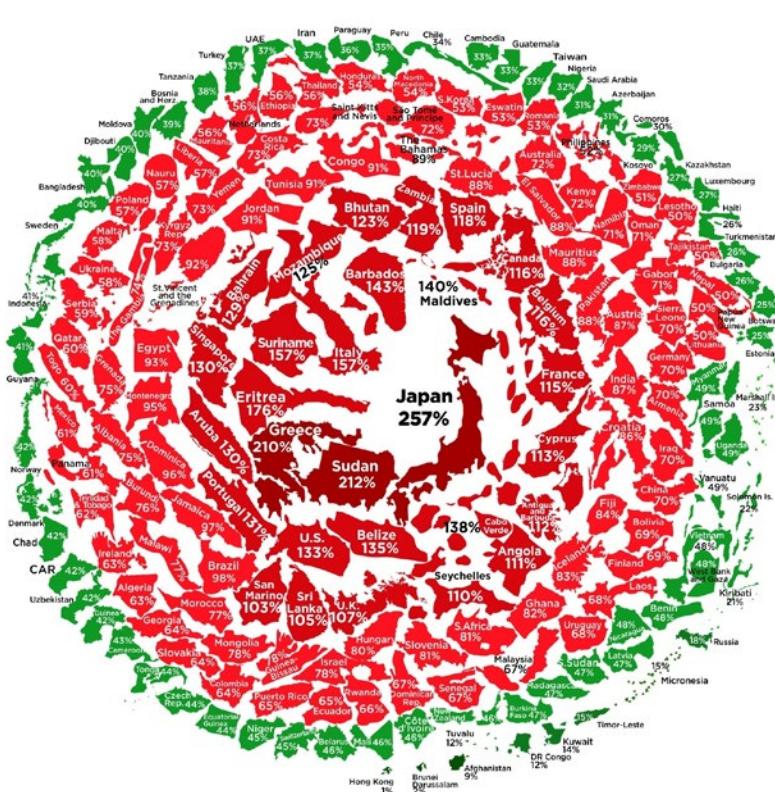
5.2.3 O peso da dívida global

Como resultado do sistema fiduciário, os governos do mundo inteiro encontram-se encurralados numa enorme teia de dívida, presos naquilo a que se chama uma espiral de dívida global. Imagina uma situação em que pedes mais dinheiro emprestado do que alguma vez conseguirás pagar. Isto está a acontecer em grande escala, no mundo inteiro. As enormes dívidas acumuladas pelos governos já ultrapassam qualquer valor que os mesmos seriam capazes de pagar. É uma história de gastos e empréstimos imprudentes e falta de previdência, que está a arrastar as nações de todo o mundo para o desastre financeiro.



Até hoje, o governo federal dos EUA já aumentou a sua dívida em 10 mil milhões de dólares, desde 2019. A dívida total aumentou de cerca de 23 mil milhões de dólares, no quarto trimestre de 2019, para um astronómico valor atual de 34 mil milhões de dólares. O ritmo a que os governos a nível global produzem novas dívidas não está a abrandar. Pelo contrário, está até a acelerar. Prevê-se que o ano de 2023 seja o ano em que se acumulou mais dívida, desde o turbulento ano de 2021, marcado pela Pandemia do Covid.

A situação da Dívida Pública Mundial



Então, o que é que isto significa para os indivíduos e sociedades que já se veem obrigados a lidar com as consequências do sistema fiduciário? A espiral da dívida em que estão envolvidos é como uma bola de neve a descer colina abaixo – fica cada vez maior, e não se sabe ao certo como pará-la.

As consequências já mencionadas, desde a desigualdade na distribuição da riqueza à agitação social, não vão desaparecer. Pelo contrário, o peso da dívida global atingiu um ponto irreversível, o que nos dá a certeza de que a situação só vai piorar.

Rácio Dívida/PIB 2021 (%)



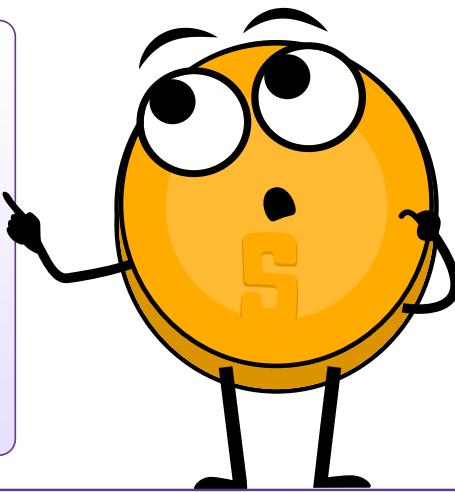
A criação de soluções, com base nos problemas



Não acredito que alguma vez voltemos a ter uma boa moeda, enquanto não a tirarmos das mãos do governo. (...) A única opção que temos é, de uma forma manhosa e indireta, introduzir algo que eles não consigam impedir.

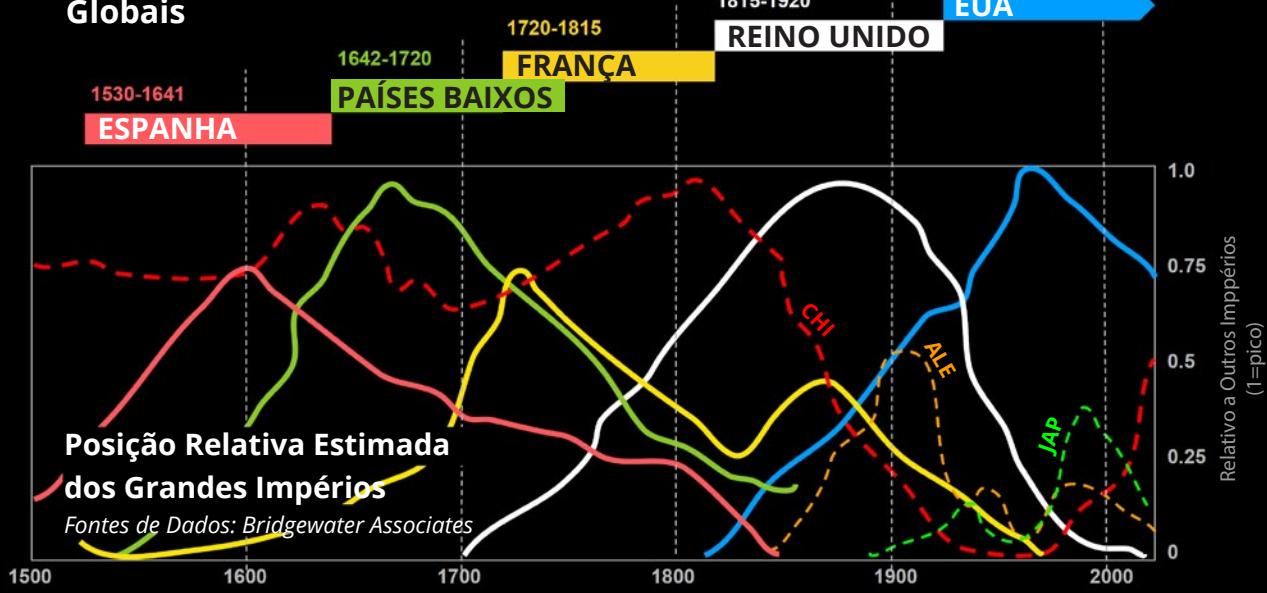
Friedrich Hayek

Vencedor do Prémio Nobel de Economia



@anilsaidso

Moedas de Reserva Globais



5.3 Os Cypherpunks e a procura de uma moeda descentralizada

Ao longo da História, observámos uma apreensão progressiva de dinheiro por parte dos bancos e governos, que deu origem ao sistema fiduciário que conhecemos hoje e às suas desastrosas consequências para a sociedade. Mas a ascensão das novas tecnologias, como a criptografia e a internet, permitiu o aparecimento de novas ideias, como é o caso do dinheiro digital independente, livre da intervenção governamental, aberto e acessível a todos. Vamos analisar o trajeto de quem liderou este movimento revolucionário: os Cypherpunks.

5.3.1 Os Cypherpunks



O computador pode ser usado como uma ferramenta para libertar e proteger as pessoas, em vez de as controlar.

Hal Finney



Na segunda metade do século XX, surgiram vários avanços tecnológicos, como o computador e a internet, que abriram caminho para uma nova era digital.

Houve um grupo de pessoas que percebeu que estas enormes inovações iriam, em breve, transformar o funcionamento da sociedade. Eles previram ambos o potencial e o perigo dos computadores pessoais, como ferramentas libertadoras para capacitar o povo, mas também como ferramentas de controlo absoluto e vigilância.

Este grupo chamava-se Cypherpunks. Emergiu como um grupo de ativistas, criptógrafos, programadores e ativistas pela privacidade, que tinham um objetivo comum: uma forma de obter privacidade, segurança e um futuro digital descentralizado. O termo Cypherpunk deriva das palavras cypher (cifra), que se refere ao código criptográfico, e punk, que representa o ethos alternativo da rebelião.

Os Cypherpunks acreditavam na capacidade da criptografia de proteger as liberdades individuais. Os seus objetivos incluíam desenvolver ferramentas para proteger as comunicações online, anonimizar atividades na internet e estabelecer moedas digitais que operassem fora do controlo das autoridades centralizadas.

Os Cypherpunks entenderam as consequências do sistema fiduciário e viram a ameaça de um “futuro orwelliano”. Eles acreditavam que era necessário garantir que o computador pessoal e a internet teriam um impacto positivo na humanidade, em vez de servirem de ferramentas para exacerbar o controlo do Estado sobre o povo.



A DEFINIÇÃO DE UM FUTURO ORWELLIANO:

Um futuro orwelliano refere-se a uma visão distópica inspirada nos trabalhos de George Orwell. O termo está associado a uma sociedade totalitária e aterradora, caracterizada por um controlo governamental opressivo, vigilância excessiva, propaganda e manipulação de informações. O termo “orwelliano” descreve, muitas vezes, um cenário em que as liberdades dos cidadãos e a autonomia individual sofrem restrições rígidas, a dissidência é suprimida e a realidade é distorcida, para servir os interesses de um regime poderoso e autoritário. O nome deste conceito deriva do nome do autor George Orwell, que, nas suas obras, avisou-nos contra os potenciais perigos de um poder governamental descontrolado e da eliminação gradual dos direitos humanos fundamentais.

A criação de soluções, com base nos problemas

Os principais intervenientes do movimento Cypherpunk incluíram luminares como Eric Hughes, Timothy C. May e John Gilmore. Em 1992, Eric Hughes escreveu "A Cypherpunk Manifesto", delineando os princípios do grupo. Este manifesto destacou a importância da privacidade, da encriptação e da necessidade dos indivíduos de assumir o controlo das suas identidades digitais.



**Assiste a este
vídeo e descobre a
história dos
Cypherpunks!**

Uma das invenções mais notáveis dos Cypherpunks foi a criação de ferramentas e protocolos criptográficos. Em 1991, Phil Zimmermann apresentou a PGP (Pretty Good Privacy), um software de encriptação de e-mails que se tornou um projeto de referência. O PGP permitiu aos utilizadores enviar mensagens encriptadas na internet, impossibilitando a desencriptação, exceto pelo destinatário pretendido. Antes disso, qualquer mensagem enviada pela internet podia ser intercetada e lida por outras entidades, tais como os governos.

Os Cypherpunks acreditavam que o avanço da criptografia, juntamente com a internet e o computador, estabelecia uma base forte para a criação de redes descentralizadas no espaço digital, que permitiriam aos indivíduos comunicar e realizar transações na internet com privacidade e sem a interferência de uma autoridade central.

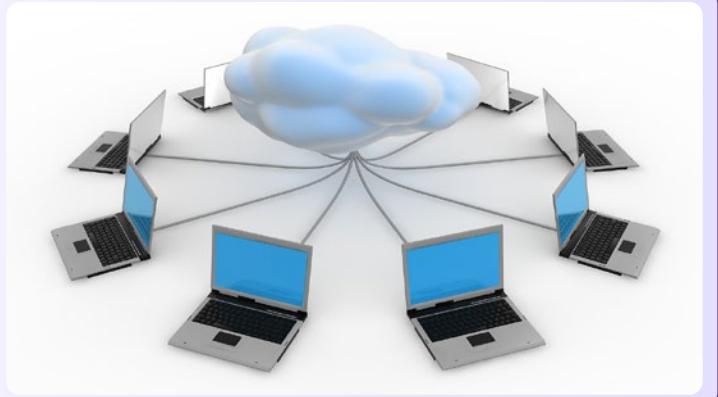
Os Cypherpunks estavam no caminho certo para promover um melhor futuro para a humanidade, onde a tecnologia seria uma ferramenta para maximizar a liberdade e não para controlar. A única peça que faltava era uma rede descentralizada e uma moeda digital descentralizada.

5.3.2 Sistemas centralizados e descentralizados

Sistemas centralizados: Um governante, vários problemas

Num sistema centralizado, tudo gira em torno de uma autoridade principal, como um edifício alto numa cidade. Essa autoridade controla o funcionamento do sistema inteiro. Pensa no exemplo dos bancos tradicionais, onde um pequeno grupo toma todas as decisões.

Exemplo verídico: Em 2022, durante manifestações pacíficas no Canadá, os bancos congelaram as contas dos protestantes - uma demonstração do poder da autoridade central de intervir e controlar o acesso financeiro.





Capítulo #5

Desvantagens dos sistemas centralizados:

- 💡 Ponto de falha central: Se ocorrer uma falha na autoridade central, o sistema inteiro pode entrar em colapso.
- 💡 Controlo: O controlo e o poder estão concentrados num pequeno grupo no topo, que toma muitas decisões que os beneficiam mais a eles do que a todos os outros.
- 💡 Ineficiência e intermediários: Tal como os engarrafamentos nas cidades, os sistemas centralizados podem tornar-se lentos e dispendiosos, devido a intermediários desnecessários.
- 💡 Falta de autonomia: As pessoas podem não conseguir fazer as suas próprias escolhas financeiras; é tudo decidido pela autoridade superior.
- 💡 Censura e restrições: Da mesma forma que se pode fechar algumas zonas de uma cidade, os sistemas centralizados podem bloquear ou limitar o acesso a determinados recursos financeiros.
- 💡 Problemas de escalabilidade: Quando há mais pessoas a precisar de serviços financeiros, os sistemas centralizados podem ter dificuldade em acompanhar a procura.
- 💡 Riscos de segurança: Quaisquer problemas com a autoridade central podem colocar o sistema inteiro em risco de ataques cibernéticos.
- 💡 Falta de transparência e de confiança: O funcionamento interno dos sistemas centralizados pode ser difícil de compreender, o que faz com que seja difícil para as pessoas confiar nos mesmos.

Sistemas descentralizados: Poder ao povo

Agora, imagina que um sistema descentralizado é como uma grande floresta. Cada árvore representa uma parte separada, e a floresta inteira representa o sistema. Ao contrário de uma cidade com um único ponto central, um sistema descentralizado é mais semelhante a uma floresta resiliente, capaz de perseverar, mesmo que uma parte do seu todo passe dificuldades.

- 💡 Exemplo verídico: A rede Tor e o respetivo navegador Tor criam um sistema descentralizado, onde as pessoas conseguem manter a sua anonimidade na internet. É também difícil parar ou censurar este sistema.



Benefícios dos sistemas descentralizados:

- 💡 Maior resiliência e fiabilidade: Não existe um único ponto de falha, o que torna o sistema forte, mesmo que existam alguns problemas.
- 💡 Maior segurança: Com o nível certo de encriptação/proteção, um sistema descentralizado resiste melhor ao controlo por parte de uma única autoridade.

A criação de soluções, com base nos problemas

- ◆ Maior soberania: As pessoas têm mais controlo sobre o seu dinheiro, dados e decisões.
- ◆ Maior transparéncia: Todos veem as mesmas informações, o que torna o sistema mais fidedigno.
- ◆ Natureza livre e ilimitada: Qualquer pessoa pode aderir e participar no sistema, o que o torna inclusivo.
- ◆ Igualdade de oportunidades: Toda a gente tem as mesmas oportunidades de contribuir e de ter uma opinião.
- ◆ Maior privacidade: As informações são distribuídas por vários participantes, maioritariamente sob pseudónimos, o que torna os sistemas descentralizados mais privados.

Embora os sistemas descentralizados tenham muitas vantagens, a tomada de decisões em conjunto pode não ser um processo fácil - requer que todos trabalhem em conjunto.

Alterar a forma como se exerce o poder

A principal diferença entre os sistemas centralizados e descentralizados reside em quem detém o poder. Os sistemas centralizados dão poder a um pequeno grupo de indivíduos, enquanto os sistemas descentralizados dispersam o poder, para permitir que todos contribuam para as decisões. Esta mudança na distribuição do poder daria origem a um futuro financeiro mais justo e democrático, onde um grande número de pessoas influencia o sistema que molda as suas vidas.

5.3.3 História resumida das moedas digitais

Um dos conceitos mais importantes abordados pelos Cypherpunks é o dinheiro digital. Os Cypherpunks aperceberam-se de que tinha de haver uma separação entre o Estado e o dinheiro, para garantir que o futuro beneficiaria o bem comum. O trabalho inovador de David Chaum estabeleceu uma boa base, com protocolos criptográficos para transações seguras e privadas. A desvantagem deste protocolo é que exigia uma autoridade central para funcionar de forma eficiente, o que suscitou preocupações, por haver um único ponto de falha e a possibilidade de censura.

Nos anos que se seguiram, vários Cypherpunks tentaram iterar as ideias uns dos outros, com o objetivo de criar uma solução viável para uma moeda digital livre do controlo governamental. A tabela abaixo inclui várias inovações importantes que os Cypherpunks desenvolveram, na tentativa de criar uma moeda digital:

Nome e Data	Descrição	Limitações
E-Cash (1982)	O E-Cash de David Chaum foi um conceito inicial de dinheiro eletrónico, com um grande foco na privacidade, por meio de técnicas criptográficas.	Exigia uma autoridade central, o que suscitou preocupações, por haver um único ponto de falha e a possibilidade de censura.
DigiCash (1990)	O DigiCash, fundado por David Chaum, tinha o objetivo de criar uma forma digital de moeda e priorizar a sua privacidade.	O facto de ser um modelo centralizado contribuiu para a sua eventual falência em 1998.



Capítulo #5

B-Money (1996)	O B-Money, proposto por Wei Dai, foi uma proposta teórica para um sistema financeiro eletrónico, anónimo e distribuído.	Nunca foi implementado, pelo que permaneceu uma ideia conceitual.
HashCash (1998)	O HashCash, desenvolvido por Adam Back, era um sistema de proof-of-work, concebido para limitar e-mails não solicitados e ataques de negação de serviço.	Não abordou diretamente o problema dos gastos duplos associado às moedas digitais.
Bit Gold (1998)	O Bit Gold, proposto por Nick Szabo, descrevia um sistema de moeda digital descentralizado, com elementos de proof-of-work.	Nunca foi implementado, pelo que permaneceu um conceito teórico.
e-Gold (2004)	O e-Gold era uma moeda digital centralizada com correspondência ao ouro físico, que permitia aos utilizadores comprar e transferir unidades e-Gold.	Surgiram questões jurídicas, que conduziram ao seu encerramento em 2009, o que destacou os problemas associados às moedas digitais centralizadas.

Apesar das inúmeras tentativas dos Cypherpunks, ao longo de décadas, de criar uma moeda digital livre do controlo de qualquer grupo ou governo, os seus projetos enfrentaram problemas práticos e não puderam ser concretizados no mundo real. Os Cypherpunks concluíram que não era assim tão fácil construir uma forma digital de dinheiro segura, escalável e com o potencial de ser amplamente adotada.

Mas tudo mudou, quando um indivíduo, após aprender com os erros dos Cypherpunks, elevou o conceito de uma moeda digital descentralizada para novos patamares. Nos capítulos seguintes, vamos descobrir de que forma a contribuição desta pessoa, com o culminar de 40 anos de trabalho, permitiu a criação de um sistema funcional.

Capítulo #6

Uma introdução ao Bitcoin

6.0 Satoshi Nakamoto e a criação do Bitcoin

6.1 Como funciona o Bitcoin?

6.1.1 O mecanismo de consenso Nakamoto

6.1.2 Os intervenientes

Atividade - Obtenção de consenso numa rede ponto a ponto

6.2 O bitcoin como moeda digital forte

6.2.1 Introdução

6.2.2 Características do bitcoin

Atividade - Debate de turma - Será o bitcoin uma moeda forte?

6.2.3 Adoção da responsabilidade pessoal

Manual do Aluno

Versão Portuguesa | 2025

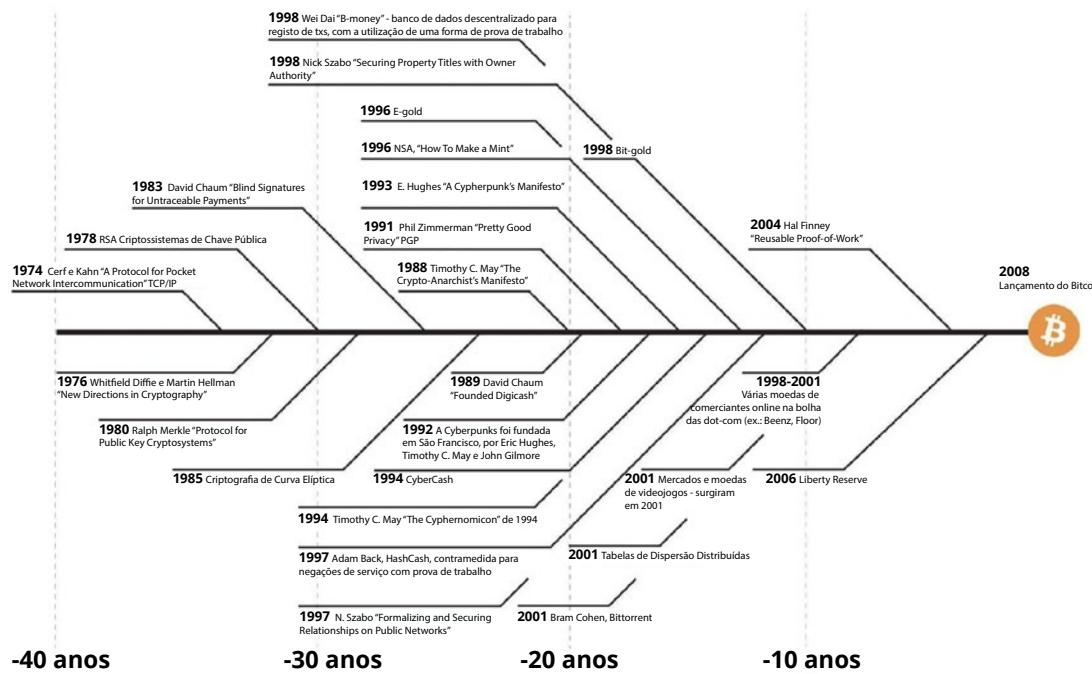
Uma introdução ao Bitcoin

6.0 Satoshi Nakamoto e a criação do Bitcoin

Muitas pessoas assumem, à partida, que as moedas eletrónicas são uma causa perdida, graças a todas as empresas que não conseguiram concretizá-las, desde a década de 1990. Espero que fique claro que esses sistemas só falharam devido à sua natureza de controlo centralizado. Acho que esta é a primeira vez que experimentamos um sistema descentralizado que não depende da confiança.

Satoshi Nakamoto

Pré-história do Bitcoin - É o resultado de 40 anos de investigação, desenvolvimento e procura



Como leste no capítulo anterior, houve vários Cypherpunks que tentaram criar um sistema monetário alternativo. Este capítulo continua a história de um deles: uma mente visionária com o nome Satoshi Nakamoto. Já muito antes do Bitcoin, esta entidade (homem, mulher ou grupo) anónima pertencia a grupos de entusiastas da criptografia, onde estavam incluídos especialistas e piratas informáticos, e participava em debates para encontrar soluções práticas que substituíssem o sistema fiduciário.

Page: [1] [« previous topic](#) [next topic »](#) [print](#)

Author: satoshi (OP)
Topic: Added some DoS limits, removed safe mode (0.3.19). (Read 25115 times)

Dec 12, 2010, 06:22:33 PM
Merged by ETS (#100), fillipone (#5), OlegNikonov (#4), hamilton (#3), iwave (#2), krogoth (@mention) (#47), suanq (#1), vymazal (#1), yzj (#1), zzz (#1), zzzzz (#2), Welsh (#2), minaract (#20), AdiCach (#1), dragonmantis (#11), legendster (#1), logjammin (#1), a7r (#2), Belerwyr (#5), MrPumpkin (#5), Lauda (#5), MicroGuy (#5), TMXH (#5), Steeler (#5), minorman (#5), Sjyre (#4), Danilje (#3), Jmistedx (#3), Ayu_Art (#3), Yaunfida (#2), Bithd (#2), cosperBG (#2), jay (#2), jay (#2), edgycore (#2), Syke (#1), Zeta (#1), Bitcoin (#1), rando (#1), b001 (#1), b002 (#1), Semper (#1), HIT-FC9 (#1), p001 (#1), p002 (#1), p003 (#1), p004 (#1), p005 (#1), p006 (#1), p007 (#1), famosoMuerto (#1), crypto_trader #43xDoP (#1), bill_gator (#1), denekilm (#1), DaCryptoRaccoon (#1), b001 (#1), alberto (#1), danielman (#1), Wallaby (#1), imlives (#1), Scarecrow (#1), RoosterFest (#1), p008 (#1), dark08 (#1), lesson (#1), tyce (#1), Coaklow (#1), mikey_beaver (#1), p009 (#1), p010 (#1), p011 (#1), p012 (#1), Dog (#1), TheTechnologist (#1), ritacoscience (#1), mrrympoint (#1), oktopug (#1), sigr4d (#1), OW21337 (#1), liveness (#1), zarne (#1), TechIt (#1), Ed4Q (#1)

Activity: 364
Merk: 6671

Ignore

There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this version 0.3.19.

- Added some DoS controls
As Gavin and I have said clearly before, the software is not at all resistant to DoS attack. This is one improvement, but there are still more ways to attack than I can count.

I'm leaving the -lmtfreerelay part as a switch for now and it's there if you need it.

- Removed "safe mode" alerts
"safe mode" was a temporary measure after the 0.3 overflow bug. We can say all we want that users can just run with "disablesafemode", but it's better just not to have it for the sake of appearances. It was never intended as a long term feature. Safe mode can still be triggered by seeing a longer (greater total POW) invalid block chain.

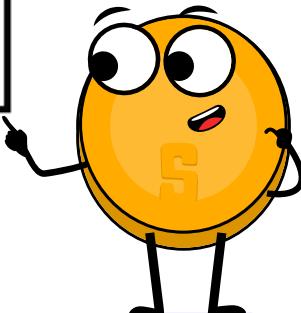
Builds:
<http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/>

Capítulo #6

Em outubro de 2008, Nakamoto revelou um *whitepaper* (documento que apresenta informações detalhadas sobre um projeto, produto ou tecnologia, geralmente explicando sua finalidade, funcionamento e benefícios) inovador com o título Bitcoin: Um Sistema de Dinheiro Eletrônico Ponto a Ponto, numa lista de correspondência relacionada com criptografia. Este documento estabeleceu as bases para um protocolo descentralizado ponto a ponto (peer-to-peer), concebido para facilitar transações online seguras, sem a necessidade de intermediários.

A visão de Nakamoto era óbvia: criar uma versão de dinheiro eletrônico completamente ponto a ponto, livre do controlo de governos e instituições financeiras poderosas.

No dia 3 de janeiro de 2009, Nakamoto minerou o primeiro bloco do Bitcoin, conhecido como Bloco Génesis (Genesis Block). Isto marcou o lançamento oficial da rede Bitcoin, um novo sistema monetário baseado na confiança e segurança oferecidas por um livro-razão (ledger) descentralizado. Nos meses e anos que se seguiram, cada vez mais entusiastas começaram a aderir à rede e a contribuir para o seu conceito.



Bloco Génesis do Bitcoin

Versão Hexadecimal Não Formatada

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3B .....;Íýz(.zç,>  
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.ß.À.ÙQ2;Ù.à  
00000040 4B 1B 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)*_Íyy...~+|  
00000050 01 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 .....  
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....yyyyM.yy..  
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/  
00000090 4A 61 6B 2F 32 30 30 39 20 43 68 61 6B 63 65 6C Jan/2009 Chancel  
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of  
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f  
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksyjjy.ò.  
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....Ca.gß'þpuH'  
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gn|q0..Vð~(ð9.|  
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybåðe.apø1ø?Løøñ  
00000100 F3 55 04 E5 1B C1 12 DB 5C 3B 4D F7 BA OB BD 57 ðU.å.ð\ØMøø..W  
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ_~.
```

Em 2011, após comprovar que a rede Bitcoin conseguia funcionar perfeitamente sem a necessidade do seu influente criador, Nakamoto enviou um e-mail a um colega programador de Bitcoin a anunciar que iria deixar de estar envolvido no projeto Bitcoin e que iria deixar o futuro do mesmo nas *boas mãos* que partilhavam a sua visão.

Embora a identidade de Nakamoto continue a ser um mistério até hoje, o objetivo que tinha ao criar o Bitcoin nunca foi um mistério. Essencialmente, Nakamoto criou o Bitcoin para retirar o poder das elites e devolvê-lo à maioria, ao criar uma solução alternativa, na forma de um sistema monetário descentralizado, de código aberto e transparente, que estabelece uma separação entre o dinheiro e o Estado. A criação do Bitcoin foi a resposta de Nakamoto à crise financeira de 2008, que prejudicou pessoas trabalhadoras no mundo inteiro, enquanto a elite continuava a enriquecer. O Bitcoin foi a resposta de Nakamoto à corrupção e fragilidade do sistema fiduciário. Nakamoto estabeleceu a base para uma nova revolução e afastou-se da mesma, em vez de reclamar os louros.

Uma introdução ao Bitcoin

Nos anos que se seguiram, o Bitcoin começou a crescer rapidamente e tornou-se um símbolo de esperança, capacitação e resiliência, por desafiar o sistema fiduciário e por oferecer uma forma de fazer transações financeiras que é segura e resistente à censura. O Bitcoin é um protocolo de código aberto, o que significa que ninguém tem o poder de o possuir ou controlar. Tem um design público e está aberto à participação de todos.

O sonho de Nakamoto de um sistema financeiro sem fronteiras, transparente e seguro continua em funcionamento, a dar poder à revolução global da liberdade que estamos a testemunhar hoje. Todos os dias, há pessoas como nós a abandonar o sistema fiduciário e a aderir ao mundo do Bitcoin. Os centros Bitcoin – as chamadas economias circulares do Bitcoin – foram lançados por defensores da liberdade em várias regiões do mundo. Até mesmo países inteiros, que procuram um caminho alternativo, já estão a começar a adotar o Bitcoin à sua maneira, como é o caso de El Salvador.

6.1 Como funciona o Bitcoin?

6.1.1 O mecanismo de consenso Nakamoto

Afinal, como funciona o Bitcoin? O Bitcoin tem muitas características e um funcionamento muito mais complexo do que aparenta. Felizmente, quando entras no mundo Bitcoin, não precisas de compreender todos os detalhes do seu funcionamento, para poderes começar a usá-lo.

O princípio é semelhante ao do uso da internet. A maioria das pessoas não sabe como é que o protocolo TCP/IP funciona, apesar de enviarem e-mails e mensagens e fazerem publicações nas redes sociais todos os dias. O mesmo se aplica a conduzir um carro. A maioria das pessoas não sabe exatamente como é que um carro funciona, apesar de saberem conduzir.



No entanto, o Bitcoin ainda não é amplamente adotado. Continua a ser uma tecnologia bastante recente, tal como era a internet nos anos 90. É por isso que poderá ser mais fácil compreender-se os princípios básicos do Bitcoin de uma forma simplificada e menos técnica.

Capítulo #6

O conceito fundamental por trás do funcionamento do Bitcoin pode ser resumido numa frase: O Bitcoin é um acordo online entre pessoas. Imagina que é como jogar a um jogo de tabuleiro com amigos. Quando jogamos um jogo de tabuleiro como o Monopólio, acordamos regras específicas com os outros jogadores. Uma das regras do Monopólio é que só são aceites notas especiais de Monopólio. Se o João (um dos jogadores) quebrar as regras, ao usar papel higiénico, em vez de notas de Monopólio, para comprar uma casa, os outros jogadores chamam-no batoteiro e deixam de jogar com ele. Resumindo, para jogar ao jogo, existe um consenso entre todos relativamente a um conjunto de regras. E, se quebrarmos essas regras, somos rejeitados.

É fácil perceber que o Bitcoin funciona da mesma forma. O Bitcoin é uma rede de pessoas que concordam com o mesmo conjunto de regras. Essas regras estão matematicamente vinculadas, escritas em código informático, e são aceites diretamente por todas as pessoas que utilizam o software Bitcoin. As regras do Bitcoin aplicam-se igualmente a todos os participantes, o que significa que todos seguem as regras do jogo. Caso contrário, não conseguem jogar, pois são rejeitados pela rede.

Por exemplo, uma das regras é: "Nunca haverá mais de 21 milhões de bitcoins". Se alguém quisesse criar 1 milhão de bitcoins novos para uso próprio, seria inútil, pois os bitcoins seriam automaticamente identificados e rejeitados por todos os outros. É isto que torna o Bitcoin tão robusto.

Não importa quem tu és ou de onde vens, se entreas no mundo do Bitcoin, precisas de seguir as mesmas regras que todos os outros.

Isto também se aplica a todas as pessoas e entidades que têm uma enorme influência e controlo no mundo fiduciário. No mundo Bitcoin, não há batotices, nem sabotagens. Toda a gente é tratada da mesma forma, e ninguém consegue mudar isso.

Sabias que, desde 2009, o Bitcoin resistiu a dezenas de milhares de tentativas de pirataria, sabotagem e alteração? O Bitcoin provou que não pode ser parado, controlado nem manipulado.



Uma introdução ao Bitcoin

6.1.2 Os intervenientes

Para entender melhor a descentralização do Bitcoin, precisamos de compreender muito bem as diferentes funções na rede. No mundo Bitcoin, há vários participantes com funções distintas e harmoniosas, que contribuem para um funcionamento perfeito da rede.

1. Mineradores: Os arquitetos da segurança

Os mineradores são o pilar do Bitcoin. São pessoas ou grupos de pessoas que trabalham nos bastidores, para gerir e proteger a rede, através de um mecanismo chamado *Proof-of-Work* (PoW; Prova de Trabalho). Estes intervenientes têm computadores especiais com uma elevada capacidade de computação. Disponibilizam o seu hardware à rede Bitcoin, para competir uns com os outros na procura de números criptográficos complexos, para verificar transações e adicionar novos blocos de informações transacionais ao livro-razão descentralizado do Bitcoin (a qual a que chamamos blockchain). A sua dedicação garante a imutabilidade do livro-razão e protege o mesmo de ataques maliciosos.



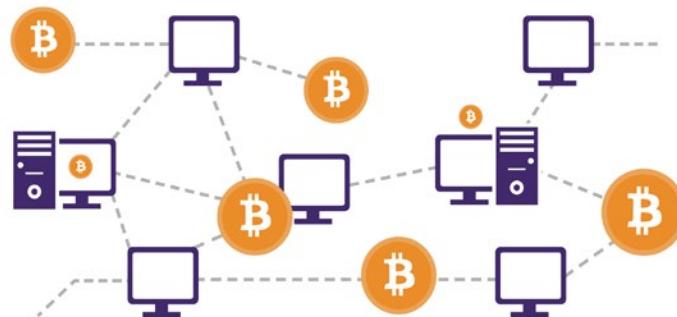
A natureza descentralizada da mineração permite a participação de qualquer pessoa com recursos computacionais suficientes. Como recompensa pelo seu trabalho árduo, os primeiros mineradores a resolver o quebra-cabeças recebem bitcoin.

Os mineradores do Bitcoin estão distribuídos pelo mundo inteiro, para proteger a rede contra a centralização e garantir que a segurança do Bitcoin permanece forte e distribuída.

2. Nós: Guardiões da validação

Os nós do Bitcoin são pessoas normais de qualquer canto do mundo. Estes participantes são os guardiões da rede Bitcoin, que utilizam o software Bitcoin nos seus pequenos computadores, nos quais mantêm uma cópia integral do livro-razão. Os nós validam as transações e garantem que todos os participantes cumprem as regras de consenso.

Ao distribuir a responsabilidade da validação por uma rede de nós, o Bitcoin permanece resistente a ataques e mantém a sua natureza independente da confiança entre as partes. Os nós desempenham um papel essencial na defesa da integridade do livro-razão, o que contribui para o etos de descentralização do Bitcoin.





Capítulo #6

3. Utilizadores: Participantes com poder

Os utilizadores, a alma da rede Bitcoin, são indivíduos que efetuam transações. Os utilizadores são mera pessoas normais a viver as suas vidas, mas que também se estão a capacitar, ao aderir ao Bitcoin. Por exemplo, alguns utilizadores guardam as suas poupanças em bitcoin. Outros, como os cidadãos de El Salvador, usam o bitcoin como dinheiro para comprar mercadorias e recebem o seu salário em bitcoin.

O Bitcoin dá poder aos utilizadores, ao eliminar a necessidade de intermediários como bancos e governos, permitindo transações diretas ponto a ponto. Isto também significa que os utilizadores têm um controlo absoluto do seu dinheiro, o que lhes dá controlo sobre os seus fundos e transações.

4. Programadores e Projetos: Arquitetos da inovação

O sistema monetário do futuro não se constrói sozinho e requer trabalho para obter uma adoção global de uma forma éticamente correta. É aqui que entram os programadores e projetos do Bitcoin.

Os programadores usam a sua especialização técnica para melhorar e inovar o protocolo Bitcoin. Estes indivíduos contribuem com código informático, propõem melhorias e corrigem vulnerabilidades, para garantir que a rede evolui em resposta a todo o tipo de desafios. A natureza de acesso livre e gratuito (código aberto) do Bitcoin convida à colaboração, ao permitir que programadores de todo o mundo contribuam para o seu crescimento.

O que este desenvolvimento descentralizado tem de melhor é que impede que uma única entidade monopolize o controlo do protocolo. Isto deve-se a um processo baseado no consenso. Os programadores propõem ideias e alterações, e só quem tiver as melhores ideias (que correspondam à visão mais alargada de um mundo melhor) é que obtém o apoio da comunidade. Isto permite uma evolução transparente e democrática do Bitcoin, até que o mesmo esteja pronto para 8 mil milhões de pessoas.

Os projetos Bitcoin envolvem diversos grupos, incluindo organizações sem fins lucrativos com objetivos específicos, bem como empresas, grupos e indivíduos que criam conteúdo de qualidade, entre outros. São pessoas que colaboram umas com as outras em projetos específicos, ou que se focam no objetivo principal do Bitcoin de alcançar a liberdade coletiva.

Os projetos Bitcoin desempenham um papel crucial na formação e promoção da adoção do Bitcoin, ao contribuir para um futuro que prioriza a capacitação e a liberdade da humanidade.

A sinfonia

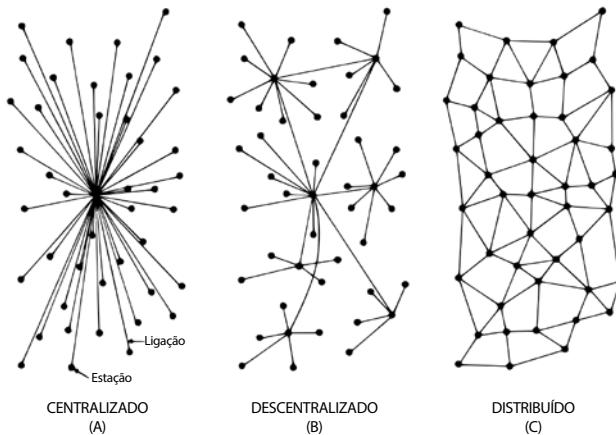
Podemos comparar a descentralização do Bitcoin a uma orquestra musical sinergética, uma demonstração de harmonia onde todos os músicos, cada um com o seu instrumento, compõem uma bela sinfonia em conjunto. A rede Bitcoin não tem líder. Em vez disso, os mineradores, nós, utilizadores, programadores e projetos desempenham as suas funções com autonomia e colaboração.

O livro-razão descentralizado, gerido pelos nós, assegura a transparência, enquanto o mecanismo de Proof-of-Work aumenta a segurança e impede a centralização da mineração. Os utilizadores usufruem de soberania e poder financeiro, livre do controlo do sistema fiduciário. Os programadores, com base no consenso, garantem que o protocolo se adapta à evolução das necessidades da humanidade. Os projetos Bitcoin contribuem, à sua maneira, para a missão principal de obter liberdade coletiva.

Uma introdução ao Bitcoin

Como podes ver, todos os participantes desempenham uma função indispensável no aumento da adoção do Bitcoin e na capacitação da humanidade. Cada participante desta orquestra descentralizada contribui para a resiliência e longevidade do Bitcoin, ao criar um ecossistema sem fronteiras, capacitador e independente da confiança entre as partes.

Em resumo, a sinfonia da descentralização do Bitcoin é um testemunho da visão de Satoshi Nakamoto e da imensa paixão de uma comunidade global em busca de liberdade e capacitação.



Atividade de turma – Obtenção de consenso numa rede ponto a ponto

Objetivo



Entender como se pode alcançar o consenso num grupo, aprender criptografia e conhecer o intrínseco mecanismo de consenso do Bitcoin.

Materiais



Mensagem com instruções encriptadas e não encriptadas (“atacar” ou “não atacar”).

Preparação da atividade



O professor vai escolher um grupo de 3 ou 4 alunos antes da aula, para representarem nós maliciosos na atividade que se segue. O professor vai atribuir a estes nós maliciosos um quebra-cabeças criptográfico na aula anterior, como trabalho de casa.



Capítulo #6

Instruções do exercício:

1 O professor vai selecionar um *iniciador*, que receberá um papel com a mensagem "ATACAR" e a sequência de números "14-1-15-1-20-1-3-1-18".

2 Os alunos devem formar uma roda no espaço designado para esse fim, de forma a garantir que os nós maliciosos ficam separados, para aumentar a eficácia da atividade.



3 Quando se tiver formado uma roda, o *iniciador* deve passar o papel à pessoa que está à sua direita.

4 Após a mensagem ter sido lida por todos, quando o *iniciador* disser "agora", o grupo deverá reagir à mensagem ao mesmo tempo. Se a mensagem der indicação para "ATACAR", todos os participantes deverão dar um passo em frente.

5 Após a reação inicial, alguns alunos (quem recebeu e interpretou corretamente a mensagem encriptada) terão ficado no mesmo sítio, enquanto os outros seguiram a instrução original, o que revela uma falta de consenso.

Conclusão:

Debatam sobre o porquê de não se ter alcançado o consenso, introduzindo o conceito do Problema dos Generais Bizantinos (que ilustra os desafios de alcançar consenso em sistemas distribuídos, onde alguns participantes podem falhar ou agir de forma maliciosa), bem como a relação entre o mesmo e a necessidade de um objetivo comum. Depois, discutam a forma como o Bitcoin oferece uma solução para este problema.

Uma introdução ao Bitcoin

6.2 O bitcoin como moeda digital forte

6.2.1 Introdução

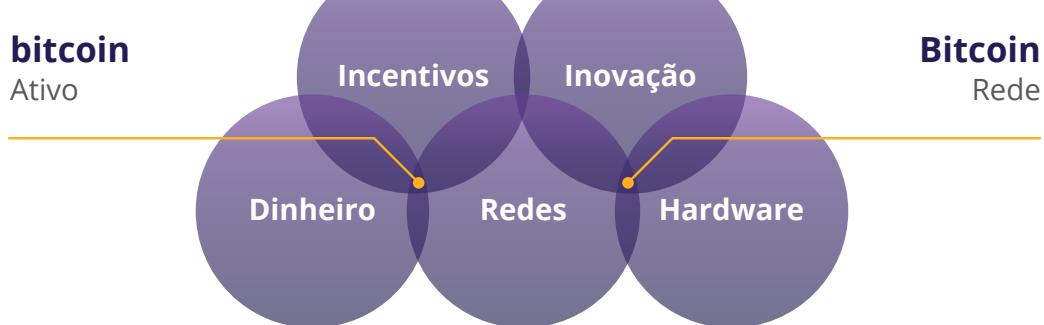
Atividade:

Vê o vídeo de minuto e meio “What is Bitcoin”



Em termos simples, o bitcoin é dinheiro. O bitcoin não é um investimento, mas sim uma forma segura e capacitadora de poupar o dinheiro que te custou a ganhar.

Ter bitcoin não significa que vais ficar rico, visto que os bitcoins não se multiplicam. Sim, o seu valor em relação às moedas fiduciárias aumenta, mas isso deve-se apenas à sua crescente adoção e à desvalorização das moedas fiduciárias.



O bitcoin é uma nova forma de dinheiro. É a “internet do dinheiro”, o que significa que o Bitcoin permite a toda a gente aderir e começar a fazer transações de valor com os outros utilizadores do Bitcoin. Até as comunidades mais isoladas e pobres do mundo têm, por fim, acesso a um sistema monetário. Tal como qualquer pessoa com um telemóvel e uma ligação à internet consegue usar um motor de busca, o Bitcoin faz com que qualquer pessoa com um telemóvel e uma ligação à internet consiga aceder a um novo sistema monetário global.



**Pagamentos
mais rápidos
e baratos**

Envia dinheiro para todo o mundo em minutos, com taxas extremamente baixas.



**Inclusão
Financeira**

2,5 mil milhões de pessoas sem acesso a banco podem ter acesso a dinheiro através de um telefone ou computador.



**Maior
Privacidade**

As transações de Bitcoin são públicas, mas a tua identidade não é.

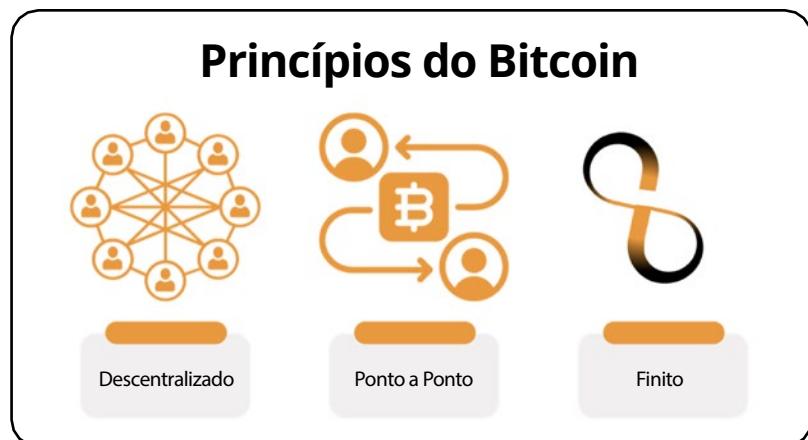


Capítulo #6

O Bitcoin é completamente digital e sem fronteiras. A localização do utilizador é irrelevante, pois o Bitcoin está presente em computadores e smartphones distribuídos pelo mundo todo. Há inúmeros utilizadores de todos os cantos do mundo que utilizam o software Bitcoin e têm uma cópia do seu livro-razão.

Este software e registo de todas as transações tem uma probabilidade muito baixa de desaparecer, uma vez que existem inúmeras cópias do mesmo. Para o encerrar, seria preciso encerrar permanentemente toda a internet, o que é extremamente improvável que aconteça.

Por fim, o Bitcoin é escasso, o que significa que a quantidade de unidades de bitcoin que podem existir é absolutamente limitada. Não é possível falsificar Bitcoin. Nem mesmo os governos e instituições financeiras mais poderosos.



6.2.2 Características do bitcoin

A evolução do dinheiro forte

Como já aprendeste no capítulo 2, uma moeda forte tem de passar por três fases no seu ciclo de vida, para obter a aceitação geral da sociedade humana: Começa por ser uma Reserva de Valor, antes de se tornar um Meio de Troca e, por fim, uma Unidade de Conta.

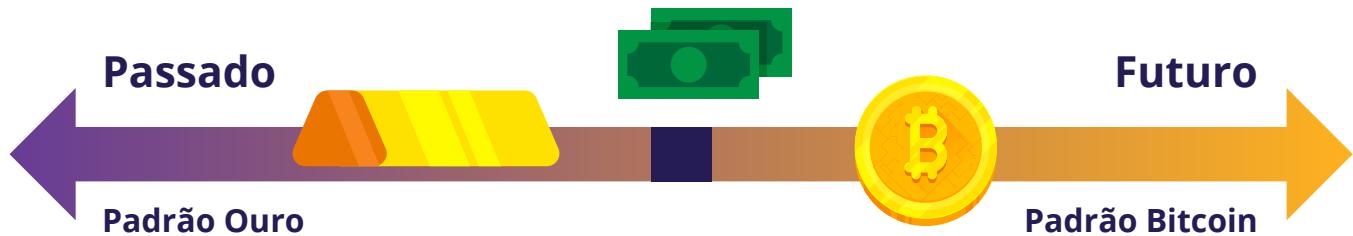
A primeira etapa do dinheiro – ser uma Reserva de Valor – é quando uma moeda começa a ganhar a confiança das pessoas como ativo estável (ou que valoriza) ao longo do tempo. Quem reconhece isto antecipadamente procura armazenar a sua riqueza nesta forma de dinheiro, por forma a protegê-la, especialmente em tempos de incerteza geopolítica e macroeconómica.

Alguns grupos, como os meios de comunicação, dizem que o Bitcoin é *ouro digital*. Isto porque o Bitcoin já se estabeleceu inequivocamente como uma reserva de valor, durante a última década. Todos os dias, cada vez mais pessoas começam a ver o bitcoin como um seguro contra a inflação, tal como foi o ouro ao longo da História.

A fase que se segue é quando se estabelece a confiança na estabilidade da moeda. É a altura em que a moeda se transforma num meio de troca, para facilitar as transações diárias das pessoas. Durante esta fase, começa a ser amplamente aceite na troca de bens e serviços.

O Bitcoin está cada vez mais a tornar-se um meio de troca. Com a crescente aceitação dos comerciantes e o desenvolvimento do protocolo, as transações Bitcoin estão a tornar-se mais eficientes e comuns no comércio diário. Um exemplo disto é El Salvador, onde o Bitcoin é oficialmente reconhecido como tendo curso legal. A cada dia que passa, cada vez mais cidadãos e empresas comuns começam a usar o Bitcoin como meio de troca.

Uma introdução ao Bitcoin



Na fase final, quando uma moeda passa a servir de medida comum para a fixação dos preços de bens e serviços, atinge o estatuto de unidade de conta. É nesta fase que se torna a unidade padrão através da qual são medidos todos os outros valores.

O processo de se tornar uma unidade de conta é mais demorado (longo prazo). Atualmente, o mundo só mede o valor de bens e serviços em moedas fiduciárias. Por isso, o Bitcoin precisa de uma adoção e integração mais generalizadas em vários sistemas financeiros. No entanto, já foi estabelecida uma base, visto que já há empresas e indivíduos que começam a aceitar e a denominar valores em Bitcoin.



Como podes ver, o Bitcoin está no caminho certo, neste ciclo evolutivo do dinheiro forte. Quando o Bitcoin se integrar por completo no sistema financeiro global, tornar-se-á uma unidade de conta padrão e mudará o sistema monetário global inteiro.



Capítulo #6

Propriedades do dinheiro

Como aprendeste no capítulo 2, a humanidade descobriu, ao longo do tempo, que um dinheiro verdadeiramente forte tem de ter determinadas propriedades para ser eficaz. Estas características são a durabilidade, a divisibilidade, a portabilidade, a aceitabilidade, a escassez e a fungibilidade.

Vamos ver se o Bitcoin passa no teste.

Durabilidade: O Bitcoin é inteiramente digital e, portanto, perfeitamente durável.

Divisibilidade: Para podermos comparar, a moeda fiduciária EUR pode ser dividida em cêntimos (0,01). O Bitcoin pode ser dividido naquilo a que chamamos de satoshis, ou sats (0,00000001). E, graças à natureza digital do Bitcoin, ainda pode ser dividido por unidades menores no futuro, se a humanidade precisar. O Bitcoin é atualmente o ativo monetário mais divisível do mundo.

Portabilidade: Em abril de 2020, foi feita uma transferência de 1,1 mil milhões de dólares num espaço de alguns minutos. E o custo da transação foi de apenas 68 cêntimos. Nenhuma outra forma de pagamento tem a capacidade, por si só, de mover tanto dinheiro, tão rápido e com um custo tão baixo. É isto que torna o Bitcoin a forma de dinheiro mais fácil de transferir do mundo.

Aceitabilidade: O Bitcoin ainda está na fase inicial de se tornar um meio de troca e, comparado com as moedas fiduciárias, a aceitabilidade do Bitcoin é atualmente baixa.

Escassez: Nunca existirão mais de 21 milhões de bitcoins. Devido ao seu código, é impossível aumentar esta quantia, o que significa que o Bitcoin não só é escasso, como também é o ativo monetário mais escasso do mundo.

Fungibilidade: Cada unidade de bitcoin é igual a qualquer outra unidade de bitcoin, e pode ser trocada e transferida no protocolo Bitcoin numa base de equivalência, o que o torna uma moeda fungível.

Uma introdução ao Bitcoin

Bitcoin, Ouro e Dólar Americano

Propriedades do dinheiro	Ouro	Moeda Fiduciária	Bitcoin
Durabilidade	Alta	Moderada	Alta
Portabilidade	Moderada	Alta	Alta
Divisibilidade	Moderada	Moderada	Alta
Fungibilidade	Alta	Alta	Alta
Escassez	Moderada	Baixa	Alta
Verificável	Moderada	Moderada	Alta
Bem Estabelecido	Alta	Moderada	Baixa
Resistente à Censura	Moderada	Moderada	Alta
Inteligente/Programável	Baixa	Moderada	Alta

"Bitcoin vs Gold vs US Dollar" Bitcoin Magazine, <https://bitcoinmagazine.com>

O Bitcoin é um tipo de dinheiro inteligente que é programável, que não pode ser confiscado e que tem todas as qualidades que o tornam excelente para poupar, bem como fácil de usar para comerciantes que querem transações rápidas.

Visto que se trata de um livro-razão digital transparente, o Bitcoin consegue ser extremamente eficiente em tarefas como a deteção de fraude e a avaliação de riscos nos seus serviços. Tem as boas características do ouro, tais como o facto de ter uma quantidade limitada, mas também tem os benefícios das moedas fiduciárias, pois pode ser facilmente dividido e transportado. Além disso, tem novas características que se adaptam bem ao nosso mundo digital.

Qual é a tua opinião? O Bitcoin ainda não é amplamente reconhecido e adotado. Mas será que é uma moeda forte?



Capítulo #6

Atividade: Debate de turma – Será o bitcoin uma moeda forte?

Agora que analisámos mais detalhadamente o bitcoin, voltemos à nossa tabela de comparação de dinheiro do Capítulo 2 e vejamos como o bitcoin se compara a outras formas de dinheiro:

Características de bom dinheiro	Vacas	Cigarros	Diamantes	Euros	Bitcoin
Durabilidade					
Portabilidade					
Fungibilidade					
Aceitabilidade					
Escassez					
Divisibilidade					
Total					

6.2.3 Adoção da responsabilidade pessoal

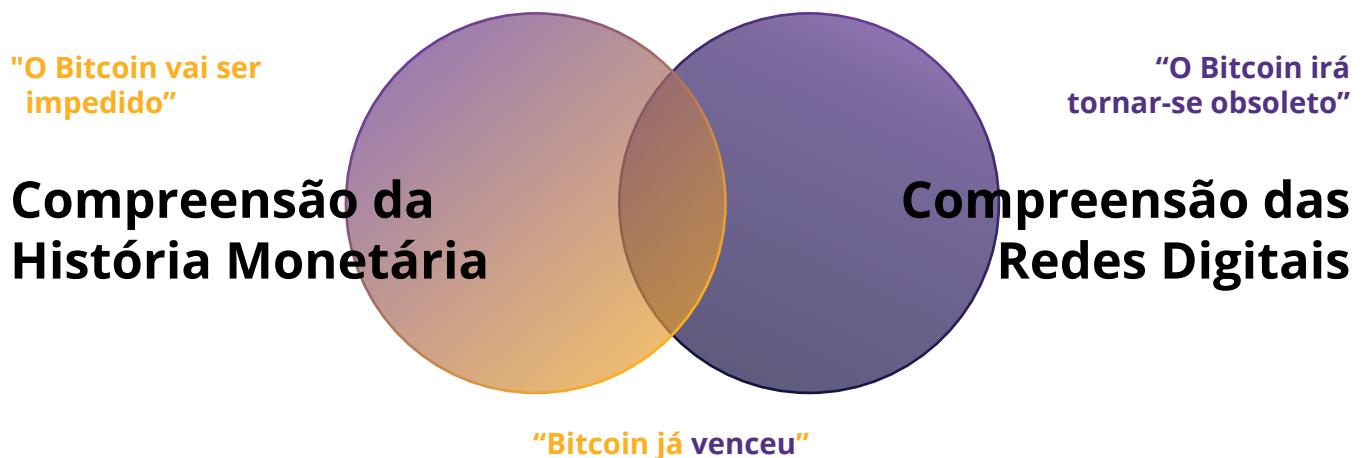
O resultado é um sistema distribuído sem um ponto de falha único. Os utilizadores detêm as chaves criptográficas do seu próprio dinheiro e fazem transações diretamente entre si, com a ajuda da rede P2P (ponto a ponto), para verificar se existem gastos duplos.

Satoshi Nakamoto

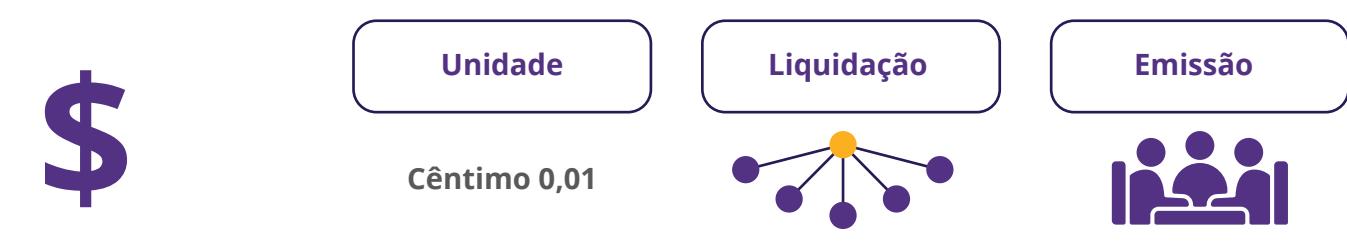
Uma introdução ao Bitcoin

No mundo fiduciário, as pessoas dependem de governos, bancos e provedores de pagamentos reconhecidos. Os diretores destas instituições (financeiras) estabelecem as regras da rede, e os participantes, maioritariamente cidadãos comuns, têm de cumprir essas regras. Independentemente de onde vives, há sempre um conjunto de procedimentos normalizados que te indicam o que fazer e como fazê-lo. Ao longo do tempo, isto originou um ciclo de dificuldades, especialmente para famílias que enfrentam cada vez mais limitações no dia a dia.

Graças a este sistema, as pessoas estão acostumadas a colocar a responsabilidade das suas finanças nas mãos dos outros. Por exemplo, a maioria das pessoas depende de outra pessoa para os ajudar, especialmente quando alguma coisa corre mal (por exemplo, se perderem o acesso à sua conta bancária).



Como sabemos, o sistema monetário do Bitcoin é muito diferente. O Bitcoin opera de uma forma específica, e os governantes foram substituídos por um sistema de regras autónomo. Não há ditadores, nem líderes, o que também significa que não há ninguém que te diga o que deves fazer. Se desejas a liberdade e o poder que o Bitcoin tem para oferecer, tens de aprender como funciona e integrar essa tecnologia da forma que for melhor para ti.





Capítulo #6

Com o Bitcoin, tens o controlo absoluto do teu dinheiro, mas este controlo adicional acarreta uma maior responsabilidade. Por exemplo, se perderes as chaves da tua carteira digital e, com isso, o acesso ao teu Bitcoin, isso significa que perdeste as tuas poupanças para sempre. Não existem linhas de apoio ao cliente ou outras pessoas que possas contactar, quando surge um problema. Tens de resolvê-lo sozinho.

Felizmente, isto não vai acontecer a quem decide assumir a inteira responsabilidade das suas próprias vidas. Usar o Bitcoin não é inherentemente complicado; é apenas um conceito novo. Por ser desconhecido, pode causar algum desconforto. Mas, se estiveres disposto a aprender a usar o Bitcoin e a assumir toda a responsabilidade de salvaguardar a tua riqueza, o Bitcoin torna-se uma ferramenta capacitadora, pois tens um controlo absoluto, e ninguém pode apreender o teu dinheiro.

Resumindo, o mais importante é agir, compreender o funcionamento do Bitcoin e implementá-lo de acordo com as tuas necessidades individuais e filosofia de vida. Em seguida, vamos começar a usar bitcoin, ao configurar uma carteira Bitcoin, ao enviar e receber as tuas primeiras transações e ao analisar as melhores práticas de segurança.

Capítulo #7

Como usar o bitcoin

7.0 Introdução

7.1 Adquirir e transferir bitcoin

7.1.1 Ponto a ponto: presencial

7.1.2 Ponto a ponto: online

7.1.3 Corretoras centralizadas

7.2 Uma introdução às carteiras Bitcoin

7.2.1 Carteiras custodiais e não-custodiais

7.2.2 Diferentes tipos de carteiras Bitcoin

7.2.3 Código aberto e código fechado

Atividade - Avaliação de turma de carteiras Bitcoin

7.3 Configurar uma carteira móvel de Bitcoin

Atividade - Configurar/recuperar uma Carteira Bitcoin

7.4 Receber e enviar transações

Atividade - Transações bitcoin em ação

7.5 Poupar em bitcoin

7.6 Não confies, verifica

Como usar o bitcoin

7.0 Introdução



Porque haveria alguém de confiar em “dinheiro de nerds”, em vez do dinheiro do banco central?
Foram “nerds” que deram origem à internet. Os bancos deram origem à Grande Depressão.

Andreas M. Antonopoulos



Agora que compreendemos melhor o que é o Bitcoin e o seu objetivo, está na altura de aprender a utilizá-lo na prática. Neste capítulo, vamos ensinar-te os passos para adquirir bitcoin, descobrir os vários tipos de carteiras disponíveis, ajudar-te a configurar a tua própria carteira Bitcoin, e vamos até praticar o envio e seguimento de uma transação Bitcoin na rede. Está na hora de colocares os teus conhecimentos em prática!

7.1 Adquirir e transferir bitcoin

Existem muitas formas de adquirir bitcoin.

Por exemplo, podes:

- 💡 Receber o teu salário em bitcoin e usá-lo para adquirir produtos e serviços de outras pessoas. (Mais informações no Capítulo 8)
- 💡 Minerar bitcoin. (Mais informações no Capítulo 9)
- 💡 Trocar a tua moeda fiduciária por bitcoin, ou vice-versa, presencialmente.
- 💡 Trocar a tua moeda fiduciária por bitcoin, ou vice-versa, online.



De seguida, vamos analisar a troca de moedas fiduciárias por bitcoin e vice-versa, tanto por meio de transações presenciais como através de métodos online, pois são as opções mais comuns.

7.1.1 Ponto a ponto: presencial

A participação em transações ponto a ponto (P2P), para adquirir e vender bitcoin, envolve uma troca direta da tua moeda fiduciária (ou qualquer outro bem ou serviço) por bitcoin com outro indivíduo, o que elimina a necessidade de envolver bancos ou outras entidades na transação.

Ambas as partes determinam mutuamente o montante e a taxa de câmbio. O comprador dá o dinheiro, o vendedor transfere o bitcoin, e a transação fica concluída. Embora seja mais fácil fazer trocas P2P físicas, ao encontrarmo-nos presencialmente com a outra pessoa, também é possível fazê-lo em praticamente qualquer lugar do mundo, graças à internet. Além disso, a troca de bitcoin por moedas fiduciárias tem um processo inverso semelhante.





Capítulo #7

7.1.2 Ponto a ponto: online

É aqui que entram as plataformas P2P, onde os compradores e vendedores de bitcoin se reúnem no ciberespaço, para realizar transações diretamente na internet, sem quaisquer intermediários.

Com estas plataformas, não precisas de confiar os teus dados ou o teu dinheiro a ninguém. Podes encontrar outros participantes e fazer transações diretamente com eles.



Na maioria das plataformas P2P, os participantes têm de bloquear alguma do seu dinheiro, para garantir que cumprem a sua parte. Bloquear significa colocar o dinheiro num local seguro controlado pela plataforma, até que ambas as partes cumpram as suas obrigações. É como se um amigo de confiança guardasse as tuas coisas, até que todos cumprissem a sua palavra.

7.1.3 Corretoras centralizadas

As corretoras centralizadas são, provavelmente, a forma mais fácil de adquirir e vender bitcoin, mas também implicam que abdiques de algumas coisas. As corretoras centralizadas são empresas que permitem aos clientes comprar e vender bitcoin diretamente nas mesmas. No entanto, esta conveniência tem um custo.

Corretoras centralizadas e escolhas envolvidas



É importante lembrar que, quando compras bitcoin numa corretora centralizada, normalmente, és obrigado a fornecer dados pessoais e a verificar a tua identidade. Isto cria um risco de roubo de identidade e expõe os teus dados pessoais a possíveis ameaças. Além disso, as corretoras centralizadas guardam o teu bitcoin, o que significa que não és tu que controlas o teu dinheiro, enquanto o mesmo permanecer na plataforma.

Como se não bastasse, as corretoras centralizadas podem desviar os fundos dos utilizadores ou emprestar mais bitcoin do que têm em reserva, até entrarem em colapso. Sim, tal como fazem os bancos! No entanto, no mundo do Bitcoin, não existe um banco central para criar mais dinheiro e resgatar bancos fraudulentos, visto que não é possível criar mais bitcoin!

CENTRALIZADO

Como usar o bitcoin

7.2 Uma introdução às carteiras Bitcoin

Ao contrário do dinheiro físico, os bitcoins não estão verdadeiramente presentes numa carteira Bitcoin. Os bitcoins existem no livro-razão distribuído que a rede Bitcoin verifica e protege constantemente. Então, como é que se pode deter bitcoin?

Só se é proprietário de bitcoin quando se tem as chaves privadas que permitem assinar transações e transferir a propriedade desse bitcoin para outra pessoa. É assim que se envia bitcoin.

Com isto em mente, vamos analisar dois conceitos que utilizamos, quando nos referimos a uma “**carteira**”:



- ◆ Uma chave mestra privada (que é como uma palavra-passe), a partir da qual se pode gerar chaves públicas para partilhar com outras pessoas, com o objetivo de receber e enviar bitcoins.
- ◆ A interface móvel ou de computador, a partir da qual se pode interagir com a rede Bitcoin, para consultar o saldo de bitcoin, enviar e receber transações e transmitir as mesmas para a rede. Na próxima secção, vamos descrever os diferentes tipos de carteiras, bem como os respetivos benefícios e desvantagens.

7.2.1 Carteiras custodiais e não-custodiais

Antes de analisarmos em detalhe os diferentes tipos de carteiras Bitcoin e respetivas características, vamos fazer uma distinção importante entre carteiras custodiais e não-custodiais. A tabela abaixo inclui os dois tipos principais de carteiras Bitcoin: custodiais e não-custodiais. Podes ver os benefícios e riscos de usar cada tipo de carteira e quem controla o bitcoin em cada caso. Não-custodial significa que é o utilizador que detém as chaves privadas, o que quer dizer que o bitcoin lhe pertence por completo. Por outro lado, com o segundo tipo de carteiras, o teu bitcoin está na posse de terceiros (custódios).

Tipo de Carteira	Quem controla o meu bitcoin?	Benefícios	Riscos
Carteiras não-custodiais	Utilizador	Controlo total sobre fundos e transações, sem processo de aprovação ou congelamento de conta, sem controle corporativo ou governamental, protegido contra confiscações arbitrárias, como guardar dinheiro em casa.	Sem recuperação caso a frase de recuperação seja perdida, menos suporte ao cliente, toda a responsabilidade recai sobre o utilizador.
Carteiras custodiais	Fornecedor externo	Recuperação fácil em caso de perda de acesso, suporte ao cliente mais simples.	Os fundos estão sempre conectados à internet, mais vulneráveis a ataques e violações. Os custódios controlam e podem congelar contas.



Capítulo #7

Numa carteira não-custodial, o utilizador é o único que tem as chaves da carteira e o controlo absoluto daquilo que entra e sai. Por outro lado, numa carteira custodial, a chave privada está na posse de outra entidade, que pode aceder e gerir o conteúdo da carteira em teu nome.

- 💡 Quando usas uma carteira não-custodial, é como se fosses o teu próprio banco. As transações não estão sujeitas ao controlo ou autoridade de qualquer governo ou empresa, mas isso também significa que és inteiramente responsável pela segurança do teu bitcoin.
- 💡 As carteiras não-custodiais garantem que o teu bitcoin nunca será apreendido sem o teu consentimento.
- 💡 As carteiras não-custodiais oferecem tranquilidade em tempos de incerteza, por saberes que o teu bitcoin está seguro.

É importante escolher a carteira certa para as necessidades de cada indivíduo. Por vezes, pode ser difícil distinguir se estás a instalar uma carteira custodial ou não-custodial. Esta tabela mostra as diferenças no processo de instalação.

Tipo de Carteira	1º Passo: Escolher uma carteira	2º Passo: Instalar a carteira	3º Passo: Criar uma nova carteira	4º Passo: Protege a tua frase de recuperação	5º Passo: Começa a usar a tua carteira
Carteiras não-custodiais	Escolhe um fornecedor de carteira não-custodial	Segue as instruções do fornecedor	Gera a frase de recuperação	Guarda a frase de recuperação num local seguro	Começa a usar a carteira para enviar e receber bitcoin
Carteiras custodiais	Escolhe um fornecedor de carteira custodial	Segue as instruções do fornecedor	Cria uma conta com o fornecedor da carteira	N/A (fornecedor da carteira detém a chave privada)	Começa a usar a carteira para enviar e receber bitcoin



**SE AS CHAVES NÃO SÃO TUAS
AS MOEDAS TAMBÉM NÃO**

“Se as chaves não são tuas, as moedas também não” é um ditado muito usado por proprietários de bitcoin. Refere-se à ideia de que, se não tiveres um controlo direto das chaves privadas associadas à tua carteira Bitcoin, as moedas, na verdade, não te pertencem a ti.

Quem tiver acesso às tuas chaves privadas obterá a propriedade do teu bitcoin. É por isso que é extremamente importante mantê-las longe de olhares curiosos, para as proteger! Mais à frente, veremos algumas formas de como fazer precisamente isso.

Em seguida, vamos falar apenas de carteiras não-custodiais, nas quais é o utilizador que tem as suas próprias chaves e o controlo absoluto do seu bitcoin.

Se parecer complicado ou não compreenderes tudo, não te preocupes. É um processo de aprendizagem longo, e vais começar a perceber melhor à medida que vais usando o Bitcoin!

Como usar o bitcoin

7.2.2 Diferentes tipos de carteiras Bitcoin

Conforme o local onde é criada e guardada a tua chave privada, existem diferentes nomes que usamos para descrever carteiras Bitcoin. Se as chaves estiverem guardadas no teu telemóvel, chamamos a isto uma carteira móvel. Se estiverem guardadas em segurança num dispositivo próprio, chamamos ao mesmo uma carteira física. Se a chave só existir escrita em papel, podemos chamar-lhe uma "carteira de papel."

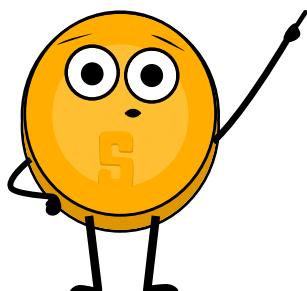
A tabela seguinte contém os diferentes nomes que damos às carteiras Bitcoin, dependendo da estrutura de cada uma:

Tipo de Carteira	Descrição	Vantagens	Desvantagens	Exemplo de utilizador
Carteira Online	Uma carteira que se aceede através de um browser.	Acessível de qualquer dispositivo com ligação à internet. Fácil de usar.	Menos segura. Pode ser hackeada ou comprometida.	Alguém que precise de aceder à sua carteira com frequência e não tenha muitos fundos para armazenar.
Carteira Móvel	Uma carteira instalada num telemóvel.	Conveniente. Acesso em qualquer lado.	Pode ser perdida se o dispositivo desaparecer, for roubado ou hackeado.	Alguém que precise de fazer transações em movimento e não tenha muitos fundos para armazenar.
Carteira de Computador	Uma carteira instalada num computador.	Mais segura do que as carteiras online. Pode ser usada offline.	Pode ser hackeada se o computador for infetado com malware.	Alguém que queira armazenar uma grande quantidade de bitcoin e se sinta confortável a usar um computador.
Carteira Física	Um dispositivo físico que armazena bitcoin offline.	Muito segura. Pode ser utilizada offline.	Os fundos podem ser irrecuperáveis se o dispositivo for perdido ou roubado.	Alguém que queira armazenar uma grande quantidade de bitcoin e esteja disposto a pagar pela segurança adicional de uma carteira física.
Carteira de Papel	Um registo físico das chaves privadas e públicas de uma carteira Bitcoin.	Muito segura. Pode ser utilizada offline.	Pode ser perdida ou roubada se o registo físico for perdido ou roubado.	Alguém que queira armazenar uma grande quantidade de bitcoin e esteja disposto a tomar precauções adicionais para garantir a sua segurança.



Capítulo #7

Tendo em conta que as chaves podem ser movidas de um dispositivo para outro, o estatuto da tua carteira Bitcoin não é definitivo. Por exemplo, se eu gerar as chaves da minha carteira Bitcoin num computador e, mais tarde, as transferir para o meu telemóvel, a carteira de computador torna-se uma *carteira móvel*.



No que diz respeito ao armazenamento do teu bitcoin, não se deve ter em conta apenas quem o controla – existem muitos outros riscos importantes. É por isso que é importante encontrar uma solução de armazenamento segura e conveniente.

Quando analisas aquilo de que tens de abdicar com cada tipo de carteira, vais perceber que não existe uma carteira ideal que satisfaça todas as necessidades.

Ao escolher uma carteira Bitcoin, há várias coisas a ter em conta:

- 💡 **Segurança:** Certifica-te de que a carteira tem fortes medidas de segurança implementadas, tais como a autenticação de dois fatores e políticas de palavra-passe seguras.
- 💡 **Privacidade:** Verifica se a carteira te permite permanecer anónimo ou se requer dados pessoais para configurar uma conta.
- 💡 **Facilidade de utilização:** Escolhe uma carteira fácil de usar e de compreender, especialmente se fores inexperiente no Bitcoin.
- 💡 **Compatibilidade:** Certifica-te de que a carteira é compatível com o teu dispositivo e sistema operativo.
- 💡 **Taxas:** Compara as taxas cobradas por cada carteira, para garantir que obténs a melhor oferta disponível.
- 💡 **Reputação:** Verifica a reputação da carteira e respetiva equipa, para garantir que é uma carteira de confiança.
- 💡 **Controlo:** Algumas carteiras dão-te mais controlo sobre as tuas chaves privadas, o que pode ser uma vantagem, em termos de segurança.

Decide se queres uma carteira que te dê um controlo absoluto ou uma que seja mais fácil de utilizar, mas na qual tens menos controlo.

7.2.3 Código aberto e código fechado

Outro fator importante a ter em conta, ao escolher uma carteira Bitcoin, é saber se a aplicação ou software é de código aberto (*open-source*).

O código aberto é muito importante, porque permite que a comunidade reveja o código e continue a desenvolver o projeto, caso a respetiva equipa deixe de o fazer.

Como usar o bitcoin



Tal como o código do Bitcoin é completamente aberto, para que todos o possam consultar, usar e modificar, o mesmo se deve aplicar ao código da carteira que usas para guardar o teu bitcoin.

Atividade - Debate e avaliação de turma das carteiras Bitcoin em [bitcoin.org](https://bitcoin.org/en/choose-your-wallet)

Entra no seguinte website:

<https://bitcoin.org/en/choose-your-wallet> e coloca em prática os conhecimentos que adquiriste sobre carteiras Bitcoin, ao selecionar a melhor carteira, com base nos critérios que discutimos hoje.



7.3 Configurar uma carteira móvel de Bitcoin

Agora que compreendemos melhor as várias carteiras Bitcoin e as respetivas diferenças, vamos ver como são usadas na prática. Para este exemplo, vamos criar uma carteira móvel diretamente no nosso telemóvel.

Atividade - Configurar/recuperar uma carteira Bitcoin

Se os alunos não tiverem telemóveis, o professor emprestará um a cada aluno. Existem duas opções para esta atividade:



Capítulo #7

22:03

Carteira Bitcoin

Uma carteira de bitcoin simples, para que desfrutes de a usar.

Criar uma carteira

Restaurar carteira existente

A tua carteira, as tuas moedas 100% código aberto e design aberto

A tua frase de recuperação
A tua frase de recuperação é utilizada para criar e recuperar a tua conta.

1. issue	2. flame	3. sample
4. lyrics	5. find	6. vault
7. announce	8. banner	9. cute
10. damage	11. civil	12. goat

Anota estas 12 palavras num papel. A ordem das mesmas é importante. Esta frase permite-te recuperar a tua conta.

Opção 1: Descarrega uma nova carteira.

Como criar e usar uma carteira Bitcoin:

- 1 Procura a aplicação na App Store (iOS) ou Google Play Store (Android).
- 2 Abre a aplicação e digita a tua frase de recuperação de 12 ou 24 palavras (também chamada frase semente). **Certifica-te de que anotas a frase e a guardas num local seguro!** Esta frase de recuperação permite-te recuperar o acesso total ao teu dinheiro, quando for necessário.
- 3 De seguida, deves confirmar que guardaste a tua **frase semente** ou de recuperação. Para isso, tens de **introduzir**, pela mesma ordem, as **palavras** da tua frase de recuperação.
- 4 Como medida de segurança adicional, algumas carteiras permitem-te **escolher uma palavra-passe segura**. A tua **chave privada** é criada automaticamente pela tua carteira. E o primeiro **endereço de bitcoin** é-te dado a conhecer.

O teu endereço público é como um endereço de e-mail: deves partilhá-lo com outras pessoas, para que estas te possam enviar bitcoin (ou um e-mail, no caso de um endereço de e-mail).

O teu endereço privado é como a palavra-passe do teu e-mail: não deves partilhá-la com ninguém, pois permite o acesso ao teu e-mail.

- 5 Procura a opção “**receber**” e utiliza o teu endereço para receber bitcoin. **Transfere bitcoin para a tua carteira**. Com uma carteira não-custodial, nem sempre consegues comprar **bitcoin** diretamente com uma moeda fiduciária, pelo que poderás ter de comprá-lo primeiro numa corretora e transferi-lo.

Como usar o bitcoin

22:03

< Voltar

Esta é a tua frase de recuperação
Não te esqueças de a anotar, tal como a vês
aqui. Terás de a verificar mais tarde.

1	gloom	2	police
3	month	4	stamp
5	viable	6	claim
7	hospital	8	heart
9	alcohol	10	off
11	ocean	12	ghost

Imprimir modelo

Verificar

Opção 2. Recuperar carteira (Com tempo limitado).

Descarrega uma carteira de Bitcoin e adiciona alguns satoshis para cada aluno.

Dá a cada aluno um papel com a frase de recuperação de uma carteira.

Orienta os alunos passo a passo:

- 1 Quando abrires a tua carteira pela primeira vez, terás três métodos à escolha para criar uma carteira. Selecciona **[Importar uma carteira existente]**. Surgirá uma página de introdução. Selecciona **[Restaurar com frase de recuperação]**.
- 2 Introduz a tua frase de recuperação de 12/18/24 palavras, uma a uma, na ordem correta.
- 3 Quando terminares, selecciona **[Recuperar]**.
- 4 Quando a tua carteira tiver sido corretamente importada, verás a mensagem: "Importação concluída".

7.4 Receber e enviar transações

Uma transação Bitcoin é uma transferência de propriedade do bitcoin existente para um novo proprietário. Mas, em vez de transferir as moedas propriamente ditas, todos os nós da rede atualizam a sua cópia local do livro-razão público, por forma a refletir a alteração à propriedade das mesmas.

Ao enviar uma transação Bitcoin, o remetente assina uma mensagem que só ele pode assinar com a sua chave privada, para confirmar à rede que a propriedade do bitcoin deve ser alterada para o endereço do destinatário.

O bitcoin passa a estar associado a um endereço do qual só pode ser enviado pelo novo proprietário, o que dá ao mesmo a propriedade do bitcoin.

Livro-razão

Proprietário da conta	Valor
Luis	2.50
Pedro	3.00
Miguel	6.00
David	1.50
Roberto	2.00
Eliana	1.75
Daniel	5.25

Mensagem de Pedido de Transação de Bitcoin
David envia 0.50 BTC à Eliana
David ➤ Eliana 0.50 BTC

Livro-razão

Proprietário da conta	Valor
Luis	2.50
Pedro	3.00
Miguel	6.00
David	1.00
Roberto	2.00
Eliana	2.25
Daniel	5.25

São iniciadas novas transações Bitcoin em carteiras espalhadas pelo mundo todo, mas não existe um processador de pagamentos central. Em vez disso, são mineradores de todo o mundo que competem para registar transações no livro-razão.

Digamos que o David deve à Eliana 0,5 BTC e está pronto para lhe pagar. Ambos têm carteiras digitais.





Capítulo #7

- 1 A Eliana partilha o seu endereço com o David.
- 2 O David usa o seu software de carteira para criar a transação, que inclui o endereço da Eliana, o montante a ser transferido (0,5 BTC) e uma taxa para o minerador.
- 3 Após assinar a transação, a mesma é transmitida para a rede, onde é verificada pelos nós. Os nós verificam a validade da transação e certificam-se de que o David tem dinheiro suficiente. Se assim não for, rejeitam a transação imediatamente.
- 4 Assim que for verificada a transação, a mesma é adicionada à *blockchain* pelos mineradores, e o dinheiro é transferido para o endereço da Eliana.
- 5 A Eliana pode, depois, usar a sua chave privada para aceder à quantia transferida na sua carteira.

É importante lembrar que, assim que a transação estiver concluída, já não pode ser revertida.

Como Funciona uma Transação de Bitcoin



Alguém solicita uma transação

A transação é transmitida para os computadores P2P (nós)

Os mineradores verificam a transação

As transações são combinadas para formar um bloco de dados

O novo bloco é adicionado à blockchain existente

A transação está completa

Receber transações Bitcoin:



Para receber bitcoin, terás de fornecer ao remetente um endereço da tua carteira de Bitcoin. Este endereço é uma sequência única de letras e números, que representa a tua carteira e é usada para a identificar na Rede Bitcoin. Para encontrar um endereço da tua carteira, inicia sessão na tua carteira Bitcoin e procura a opção de “Receber” ou “Depositar” bitcoin. **Depois, poderás partilhar o teu endereço Bitcoin com o remetente de várias formas:**

- 1 Copiar e colar o endereço: Podes copiar o endereço, ao selecioná-lo e pressionar “Copiar” no teclado, e colá-lo num e-mail ou mensagem para o remetente.
- 2 Partilhar um link para a tua carteira Bitcoin: Algumas carteiras Bitcoin permitem-te criar um link para a tua carteira, o qual podes partilhar com o remetente. O remetente pode, depois, clicar no link para aceder à sua carteira e enviar bitcoin.
- 3 Partilhar um código QR: Se o remetente tiver um telemóvel com uma aplicação de carteira Bitcoin, pode ler o código QR para obter o endereço Bitcoin do destinatário.

Como usar o bitcoin

Assim que o remetente tiver o teu endereço de Bitcoin, conseguirá enviar-te bitcoin, ao introduzir o teu endereço e o montante que pretende enviar, iniciando a transação. O bitcoin será enviado para a tua carteira e ficará visível assim que a transação for confirmada na Rede Bitcoin. Normalmente, isto demora alguns minutos.

De seguida, vamos analisar o processo de envio de transações de bitcoin.



Enviar transações de Bitcoin:

Para enviar Bitcoin, precisas de algumas coisas: uma carteira Bitcoin, o endereço de bitcoin do destinatário e a quantia de bitcoin que desejas enviar.

- 1 Abre a tua carteira Bitcoin. Receberás um código no teu telemóvel, por SMS, e terás de o introduzir na caixa de diálogo. Em alternativa, se tiveres ativado o Google 2FA, terás de introduzir o código de seis dígitos da aplicação Google Authenticator.
- 2 Procura a opção de "Enviar" ou "Retirar" e copia o endereço do destinatário.
- 3 Para introduzir o endereço de Bitcoin do destinatário, cola-o no campo "Para".
- 4 Introduz a quantia de bitcoin que pretendes enviar no campo "Montante".
- 5 Verifica novamente o endereço do destinatário e a quantia a enviar.
- 6 Antes de clicar em "Confirmar e Enviar", recomendamos que verifiques novamente os dados da transação, para garantir que estás a enviar a quantia correta de bitcoin para o endereço correto.
- 7 Confirma a transação e aguarda que a rede também a confirme.

Agora, já sabes como avaliar, escolher e configurar uma carteira Bitcoin não-custodial. Enviar bitcoin de uma carteira para outra na rede Bitcoin é um processo conhecido como envio de transação "*on-chain*". Isto porque a transação ocorre na *blockchain* da rede Bitcoin principal. As transações "*on-chain*" são a forma mais segura de transferir bitcoin. No entanto, estas transações são mais caras e lentas do que outras opções das quais iremos falar no Capítulo 8.

Atividade - Transações Bitcoin em ação

Objetivo: Compreender os conceitos subjacentes e o processamento de uma transação Bitcoin ponto a ponto.

Antes de começar, é importante recordar os principais intervenientes numa transação Bitcoin:

- 💡 Os Remetentes e os Destinatários são as partes que pretendem realizar transações entre si.
- 💡 Os Nós validam as transações e guardam uma cópia completa da *blockchain*. Os nós simples permitem a validação de transações com menos espaço de armazenamento e menos recursos computacionais.
- 💡 Os mineradores são responsáveis pela adição de novas transações à *blockchain*.



Capítulo #7

Entende a tua função. Foi-te atribuída uma das seguintes funções: remetente, destinatário, nó ou minerador.

- ✿ Os remetentes ficarão responsáveis pela criação e transmissão de transações.
- ✿ Os destinatários têm a função de receber e verificar transações.
- ✿ Os nós têm a função validar a transação.
- ✿ Os mineradores são responsáveis pela adição de novas transações à *blockchain*.

Tanto os nós como os receptores têm de verificar as transações.

1 Remetente: Cria uma transação.

Para criar uma transação, segue as seguintes instruções: Tira uma nota de transação e escreve o número de moedas que pretendes enviar e o nome ou iniciais do destinatário. Assina a nota com o teu nome ou iniciais, para simular uma chave privada. Passa a nota de transação e o respetivo número de moedas ao destinatário.

2 Destinatário: O destinatário tem a responsabilidade de verificar as transações. Segue as instruções:

- ✿ Verifica a nota de transação, para garantir que tens escritos o número correto de moedas e o nome ou iniciais do destinatário.
- ✿ Conta as moedas recebidas e compara-as com o número de moedas que está escrito na nota.
- ✿ Se o número de moedas corresponder, assinala a caixa de aprovação. Se os números não baterem certo ou tiveres dúvidas, rejeita a transação.

Moeda Enviada	Remetente	Assinatura do Remetente	Destinatário	Data e Hora	Aprovação do Destinatário

3 Nós: Verifica e valida as transações. Tens a responsabilidade de verificar se a transação é válida.

- ✿ Verifica se os endereços do remetente e do destinatário são válidos.
- ✿ Verifica se o remetente tem dinheiro suficiente para concluir a transação e se a transação não gasta duas vezes a mesma moeda (duplo gasto).

Moeda Enviada	Remetente	Assinatura do Remetente	Destinatário	Data e Hora	Aprovação do Nós

Como usar o bitcoin

4 Minerador: Ficarás responsável pelo registo das transações na *blockchain*. Segue as instruções:

- ✿ Verifica as transações que foram aprovadas pelos destinatários e validadas pelos nós.
- ✿ Lança os dados e compara os números com o outro minerador. O minerador com o resultado mais baixo adiciona a transação à *blockchain*.
- ✿ Ganhas um ponto pelo teu tempo, energia e trabalho. No final da atividade, o minerador com mais pontos ganha.

**Quando uma transação é adicionada à *blockchain*, já não pode ser alterada, nem revertida.

5 Monitoriza o teu saldo: Ao longo da atividade, conta as moedas que tens na tua carteira digital, para monitorizares o seu saldo.

Moeda Enviada	Remetente	Assinatura do Remetente	Destinatário	Data e Hora	Aprovação

6 Conversa com a turma sobre os conceitos que aprendeste.

7.5 Poupar em bitcoin

O Bitcoin é uma forma de protegeres o teu dinheiro contra a inflação e, se o fizeres corretamente, contra o controlo por parte de qualquer outra entidade. Poupar em bitcoin é uma forma de guardar, acumular e criar riqueza a longo prazo. Como já deves ter percebido, o tipo de dinheiro que escolhes poupar é uma das decisões mais importantes que podes tomar. Ao fazeres uma escolha sensata, consegues construir um futuro melhor para ti e para a tua família.



Tranquilidade: Quando armazenado corretamente, o bitcoin é a única forma de propriedade que ninguém te pode tirar.





Capítulo #7

7.6 Não confies, verifica

Faças o que fizeres no Bitcoin, lembra-te do seguinte: "Não confies, verifica." Não existem líderes no Bitcoin. Nunca deves confiar cegamente naquilo que alguém te diz. Pelo contrário, deves sempre questionar o que te está a ser dito e verificar-lo por ti mesmo. Ao seguir este princípio, estás a proteger-te contra perdas de bitcoin. Isto aplica-se a entidades que dizem ser "o próximo Bitcoin" ou "oportunidades de investimento", bem como a "promessas de lucro rápido e fácil".

Resumindo, o Capítulo 7 deu-te os conhecimentos de que precisas para usar o Bitcoin no teu dia a dia. Aprendeste diferentes formas de adquirir e trocar bitcoin e as formas de o proteger utilizando vários tipos de carteiras.

Quando configuras a tua carteira móvel Bitcoine fizeres transações com outras pessoas, ganhas experiência prática para usar o Bitcoin com confiança todos os dias. Se compreenderes o Bitcoin como forma de poupar dinheiro e seguir o conceito "Não confies, verifica.", passas a ter o controlo do teu dinheiro.

No próximo capítulo, vamos descobrir a rede Lightning. Vamos ver como esta tecnologia inovadora está a mudar a forma como as pessoas acedem ao dinheiro e o utilizam no mundo todo. Desde transações do dia a dia até utilizações mais complexas, vais aprender a forma como a rede Lightning dá poder aos indivíduos, comunidades e empresas, ao permitir-lhes o acesso a serviços financeiros.

Capítulo #8

Rede Lightning Usar bitcoin no dia a dia

8.0 Introdução

Atividade - vê o vídeo *Bitcoin Lightning Network Explained: How it Actually Works*

8.1 A rede Lightning

8.2 Diferentes tipos de Carteiras Lightning

8.2.1 Carteiras custodiais e não-custodiais

8.2.2 Código aberto e código fechado

8.3 Configurar uma Carteira de Bitcoin Lightning

8.4 Receber e enviar transações Lightning

Atividade - Corrida de estafetas com a carteira Lightning

8.5 Comprar café e mercearias com bitcoin

8.5.1 Online: Plug-ins de pagamento - Comércio eletrónico

8.5.2 Presencialmente: Encontra um comerciante na tua área de residência

8.5.3 Ferramentas de transição: vales, cartões de oferta e cartões de pagamento

8.5.4 Economias circulares e o bitcoin como meio de troca

Rede Lightning: Usar bitcoin no dia a dia

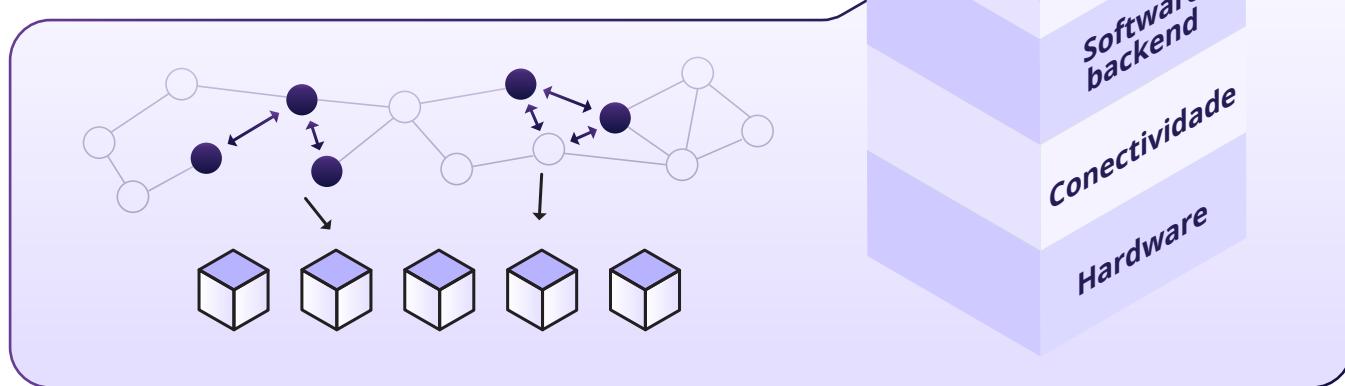
8.0 Introdução

Estamos a construir a rede Visa do bitcoin. Mas o que eu acho poderoso é que, ao contrário da Visa, qualquer pessoa pode expandir a rede.

Elizabeth Stark

Normalmente, as tecnologias crescem e expandem-se em camadas, como uma torre. Pensa no teu website, e-mail ou rede social favorita: estes foram construídos a partir do protocolo de internet, o qual foi construído a partir de computadores, que, por sua vez, foram construídos a partir da eletricidade, etc. Estas tecnologias começaram com uma ideia muito simples e continuaram a melhorar ao longo do tempo.

O Bitcoin não é exceção. Tal como diz a famosa frase de Andreas Antonopoulos: "O Bitcoin é a internet do dinheiro." Constitui a base de um dinheiro digital forte e será uma boa base para construir novas tecnologias.

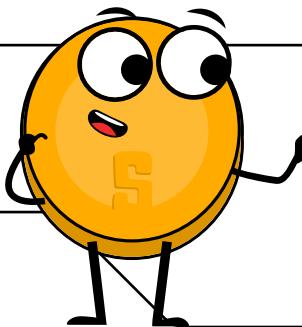


Uma destas tecnologias chama-se rede Lightning. A rede Lightning é como uma autoestrada super-rápida para o Bitcoin. Ajuda as pessoas a enviar e a receber bitcoin de forma muito rápida e com taxas muito baixas. Permite aos utilizadores fazer pequenas transações instantâneas, numa extensão da rede Bitcoin normal. Com esta rede, comprar um café ou enviar dinheiro a um amigo é simples e rápido!

Lembra-te: Um Satoshi é a unidade mais pequena do Bitcoin. Tal como se pode dividir um euro em céntimos, um Bitcoin pode ser dividido em unidades mais pequenas chamadas Satoshis. Um Bitcoin equivale a 100 milhões de Satoshis, o que faz dos mesmos as unidades de valor mais baixas do sistema Bitcoin. Neste capítulo, quando falarmos do envio de bitcoin na rede Lightning, vamos chamar a isto enviar sats, que são apenas partes mais pequenas de um bitcoin.

Satoshi	Bitcoin
1	0,00000001
10	0,00000010
100	0,00000100
1 000	0,00001000
10 000	0,00010000
100 000	0,01000000
1 000 000	0,10000000
10 000 000	0,10000000
100 000 000	1,00000000

Atividade: Vê este vídeo sobre a rede Lightning



8.1 A rede Lightning

Como acabámos de ver, a rede Lightning é um sistema de pagamento que facilita transações de bitcoin rápidas e baratas. O seu funcionamento envolve a criação de uma carteira partilhada, onde ambas as partes detêm bitcoin. As partes podem realizar várias transações entre si, sem a necessidade de as registar a todas no livro-razão principal. O saldo final é, depois, registado no livro-razão, assim que as transações estiverem concluídas.



Rede Lightning é um sistema de pagamentos que permite aos utilizadores enviar e receber pagamentos de forma rápida e económica utilizando bitcoin. Funciona através da criação de uma carteira partilhada onde ambas as partes armazenam os seus bitcoins, permitindo realizar transações ilimitadas entre si sem recorrer à blockchain principal. Quando terminam, o saldo final é registado na *rede* principal.

Imagina um dia passado a trabalhar num café. Sabendo que vais ficar por ali o dia todo, abres uma conta e pagas algum dinheiro adiantado, em vez de pagar sempre que consumes alguma coisa. No final do dia, antes de te ires embora, analisas a conta com o proprietário, para liquidar a conta final. Se pagaste mais do que o que consumiste, recebes o troco.

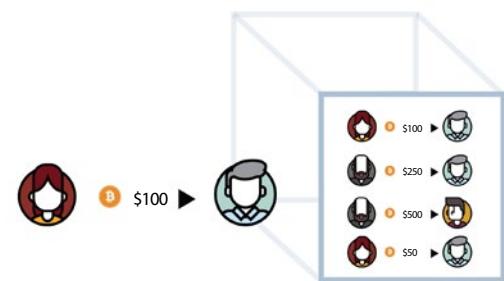
Agora, imagina milhares de pessoas a fazer a mesma coisa ao mesmo tempo e a permitir que as suas contas sejam usadas por outros para estabelecer ligações com mais pessoas. A rede Lightning é precisamente isto!

Com Lightning, é possível enviar dinheiro a qualquer pessoa da rede e não apenas à pessoa com quem partilhas diretamente uma conta. O teu pagamento consegue atravessar a rede até chegar ao seu destino, mesmo que não tenhas um canal aberto com o destinatário.

Vejamos a diferença entre as transações *on-chain* (a variante que abordámos no Capítulo 7) e as transações *off-chain* (Rede Lightning):

Transações *on-chain*:

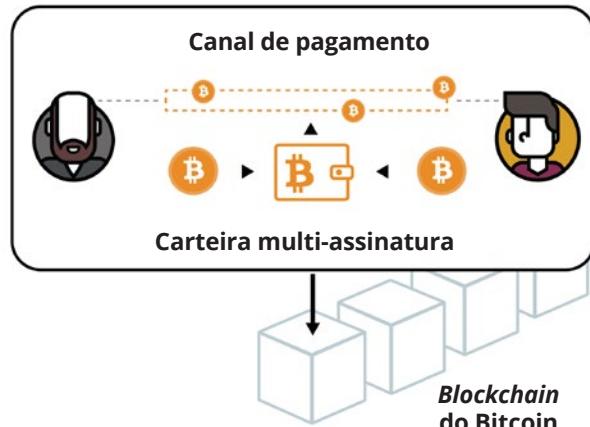
Estas transações são as que ocorrem diretamente na *blockchain* do Bitcoin. Demoram cerca de 10 minutos a serem confirmadas, e as taxas dependem do tamanho da transação em bytes. São mais seguras, mas mais lentas.



Rede Lightning: Usar bitcoin no dia a dia

Transações off-chain (rede Lightning):

Estas transações ocorrem numa rede separada, construída a partir da *blockchain* do Bitcoin. São liquidadas mais rapidamente e com taxas mais baixas. Geralmente, são utilizadas quando as leis e regulamentos apoiam a sua adoção e quando se dá mais importância a certos aspectos como a velocidade e o custo das transações. Quando comparadas com transações on-chain, são menos seguras.



Rede de Pagamentos	Rede Bitcoin	Rede Lightning
Definição	Uma rede digital descentralizada que utiliza criptografia para garantir a segurança das transações financeiras.	Um protocolo de pagamento de segunda camada que funciona sobre a <i>blockchain</i> do Bitcoin, permitindo transações mais rápidas e económicas.
Vantagens	Descentralizada e segura. Sem devoluções de cobrança ou fraude. Pode ser utilizado anonimamente. Aceitação global.	Transações mais rápidas e económicas. Maior escalabilidade. Transações <i>off-chain</i> não congestionam a <i>blockchain</i> .
Desvantagens	Tempos de transação lentos. Taxas elevadas para certos tipos de transações. Complexo para principiantes.	Requer confiança nos operadores dos canais. Ainda é experimental e não amplamente adotada. Requer uma transação <i>on-chain</i> para abrir e fechar canais.



Capítulo #8

8.2 Diferentes tipos de carteiras Lightning

Uma carteira Lightning é um pouco diferente de uma carteira Bitcoin, embora desempenhe a mesma função: receber e enviar bitcoin. A diferença é que uma carteira Lightning permite enviar bitcoin na rede Lightning, uma rede secundária que deriva da rede Bitcoin.

Tal como as carteiras Bitcoin, que vimos no capítulo anterior, as carteiras Lightning têm diferentes características que devem ser tidas em conta antes de se tomar uma decisão.

8.2.1 Carteiras custodiais e não-custodiais

As carteiras Lightning podem ser divididas em categorias muito específicas. Mas, por uma questão de simplicidade, dividimo-las em duas categorias: carteiras custodiais e não-custodiais.

Tal como nas carteiras Bitcoin, as carteiras Lightning não-custodiais são carteiras cujas chaves estão na posse do utilizador, e as carteiras Lightning custodiais são carteiras cujas chaves estão sob o controlo de terceiros.

Se usares uma carteira custodial, terás acesso à tua carteira, mas ficarás dependente da aprovação de terceiros para usares o teu dinheiro. Abdicas da propriedade do teu dinheiro, em troca de conveniência.

Poderá ser uma opção viável para pequenas quantias. No entanto, será sempre mais aconselhável usar uma carteira não-custodial, desde que compreendas a tecnologia da mesma.

Daqui para a frente, vamos falar apenas de carteiras Lightning não-custodiais.

8.2.2 Código aberto e código fechado

Tal como as carteiras Bitcoin que vimos no capítulo anterior, as carteiras Lightning podem ser de código aberto ou de código fechado. Utiliza sempre carteiras de código aberto, pois estas estão completamente abertas a revisões e são aprovadas pela comunidade.

Uma aplicação de código aberto também implica que qualquer pessoa pode contribuir para a melhoria do software, o que a torna uma melhor opção para os utilizadores.

8.3 Configurar uma carteira de Bitcoin Lightning

Configurar uma carteira de Bitcoin Lightning não-custodial é um processo semelhante à configuração de uma carteira Bitcoin on-chain não-custodial.

Rede Lightning: Usar bitcoin no dia a dia

Exercício de turma - Opção 1. Descarrega uma nova carteira Lightning não-custodial

Como criar e usar uma carteira de Bitcoin Lightning.

- 1** Procura a aplicação na App Store (iOS) ou na Google Play Store (Android).
- 2** Abre a aplicação e digita a tua frase de recuperação de 12 ou 24 palavras (também chamada frase semente). **Certifica-te de que anotas a frase e a guardas num local seguro!** Esta frase de recuperação permite-te recuperar o acesso total ao teu dinheiro, quando for necessário.
- 3** De seguida, deves confirmar que guardaste a tua frase semente ou de recuperação. Para isso, tens de introduzir, pela mesma ordem, as palavras da tua frase de recuperação.
- 4** Como medida de segurança adicional, algumas carteiras permitem-te escolher uma palavra-passe segura. A tua chave privada é criada automaticamente pela tua carteira. E o primeiro endereço de bitcoin é-te dado a conhecer.
- 5** Para receber bitcoin, cria uma fatura, endereço ou código QR Lightning. Transfere bitcoin para a tua carteira. Com uma carteira não-custodial, nem sempre consegues comprar bitcoin diretamente com uma moeda fiduciária, pelo que poderás ter de comprá-lo primeiro numa corretora e transferi-lo.

Frase Semente A tua frase semente é utilizada para gerar e recuperar a tua conta.

1 Issue	2 Flame	3 Sample	4 Lyrics	5 Find
6 Vault	7 Scissors	8 Banner	9 Cute	10 Damage
11 Civil	12 Goat			

Por favor, guarda estas 12 palavras num pedaço de papel. A ordem é importante. Esta frase semente permitirá recuperares a tua conta.

*Observação: Se estiveres a utilizar uma carteira custodial, não precisas de seguir algumas das instruções na secção 8.3. Usar uma carteira custodial acarreta riscos, visto que a tua chave privada não está na tua posse, o que significa que o dinheiro que guardas na tua carteira não é controlado por ti.

Agora que criámos a nossa carteira de Bitcoin Lightning, vamos ver como se recebe e envia transações Lightning tal como as diferenças entre estas transações e as transações *on-chain* que enviámos no Capítulo 7.



8.4 Receber e enviar transações Lightning

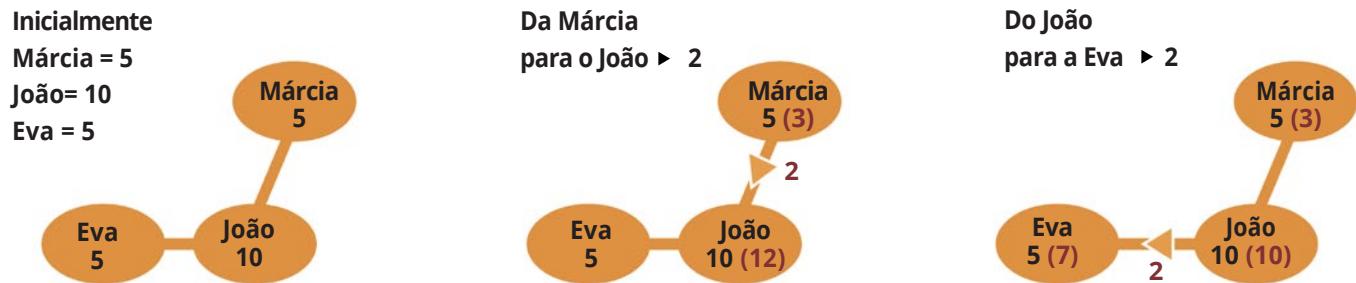
Com uma carteira Lightning, consegues utilizar Bitcoin de forma rápida, barata e privada, o que facilita transações entre duas pessoas. Consegues enviar e receber bitcoin rapidamente, para coisas do dia a dia como comprar café ou ir ao supermercado.

Vejamos alguns exemplos práticos da rede Lightning:

Exemplo 1:

Na ilustração que se segue, a Márcia tem 5 unidades de uma moeda, e a Eva também tem 5 unidades. A Márcia quer enviar 2 das suas unidades para a Eva, pelo que envia 2 unidades para o João. O João envia, depois, as 2 unidades para a Eva, que passa a ter 7 unidades. A Márcia fica com 3 unidades. E é só isto! A transação está concluída.

O que é importante lembrar é que a Márcia e a Eva não precisaram de recorrer a um banco ou outro intermediário para completar a transação.



Neste exemplo, o João é um intermediário (ou terceiro de confiança) numa situação em que a Márcia e a Eva não confiam diretamente uma na outra. O João recebe as 2 unidades da Márcia e envia-as à Eva, por forma a concluir a transação. Ao usar o João como intermediário, a Márcia e a Eva concluem a transação, sem a necessidade de um banco ou qualquer outra instituição centralizada, o que torna a transação mais rápida, barata e segura. O João é um elemento muito importante neste processo de transação ponto a ponto.

Como operador de um nó da rede Lightning, o João tem várias vantagens:



Taxas de transação

O João recebe uma pequena taxa por cada transação que passa pelo seu nó, como recompensa pelo tempo e trabalho que dedica à manutenção e gestão do seu nó.



Participação na rede

Com o seu nó Lightning, o João está a participar na rede e a ajudar a aumentar a sua descentralização, segurança e estabilidade. Isto pode aumentar a reputação e credibilidade do João e, com isso, torná-lo um operador de nó fiável e um intermediário mais atrativo para transações futuras.

Rede Lightning: Usar bitcoin no dia a dia

3

Crescimento da rede

À medida que a rede Lightning cresce e é usada por mais pessoas, é provável que o número de transações que passam pelo nó do João aumente, o que pode resultar num aumento dos seus rendimentos provenientes de taxas de transação.

4

Maior segurança da rede

A função de intermediário que o João desempenha ajuda a aumentar a segurança da rede, pois representa uma camada adicional de proteção entre a Márcia e a Eva. Isto aumenta a confiança dos utilizadores na rede, o que a torna mais atrativa para novos utilizadores e contribui para o seu crescimento. Em geral, a função de operador de nó da rede Lightning pode dar ao João um rendimento estável, bem como a oportunidade de contribuir para o crescimento e desenvolvimento da rede.

Resumindo, **as transações *on-chain* são mais lentas, mas mais seguras, enquanto as *off-chain* (rede Lightning) são mais rápidas, mas menos seguras.** Tem em conta a escolha que fazes entre segurança e rapidez, com base nas tuas necessidades.

Exemplo 2:

A Mina adora ir ao McDonald's. Come lá ao pequeno-almoço, almoço e jantar todos os dias! Mas, com tantas opções de pagamento à escolha, ela não tem a certeza de qual será a melhor opção. Felizmente, ela já conhece o Bitcoin e a rede Lightning. Depois de comparar as tabelas abaixo, a Mina não tem dúvidas de que a melhor opção é usar um método de pagamento Lightning.

Rede Lightning vs O Sistema Bancário Tradicional

Benefícios	Lightning	Sistema Bancário Tradicional	Benefícios	Lightning	Sistema Bancário Tradicional
Velocidade	Rápida	Lenta	Escalabilidade	Alta	Baixa
Transparência	Transparente	Opaco	Privacidade	Alta	Moderada
Segurança	Segura	Vulnerável	Interoperabilidade	Alta	Baixa
Taxas de Transação	Baixas	Altas	Conformidade Legal	Moderada	Alta
Inclusão Financeira	Alta	Limitada	Rentabilidade	Alta	Moderada

Visa, Inc.

Em média 1 700
transações por segundo.



Capacidade para 65 000
transações por
segundo.

Bitcoin On-chain



Capacidade para 7
transações por
segundo.

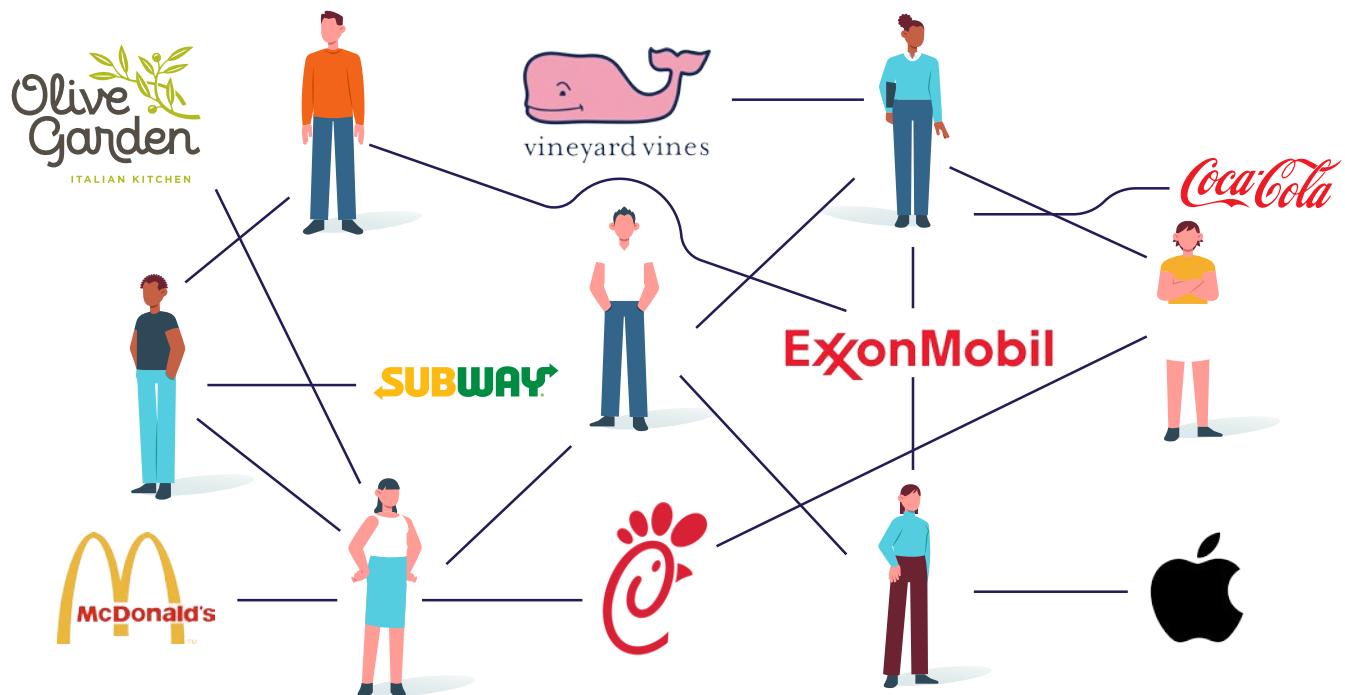
Rede Bitcoin
Lightning



Milhões de
transações por
segundo.

A Mina também adora transações rápidas, seguras e económicas, pelo que decidiu usar a Rede Lightning para fazer pagamentos no McDonald's. Com Lightning, as suas refeições sabem ainda melhor, pois ela sabe que os seus pagamentos são processados instantaneamente, de forma segura e com taxas baixas. Além disso, graças à inclusão financeira que a rede Lightning lhe dá, a Mina já consegue pagar as suas refeições, mesmo em áreas remotas de El Salvador.

Para começar a usar a Rede Lightning, a Mina descarrega uma carteira Lightning para o seu telemóvel. Depois, envia bitcoin da sua carteira Bitcoin normal para a sua nova carteira Lightning, para que a mesma fique com saldo disponível. É este o processo que se usa para depositar dinheiro na carteira ou canal de pagamento. A Mina pode depositar qualquer quantia de bitcoin na sua carteira, mas deve ter em conta que a quantia que ela colocar na sua carteira Lightning ficará indisponível para uso nas suas transações *on-chain*.



Assim que a sua carteira Lightning tiver saldo disponível, ela pode utilizá-lo para fazer pagamentos no McDonald's.

O McDonald's tem um nó Lightning, pelo que a Mina pode abrir um canal de pagamento com eles enviando alguns dos seus bitcoins através de uma transação *on-chain* que bloqueia esses fundos enquanto o canal Lightning estiver aberto. Desta forma, transfere o seu bitcoin da *blockchain* Bitcoin para um canal *off-chain* na rede Lightning.

Com um canal de pagamento aberto, a Mina já pode fazer compras no McDonald's, sem ter de abrir um novo canal ou pagar taxas altas por cada pagamento. A Mina e o McDonald's podem manter o canal aberto enquanto precisarem do mesmo. Por exemplo, se a Mina comprar um hambúrguer por 0,0005 bitcoin, o canal regista que a Mina fica com 0,9995 bitcoin. No dia seguinte, se ela comprar um batido por 0,0003 bitcoin, o canal regista que a Mina passa a ter 0,9992 bitcoin.

Rede Lightning: Usar bitcoin no dia a dia

Quando a Mina decide que quer usar o seu saldo de bitcoin para outros fins, transmite uma transação de fecho para a *blockchain* do Bitcoin, para fechar o canal. Para isso, inicia uma transação de fecho na sua carteira Lightning, que contém o saldo final do canal acordado por ambas as partes. Depois, a transação é transmitida para a *blockchain* do Bitcoin e confirmada por um minerador. Quando a transação for confirmada, o canal é fechado e o bitcoin que resta no canal será devolvido à Mina e ao McDonald's.

É importante lembrar que a confirmação de fecho de um canal, na *blockchain*, pode demorar algum tempo. Enquanto se aguarda a confirmação, o bitcoin permanece bloqueado no canal e não pode ser utilizado para transações *on-chain*. Assim que a transação de fecho estiver confirmada, a Mina receberá uma notificação.

Agora que configurámos a nossa carteira Lightning e aprendemos a utilizar a rede Lightning para enviar transações, vamos jogar a um jogo onde usamos a rede Lightning para enviar satoshis (a unidade mais pequena de bitcoin) a outros alunos da turma.



Isto é um mapa do mundo inteiro. Com a rede Lightning, podes enviar satoshis a qualquer utilizador da rede, desde que este tenha uma carteira de Bitcoin Lightning. O pagamento demora alguns segundos a chegar ao destino e custa apenas alguns céntimos.





Capítulo #8

Atividade: Exercício de turma - Corrida de estafetas com a carteira Lightning

- 1** Primeiro, terás de descarregar uma carteira Lightning para o teu telemóvel ou computador.
- 2** Para instalar a carteira no teu dispositivo, segue as instruções da secção 8.3 deste Capítulo.
- 3** Assim que a carteira estiver instalada, abre-a e segue as instruções de configuração. Isto pode incluir a criação de uma nova carteira ou a recuperação de uma existente, bem como a proteção da mesma com uma palavra-passe ou outra forma de autenticação.
- 4** Para receber bitcoin, cria uma fatura, endereço ou código QR Lightning.
- 5** Quando a tua carteira estiver configurada e pronta a receber satoshis, o professor vai dar ao teu grupo uma quantia inicial de satoshis, ao enviá-la diretamente para uma das vossas carteiras.



A O objetivo do teu grupo é transferir os satoshis de uma carteira para outra com a rede Lightning, até chegarem à última pessoa do grupo.



B Para enviar satoshis a outra pessoa, abre a tua carteira e segue as instruções de pagamento. Terás de inserir a fatura Lightning do destinatário ou ler um código QR e introduzir a quantia de satoshis que pretendes enviar.



C Se o teu grupo for o primeiro a enviar corretamente os satoshis para a última pessoa, serão os vencedores do jogo (e podem ficar com os sats)!

Conversa com a turma sobre as dificuldades que o teu grupo sentiu durante a atividade. Acham que foi fácil, rápido e barato fazer uma transação? Sentem que a rede Lightning é fácil de usar e entender?

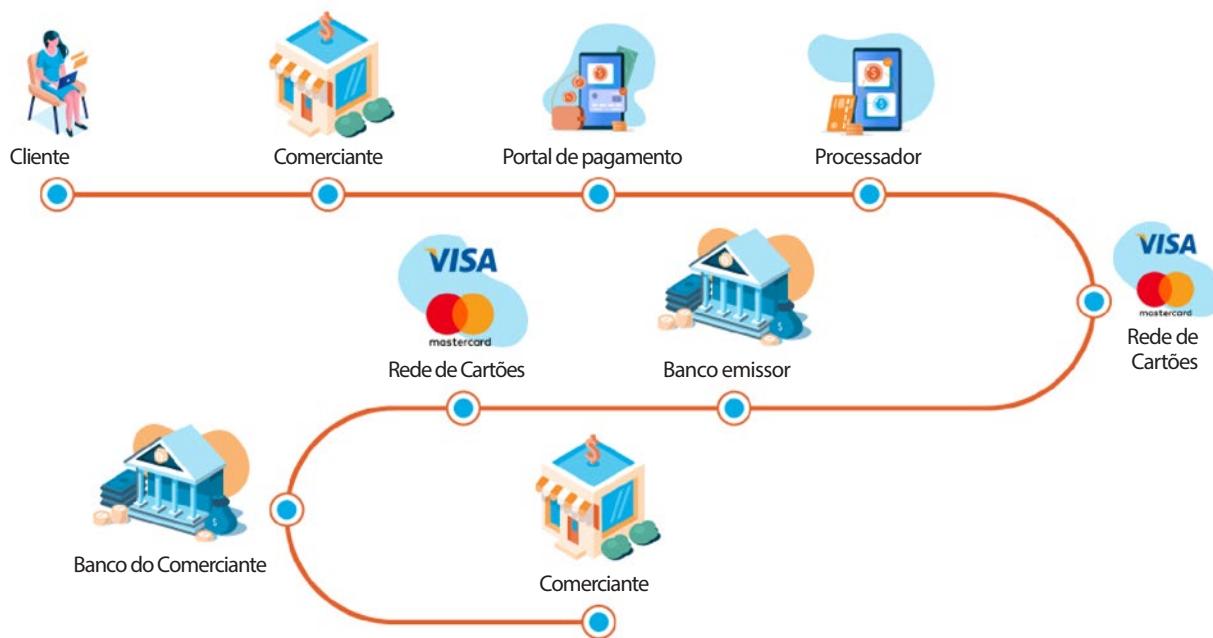
Rede Lightning: Usar bitcoin no dia a dia

8.5 Comprar café e mercearias com bitcoin

Alguma vez questionaste se seria possível usar bitcoin para comprar o teu cafezinho diário ou para ir ao supermercado? Está comprovado que sim. Existem muitas opções, tanto online como presenciais, que te permitem pagar com bitcoin. Vamos conhecer algumas destas opções e ferramentas que te ajudam a encontrar lojas locais onde podes gastar bitcoin.

Embora os pagamentos com cartões de crédito ou aplicações possam parecer simples para quem está a pagar, o processamento desses pagamentos é, na verdade, muito complexo e envolve muitos intervenientes.

Como Funciona o Processamento de Pagamentos



Quando fazes uma compra, existem muitas partes envolvidas, e cada uma delas cobra uma taxa. Para os donos das lojas, estas taxas podem ser muito altas, mais de 3% do preço de venda, o que é um valor bastante alto.

Já para não falar das taxas de câmbio!



Capítulo #8

Taxas de Processamento do Cartão de Crédito



Com o Bitcoin e a rede Lightning, as empresas podem receber pagamentos instantâneos de qualquer parte do mundo, através de um sistema monetário aberto, seguro, criado na internet, sem fronteiras e resistente à censura.

Em seguida, vamos analisar algumas formas que os comerciantes têm de aceitar facilmente pagamentos em bitcoin.

8.5.1 Online: Plug-ins de pagamento – Comércio eletrónico

O BTCPay Server é um processador de pagamentos de código aberto, que permite aos comerciantes aceitar pagamentos em bitcoin, sem a necessidade de grandes conhecimentos técnicos. É completamente gratuito e não cobra comissões.

As empresas online podem integrar facilmente o BTCPay Server, ao adicionar o plug-in BTCPay ao seu site.

Sê o teu próprio processador de pagamentos

Date	Orderid	Invoiceid	Status	Amount
4/12/2020 11:57:47 AM	MiQCrStIHPw7KUZCSq1qp		paid	\$2.00 (USD)
4/12/2020 11:57:37 AM	GGa21TUGnCwzuU5VEh02		paid	0.01000000 BTC 1 BTC = \$1/USD
4/12/2020 11:57:26 AM	KJwgOpdPmnyH8lcwMmgHf		new	120.00 € (EUR)
4/12/2020 11:57:15 AM	VUpWH4UvLugGP3lyGwNaf		new	\$5.00 (USD)
4/10/2020 11:53:52 PM	YVh47cWQj3tK9QmUtgj		expired	\$50.00 (USD)
4/6/2020 12:15:43 PM	SVNk3Ny2zyPQ5hYQq8d2		expired	\$10.00 (USD)



Rede Lightning: Usar bitcoin no dia a dia

Visto que o BTCPay Server é um projeto de código aberto e não uma empresa, podes até contribuir para o mesmo, se estiveres disposto a conhecê-lo melhor e a aprender programação informática.

Visita o BTCPayServer

<https://btcpayserver.org/>, para obter mais informações sobre a utilização deste sistema de pagamento no teu negócio presencial ou online.



8.5.2 Presencialmente: Encontra um comerciante na tua área de residência



As lojas físicas também podem usar o BTCPay Server para aceitar pagamentos, ou podem simplesmente descarregar uma carteira Bitcoin e aceitar pagamentos Bitcoin diretamente no seu telemóvel.





Capítulo #8

Para encontrar um comerciante que aceite Bitcoin na tua área, visita o BTCMap.org e faz uma pesquisa na tua região.

O BTCMap.org é um mapa de código aberto, onde os comerciantes que aceitam Bitcoin podem registar os seus negócios. É uma ferramenta poderosa para quem deseja fazer compras em bitcoin.

The image shows the BTCMap.org website on the left and a mobile phone displaying the app on the right. The website features a logo with a green location pin and a Bitcoin symbol, followed by the text 'BTCMap.org'. Below this, there is a large teal-colored text box containing the slogan: 'Encontra facilmente locais para gastar sats em qualquer parte do mundo.' (Find easily places to spend sats anywhere in the world.) Below the slogan are five circular icons representing different platforms: a globe, a camera, an Android phone, a play button, and an iPhone. To the right of the phone screen is a map of Los Angeles, California, showing various neighborhoods and landmarks. Green location pins are placed on the map, each with a small icon indicating a Bitcoin-friendly merchant, such as a trash can or a burger.

8.5.3 Ferramentas de transição: vales, cartões de oferta e cartões de pagamento

Para comprar produtos ou serviços de empresas que ainda não aceitam bitcoin, existe uma ferramenta intermediária que podes usar: cartões de oferta.

Existem empresas que compram e vendem cartões de oferta, em troca de bitcoin. Isto significa que é possível adquirir um cartão de oferta para a loja onde pretendes fazer compras, em troca de bitcoin, e usar esse cartão de oferta diretamente na loja.

Bilhetes de avião, hotéis, jogos, cartões SIM... podes comprar praticamente tudo com bitcoin e cartões de oferta!

8.5.4 Economias circulares e o bitcoin como meio de troca

O conceito de economia circular surge com a ideia de minimizar o desperdício numa economia, ao reutilizar e reciclar o máximo de produtos e subprodutos possível.

Com base neste conceito, numa economia circular Bitcoin, as transações são feitas em bitcoin, e o dinheiro em bitcoin permanece e cresce dentro da economia, para beneficiar os indivíduos e empresas que existem na mesma.



Rede Lightning: Usar bitcoin no dia a dia

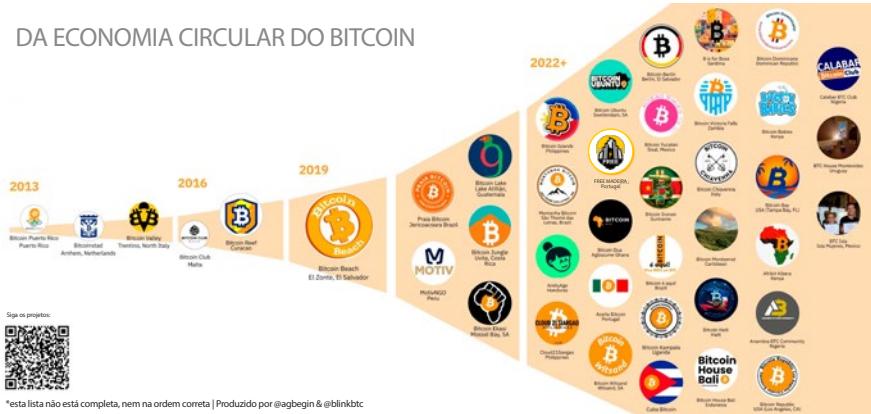
A rede Lightning permite que se desenvolvam economias circulares de Bitcoin no mundo todo, graças a transações de bitcoin quase instantâneas e com taxas baixas.



A primeira economia circular de Bitcoin que alguma vez existiu está localizada em Arnhem, nos Países Baixos. Foi criada muito antes da rede Lightning, embora as taxas *on-chain* fossem muito baixas naquela altura!

O BIG BANG

DA ECONOMIA CIRCULAR DO BITCOIN



A segunda foi a Bitcoin Beach, localizada em El Zonte, El Salvador. Esta aproveitou o poder da rede Lightning para dar à sua comunidade (que, na sua maioria, não tinha acesso a serviços bancários) a opção de fazer pagamentos eletrónicos instantâneos diretamente nos seus telemóveis!

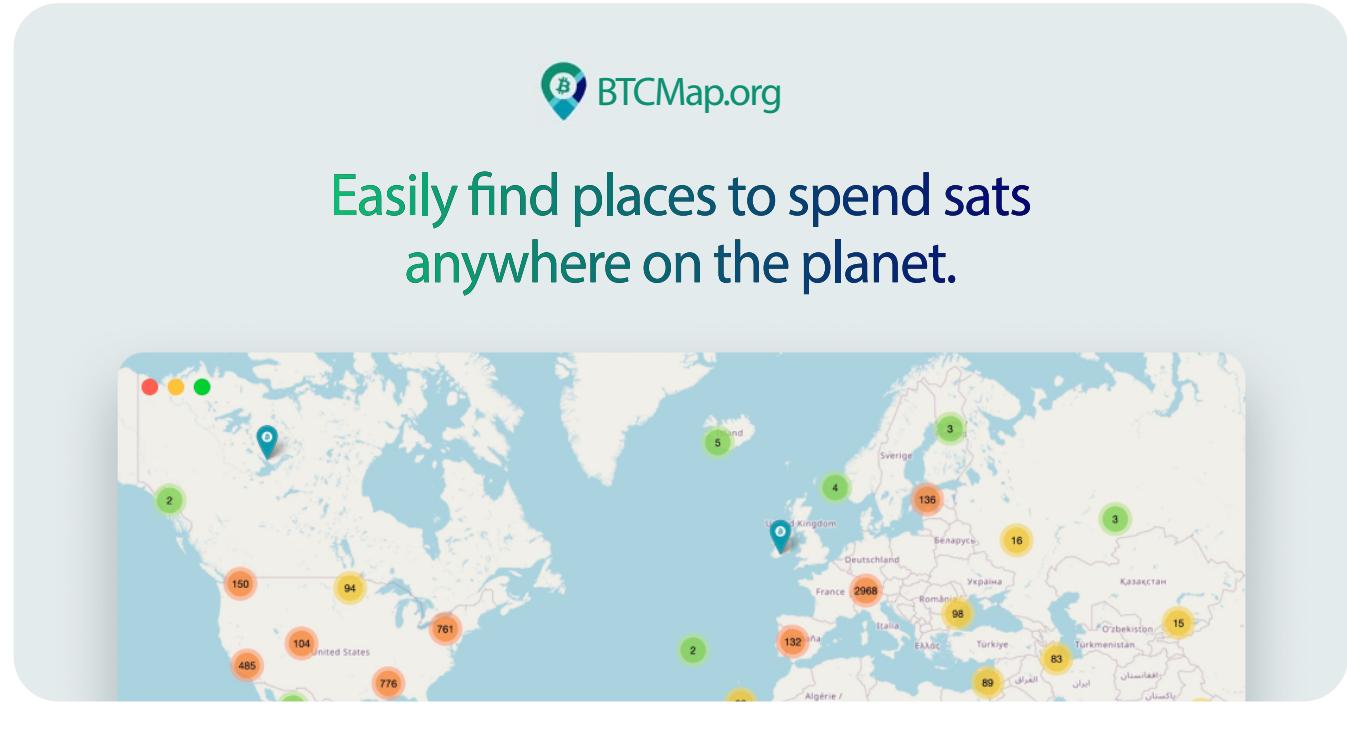
Atualmente, estão a ser criadas centenas de economias circulares no mundo inteiro, que utilizam o Bitcoin, a rede Lightning e recursos educacionais.



Capítulo #8

O Meu
Bitcoin

No BTCMap.org, também é possível encontrar comunidades Bitcoin, onde podes conhecer outros utilizadores Bitcoin e empresas que aceitam bitcoin. Aliás, alguns dos nossos professores e alunos já adicionaram empresas e economias circulares ao BTCmap.org. Quando te sentires preparado, também o podes fazer!



Recurso: btcmap.org/communities

Chegámos ao fim do Capítulo 8, e já aprendeste a usar o Bitcoin no teu dia a dia, através da rede Lightning. A rede Lightning torna as transações mais rápidas e acessíveis, e dá-nos uma ideia da futura evolução e ramificações do Bitcoin.

No Capítulo 9, vamos analisar o lado técnico do Bitcoin. A criptografia, os nós, os mineradores e muito mais. Prepara-te para conhecer melhor o verdadeiro funcionamento do Bitcoin.

Capítulo #9

Uma introdução ao lado técnico do Bitcoin

9.0 Introdução

Atividade - veja o vídeo *How Bitcoin Works Under the Hood*

9.1 Chaves públicas e privadas: Segurança com base na criptografia

9.1.1 Criptografia de chave privada e criptografia de chave pública

9.1.2 Explicação de *hashing* (dispersão)

Atividade - Gerar *hash* (valor de dispersão) SHA256

9.2 O modelo UTXO

9.3 Uma análise mais detalhada dos nós e mineradores do Bitcoin

9.3.1 O que é um nó do Bitcoin e como posso criar o meu próprio nó?

Atividade - Vê o vídeo sobre os nós do Bitcoin

9.3.2 O que é um minerador do Bitcoin e como funciona a mineração?

9.4 O que é a *mempool* (memória de transações)

Atividade - *Mempool*

9.5 O processo completo das transações Bitcoin

Manual do Aluno

Versão Portuguesa | 2025

Uma introdução ao lado técnico do Bitcoin

9.0 Introdução

O Bitcoin não é *desregulado*. É regulado por algoritmos, em vez de ser regulado por burocracias governamentais. Incorruptível.

Andreas M. Antonopoulos

Neste capítulo, vamos analisar mais pormenorizadamente a tecnologia que permite à rede Bitcoin operar de forma totalmente descentralizada. Vamos explicar, em termos simples, o que acontece quando envias uma transação Bitcoin, o processamento dessas transações e a função dos mineradores e dos nós na rede Bitcoin. Neste capítulo, vamos abordar alguns conceitos complexos e técnicos. Lembra-te que há muitas pessoas que não entendem o funcionamento da internet e, ainda assim, conseguem usá-la todos os dias para enviar e-mails, contactar amigos nas redes sociais e até mesmo para pagar as suas contas. Aprender o lado técnico do funcionamento do Bitcoin é um processo demorado, que pode não interessar a toda a gente, mesmo que decidam usá-lo como forma de dinheiro. Embora nós vos incentivemos a conhecer melhor os aspetos técnicos do Bitcoin, vamos manter o foco deste capítulo nos principais conceitos básicos.

Mecanismos do Protocolo Bitcoin

Proof-of-Work



Registos Criptográficos de Data e Hora



Ajuste de Dificuldade



Arquitetura de Rede Ponto a Ponto

Funções de Hash (ou de dispersão) e Árvores de Merkle

Criptografia de Chave Pública

Redução da Recompensa de Bloco para Metade

Caso queiras obter uma compreensão técnica mais aprofundada do funcionamento do Bitcoin, incluímos recursos no verso deste manual. Também tens a opção de te registares no nosso website do Diploma Bitcoin - Edição Técnica, para seres notificado quando esse curso mais técnico estiver disponível.

Vamos começar com um vídeo que mostra o funcionamento da rede Bitcoin.

Atividade: vê o vídeo *How Bitcoin Works Under the Hood*



Como viste no vídeo, a rede Bitcoin é apenas um livro-razão, ou registo de transações, que é guardado em vários computadores chamados nós. O livro-razão do Bitcoin é pseudonimizado, ou seja, não tem dados pessoais. Contém apenas informações relativas a transações e endereços. O livro-razão mostra cada bitcoin e respetivas transferências, desde o dia em que a rede surgiu, a 3 de janeiro de 2009.

Em seguida, vamos analisar mais detalhadamente a tecnologia que possibilita este sistema...



Capítulo #9

9.1 Chaves públicas e privadas: Segurança com base na criptografia



O que o Bitcoin nos dá é uma promessa difícil de cumprir: a de que o programa será executado exatamente conforme especificado.

Andreas M. Antonopoulos



9.1.1 Criptografia de chave privada e criptografia de chave pública

A criptografia é uma forma de esconder informações secretas, através da sua codificação.



A encriptação é o processo no qual as informações são transformadas num código especial, que as torna ilegíveis para quem não tem o método de desencriptação correto. É como trancar um cofre que só pode ser aberto pela pessoa com a chave ou combinação certa.

Por outro lado, a desencriptação é o processo no qual as informações encriptadas são tornadas legíveis. É como abrir o cofre e conseguir ler as informações que o mesmo contém.

Por exemplo, digamos que o João quer enviar ao Ari uma mensagem secreta e não quer que mais ninguém a leia. Concordam em utilizar a Cifra de Pigpen para disfarçar a mensagem, antes de a enviar. Só quem conhece o método de encriptação é que consegue desencriptar a mensagem, o que a torna ilegível para todas as outras pessoas. Este método, embora considerado pouco seguro atualmente, ilustra o conceito da criptografia de chave privada no envio de mensagens.

Então, como é usada a criptografia nas transações Bitcoin?

Na criptografia de chave privada tradicional, o João e o Ari teriam de partilhar uma chave secreta antes do envio da mensagem, como uma palavra-passe ou a Cifra de Pigpen. Depois, o João teria de usar esta chave para encriptar a sua mensagem, antes de a enviar para o Ari. O Ari, que também conhece a chave secreta, usaria a mesma para desencriptar e ler a mensagem.

No entanto, se mais alguém tivesse a chave e intercetasse a mensagem, conseguiram desencriptar e ler a mensagem.

Como Resolver Cifra Pigpen

Para resolver a Cifra Pigpen, o jogador recebe uma mensagem encriptada e uma cifra. Para desencriptar a mensagem, o jogador tem de encontrar o símbolo da mensagem encriptada na cifra, de modo a encontrar a letra desencriptada.

Exemplo de uma mensagem encriptada

— • — — — —

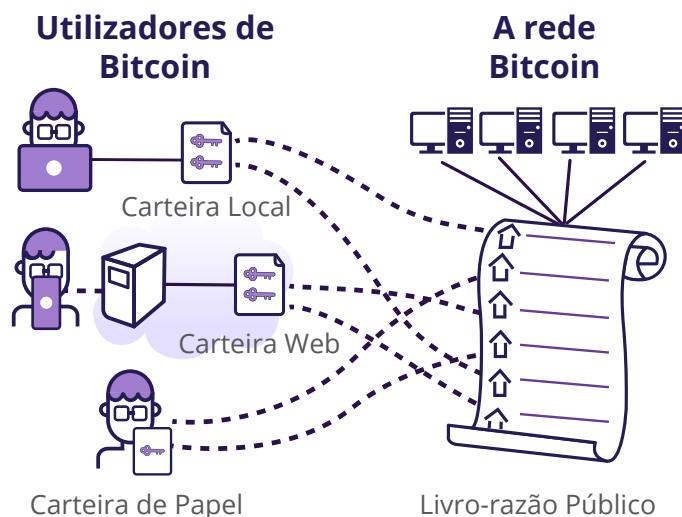
— — — — — —

A	B	C	J.	K.	L	S	T	W
D	E	F	M.	N.	F	U	X	Y
G	H	I	P.	Q.	R	V	Z	

Uma introdução ao lado técnico do Bitcoin

A criptografia de chave pública, usada nas transações de bitcoin, resolveu este problema. Com a encriptação de chave pública, o João e o Ari não precisam de partilhar a palavra-passe ou método de encriptação um com o outro. Em vez disso, cada um tem duas chaves diferentes: a **chave pública** (que pode ser partilhada com qualquer pessoa) e a **chave privada** (que nunca deve ser partilhada).

Neste caso, quando o João quer enviar uma mensagem para o Ari, pode usar a **chave pública** do Ari para encriptar a sua própria mensagem, antes de a enviar. Quando o Ari recebe a mensagem, só ele é que consegue desencriptá-la com a sua **chave privada**. Mesmo que a mensagem fosse intercetada por outra pessoa, seria ilegível para a mesma. A probabilidade de a chave ser roubada também é muito reduzida, visto que o João e o Ari nem precisam de partilhar a chave um com o outro.



Portanto, a principal vantagem da criptografia de chave pública, em relação à criptografia de chave privada, é que permite uma comunicação segura, sem precisar que o remetente e o destinatário partilhem uma chave secreta (ou outro método de encriptação como a cifra *Pigpen*) que possa ser intercetada por terceiros.

No Bitcoin, a criptografia de chave pública não é usada para enviar mensagens encriptadas. Em vez disso, é usada para criar **assinaturas digitais** únicas, que tornam as transações Bitcoin imutáveis. Uma **assinatura digital** é uma forma de comprovar a autenticidade de uma transação Bitcoin, de forma semelhante a uma assinatura num documento físico.



Criptografia de Chave Pública (para transações entre dois utilizadores):

Cada utilizador tem duas chaves: uma **chave privada**, que é **secreta**, e uma **chave pública**, que é **partilhada com outros**.

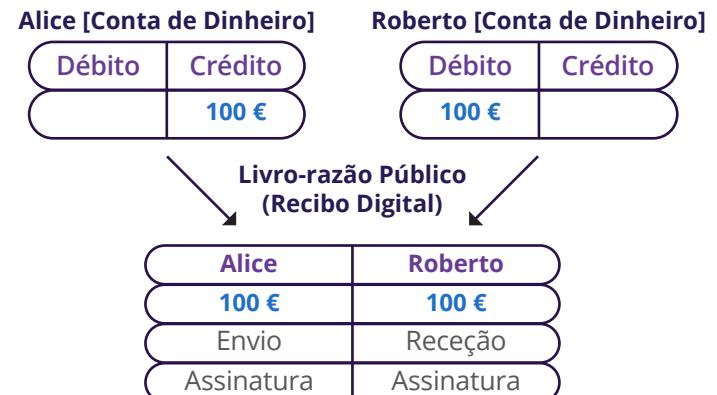
A **chave privada** é uma forma de identificação e prova de propriedade que diz: "Eu sou proprietário deste endereço e tenho controlo sobre o mesmo".

Assinaturas digitais são criadas para identificar transações únicas.

Assinatura Digital



- 💡 As transações Bitcoin envolvem a transferência de uma determinada quantia de bitcoin diretamente para a conta de outra pessoa.
- 💡 A encriptação é usada para garantir que só o verdadeiro titular do bitcoin é que consegue enviar o seu dinheiro a outra pessoa. É uma forma de assegurar que esse dinheiro está protegido contra malfeiteiros.
- 💡 Como medida de proteção adicional, cada transação de bitcoin que envias terá automaticamente uma **assinatura ÚNICA**. Esta **assinatura única** potenciada por uma tecnologia inviolável, que ajuda a rede a verificar se foi o verdadeiro proprietário do bitcoin que o enviou e não outra pessoa.



Em termos simples, as transações Bitcoin aplicam este método da seguinte forma:

- 1 Envio da transação:**
Para iniciar uma transação de bitcoin, o utilizador insere dados específicos, tais como o endereço do destinatário e a quantia de bitcoin a ser enviada.
- 2 Emissão da Assinatura Digital:**
O remetente usa a sua **chave privada** para gerar uma **assinatura digital única**. Esta assinatura é um código criptográfico único, que verifica a autenticidade da transação.
- 3 Transmissão da transação:**
A transação assinada é transmitida para a rede Bitcoin, para assinalar a intenção de transferir a propriedade do bitcoin do remetente para o destinatário.
- 4 Verificação da Rede:**
Os nós da rede Bitcoin recebem a transação e usam a **chave pública** do destinatário para desencriptar e verificar a integridade da transação. Ao mesmo tempo, utilizam a **chave pública** do remetente para verificar a **assinatura digital**.
- 5 Confirmação na Rede Bitcoin:**
Se a transação for aprovada, é adicionada ao livro-razão, que é um registo seguro e transparente de todas as transações. Quando a transação estiver confirmada, a propriedade do bitcoin é oficialmente transferida do remetente para o destinatário.



Resumindo, a assinatura digital, criada com a chave privada do remetente, serve de prova criptográfica de autenticidade e propriedade, por forma a permitir que a rede descentralizada do Bitcoin valide e registe a transação no livro-razão.

Uma introdução ao lado técnico do Bitcoin

9.1.2 Explicação de hashing (dispersão)

Não te deixes intimidar pelos termos técnicos e conceitos matemáticos que se seguem. Nós sabemos que nem toda a gente adora matemática. Mas, com algum esforço, talvez te surpreendas e até consigas entender conceitos bastante complexos.

O que é uma função?

Uma **função** é como uma máquina que recebe informação e a transforma em algo novo. A informação que inseres na função chama-se **variável**. A nova informação que a função cria chama-se **resultado**. As funções ajudam os computadores a realizar tarefas e a resolver problemas.



Imagina que é como a receita de uma salada. A receita (ou função) diz-te os ingredientes que deves utilizar e como misturá-los para fazer a salada. Podes usar ingredientes diferentes, mas o resultado da receita é sempre uma salada. As funções podem ser utilizadas para ajudar a tornar tudo mais fácil e eficiente.

Esta receita é, portanto, uma função que recebe os ingredientes como **variáveis** e gera a salada misturada como **resultado**.

No Bitcoin, as funções são utilizadas para executar transações. Já sabemos que as transações de bitcoin são, essencialmente, transferências de valor (dinheiro) de um endereço para outro. Para efetuar uma transação, são utilizadas várias funções criptográficas, para validar a transação e atualizar o estado do livro-razão do Bitcoin.

As funções usadas nas transações Bitcoin incluem a verificação da autenticidade das entradas de transação, a verificação de que o remetente tem saldo suficiente e a atualização dos saldos dos respetivos endereços. Quando uma transação é verificada e adicionada a um bloco no livro-razão, torna-se parte do registo permanente de todas as transações da rede.



O que é uma função unidirecional?

Uma função unidirecional utiliza um conjunto de instruções para processar as informações e transformá-las em algo novo, tal como a receita de um batido transforma os ingredientes numa bebida nova. No entanto, tal como não é possível desmisturar um batido e recuperar os ingredientes originais, também não é possível reverter uma função unidirecional e recuperar as informações originais.





Capítulo #9

A criptografia de chave pública, da qual faz parte a **chave pública**, depende da utilização de funções unidireccionais, que dificultam a obtenção da **chave privada** a partir da **chave pública**. Em teoria, não é completamente impossível obter uma **chave privada** a partir da respetiva **chave pública**. Mas é extremamente difícil fazê-lo, e seria necessária uma quantidade desmesurada de tempo e capacidade de computação para realizar tal feito.

No Bitcoin, obter uma **chave privada** a partir de uma **chave pública** é como tentar encontrar uma agulha num palheiro do tamanho de um campo de futebol. A agulha representa a **chave privada** e o palheiro representa todas as **chaves privadas** possíveis.

De igual forma, as funções unidireccionais foram concebidas para serem irreversíveis e impossíveis de desencriptar.

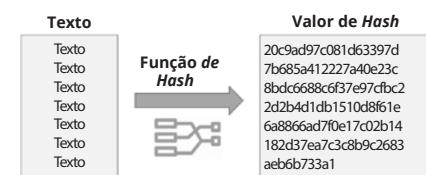


O que é uma função hash (função de dispersão)?

A **dispersão (hashing)** é como uma impressão digital para informações digitais. É um processo de transformação de uma mensagem digital num código de tamanho fixo, que serve de identificador único.



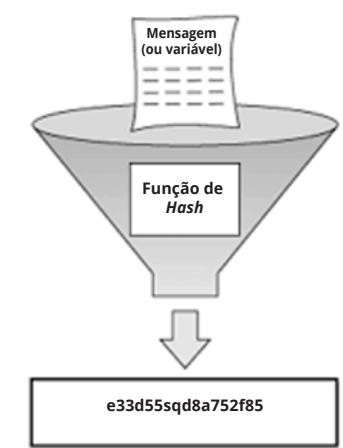
Tal como uma impressão digital identifica uma pessoa, um valor de dispersão identifica uma mensagem digital. Os valores de dispersão são usados para muitos fins, incluindo transações Bitcoin.



A utilização de valores de dispersão nas transações Bitcoin

No Bitcoin, todas as transações passam por uma função de dispersão, antes de serem adicionadas a um bloco no livro-razão. O valor de dispersão serve de assinatura para a transação, para confirmar que a mesma é válida e não foi adulterada. Se alguém tentar alterar uma única letra na transação, o valor de dispersão será completamente diferente, o que alerta outros intervenientes para essa alteração.

Informação de Tamanho Aleatório



O papel da dispersão na segurança

A dispersão é essencial para a segurança da Rede Bitcoin. Ao utilizar valores de dispersão para identificar transações, a rede consegue detetar qualquer tentativa de alterar ou manipular uma transação. Isto ajuda a prevenir fraudes e a garantir que todas as transações são registadas com precisão no livro-razão.

Uma função de dispersão é uma função unidirecional, que recebe uma **variável** (normalmente designada de mensagem ou dados) e converte-a numa representação numérica chamada valor de dispersão. O valor de dispersão (resultado) corresponde exclusivamente a esta variável (mensagem), ou seja, qualquer alteração, por mais insignificante que seja, à **variável** que a função recebe resulta num valor de dispersão completamente diferente.

Uma função de dispersão (função hash) é como uma máquina de códigos secretos. Recebe uma **mensagem** e transforma-a num código.



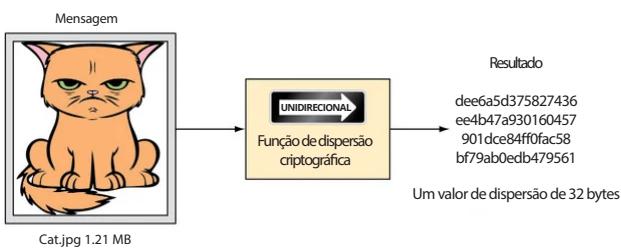
Uma introdução ao lado técnico do Bitcoin

O código é sempre igual para a mesma mensagem. Se fizeres alterações à mensagem, ainda que pequenas, o código muda completamente. Isto ajuda os computadores a memorizar informação e a verificar se houve alterações.

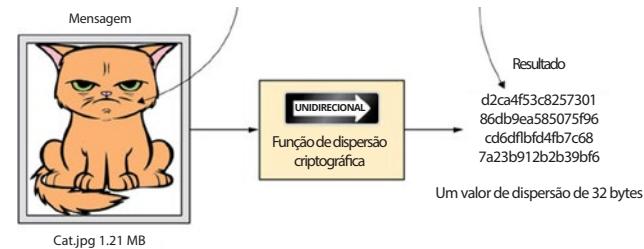


Gera instantaneamente um hash SHA256 de qualquer mensagem ou variável. As funções de hash são usadas como métodos unidirecionais.

Atividade - Gerar SHA256 →



Falta um bigode! Agora, já tem uma razão para estar maldisposto.



Completamente diferente do valor de dispersão anterior

O **resultado**, ou valor de dispersão (*hash*), tem sempre o mesmo tamanho, independentemente do tamanho da informação original (mensagem).

O Bitcoin usa **funções** de dispersão específicas chamadas **SHA256** e **RIPEMD160**.
Seguem-se alguns exemplos:

- 💡 Repara que uma pequena alteração na segunda mensagem altera completamente o resultado (hash), quando comparado com o primeiro.
- 💡 A terceira mensagem é um ficheiro enorme, mas o resultado tem o mesmo tamanho fixo que os outros.

- hash SHA256 da mensagem “**hello world**”
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- hash SHA256 da mensagem “**hello world**”
7ddb227315f423250fc67f3be69c544628dffef1752af91c50ae0a9c49faeb87
- hash SHA256 da mensagem que é o ficheiro **ISO Ubuntu 18.10**
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

Também podemos comparar a dispersão (*hashing*) a uma partitura musical que capta a essência de uma música. Tal como uma partitura musical é uma representação única de uma música, um valor de dispersão é uma representação única de um conjunto de dados. Ao comparar a partitura de uma música com a atuação, um músico consegue determinar se a atuação foi bem executada. Da mesma forma, ao comparar o valor de dispersão dos dados recebidos com o valor de dispersão original, é possível determinar se as informações foram alteradas durante a transmissão.

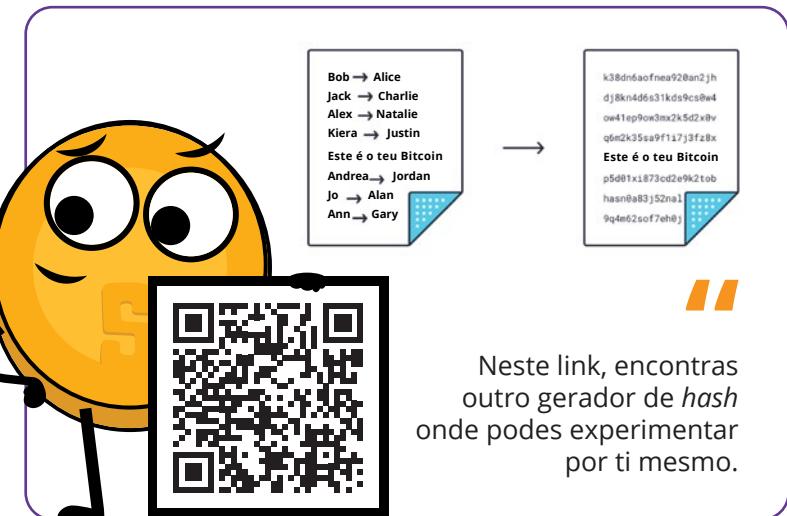




Capítulo #9

Numa atuação musical, uma pequena variação pode fazer com que a música soe diferente. De igual forma, até mesmo uma alteração minúscula aos dados originais resulta num valor de dispersão diferente. Isto faz da dispersão uma ferramenta poderosa para garantir a integridade e autenticidade de uma transação de bitcoin.

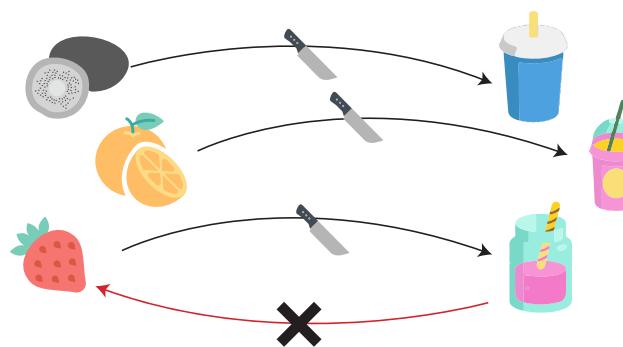
O processo de codificação da **chave pública** através da dispersão tem a função de aumentar a segurança das informações, ao convertê-las num formato de tamanho fixo e ilegível. O Bitcoin utiliza os algoritmos SHA256 e RIPEMD160 para produzir endereços públicos. O **resultado** serve de identificador único para a **chave pública** e ajuda a garantir a integridade e segurança das transações registadas no livro-razão. Esta forma de encriptação dificulta o acesso a informações, bem como a manipulação das mesmas por parte de pessoas não autorizadas.



Hashing

Uma função de *hash* pega em qualquer **variável** e gera um **resultado** de comprimento fixo (*hash*).

Ingredientes Função de Hash Batidos



Determinístico.

Os mesmos ingredientes geram sempre o mesmo batido.



Resistência a Pré-Imagens.

Não podes reconstruir um morango quando te dão um batido.



Resistência à Correlação.

Alterar ligeiramente os ingredientes resulta num batido completamente diferente.



Resistência a Colisões.

É difícil fazer dois batidos com ingredientes diferentes e terem exatamente o mesmo resultado.



Velocidade e Verificabilidade.

Coloca a fruta no misturador. É rápido e o que sai, com certeza, é um batido.

9.2 O modelo UTXO

UTXO é a sigla de *Unspent Transaction Output* (Saída de Transação Não Gasta)

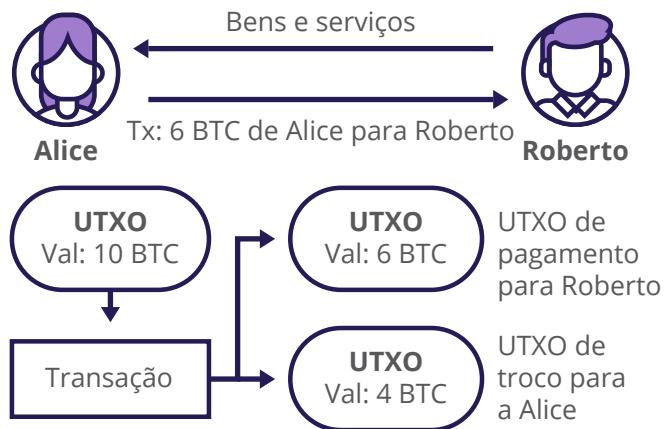


Uma introdução ao lado técnico do Bitcoin

O que são as UTXO?

As transações Bitcoin são processadas de uma certa forma, que é como se dividisse uma grande pepita de ouro em pepitas mais pequenas e as enviasse para outras pessoas e para si mesmo.

Imagina que os UTXO representam diferentes quantias de bitcoin, ou notas de diferentes denominações na tua carteira. Quando gastas um UTXO, este é transformado num novo UTXO para o destinatário, e o que sobra é-te devolvido na forma de um outro novo UTXO, conhecido como o UTXO de troco. É como usar uma nota de 10 € para comprar dois cafés por 6 €. O estabelecimento fica com 6 € e dá-te 4 € de troco.



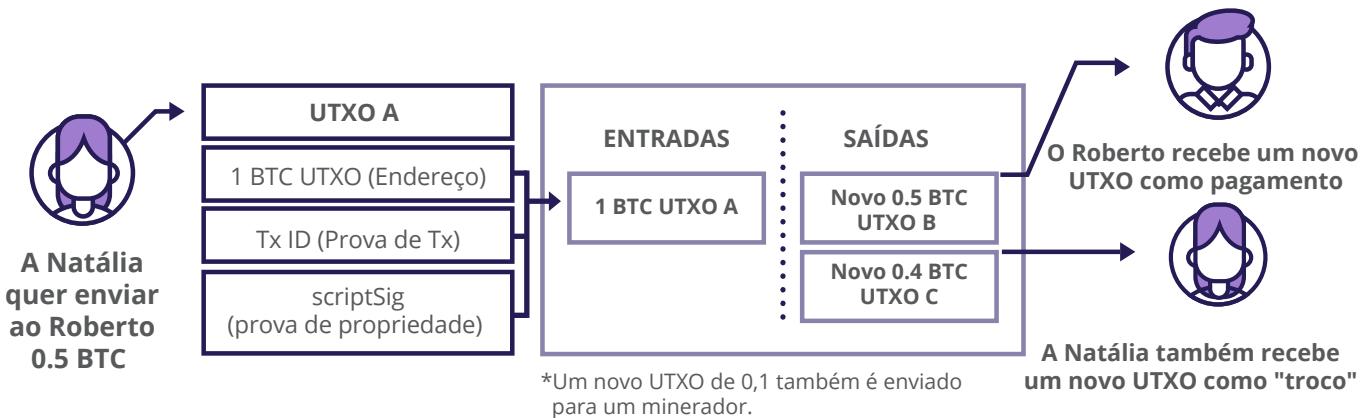
Quando envias bitcoin, envias sempre a quantidade total de um (ou vários) dos UTXO que tens na tua carteira Bitcoin. O que acontece? Envias uma quantia ao destinatário e recebes o valor restante como troco, num dos teus novos endereços Bitcoin. O troco que recebes chama-se saída de transação não gasta, ou UTXO, e pode ser usado como entrada para uma nova transação futura.

O saldo da tua carteira Bitcoin é a soma de todos os teus diferentes UTXO. Por isso, a soma dos teus UTXO equivale à quantia total de bitcoin que tens.



É de salientar que não deves divulgar informações relativas aos teus UTXO, porque, se alguém reconhecer os teus UTXO, consegue também seguir as tuas transações de bitcoin na rede e, consequentemente, saber quanto dinheiro tens.

Concluindo, sempre que fazes uma transação, utilizas um ou vários dos teus UTXO existentes para gastar bitcoin, e são emitidos novos UTXO (tanto para ti como para o destinatário).



Quando se faz uma transação, a quantidade de bitcoin que é enviada é dividida em várias saídas, cada uma das quais está associada a um novo endereço Bitcoin, o que representa um novo UTXO.

Capítulo #9

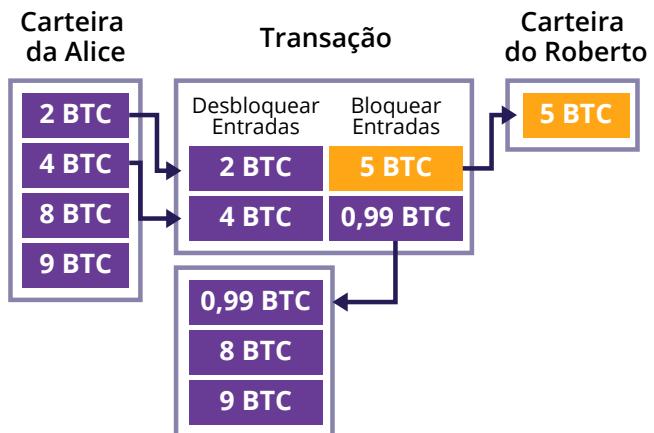
Quando envias bitcoin para alguém, usas um ou vários UTXO como origem dos fundos (entrada). Caso seja necessário, esses UTXO são acumulados para criar saídas que te pertencem a ti e ao destinatário da transação. Estas novas saídas (UTXO) tornam-se propriedade tua e do destinatário. Estes UTXO podem, depois, ser utilizados como origem dos fundos em transações futuras. Esta sequência de UTXO cria um histórico transparente e monitorizável de todas as transações de bitcoin no livro-razão do Bitcoin, desde o primeiro bloco (3 de janeiro de 2009).

Eis um exemplo que ilustra este processo: Se quiseres enviar 2 bitcoins, mas só tiveres um UTXO no valor de 5 bitcoins, a diferença de 3 bitcoins é-te devolvida na forma de "troco". Este "troco" é um novo UTXO teu, que podes gastar numa transação futura.

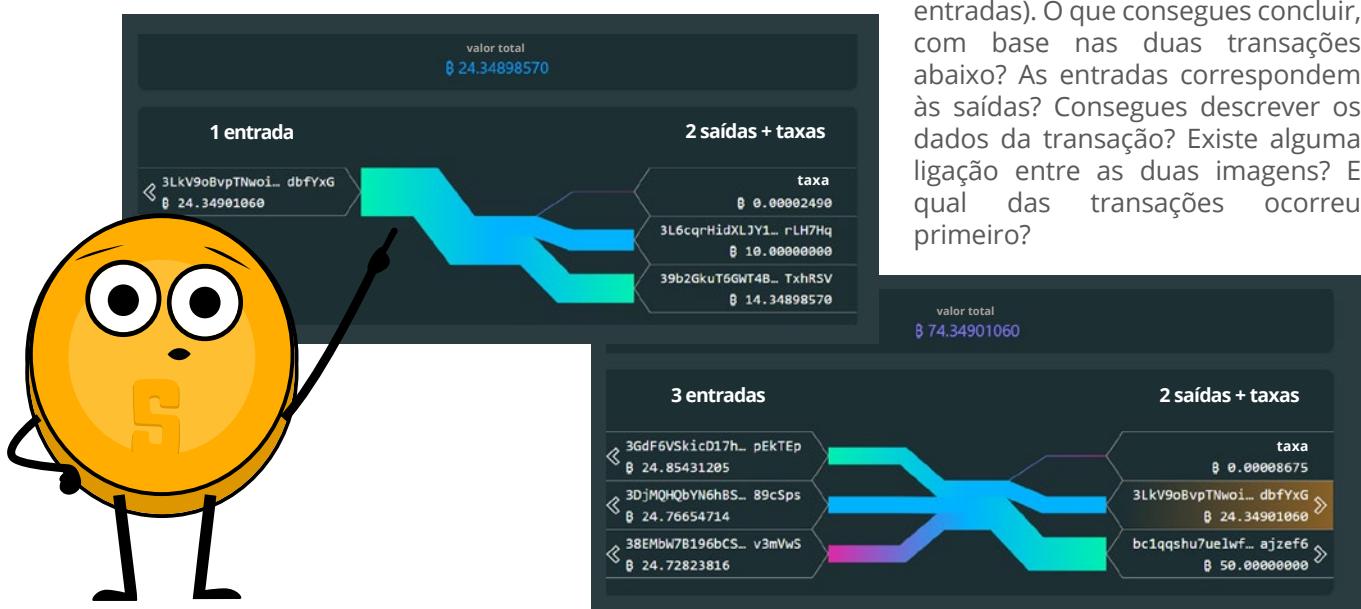
Outro exemplo:

- 1** A Alice quer enviar 5 bitcoins ao Roberto.
- 2** Ela reúne 6 bitcoins com dois dos seus UTXO.
- 3** Com estes UTXO, ela envia 5 bitcoins para o Roberto, recebe 0,99 bitcoins de troco, e tem de pagar uma taxa de transação de 0,01.
- 4** Após a confirmação, a transação é adicionada ao livro-razão do Bitcoin, para atualizar os registo de todos os nós que têm uma cópia do livro-razão.

Se a Alice tentar usar uma das suas saídas já gasta noutra transação, esta será automaticamente rejeitada pelos nós. Isto porque os nós mantêm uma cópia do livro-razão do Bitcoin (e de todas as suas transações), para que possam facilmente verificar o saldo de UTXO da Alice e confirmar que a transação não é válida.



Segue-se uma imagem de uma transação real, na qual há apenas uma entrada. No entanto, o saldo inicial poderia, noutros casos, ser a soma de vários UTXO (várias entradas). O que consegues concluir, com base nas duas transações abaixo? As entradas correspondem às saídas? Consegues descrever os dados da transação? Existe alguma ligação entre as duas imagens? E qual das transações ocorreu primeiro?



Uma introdução ao lado técnico do Bitcoin

9.3 Uma análise mais detalhada dos nós e mineradores de Bitcoin

Nesta secção, vamos analisar mais detalhadamente duas partes (e participantes) muito importantes da Rede Bitcoin, que foram mencionadas pela primeira vez no Capítulo 6. Vamos analisar:

Nós de Bitcoin:

1 Guardiões da Validação, cujas principais funções são guardar uma cópia do livro-razão do Bitcoin, certificar-se de que todas as transações são válidas e de que todos seguem as mesmas regras.

Ao dividir esta responsabilidade por muitas pessoas de todo o mundo, o Bitcoin mantém-se resistente a possíveis problemas. Estes nós ajudam a manter a confiança no sistema e a manter o mesmo fiel ao seu conceito descentralizado, no qual ninguém tem demasiado poder.

Mineradores de Bitcoin:

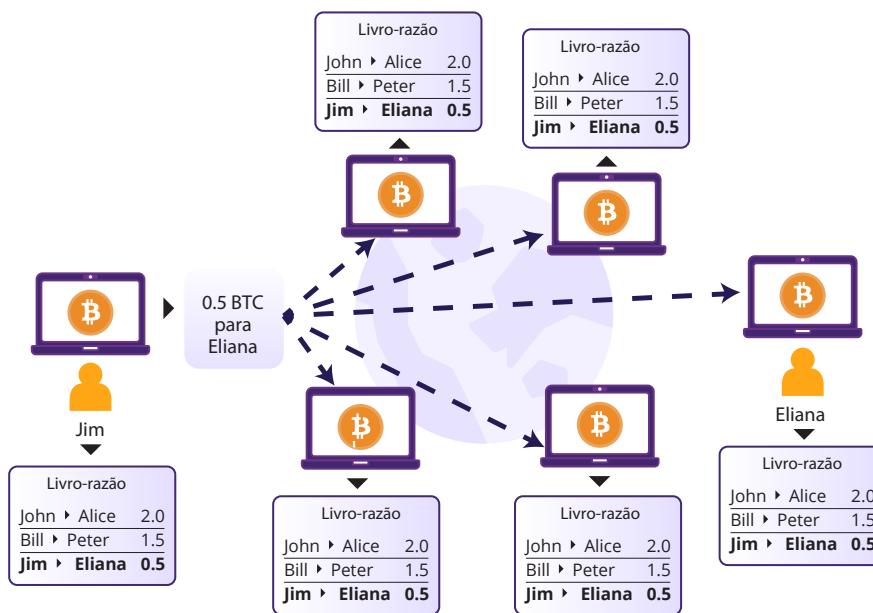
2 Arquitetos da Segurança, que utilizam eletricidade e computadores potentes para verificar e confirmar transações, por forma a garantir que tudo permanece em segurança. Este trabalho ajuda a tornar o livro-razão, ou a *blockchain*, resistente a quaisquer pessoas mal-intencionadas que tentem causar problemas.

Os nós e os mineradores de Bitcoin trabalham em conjunto para manter um sistema descentralizado, seguro e forte – uma nova forma de lidar com o dinheiro, na qual toda a gente pode confiar. Vamos analisar estas funções mais detalhadamente, para compreender a sua contribuição para o inovador sistema Bitcoin.

9.3.1 O que é um nó de Bitcoin e como posso configurar o meu próprio nó?

Um nó de Bitcoin pode parecer complicado, mas não passa de um software que contém uma cópia do livro-razão do Bitcoin. Se tiveres o teu próprio nó de Bitcoin, tens influência nas regras da rede Bitcoin.

Imagina o seguinte: Se um grupo de pessoas tentar alterar o funcionamento do Bitcoin (por exemplo, alterar a massa monetária do Bitcoin), a decisão também é tua. Podes optar por não atualizar o teu nó para o novo sistema, o que é equivalente a um voto teu nas regras da rede que estás a defender.



Imaginemos que os nós de Bitcoin são polícias de trânsito digitais, com algumas tarefas essenciais:

1

Guardiões da validação:

Um nó de Bitcoin guarda uma cópia digital da *blockchain*, que é um género de livro-razão partilhado que contém todas as transações de bitcoin. Existem muitos nós espalhados pelo mundo com o mesmo registo.

2

Centro de comunicações:

Os nós estão conectados uns aos outros, o que cria uma vasta rede de comunicações. Eles partilham informações, especialmente transações a aguardar a sua adição à *blockchain*, colocadas numa sala de espera digital chamada *mempool* (memória de transações).

3

Controlador de qualidade:

Todas as transações adicionadas à blockchain são analisadas. Os nós certificam-se de que as transações são válidas e rejeitam quaisquer transações que não cumpram as regras da rede Bitcoin.

4

Informador da *blockchain*:

Existem outros softwares, tais como carteiras, que podem solicitar aos nós informações da *blockchain*, tais como saldos de bitcoin. Os nós têm a função de centro de informações.

5

Apoio aos novos nós:

Quando um novo nó se quer juntar à rede, os nós existentes fornecem-lhe uma cópia da *blockchain*. O novo nó verifica, de forma independente, a validade de cada transação, o que destaca um sistema que não depende da confiança entre as partes.

Atividade: Vê o vídeo sobre os nós de Bitcoin



Uma das formas de teres o teu próprio nó é transferir o software Bitcoin Core e esperar algum tempo, para que o software descarregue a *blockchain* inteira. Quando estiver pronto, podes deixá-lo ativo e, aproximadamente a cada 10 minutos, surgem novos blocos com transações. O teu nó verifica a validade dos mesmos e adiciona-os à tua cópia local da *blockchain*.

Recurso: Software Bitcoin Core



Um nó dá ao seu proprietário soberania e independência. Não dependes de outras pessoas, pois tens o teu próprio polícia de trânsito. Ao contrário da tua carteira Bitcoin, que não tem uma cópia da *blockchain*, um nó dá-te autossuficiência. Em vez de confiar a outros o teu saldo de bitcoin (e o estado da rede Bitcoin), a tua carteira comunica com o teu próprio nó, o que torna a tua experiência digital mais segura e fiável.

9.3.2. O que é um minerador de Bitcoin e como funciona a mineração?



O objetivo da mineração não é criar bitcoin novo. Isso é apenas um incentivo. A mineração é o mecanismo através do qual a segurança do Bitcoin se torna descentralizada.

Andreas M. Antonopoulos



Uma introdução ao lado técnico do Bitcoin

Os **mineradores** recolhem transações não confirmadas, formam um bloco e gastam energia a procurar uma valiosa chave, que **adiciona e fixa o seu bloco à blockchain**.



Os mineradores competem para adicionar o bloco seguinte à *blockchain*. Todos eles procuram um valor de dispersão de bloco válido, muito bem escondido entre milhares de milhões de outros, e só uma chave específica atribuída pela rede o consegue desbloquear.

Imagina um enorme palheiro cheio de milhões de chaves, em que cada uma representa um valor de dispersão de bloco único. A rede elegeu uma chave específica para desbloquear uma valiosa recompensa. Os mineradores revistam o palheiro e testam cada chave que encontram na fechadura, mas só um minerador sortudo é que encontrará a correspondência certa.

Quando um minerador encontra o valor de dispersão de bloco correto, partilha-o com a rede, juntamente com o bloco que criou com novas transações. Os outros mineradores verificam a solução, para se certificarem que corresponde. Se estiver tudo certo, o bloco é adicionado à *blockchain*, o que ajuda a construir um livro-razão seguro e público.

Os mineradores ganham dois tipos de recompensa pelo seu trabalho:

- 1 Recompensas de bloco
- 2 Taxas de transação

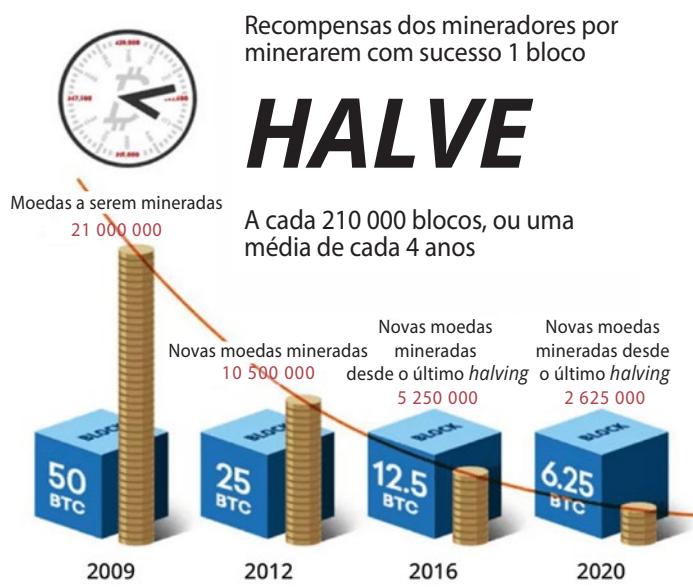
As recompensas de bloco são quantias de bitcoin novo, colocado em circulação a cada bloco que é adicionado à *blockchain*. As taxas de transação são pequenos pagamentos em bitcoin que os utilizadores fazem, para que o minerador priorize e acelere o processamento das suas transações. Os mineradores podem escolher as transações que vão incluir no bloco que mineram e, geralmente, dão prioridade às que têm as maiores taxas de transação.

Bitcoin halvings

Um *halving* é uma parte essencial do universo Bitcoin, que ajuda a manter a sua escassez e valor ao longo do tempo. Como já sabes, existe uma massa monetária total fixa de 21 000 000 de bitcoins. Esta massa monetária não ficou totalmente disponível no dia do lançamento do Bitcoin. Em vez disso, esta massa monetária entra no universo Bitcoin pouco a pouco.

Satoshi Nakamoto concebeu um engenhoso sistema de recompensas de bloco, por forma a distribuir bitcoin novo sem uma autoridade central. No início do Bitcoin, os mineradores recebiam uma ótima recompensa de 50 bitcoins por cada bloco que mineravam, o que os motivou a investir em eletricidade e equipamento de alta potência para as suas operações de mineração.

Para manter a rede estável e gerir a nova oferta de bitcoin, a recompensa de bloco é reduzida para metade a cada 210 000 blocos. Este evento, chamado *halving*, diminui a quantia de bitcoin novo que entra em circulação e continua a motivar os mineradores a proteger a rede e a manter a sua descentralização. Ao longo da sua história, os *halvings* já causaram aumentos significativos do preço de Bitcoin, devido à redução da oferta de bitcoin novo a entrar em circulação.



A oferta em circulação refere-se à quantia total de uma moeda. No caso do Bitcoin, a oferta total em circulação é o número de moedas que já foram mineradas e estão em circulação em dado momento, excluindo quaisquer moedas que estejam permanentemente perdidas.

A cada *halving*, os mineradores passam a receber menores recompensas de bitcoin, o que reduz a taxa de emissão de novas unidades. A redução das recompensas da mineração não significa necessariamente que os mineradores obtenham menos lucro, visto que também podem ganhar taxas de transação por verificar transações e adicioná-las à *blockchain*, o que pode compensar a diminuição das recompensas de mineração.

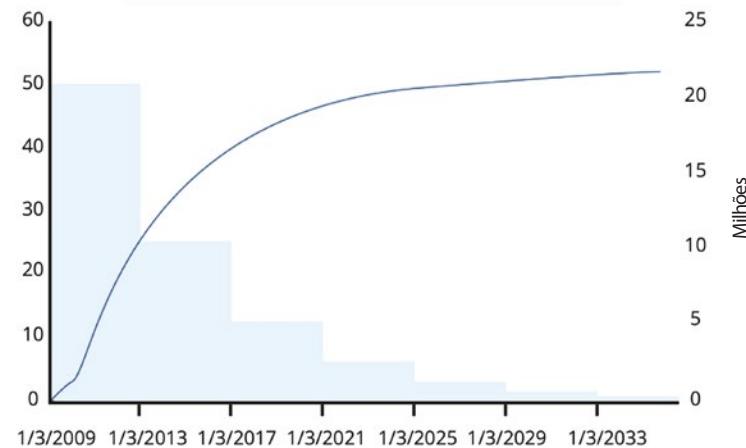
Os *halvings* estão pré-programados no protocolo Bitcoin, o que torna o plano de emissão do Bitcoin previsível e transparente.



O plano de emissão do Bitcoin é o plano pré-determinado e público da colocação de bitcoin novo em circulação, concebido para manter a escassez do Bitcoin ao longo do tempo.

A tabela que se segue contém os detalhes dos próximos *halvings* do Bitcoin, incluindo a data prevista do próximo *halving*, o número do bloco no qual o *halving* vai acontecer, as recompensas de bloco (por cada bloco minerado) durante esse *halving* e a percentagem da massa monetária total que ficará minerada.

Calendário de Emissão do Bitcoin



Evento	Data Esperada	Bloco	Recompensa do Bloco	Percentagem Minerada
Quarto Halving	2024	840 000	3,125	96,875 %
Quinto Halving	2028	1 050 000	1,5625	98,4375 %
Sexto Halving	2032	1 260 000	0,78125	99,21875 %

Uma introdução ao lado técnico do Bitcoin

À medida que se vai minerando mais bitcoin, a oferta em circulação e a percentagem da massa monetária total que já foi minera da continuarão a aumentar, até alcançar a massa monetária total de 21 000 000. A oferta reduzida, em conjunto com o aumento da procura, pode aumentar o preço do Bitcoin (em relação ao dólar). Isto beneficia os primeiros a adotar o Bitcoin e também motiva os mineradores a continuar a proteger a rede e a contribuir com a sua capacidade de computação e recursos.

Percentagem de BTC minerado (do total de 21M)

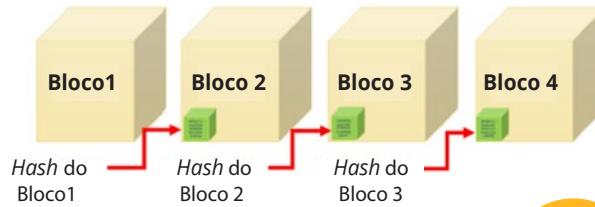


O que é um valor de dispersão de bloco (*hash*) válido no Bitcoin?

No Bitcoin, um valor de dispersão de bloco válido é um género de código especial que os mineradores tentam encontrar. É um número único que ajuda a manter o registo de cada bloco na blockchain que armazena informações sobre transações. Os blocos estão ligados uns aos outros numa cadeia, desde o primeiro (génesis) ao último, para formar um registo público de todas as transações. Este valor de dispersão de bloco é fundamental, pois é a ligação entre cada bloco e o bloco que o precedeu, o que faz com que seja fácil, para qualquer pessoa, verificar o histórico de transações. É um género de impressão digital para cada bloco e certifica que as informações estão corretas e seguras. O valor de dispersão de bloco é uma forma de confirmar que os dados presentes no bloco não foram alterados.



Os blocos estão "ligados" entre si ao impor uma relação específica entre eles. Ou seja, um bloco deve conter uma "impressão digital", que é o valor *hash* (ou valor de dispersão) dos dados do bloco anterior. Uma função de *hash* pode condensar uma mensagem arbitrária (as informações do bloco) num tamanho fixo (por exemplo, 160 bits) e produzir uma impressão digital da mensagem.



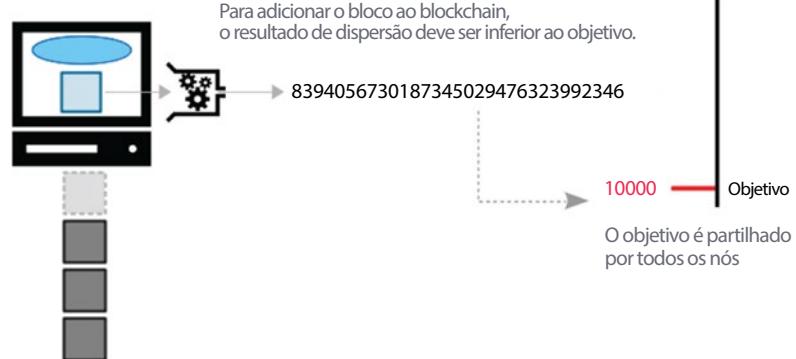
Foi Satoshi Nakamoto, o criador do Bitcoin, que minerou o bloco original, que tinha um total de 50 bitcoins.



A competição para minerar um bloco

Os mineradores competem entre si para descobrir o valor de dispersão de bloco (*hash*) que corresponde ao objetivo (um número especial) definido pela rede. O primeiro minerador a descobrir o valor de dispersão de bloco correto tem a oportunidade de adicionar esse bloco à *blockchain* e de lhe atribuir um ID de valor de dispersão correspondente. Esta solução tem a função de validar a autenticidade do bloco.

A mineração pode ser comparada a uma corrida na qual o objetivo é chegar à meta o mais rapidamente possível. A dificuldade em encontrar o valor de dispersão do bloco é ajustada periodicamente, para garantir que a mineração de cada bloco continua a demorar cerca de 10 minutos (tendo em conta os mineradores que se juntam ou que abandonam a rede). Este mecanismo chama-se ajuste da dificuldade.



Digamos que o número definido pela rede Bitcoin como o objetivo é 1 000. Os mineradores teriam de usar energia e a sua capacidade de computação para procurar um valor de dispersão de bloco (um número específico) inferior a 1 000. O primeiro minerador a encontrar um valor de dispersão de bloco inferior a 1000 consegue adicionar o novo bloco à *blockchain* e é recompensado com bitcoin.

O nível de dificuldade da mineração do Bitcoin é a dificuldade em encontrar um valor de dispersão de bloco válido que corresponda ao objetivo definido pela rede. É ajustado a cada 2 016 blocos, ou aproximadamente a cada duas semanas, para garantir que os blocos são adicionados à *blockchain* a uma velocidade constante. O nível de dificuldade é expresso na forma de um número e, quanto maior for o nível de dificuldade, mais difícil é encontrar um valor de dispersão de bloco válido.



Por exemplo, vê os dois valores de dispersão diferentes que se seguem:

Hash 1: 0000A1mINgF0RbL0cK5wltHth3hAy5tAck
Nível de dificuldade: 1

Hash 2: 00000000A1mINgF0RbL0cK5wltHth3hAy5tAck
Nível de dificuldade: 2

Neste exemplo, o *Hash 2* tem um nível de dificuldade mais alto do que o *Hash 1*, porque é um valor de dispersão maior e com mais zeros no início. Para um minerador, seria mais difícil encontrar o *Hash 2*, pois requer mais trabalho de computação.

Ao encontrar um valor de dispersão de bloco válido, o minerador demonstra que fez o trabalho exigido para adicionar o novo bloco à *blockchain* e é recompensado pelo seu trabalho com bitcoin e taxas de transação. O *Proof-of-Work (PoW)* é o método que a rede Bitcoin usa para validar transações e adicionar novos blocos à *blockchain*.



Uma introdução ao lado técnico do Bitcoin

O PoW mantém o Bitcoin seguro, pois torna difícil, para alguém com más intenções, assumir o controlo.

Resumindo, as funções dos mineradores são:

1 Agrupar transações em blocos:

Enquanto os nós verificam as novas transações que estão em espera na memória de transações (*mempool*), os mineradores selecionam um subconjunto destas transações para incluir no bloco candidato.

2 Proof-of-work:

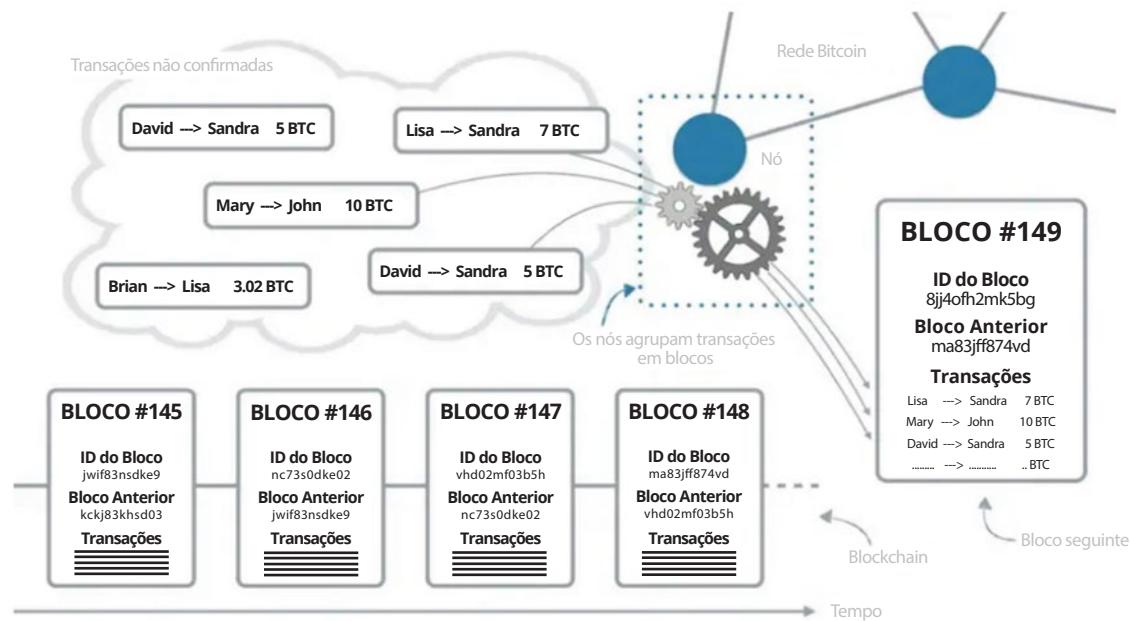
Os mineradores competem entre si para encontrar o valor de dispersão (*hash*) de bloco válido.

3 Transmitir blocos válidos:

Após encontrar o valor de dispersão de bloco válido, partilham o novo bloco com a rede.

4 Receber recompensas:

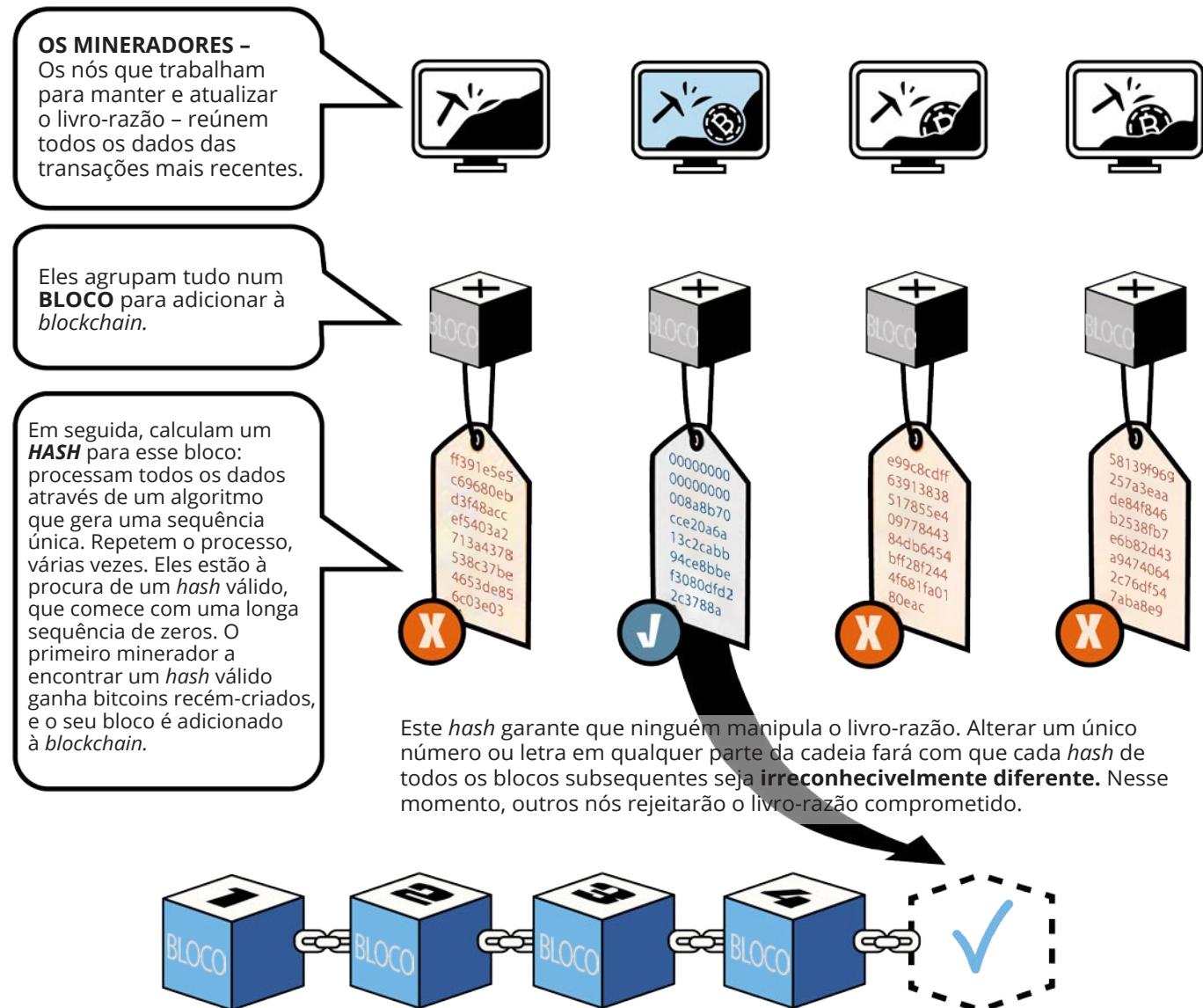
Por fim, recebem bitcoin novo e taxas de transação por adicionar corretamente o bloco à *blockchain*.



Pode haver vários mineradores a criar blocos ao mesmo tempo. O primeiro minerador a descobrir um valor de dispersão de bloco que corresponda ao objetivo definido pela rede partilha-o com a rede. Os nós verificam as transações do bloco candidato desse minerador, para garantir que são válidas. Se se comprovar que as transações são válidas, o bloco é adicionado à blockchain. Os outros blocos, que foram criados por outros mineradores, não são adicionados e são eliminados. Este processo ajuda a manter o consenso dentro da rede e evita gastos duplos.

Um **bloco candidato** é um conjunto de transações que poderá vir a ser adicionado à *blockchain*, mas que ainda não o foi.





9.4 O que é a *mempool* (memória de transações)

A *mempool*, ou memória de transações, é uma espécie de sala de espera para transações, na rede Bitcoin. Quando se faz uma transação, esta é transmitida para a memória de transações, antes de ser verificada, selecionada e adicionada à *blockchain*.

Imagina que estás numa fila para entrar num restaurante. O teu nome é adicionado à lista de pessoas que estão à espera de uma mesa. Quando houver uma mesa disponível, o empregado chama-te e leva-te à tua mesa. Da mesma forma, quando se cria uma transação de bitcoin, a mesma é adicionada à memória de transações e, quando um minerador a inclui num bloco, a transação é confirmada e adicionada à *blockchain*.

Uma introdução ao lado técnico do Bitcoin

Uma **mempool** é o local onde as transações aguardam para serem confirmadas num bloco.

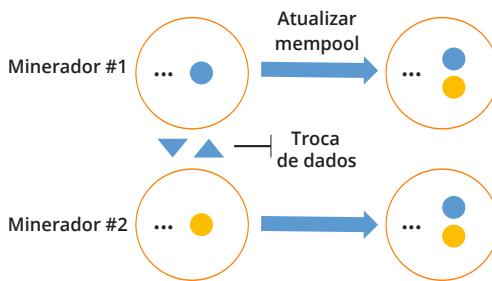
- tx hsh 6053b699...
taxa de transação: 3 sat/vB
- tx hsh bb3b8clfc...
taxa de transação: 1 sat/vB
- tx hsh d7c2532a9...
taxa de transação: 15 sat/vB
- tx hsh 0ecdd9c6...
taxa de transação: 2 sat/vB



Quando um nó recebe pela primeira vez uma transação de um par, tem de verificar se a transação é legítima. Ninguém quer transações defeituosas ou enganosas.



A **sincronização da mempool** permite que os nós partilhem as suas transações com outros nós, ao enviar uma mensagem que contém uma lista de transações **verificadas** na mempool.



O principal objetivo da **mempool** é:

1

Reencaminhar transações não confirmadas.



2

Fornecer aos mineradores transações para serem mineradas.



A **Aceitação na Mempool (ATMP - Accept to Memory Pool)** envolve a verificação de aspectos como:

- Já tenho esta transação?
Existe algum conflito com outra transação na mempool?
- O **bitcoin** que entra cobre o **bitcoin** que sai?
- As assinaturas provam que as saídas anteriores podem ser gastas?
- Há taxas suficientes?

Como é que as transações são verificadas e adicionadas à Memória de Transações?

Quando as transações criadas são transmitidas para a rede Bitcoin, os nós verificam estas transações, para garantir que são válidas e que o respetivo saldo ainda não foi gasto. Quando estas transações estiverem verificadas, os nós adicionam-nas à sua mempool. Depois, os nós partilham as transações com outros nós, para se fazer uma nova verificação. Por fim, se a maioria dos nós concordar, as transações ficam disponíveis para os mineradores, para as selecionar e incluir num bloco. No entanto, existem vários motivos pelos quais uma transação pode não ficar confirmada num prazo de 72 horas:

Taxas de transação baixas:

1

As transações com taxas baixas podem não ser processadas suficientemente rápido, tendo em conta que os mineradores tendem a incluir transações com taxas mais altas nos seus blocos.

2

Congestionamento da rede:

Se a rede estiver congestionada, pode haver atrasos na confirmação de transações, ainda que tenham taxas altas.

3

Tentativa de gasto duplo:

Se alguém tentar fazer um gasto duplo, a respetiva transação pode ser rejeitada pela rede.

4

Dados incorretos ou incompletos:

Se uma transação contiver dados incorretos ou incompletos, pode ser rejeitada pela rede.

5

Transação malformada:

Se uma transação for malformada, pode ser rejeitada pela rede.

Para evitar que as transações sejam rejeitadas, recomenda-se incluir uma taxa suficientemente alta, para garantir que a transação é processada rapidamente, e verificar várias vezes se todos os dados da transação estão corretos, antes de a enviar.

Atividade: *Mempool (memória de transações)*

1

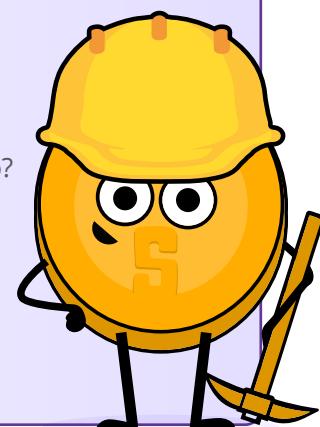
Lê o seguinte código QR :

2

Analisa os vários elementos visíveis na página, incluindo os blocos mais recentes, as transações confirmadas, o número de transações, a utilização da memória e o valor aproximado do bloco inteiro.
Responde às seguintes questões:



- 💡 Qual foi o último bloco minerado?
- 💡 Quantas transações foram incluídas nesse bloco?
- 💡 Qual é a quantia total transacionada em bitcoin?
- 💡 Qual era o tamanho do bloco, em megabytes?
- 💡 Quantos zeros estão no início do número aleatório (nonce) do bloco?
- 💡 Quantos bitcoins é que o minerador ganhou no total?
- 💡 Qual foi o valor total das taxas recebidas pelo minerador, por adicionar as transações à rede?
- 💡 Escolhe uma das transações de maior valor do bloco. Para quantos endereços Bitcoin foi distribuído o respetivo montante?



Uma introdução ao lado técnico do Bitcoin

9.5 O processo completo das transações Bitcoin

1

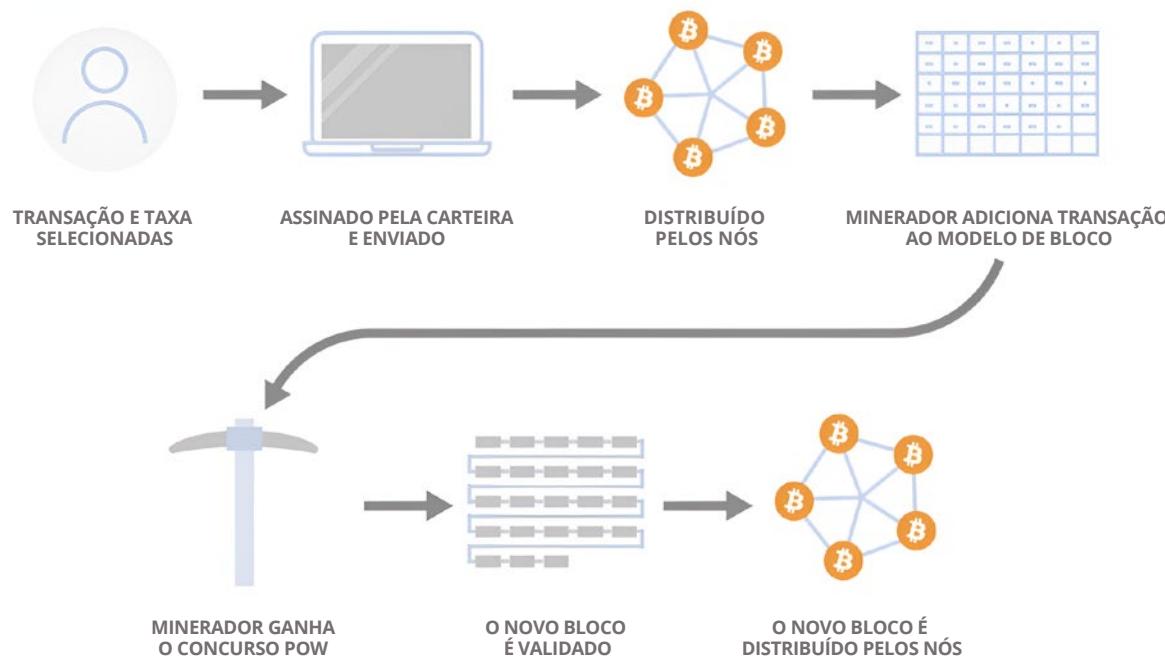
O André quer enviar bitcoin para o Gonçalo. Ele escolhe um dos seus UTXO, cria uma transação e adiciona todos os dados necessários, incluindo a quantia de bitcoin que pretende enviar, o endereço de destino do Gonçalo e uma taxa de transação acima da média.

2

Após fazer uma verificação final e confirmar que todos os detalhes estão corretos, o André usa a sua chave privada para assinar a transação.

3

O André transmite a transação para a rede Bitcoin.



Origem: Ted Stevenot: "What is a bitcoin node and how does one work?". Unchained Capital, 17 de janeiro de 2023, <https://unchained.com/blog/what-is-a-bitcoin-node/>

4

Os nós da rede recebem a transação e verificam a sua validade, de acordo com as regras de consenso (por exemplo, verificam se a assinatura do André é válida e se ele tem saldo suficiente para fazer a transação).

5

A transação é marcada como válida, e os nós partilham-na com outros nós da rede, ao adicioná-la à mempool (memória de transações).

6

Tendo em conta que o André incluiu uma taxa de transação alta, quase todos os mineradores incluem esta transação nos seus blocos.

7

Proof-of-Work: Cada minerador compete para minerar o seu bloco, ao procurar um valor de dispersão de bloco válido (*hash*). Um dos mineradores encontra o *hash* e partilha o seu bloco com a rede.

8

Os nós recebem o novo bloco e verificam a validade do mesmo. Isto envolve a validação de todas as transações incluídas no bloco e a confirmação de que foi cumprido o requisito de *Proof-of-Work*.

9

A maioria dos nós concorda que o bloco é válido e adiciona-o à *blockchain*. O Gonçalo recebe o bitcoin confirmado no seu endereço de destino.

10

Durante a hora seguinte, com a adição de mais blocos à *blockchain*, o número de confirmações desta transação aumenta. Com o aumento do número de confirmações desta transação, o Gonçalo fica mais confiante de que a transação foi corretamente processada e é irreversível.



Resumindo, o remetente assina a transação com a sua chave privada, os nós verificam os UTXO da transação, e os mineradores adicionam a transação verificada à *blockchain*. Depois, o destinatário consegue aceder ao bitcoin com a sua chave privada. Quando um bloco é minerado, todas as transações nele incluídas são consideradas confirmadas, e os UTXO utilizados como entradas nessas transações são consideradas gastos e não podem ser utilizadas novamente.

Chegámos ao fim deste capítulo, e obtiveste informações valiosas sobre os conceitos fundamentais do funcionamento do Bitcoin. Abordámos aspetos essenciais, desde os conceitos básicos do dinheiro ao lado técnico da tecnologia Bitcoin. Agora, vamos juntar tudo o que aprendestes no próximo capítulo. Segue-se o Capítulo 10, onde vamos aprofundar uma questão muito importante: “Porquê o Bitcoin?”

Capítulo #10

Porquê o Bitcoin?

10.0 Introdução

Atividade - Como seria um futuro Bitcoin?

10.1 O que são Moedas Digitais do Banco Central (CBDC) e quem as controla?

10.2 A filosofia do Bitcoin

Atividade - Debate de turma - Será que temos o direito de controlar o nosso próprio dinheiro?

10.3 Os benefícios do Bitcoin

10.4 Um futuro capacitado

Atividade - Debate de turma - Em que medida mudaste a tua perspetiva?

Porquê o Bitcoin?

10.0 Introdução

O Bitcoin é mais do que uma moeda; é uma revolução que devolve o poder ao povo e oferece paz e liberdade, num mundo que anseia por empoderamento.

My First Bitcoin

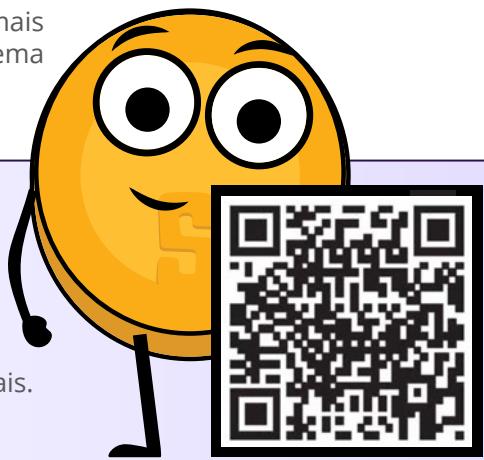
Neste último capítulo, vamos resumir o que aprendeste ao longo deste curso, vamos colocar e debater algumas questões importantes e analisar o futuro do Bitcoin.

O Bitcoin é mais do que uma tecnologia. É um tipo de rede que dá vida a uma nova forma de dinheiro, na qual nenhuma entidade tem o poder de alterar a respetiva massa monetária. A humanidade nunca teve uma forma de dinheiro com uma massa monetária fixa e sem um controlo centralizado. Se for amplamente adotado, o Bitcoin é uma ferramenta que possibilita um movimento de mudança positiva, capaz de transformar as vidas das pessoas no mundo inteiro. Representa uma revolução pacífica em direção à liberdade e igualdade coletiva e, com a criação de um sistema monetário global partilhado, traz consigo novas oportunidades para a humanidade.

Como sistema global descentralizado, o Bitcoin permite uma maior liberdade financeira, ao transferir o poder das elites para a maioria. Oferece uma plataforma segura e resistente à censura, para armazenar e transferir valor, o que dá às pessoas o poder de assumir o controlo do seu dinheiro e proteger o seu poder de compra. Isto é ainda mais importante no atual clima de instabilidade económica, onde o sistema financeiro tradicional enfrenta dificuldades sem precedentes.

Atividade: Vê o seguinte vídeo

As possibilidades de mudança positiva são imensas, e é por isso que te convidamos a assistir a este vídeo para saber mais.



Em seguida, vamos analisar outra forma de moeda digital chamada Moeda Digital do Banco Central (CBDC) e avaliar as semelhanças e diferenças entre a mesma e o Bitcoin.



Capítulo #10

10.1 O que são Moedas Digitais do Banco Central (CBDC) e quem as controla?

As Moedas Digitais do Banco Central (ou CBDC) são versões digitais do dinheiro fiduciário normal. As CBDC seguem as mesmas regras que o dinheiro fiduciário normal, ou seja, há uma autoridade central (como o governo) que tem o poder de criar mais dinheiro e, consequentemente, de reduzir o poder de compra das pessoas. No entanto, as CBDC também dão aos governos novas e poderosas ferramentas para controlar a utilização desse dinheiro por parte das pessoas no mundo inteiro.

De acordo com o estudo da Fundação dos Direitos Humanos (*HRF- Human Rights Foundation*), 119 dos 193 governos do mundo todo estão a investigar, a testar ou a usar CBDC.

Podes verificar se o teu país está a testar CBDC no localizador de CBDC da Fundação dos Direitos Humanos, no site <https://cbdctracker.hrf.org/home> or <https://cbdctracker.org/>

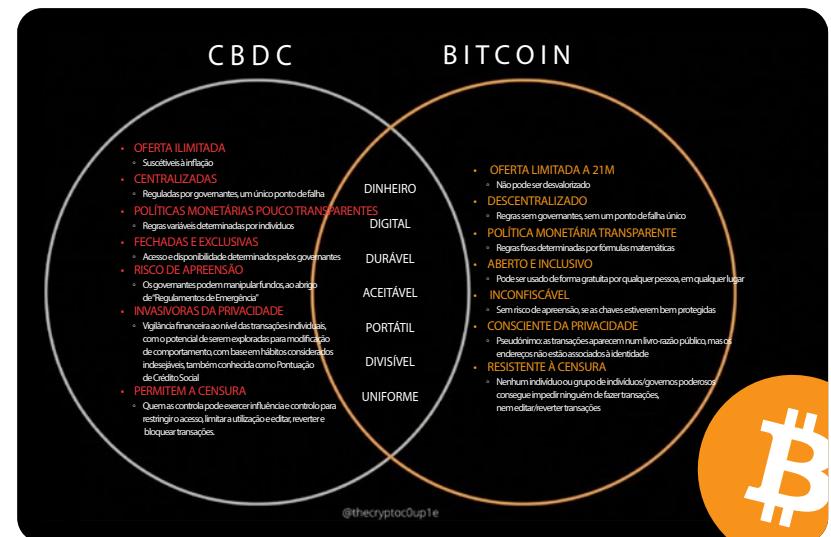
Então, o que é que torna as CBDC diferentes do dinheiro fiduciário normal, para além do facto de serem digitais? É muito importante entender que, ao contrário do dinheiro fiduciário normal na forma de papel ou moedas, as CBDC permitem ao governo ver e controlar digitalmente todas as transações a nível global. Isto significa que o governo pode impedir determinadas transações ou até mesmo congelar por completo a tua conta, se eles não gostarem de ti ou da forma como estás a usar o teu dinheiro.



Por exemplo, imagina que queres enviar dinheiro a um familiar que precisa de ajuda e que vive num determinado país, mas o teu governo local rejeita a tua transação, porque não concorda com os líderes desse país. Ou imagina que vais a uma loja para comprar algo de que gostas, mas não consegues, porque expressaste a tua opinião nas redes sociais.

As CBDC dão aos governos um poder ilimitado para controlar a forma como o dinheiro é utilizado em todo o mundo, o que limita a capacidade dos indivíduos de gastar o dinheiro com base nas suas próprias decisões. Até já se argumentou que as CBDC permitiriam aos governos mais poderosos aplicar centralmente políticas tirânicas a uma escala global, sem a necessidade de intervenientes humanos para as impor bastaria carregar num botão.

As CBDC e o Bitcoin são ambos digitais. Mas, à exceção desta semelhança, representam formas muito diferentes de dinheiro, com filosofias distintas e com resultados diferentes para a humanidade.



Porquê o Bitcoin?

10.2 A filosofia do Bitcoin

Nos capítulos 6 e 9, descobrimos que os indivíduos que operam um nó ajudam a proteger as regras do Bitcoin. Isto é muito importante, porque, pela primeira vez na História, qualquer pessoa pode fazer parte de uma equipa que contribui para a proteção das regras do nosso sistema monetário. Estas regras incluem o facto de haver apenas uma quantia limitada de bitcoin, e não existe nenhuma entidade capaz de alterar estas regras. É uma grande oportunidade para o cidadão comum de ajudar a manter a segurança e fiabilidade do nosso dinheiro.

A filosofia do Bitcoin é a de capacitação, liberdade, independência financeira e pensamento crítico. E o conceito do Bitcoin é o de que todos devemos ter poder de decisão, em relação às regras do sistema que escolhemos utilizar. Ao contrário do sistema fiduciário, controlado por entidades centrais poderosas, o Bitcoin funciona numa rede onde nenhuma entidade detém o controlo absoluto. Isto significa que, ao contrário de outros tipos de dinheiro como as CBDC, ninguém tem o poder de apreender o que é teu, nem de te impedir de gastar o teu dinheiro como quiseres.

No mundo fiduciário, quanto mais riqueza se acumula, mais influência e controlo se tem. Por outro lado, o funcionamento do Bitcoin foi concebido para dar poder ao povo. É um trabalho de equipa, no qual toda a gente desempenha um papel importante no sistema, independentemente do dinheiro que têm. É como uma força coletiva, onde o estatuto financeiro de uma pessoa não lhe dá automaticamente um controlo sobre tudo. O Bitcoin foi concebido com regras inalteráveis. Com tal harmonia, é como se o sistema estivesse sob o controlo de toda a humanidade. Não são só alguns magnatas a ditar as regras. Todos nós trabalhamos em conjunto, como uma comunidade resiliente, para moldar o futuro do Bitcoin, sem ter qualquer autoridade a mandar em nós.

No sistema fiduciário, são os poderosos que ditam as regras. Contrariamente, no ecossistema Bitcoin, é a força coletiva dos indivíduos que sustenta a rede. Não há nenhuma entidade, rica ou pobre, que possa ditar o futuro do ecossistema Bitcoin. É uma inversão da dinâmica de poder tradicional, onde a resiliência do sistema não está nas mãos das elites, mas sim no poder coletivo de cada participante.

O objetivo principal é criar um sistema seguro, transparente e justo, onde todos têm o mesmo acesso ao dinheiro a nível global.

Atividade – Debate de turma – Será que temos o direito de controlar o nosso próprio dinheiro?

- 1** Será o dinheiro uma necessidade e um direito humano? Porquê?
- 2** Se não consegues gastar o teu dinheiro como bem entenderes, enviá-lo para quem quiseres ou levá-lo contigo para um novo país, será que o dinheiro é mesmo teu? Porquê?
- 3** Porque é que se deixou de usar a troca direta? Qual é o problema da coincidência de vontades?
- 4** Que evento histórico teve mais impacto para ti? Porque é importante compreender o choque Nixon e a sua relevância para todos no mundo atual?
- 5** Qual é a diferença entre uma moeda com uma massa monetária fixa e as moedas fiduciárias tradicionais?



Capítulo #10

- 6** Quando é que foi criado o Bitcoin? Quem o criou? Qual era o seu objetivo e como é que esse objetivo define o conceito de um sistema descentralizado?
- 7** Qual é a diferença entre uma carteira custodial e uma carteira não-custodial? Qual é a tua carteira favorita?
- 8** O que é que sabes acerca da rede Lightning? Para que tipo de transações a utilizarias?
- 9** Como é que o facto de teres o teu próprio nó ajuda a rede?
- 10** Como é que o controlo do teu próprio dinheiro te capacita no teu dia a dia e no teu planeamento do futuro?
- 11** De que formas pode a liberdade financeira aumentar a tua capacidade de contribuir de forma positiva para a tua comunidade ou sociedade?

10.3 Os benefícios do Bitcoin

A “hiperbitcoinização” é um futuro teórico, no qual o Bitcoin se torna o sistema monetário dominante a nível global. Isto significa que o bitcoin seria usado por todos, em todo o lado e para tudo, fosse para pagar um café, as contas ou até mesmo para comprar uma casa.

O crescente interesse das pessoas, empresas, países e governos no Bitcoin destaca o possível impacto da sua adoção generalizada na economia e na sociedade. Estes são alguns dos benefícios de um mundo hiperbitcoinizado:

- 1 Um futuro soberano:**
Num futuro soberano, todas as pessoas do mundo têm o controlo absoluto da sua própria identidade e ativos digitais. Isto poderá trazer uma maior liberdade, privacidade, segurança e inclusão financeira, e, consequentemente, contribuir para um maior desenvolvimento, abundância e felicidade em geral.
- 2 Uma reserva de valor fiável:**
A escassez digital do Bitcoin torna-o uma reserva de valor fiável, o que pode incentivar mais pessoas a usá-lo como forma de poupar para o futuro.
- 3 Alterações nas políticas monetárias:**
Se o Bitcoin fosse amplamente adotado, conseguiria retirar a capacidade dos governos de usar instrumentos de política monetária tradicionais para controlar a massa monetária. A adoção em massa do Bitcoin teria o potencial de aumentar o poder de compra das pessoas e incentivaria a sociedade a adotar atividades de preferência temporal baixa.
- 4 Maior transparência e monitorização:**
O registo inviolável e imutável de todas as transações da *blockchain* pode aumentar a transparência e a responsabilização em várias indústrias e setores. Atualmente, as entidades poderosas conseguem desviar biliões de euros em todo o mundo, sem haver transparência em relação ao destino destes fundos ou a forma como são utilizados. Ao disponibilizar um registo aberto e verificável de transações financeiras, o Bitcoin consegue garantir que os movimentos de capital se tornam mais contabilizáveis e acessíveis ao público.

Porquê o Bitcoin?

Uma revolução no mercado de remessas:

5

O mercado de remessas envolve a transferência de dinheiro de uma pessoa para outra e, muitas vezes, atravessam fronteiras internacionais. Apesar da redução dos custos, as remessas continuam a ser relativamente caras, em comparação com as transferências bancárias nacionais, especialmente quando se trata de quantias mais pequenas. A rede Lightning permite transações rápidas e de baixo custo, o que a torna adequada para o mercado de remessas, e aborda os altos custos e outros inconvenientes associados às remessas, tais como os longos tempos de liquidação e as restrições ao horário de funcionamento.

6

Quando existe muita energia acessível, as sociedades têm um bom desempenho e muitas das suas indústrias e comunidades conseguem satisfazer a crescente necessidade de energia em casas, empresas e novas tecnologias. A mineração do Bitcoin incentiva os mineradores a usar energia excedente de fontes de energia sustentáveis, como a energia solar, eólica e hidroelétrica, energia essa que é geralmente desperdiçada. Os mineradores do Bitcoin usam essa energia excedente para criar mais bitcoin, através da mineração, e para proteger a rede. E devolvem o excesso de energia que criam à rede energética que a sociedade usa quando precisa.

10.4 Um futuro capacitado

Bitcoin é dinheiro.

O dinheiro ajuda as pessoas a comunicar as suas preferências, em relação a atividades, bens e serviços. Como vimos neste curso, quando o dinheiro é controlado por autoridades centralizadas, acaba sempre por ser manipulado.

Um dos erros que a humanidade sempre cometeu e continua a repetir é a manipulação do dinheiro, que, por sua vez, tem um impacto negativo nas pessoas, famílias, empresas, governos e, em última análise, na prosperidade da população mundial.

Ao tirar o controlo das entidades centralizadas sobre o dinheiro e ao utilizar dinheiro com uma massa monetária fixa inalterável, criamos um mundo diferente. Um mundo no qual não temos de confiar que alguém tomará decisões acertadas, mas sim onde as pessoas não têm a possibilidade de tomar más decisões.

Este é um mundo fundamentalmente diferente.

E vocês, caros estudantes, podem contribuir para a criação deste mundo. Ao usar o Bitcoin, ao ter os vossos próprios nós e ao ajudar os outros a entender melhor o futuro do dinheiro, estão a votar num mundo diferente.



Capítulo #10

Atividade: Debate final de turma - Em que medida mudaste a tua perspetiva?

Responde às 5 perguntas que se seguem:

Porque é que precisamos de dinheiro?

O que é o dinheiro?

Porquê o Bitcoin?

Quem controla o dinheiro?

O que dá “valor” ao dinheiro?



Capítulo #10

Escreve as questões colocadas pelos alunos que foram selecionadas no Capítulo 1 e responde-as.

- 1** Volta à primeira atividade do capítulo 1 e compara as tuas novas respostas com as que deste antes.
- 2** Compara e debate as respostas e perguntas originais. Mudou alguma coisa?
- 3** Pensa nesta questão final: Qual será o teu próximo passo? E como poderás usar estes novos conhecimentos para te capacitares?



Se estiveres pronto para dar o próximo passo, consulta a secção de recursos adicionais que se segue, na qual seleccionámos os melhores materiais para uma aprendizagem e sucesso futuros.

Recursos Adicionais

1. Porquê usar bitcoin?

a Boyapati, V., The Bullish Case for Bitcoin:

Este artigo explica o que faz do Bitcoin um ativo valioso e o que lhe dá o potencial de se tornar uma moeda dominante a nível global. O autor aborda os aspectos técnicos e económicos do Bitcoin que fazem do mesmo uma forte oportunidade de investimento.

b Svetski, A., Why Bitcoin Matters (1 hora):

Este vídeo fala da importância do Bitcoin como ativo digital descentralizado e do seu impacto no sistema financeiro atual. O orador fala do potencial que o Bitcoin tem de trazer liberdade financeira a pessoas de todo o mundo.

c Wiz, "Why Bitcoin":

Este artigo apresenta uma visão geral dos benefícios de usar o Bitcoin como moeda e reserva de valor. Destaca a natureza descentralizada do Bitcoin e a forma como permite uma maior liberdade e segurança financeira.

2. O que é o Bitcoin?

a CuriousInventor, "How Bitcoin Works Under the Hood":

<https://www.youtube.com/watch?v=Lx9zgZCMqXE> Este vídeo contém uma explicação detalhada dos aspectos técnicos e funcionamento do Bitcoin.

b Walker, G., What Is Bitcoin:

Este artigo contém uma explicação abrangente daquilo em que consiste o bitcoin, incluindo a sua história, tecnologia e diferenças entre o mesmo e as moedas tradicionais.

c RT, Bitcoin - The Genesis (30 minutos):

Este vídeo aborda a criação do Bitcoin e a sua fase inicial. Fala das motivações do seu misterioso criador Satoshi Nakamoto e da evolução do conceito do Bitcoin.

3. Aprendizagem contínua:

a The Bitcoin Standard (1 hora e 40 minutos):

Este audiolivro aborda o contexto económico e histórico que levou à criação do Bitcoin. Abrange os benefícios de uma moeda descentralizada e o potencial que o Bitcoin tem de se tornar um padrão global.

c Wambui, N., Bitcoin Babies:

by Naomi Wambui - <https://bitcoinbabies.com/>
Twitter: @btcbabies - @ngachanaomi1

Um recurso gratuito em formato PDF, que visa capacitar mães com conhecimentos essenciais, incluindo a nutrição, o Bitcoin e o bem-estar mental em geral.

b Intro to Bitcoin Austrian Thought (1 hora):

Esta palestra em formato áudio fala da Escola Austríaca de Economia e da forma como a mesma se relaciona com o conceito do Bitcoin. Dá a conhecer melhor os princípios económicos por trás do Bitcoin e a forma como vão ao encontro do pensamento austríaco.

d BTC Sessions

Um canal do YouTube alusivo apenas à educação relativa ao Bitcoin, com tutoriais e guias úteis: <https://www.youtube.com/@BTCSessions>

4. Cursos:

a Summer of Bitcoin

<https://www.summerofbitcoin.org/>: Um programa de estágio de verão online a nível global, com foco na introdução dos estudantes universitários ao conceito de código aberto do Bitcoin e à programação do mesmo.



b Chaincode Labs

<https://learning.chaincode.com/#FOSS>: Cursos online e um programa presencial, que permite aos alunos desenvolver as competências necessárias para contribuir para o desenvolvimento do protocolo Bitcoin.

5. Autores de Referência

- a Gladstein, A., *Check Your Financial Privilege*
- b Swan, A., *Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications*
- c Cavalieri, A., *Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide*
- d Posch, A., *Aprenda Bitcoin: Torne-se Financeiramente Soberano*
- e Yakes, E., *The 7th Property: Bitcoin and the Monetary Revolution*

c Saylor Academy

Educação gratuita em várias disciplinas:
<https://www.saylor.org/>

- f Booth, J., *O Preço do Amanhã: A Deflação como a Chave para um Futuro de Abundância*
- g Song, J., *O Pequeno Livro do Bitcoin: Por que Bitcoin Importa para Sua Liberdade, Finanças e Futuro*
- h Bhatia, N., *Dinheiro em Camadas: Do Ouro e Dólares ao Bitcoin e Moedas Digitais de Banco Central*
- i Breedlove, R., *Graças a Deus pelo Bitcoin: A Criação, Corrupção e Redenção do Dinheiro*
- j Alden, L., *Broken Money*

6. Autores Citados

a Curious Inventor:

<https://www.youtube.com/@CuriousInventor>

b Anil Patel:

Twitter: @anilsaidso

7. Outros Recursos:

- 1 **Bitcoin.org:** O website oficial do protocolo Bitcoin.
- 2 **Bitcointalk.org:** O Bitcointalk é um fórum onde os utilizadores podem debater tópicos relacionados com o Bitcoin, fazer perguntas e partilhar informações. É um ótimo sítio para aprender com outros entusiastas e especialistas do Bitcoin.
- 3 **Bitcoincore.org:** Este é o software original do Bitcoin, que continua a ser bastante utilizado por muitos utilizadores e programadores. Oferece um ótimo conjunto de ferramentas para interagir com a rede Bitcoin e criar aplicações Bitcoin.
- 4 **Bitcoinwiki.org:** Este é um recurso gerido pela comunidade, que explica em detalhe tudo o que está relacionado com o Bitcoin. Abrange tudo, desde os aspectos técnicos do Bitcoin à sua história e utilizações.
- 5 **Bitcoinmagazine.com:** Esta é uma publicação online, que contém notícias e informações relacionadas com o Bitcoin e outras criptomoedas. É uma excelente forma de te manteres a par das últimas novidades do ecossistema Bitcoin.
- 6 **Bitcoin.Design:** Um repositório de código aberto para ficheiros de design relacionados com o bitcoin, para ilustrações, websites, modelos e ícones.
- 7 **NOSTR:** <https://nostr.com/> - Rede social onde somos os verdadeiros proprietários dos nossos dados.
- 8 **Simple X:** <https://simplex.chat/> - Um protocolo de aplicação privado e descentralizado.
- 9 **Criar um Nó no Bitcoin:** Mukai, K., Raspberry Pi DIY: https://github.com/kdmukai/raspberrypi_bitcoin_node_tutorial?tab=readme-ov-file.
- 10 **Como escolher uma carteira de bitcoin:** <https://bitcoin.org/en/choose-your-wallet> - Usa o que acabaste de aprender para escolher a carteira certa para ti.
- 11 **BitcoinIcons.com:** <https://bitcoinicons.com/> - Uma coleção de ícones gratuitos alusivos ao Bitcoin.
- 12 **Bitcoin For Local Business:** <https://bitcoinfoforlocalbusiness.com/> - Um conjunto de panfletos, para te ajudar a partilhar o valor do Bitcoin com as empresas locais que frequentas.
- 13 **Mempool.Space:** <https://mempool.space/> - Um projeto mempool de código aberto, que também contém informações e gráficos da rede Lightning.
- 14 **Yzer:** <https://yzer.io/> - Educação Bitcoin, simples e móvel. Aprende sobre Bitcoin, finanças, economia e ganha Sats.

Conceitos principais de cada capítulo

Capítulo 1:

Introdução ao curso:

Conhecer os objetivos e expectativas do curso Diploma Bitcoin.

Atividade de reflexão - Definição de dinheiro:

Participar num exercício de reflexão, no qual se responde a cinco questões principais sobre o dinheiro.

Debate de turma – Porque é que precisamos de dinheiro:

-  Participar num debate de turma, para discutir o dinheiro como necessidade fundamental.
-  Partilhar e comparar perspetivas individuais relativas à importância do dinheiro.
-  Adquirir as bases para compreender o papel do dinheiro nos sistemas económicos.

Capítulo 2:

Compreender o dinheiro:

-  Conhecer a definição e o conceito fundamental do dinheiro.
-  Debater com a turma as diversas perspetivas, por forma a compreender a natureza multifacetada do dinheiro.

Psicologia do dinheiro:

-  Compreender os aspetos psicológicos do dinheiro, incluindo a escassez, a preferência temporal e escolhas envolvidas.
-  Participar na atividade “Preferência Temporal”, para corresponder elementos psicológicos com situações da vida real.

Funções, características e categorias:

-  Analisar em detalhe as funções, propriedades e diferentes tipos de dinheiro.
-  Reconhecer a importância destes aspetos na definição e utilização do dinheiro.

Capítulo 3:

Introdução à história e evolução do dinheiro:

Aprender a história e evolução do dinheiro. Compreender a forma como as antigas formas de comércio levaram ao desenvolvimento das moedas que usamos atualmente.

Evolução das moedas:

Conhecer a transição das moedas antigas, tais como conchas e contas, para o surgimento de moedas metálicas e papel-moeda. Acompanhar a transição do papel para o plástico e conhecer a evolução das moedas ao longo da História.

Revolução das moedas digitais:

-  Conhecer o auge atual da evolução do dinheiro – as moedas digitais.
-  Compreender que existem apenas em formato eletrónico, o que permite transações instantâneas e de baixo custo, a nível global.
-  Conhecer melhor a importante contribuição do Bitcoin para resolver os problemas iniciais das moedas digitais, por forma a torná-las adequadas a uma utilização a nível mundial.

Atividade com jogo das trocas diretas:

Participar na experiência prática do jogo das trocas diretas, para compreender os desafios da troca direta e reconhecer a necessidade de um sistema mais eficiente.



Capítulo 4:

Origens do dinheiro fiduciário:

Descobrir as origens do dinheiro fiduciário, através de um curto resumo da sua história, para entender a razão pela qual se tornou uma forma dominante de moeda.

Atividade alusiva ao sistema de reservas mínimas obrigatórias:

Participar na atividade alusiva ao sistema de reservas mínimas obrigatórias, para compreender o funcionamento deste sistema, com destaque para a inerente dependência da dívida e as suas implicações para a economia em geral.

O sistema fiduciário:

Entender os aspetos fundamentais do sistema fiduciário, incluindo a sua natureza como sistema monetário obrigatório, o papel das reservas mínimas obrigatórias e os principais intervenientes que controlam este sistema.

Capítulo 5:

Redução do poder de compra:

Compreender o conceito de inflação monetária e o seu impacto no poder de compra. Participar na atividade alusiva aos efeitos da inflação (uma atividade de leilão), para sentir estes efeitos em primeira mão.

Atividade alusiva às consequências do sistema fiduciário:

Participar na atividade alusiva às consequências do sistema fiduciário, para conhecer as repercussões globais do enquadramento monetário atual.

Moedas Digitais do Banco Central (CBDC):

Descobrir o panorama em evolução das Moedas Digitais do Banco Central (CBDC) e o seu possível impacto no futuro do dinheiro.

O peso da dívida global e a desigualdade social:

Aprender o duplo impacto do peso da dívida global e da desigualdade social. Reconhecer as consequências para o indivíduo e para a sociedade, com destaque para a perda de poder de compra e para o aumento do fosso entre ricos e pobres.

Os Cypherpunks e a descentralização:

Aprender a história dos Cypherpunks e o que os motivou a procurar uma moeda descentralizada. Diferenciar os sistemas centralizados e descentralizados e aprender com um resumo da história das moedas digitais.

Capítulo 6:

Satoshi Nakamoto e a criação do Bitcoin:

Conhecer a misteriosa entidade Satoshi Nakamoto e a história da origem do Bitcoin, para compreender a motivação inicial por trás do seu desenvolvimento.

Atividade de turma - Obtenção de consenso:

Participar num processo de obtenção de consenso, numa atividade de rede ponto a ponto, para adquirir uma perspetiva prática do processo de obtenção de consenso da rede Bitcoin.

Adotar uma responsabilidade pessoal:

Destacar o conceito de responsabilidade pessoal no contexto do Bitcoin, por forma a incentivar um entendimento das funções individuais e da responsabilização num ecossistema descentralizado.

O funcionamento do Bitcoin:

Um olhar sobre o funcionamento do Bitcoin, incluindo o Mecanismo de Consenso Nakamoto. Identificar os principais intervenientes da rede Bitcoin, nomeadamente os mineradores, os nós, os utilizadores, os programadores e os projetos, e compreender a dinâmica de colaboração entre eles.

O Bitcoin como moeda digital forte:

Examinar o papel do Bitcoin como dinheiro digital forte, falar sobre a sua evolução, funções e propriedades, e participar num debate de turma para determinar se o Bitcoin é considerado uma moeda forte.

Conceitos principais de cada capítulo

Capítulo 7:

Transações ponto a ponto:

Participar em transações descentralizadas, para testemunhar os princípios fundamentais das transações Bitcoin.

Configurar uma carteira Bitcoin:

Aprender os passos principais para descarregar uma carteira, criar chaves e fazer uma cópia de segurança da carteira, por forma a fazer transações seguras.

Poupar e fazer a sua própria pesquisa:

Compreender o conceito de poupanças em bitcoin, como reserva de valor, e a importância de uma pesquisa independente para tomar decisões informadas.

Capítulo 8:

Introdução à rede Lightning:

Reconhecer a evolução do Bitcoin através de tecnologias como a rede Lightning, que melhoraram as suas capacidades.

Configurar uma carteira Lightning:

Aprender os passos principais para configurar uma carteira Bitcoin Lightning, para facilitar transações mais rápidas e em maior número.

Atividade prática:

Participar numa corrida de estafetas prática com uma carteira Lightning, por forma a adquirir uma compreensão dinâmica das transações da rede Lightning.

Capítulo 9:

O livro-razão do Bitcoin:

Compreender o conceito de um livro-razão descentralizado e promovido por nós e mineradores, que garantem a sua transparência e segurança.

O modelo UTXO:

Entender o modelo de Saída de Transação Não Gasta (UTXO) como aspecto fundamental do processamento de transações Bitcoin.

Chaves públicas e privadas:

Aprender a importância da segurança criptográfica nas transações Bitcoin, por meio de chaves públicas e privadas, e participar numa atividade que demonstra a função de *hash* SHA256.

Tipos de carteiras Bitcoin:

Diferenciar as carteiras de código aberto, de código fechado, custodiais e não-custodiais, para entender o papel das chaves na segurança.

Adquirir Bitcoin:

Conhecer métodos como transações ponto a ponto e corretoras, por forma a abordar as questões de privacidade relacionadas com os processos KYC - Know Your Customer (conhecer o cliente).

Tipos de carteira Lightning:

Diferenciar as carteiras Lightning de código aberto, de código fechado, custodiais e não-custodiais, de acordo as várias preferências dos utilizadores.

Transações Lightning:

Aprender o processo de envio e receção de transações Lightning, com destaque para a velocidade e eficiência da rede Lightning.

Nós e mineradores do Bitcoin:

Analizar as funções dos nós e mineradores na preservação da rede Bitcoin, incluindo aspectos como a emissão, a escassez, os *halvings* e o nível de dificuldade.

O processamento das transações Bitcoin:

Compreender melhor todas as etapas do processamento de uma transação Bitcoin, que passa pelo remetente, destinatário, nós, mineradores e *mempool* (memória de transações), com uma atividade focada na *mempool*.

Capítulo 10:



Bases filosóficas do Bitcoin:

Conhecer a filosofia fundamental por trás do Bitcoin, compreender que surgiu como resposta às crises económicas, com foco no impacto que tem na liberdade financeira e na forma como difere das moedas tradicionais.



O futuro do Bitcoin:

Analizar em detalhe o possível trajeto e evolução futuros do Bitcoin, como moeda digital revolucionária.



Reflexão sobre o diploma:

Resumir as principais conclusões do Diploma Bitcoin e incentivar os alunos a pensar no seu trajeto e perspetivas adquiridas.

As atividades incluem a visualização de um vídeo sobre o tema "Porquê o Bitcoin?" e a revisão das questões do Capítulo 1, para avaliar o crescimento pessoal em relação à aprendizagem.

Glossário

Altcoins: Altcoins é a abreviação de *Alternative Coins* (moedas alternativas). São todas as moedas digitais que não incluem o Bitcoin.

Armazenamento a Frio: Um método de guardar bitcoins offline, afastado do risco de hackers ou outras ameaças online.

Árvore de Merkle: Uma estrutura de dados em forma de árvore usada na *blockchain* do Bitcoin para verificar de forma eficiente a integridade de grandes conjuntos de dados.

Assinatura: Um mecanismo matemático que permite a alguém provar a propriedade.

Ataque de 51%: Um tipo de ataque a uma *blockchain* em que uma única entidade ou grupo controla a maioria do poder computacional da rede, permitindo-lhes manipular transações e, potencialmente, interromper o funcionamento da rede.

Ativo Digital: Uma representação digital de valor que pode ser trocada por outra unidade de valor ou utilizada como reserva de valor, como os bitcoins.

Autenticação de Dois Fatores (2FA): Uma medida de segurança que requer dois métodos de autenticação, geralmente uma palavra-passe e um código ou dispositivo separado, para aceder a uma conta ou concluir uma transação.

Baleia (Whale): Um indivíduo ou uma organização que detém uma quantidade significativa de criptomoeda, tendo a capacidade de influenciar os preços de mercado através de grandes transações.

Banca Restritiva: Restrições ou limitações nos serviços bancários ou no acesso aos mesmos. Banco Central (Fed): Uma instituição estatal responsável por gerir a política monetária de um país.

Bitcoin: Uma moeda/sistema digital que permite às pessoas enviarem dinheiroumas às outras sem a necessidade de um banco.

Blockchain Privada: Uma cadeia de blocos controlada por uma única organização, em vez de ser descentralizada.

Blockchain Pública: Uma cadeia de blocos aberta a qualquer pessoa para participar e verificar transações, tornando-a descentralizada.

Blockchain: Um registo público de todas as transações da rede Bitcoin.

Bloco Órfão: Um bloco não incluído na cadeia principal da *blockchain*, por ter sido invalidado por uma cadeia concorrente mais longa.

BTC: A unidade utilizada para bitcoins. Uma moeda digital que pode ser utilizada para efetuar compras ou para ser negociada.

Cabaz de Bens e Serviços: Um conjunto de bens ou serviços utilizado para medir as variações no custo de vida.

Carteira de Criptomoedas: Um programa de software que armazena chaves privadas e permite aos utilizadores enviar, receber e gerir as suas criptomoedas.

Carteira de Papel: Uma cópia impressa das chaves privadas e públicas de um utilizador, usada para armazenar e gerir criptomoedas offline.

Carteira Física: Um dispositivo físico utilizado para armazenar chaves privadas e gerir criptomoedas, oferecendo maior segurança em relação às carteiras online.

Carteira Multi-Assinatura (Multisig): Uma carteira que exige múltiplas assinaturas ou aprovações antes que uma transação possa ser executada, oferecendo segurança e controlo adicionais.

Carteira Online: Uma carteira de Bitcoin conectada à internet, permitindo fácil acesso aos bitcoins.

Carteira: Um recipiente virtual para bitcoins, semelhante a uma carteira física. Contém a(s) chave(s) privada(s) que permite(m) gastar os respetivos bitcoins na *blockchain*.

Centralização: A concentração de poder ou controlo numa única entidade.

Chave Privada: Uma série de dados secretos, que prova o direito de uma pessoa gastar bitcoins de uma carteira específica, através de uma assinatura criptográfica.

Chave Pública: Um identificador único utilizado para receber bitcoin, derivado da chave privada do utilizador, calculado através de um processo matemático.

Chave Pública/Endereço Bitcoin: Uma chave (ou endereço) pública usada para receber bitcoins.

Coincidência de Vontades: O fenómeno em que duas partes, numa economia de troca direta, possuem o que a outra parte deseja e desejam o que a outra parte possui.

Confirmação: O processo pelo qual uma transação é processada pela rede e torna-se altamente improvável de ser revertida. O método pelo qual os mineradores verificam a autenticidade das transações com o seu hardware e software. Recomenda-se aguardar pelo menos seis confirmações para prevenir o duplo gasto.

Contrato Inteligente: Um contrato autoexecutável com os termos do acordo escritos em código.

Controlo de Capitais: Restrições à movimentação de dinheiro entre fronteiras.

Cópia de Segurança da Carteira: Uma cópia da(s) chave(s) privada(s) e a frase semente (frase de recuperação) de uma carteira Bitcoin. Estes dados podem ser utilizados para restaurar o acesso à carteira, em caso de perda ou roubo.

Criptografia: Um ramo da matemática que ajuda a criar sistemas seguros.

Descentralização: A distribuição de poder e controlo por toda a rede, em vez de ter uma autoridade central.

Desvalorização: A redução no valor de uma moeda, frequentemente através da diminuição da quantidade de metal precioso numa moeda.

Dívida: Dinheiro que é devido a outra pessoa.

Duplo Gasto: Quando uma pessoa tenta enviar os seus bitcoins para dois destinatários diferentes ao mesmo tempo.

Glossário

Endereço: Um identificador único, utilizado para enviar e receber bitcoins na rede Bitcoin, normalmente representado como uma sequência de letras e números.

Explorador de Blocos: Uma ferramenta utilizada para visualizar e explorar a *blockchain*, permitindo aos utilizadores consultar blocos individuais, transações e endereços de carteiras.

Finanças Descentralizadas (DeFi: Decentralized Finance): Um movimento dentro da indústria de criptomoedas para criar produtos e serviços financeiros descentralizados que operam numa *blockchain*.

FOMO: Medo de ficar de fora (*fear of missing out*), um termo usado para descrever o sentimento de ansiedade ou arrependimento por achar que se pode perder uma oportunidade lucrativa no mercado de criptomoedas.

Frase de Recuperação/Frase Semente: Uma série de 12, 18 ou 24 palavras que podem ser usadas para gerar múltiplos pares de chaves privadas e públicas. Estas podem ser usadas para restaurar uma carteira de Bitcoin.

FUD: Medo, incerteza e dúvida (*fear, uncertainty, and doubt*), um termo usado para descrever rumores ou informações negativas que podem causar pânico ou declínio no mercado.

Função de Hash (Função de Dispersão): Uma função matemática que recebe dados de qualquer tamanho e gera uma cadeia de caracteres de tamanho fixo, comumente usada em criptografia e tecnologia de *blockchain*.

Hacker de Chapéu Branco (White Hat Hacker): Um hacker ético que utiliza as suas competências para identificar e corrigir vulnerabilidades em sistemas e redes informáticas.

Hard Fork: Uma alteração ao protocolo do Bitcoin que cria uma nova versão da *blockchain* que não é compatível com a versão anterior (por exemplo, Bitcoin Cash).

HODL: Um termo utilizado na comunidade de criptomoedas para descrever a ação de manter criptomoedas a longo prazo, em vez de vender ou negociar.

ID da Transação: Uma sequência de números e letras que mostra os detalhes de uma transferência de bitcoin (como o valor enviado, os endereços do remetente e do destinatário, e a data da transferência) na cadeia de blocos do Bitcoin.

Importações: Bens e serviços produzidos noutro país e vendidos no mercado interno.

Inflação: Um aumento no nível geral de preços de bens e serviços numa economia.

Leilão: Um processo pelo qual bens ou ativos são vendidos ao comprador que oferecer o valor mais alto.

Livro-razão: Um registo de transações financeiras.

Livro-razão Distribuído: Uma base de dados que é distribuída por uma rede de computadores, em vez de ser armazenada num local central.

Livro-razão Público: Uma base de dados descentralizada que mantém um registo público de todas as transações realizadas na rede Bitcoin.

Massa monetária: A quantidade total de dinheiro em circulação numa economia.

Mecanismo de Consenso: Um método utilizado na tecnologia de *blockchain* para validar transações e garantir a integridade da *blockchain*.

Meios de Troca: Objetos ou sistemas que são amplamente aceites na troca de bens e serviços.

Mineração: O processo de utilização de hardware para realizar cálculos matemáticos para a rede Bitcoin, com o objetivo de confirmar transações e aumentar a segurança.

Moeda Mercadoria: Objetos que têm valor em si mesmos e são usados como meio de troca, como ouro ou prata.

Multi-Assinatura: Uma funcionalidade de segurança que exige mais de uma chave privada para autorizar uma transação de bitcoin.

Nó: Um computador ou dispositivo conectado à rede Bitcoin, que participa na verificação e transmissão de transações.

Nonce: Um número aleatório incluído no cabeçalho de um bloco para gerar um *hash* que satisfaz o nível de dificuldade exigido.

Oferta e Procura: O princípio económico que estabelece que o preço de bens ou serviços é determinado pela interação entre a quantidade de bens ou serviços oferecidos e a quantidade procurada pelo mercado.

Oferta Inicial de Moedas (ICO: Initial Coin Offering): Um método de angariação de fundos em que uma nova criptomoeda é vendida a investidores em troca de uma criptomoeda mais estabelecida, como o Bitcoin.

Organização Autónoma Descentralizada (DAO: Decentralized Autonomous Organization): Uma organização ou rede governada por contratos inteligentes e operada numa *blockchain*, sem uma autoridade central ou estrutura de gestão.

Par de Negociação (Trading Pair): Um conjunto de duas moedas ou ativos que podem ser negociados entre si numa plataforma de troca de criptomoedas.

Paridade (Peg): Uma taxa de câmbio fixa entre duas moedas, onde uma está vinculada ao valor da outra.

PIB: Produto Interno Bruto, o valor total dos bens e serviços produzidos num país durante um determinado período de tempo.

Plataforma de Troca de Criptomoedas: Uma plataforma onde os utilizadores podem comprar, vender e negociar criptomoedas por outros ativos, como moeda fiduciária ou outras criptomoedas.

Poder de Compra: Capacidade financeira de aquisição de bens e serviços.

Política Monetária e Fiscal: As políticas de um banco central e de um governo, respetivamente, que influenciam a oferta de dinheiro e as taxas de juro numa economia.

Ponto a Ponto (P2P: Peer-to-Peer): Uma rede descentralizada na qual os participantes interagem diretamente entre si, em vez de o fazerem através de uma autoridade central.

Pool de Mineração: Um grupo de mineradores que trabalham juntos para aumentar as suas hipóteses de encontrar novos blocos e ganhar bitcoins.

Glossário

Proof-of-Stake (PoS; Prova de Participação): Um mecanismo de consenso utilizado em algumas redes de *blockchain* que exige que os utilizadores mantenham uma certa quantidade de criptomoeda para participar na validação de transações.

Proof-of-Work (PoW; Prova de Trabalho): Um mecanismo de consenso que exige que os utilizadores realizem uma certa quantidade de trabalho computacional para participar na rede.

Protocolo de Camada 1: A camada subjacente de uma rede de *blockchain* que lida com os aspetos fundamentais de consenso, validação de transações e armazenamento de dados.

Protocolo de Camada 2: Uma camada secundária construída sobre uma rede de *blockchain* de camada 1, frequentemente usada para melhorar a escalabilidade, velocidade e funcionalidade.

Rácio de Reservas: A proporção de depósitos que um banco deve manter como reservas.

Recompensa de Bloco: A quantidade de novos bitcoins atribuída aos mineradores por adicionarem um novo bloco à *blockchain*.

Rede: Um grupo de entidades interconectadas.

Rede de Nós: Uma rede de computadores ou dispositivos conectados que suportam e mantêm a rede Bitcoin.

Rede Lightning: Um protocolo de pagamento de camada 2 que permite transações de bitcoin mais rápidas e baratas, utilizando canais fora da *blockchain* para transações menores.

Satoshi: A unidade mais pequena de Bitcoin, equivalente a 1/100 000 000 de um bitcoin. O nome é uma homenagem ao criador do Bitcoin, Satoshi Nakamoto.

Satoshi Nakamoto: O pseudónimo usado pelo(s) criador(es) anónimo(s) do Bitcoin.

Satoshis por Byte (sat/b): Uma unidade utilizada para medir a taxa de transação em bitcoin paga por byte de dados da transação.

SegWit (Testemunha Segregada / Segregated Witness): Uma atualização do protocolo do Bitcoin que altera a forma como os dados são armazenados na *blockchain*, permitindo uma maior capacidade e taxas de transação mais baixas.

Sem Banco (Unbanked): Indivíduos ou comunidades sem acesso aos serviços bancários tradicionais.

Sem Necessidade de Confiança (Trustless): Um sistema ou transação que não requer confiança em qualquer terceiro ou intermediário, dependendo, em vez disso, na segurança e transparência da tecnologia subjacente.

Sidechain: Uma cadeia de blocos conectada a outra *blockchain*, permitindo a transferência de ativos ou informações entre as duas cadeias.

Sistema Centralizado: Um sistema em que o poder ou controlo está concentrado numa única entidade.

Sistema Descentralizado: Um sistema em que o poder ou controlo é distribuído entre várias entidades.

Soft Fork: Uma alteração ao protocolo do Bitcoin que é compatível com versões anteriores do software.

Stablecoin: Um tipo de criptomoeda projetada para manter um valor estável, muitas vezes vinculada a uma moeda fiduciária ou a outro ativo.

Taxa de Câmbio: O valor de uma moeda em relação a outra.

Taxa de Hash: Uma forma de medir o poder de processamento da rede Bitcoin.

Temporada de Altcoins: Um período em que criptomoedas alternativas ao Bitcoin registam aumentos significativos de preço, geralmente devido a um maior interesse e adoção por parte dos investidores.

Token: Uma unidade de valor criada numa *blockchain*, frequentemente usada para representar um ativo ou utilidade específicos dentro de um determinado ecossistema.

Token Não Fungível (NFT: Non-Fungible Token): Um tipo de ativo digital que representa um item único ou exclusivo, frequentemente usado para representar arte, colecionáveis ou outros objetos únicos.

Tokenização: O processo de criação de uma representação digital de um ativo ou classe de ativos numa *blockchain*, permitindo a propriedade fracionada e a transferibilidade.

Transação: A transferência de bitcoins de um endereço para outro na rede Bitcoin.

Transação de Poeira: Uma transação que envia uma quantidade muito pequena de bitcoins, que é demasiado reduzida para ser economicamente viável.

Troca Atómica: Uma troca ponto a ponto de uma criptomoeda por outra, sem a necessidade de uma troca centralizada ou de um intermediário.

Troca Direta: A troca de bens e serviços sem a utilização de dinheiro.

Unidade de Conta: Uma unidade de referência usada para expressar o valor de bens e serviços.

Valor de Taxa de Transação: Uma pequena quantia de bitcoins paga pelo remetente de uma transação, incentivando os mineradores a incluir a transação num bloco e adicioná-la à *blockchain*.

Valor Temporal do Dinheiro: O princípio de que o dinheiro vale mais no presente do que no futuro.

Volatilidade: O grau de variação do preço de um ativo ao longo do tempo.

Whitepaper: Um relatório que explica o problema que um projeto de *blockchain* ou criptomoeda está a tentar resolver e a respetiva solução.

XBT e BTC: Abreviaturas de bitcoin.



Versão Portuguesa | 2025