



# Diploma Bitcoin

*Educação Financeira para a Era do Bitcoin*



***Livro do Estudante***

Versão em Português | Julho de 2023









**Meu Primeiro Bitcoin** criou este trabalho e o disponibilizou gratuitamente sob a licença **Creative Commons**.

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



# Diploma Bitcoin

*Educação Financeira para a era Bitcoin*

## ***Livro do Estudante***

Versão em Português | Julho de 2023

*DOE AGORA:*



bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf



## **Agradecimentos**

O Diploma Bitcoin foi um sucesso estrondoso e cresceu mais rápido do que qualquer um esperava. Gostaríamos de dar crédito a todas as pessoas maravilhosas que nos trouxeram até aqui.

Dalia Platt é a responsável pelo desenvolvimento do currículo e a força motriz por trás do nosso conteúdo desde o início. Ela é uma estrela. Ela contou com uma ótima ajuda para esta edição de alguns contribuidores incríveis, incluindo Madelyn Hereford, Greg Foss, Ronny Avendano, Alejandro Galán, Evelyn Lemus, Gerardo Linares, Marc Platt, Jim Platt, Napoleón Osorio, Victor Yusbek, Robert Malka e Arel Edelkamp. Gloriana Solano, Raul Guirola, Giacomo Zucco, Gerson Martinez, Vriti Saraf e outros apoiaram edições anteriores. Gerardo Apostolo e Enrique Jubis, da ACTIVA, também contribuíram com seu incrível trabalho.

A história do Diploma Bitcoin começou em fevereiro de 2022 em uma reunião na Escola Pública La Pacheco, em San Marcos, El Salvador. Entre os presentes estavam o diretor inovador da escola, Asael Rodriguez, o defensor da educação sobre o bitcoin e congressista Rodrigo Ayala, e o construtor comunitário do Ibex Mercado, Carlos Toriello, que convidou outros entusiastas do Bitcoin, incluindo eu, para visitar a escola e discutir sobre educação.

Os primeiros alunos do Diploma Bitcoin começaram em abril, com o apoio inicial do Ibex, bem como centenas de doadores individuais. Em junho, o primeiro grupo de 38 alunos se formou na La Pacheco e começamos a expandir. Com um tremendo apoio de novos doadores e patrocinadores, incluindo a Bitfinex, prefeitos locais e Bitcoin Beach, a matrícula continuou a mais do que dobrar de tamanho a cada dez semanas, uma tendência que nos permitirá alcançar milhares de alunos em todo o país este ano. Em fevereiro de 2023, a entrega do currículo começou na Guatemala, com planos de levá-lo para muitas outras nações antes do final do ano, incluindo Colômbia, Honduras, África do Sul, Equador e Estados Unidos. As doações desses programas subsidiarão ainda mais estudantes em El Salvador.

O livro de trabalho do Diploma Bitcoin foi disponibilizado como código aberto. Ele está disponível gratuitamente e foi traduzido, impresso e ensinado de forma independente para comunidades ao redor do mundo, da Coreia do Sul ao Uruguai.

Mi Primer Bitcoin é uma organização sem fins lucrativos com uma missão singular: fornecer educação comunitária de qualidade, independente e imparcial sobre o Bitcoin para todos em El Salvador o mais rápido possível. Como a primeira nação a adotar o Bitcoin, El Salvador será um exemplo para o mundo; cabe a nós decidir que tipo de exemplo será esse. Nossa visão é ensinar uma nação e mudar o mundo. Eu sei que parece loucura, mas acredito que estamos no caminho certo e o Bitcoin Diploma é uma grande parte disso.

Por um mundo melhor,

**John Dennehy**

Fundador

**Mi Primer Bitcoin**

Março 2023

# Sumário

<b>Capítulo #1 - O Poder do Dinheiro .....</b>	<b>11</b>
<b>1.0 Pronto? .....</b>	<b>12</b>
<b>1.1 Discussão em classe: O que é dinheiro? .....</b>	<b>12</b>
<b>1.2 O Mundo Limitado - Navegando pela Escassez em uma Economia em Crescimento .....</b>	<b>13</b>
<b>1.3 Definição de Dinheiro .....</b>	<b>15</b>
<b>1.3.1 Podemos Usá-lo, mas Podemos Definir-lo? .....</b>	<b>15</b>
<b>1.3.2 Funções do Dinheiro .....</b>	<b>17</b>
<b>1.3.3 Características do Dinheiro .....</b>	<b>18</b>
<b>1.3.4 Tipos de Dinheiro .....</b>	<b>21</b>
<b>Capítulo #2 - Da Troca Direta para o Bitcoin e CBDCs: Uma Viagem no Tempo .....</b>	<b>27</b>
<b>2.0 Introdução .....</b>	<b>28</b>
<b>2.0.1 Atividade em Classe: Jogo de Trocas .....</b>	<b>28</b>
<b>2.1 Formas Primitivas de Dinheiro .....</b>	<b>30</b>
<b>2.2 De Commodities a Notas Promissórias .....</b>	<b>31</b>
<b>2.3 Transição do Dinheiro Sólido para o Dinheiro Insustentável .....</b>	<b>32</b>
<b>2.4 Onde Estamos Hoje? .....</b>	<b>35</b>
<b>2.5 O Preço do Controle: Uma Análise da Vigilância, Censura e Regulação .....</b>	<b>35</b>
<b>2.5.1 A Ascensão de uma Sociedade Sem Dinheiro em Espécie .....</b>	<b>35</b>
<b>2.5.2 Vigilância .....</b>	<b>40</b>
<b>2.5.3 Regulações Financeiras e Censura .....</b>	<b>40</b>
<b>Capítulo #3 - Revelando o Lado Obscuro do Dinheiro Fiduciário .....</b>	<b>45</b>
<b>3.0 Atividade em Classe: Os Efeitos da Inflação: Uma Atividade de Leilão .....</b>	<b>46</b>
<b>3.1 As Maiores Ameaças ao seu Dinheiro: Inflação, Desvalorização e Perda do Poder de Compra .....</b>	<b>48</b>
<b>3.2 Dívida: A Linha Tênu entre Ajuda e Prejuízo .....</b>	<b>52</b>
<b>3.3 O Fed e seus Parceiros: Como o Governo e os Bancos Controlam a Oferta Monetária .....</b>	<b>53</b>
<b>3.4 A Magia da Criação de Dinheiro .....</b>	<b>55</b>
<b>3.4.1 O Valor Temporal do Dinheiro e seu Papel no Crescimento Econômico .....</b>	<b>55</b>
<b>3.4.2 Economizando Dinheiro em Tempos Difíceis .....</b>	<b>56</b>
<b>3.4.3 Sistema Bancário de Reserva Fracionária .....</b>	<b>57</b>
<b>3.4.4 Atividade em Classe: Sistema Bancário de Reserva Fracionária .....</b>	<b>58</b>

<b>Capítulo #4 - O Futuro é Descentralizado: Capacitando Indivíduos .....</b>	<b>63</b>
<b>4.0 Da Crise à Inovação: Os Cypherpunks e a Criação de uma Moeda Digital Descentralizada</b>	
<b>4.1 Abuso da Centralização</b>	64
<b>4.1.1 Sistemas Centralizados</b>	64
<b>4.1.2 Contando os Intermediários: Um Olhar sobre os Intermediários em uma Transação com Cartão de Crédito</b>	64
<b>4.2 Uma Ferramenta Poderosa para Superar as Limitações da Centralização</b>	66
<b>4.2.1 Exercício em Grupo: Jogo de Consenso Descentralizado com Atores Maliciosos</b>	68
<b>4.3 Transações são Apenas Acordos de Troca</b>	69
<b>4.3.1 Confiar ou Não Confiar</b>	70
<b>4.3.2 Vamos Trocar Confiança por Regras</b>	71
<b>4.4 Desbloqueando o Poder do Blockchain: Uma Tecnologia que Revoluciona o Futuro</b>	72
<b>Capítulo #5 - Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin.....</b>	<b>75</b>
<b>5.0 O Criador Misterioso do Bitcoin: Descobrindo a Identidade de Satoshi Nakamoto e seu White Paper</b>	76
<b>5.1 Introdução ao Bitcoin e ao bitcoin</b>	78
<b>5.1.1 O que é bitcoin? O que é Bitcoin?</b>	78
<b>5.1.2 Qual é a diferença entre Bitcoin e bitcoin?</b>	79
<b>5.1.3 Por que aprender sobre bitcoin se não posso comprá-lo?</b>	79
<b>5.1.4 Do que é feito o bitcoin?</b>	79
<b>5.1.5 Por que o bitcoin é uma boa moeda??</b>	80
<b>5.1.6 Por que devo me importar?</b>	80
<b>5.1.7 Como usar o bitcoin?</b>	81
<b>5.1.8 Como <b>enviar</b> ou <b>gastar</b> bitcoin?</b>	81
<b>5.1.9 Como <b>receber</b> bitcoin?</b>	81
<b>5.1.10 O Bitcoin pode ser desativado?</b>	81
<b>5.1.11 Como o blockchain acompanha quem gasta qual bitcoin?</b>	82
<b>5.1.12 Como novos bitcoins entram na rede?</b>	82
<b>5.1.13 O que é uma transação de bitcoin?</b>	82
<b>5.1.14 As transações de bitcoin são seguras?</b>	84
<b>5.2 Quem é quem e o que é o quê no Mundo do Bitcoin?</b>	87
<b>5.3 Me mostre uma Transação de bitcoin Real</b>	89
<b>5.3.1 Exercício em Grupo: Transações de Bitcoin em Ação</b>	93
<b>5.4 O que dá Valor ao bitcoin?</b>	95



<b>Capítulo #6 - Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras</b>	<b>99</b>
<b>6.0</b> De Novato a Profissional: Navegando no Mundo da Carteira de Bitcoin	100
<b>6.1</b> O Processo de Adoção e Segurança do seu bitcoin	103
<b>6.1.1</b> Exercício em Grupo: Dominando a Autocustódia e Usando sua Carteira com Confiança	104
<b>6.1.2</b> Exercício em Grupo: Como Receber bitcoin (em detalhes)	105
<b>6.1.3</b> Exercício em Grupo: Como Enviar bitcoin e Pagar por Bens e Serviços (em detalhes)	105
<b>6.2</b> On-Chain vs. Off-Chain	106
<b>6.3</b> A Lightning Network	107
<b>6.3.1</b> Uma Transação Lightning	109
<b>6.3.2</b> Exercício em Grupo: Corrida de Revezamento de Carteiras Lightning	112
<b>6.3.3</b> Exercício em Grupo: Demonstração Interativa Online da Lightning	112
<b>Capítulo #7 - Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, Mempool e UTXOs</b>	<b>115</b>
<b>7.0</b> Resolvendo o Problema de Gasto Duplo: Entendendo a Solução do Bitcoin	117
<b>7.1</b> Rastreando a Jornada da sua Moeda	119
<b>7.2</b> Segurança e Sigilo	122
<b>7.3</b> O “Mempool” ou Pool de Memória: Compreendendo o Tanque de Retenção das Transações de Bitcoin	127
<b>7.3.1</b> Exercício em Grupo: Em Espera: Examinando as Transações Não Confirmadas da Rede Bitcoin	128
<b>7.4</b> Por Trás dos Blocos: O Mistério da Scripting do Bitcoin	129
<b>7.4.1</b> Uma Profundidade Técnica nas Transações de Bitcoin	131
<b>Capítulo #8 - Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração de Bitcoin e seu Papel na Blockchain</b>	<b>135</b>
<b>8.0</b> Descobrindo as Joias da Blockchain: Conheça os Mineradores e o Processo de Mineração	136
<b>8.1</b> O Sistema de Recompensas Dinâmicas da Mineração de Bitcoin: Recompensas de Bloco, Taxas de Transação e Halvings	137
<b>8.2</b> A Tarefa Vital da Mineração de Bitcoin: Segurança da Blockchain	139
<b>8.3</b> Dissecando o Bloco	142

<b>8.4</b> Revisitando os Hashes - Sem Trocadilhos Intencionais	146
<b>8.5</b> O Processo Passo a Passo da Mineração de um Bloco	148
<b>8.5.1</b> Exercício em Grupo: Exercício Interativo de Mineração	150
<b>8.5.2</b> Resumo da transação do início ao fim	151
<b>8.5.3</b> Não Confie, Verifique	152
<b>8.6</b> Exercício em Grupo: Transação com UTXOs	153
<b>Capítulo #9 - Por que o Valor Intrínseco do Bitcoin vai Além da Superfície</b>	<b>157</b>
<b>9.0</b> Por que o Bitcoin?	158
<b>9.1</b> O Futuro do Bitcoin	158
<b>9.1.1</b> O Efeito Lindy	159
<b>9.2</b> Usando o Bitcoin para Mais do que Apenas Dinheiro Digital	160
<b>9.3</b> Os Desafios	161
<b>9.3.1</b> O Ambiente Regulatório para o Bitcoin	161
<b>9.3.2</b> Compreendendo o Consumo de Energia da Mineração de Bitcoin	162
<b>9.4</b> Os Riscos	163
<b>9.5</b> Negociando e Investindo em bitcoin	164
<b>Capítulo #10 - Dos Bits ao Bitcoin: Montando o Quebra-Cabeça</b>	<b>171</b>
<b>10.0</b> Apenas Alguns Fatos, Algumas Piadas... e o Jargão	172
<b>10.1</b> Projeto Final de Submissão e Diretrizes de Avaliação do Mi Primer Bitcoin	174
<b>Recursos Adicionais</b>	<b>177</b>
<b>Glossário</b>	<b>181</b>





## **Por que Bitcoin?**

**Pensamento Crítico.** Por que o *Bitcoin* é importante para você e como você acha que ele vai mudar a humanidade?

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

# Diploma Bitcoin

*Uma Jornada Transformadora de  
Dez Semanas Através de Educação  
Independente, Imparcial, de Qualidade  
e Gratuita.*



Seja lá o que o Bitcoin for, a maioria das pessoas ainda não entende o que essa inovação controversa e influente é e como funciona. Este é um documentário premiado que o ajuda a responder essas perguntas.

É essencial ter um entendimento sólido dos conceitos básicos do dinheiro, sua história e o sistema financeiro atual antes de estudar o **Bitcoin**. Compreender esses conceitos proporciona uma base sólida para compreender a natureza única e disruptiva do **Bitcoin**. Ao aprender sobre a evolução do dinheiro, você será capaz de entender melhor o potencial e as limitações do sistema financeiro atual e como o **Bitcoin** busca abordá-los. Sem essa base, pode ser desafiador apreciar completamente a importância e o impacto potencial do **Bitcoin**. Confie no processo de aprendizado e mantenha o foco, pois a recompensa de um entendimento mais profundo e uma apreciação desse campo inovador valerá a pena.

---

*Uma Mensagem de Nossa Fundadora*

---





# *Capítulo #1*



## *O Poder do Dinheiro*

**1.0** Pronto?

**1.1** Discussão em classe: O que é dinheiro?

**1.2** O Mundo Limitado - Navegando pela Escassez em uma Economia em Crescimento

**1.3** Definição de Dinheiro

**1.3.1** Podemos Usá-lo, mas Podemos Definí-lo?

**1.3.2** Funções do Dinheiro

**1.3.3** Características do Dinheiro

**1.3.4** Tipos de Dinheiro



# O Poder do Dinheiro

## 1.0 Pronto?

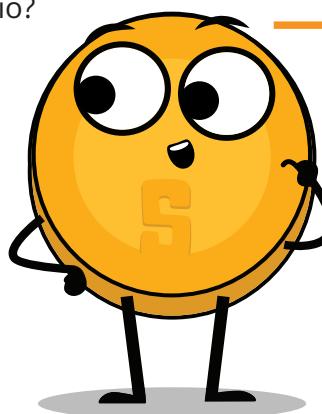
O **Bitcoin** tem sido chamado por muitos nomes - uma moda passageira, um golpe e “dinheiro mágico da internet”. Mas por trás da moda, há uma poderosa tecnologia que tem o potencial de mudar a forma como pensamos e usamos o dinheiro; o potencial de mudar o mundo de uma maneira que pessoas “normais” como você e eu tenham a oportunidade de construir riqueza, alcançar verdadeira liberdade e viver as vidas que desejamos. Neste curso, exploraremos as falhas e limitações do nosso sistema financeiro atual e como o **Bitcoin** oferece uma solução potencial. Portanto, se você está pronto para ir além das manchetes e aprender sobre as possibilidades reais do **Bitcoin**, vamos mergulhar!

Olá! sou **Satoshi**, um assistente interativo que irá ajudá-lo durante o Diploma Bitcoin. Irei fornecer dados e recomendações para melhorar o seu entendimento.



## 1.1 Discussão em Classe: O que é Dinheiro?

- Por favor, não coma o pedaço de doce colocado em sua mesa ainda.
- Quem estaria disposto a trocar seu doce por uma nota de US\$1?
- Agora, mantenham as mãos levantadas se vocês ainda estariam dispostos a trocar seu doce por uma nota de \$1 do jogo Banco Imobiliário?
  - Por que sim ou por que não?



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

- O que torna uma nota tão desejável e outra praticamente inútil?
- O que confere “valor” ao dinheiro?
- De onde vem o dinheiro e quem decide quanto imprimir?
- Por que não imprimir mais dinheiro e distribuí-lo igualmente para todos?
- O dinheiro é lastreado em ouro? Ou em alguma outra mercadoria?
- Quantas pessoas ainda utilizam dinheiro em espécie mesmo?



## 1.2 O Mundo Limitado: Navegando a Escassez em uma Economia em Crescimento

Imagine que você esteja perdido em um deserto e só tenha uma garrafa de água restante. Você está com sede e desesperado por uma bebida, mas também sabe que precisará dessa água para sobreviver até encontrar mais. Esse é um exemplo clássico de escassez - você só possui uma quantidade limitada de um recurso (água) e precisa fazer uma escolha sobre como utilizá-lo.

Nessa situação, você pode decidir racionar a água e tomar pequenos goles ao longo de um período mais longo, para fazê-la durar o máximo possível. Por outro lado, você pode decidir beber o máximo que puder de uma só vez, esperando que a hidratação intensa lhe dê a energia necessária para encontrar mais água. Independentemente da escolha que você fizer, estará diante de uma decisão difícil.



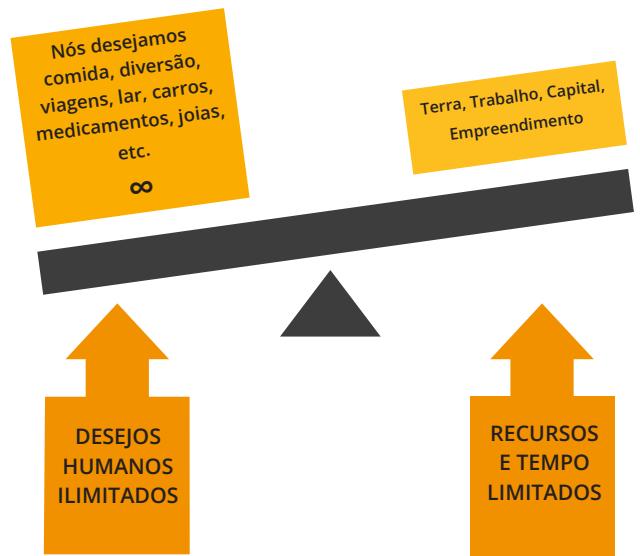
A **Escassez** nos obriga a avaliar os prós e contras de como usamos nossos recursos e a fazer compensações.

Nesse caso, a escolha é entre saciar imediatamente sua sede e conservar a água para depois.

Esse conceito de escassez se aplica a todos os tipos de recursos, não apenas à água. Seja dinheiro, tempo ou até mesmo amor e atenção, constantemente nos deparamos com escolhas sobre como alocar nossos recursos

limitados.

- Existem dois tipos de escassez: escassez artificial e escassez natural.
    - **Escassez Artificial**, também conhecida como escassez centralizada, inclui coisas como bolsas de edição limitada de designers, cartões esportivos raros e obras de arte numeradas. Esses itens podem ser facilmente replicados ou falsificados.
    - **Escassez Natural**, também conhecida como escassez descentralizada, inclui coisas como sal, conchas e metais preciosos como ouro. Esses itens são mais difíceis de replicar ou falsificar.
  - A principal diferença entre os dois é o controle. A escassez centralizada é controlada por uma única entidade, como uma empresa ou governo, enquanto a escassez descentralizada não é controlada por ninguém.
- A Escassez** afeta nossas escolhas e compreendê-la pode melhorar nosso processo de tomada de decisão. Frequentemente, somos obrigados a escolher entre ganhos imediatos e benefícios de longo prazo, e esses compromissos moldam nosso caminho para alcançar nossos objetivos.



# O Poder do Dinheiro

- No contexto do exemplo do deserto, isso significa que você pode estar mais inclinado a beber toda a água imediatamente, mesmo que isso signifique que você não terá nenhuma sobra para depois. Isso ocorre porque a sede que você sente agora é mais urgente do que a sede potencial que você pode sentir no futuro.
- Por outro lado, se você escolher racionar a água e beber lentamente ao longo do tempo, estará demonstrando uma preferência temporal mais baixa. Isso significa que você está disposto a esperar para satisfazer sua sede, a fim de ter uma maior chance de sobrevivência a longo prazo.



## Preferência temporal



- Por exemplo, digamos que você tenha a opção de receber \$100 hoje ou \$110 daqui a um ano. Se você tiver uma alta preferência temporal, pode escolher receber os \$100 hoje, porque valoriza a satisfação imediata de ter o dinheiro agora mais do que o benefício potencial de esperar por mais \$10 em um ano. Por outro lado, se você tiver uma baixa preferência temporal, pode estar disposto a esperar pela recompensa maior no futuro, porque está menos preocupado com a gratificação imediata e mais focado em planejamento de longo prazo.



**Custo de oportunidade** refere-se ao valor da melhor alternativa que você abre mão ao tomar uma decisão.  
**Toda decisão envolve trade-offs.**

O conceito de **custo de oportunidade** está intimamente relacionado à ideia de **escassez** e **preferência temporal**.

- No exemplo do deserto, o custo de oportunidade de beber toda a água imediatamente é o benefício de sobrevivência que você teria obtido ao racionar a água e usá-la ao longo de um período mais longo.





- Digamos que você decida racionar a água e tomar pequenos goles ao longo de um período mais longo. Como resultado, você terá a energia e hidratação necessárias para procurar mais água.
- No entanto, enquanto você está procurando, você encontra um cacto que tem uma pequena quantidade de água dentro. Não é muito, mas é o suficiente para saciar sua sede no momento. Se você tivesse decidido beber toda a sua água de uma vez, talvez não tivesse tido energia para procurar mais água e encontrar o cacto. Nesse caso, o custo de oportunidade de beber toda a sua água de uma vez teria sido a oportunidade de encontrar o cacto e obter mais hidratação.

Esse exemplo ilustra como o custo de oportunidade envolve não apenas a troca imediata entre duas opções, mas também as oportunidades futuras que podem ser ganhas ou perdidas como resultado de nossas escolhas. Nossa disposição em abrir mão de uma recompensa maior no futuro em troca de uma recompensa menor agora é influenciada pela nossa **preferência temporal**, ou seja, o quanto valorizamos a gratificação imediata versus o planejamento de longo prazo.

Corporações, governos e sociedades também precisam tomar decisões.

CORPORAÇÕES	GOVERNOS / SOCIEDADES
Demissão de 200 funcionários versus congelamento de salários.	Construção de uma nova rodovia versus aumento dos salários dos professores.
Solicitar um empréstimo versus aumentar as receitas.	Financiar pesquisa sobre tratamento do câncer versus energia limpa.

## 1.3 Definição de Dinheiro

### 1.3.1 Podemos Usá-lo, mas Podemos Defini-lo?

Você já parou para pensar no que realmente é o dinheiro? Alguma vez já se perguntou o que faz do dinheiro, bem, dinheiro? A maioria de nós sabe como usá-lo, mas poucos entendem de onde ele vem ou como funciona.

O dinheiro é essencialmente uma forma de trocar bens e serviços. Ele representa o valor



# O Poder do Dinheiro

desses itens de forma que possa ser facilmente negociado. Isso pode assumir muitas formas diferentes, como notas de papel, moedas de metal e pagamentos eletrônicos. Normalmente, os governos ou outras autoridades emitem e controlam o dinheiro.

Mas o dinheiro é muito mais do que apenas um meio físico ou digital de troca. É como uma linguagem universal que nos permite negociar com pessoas de todo o mundo, mesmo que não falemos o mesmo idioma ou tenhamos a mesma cultura. Por exemplo, você pode estar do outro lado do mundo e ainda “falar” dinheiro ao colocar um produto no balcão e trocá-lo pela moeda local ou usar um cartão de crédito. O dinheiro é como um contrato social que nos permite fazer trocas sem precisar depender da troca de mercadorias ou encontrar alguém que especificamente queira o que temos a oferecer. Se um grupo de pessoas começasse a aceitar chocolate como pagamento pela maioria dos bens e serviços, o chocolate se tornaria dinheiro. (Entretanto, como ele derreteria em algumas partes do mundo, poderíamos considerá-lo um mau dinheiro.)

Como o economista francês Jean Baptiste Say apontou: “O dinheiro desempenha apenas uma função momentânea em uma troca; e quando a **transação** é finalmente concluída, sempre será encontrado que um tipo de mercadoria foi trocado por outro.”

Em outras palavras, o dinheiro em si não possui o poder de satisfazer desejos humanos. Ele é apenas uma ferramenta que nos permite trocar uma mercadoria por outra.



*Sem dinheiro, quanto fácil ou viável seria essa troca?*

*Você trocaria uma vaca por 1.000.000 de morangos?*

*Ou seriam 600.000 morangos?  
E quanto a 50.000?*



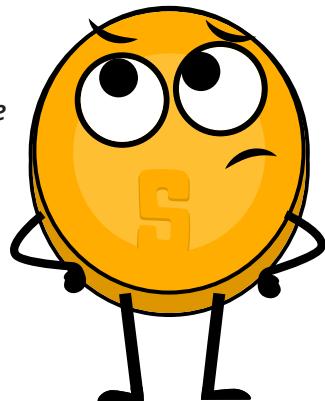
**Transação** é uma troca ou transferência de bens e serviços. É uma forma de trocar valor entre duas ou mais partes.

Existem muitos tipos diferentes de **transações**, desde trocas simples (como comprar um sanduíche em uma lanchonete) até **transações** financeiras mais complexas (como comprar uma casa ou investir em ações ou títulos). As **transações** podem ser realizadas pessoalmente, por telefone, online ou por outros meios, e podem envolver uma ampla variedade de partes, incluindo indivíduos, empresas e instituições financeiras.



Dinheiro **É** o valor **PELO QUAL** os bens são trocados.

Dinheiro **NÃO É** o valor **PARA QUE** os bens são trocados.





## Capítulo #1



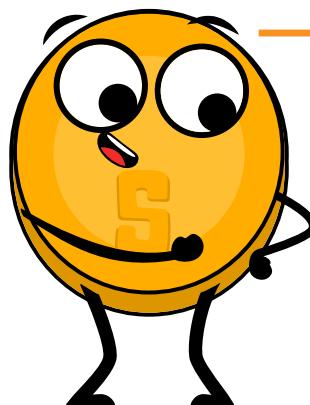
Dê uma olhada  
neste vídeo curto!



### 1.3.2 Funções do Dinheiro

Quando se trata de comprar e vender bens e serviços, o dinheiro é o protagonista principal. Ele desempenha várias funções importantes, tais como:

- **Facilitar as trocas:** Com dinheiro, você não precisa encontrar alguém que queira exatamente o que você tem para trocar. Em vez disso, você pode usar dinheiro para comprar e vender qualquer coisa que desejar. Isso torna as negociações e o comércio muito mais convenientes e eficientes.
- **Servir como unidade de conta:** O dinheiro fornece um padrão universal de valor que permite às pessoas expressar e comparar o preço de diferentes bens e serviços. Isso permite um mercado mais eficiente e transparente, onde as pessoas podem tomar decisões informadas sobre o que comprar e vender.
  - Pense assim: se você quisesse comprar um carro novo, poderia comparar os preços de diferentes concessionárias e tomar uma decisão informada sobre qual comprar com base no preço em dólares. Sem uma unidade de conta, você teria que tentar comparar o valor de um carro com outro usando algo diferente, como o número de vacas que ele valia ou o tempo que levou para fabricar o carro.



#### Unidade de Conta

*Os consumidores  
conhecem o valor  
de algo quando você  
atribui um preço  
(valor monetário) a  
ele.*

Em resumo, o dinheiro:

- Facilita o comércio porque todos o aceitam como pagamento final.
- Permite que mensuremos o valor e façamos comparações entre diferentes bens e serviços.
- Reduz nossa preferência temporal, pois nos permite economizar e gastar no futuro.

#### Meio de Troca



MP3 Player  
\$29.00



MP3 Player  
\$129.00



# O Poder do Dinheiro

- **Servir como reserva de valor:** O dinheiro deve manter seu valor ao longo do tempo, tornando-se útil como uma forma de poupar e investir o valor do trabalho humano. Isso permite que as pessoas usem o dinheiro como uma ferramenta para planejar o futuro e emprestar dinheiro umas às outras.

Qual é a sua reserva de valor?	BTC (USD)	Gold (USD)	USD (EUR)	ETH (USD)
March 14, 2019	\$3,846	\$1,293	€0.8817	\$136.86
March 14, 2020	\$5,258	\$1,529	€0.90056	\$127.76
Gain/Loss	+36.71%	+18.25%	+2.14%	-6.65%

Portanto, da próxima vez que você estiver economizando para algo especial, lembre-se de que o dinheiro é mais do que apenas uma forma de pagar por coisas - é uma ferramenta que o ajuda a planejar e investir no seu futuro.

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

**Exercício de classe.** De que função do dinheiro este é um exemplo?

1. Roby decidiu economizar uma parte de seus contracheques semanais para comprar um filhote de cachorro.
2. Jim compra duas fatias de pizza por \$8.30 na Ray's Pizza.

## 1.3.3 Características do dinheiro

Ao longo do tempo, as pessoas perceberam que o dinheiro deve possuir certas qualidades para ser eficaz como meio de troca. Essas características incluem durabilidade, portabilidade, divisibilidade, fungibilidade, escassez e aceitabilidade.

- **Durabilidade** se refere à capacidade do dinheiro de resistir à deterioração física e durar ao longo do tempo. Isso garante que o dinheiro possa circular na economia em um estado aceitável e reconhecível.

O ouro é um material durável que pode resistir ao desgaste, o que o torna uma boa representação da característica de durabilidade do dinheiro.

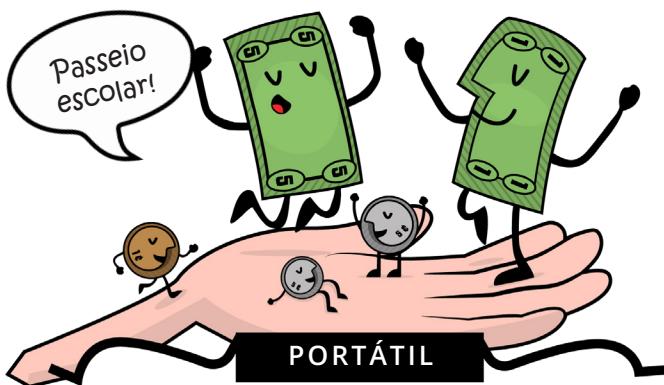




## Capítulo #1

- **Portabilidade** se refere à facilidade com que o dinheiro pode ser transportado e carregado. Isso permite que as pessoas usem o dinheiro para comprar e vender bens e serviços sem dificuldade.

Cartões de crédito são portáteis, pois podem ser facilmente carregados em uma carteira ou bolsa, sendo uma boa representação da característica de portabilidade do dinheiro.



- **Escassez** se refere à oferta limitada de dinheiro, o que ajuda a manter seu valor e evitar que tenhamos que gastar mais dinheiro para comprar a mesma quantidade de bens.

Selos colecionáveis, especialmente os raros e valiosos, podem ser uma boa forma de dinheiro porque são escassos e podem valorizar ao longo do tempo. Colecionadores de selos frequentemente usam seus selos como uma forma de investir sua riqueza e diversificar seu portfólio.



- **Aceitabilidade** Refere-se à ampla aceitação do dinheiro como forma de pagamento, para que as pessoas possam usá-lo para comprar e vender bens e serviços com confiança.

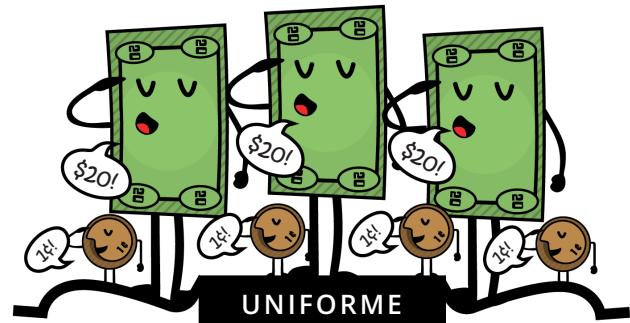
O dólar americano é amplamente aceito como forma de pagamento, o que o torna uma boa representação da característica de aceitabilidade do dinheiro.



- **Fungibilidade** refere-se à intercambiabilidade do dinheiro, de modo que uma unidade de dinheiro seja equivalente a outra unidade de mesmo valor.

O dinheiro deve ser uniforme.

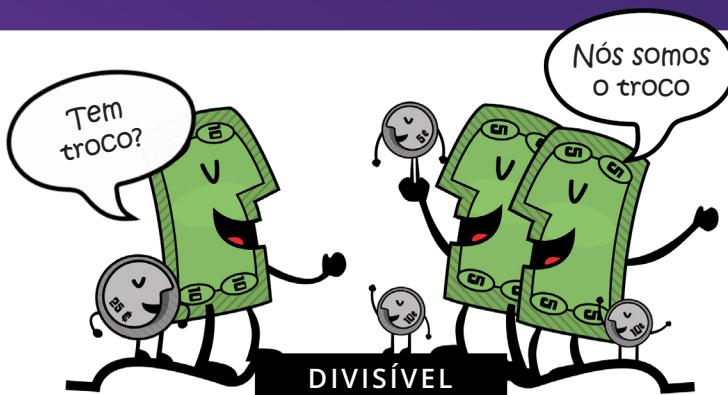
As moedas de cobre são uniformes em tamanho e peso, o que as torna uma boa representação da característica de uniformidade do dinheiro.



# O Poder do Dinheiro

- **Divisibilidade** refere-se à capacidade do dinheiro de ser dividido em unidades menores, para que as pessoas possam usá-lo para fazer compras de diferentes valores.

As cédulas de papel podem ser facilmente divididas em denominações menores, o que as torna uma boa representação da característica de divisibilidade do dinheiro.



No geral, essas características tornam o dinheiro uma ferramenta útil e eficaz para facilitar a troca e o comércio, e são essenciais para o desenvolvimento e a estabilidade das economias.

**Exercício em Classe.** Diferentes ativos possuem propriedades diferentes e desempenham as funções do dinheiro em graus variados. A sociedade determina, em última instância, qual ativo é utilizado como dinheiro com base em fatores como estabilidade, escassez, divisibilidade, transferibilidade e aceitação como meio de troca.

Para determinar o quão bem diferentes itens atendem às características específicas do dinheiro, você pode atribuir uma pontuação de 1 a 5 para cada característica. Ao somar as pontuações para cada item, você pode determinar qual é mais adequado para ser uma forma de dinheiro.

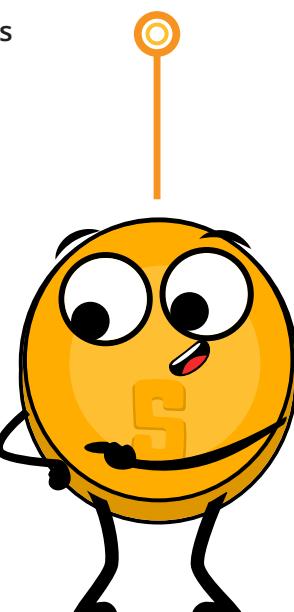
[ 0 = Terrível; 3 = Ok; 5 = Excelente ]

\* Por favor, não preencha a coluna para **Bitcoin**; retornaremos a ele mais tarde no curso.



Use as seguintes perguntas para ajudar a determinar o quão bem os diferentes itens na tabela atendem às características do dinheiro:

- **Durabilidade:** O dinheiro pode resistir ao desgaste ao longo do tempo?
- **Portabilidade:** O dinheiro pode ser facilmente transportado e usado em diferentes locais?
- **Fungibilidade:** O dinheiro é intercambiável com outras formas de dinheiro?
- **Aceitabilidade:** O dinheiro é amplamente aceito como forma de pagamento?
- **Escassez:** O dinheiro é escasso e não excessivamente abundante?
- **Divisibilidade:** O dinheiro pode ser dividido em unidades menores para transações?





Características de um bom dinheiro	Vacas	Cigarros	Dimantes	Euros	Bitcoin
<b>DURÁVEL</b>					
<b>PORTÁTIL</b>					
<b>UNIFORME</b>					
<b>ACEITÁVEL</b>					
<b>ESCASSO</b>					
<b>DIVISÍVEL</b>					
<b>TOTAL</b>					

### 1.3.4 Tipos de Dinheiro

Quando se trata de dinheiro, existem duas principais categorias: **física e digital**.

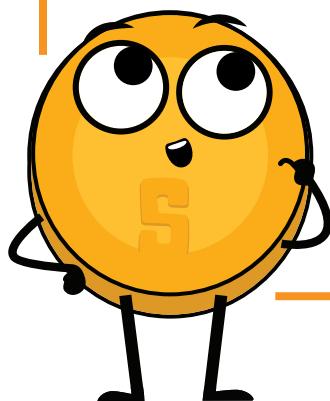
Para o **dinheiro físico**, temos três opções:

- **Dinheiro fiduciário** é o que usamos todos os dias, como notas de papel e moedas. É emitido pelo governo e aceito como meio de troca, mesmo que não seja respaldado por nenhuma mercadoria física.
- **Dinheiro representativo** representa uma reivindicação sobre uma mercadoria física. Assim como o dinheiro fiduciário, ele também pode ser uma nota de papel (como um certificado de ouro ou prata), mas, ao contrário do dinheiro fiduciário, é respaldado por uma mercadoria física considerada valiosa pela sociedade. Isso significa, por exemplo, que um certificado de ouro no valor de um dólar pode ser trocado por uma quantia equivalente a um dólar em ouro em um banco, o que costumava ser o caso em muitos países.
- **Dinheiro comoditizado** é um objeto físico que possui valor intrínseco e é amplamente aceito como meio de troca. Ouro e prata se encaixam nessa categoria.

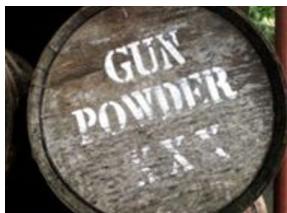
# O Poder do Dinheiro



Nem todo dinheiro é igual!



## Dinheiro Mercadoria



Objetos como pólvora já serviram como dinheiro mercadoria.

## Dinheiro Representativo



Dinheiro representativo como esse certificado de prata poderia ser trocado por prata.

## Dinheiro Fiduciário



Hoje, as notas do Federal Reserve são dinheiro fiduciário, decretado pelo governo federal como uma forma aceitável de pagar dívidas.



As **Commodities** (ou dinheiro mercadoria) são frequentemente considerados “fungíveis” e têm uma qualidade consistente. Por exemplo, um barril de petróleo é geralmente considerado o mesmo que qualquer outro barril de petróleo, independentemente de onde ele venha ou quem o produziu.

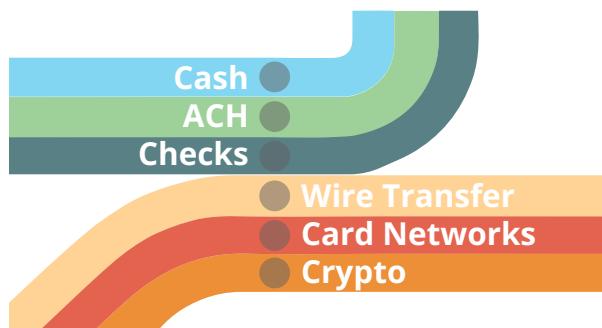


As **Plataformas de pagamento** são como rodovias digitais que auxiliam as moedas eletrônicas a se moverem de um lugar para outro online. Elas facilitam, agilizam e tornam mais seguros os pagamentos online, seja utilizando uma criptomoeda como o **Bitcoin** ou um método de pagamento tradicional, como um cartão de crédito.



**Moedas Digitais do Banco Central (CBDCs):** Essas são versões digitais da moeda fiduciária de um país, emitidas e respaldadas pelo banco central, e, portanto, intermediadas pelo governo. Isso significa que o governo atua como intermediário na transação.

**Moedas eletrônicas** são um tipo de dinheiro que pode ser usado para transações online. Elas são como versões digitais do dinheiro convencional, como dólares ou euros, e podem ser usadas para comprar e vender produtos e serviços online por meio de **plataformas de pagamento**.





**As plataformas de pagamento digital no sistema financeiro tradicional** consistem na tecnologia e sistemas que permitem que os pagamentos eletrônicos sejam feitos e processados, como servidores bancários, bancos de dados e redes seguras. No entanto, sempre há um intermediário, como um banco ou instituição financeira, que cobra uma taxa e tem autoridade para aceitar, cancelar, reverter ou atrasar transações.

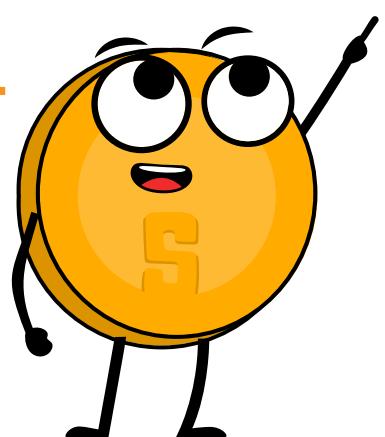
Os principais tipos de plataformas de pagamento digital no sistema financeiro intermediado incluem:

- **Redes de Cartões:** São redes que facilitam a transferência de fundos entre instituições financeiras e comerciantes quando um cliente faz uma compra usando um cartão de débito ou crédito. Exemplos incluem Visa, Mastercard e American Express.
- **Carteiras Digitais:** Uma carteira digital é uma conta online que permite aos usuários armazenar e gerenciar suas moedas eletrônicas (ou seja, ativos digitais, como moeda digital, criptomoeda ou pontos de fidelidade). Os usuários podem fazer pagamentos usando sua carteira eletrônica transferindo fundos de sua conta para a conta do destinatário.
- **Criptomoedas:** São moedas digitais que utilizam plataformas de pagamento digital, ou “rodovias digitais”, para se moverem de um lugar para outro online. Podemos pensar nelas como carros que podem viajar diretamente de um ponto a outro sem parar em intermediários, como praças de pedágio em uma rodovia. Isso significa que as criptomoedas podem ser transferidas e trocadas diretamente, sem a necessidade de um intermediário como um banco.

## O Processo de Pagamento com Cartão de Crédito



O processo de pagamento com cartão de crédito é um exemplo de uma plataforma de pagamento.



As **Stablecoins** são criptomoedas projetadas para manter um valor estável em relação a um ativo, como o dólar americano. Algumas são respaldadas por ativos físicos e todas são utilizadas como forma de armazenar valor ou realizar transações sem a volatilidade que pode estar associada a outras criptomoedas.

## O Poder do Dinheiro

Uma moeda que opera sem intermediários é mais eficiente e benéfica para a sociedade. Isso impede que algumas pessoas controlem o fornecimento de dinheiro e concentrem seu poder.

No entanto, encontrar uma tecnologia que facilite transações seguras sem depender da confiança entre as partes tem sido um desafio ao longo da história. Para alcançar isso, uma moeda deve ser criada para operar como a internet, onde o controle é distribuído entre todos e ninguém ao mesmo tempo. Isso requer o acordo de todas as partes, incluindo aqueles que possuem poder, para abrir mão do controle pelo bem maior.

Mas como seria essa moeda?





*Capítulo #1*





# *Capítulo#2*

## *Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo*

### **2.0** Introdução

#### **2.0.1** Exercício em Classe: Jogo de Trocas

### **2.1** Formas Primitivas de Dinheiro

### **2.2** De Commodities para Promissórias

### **2.3** Transição de Dinheiro Sólido para Dinheiro Instável

### **2.4** Onde Estamos Hoje?

### **2.5** O Preço do Controle: Uma Análise sobre Vigilância, Censura e Regulação

#### **2.5.1** O Surgimento de uma Sociedade sem Dinheiro em Espécie

#### **2.5.2** Vigilância

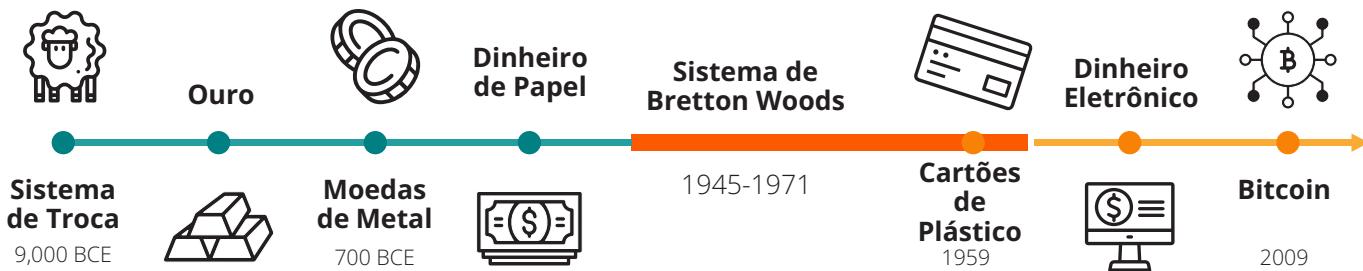
#### **2.5.3** Regulações Financeiras e Censura

# Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo

## 2.0 Introdução

O conceito de dinheiro evoluiu ao longo do tempo. Em suas formas iniciais, o dinheiro era usado para facilitar o comércio e a troca de bens e serviços.

- Nas civilizações antigas, as pessoas dependiam da troca direta de bens e serviços, conhecida como troca direta, sem o uso de um meio de troca.
- Posteriormente, moedas de metal e cédulas de papel foram introduzidas como formas mais convenientes de dinheiro, abrindo caminho para os sistemas financeiros sofisticados que temos hoje em dia.



Neste capítulo, embarcaremos em uma jornada através do tempo, vivenciando a evolução do dinheiro em primeira mão. Vamos rastrear suas origens e observar como ele mudou e se adaptou ao longo da história.

### 2.0.1 Exercício em Classe: Jogo de Trocas

#### ● Rodada #1 - Troca Direta

Estamos no ano 6000 a.C. e, como podemos imaginar, o dinheiro como o conhecemos ainda não foi inventado. Você está na Mesopotâmia e realiza trocas diretas de bens e serviços com outras pessoas através da **troca direta**.



Como observação adicional, muitas empresas ainda aceitam pagamentos não monetários por seus serviços, e os governos tratam essas transações de troca da mesma forma que as transações em moeda para fins de relatórios fiscais.

● Corte sua folha de papel na linha tracejada. Seu objetivo é trocar seu “ter” o maior número de vezes necessário para finalmente obter seu “desejo” original. Você não pode mudar seu “desejo” original. Você terá 5 minutos para alcançar o objetivo deste exercício.

● Quando seu novo “ter” corresponder ao seu “desejo” original, retorne ao seu assento. Após o tempo acabar, se você não tiver encontrado um parceiro de troca, retorne ao seu assento mesmo assim.



Levante a mão se você conseguiu obter o que queria após uma troca. Duas? Três?

**Perguntas.** Responda as seguintes perguntas de forma breve, porém substancial..

1. Por que alguns de vocês conseguiram encontrar alguém para trocar e outros não?

---

---

2. Quais são os benefícios do escambo?

---

---

3. Com base na sua experiência com este exercício, quais são as desvantagens de usar o escambo?

---

---

### ● Rodada #2 - Dinheiro Mercadoria

Avance rapidamente e viaje para a costa oeste da África por volta do século XIV a.C. O escambo se tornou tedioso e ineficiente. Evoluímos como civilização e agora estamos usando **dinheiro mercadoria**.

#### *Conchas de caramujo para moedas*



1,300 BCE



1,000 BCE



687 BCE

**FUN FACT**  
As conchas de caramujo eram aceitas como moeda de curso legal em algumas partes da África até o século XX.

Essas proto-moedas tinham formato oval, eram feitas de "eletro" (uma liga de ouro/prata) e tinham um desenho em apenas um dos lados.

**1,300 BCE**

As conchas de caramujo são a forma predominante de pagamento na maioria da Ásia, África, Oceania e algumas partes da Europa.

**1,000 BCE**

A dinastia Zhou Ocidental da China começa a utilizar moedas de metal.

**687 BCE**

O rei Alyattes da Lídia (atualmente Turquia) ordena a primeira cunhagem de moedas de metal no mundo ocidental.

# **Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo**

Seu professor deu a você um macarrão (por simplicidade). Vamos supor que, por convenção, o preço de cada bem vale um macarrão. Seu objetivo novamente é obter o que você “quer”. Mas agora, nossa espécie se tornou um pouco mais inteligente e encontrou uma maneira de resolver certos problemas.

- Por que consideramos o macarrão como uma mercadoria-moeda?
- Como obtemos as coisas que queremos agora?
- O macarrão redondo foi mais fácil?
- Por que você acha que o dinheiro substituiu as mercadorias?
- De que maneiras o uso de mercadoria-moeda é mais eficiente do que a troca direta?
- Quais são as desvantagens de usar macarrão como moeda?

O que você acha que aconteceu quando a Espanha começou a trazer grandes carregamentos de macarrão para a sua comunidade (ouro e prata das Américas de volta para a Espanha)?

---

---

---

---

---

## **2.1 Formas Primitivas de Dinheiro**



Assista a este curto vídeo para aprender sobre as Origens das Trocas, na série “A História do Dinheiro em Papel”.



Uma situação, conhecida como **dupla coincidência de desejos**, é necessária em qualquer sistema de troca, pois as pessoas devem sempre encontrar alguém que tenha o que desejam, mas também queira o que têm para oferecer.



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

Eu te darei sapatos em troca do seu trigo.

Eu não preciso de sapatos. Eu preciso de roupas.

Eu quero sapatos, mas eu não tenho trigo.



Vamos supor:

- Joseph quer trocar sua banana pelo coco de Yael.
- Mas Yael só quer trocar seu coco pela manga de Tammy.
- E Tammy só quer trocar sua manga pela banana de Joseph.
- Eles estão presos em um ciclo interminável de troca de frutas sem uma coincidência dupla de desejos.
- Joseph sugere que eles troquem suas frutas por um refrigerante gelado, mas eles percebem que estão em uma ilha remota e não há refrigerante.
- Eles decidem apenas sentar na praia e desfrutar de suas frutas em silêncio.

O uso de uma **unidade de conta comum**, como um “refrigerante”, torna a troca e o comércio muito mais eficientes. Nos tempos antigos, as pessoas começaram a usar contas, conchas e outros itens que tinham valor em sua sociedade como meio de troca.

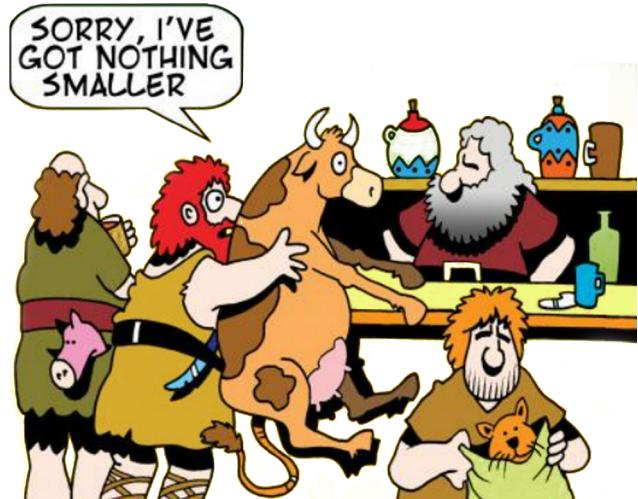
### 2.2 De Commodities para I.O.U's

Conforme você e sua comunidade se envolvem cada vez mais na troca e no comércio, você percebe as limitações do uso da troca direta e de outras formas de troca não monetária. Você decide adotar o uso de **moedas de metal como forma de dinheiro**.



Essas moedas de metal são feitas de materiais valiosos como ouro e prata, e elas funcionam como meio de troca e unidade de conta para facilitar a troca e o comércio: **dinheiro comoditizado**.

### Por que o dinheiro foi inventado



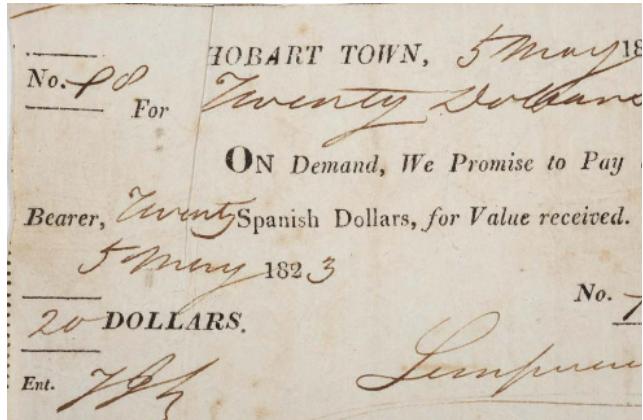
Este é o segundo episódio, chamado “Não Apenas Macarrão”, de “A História do Dinheiro em Papel”.



# ***Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo***

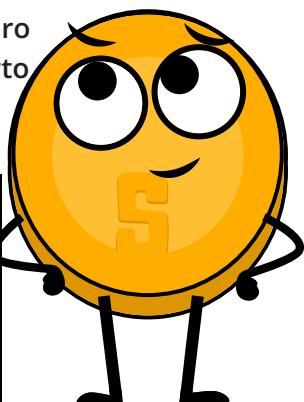
No entanto, à medida que você começa a usar moedas de metal com mais frequência, você encontra algumas desvantagens. Elas podem ser pesadas e inconvenientes de carregar em transações grandes, e você percebe que algumas pessoas estão se aproveitando do sistema derretendo as moedas e criando novas misturando-as com metais mais baratos, o que faz os preços subirem e prejudica a confiança no sistema.

Na tentativa de resolver esses problemas, você e sua comunidade começam a usar recibos de papel como forma de dinheiro. Esses recibos de papel, que têm suas origens na antiga China, são uma forma conveniente e facilmente trocável de moeda. Eles são lastreados em ouro e outros metais valiosos e podem ser convertidos nesses metais durante os séculos XVII ao XIX. Isso permite que você tenha uma forma mais portátil e facilmente transferível de dinheiro, ao mesmo tempo em que mantém o valor e a segurança dos metais preciosos.



## **2.3 Transição de Dinheiro Seguro para Dinheiro Insustentável**

O que acontece quando você realmente tenta colocar em prática a doutrina do dinheiro de papel? Descubra no quarto episódio de "A História do Dinheiro em Papel".



Avançando rapidamente para o século XVII na Suécia. Agora você depende completamente dos bancos para armazenar seus ativos valiosos. No entanto, você começa a perceber algo suspeito acontecendo com esses banqueiros. Parece que eles estão emitindo mais recibos de papel do que possuem em ouro armazenado, permitindo-lhes criar mais dinheiro do que têm ativos para respaldá-lo. Essa prática sorrateira permite que os banqueiros lucrem com a diferença entre o valor dos recibos de papel e o valor do ouro que estão mantendo para seus clientes.





Você percebe que isso marca uma mudança importante na forma como o dinheiro funciona. Você está passando de um sistema de dinheiro sólido (ou seja, dinheiro respaldado por metais preciosos) para um sistema de dinheiro falso (ou seja, moeda fiduciária não respaldada por uma mercadoria física). Essa transição não aconteceu da noite para o dia, mas foi um processo gradual influenciado por vários fatores. A Revolução Industrial, com sua produção em massa e urbanização, desempenhou um papel, assim como o crescimento de sistemas financeiros avançados, como bancos e mercados de ações. O surgimento de bancos centrais e outras autoridades monetárias contribuiu para a centralização ou controle do dinheiro, levando à emissão de moedas fiduciárias para sustentar o crescimento econômico.

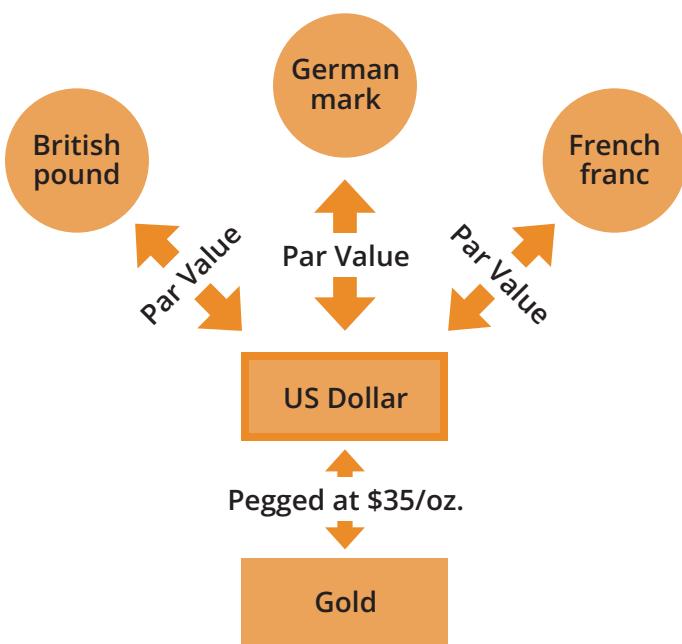


No entanto, você também começa a ver as **desvantagens dessa centralização**, incluindo o consumo irresponsável, o aumento da dívida e a manipulação dos cidadãos por meio de incentivos econômicos.

Até a Primeira Guerra Mundial, você podia converter seu dinheiro em papel em uma quantidade pré-determinada de ouro. Mas as duas guerras mundiais e a crise econômica de 1929 puseram fim a isso. Em 1944, foi assinado o Acordo de Bretton Woods, estabelecendo o dólar dos Estados Unidos como a moeda de reserva mundial e fixando o valor do dólar americano ao preço do ouro a uma taxa de US\$ 35 por onça. As moedas de outros países são vinculadas ao dólar, o que ajuda a estabilizar os mercados financeiros internacionais.

### Sistema Bretton Woods

(1945-1972)



Infelizmente, o sistema começa a entrar em colapso no final da década de 1960, levando ao Choque de Nixon em 1971, quando o governo dos Estados Unidos suspende a conversibilidade do dólar em ouro. Isso marca o fim do padrão ouro e o início de um mundo impulsionado pela criação e acumulação de dívidas.

Conforme você segue com sua vida diária, você começa a perceber que o valor do dinheiro não é mais tão estável como costumava ser. Assim como uma régua flexível dificulta a medição precisa do comprimento de uma mesa, viver em um mundo de moeda fiduciária, onde o valor do dinheiro está sujeito à imprevisibilidade daqueles no poder, também pode dificultar a medição precisa do valor de bens e serviços. Você sente confusão e desconforto ao se adaptar a um mundo onde o valor do dinheiro não está mais ligado a uma mercadoria física como o ouro.

# **Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo**

Você observa os impactos dessa mudança na economia global e começa a questionar a estabilidade e confiabilidade das moedas fiduciárias. Você percebe que, neste mundo moderno, o dólar já não é mais fixo e consistente como era quando estava vinculado ao ouro, mas sim sujeito a flutuações. Isso torna mais difícil usar o dólar como unidade de conta, pois seu valor é afetado por vários fatores, incluindo inflação (aumento de preços), taxas de juros, força da economia do país, eventos políticos, especulação de mercado e demanda no comércio internacional. Pode ser um momento confuso e imprevisível, enquanto você tenta navegar pelo valor em constante mudança do dólar e seu impacto em sua vida diária.

Apesar dos esforços para melhorar a qualidade de vida por meio de sistemas monetários modernos, maior eficiência, maior acesso à informação e comunicação aprimorada, a maioria das pessoas começa a experimentar uma queda em seus padrões de vida devido a:

- ① Abuso da centralização.
- ② Aumento dos preços.
- ③ Estagnação dos salários reais.
- ④ Enfraquecimento das moedas.
- ⑤ A necessidade de gastar mais dinheiro por menos coisas.

Isso representa desafios para aqueles com recursos econômicos mais baixos, que podem ter acesso limitado à educação, crédito, recursos, redes sociais e representação política, o que pode resultar em desvantagens em sua capacidade de ter sucesso.

Como resultado, os ricos parecem continuar enriquecendo e os pobres parecem continuar empobrecendo.

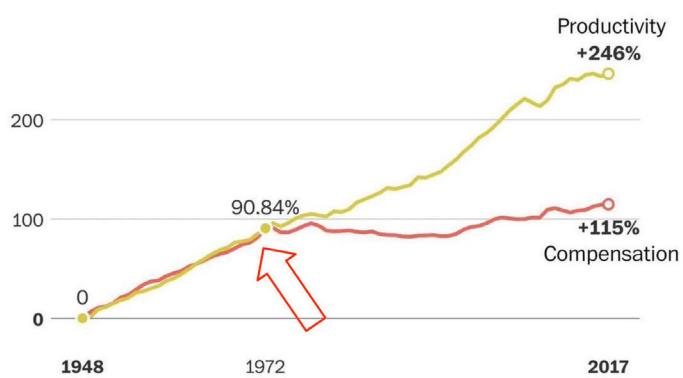


"Eu não acredito que teremos dinheiro bom novamente até tirarmos a coisa das mãos do governo... tudo o que podemos fazer é, de alguma forma dissimulada e indireta, introduzir algo que eles não possam impedir."

**Friedrich Hayek,**

Nobel Prize Winner of Economics

**Crescimento da produtividade e da remuneração por hora (1948-2017)**



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

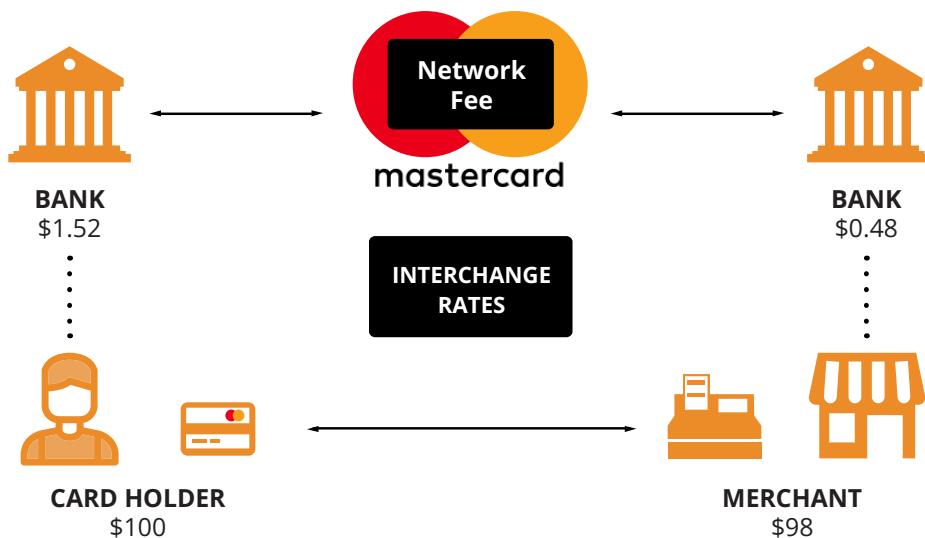




## 2.4 Onde estamos hoje?

Hoje, chegamos longe desde a introdução do primeiro cartão de crédito nos anos 1950. Com um simples deslize do plástico, podemos comprar o que quisermos, quando quisermos, sem complicações. É como abrir um mundo de possibilidades infinitas, e a emoção de descobrir o que ele reserva é palpável... ou assim pensávamos. Pouco sabíamos que nossa dependência do crédito teria efeitos colaterais dolorosos, como o aumento do custo geral dos bens e o incentivo a uma certa economia condenada ao fracasso.

À medida que a tecnologia avança, também muda a forma como lidamos com o dinheiro. A internet se torna um grande player no mundo financeiro, com serviços bancários online e sites de comércio eletrônico que possibilitam gerenciar e gastar dinheiro inteiramente online.



Então, em 2009, a primeira criptomoeda descentralizada, o **Bitcoin**, é criada. À medida que sua popularidade cresce, ela inspira a criação de novas tecnologias e fronteiras desconhecidas para o futuro do dinheiro. E assim, como vamos aprender, voltamos ao ponto de partida, do dinheiro sólido ao dinheiro insustentável e de volta novamente, o dinheiro sólido encontrando novo impulso pela primeira vez em quase cem anos.

## 2.5 O Preço do Controle: Um Olhar sobre Vigilância, Censura e Regulação

### 2.5.1 A Ascensão de uma Sociedade sem Dinheiro em Espécie

Quando o primeiro cartão de crédito foi introduzido na década de 1950, as pessoas comemoraram a ideia de nunca mais precisarem carregar dinheiro em espécie. Não mais ter que procurar por moedas soltas ou momentos embaralhos ao escrever cheques no caixa. Todos esses intermediários chatos agora podem levar sua parte sem você nem perceber, assim como uma tarifa em uma rede. Ah, a conveniência das finanças modernas.

# ***Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo***

Mas com o surgimento das moedas digitais, como as CBDCs (Central Bank Digital Currencies), parece que passamos de pagar uma taxa pelo uso da rede para ter que pedir permissão. Pior ainda, agora esperamos ser revistados, escaneados e examinados pelo governo sempre que passamos por algum lugar. Controle e vigilância tomaram o lugar da conveniência. E assim como a taxa da rede, essas intrusões em nossas vidas financeiras vêm com um custo, seja monetário, uma violação da privacidade ou a perda da autonomia.

À medida que mais de nossas **transações** diárias se tornam online, o uso de dinheiro em espécie diminui. Governos e instituições financeiras ao redor do mundo estão promovendo o uso de pagamentos eletrônicos e reprimindo o uso de dinheiro físico. Essa tendência tem gerado um debate sobre o futuro do dinheiro em espécie e as potenciais consequências de uma sociedade sem dinheiro em papel.

A “**guerra ao dinheiro em espécie**” é um termo que se refere aos diversos esforços para reduzir o uso de dinheiro físico, remover notas de alto valor e promover o uso de pagamentos eletrônicos.

Os defensores da guerra ao dinheiro em espécie argumentam que isso tornará as **transações** mais rápidas, convenientes e seguras. No entanto, os críticos temem que isso possa levar à perda de privacidade e inclusão financeira, além de aumentar os riscos de fraudes e ataques cibernéticos.



**Q:** Como os métodos bancários tradicionais colocam em risco os dados financeiros dos indivíduos?

**R:** Com cartões de crédito, cartões de débito, transferências bancárias e outras redes de pagamento controladas centralmente, os indivíduos estão fornecendo seus dados privados de transações financeiras a terceiros e potencialmente sacrificando seus direitos à privacidade.

Neste infográfico, forneceremos uma visão geral da guerra ao dinheiro em espécie e exploraremos todos os lados do debate. Analisaremos os motivos por trás da busca por uma sociedade sem dinheiro em espécie, os desafios e preocupações que isso levanta e os impactos potenciais sobre indivíduos, empresas e a sociedade como um todo.



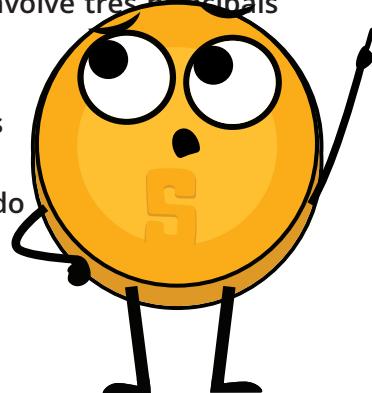
A pergunta é: estamos dispostos a pagar o preço pela conveniência das finanças modernas, ou vamos buscar opções alternativas que priorizem nossa liberdade e privacidade?



## **A Guerra Global ao Dinheiro em Espécie**

Existe um esforço global por parte dos legisladores para eliminar o uso de dinheiro físico em todo o mundo. Esse movimento é frequentemente chamado de “A Guerra ao Dinheiro em Espécie” e envolve três principais atores:

- Os Iniciadores
- O Inimigo
- O Fogo Cruzado



Desjardins, Jeff. “The Global War on Cash.” Visual Capitalist, 27 Jan. 2017, <https://www.visualcapitalist.com/global-war-cash/>.



## Capítulo #2



**QUEM?**  
Governos, bancos centrais

**POR QUE?** A eliminação do dinheiro em espécie tornará mais fácil rastrear todos os tipos de transações, incluindo aquelas realizadas por criminosos.

**QUEM?**  
Criminosos, terroristas.

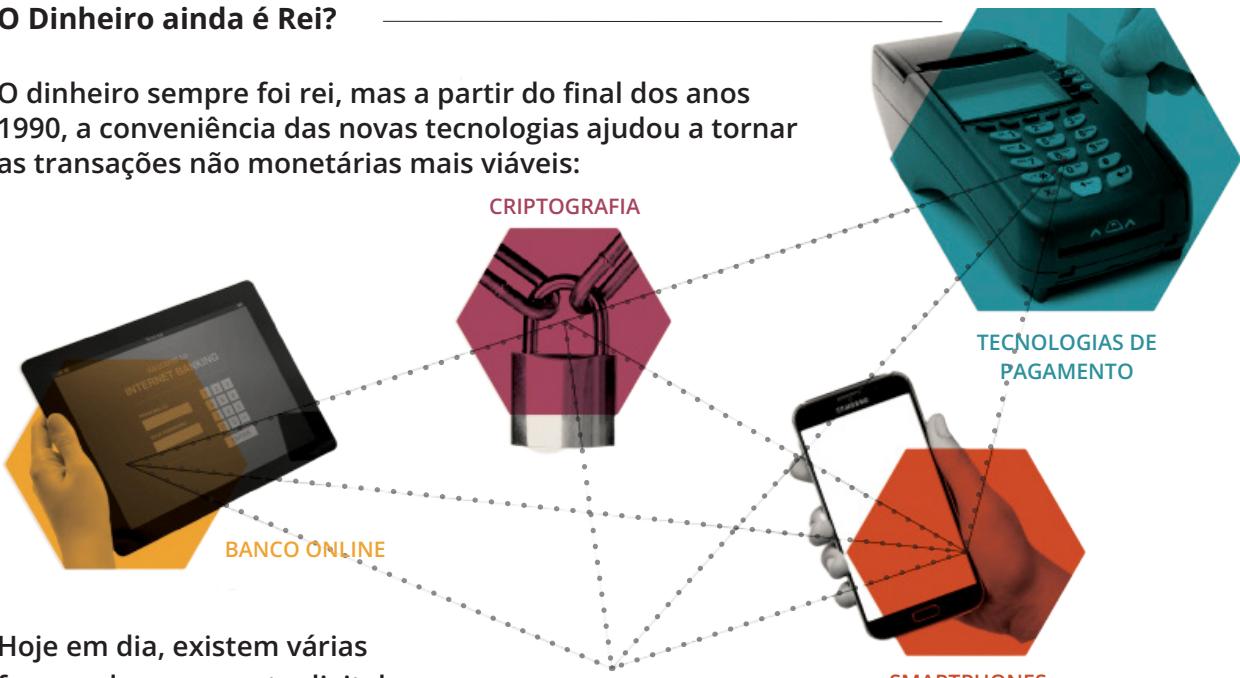
**POR QUE?** As notas de grande denominação facilitam a realização de transações ilegais e aumentam o anonimato.

**QUEM?**  
Cidadãos

**POR QUE?** A eliminação coercitiva do dinheiro físico terá potenciais repercussões na economia e nas liberdades sociais.

### O Dinheiro ainda é Rei?

O dinheiro sempre foi rei, mas a partir do final dos anos 1990, a conveniência das novas tecnologias ajudou a tornar as transações não monetárias mais viáveis:



Hoje em dia, existem várias formas de pagamento digital, incluindo:



INTERMEDIÁRIOS



BANCO ONLINE



SMARTPHONES



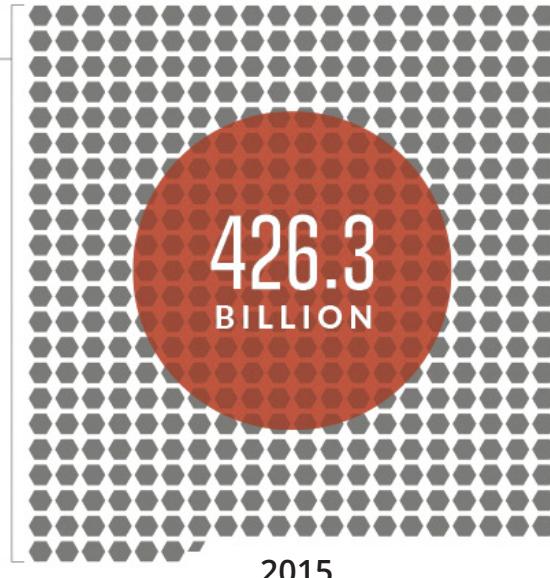
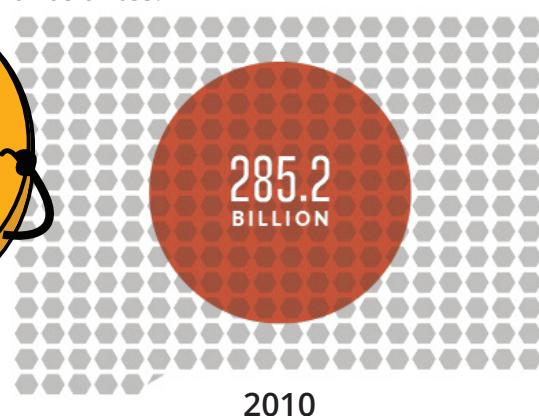
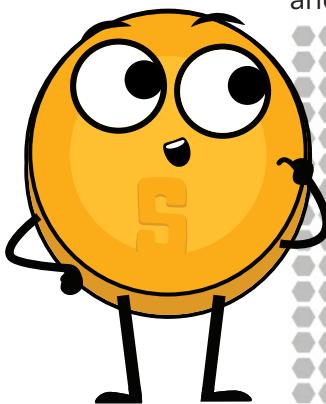
CRİPTOMOEDAS

# Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo



Até 2015, houve 426 bilhões de transações sem dinheiro em todo o mundo.

- um aumento de 50% em relação a cinco anos antes.

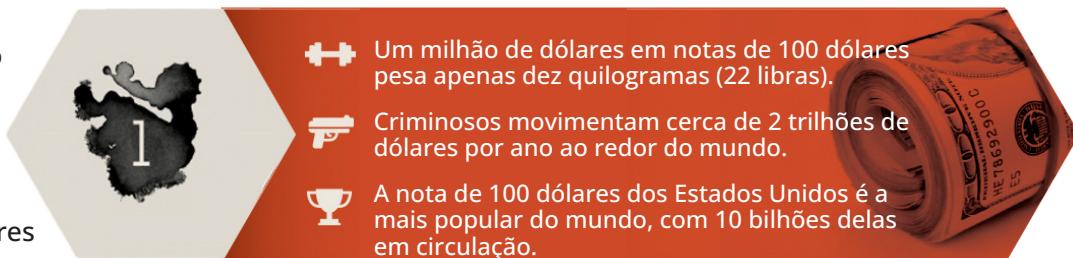


## Os Primeiros Tiros Disparados.

O sucesso dessas novas tecnologias levou os legisladores a propor que todas as transações agora sejam digitais. Aqui está o argumento deles a favor de uma sociedade sem dinheiro em espécie:



A remoção de notas de alta denominação de circulação torna mais difícil para terroristas, traficantes de drogas, lavadores de dinheiro e sonegadores



Dinheiro que é rastreável significa maiores receitas fiscais.

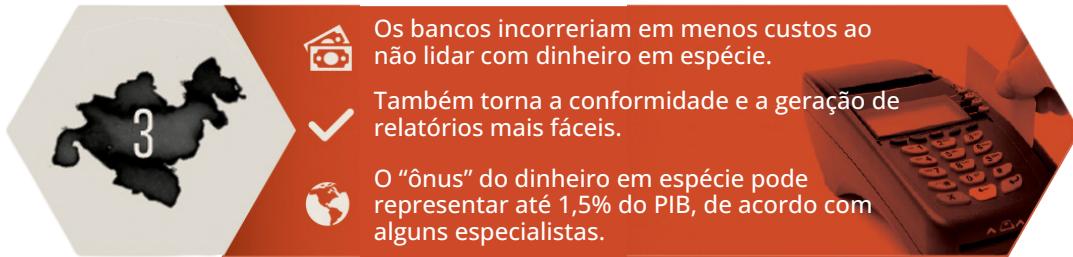
Isso também significa que há um terceiro envolvido em todas as transações.

Os bancos centrais podem ditar as taxas de juros para incentivar (ou desencorajar) os gastos, a fim de controlar a inflação. Isso inclui políticas de ZIRP (taxa de juros nominal próxima de zero) ou NIRP (taxa de juros nominal negativa).



Isso confere aos reguladores maior controle sobre a economia.

As transações sem dinheiro em espécie são mais rápidas e eficientes.





## Capítulo #2

Para que isso seja possível, dizem que o dinheiro em espécie, especialmente as notas de alta denominação, devem ser eliminadas.



Afinal, o dinheiro em espécie ainda é utilizado em cerca de 85% de todas as transações em todo o mundo.

### Pego no Fogo Cruzado

Os tiros disparados pelos governos na guerra contra o dinheiro em espécie podem ter várias vítimas não intencionais.



- ▶ Transações sem dinheiro em espécie sempre envolveriam algum intermediário ou terceiro.
- ▶ Aumento do acesso do governo às transações pessoais e registros.
- ▶ Certos tipos de transações (jogos de azar, etc.) poderiam ser proibidos ou congelados pelos governos.
- ▶ Criptomoedas descentralizadas poderiam ser uma alternativa para tais transações.

Poupadoresem não teriam mais a liberdade individual de armazenar riqueza "fora" do sistema.



Eliminar o dinheiro em espécie torna as taxas de juros negativas (NIRP) uma opção viável para formuladores de políticas.

Uma sociedade sem dinheiro em espécie também significa que todos os poupadoresem estariam "na linha de fogo" em cenários de resgate bancário.

Os poupadoresem teriam habilidades limitadas para reagir a eventos monetários extremos, como deflação ou inflação.



- ▶ A demonetização rápida violou os direitos das pessoas à vida e alimentação..
- ▶ Na Índia, a remoção das notas de 500 e 1.000 rúpias causou várias tragédias humanas, incluindo pacientes que estão sendo negados tratamento e pessoas incapazes de comprar alimentos.
- ▶ A demonetização também prejudica as pessoas e pequenos negócios que obtêm seu sustento nos setores informais da economia

Com toda a riqueza armazenada digitalmente, o potencial risco e impacto do cibercrime aumenta.



Hackeamento ou roubo de identidade poderiam destruir as economias de uma vida das pessoas.

O custo de violações de dados online atingiu US\$ 2,1 trilhões até 2019, de acordo com a Juniper Research.



# **Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo**

## **2.5.2 Vigilância**

A vigilância é uma questão delicada. Por um lado, ela ajuda a identificar pessoas envolvidas em atividades ilícitas, como lavagem de dinheiro. No entanto, quanto mais fraudes ocorrem, mais vigilância é necessária, o que pode levar a invasões de privacidade por meio da tecnologia. Empresas privadas também podem coletar e comercializar suas informações pessoais em benefício próprio, e os riscos dessa vigilância podem incluir golpes, assédio, extorsão, roubo de identidade e até mesmo rastreamento de suas compras com cartão. Além disso, com o aumento da inteligência artificial e do aprendizado de máquina, está se tornando ainda mais fácil para governos e empresas invadirem nossa privacidade. Além disso, muitas vezes são as pessoas que já estão em desvantagem ou desprivilegiadas que são as mais afetadas.

*O impacto da inteligência artificial e da tecnologia na privacidade e vigilância futuras.*

Efeito Futuro	Os ricos	Os Pobres
Acesso a informações pessoais.	Podem ter acesso a informações pessoais extensas e usá-las para tomar decisões informadas.	Podem não ter acesso a essas informações e podem depender de fontes desatualizadas ou não confiáveis.
Capacidade de moldar o mundo de acordo com seus próprios interesses.	Podem usar seu acesso aos dados para moldar o mundo de acordo com seus próprios interesses.	Podem ter pouca influência sobre o que acontece.
Controle sobre os outros.	Podem exercer controle sobre os pobres por meio de seu acesso aos dados, resultando em uma perda de liberdade individual.	Têm pouco controle; frequentemente são controlados.
Vulnerabilidade a golpes digitais, assédio online, extorsão e roubo de identidade.	Provavelmente são menos vulneráveis a esses problemas com mais informações e mais proteção contra tais golpes.	Podem ser mais vulneráveis a esses problemas devido à falta de acesso a recursos e informações.

## **2.5.3 Regulações Financeiras e censura**

Regulações financeiras, censura e proibições podem ser uma realidade emocional e financeiramente onerosa para a sociedade e seus cidadãos. Elas assumem muitas formas, tais como:

- **Controles de Capital ou Sanções:** Quando os gastos ficam fora de controle, os governos podem impor controles de preços para tentar resolver o problema. No entanto, às vezes esses controles pioram as coisas. Os governos também podem limitar a quantidade de dinheiro que os cidadãos podem transferir, trocar ou levar para fora do país. Além disso, alguns governos podem criar um sistema de Pontuação de Crédito Social que pode ser usado para controlar os cidadãos.



- Como funciona o sistema de Pontuação de Crédito Social da China? Na China, transações financeiras e outros dados de todos os cidadãos são coletados centralmente e utilizados para criar um sistema de Pontuação de Crédito Social que pode ser usado para controlar os cidadãos.
- Considere o que aconteceu na Grécia em 2015 - os cidadãos só podiam sacar 60 euros por dia por determinação do governo. Da mesma forma, os chineses só podem enviar quantias limitadas de renminbi para fora do país.
- Houve várias ocasiões na Argentina em que o governo impôs controles cambiais rigorosos para tentar estabilizar o peso. Um exemplo foi em 2011, quando o governo implementou controles de capital para conter a saída de dólares do país e evitar uma desvalorização maior do peso. Outro exemplo ocorreu em 2019.
- **Políticas Bancárias Restritivas:** Você já tentou sacar dinheiro de um caixa eletrônico apenas para descobrir que atingiu o limite diário?

Outalvez você tenha tentado transferir dinheiro para um amigo e tenha sido informado que existe um valor máximo que você pode enviar. Esses são apenas alguns exemplos de políticas bancárias restritivas que podem dificultar o acesso ao seu próprio dinheiro e fazer o que você quiser com ele.

Os bancos também podem cobrar taxas para a maioria das transações e podem ter horários de funcionamento limitados, dificultando o acesso ao seu dinheiro ou a tomada de decisões financeiras. Carregar muito dinheiro aumenta o risco de roubo. Além disso, os bancos às vezes oferecem empréstimos com juros mais baixos para os ricos, enquanto expõem os pobres a agiotas e empréstimos com juros mais altos. Com isso, o sistema financeiro muitas vezes se beneficia da lacuna entre ricos e pobres.



Verifique o seguinte artigo: "O que você precisa saber sobre movimentação de dinheiro dentro e fora da China".

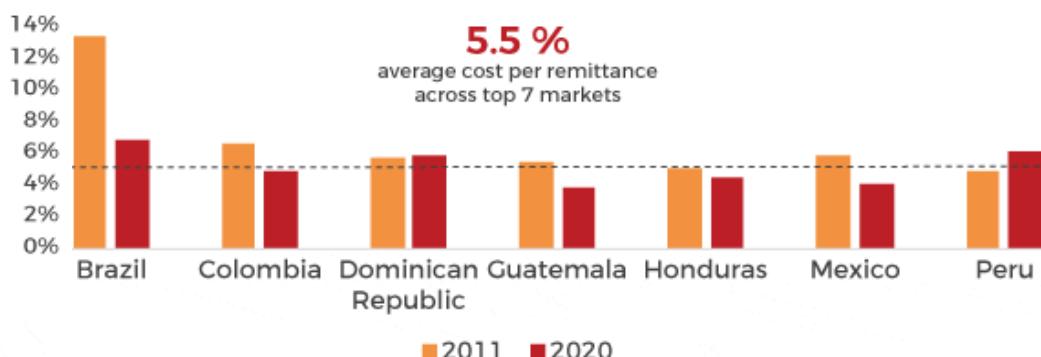


# ***Da Troca Direta para o Bitcoin e as Moedas Digitais do Banco Central: Uma Viagem no Tempo***

- **Remessas caras:** Enviar dinheiro para outros países pode ser caro devido às taxas cobradas pelos bancos e outras instituições financeiras. Muitas famílias de baixa renda em países em desenvolvimento dependem do dinheiro enviado por parentes que vivem no exterior para sobreviver. No entanto, as altas taxas cobradas pelas transferências internacionais podem reduzir o valor recebido pelo destinatário. Isso pode dificultar para as famílias o acesso a necessidades básicas como comida, moradia e educação.

**Taxas médias de remessa na América Latina**

(% of transaction)



- Imagine uma família em uma vila rural no Brasil que depende do dinheiro enviado por um parente que trabalha nos Estados Unidos. Se o parente enviar \$100, mas o banco cobrar uma taxa de \$7 pela transferência, a família receberá apenas \$93. Isso pode não parecer muito, mas para uma família que vive com um orçamento apertado, perder \$7 pode fazer uma grande diferença.



**45%**  
das famílias  
subbancarizadas  
possuem criptomoedas,  
em comparação com



**19%**  
da população  
em geral

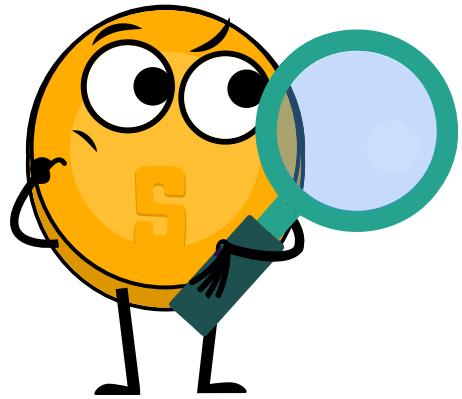
- **Os não bancarizados e subbancarizados:** Infelizmente, nem todos têm acesso aos serviços bancários tradicionais, seja porque não atendem aos requisitos para abrir uma conta ou porque vivem em áreas onde os serviços bancários não estão disponíveis. Isso

pode dificultar o acesso das pessoas aos serviços financeiros e sua participação na economia global.

- Mas espere, há mais! Os governos também podem controlar a taxa de câmbio de sua moeda, o que pode dificultar a troca de dinheiro entre países ou levar a **taxas de câmbio desfavoráveis**. Instituições financeiras podem **bloquear doações** para determinadas organizações ou indivíduos, ou até mesmo encerrar sua conta bancária. Plataformas de mídia social e instituições financeiras podem remover determinado conteúdo se acreditarem que ele está espalhando desinformação ou violando seus padrões ou políticas da comunidade. Isso é às vezes chamado de **censura** e pode incluir uma ampla gama de atividades, como bloquear ou suprimir conteúdo, limitar o acesso ou remover informações completamente.



## Capítulo #2



Vigilância, controle e taxas ocultas são apenas as desvantagens políticas do atual sistema em que vivemos. Infelizmente, também existem uma série de custos econômicos ocultos - aqueles que muitas vezes nunca chegamos a conhecer.



## *Capítulo #3*

# *Revelando o Lado Obscuro do Dinheiro Fiduciário*

**3.0** Exercício em Classe: Os Efeitos da Inflação: Uma Atividade de Leilão

**3.1** As Maiores Ameaças ao Seu Dinheiro: Inflação, Degradação e Perda do Poder de Compra

**3.2** Dívida: A Linha Tênué Entre Ajuda e Prejuízo

**3.3** O Fed e Seus Parceiros: Como o Governo e os Bancos Controlam a Oferta Monetária

**3.4** A Magia da Criação de Dinheiro

**3.4.1** O Valor do Tempo do Dinheiro e Seu Papel no Crescimento Econômico

**3.4.2** Economizando Dinheiro em Tempos Difíceis

**3.4.3** Sistema Bancário de Reserva Fracionária

**3.4.4** Exercício em Classe: Sistema Bancário de Reserva Fracionária

# Revelando o Lado Obscuro do Dinheiro Fiduciário

## 3.0 Exercício em Classe: Os Efeitos da Inflação: Uma Atividade de Leilão

Objetivo: Compreender o conceito de oferta monetária e como isso afeta os preços de bens e serviços em uma economia.

Definições:

- **Oferta Monetária** é o montante total de dinheiro em circulação dentro de uma economia em um momento específico. Isso inclui:
  - Moeda física, como moedas e notas
  - Dinheiro eletrônico mantido em contas bancárias

- A oferta monetária é um conceito importante na economia, pois pode afetar a saúde geral de uma economia.
- **Leilão** é uma venda pública na qual bens ou propriedades são vendidos ao maior lance.

**Atividade em Classe.** Siga as instruções abaixo.

1. Você receberá uma quantidade aleatória de dinheiro do jogo Banco Imobiliário do professor. Isso representa a oferta monetária em uma sociedade.
2. Anote a oferta monetária total no gráfico fornecido.
3. O professor leiloará uma barra de chocolate para os alunos. Para vencer a barra de chocolate, você precisará fazer o lance mais alto usando seu dinheiro do jogo Banco Imobiliário. Registre o lance vencedor ao lado da oferta monetária.
4. O professor então adicionará uma quantidade significativa de dinheiro do jogo Banco Imobiliário à oferta monetária total. Isso representa um aumento na oferta monetária em uma economia. Mais tarde, você aprenderá como a oferta monetária é aumentada ou reduzida em uma economia.
5. O professor leiloará uma segunda barra de chocolate para os alunos usando o mesmo processo anterior. Registre o lance vencedor ao lado da oferta monetária no gráfico.
6. O professor repetirá o leilão uma terceira vez.



As sociedades frequentemente podem ser imprevisíveis e injustas, exemplificadas pela simulação de um professor dando aleatoriamente uma quantia significativa de dinheiro apenas para alguns alunos selecionados. Isso imita situações da vida real onde ocorre uma distribuição desigual de recursos e oportunidades, destacando a aleatoriedade e injustiça inerentes em muitas situações.





## Capítulo #3



Rodada	Oferta Monetária	Lance Vencedor

**Perguntas.** Com base no que você aprendeu com o exercício, responda às seguintes perguntas.

1. Como o aumento na oferta monetária afetou os lances vencedores para as barras de chocolate?

---

---

2. Qual é a relação entre a oferta monetária e a inflação?

---

---

---

3. Como a oferta monetária é relevante no mundo real?

---

---

---

4. Você consegue pensar em outros fatores que podem afetar os preços de bens e serviços?

---

---

---

---

---

# Revelando o Lado Obscuro do Dinheiro Fiduciário

## 3.1 As Maiores Ameaças ao Seu Dinheiro: Inflação, Degradação e Perda do Poder de Compra

O atual cenário econômico global é desafiador, o que pode dificultar a economia. Um fator que contribui para isso é a inflação, um fenômeno que ocorre quando o valor do dinheiro diminui ao longo do tempo. Isso significa que, mesmo se você economizar mais dólares agora, eles podem não ter o mesmo poder de compra no futuro, ou seja, mais dinheiro poderá comprar menos coisas. Reconhecer as condições econômicas e seu impacto em suas finanças pessoais ajudará você a tomar decisões informadas sobre poupança e gastos.



### O poder de compra

é a quantidade de bens ou serviços que podem ser comprados com uma determinada quantia de dinheiro.

Vamos começar com um cenário realista para explicar cada termo.

Jaime é um estudante universitário que vive em um pequeno apartamento. Ele trabalha meio período em uma cafeteria para pagar suas despesas de moradia e mensalidade. Assim que começou a viver de forma independente, Jaime se tornou um especialista em gerenciar seu próprio orçamento.

No início do ano, ele planejou um orçamento de \$10.000 para suas despesas de vida, incluindo aluguel, comida e outras necessidades.



1956



2020



2056



A **inflação** é o aumento do nível geral de preços de bens e serviços em uma economia ao longo do tempo. Quando o nível geral de preços aumenta, cada unidade de moeda compra menos bens e serviços; consequentemente, a inflação reflete uma **redução no poder de compra** do dinheiro - uma perda de valor real no meio de troca e unidade de conta dentro de uma economia.



Um **livro-caixa** é um registro detalhado de todas as suas transações monetárias. Seja dinheiro que você está ganhando ou gastando, um livro-caixa ajuda você a acompanhar tudo.



## Capítulo #3

Essas foram as **transações** dele em janeiro:

Data	Descrição	Quantidade	Tipo	Saldo
01/01/2023	Saldo Inicial			\$1,600.00
01/01/2023	Aluguel de janeiro	\$800.00	Débito	\$800.00
01/05/2023	Compras de supermercado	\$100.00	Débito	\$700.00
01/15/2023	Salário de meio período	\$500.00	Crédito	\$1,200.00
01/20/2023	Combustível para o carro	\$50.00	Débito	\$850.00
01/30/2023	Livros didáticos	\$150.00	Débito	\$650.00

Este livro-caixa mostra que o saldo inicial da conta corrente de Jaime em 1º de janeiro era de \$1.600, dos quais ele gastou \$800 para pagar o aluguel do mês. Em seguida, ele **gastou** (um **débito**) \$100 em compras de supermercado e recebeu **\$500.00** (um **crédito**) de salário do seu trabalho de meio período, chegando a um saldo de \$1.200. Em seguida, ele **gastou** dinheiro com combustível e livros didáticos, reduzindo seu saldo para \$650 no final do mês.

Doze meses depois, durante o almoço com seu avô, Jaime percebe que seu orçamento não está se esticando tanto quanto costumava. Ele percebe que os preços dos bens e serviços de que precisa aumentaram significativamente no último ano e se perguntou por quê. Então ele viu essa imagem e não podia acreditar no que via.

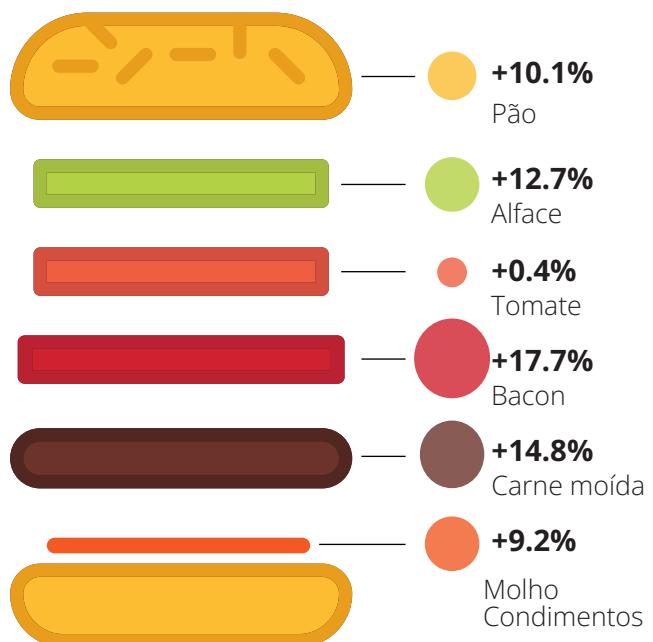
Quando ele mencionou isso ao seu avô, foi-lhe dito: "Em 1956, eu era apenas um jovem começando no mundo. Lembro-me de que ganhava \$100 por mês como operário de fábrica. Pode não parecer muito pelos padrões de hoje, mas era um salário decente na época. Na verdade, consegui economizar dinheiro suficiente para comprar uma pequena casa nos subúrbios".

Como podemos ver, o custo de cada item na **cesta** aumentou, levando a uma diminuição geral no poder de compra dele.

Felizmente, Jaime dominou o uso de um livro-caixa, pois isso claramente mostrou como seu poder de compra anual diminuiu.

### Como a Inflação Alterou o Preço de um Hambúrguer

Variação ano a ano no preço de ingredientes selecionados de um hambúrguer (abril de 2021 - abril de 2022)



\* Com base nos preços de varejo, consumidores

# Revelando o Lado Obscuro do Dinheiro Fiduciário

**Jaime:** "O quê? Isso é loucura. Nem consigo imaginar quanto meu aluguel custaria naquela época."

**Avô:** "Bem, deixe-me ver. Se levarmos em conta a inflação, \$1USD me compraria cerca de 10 sacos de pretzels naquela época."

**Jaime:** "Uau, isso é realmente interessante, vovô. Mas quanto isso valeria hoje?"

**Avô:** "Ah, as coisas eram muito mais baratas! Um pão custava apenas alguns centavos, e você podia comprar um galão de gasolina por apenas um quarto. É inacreditável como o custo de vida aumentou."

## O Valor de um Dólar

### Poder de Compra do Dólar Americano

A Lei do Sistema de Reserva Federal cria um banco central com a capacidade de gerenciar a oferta monetária do país.

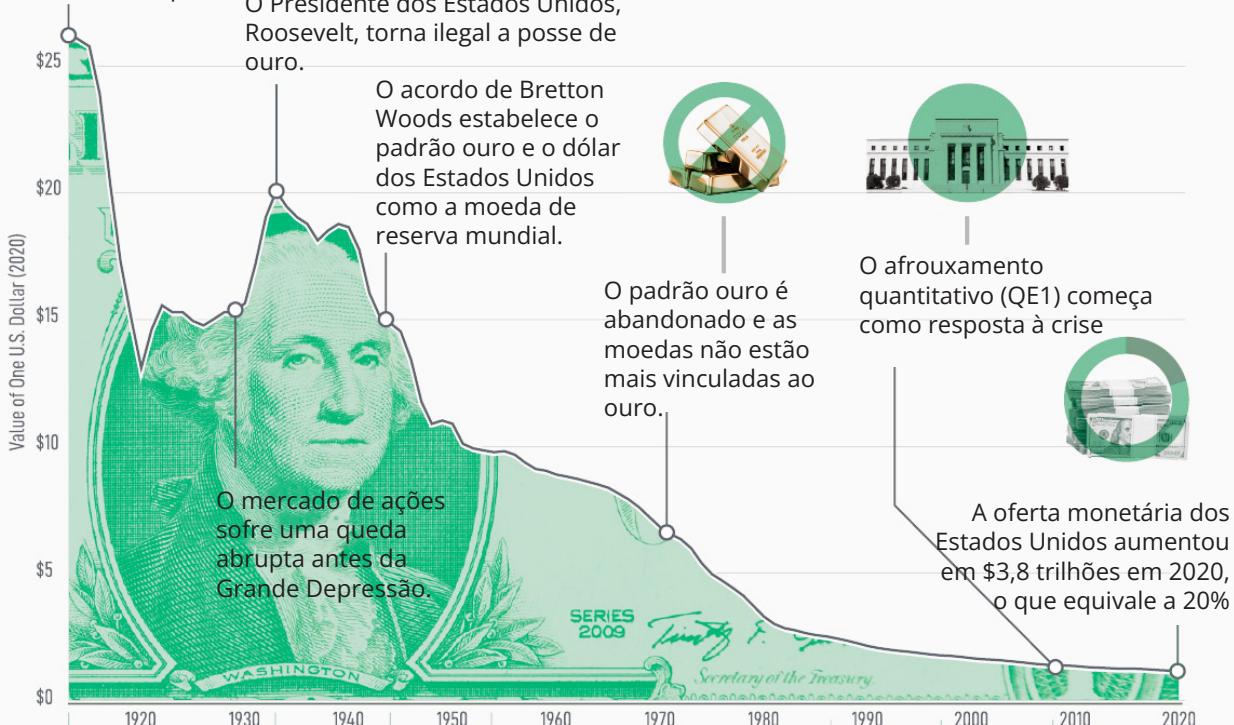
O Presidente dos Estados Unidos, Roosevelt, torna ilegal a posse de ouro.

O acordo de Bretton Woods estabelece o padrão ouro e o dólar dos Estados Unidos como a moeda de reserva mundial.

O padrão ouro é abandonado e as moedas não estão mais vinculadas ao ouro.

O afrouxamento quantitativo (QE1) começa como resposta à crise

A oferta monetária dos Estados Unidos aumentou em \$3,8 trilhões em 2020, o que equivale a 20%



O poder de compra do dólar americano caiu acentuadamente ao longo do último século, devido à inflação crescente e ao aumento da oferta de dinheiro.



## Capítulo #3

- Jaime precisa reservar um valor adicional de \$1.000 para a mesma cesta de bens e serviços que ele comprou no ano anterior.
  - Isso significa que seu poder de compra diminuiu em \$1.000, pois *agora ele precisa gastar mais dinheiro para comprar os mesmos bens e serviços.*
- A cesta de bens e serviços inclui aluguel de seu apartamento, compras de supermercado e outras necessidades.
- A tabela a seguir mostra o custo de cada item na **cesta** no primeiro ano e no segundo ano, bem como a porcentagem de aumento no preço:

Item	Custo Ano #1	Custo Ano #2	% Aumento
Aluguel	\$4,000	\$4,500	12.5%
Compras	\$2,000	\$4,300	15%
Necessidades	\$4,000	\$4,200	5%
<b>Total</b>	<b>\$10,000</b>	<b>\$11,000</b>	<b>10%</b>

Jaime ganha mais em um ano do que seu avô jamais ganhou, mas isso também desincentiva a poupança. É mais vantajoso gastar o dinheiro agora, já que seu valor diminui. Isso dificulta a capacidade de planejar o futuro. Conforme mostrado em um gráfico anterior (na Seção 2.3), o crescimento salarial ano após ano nos Estados Unidos tem permanecido estagnado para o cidadão médio, o que significa que a maioria das pessoas não está recebendo aumentos na mesma proporção que a diminuição do valor de seu dinheiro, apesar de trabalharem mais.

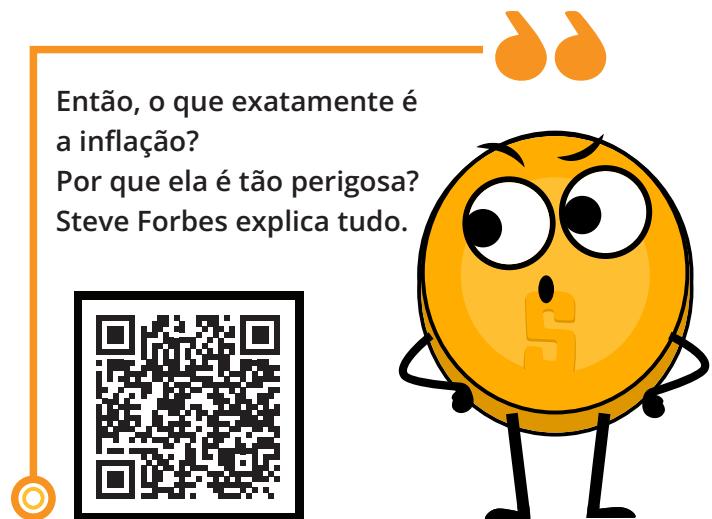
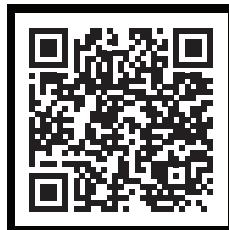
Poderia ter sido pior para Jaime. Por exemplo, o Zimbábue experimentou hiperinflação no final dos anos 2000, quando a economia do país foi atingida por uma combinação de instabilidade política, má gestão econômica e fatores externos, como seca e sanções. Como resultado, o valor do dólar do Zimbábue (ZWD) despencou e o governo foi obrigado a imprimir mais dinheiro.

- A nota de 100.000 ZWD foi introduzida no Zimbábue em 2008. Devido à hiperinflação, ela valia apenas alguns dólares americanos na época.
- Apesar de ter um alto valor nominal, a nota de 100.000 ZWD não era suficiente para comprar necessidades básicas como comida ou combustível, e as pessoas precisavam carregar grandes pacotes de dinheiro para fazer compras diárias.

Após considerar os significativos aumentos de preços desde meados dos anos 50 nos Estados Unidos e o exemplo da hiperinflação no Zimbábue, fica claro que o impacto da inflação no poder de compra de um indivíduo pode variar amplamente, dependendo de sua localização e do período em que viveu.

A inflação tende a afetar mais aqueles que vivem em países pobres do que aqueles que vivem em países ricos. Isso destaca o fato de que muitas vezes é pura sorte o lugar e a época em que um indivíduo nasce, e que as circunstâncias do nascimento de uma pessoa podem ter um impacto significativo em sua qualidade de vida e oportunidades econômicas.

Então, o que exatamente é a inflação?  
Por que ela é tão perigosa?  
Steve Forbes explica tudo.



# Revelando o Lado Obscuro do Dinheiro Fiduciário

## 3.2 Dívida: A Linha Tênué entre Ajuda e Prejuízo

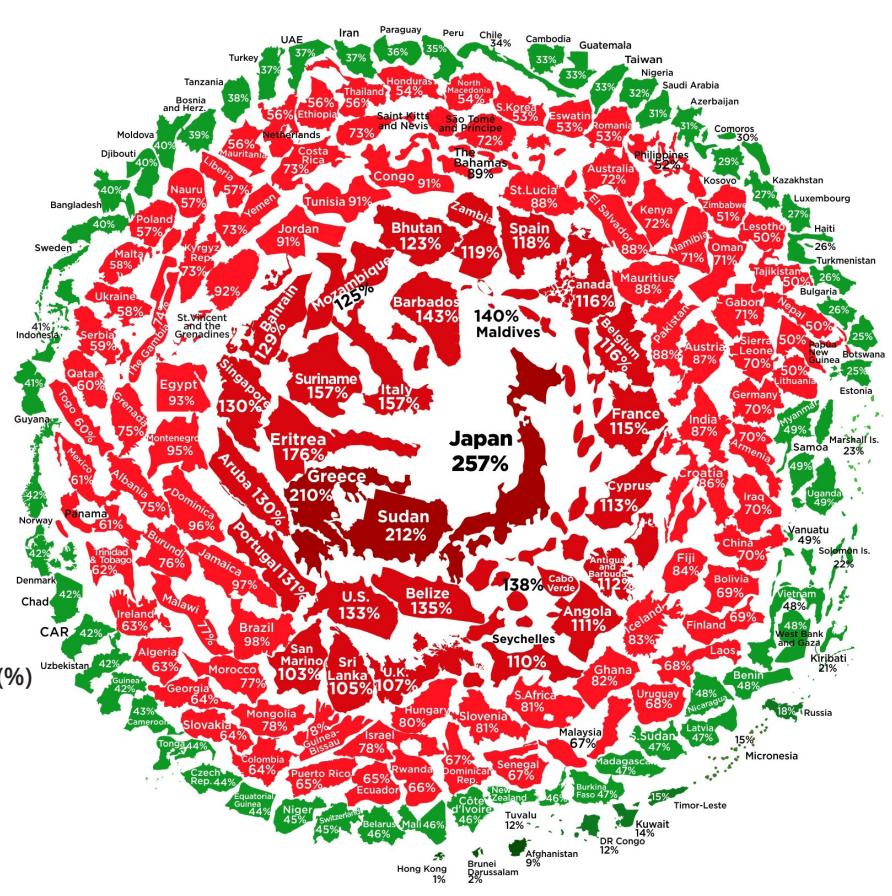
A dívida é uma espada de dois gumes. É verdade que pegar dinheiro emprestado pode fornecer um impulso financeiro muito necessário, seja para indivíduos que estão fazendo uma grande compra, empresas que estão investindo em seu crescimento ou governos que estão financiando serviços importantes. Mas pegar emprestado demais pode levar à ruína financeira. Quando você não consegue pagar os juros de suas dívidas, torna-se mais difícil pagar suas contas e se manter em dia. Isso é especialmente verdadeiro quando uma entidade assume mais dívidas para pagar dívidas existentes e acaba presa em um ciclo vicioso conhecido como “espiral de dívida”.

A crise da dívida é um problema global, inclusive nos Estados Unidos. Atualmente, o governo está gastando mais dinheiro do que está recebendo. Para pagar suas contas, tem se endividado cada vez mais. No entanto, esse ciclo de dívida e custos de empréstimos mais altos pode em breve prejudicar a classificação de crédito do governo. Se a dívida se tornar insustentável, o governo pode enfrentar dificuldades financeiras e potencialmente declarar falência, assim como muitos outros países fizeram no passado.



**Dívida** é o dinheiro que uma pessoa ou organização deve a outra. Quando você possui uma dívida, é necessário pagar o dinheiro que deve, geralmente com juros, até uma determinada data.

O Estado da Dívida Governamental Mundial





- A dívida assumida pelo governo pode ter efeitos de longo prazo nas gerações futuras.
- Imprimir mais dinheiro para financiar despesas pode resultar na desvalorização da moeda e em um possível colapso do sistema monetário.

Mas como podemos medir o risco de um país assumir uma dívida excessiva? Uma maneira é por meio da **relação dívida/PIB**, que mostra a quantidade da dívida total de um país como porcentagem do seu PIB.

- **A relação dívida/PIB** é uma maneira de verificar se um país pode pagar suas dívidas.
  - Se a relação for alta, o país pode enfrentar dificuldades para pagar suas dívidas no futuro.
  - Se a relação for baixa, o país pode ser capaz de pagar suas dívidas facilmente e estar em boa situação financeira.
- É importante lembrar que a relação dívida/PIB é apenas uma parte do entendimento da situação financeira de um país.



**O Produto Interno Bruto (PIB)** é uma medida do valor total de bens e serviços produzidos dentro de um país durante um período específico de tempo, geralmente um ano. É frequentemente utilizado como uma medida do tamanho e da saúde de uma economia.

### 3.3 O Fed e seus parceiros:

#### Como o governo e os bancos controlam a oferta de dinheiro

Você já parou para pensar de onde vêm os trilhões de dólares em fundos de estímulo que foram distribuídos durante a pandemia, e quem decide quanto é dado e para quem? A alocação desses fundos tem o poder de impactar significativamente a sociedade e a economia, mas muitas vezes passa despercebida..

Existem várias ferramentas que os governos centralizados podem usar para gerenciar a quantidade de oferta de dinheiro em um momento específico.

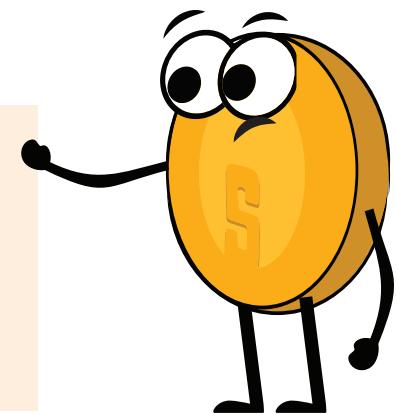
- Os bancos centrais e os governos podem usar políticas monetárias e fiscais para influenciar a oferta de dinheiro e a economia.



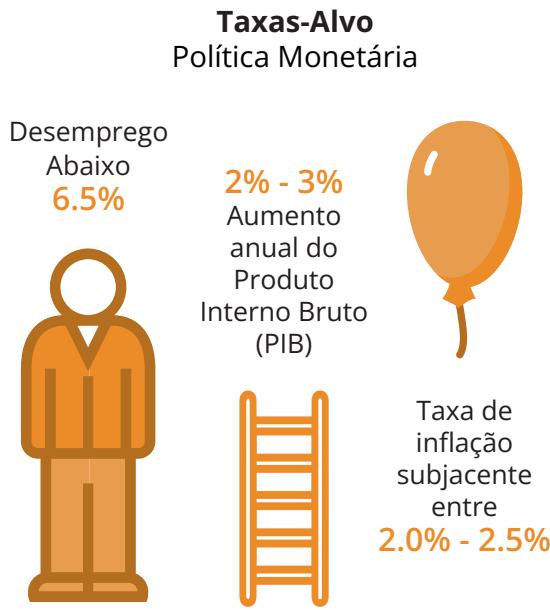
O banco central dos Estados Unidos é chamado de **Federal Reserve**, ou The Fed.



Os governos podem tomar empréstimos para estimular a economia, mas isso pode levar à inflação se eles tiverem que imprimir mais dinheiro para pagar os empréstimos.



# Revelando o Lado Obscuro do Dinheiro Fiduciário



## Política fiscal expansionista VS Política fiscal restrictiva

A política fiscal expansionista tem como objetivo aumentar os gastos dos consumidores e os investimentos empresariais para impulsionar a demanda agregada e o crescimento econômico.

Reduzir os impostos

Aumentar os gastos do governo.

Diminuir os gastos do governo.

Aumentar os impostos

Política/Ferramenta	Descrição	Exemplo
<b>Política Monetária</b>	A política monetária envolve ajustar as taxas de juros para controlar a quantidade de dinheiro em circulação.	O <b>Federal Reserve</b> aumenta as taxas de juros para desacelerar a inflação ou pode reduzi-las para estimular o emprego.
<b>Política Fiscal</b>	A política fiscal envolve o uso de políticas de gastos e impostos para influenciar a economia.	O governo aumentando os gastos em projetos de infraestrutura para estimular o crescimento econômico. Ele também pode reduzir os impostos para que as pessoas gastem mais.
<b>Política Cambial</b>	O uso da taxa de câmbio de um país (o valor de sua moeda em relação a outras moedas) para influenciar o comércio e a economia.	O governo chinês fixando o valor do yuan em relação ao dólar dos Estados Unidos para estabilizar as taxas de câmbio.
<b>Choque de oferta</b>	Um evento repentino e inesperado que perturba o fornecimento de bens e serviços, levando a mudanças nos preços e na oferta monetária.	Um desastre natural que destrói uma parte significativa da produção agrícola de um país, resultando em escassez de alimentos e aumento de preços.
<b>Controles de preços</b>	Limites impostos pelo governo sobre os preços de bens e serviços para controlar a inflação ou estabilizar os preços.	O governo estabelecendo um preço máximo para a gasolina para evitar a exploração de preços durante uma crise.



### 3.4 A Magia da Criação de Dinheiro

#### 3.4.1 O Valor do Tempo do Dinheiro e seu Papel no Crescimento Econômico

Você já se perguntou por que os bancos oferecem tantos serviços aos seus clientes? Embora possa parecer que eles estão sendo generosos, é importante lembrar que os bancos são empresas e seu objetivo principal é obter lucro. Mas como eles lucram se estão emprestando dinheiro?

Além de receber juros sobre os depósitos, os bancos geram receita de outras maneiras, incluindo:

1. Cobrando juros sobre os empréstimos concedidos;
2. Cobrando taxas por serviços como uso de caixas eletrônicos e manutenção de contas;
3. Ganhar dinheiro por meio de investimentos, como compra e venda de títulos ou investimento em imóveis;
4. Mantendo uma porcentagem dos empréstimos em reserva e investindo ou emprestando o restante;
5. Pagando juros sobre depósitos e cobrando taxas em contas correntes e de poupança.



**Ao pegar dinheiro emprestado a taxas de juros baixas e emprestá-lo a taxas mais altas, os bancos conseguem obter lucro. Eles também geram receita por meio de taxas e atividades de investimento.**

Mas por que isso deve importar para você como indivíduo? Bem, você já ouviu a frase "um dólar hoje vale mais do que um dólar amanhã"? Esse conceito é conhecido como o **valor do dinheiro no tempo**, e trata da ideia de que o dinheiro vale mais no presente do que no futuro. Isso ocorre porque *o dinheiro pode ser investido para render juros e porque o dinheiro pode perder valor ao longo do tempo devido à inflação*.

Em outras palavras, se você tem dinheiro guardado em uma conta poupança que rende uma taxa de juros baixa, ele não terá o mesmo valor no futuro como tem hoje. Por outro lado, se você investir seu dinheiro em algo que tenha a possibilidade de obter um retorno mais alto, você pode se beneficiar no longo prazo.



Os bancos pegam emprestado dinheiro dos depositantes a uma taxa de juros (digamos, 5%).



Os bancos emprestam esse dinheiro aos tomadores de empréstimo a uma taxa de juros mais alta (digamos, 9%).



Os bancos pagam juros com os juros recebidos pelos empréstimos ( $9\% - 6\% = 4\%$ ) e mantêm o restante como lucro.



Para garantir que seu dinheiro mantenha seu valor ao longo do tempo, o objetivo de investir é obter um retorno que seja maior do que a taxa de inflação. Dessa forma, seu dinheiro valerá mais no futuro do que vale hoje.

# Revelando o Lado Obscuro do Dinheiro Fiduciário

## 3.4.2 Economizando Dinheiro em Tempos Difíceis

A situação econômica global atual, que foi afetada negativamente pela pandemia, trouxe desafios como alta inflação e baixas taxas de juros em contas de poupança. Essas condições podem dificultar a economia efetiva de dinheiro, já que a inflação diminui o valor da moeda ao longo do tempo. Mesmo que você poupe hoje, pode acabar tendo menos poder de compra no futuro.

Mas não se preocupe! Ainda existem maneiras de economizar dinheiro e estar financeiramente seguro. Aqui estão algumas ideias para tentar:

- **Faça um orçamento:** Um orçamento é um plano de como você vai usar o seu dinheiro. Ele pode ajudá-lo a ver onde você está gastando dinheiro demais e onde pode economizar. Reserve uma quantia de dinheiro a cada mês para poupar e procure maneiras de reduzir suas despesas.
- **Comece a investir:** Investir é uma maneira de fazer seu dinheiro crescer ao longo do tempo. Existem muitos tipos de investimentos para escolher, e você pode encontrar um que se ajuste ao seu orçamento e ao seu nível de risco.
- **Seja criativo:** Existem muitas maneiras criativas de economizar dinheiro. Você pode tentar cortar o próprio cabelo ou fazer trocas com outras pessoas por bens e serviços. Esteja aberto a experimentar coisas novas e buscar soluções não tradicionais para seus problemas financeiros.

○ **É geralmente aceitável assumir dívidas, desde que o dinheiro seja usado para gerar renda e aumentar o poder de compra no futuro.** Isso ocorre porque tomar empréstimos pode permitir que um indivíduo ou empresa faça investimentos que aumentem sua produtividade e eficiência, resultando em maiores lucros e estabilidade financeira.

○ Por exemplo, se um agricultor faz um empréstimo para comprar equipamentos novos que permitem colher suas safras de forma mais rápida e eficiente, ele pode gerar mais renda e aumentar seu poder de compra como resultado. Por outro lado, se o dinheiro for usado para desperdiçar recursos ou fazer investimentos improdutivos, isso pode levar a dificuldades financeiras e não seria uma decisão sábia.

Ao assumir o controle de suas finanças e ser flexível, você estará melhor preparado para enfrentar a tempestade de uma economia difícil e sair por cima.

### O Plano de Gastos 50/30/20





### 3.4.3 Sistema Bancário de Reserva Fracionária

Até agora, falamos sobre como os bancos centrais, como o Federal Reserve, gerenciam a oferta de dinheiro, como os bancos lucram para si mesmos e algumas estratégias sobre como economizar dinheiro, mas ainda não discutimos como o novo dinheiro é realmente criado e introduzido em uma sociedade. Pode parecer mágica, mas há um processo interessante por trás disso.

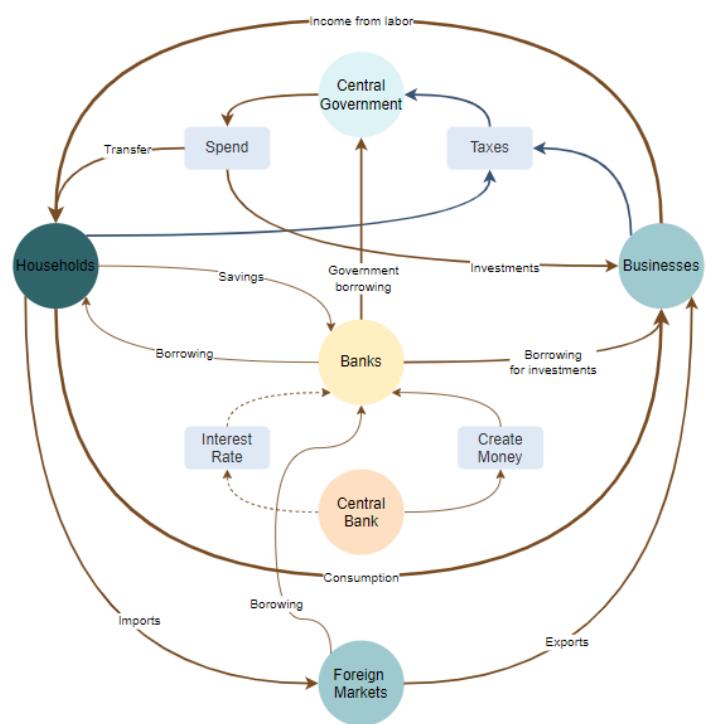
Como o dinheiro **novo** realmente entra em circulação e impulsiona o crescimento econômico? Ao contrário de recursos físicos como comida ou água, que podem se esgotar, o dinheiro não tem um limite fixo! Então, como funciona?

O **governo**, o **banco central** e os **bancos privados** desempenham um papel nesse processo.

Aqui está uma versão simplificada de como o Federal Reserve (Fed) pode adicionar US\$ 100 milhões em circulação:

1. O Fed determina que deseja aumentar a oferta de dinheiro em US\$ 100 milhões. Essa decisão é geralmente tomada com base nos **objetivos da política monetária** do Fed, como impulsionar o crescimento econômico ou estabilizar os preços.
2. O Fed instrui um grande banco comercial a criar um depósito de US\$ 100 milhões em sua conta no Fed. Esse depósito é criado do nada e não é respaldado por nenhum ativo físico.
  - Quando um banco comercial cria um depósito no Fed, ele essencialmente está pegando dinheiro emprestado do Fed. O Fed fornece ao banco os fundos para o depósito e, em troca, o banco deve pagar juros sobre o empréstimo e eventualmente quitá-lo.
3. O banco membro então usa esse novo depósito de US\$ 100 milhões para fazer empréstimos a empresas ou indivíduos, ou para comprar títulos, como títulos do governo.
4. As empresas ou indivíduos que recebem esses empréstimos podem usar o dinheiro para fazer compras, pagar contas ou investir em outros ativos. Isso aumenta a oferta geral de dinheiro na economia.
5. À medida que o dinheiro é circulado e gasto, ele acaba chegando a outros bancos, que podem usá-lo para fazer seus próprios empréstimos e investimentos. Esse processo continua até que os US\$ 100 milhões tenham sido totalmente injetados na circulação.

Em geral, a capacidade do Fed de adicionar novo dinheiro à circulação por meio do sistema bancário ajuda a estimular o crescimento econômico e atingir seus objetivos de política monetária.



# Revelando o Lado Obscuro do Dinheiro Fiduciário

Os bancos realmente criam novo dinheiro toda vez que emprestam para clientes ou fazem investimentos. O quê? Sim, você leu isso certo. Quando um banco concede um empréstimo, ele cria dinheiro ao adicionar novos fundos à conta do mutuário no valor do empréstimo. O mutuário pode então usar esse dinheiro para fazer compras ou pagar contas, aumentando efetivamente a oferta geral de dinheiro na economia. Veremos como isso acontece a seguir.

## 3.4.4 Exercício de Classe: Sistema Bancário de Reserva Fracionária

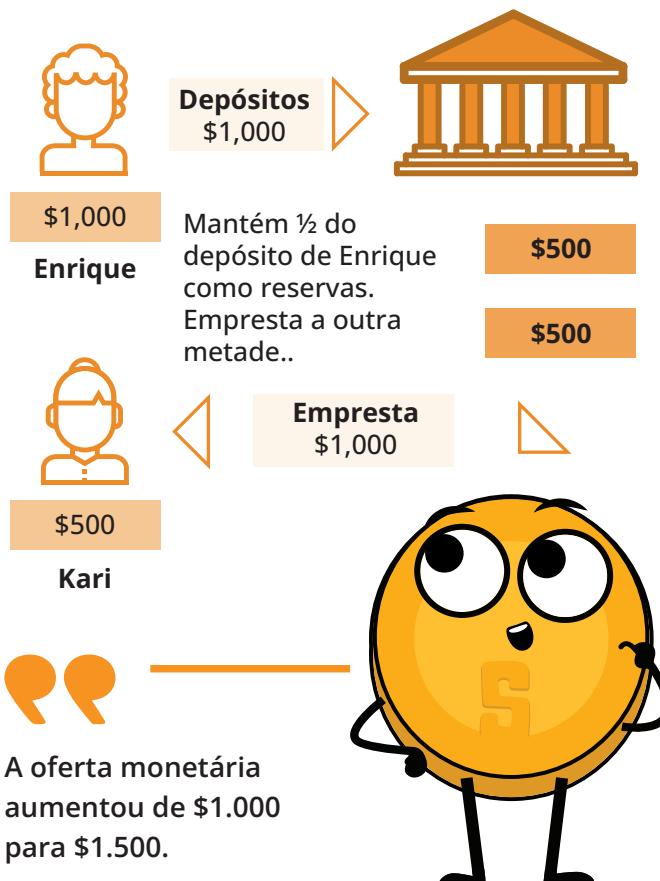
O processo conhecido como **sistema bancário de reserva fracionária** ocorre quando os bancos mantêm apenas uma fração dos depósitos como reservas e emprestam o restante. Contanto que mantenham uma determinada taxa de reserva estabelecida pelo banco central, os bancos podem criar mais dinheiro do que possuem em mãos. No entanto, essa capacidade de criar novo dinheiro também pode acarretar o risco de empréstimos excessivos e instabilidade financeira se não for gerenciada com cuidado.

A **taxa de reserva** é uma regra que diz aos bancos quanto dinheiro eles devem manter em seu cofre e quanto podem emprestar. Ela é **estabelecida pelo banco central**, que é um grupo especial de pessoas responsáveis por garantir a saúde da economia.

Nesta atividade, exploraremos o conceito de **sistema bancário de reserva fracionária** e como ele pode levar à **desvalorização** de uma moeda, à **inflação** e à diminuição do **poder de compra**.

- Vamos supor que o montante total de dinheiro na economia seja de \$1000 e a taxa de reserva seja de 50%. Isso significa que, para cada \$1000 na economia, 50% desse valor deve ser mantido como reserva pelo banco.
- Se Enrique deposita \$1000 no banco e depois Kari vai ao banco em busca de um empréstimo, de acordo com a taxa de reserva requerida, o banco pode manter metade do valor e emprestar a outra metade, ou seja, \$500. Como resultado, a oferta total de dinheiro aumentaria de \$1000 para \$1.500.

### Sistema Bancário de Reserva Fracionária Mantendo ½



A fórmula é: Dinheiro Criado = Montante Total de Dinheiro na Economia ÷ Taxa de Reserva



## Capítulo #3

**Exercício em Classe.** Usando a fórmula acima, podemos calcular a quantidade de dinheiro criado da seguinte forma:

- Dinheiro Criado =  $\$1000 / 50\% = \$2000$

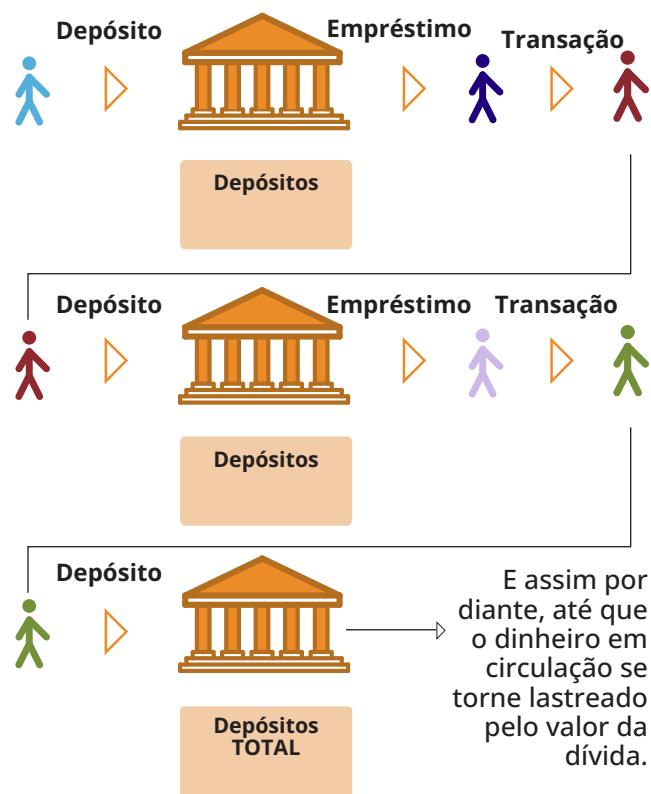
\*Por favor, observe que isso é um pouco simplificado demais.

Vamos modelar a criação de dinheiro em uma pequena economia (que consistirá em 6 participantes, sendo que um terá o papel de banco). A taxa de reserva, estabelecida pelo Banco Central, é calculada como uma proporção dos depósitos dos clientes e determina quanto os bancos comerciais devem reservar em vez de emprestar. Vamos assumir, para fins dessa simulação, que existe uma taxa de reserva obrigatória de 10%.

- Por exemplo, se um banco recebe \$100 e tem uma exigência de reserva de 10%, ele pode emprestar \$90. Se esse empréstimo for depositado em outro banco, esse banco poderá emprestar \$81, e assim por diante.
- Isso cria um **efeito multiplicador**, aumentando a **oferta geral de dinheiro**. Isso pode estimular a economia, mas também pode causar inflação se a oferta de dinheiro crescer muito rapidamente.
- Para descobrir quanto dinheiro é criado com uma determinada taxa percentual, você pode usar uma fórmula.
- Para usar a fórmula, primeiro você precisa saber o montante total de dinheiro na economia. Isso é todo o dinheiro que está sendo usado para comprar e vender bens e serviços. Em seguida, você precisa saber a taxa de reserva, que é a porcentagem de dinheiro que um banco deve manter em mãos e não emprestar.
- Em resumo, quando um banco empresta dinheiro, ele cria novo dinheiro que não existia antes, e isso aumenta o montante total de dinheiro na economia.
- Geralmente, países com economias voláteis ou altos níveis de inflação têm taxas de reserva elevadas para ajudar a mitigar os riscos e estabilizar o sistema financeiro.

Precisamos dos seguintes voluntários:

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



# Revelando o Lado Obscuro do Dinheiro Fiduciário

A acabou de ganhar \$100.000 na loteria e vai a um banco recém-aberto para depositar o dinheiro.

O banco **B** possui um requisito de taxa de reserva de 10%. Quanto o banco **B** é obrigado a manter em seu cofre? \_\_\_\_\_.

Na manhã seguinte, **C** entra no banco e pede um empréstimo. Quanto o banco pode emprestar?

\_\_\_\_\_. **C** pega o valor máximo emprestado, pois deseja fazer um pagamento inicial em uma casa.

**C** endossa o cheque e entrega-o a **D**. **D** então vai ao banco e deposita o cheque. Quanto **D** depositou? \_\_\_\_\_. Qual é o total de depósitos registrados no banco no momento? \_\_\_\_\_

**E** entra no banco e pede um empréstimo enorme. O banco diz que pode emprestar no máximo \_\_\_\_\_. **E** sai do banco com o dinheiro e vai comprar uma obra de arte de **F**. Após negociações, a obra de arte é vendida exatamente pelo valor que **E** pegou emprestado do banco. **E** paga a **F**.

**F** deposita o dinheiro no banco. Qual é o total de depósitos registrados no momento? \_\_\_\_\_ .

Nome	Depósito	Valor do Empréstimo	Valor da Reserva
<b>A</b>			
<b>C</b>			
<b>D</b>			
<b>E</b>			
<b>F</b>			

Então, quanto dinheiro é realmente criado com esses 100.000 USD se o dinheiro continuar circulando pela economia?

Quando a taxa de reserva é alta, os bancos precisam manter mais dinheiro em seus cofres e podem emprestar menos. Isso pode dificultar para as pessoas e empresas obterem empréstimos e pode desacelerar a economia. Quando a taxa de reserva é baixa, os bancos precisam manter menos dinheiro em seus cofres e podem emprestar mais. Isso pode facilitar para as pessoas e empresas obterem empréstimos e pode fazer a economia crescer mais rapidamente.



## Capítulo #3



Então podemos descobrir a resposta para nosso exercício de classe onde a reserva é de 10%?  
(Lembre-se de converter 10% para forma decimal  $10\% = 0,1$ )

---

Apenas por curiosidade, quanto dinheiro seria criado em uma economia se sua taxa de reserva fosse reduzida para 1%? (Certifique-se de dividir \$100.000 por 0,01). Surpreso(a)?

- A partir de 2020, o Federal Reserve (o Banco Central dos EUA) **reduziu as taxas de reserva obrigatória para zero por cento**, a fim de estimular a economia.



## *Capítulo #4*

# *O Futuro é Descentralizado: Empoderando Comunidades e Indivíduos*

**4.0** Da Crise à Inovação: Os Cypherpunks e a Criação de uma Moeda Digital Descentralizada

**4.1** Abuso da Centralização

**4.1.1** Sistemas Centralizados

**4.1.2** Cortando os Intermediários: Uma Visão sobre os Intermediários em uma Transação com Cartão de Crédito

**4.2** Uma Ferramenta Poderosa para Superar as Limitações da Centralização

**4.2.1** Exercício em Sala de Aula: Jogo de Consenso Descentralizado com Participantes Maliciosos

**4.3** Transações são Apenas Acordos para Negociar

**4.3.1** Confiar ou Não Confiar

**4.3.2** Vamos Trocar Confiança por Regras

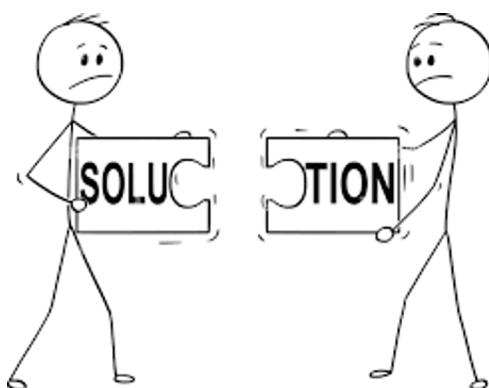
**4.4** Desvendando o Poder do Blockchain: Uma Tecnologia Revolucionando o Futuro

# O Futuro é Descentralizado: Empoderando Comunidades e Indivíduos

## 4.0 Da Crise à Inovação: Os Cypherpunks e a Criação de uma Moeda Digital Descentralizada

Antes da criação do **Bitcoin**, as pessoas estavam em busca de maneiras de lidar com os problemas das finanças tradicionais, como fraude, corrupção e falta de confiança nas instituições financeiras. Essas questões se tornaram ainda mais urgentes devido à crise financeira global de 2008. Em resposta, um grupo de indivíduos habilidosos em tecnologia e com visão de futuro, conhecidos como Cypherpunks, embarcou na missão de criar uma **moeda digital** que pudesse ser utilizada para transações online **sem a necessidade de intermediários** como bancos.

Os Cypherpunks eram rebeldes e visionários que acreditavam no poder da tecnologia para promover mudanças positivas e desafiar estruturas de poder tradicionais. Muitos deles estavam envolvidos em ativismo e questões de liberdades civis, e eles se uniram por uma paixão compartilhada pela tecnologia e o desejo de usá-la para moldar o futuro.



**Q:** Como os indivíduos podem recuperar sua autossuficiência financeira??

**R:** O movimento Cypherpunks tem como objetivo criar um novo sistema financeiro que respeite a segurança, privacidade e liberdade dos indivíduos, como solução para recuperar a autossuficiência financeira.

E assim, eles se dedicaram a criar o **bitcoin**, uma moeda digital que revolucionaria a maneira como pensamos sobre dinheiro e transações financeiras. Para isso, eles precisavam encontrar uma forma de registrar transações que fosse mais segura e transparente do que os sistemas tradicionais de registros centralizados. Por que eles sentiram essa necessidade?

## 4.1 Abuso da Centralização

### 4.1.1 Sistemas Centralizados

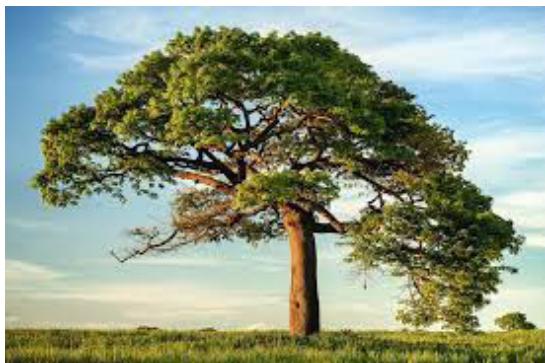
A centralização do poder frequentemente leva à corrupção, o que pode resultar na má gestão de recursos, incluindo recursos financeiros. Isso pode afetar de forma desproporcional aqueles que estão em posições inferiores na hierarquia e que possuem menos influência ou poder, fazendo com que eles suportem o maior ônus das consequências da corrupção e má gestão.

O sistema monetário moderno é caracterizado pela centralização do controle, com um pequeno



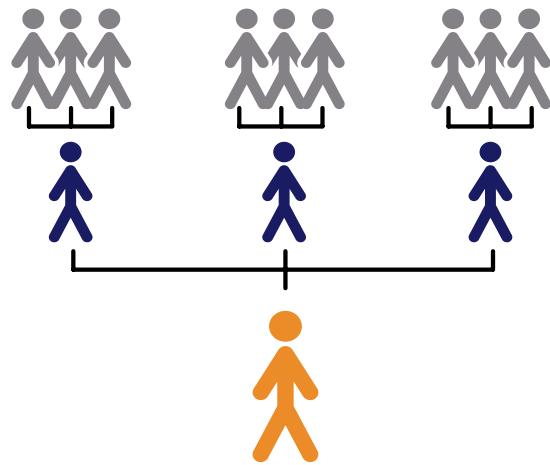
grupo de bancos e outras instituições financeiras detendo um peso significativo sobre a economia.

Um sistema centralizado pode ser pensado como uma árvore com um único tronco. O tronco representa a autoridade central ou ponto de controle, e os galhos representam as várias partes do sistema que são controladas pela autoridade central. Nessa analogia, a árvore fica vulnerável se o tronco estiver danificado ou doente, porque toda a árvore depende do tronco para sustentação.



Existem várias **desvantagens nos sistemas centralizados**, incluindo:

- **Vulnerabilidade:** Um sistema centralizado depende de um único ponto, portanto, se esse ponto falhar, todo o sistema pode falhar.
- **Controle e poder:** Aqueles que estão no controle de sistemas centralizados possuem muito poder e influência sobre seu funcionamento.
- **Ineficiência e intermediários:** Sistemas centralizados frequentemente usam intermediários, o que pode torná-los lentos e adicionar custos extras.
- **Falta de autonomia:** As pessoas podem não conseguir tomar suas próprias decisões financeiras.
- **Censura e restrição:** Existe o risco de ser bloqueado ou restrito de acessar determinados recursos financeiros em sistemas centralizados.
- **Desafios de escalabilidade:** Sistemas centralizados podem enfrentar dificuldades em lidar com a crescente demanda por serviços e recursos financeiros.
- **Riscos de segurança:** Sistemas centralizados podem ter vulnerabilidades que hackers podem explorar para obter acesso ou causar danos.
- **Falta de transparência e confiança:** Pode ser difícil entender como os sistemas centralizados funcionam e tomar decisões informadas sobre eles, pois podem não ser transparentes ou confiáveis.



# O Futuro é Descentralizado: Empoderando Comunidades e Indivíduos

## 4.1.2 Cortando os Intermediários: Uma Visão sobre os Intermediários em uma Transação com Cartão de Crédito

A banca moderna. Simples, certo? Pegue algo aparentemente simples, como comprar um hambúrguer com um cartão de crédito. A primeira vista, pode parecer fácil e inofensivo. Mas se analisarmos os passos e vermos os intermediários envolvidos, você pode se surpreender com o que descobrimos. Existem inconvenientes, ineficiências, talvez até perigos ocultos espreitando nas sombras? Vamos descobrir.

Etapa	Transações	Descrições
1	Titular do cartão-Comerciante	Você vai ao McDonald's e pede um hambúrguer usando seu cartão Citi MasterCard.
2	Comerciante-Processador de Pagamento	O McDonald's envia uma solicitação de autorização ao seu processador de pagamentos.
3	Processador de Pagamento - Rede de Cartão de Crédito	O processador recebe a solicitação e a envia para a Mastercard.
4	Rede de Cartão de Crédito - Banco Emissor	A Mastercard repassa a solicitação ao seu banco emissor, o CitiBank.
5	Banco Emissor - Rede de Cartão de Crédito	O Citibank verifica se a sua conta está em boa situação e envia o código de autorização de volta para a Mastercard.
6	Rede de Cartão de Crédito - Processador de Pagamentos	A Mastercard envia a autorização de volta para o processador.
7	Processador de Pagamentos - Comerciante	O processador envia a autorização de volta para o McDonald's.
8	Titular do cartão - Comerciante	Você recebe o seu hambúrguer.



**1 O titular do cartão**  
apresenta um cartão de crédito ao comerciante como forma de pagamento.



**2 Comerciante**  
O comerciante envia os detalhes da transação para o seu processador de pagamento.



**3 Processador de Pagamentos**  
O processador transmite os dados da transação para a rede de cartões.



**4 Rede de Cartão de Crédito**  
Envia uma solicitação de autorização para o banco emissor.



**5 Banco Emissor**  
Verifica os detalhes do cartão, verifica a disponibilidade de fundos e envia sua resposta (aprovada ou recusada) para a rede de cartões.



**6 Rede de Cartão de Crédito**  
Envia a resposta do emissor para o processador de pagamentos do comerciante.



**7 Processador de Pagamentos**  
Transmite a resposta do emissor para o comerciante.



**8 Comerciante**  
O comerciante e o titular do cartão concluem a transação.



Neste ponto, nenhum fundo real foi trocado, exceto talvez uma **pequena taxa de autorização**. A **transação** existe apenas no “papel”. O McDonald’s precisa encerrar ou agrupar suas vendas do dia. O processo de encerramento pode ser assim:

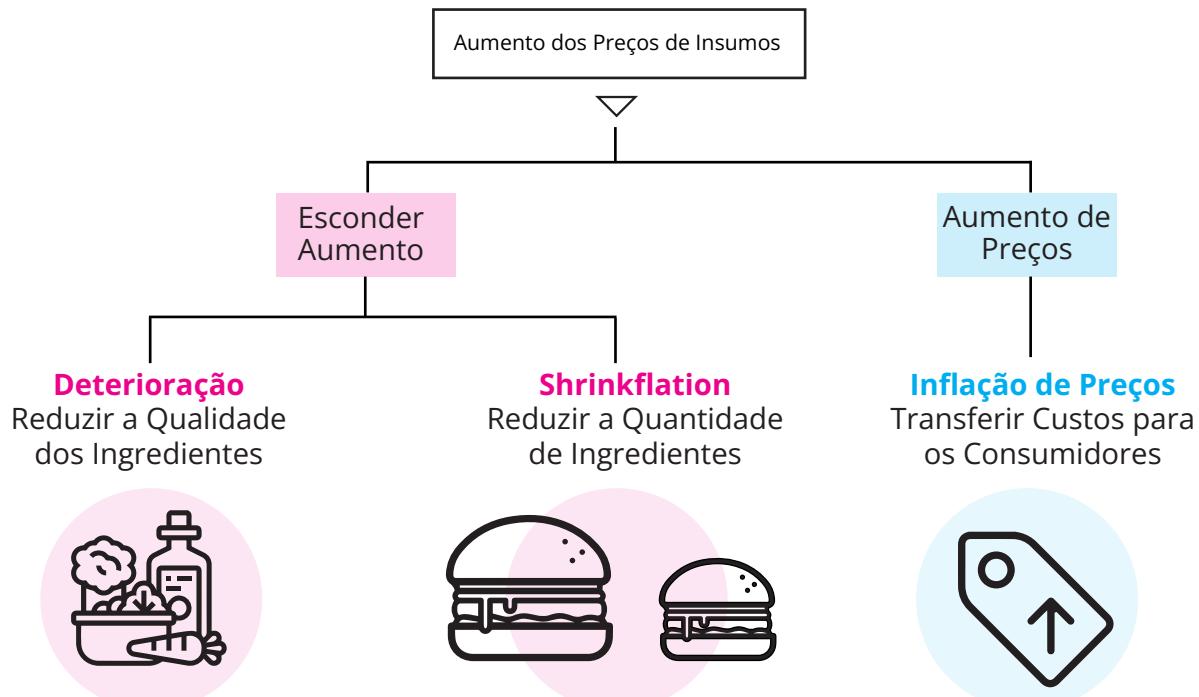
1. O terminal ou sistema de ponto de venda (POS) do McDonald’s envia as **transações** do dia para o processador.
2. O **processador** envia as informações da **transação** para a **Mastercard**.
3. A **Mastercard** envia as **transações** **Citibank**.
4. O **Citibank** confirma as autorizações, **retém as taxas de intercâmbio** (existem mais de 900 códigos de taxa possíveis na América do Norte) e transfere os fundos de volta para a **Mastercard**.
5. A **Mastercard retém sua taxa de avaliação** e envia os fundos para o **processador**.
6. O **processador retém sua parte**, conforme estabelecido no contrato com o comerciante, e deposita os fundos na conta bancária do McDonald’s.

Quem você acha que pagou pelas taxas? Claro, VOCÊ. Mas alguém informou você disso? Ah, não! Eles estavam ocultos no custo do hambúrguer.

E tudo isso acontece, acredite ou não, porque dependemos da centralização.

O mundo bancário moderno apresenta vários riscos, incluindo duplicação acidental de cobranças, fraude com cartão de crédito, erros humanos e computacionais e possíveis violações de segurança.

### Disfarçando a Inflação



# O Futuro é Descentralizado: Empoderando Comunidades e Indivíduos

## 4.2 Uma Ferramenta Poderosa para Superar as Limitações da Centralização

**Os sistemas descentralizados**, por outro lado, podem ser pensados como uma floresta. Cada árvore representa um participante independente, e a floresta representa o sistema como um todo. Nessa analogia, a floresta é mais resiliente do que uma árvore individual, pois não depende de um único ponto de falha. Se uma árvore está danificada ou doente, o resto da floresta pode continuar prosperando. As árvores na floresta compartilham o solo, os nutrientes, o sol e a chuva.



Sistemas descentralizados, assim como comunidades, redes e florestas, funcionam melhor quando há um grupo diversificado de indivíduos trabalhando juntos, em vez de uma única autoridade central ditando todas as regras.



Uma **rede** é um grupo de **nós** que estão conectados entre si de alguma forma. Essa conexão permite que os dispositivos troquem informações e se comuniquem uns com os outros.

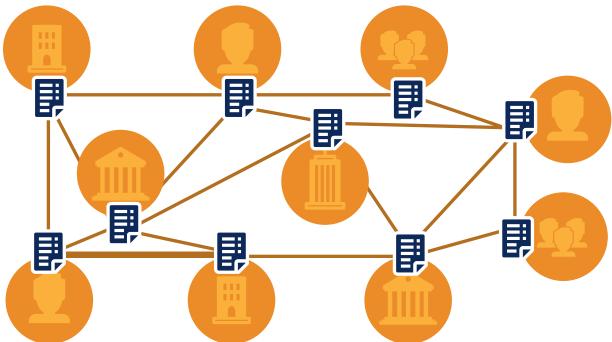


Um **nó** é um computador conectado a uma rede que pode compartilhar e/ou receber informações e se comunicar com os outros nós.

### Vantagens de um sistema descentralizado:

- É mais resiliente e confiável porque não há um único ponto de falha. Se uma parte do sistema falhar, o restante pode continuar operando.
- Com a criptografia adequada, a descentralização é mais segura, pois não há um ponto central de controle que possa ser alvo de hackers.

### Tecnologia de Registro Distribuído





- Pode ajudar a obter soberania, ou seja, você terá mais controle e autonomia sobre seus próprios ativos e decisões, em vez de depender de uma autoridade central.
- Pode ser mais transparente, pois todos os nós têm acesso às mesmas informações e podem ver o que está acontecendo no sistema.
- Pode ser sem permissão, o que significa que qualquer pessoa pode ingressar ou participar do sistema sem precisar de permissão de uma autoridade central.
- Pode ser ilimitado, ou seja, não há um limite predeterminado para o número de nós que podem ingressar no sistema.
- Cada nó tem oportunidades iguais de contribuir e influenciar a rede, tornando-a uma estrutura mais democrática e inclusiva.
- Os participantes também podem optar por usar pseudônimos ou “apelidos” para proteger sua privacidade e segurança, o que pode tornar o sistema mais resistente à censura e ataques.



A escassez descentralizada geralmente é vista como algo positivo para o dinheiro, pois impede a inflação e a manipulação por uma autoridade central.

No entanto, os sistemas descentralizados também têm seus **desafios** e limitações.

- Os sistemas descentralizados podem exigir mais trabalho para que todos os dispositivos conectados (nós) concordem e trabalhem juntos.
- Os sistemas descentralizados também podem estar mais propensos a problemas causados por atores ou dispositivos mal-intencionados (nós maliciosos) que possam prejudicar a rede.

### 4.2.1 Exercício em Sala de Aula: Jogo de Consenso Descentralizado com Atores Maliciosos

Em uma rede descentralizada, o **consenso** se refere ao processo de alcançar um acordo entre os membros da rede. Isso pode apresentar dificuldades, uma vez que não há uma autoridade central para tomar decisões ou resolver conflitos. Em vez disso, as decisões devem ser tomadas por meio de um processo de negociação e compromisso entre os membros da organização.

**Exercício em Sala de Aula.** Neste jogo, você estará desempenhando o papel de **nós** em uma rede descentralizada. Seu objetivo é chegar a um **consenso** sobre um problema **sem confiar uns nos outros**.

- Você desempenhará o papel de um nó em uma rede descentralizada e trabalhará com outros para chegar a um consenso sobre um problema.
- Pode haver atores maliciosos no grupo que tentarão enganar ou sabotar o processo.
- Como um **bom ator**, seu objetivo é trabalhar com os outros para verificar informações e alcançar o consenso.

# O Futuro é Descentralizado: Empoderando Comunidades e Indivíduos

- Como um **ator malicioso**, seu objetivo é enganar o grupo de forma sutil.
- O propósito do jogo é entender os desafios e benefícios dos sistemas descentralizados, aprender a verificar informações, alcançar consenso e identificar comportamentos maliciosos.
- Vocês serão divididos em pequenos grupos e receberão um problema para resolver dentro de um determinado período de tempo.

Lembre-se de que, **em um sistema descentralizado, você não pode simplesmente confiar nas respostas dos outros membros do grupo**. Você deve verificar a precisão das informações e chegar a um consenso por meio de discussão e colaboração.

## 4.3 Transações são apenas acordos de troca

Bem-vindo à ilha micronésia **descentralizada** de Yap! Ela é um pouco remota, mas fascinante porque as pessoas usam um tipo especial de moeda chamada “pedras Rai”. Uma característica que as torna uma ótima forma de dinheiro é sua **escassez**. O número total de pedras Rai é limitado, o que significa que elas não podem ser facilmente reproduzidas ou infladas como as moedas fiduciárias. Essa oferta fixa ajuda a manter o poder de compra das pedras Rai ao longo do tempo e as torna uma reserva confiável de valor. Essas pedras Rai são como moedas gigantes usadas para comprar coisas na ilha. A questão é que elas podem pesar uma tonelada. As pedras Rai podem realmente esmagar você, então elas são um pouco impraticáveis de carregar por aí. Como, então, as pessoas podem usar convenientemente as pedras Rai como meio de troca sem ter que transportá-las fisicamente de um lugar para outro?



### 4.3.1 Confiar ou não Confiar

Embora o dólar americano seja agora a moeda oficial da Ilha de Yap, as pedras Rai ainda são um tipo de dinheiro. Ao contrário dos dólares, as pedras Rai na Ilha de Yap não são controladas por uma única autoridade ou armazenadas em bancos. Em vez disso, as **transações** são baseadas em história oral e confiança, com as pessoas mantendo o registro próprio de quem possui quais pedras.

Esse sistema tem benefícios e desvantagens. Por um lado, ele permite um certo grau de independência de uma autoridade central. Por outro lado, também pode levar a desacordos e potencial para trapaças. Por quê?

A descentralização é fácil de alcançar em grupos pequenos. A vida é simples, pois há menos pessoas para coordenar; muitas vezes é possível que todos tenham uma opinião nos processos de tomada



de decisão e que essas decisões sejam implementadas relativamente rapidamente. À medida que um grupo se torna maior, torna-se mais difícil chegar a um acordo e para que as decisões sejam implementadas efetivamente.

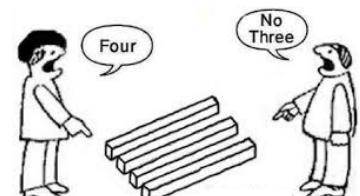
- Imagine que você tenha um campo cheio de milho maduro que precisa ser colhido. Você precisa de ajuda, então você aborda sua vizinha, Raquel, e faz uma proposta: se ela ajudar a colher o milho, você dará a ela uma pedra de 10 kg em troca. Raquel concorda, e durante o próximo dia, ela trabalha ao seu lado nos campos, ajudando a colher o milho e trazê-lo para dentro. No final do dia, vocês apertam as mãos e, em vez de entregar fisicamente a pedra, você simplesmente mostra a ela que o pagamento dela (a pedra Rai) está no seu quintal.

- A partir desse momento, vocês concordam que a pedra agora pertence a Raquel. Esse tipo de **transação**, em que nenhuma moeda é efetivamente entregue de um indivíduo para o outro como forma de pagamento, mas em vez disso um objeto físico é usado como **símbolo de valor**, é comum na Ilha de Yap e tem sido usado há séculos como forma de moeda.



- Cinco anos depois, você decide tentar reivindicar a pedra Rai como sua. Você apresenta evidências para a comunidade de que a pedra foi passada pela sua família por gerações e que você é o legítimo proprietário.

- No entanto, Raquel lembra do acordo que vocês fizeram e fornece evidências trazendo testemunhas da troca para dar um depoimento. Ela argumenta que a pedra pertence legitimamente a ela, pois foi dada a ela em troca de sua ajuda na colheita.
- Alguns membros da comunidade podem concordar com sua reivindicação, citando a tradição e a história de propriedade de sua família da pedra. No entanto, outros podem apoiar Raquel, apontando para o acordo que foi feito e o fato de que a pedra está em posse dela (figurativamente falando) há cinco anos sem objeções de outros membros da comunidade. Fatores que podem ser considerados incluem a história e a tradição da propriedade, os termos do acordo entre você e Raquel e quaisquer evidências ou argumentos relevantes. Não é uma solução muito sólida, não é mesmo?



Então, como milhares de estranhos podem concordar com uma verdade sem que ninguém tenha a palavra final? Isso é algo que tem intrigado as pessoas há muito tempo e é uma questão importante a ser considerada. Acontece que a internet nos ajudou a encontrar uma solução para esse problema. A solução é chamada de **blockchain**.

### 4.3.2 Vamos Trocar Confiança por Regras

Imagine que você e seus amigos estão em um chat em grupo onde podem comprar e vender coisas entre si. Sempre que uma compra é feita, ela é registrada em um documento compartilhado para

# O Futuro é Descentralizado: Empoderando Comunidades e Indivíduos

que todos possam ver e o saldo de cada pessoa é atualizado. Esse chat utiliza um livro-razão digital para registrar todas as **transações** que ocorreram. O livro-razão é como um livro de registros que todos podem ver.

Em um sistema descentralizado como esse, todos os participantes têm uma cópia do livro-razão. Isso torna difícil para qualquer pessoa ou grupo alterar qualquer informação sem ser notado. É uma medida de segurança para garantir que os registros sejam precisos e ninguém possa trapacear. Isso é semelhante ao funcionamento de um blockchain.

Em vez de depender de relacionamentos pessoais e interpretações subjetivas de confiança, um sistema descentralizado pode operar de forma eficaz se for baseado em um conjunto de regras claras e transparentes que todos concordem em seguir. Dessa forma, as decisões podem ser tomadas e os conflitos podem ser resolvidos de maneira justa e objetiva, sem depender da confiança das partes envolvidas. Pode não ser tão romântico quanto depender da confiança, mas é uma forma muito mais confiável de garantir que um sistema descentralizado funcione sem problemas.

- Se a Ilha de Yap tivesse um conjunto de regras inquebráveis e um registro escrito de todas as **transações** entre seus membros, o conflito entre você e Raquel poderia ter sido evitado. Essas regras e registros teriam deixado claro para todos os membros da vila quais eram seus direitos e responsabilidades.

Mas será que é tão simples assim? Na verdade, não; houve muita tentativa e erro antes que a tecnologia blockchain se tornasse um sucesso de fato.

- Quais são as regras exatas que devem ser seguidas?
- Quem define essas regras?
- Por que as pessoas vão querer seguir as regras?
- Como as regras são distribuídas pela rede?
- O que acontecerá se alguém quebrar as regras?
- Como as regras podem ser alteradas ou atualizadas posteriormente?
- Como as regras serão aplicadas para garantir que todos as sigam?
- Como as regras podem ser tornadas claras e de fácil acesso para todos no sistema?

## 4.4 Desbloqueando o poder do **Blockchain**: Uma tecnologia revolucionando o futuro.



Um **blockchain** é um livro-razão digital descentralizado que registra e verifica de forma segura todas as transações em vários computadores de maneira transparente.



## Capiítulo #4

Apesar de inúmeros contratemplos, uma pessoa muito enigmática (ou grupo de pessoas) finalmente encontrou a chave para desenvolver uma metodologia revolucionária para o mundo do comércio e finanças. Essa obra-prima tornou incrivelmente fácil rastrear e verificar transações, otimizando o processo de troca de dinheiro, bens e outros ativos. Com sua abordagem inovadora e tecnologia avançada, esse sistema revolucionou a forma como pensamos sobre transações econômicas, tornando-as mais rápidas, seguras e eficientes do que nunca.

Um **blockchain** é como um livro de história. Cada página (ou “bloco”) tem uma lista de coisas que aconteceram (**transações**). À medida que mais coisas acontecem, precisamos adicionar novas páginas (blocos) ao livro. Qualquer pessoa pode ler o livro gratuitamente, mas apenas ajudantes especiais (**mineradores**) podem adicionar novas páginas. Eles garantem que o que está escrito seja verdadeiro. Uma vez que algo é escrito no livro, não pode ser alterado ou apagado. É um registro permanente de todas as **transações** que ocorreram no **blockchain**.

- Um **blockchain** não possui uma autoridade central (como um autor, editor ou editora) que possa editar, apagar ou alterar as informações registradas nele, por isso é considerado um método mais seguro e confiável de registro em comparação com um banco de dados central tradicional.

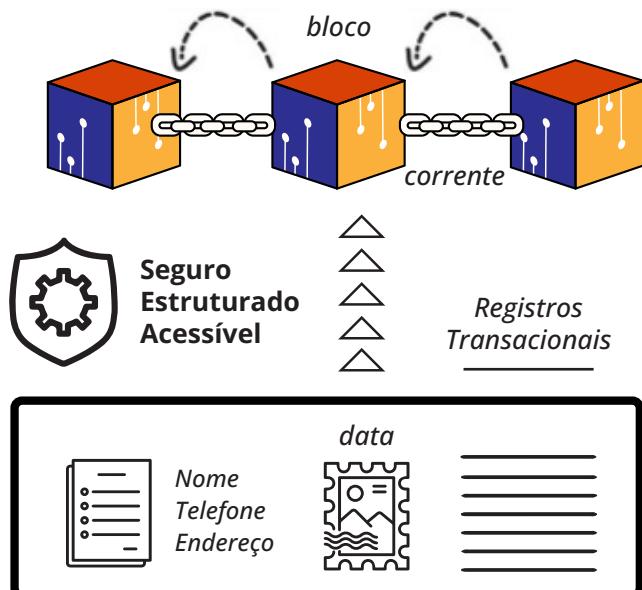


Se os ajudantes (**mineradores**) não chegarem a um **consenso** sobre a validade das páginas (**blocos**), eles serão rejeitados e não serão adicionados ao **blockchain**.

Para entender o **blockchain**, precisamos ter uma ideia do contexto em que ele existe. Embora muitos acreditem que o **blockchain** tenha usos como uma inovação independente, seu verdadeiro papel fundador é singular: criar um livro-razão imutável para que uma forma descentralizada e sem necessidade de confiança de dinheiro exista. Para entender o **blockchain**, precisamos entender o **Bitcoin** como um todo.

### O que é uma **blockchain**?

Todos os registros de ações na **blockchain** são chamados de **transações**.





# *Capítulo #5*



## *Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin*

**5.0** O Criador Misterioso do Bitcoin: Revelando a Identidade de Satoshi Nakamoto e Seu Whitepaper

**5.1** Introdução ao Bitcoin e ao bitcoin

**5.1.1** O que é bitcoin? O que é Bitcoin?

**5.1.2** Qual é a diferença entre Bitcoin e bitcoin?

**5.1.3** Por que aprender sobre bitcoin se não posso comprá-lo?

**5.1.4** Do que é feito o bitcoin?

**5.1.5** Por que o bitcoin é uma boa forma de dinheiro?

**5.1.6** Por que devo me importar?

**5.1.7** Como usar o bitcoin?

**5.1.8** Como **enviar** ou  **gastar** bitcoin?

**5.1.9** Como **receber** bitcoin?

**5.1.10** O Bitcoin pode ser desligado?

**5.1.11** Como a blockchain acompanha quem gasta qual bitcoin?

**5.1.12** Como novos bitcoins entram na rede?

**5.1.13** O que é uma transação de bitcoin?

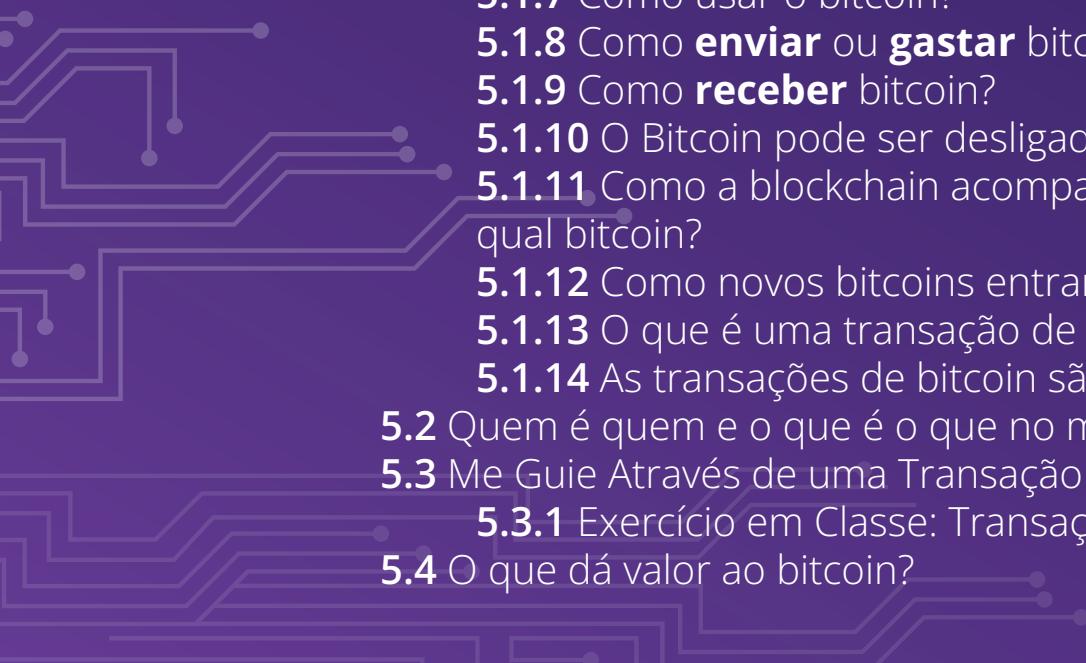
**5.1.14** As transações de bitcoin são seguras?

**5.2** Quem é quem e o que é o que no mundo do Bitcoin?

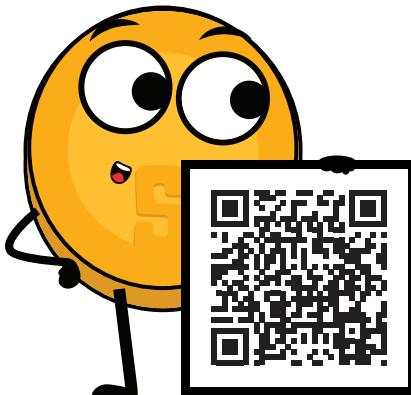
**5.3** Me Guie Através de uma Transação de bitcoin Real

**5.3.1** Exercício em Classe: Transações de Bitcoin na Prática

**5.4** O que dá valor ao bitcoin?



# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin



Assista ao seguinte vídeo: "O que é o Bitcoin? Uma Explicação Simples" por 3Blue1Brown. Você pode retornar aos momentos-chave a qualquer momento, pois o vídeo está segmentado.



O **Bitcoin** é um sistema digital revolucionário que permite transações financeiras seguras e transparentes sem a necessidade de uma autoridade central.

## 5.0 O Criador Misterioso do Bitcoin: Revelando a Identidade de Satoshi Nakamoto e Seu Whitepaper

Satoshi Nakamoto é o pseudônimo utilizado pela pessoa desconhecida ou grupo de pessoas que criaram o **Bitcoin**, e implementaram o primeiro banco de dados em **blockchain**.

Em 2008, Satoshi publicou um documento chamado "Bitcoin Whitepaper" que explicava em detalhes **o que é o Bitcoin e como ele funciona**. Ele compartilhou esse documento com a comunidade online de entusiastas de tecnologia conhecida como Cypherpunks, e rapidamente chamou atenção por sua abordagem inovadora para moeda digital.



O objetivo de Satoshi Nakamoto ao criar o **Bitcoin** era criar uma **moeda digital** descentralizada, acessível a qualquer pessoa com conexão à internet, com transações transparentes e justas que fossem permanentemente registradas em um livro-razão seguro e distribuído (a **blockchain**).

Mas aqui está o detalhe: ninguém sabe quem é realmente Satoshi Nakamoto. A identidade de Satoshi continua sendo um enigma até hoje, tornando-o uma das figuras mais fascinantes e enigmáticas no mundo da tecnologia.

- Estima-se que Satoshi Nakamoto possua cerca de 1 milhão de **bitcoins**, o que o tornaria uma das pessoas mais ricas do mundo caso sua identidade fosse revelada.
- Acredita-se que Satoshi Nakamoto seja um falante nativo de japonês, já que o software original do **Bitcoin** e o white paper foram escritos em inglês perfeito, mas alguns comentários no código estão escritos em japonês.
- Satoshi Nakamoto escreveu apenas algumas centenas de postagens em fóruns e e-mails durante seu tempo ativo, mas a maioria ainda está disponível online para dar uma visão sobre a mente e motivações do criador do **Bitcoin**.



# Capítulo #5



- Também é possível que Satoshi Nakamoto seja um grupo de pessoas e não apenas um indivíduo.
- Nos primeiros dias do **Bitcoin**, Satoshi Nakamoto era bastante ativo na comunidade, respondendo a perguntas e ajudando a resolver problemas. No entanto, ele/ela/eles desapareceram abruptamente em 2011 e não foram mais ouvidos desde então.
- A verdadeira identidade de Satoshi Nakamoto tem sido objeto de muita especulação, com várias pessoas reivindicando ser o verdadeiro Satoshi ao longo dos anos. No entanto, nenhuma dessas alegações foi comprovada de forma conclusiva.

Embora Satoshi tenha sido o principal arquiteto por trás do **Bitcoin**, ele não trabalhou sozinho. Sem dúvida, houve grande contribuição e assistência de figuras influentes na tecnologia e criptografia, incluindo Wei Dai e Nick Szabo.

Apesar dos desafios enfrentados, como problemas técnicos e ceticismo da comunidade, sua criação inspirou o desenvolvimento de muitas outras tecnologias e ganhou ampla adoção. Mesmo com as controvérsias que enfrentou, o bitcoin continua sendo o líder em um mundo de criptomoedas. A última mensagem conhecida de Satoshi foi uma garantia de que o projeto estava “em boas mãos” com o desenvolvedor de software Gavin Andresen.

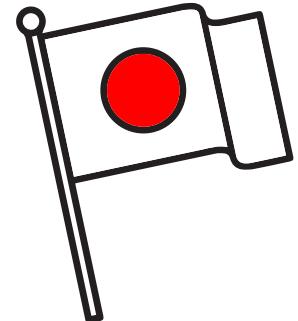
## Conspiração e Mistério do Bitcoin



O **Bitcoin** é a criação de uma pessoa ou grupo desconhecido misterioso conhecido como '**Satoshi Nakamoto**'. Até hoje, ninguém sabe quem é a pessoa (ou pessoas) por trás do Bitcoin.

### Em japonês:

- “Satoshi” se traduz como “pensamento claro; perspicaz; sábio”.
- “Naka” pode significar “dentro” ou “relação”.
- “Moto” é definido como a origem; a causa; o fundamento; a base.



Devido a isso, alguns acreditam que a tradução aponta para o **Bitcoin** ter sido criado pela CIA (Agência Central de Inteligência).

Ainda mais teóricos da conspiração acreditam que quatro empresas estão por trás das coisas:

**Satoshi = Samsung & Toshiba**  
**Nakamoto = Nakamichi & Motorola**

Pages: [1]

Author	Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 23063 times)	print
satoshi Founder Sr. Member Activity: 364 Merit: 2621	<p><b>Added some DoS limits, removed safe mode (0.3.19)</b>          December 12, 2010, 06:22:33 PM          Merited by bumbacoin (50), sukamasoto (30), yahoo62278 (25), notaek (25), mindrust (20), legendster (10), aTriz (7), Lauda (5), Betwrong (5), Mrpumperitis (5), TMAN (5), minorman (5), FruGreeds (4), EFS (3), Dänslip (3), Anon.136 (2), Yaunfida (2), cinnamon_carter (2), edgycorner (2), Searing (1), LFC_Bitcoin (1), HI-TEC99 (1), ralle14 (1), hatshepsut93 (1), finist4x (1), bill_gator (1), ix001 (1), denzukim (1), Bardman (1), Woshib (1), akirasendo17 (1), crypto_trader43xExRp (1), Rooster101 (1), ImHash (1), dark08 (1), lesom (1), Scorpion (1), CoolWave (1), glerant (1), domoy77 (1), ritaconscience (1), murrayrothbard (1), akopjuge (1), 10q (1), TheArchaeologist (1), OW21337 (1), zantezu (1)</p> <p>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 is version 0.3.19.</p> <p>- 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.</p> <p>I'm leaving the -limitfreerelay part as a switch for now and it's there if you need it.</p> <p>- Removed "safe mode" alerts          "safe mode" alerts was a temporary measure after the 0.3.9 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.</p> <p>Builds:  <a href="http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/">http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/</a></p>	#1

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

## 5.1 Introdução ao Bitcoin e bitcoin

Em 22 de maio de 2010, ocorreu a primeira troca conhecida de **bitcoin** por bens. Lazlo Hanyecz comprou duas pizzas por 10.000 BTC. Como ele fez isso?

De forma ampla, o **bitcoin** é semelhante ao dinheiro tradicional, mas em vez de ser físico, ele existe apenas na internet. Para usar **bitcoin**, você precisa baixar um programa em seu computador. Quando você executa o programa, ele se conecta a outros computadores também executando o programa. Eles compartilham um arquivo chamado **blockchain** que é uma grande lista de todas as transações de **bitcoin** já realizadas.

### 5.1.1 O que é **bitcoin**? O que é **Bitcoin**?



**bitcoin** (lowercase "b"): É o dinheiro digital que funciona na **rede do Bitcoin**.

É uma **moeda "b"** que permite às pessoas enviar e receber pagamentos online. É chamada de "digital" porque, ao contrário de moedas tradicionais como o dólar americano ou o euro, que são moedas físicas que podem ser seguradas na mão, o **bitcoin** só pode ser usado pela internet.

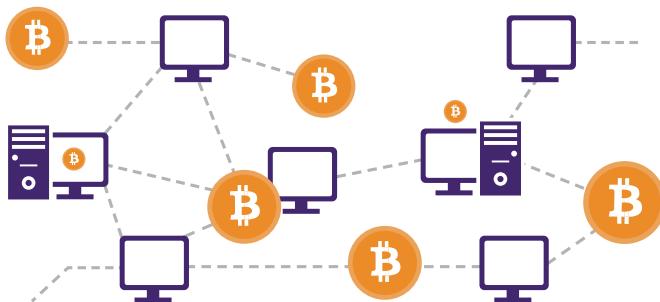


**Bitcoin** (com "B" maiúsculo): É tudo o mais; o sistema, a rede, o software, as regras, a comunidade... a criação de Satoshi.

A **rede do Bitcoin "B"** é composta por computadores de todo o mundo que trabalham juntos para processar e verificar **transações**. Essas **transações** são registradas na **blockchain**.

As regras para o uso do **Bitcoin** são implementadas no software que opera a rede do Bitcoin e seguidas por todos os participantes da rede. Elas são projetadas de forma que todos usem o Bitcoin de maneira justa e previsível.

A **comunidade** de pessoas que usa e apoia o **Bitcoin** é composta por indivíduos, empresas e organizações de todo o mundo. São eles que mantêm a rede funcional ao usar e apoiar a moeda, executar o software que alimenta a rede e contribuir para o desenvolvimento da rede.





### 5.1.2 Qual é a diferença entre **Bitcoin** e **bitcoin**?

Uma maneira de pensar na relação entre **bitcoin** e a **rede do Bitcoin** é considerar a relação entre um e-mail e a internet. Assim como um e-mail é uma mensagem enviada e recebida pela internet, o bitcoin é uma moeda digital que é transferida e recebida pela **rede do Bitcoin**. A internet fornece a infraestrutura para que os e-mails sejam enviados e recebidos, enquanto a **rede do Bitcoin** fornece a infraestrutura para que o **bitcoin** seja transferido e recebido.



### 5.1.3 Por que aprender sobre **bitcoin** se não posso pagar por ele?

Você já pensou em usar bitcoin, mas foi desencorajado pelo alto preço de uma moeda inteira? Não se preocupe, você não está sozinho! A boa notícia é que você não precisa comprar um **bitcoin** inteiro para começar a usá-lo. Assim como você pode comprar uma fração de um dólar com moedas, você também pode comprar uma fração de um **bitcoin**. Um **bitcoin** é divisível em 100 milhões de unidades chamadas **satoshis**, então você pode comprar qualquer quantidade de **bitcoin**, até mesmo uma pequena quantia. Agora que você sabe que pode comprar o equivalente a 1 centavo de bitcoin, vamos em frente e explorar as possibilidades de usar essa moeda digital!



O símbolo para **bitcoin** é **BTC** ou  e a abreviação para **satoshis** é **Sats** similarmente a como um dólar é representado por USD ou \$.

A conversão é **1 BTC = 100,000,000 sats**

Satoshi	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

- Por exemplo, digamos que você queira comprar uma maçã que custa \$1,40, mas você só tem **0.00008 bitcoin**. Não deixe a pequena quantidade te assustar! Na verdade, quando você sair da loja depois de pagar, se verificar seu saldo no celular, provavelmente notará que ainda lhe restam alguns sats para gastar.

### 5.1.4 De que é feito o **bitcoin**?

- Nada que possa ser tocado fisicamente, como uma cédula de dinheiro ou uma nota de dólar. São unidades de moeda digital que existem na **rede do Bitcoin** como um **registro de propriedade**.

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

- Assim como cada nota de dólar tem um **número de série ÚNICO** que é usado para identificá-la e evitar falsificações, e cada pessoa tem seu próprio ID, cada **transação** de **bitcoin** corresponde a uma “**impressão digital**” única do **bitcoin**, que ajuda a identificar o **bitcoin** e seu histórico de **transações**.



= 79054025255fb1a2

**Número de Série.** É uma combinação única de onze números e letras que aparece duas vezes na parte da frente da nota. Cada nota possui um número de série único.

**Transação de bitcoin.** Cada transação de bitcoin possui uma impressão digital digital única.

- Na era virtual atual, é possível que as coisas sejam reais e valiosas, mesmo que não tenham uma forma física.

## 5.1.5 Por que o **bitcoin** é um boa moeda?

Característica	Por que o bitcoin é uma boa moeda.
Durável	É uma moeda digital e não está sujeita a desgaste físico. Assim <b>como o ouro</b> .
Portável	Pode ser facilmente armazenado e transferido digitalmente, tornando-o conveniente para ser levado para qualquer lugar. <b>Como dinheiro em espécie, mas melhor.</b>
Uniforme	Todos os <b>bitcoins</b> têm o mesmo valor, não importa onde sejam usados ou quem os possui. <b>Como dinheiro em espécie, mas melhor.</b>
Aceitável	A cada dia, mais pessoas ao redor do mundo estão aceitando o bitcoin como forma de pagamento. <b>Como dinheiro em espécie, mas melhor.</b>
Escasso	O fornecimento total de <b>bitcoin</b> é limitado, exatamente 21.000.000, tornando-o valioso e desejável. <b>Como o ouro, mas melhor.</b>
Divisível	Ele pode ser dividido em unidades menores, chamadas <b>satoshis</b> , permitindo transações menores. Em teoria, por ser digital, um <b>bitcoin</b> é infinitamente divisível. <b>Como dinheiro em espécie, mas melhor.</b>

## 5.1.6 Por que eu deveria me importar?



### Pagamentos mais rápidos e mais baratos.

Enviar dinheiro ao redor do mundo em minutos, com taxas extremamente baixas.



### Inclusão financeira.

2,5 bilhões de pessoas não bancarizadas podem ter acesso a dinheiro por meio de um telefone ou computador.



### Privacidade aumentada

As transações de **Bitcoin** são públicas, mas sua identidade não é.



### Tecnologia Blockchain

A tecnologia por trás do **Bitcoin** impulsionará o futuro de muitas indústrias diferentes.



### 5.1.7 Como você usa o **bitcoin**?

Para usar o **bitcoin**, você precisará configurar uma carteira digital em seu computador ou telefone. Você pode usar sua carteira para armazenar, enviar ou receber **bitcoins** de outras pessoas, ou até mesmo para comprar coisas online.

### 5.1.8 Como enviar ou receber **bitcoin**?

Tudo o que você precisa é de uma conexão com a internet.

- O processo de envio de **bitcoin** é semelhante ao envio de um e-mail. Para enviar um e-mail, você abre seu cliente de e-mail, insere o endereço de e-mail do destinatário, digita uma mensagem e clica em enviar. De maneira semelhante, para enviar **bitcoin** para alguém ou gastar **bitcoin** ao comprar algo em troca, você abre sua carteira de **bitcoin**, insere o

**endereço**, de **bitcoin** do destinatário, insere a quantidade de bitcoin que deseja enviar (ou gastar) e clica em enviar.

### 5.1.9 Como receber **bitcoin**?

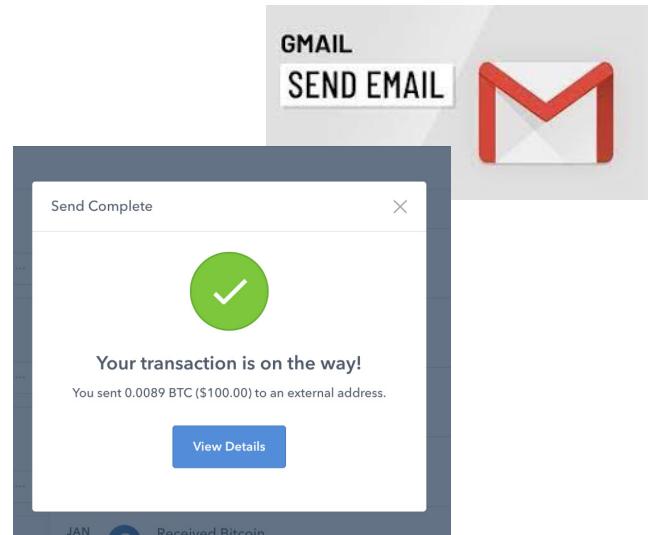
Para obter **bitcoin**, você pode comprá-lo online, aceitá-lo como presente de alguém ou como pagamento por bens ou serviços, ou “minerá-lo” (trabalhar duro por ele) usando um dispositivo de computação. Com qualquer uma dessas formas, uma vez que você o obtém, você o armazena em uma “carteira”.

### 5.1.10 O **Bitcoin** pode ser desligado?

Os governos podem tentar dificultar o **uso** do **Bitcoin**, mas é difícil desligar completamente a rede. Isso ocorre porque o **Bitcoin** é descentralizado, o que significa que não há uma empresa ou organização central que o controle. Em vez disso, o software é de **código aberto**, que significa que qualquer pessoa pode baixar, usar e executar o software em seu próprio computador.

Os governos podem tentar **restringir o acesso** ao **Bitcoin**, mas isso é semelhante à forma como os governos tentam controlar o acesso à Internet. As pessoas podem usar ferramentas como VPNs para contornar essas restrições. Além disso, devido à natureza digital do **Bitcoin**, ele pode ser ocultado relativamente facilmente. É muito mais difícil para os governos localizarem e confiscarem **bitcoin** do que é para localizar e confiscar ativos físicos como ouro ou imóveis.

Apesar de ser ilegal em alguns países, as pessoas continuam a acessar a **rede Bitcoin**. Além disso, alguns países têm tentado controlar o **Bitcoin** criando suas próprias moedas digitais do banco central, o que pode ter resultados variados. Algumas pessoas podem aceitar e se adaptar ao novo sistema centralizado, enquanto outras podem rejeitá-lo e buscar soluções descentralizadas como o **Bitcoin**.

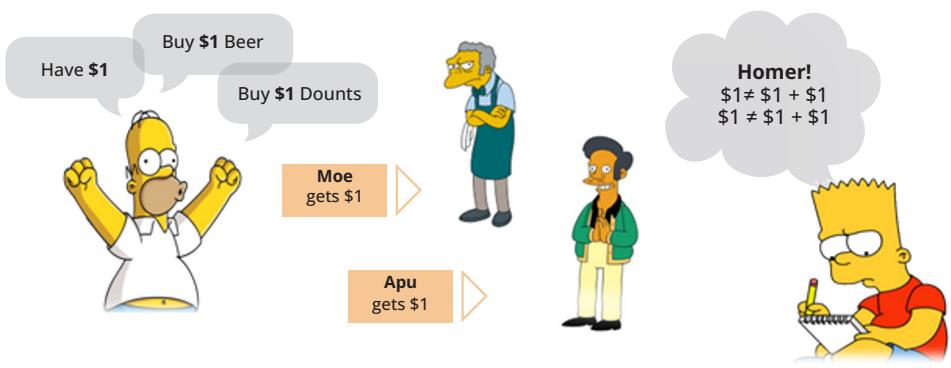


# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

## 5.1.11 Como o Blockchain acompanha quem gasta qual bitcoin?

Você sabe como não pode gastar a mesma nota de dólar duas vezes? O **Bitcoin** funciona de maneira semelhante para garantir que você não possa gastar a mesma moeda digital duas vezes.

Antes do **Bitcoin**, era possível enviar transações através de uma rede de computadores, mas havia um problema: as pessoas poderiam enviar transações conflitantes, como tentar gastar a mesma moeda duas vezes. Isso é chamado de “gasto duplo”.



O **Bitcoin** resolve esse problema fazendo com que todos os computadores da rede trabalhem juntos. Quando uma nova transação é enviada, ela é enviada para todos os computadores, e eles a mantêm na memória antes de gravá-la em um arquivo permanente (o **blockchain**).

Esse processo é chamado de “mineração” e garante que nenhuma transação de gasto duplo seja gravada no **arquivo**. É como uma grande competição em que ninguém pode trapacear, então seus **bitcoins** estão sempre seguros.

**É assim que o Bitcoin alcança consenso, tudo isso sem dar um único soco!**

Em intervalos regulares, um dos computadores adiciona todas as transações que tem na memória ao arquivo. Em seguida, ele compartilha o arquivo atualizado com todos os outros computadores da rede. Todos os computadores concordam quais transações são válidas e quais não são, e eles removem quaisquer transações conflitantes de sua memória.

## 5.1.12 Como novos bitcoins entram na rede?

Para pagar ou **recompensar os mineradores** por seu trabalho árduo, toda vez que eles adicionam um novo bloco ao blockchain, eles recebem **bitcoins** recém-criados como compensação. Atualmente, os mineradores recebem 6,25 BTC por cada bloco que mineram.

## 5.1.13 O que é uma transação de bitcoin?

Uma transação de **bitcoin** é uma transferência de propriedade de unidades de **bitcoin** existentes para um novo proprietário. Mas em vez de transferir moedas reais, o que acontece é que todos os nós da rede atualizam sua cópia local do livro-razão público para refletir a mudança de propriedade. (Lembre-se das pedras Rai! Esta é apenas uma versão mais avançada, em que o livro-razão é externalizado, em vez de ser memorizado, para que todos possam revisar e ver).



- Marc e Roby querem trocar 1 BTC. Para entender isso, é importante saber que não existem moedas físicas no **bitcoin**, apenas atualizações no **blockchain**, que são refletidas nas carteiras de ambas as partes envolvidas.
- Quando Marc deseja enviar 1 BTC para Roby, isso é chamado de **transação ponto-a-ponto** porque a propriedade do valor vai diretamente de Marc para Roby. Mas Roby não recebe realmente uma "moeda digital" de Marc. Em vez disso, todos os nós da rede atualizam sua cópia local do livro-razão público, o que altera a propriedade do **bitcoin** do endereço de Marc para o endereço de Roby.
- Uma **transação de bitcoin** é simplesmente uma **mensagem assinada** que Marc envia para a rede, que é então validada por muitos nós. A mensagem passa por várias etapas, como ser captada por alguns nós completos, ser validada e depois transmitida, até que todos os nós na rede a tenham validado independentemente.



A **assinatura** é uma representação digital dos **detalhes da transação**, incluindo a quantidade de **bitcoin** sendo enviada, o **endereço do remetente (Marc)**, e o **endereço do destinatário (Roby)**.



### O objetivo de uma assinatura digital



Uma assinatura confirma que a mensagem (documento ou e-mail) originou-se do remetente e NÃO foi alterada.

**chave privada** e transferir qualquer quantidade desejada de **bitcoin** para outro cofre..

Da perspectiva de Roby: Para **receber bitcoin**, você precisa fornecer ao remetente (Marc) seu **endereço** onde os **bitcoins** podem ser depositados.

Da perspectiva de Marc: Para  **gastar** seus **bitcoins**, você precisa acessar **sua chave privada** para desbloqueá-los.

Imagine todos os **bitcoins** existentes como estando armazenados em cofres digitais, cada um com uma quantidade diferente de BTC, juntamente com um histórico de como eles chegaram lá.

Cada cofre tem um proprietário. Portanto, ele precisa ser identificável com um **endereço**. Os endereços são protegidos por uma fechadura digital com duas chaves diferentes, como senhas de uma conta. Se um cofre contém **bitcoin**, seu proprietário pode abri-lo com sua

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

## 5.1.14 As transações de bitcoin são seguras?

Os detalhes da **transação**, como os endereços do remetente e do destinatário e a quantidade transferida, são publicamente visíveis na **blockchain**, mas a propriedade dos **bitcoins** transferidos é verificada por meio do uso de criptografia.

### O que é Criptografia?



A **criptografia** é uma forma de manter informações em segredo, disfarçando-as em código.



- A **criptografia** é o processo de pegar informações e colocá-las em um código especial, tornando-as ilegíveis para qualquer pessoa sem o método correto de descriptografia. Isso é semelhante a trancar um cofre, onde apenas a pessoa com a chave correta ou combinação pode abri-lo.

- Por outro lado, a **descriptografia** é o processo de pegar as informações codificadas e **torná-las legíveis novamente**, como desbloquear o cofre e poder ler as informações contidas nele..

Por exemplo, vamos supor que Arel e John queiram manter uma mensagem oculta de alguém chamado Ronny. Eles concordam em

usar uma chave secreta para disfarçar a mensagem antes de enviá-la um ao outro. Eles poderiam usar um método simples, como deslocar cada letra da mensagem no alfabeto, para que A se torne B, B se torne C e assim por diante. Apenas aqueles com a chave podem descriptografar a mensagem, tornando-a ilegível para Ronny. Embora esse método não seja considerado seguro hoje em dia, ele ilustra o princípio da criptografia de chave privada.

### Como Resolver o Código Pigpen

Ao resolver o Cifra Pigpen, o jogador recebe uma mensagem criptografada e um código. Para descriptografar a mensagem, o jogador encontrará o símbolo da mensagem criptografada no código para descobrir a letra descriptografada.

- Exemplo de uma mensagem criptografada:

— • — — —  
\_\_\_\_\_

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



## Capítulo #5

### Como a Criptografia Funciona nas Transações de Bitcoin?

Na criptografia de chave privada tradicional, John e Arel teriam que compartilhar primeiro uma chave secreta, como uma senha. John usaria então essa chave para embaralhar sua mensagem antes de enviá-la para Arel. Arel, que também conhece a chave secreta, usaria a mesma chave para desembaralhar a mensagem e lê-la.

No entanto, Ronny também poderia interceptar a mensagem e usar a mesma chave para desembaralhá-la e ler a mensagem.

Com a **criptografia de chave pública**, que é o tipo de criptografia usado nas transações de bitcoin, John e Arel têm cada um duas chaves: uma **chave pública** e uma **chave privada**. John pode usar a **chave pública** de Arel para embaralhar sua própria mensagem antes de enviá-la (para Arel). Apenas a **chave privada** de Arel pode desembaralhar a mensagem. Ronny, que não possui a **chave privada** de Arel, não seria capaz de ler a mensagem mesmo que a intercepte.

Além de criptografar mensagens, a criptografia de **chave pública** também pode ser usada para assinaturas digitais. Uma **assinatura digital** é uma maneira de comprovar a autenticidade de uma mensagem, semelhante a uma assinatura escrita em um documento físico. Para criar uma assinatura digital, John usaria **sua chave privada** para **criptografar sua assinatura**. Arel então usa a **chave pública** de John para descriptografá-la e verificar que ela foi realmente enviada por John.

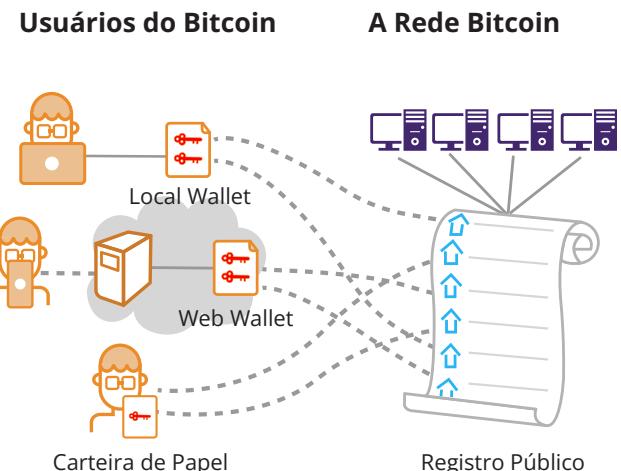


#### Criptografia de Chave Pública (Para cada transação entre dois usuários):

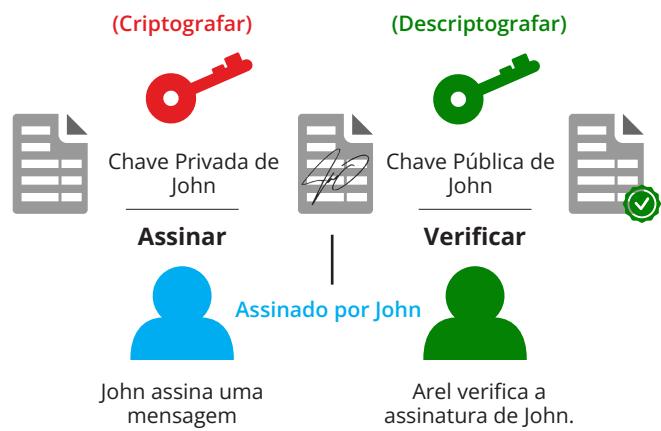
Cada usuário possui duas chaves: uma **chave privada**, que é **mantida em segredo**, e uma **chave pública** que pode ser **compartilhada com outros**.

A **chave privada** serve como uma forma de identificação e prova de propriedade, confirmando: “**Este endereço pertence a mim e tenho controle sobre ele**”

As **assinaturas digitais** são criadas para identificar transações únicas.



#### Assinatura Digital



# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

Portanto, a principal vantagem da **criptografia de chave pública** sobre a criptografia de chave privada é que ela permite comunicação segura sem a necessidade de o remetente e o destinatário compartilharem previamente uma chave secreta, que poderia ser interceptada por uma terceira parte.

- As transações de **Bitcoin** envolvem a transferência de uma certa quantidade de **bitcoin diretamente** para a conta de outra pessoa.

○ Você não gostaria que alguém roubasse o dinheiro que seu amigo enviou via Venmo porque o sistema de pagamento é inseguro, certo?

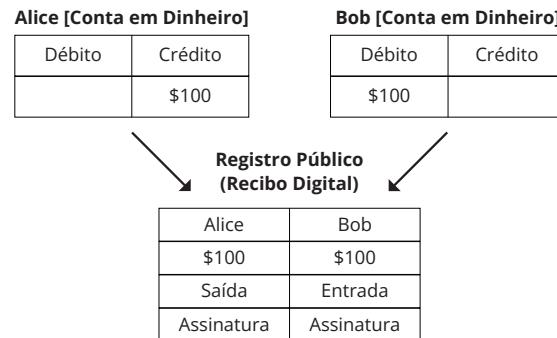
- A criptografia é uma maneira de manter informações importantes protegidas contra agentes maliciosos enquanto viajam pela rede, alguns dos quais, como hackers, podem desviar os fundos para suas contas.

- Como medida adicional de proteção, para manter os **detalhes da transação** seguros no **Bitcoin**, é adicionada uma **assinatura ÚNICA** a cada **transação**. Essa **assinatura** funciona como um código secreto que garante que ninguém possa alterar qualquer parte da **transação** sem que o software o detecte e o marque como inválido.

## Comparando as Transações de **Bitcoin** com os Bancos Tradicionais

- Nos bancos tradicionais, um **PIN** é usado para **autenticar** **transações**, de forma semelhante à forma como uma **chave privada** é usada para **assinar** **transações** em **blockchains**.

Uma analogia simples para esse processo seria uma pessoa acessando seu número de conta bancária com um PIN privado (**chave privada**), e, em seguida, usando sua própria assinatura pessoal (**assinatura única**) em um cheque online (**moeda digital**) para enviar dinheiro (**fazer uma transação**) para outra pessoa (outro usuário). Assim como a assinatura de uma pessoa em um cheque verifica sua identidade e autoriza a **transação**, a **assinatura digital** usando uma **chave privada** verifica a identidade e autoriza a **transação** da moeda digital.





### 5.2 Quem é quem e o que é o que no mundo do Bitcoin Identificando os principais papéis na rede.

Existem três tipos principais de participantes na rede **Bitcoin**:

- 1 **Mineradores** são computadores na **Rede Bitcoin** que escrevem e verificam novas transações no blockchain, adicionando novos blocos a ele. Os mineradores são recompensados com **bitcoins** pelo trabalho que realizam!
- 2 **Nós** são computadores na **Rede Bitcoin** que armazenam e verificam transações e blocos no blockchain. Os nós não são recompensados pelo seu trabalho.
- 3 **Desenvolvedores** são responsáveis por manter e propor melhorias no software **Bitcoin** (ou seja, o código). Eles garantem que todos os computadores na rede sigam as regras e funcionem de forma adequada.

No geral, esses três grupos trabalham juntos para manter a **Rede Bitcoin** em funcionamento e garantir que ela permaneça segura e descentralizada.

- **Os usuários** são indivíduos comuns que usam **bitcoin**. Eles enviam e recebem **bitcoin** por meio de suas carteiras e também podem fazer compras ou trocá-lo por outras moedas.
- **As exchanges** permitem que os usuários comprem, vendam e negoçiem **bitcoin**, além de facilitarem as transações na rede. No entanto, as exchanges não desempenham um papel direto na operação da **Rede Bitcoin** em si.

Ainda um pouco confuso? Voltando à nossa analogia em que a **Rede Bitcoin** é como um sistema de transporte, vamos reintroduzir os principais participantes.

- **Os mineradores** são como *cabinas de pedágio automatizadas ou contadores de livros*.

- Eles são responsáveis pela contabilidade. Eles registram todos os carros que passam e cobram taxas. Eles também verificam se os carros (transações de bitcoin) que passam não são roubados, possuem placas vencidas ou são conduzidos por motoristas sem licença ou embriagados.
- Esse processo ajuda a garantir que o sistema rodoviário (**Rede Bitcoin**) seja seguro e eficiente, e ajuda a prevenir colisões ou fraudes..



# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

- **Os nós** podem ser considerados como *praças de serviços* ao longo das estradas.
  - Assim como uma praça de serviços é um local para parar, comer ou usar banheiros, um nó em uma rede *blockchain* é um ponto onde as *transações* são processadas, validadas e armazenadas.
  - Assim como as praças de serviços têm áreas de descanso e estacionamentos, os nós têm suas próprias salas de espera (mempool) para *transações* verificadas antes de continuarem na *blockchain*.
  - As praças de serviços não cobram pela sua estadia ou uso do local.
- **Os desenvolvedores** são como *engenheiros* que projetam e constroem o sistema rodoviário.
- Eles são responsáveis por manter e melhorar a infraestrutura da rede, como corrigir quaisquer problemas que possam surgir ou



adicionar novos recursos.

Uma **carteira de bitcoin** é como uma *garagem* para o seu carro. Assim como uma garagem é um local seguro para armazenar seu carro quando ele não está em uso, uma **carteira de bitcoin** é um local seguro para armazenar seus *bitcoins*.





- Vamos supor que você possui um **carro** (um **bitcoin**) e deseja mantê-lo seguro quando não estiver dirigindo. Você pode colocá-lo em sua **garagem** (uma carteira de bitcoin) e **trancar a porta** (bloquear sua carteira com uma **senha**). Isso protegerá seu carro (**bitcoin**) de ladrões (hackers). Quando você quiser usar seu carro (gastar seu bitcoin), você pode abrir a porta da garagem e desbloquear sua carteira com outra **senha**, que é necessária para **ligar o carro** e **retirá-lo** da garagem (fazer uma **transação**).



**As exchanges** podem ser consideradas como **concessionárias de carros**. Assim como uma concessionária permite que você compre e venda carros, uma exchange permite que você compre e venda **bitcoin**.

- Por exemplo, se você quiser vender seu carro (**bitcoin**), pode levá-lo a uma concessionária (exchange) e eles o ajudarão a encontrar um comprador.

comprador.

Vamos analisar o **Bitcoin** em termos de venda de carro:

Imagine que você, o usuário, tenha um ativo valioso, como um **bitcoin**, que deseja vender. Você o leva a uma exchange, semelhante a uma concessionária, para encontrar um comprador. Ao longo do caminho, você passa pelos nós da rede, semelhantes a praças de serviços, para garantir que seu ativo esteja em condições ideais antes da venda. A **transação** passa então por um processo rigoroso de verificação com o departamento financeiro da exchange, semelhante a contadores em uma concessionária, para garantir que tudo esteja correto e a venda ocorra sem problemas. Uma vez concluída a venda, você recebe o pagamento em moeda fiduciária e a exchange assume a posse do ativo, transferindo-o para sua carteira. A rede também possui uma equipe de desenvolvedores, semelhantes a engenheiros em uma concessionária, trabalhando na melhoria e atualização das características e tecnologia do **Bitcoin**. Outros participantes da rede, como comerciantes e investidores, também desempenham um papel no funcionamento da **Rede Bitcoin**.

### 5.3 Me acompanhe em uma transação real de **bitcoin**

Novas **transações** de **Bitcoin** são iniciadas a partir de carteiras ao redor do mundo, mas não há um processador central de pagamentos. Em vez disso, **mineradores** ao redor do mundo competem para **registrar** as **transações** no registro.

Digamos que Jim deva **0.5 BTC** a Eliana e esteja pronto para pagar a ela. Ambos têm carteiras digitais.

1. Eliana compartilha seu **endereço** com Jim.
2. Jim usa seu software de carteira para criar a **transação**, que inclui o **endereço**, de Eliana, a quantia a ser transferida (0,5 BTC) e uma taxa para o minerador.

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin



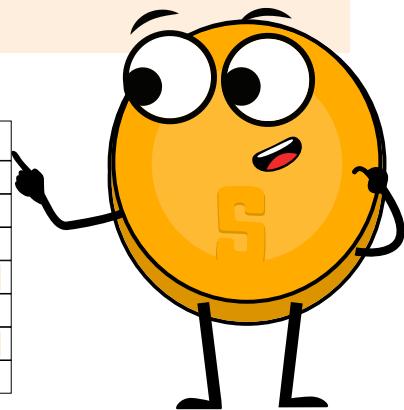
Quando Jim clica em "enviar", sua carteira usa sua **chave privada** para desbloquear 0,5 BTC, pois é assim que ele **"assina"** a transação. No entanto, **ele não revela sua chave privada** de fato.

- Ao fazer isso, Jim está informando à rede **"Eu sou o proprietário desta conta e aprovo a transferência de 0,5 bitcoin para a conta de Eliana"**.

LIVRO-RAZÃO	
Dono da Conta	Valor
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniel	5.25

Mensagem de Solicitação de Transação de Bitcoin.  
Jim envia 0.50 BTC para Eliana  
**Jim ➔ Eliana 0.50 BTC**

LIVRO-RAZÃO	
Dono da Conta	Valor
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.00
Robert	2.00
Eliana	2.25
Daniel	5.25



**3.** Após **assinar** a **transação**, ela é **transmitida** para a rede, onde é verificada por nós chamados de mineradores. Os mineradores verificam a validade da **transação** e garantem que Jim tenha fundos suficientes. Se ele não tiver, a **transação** é rejeitada imediatamente.

Uma vez que a **transação** é verificada e incluída em um bloco, ela é adicionada à **blockchain**, e os fundos são transferidos para o **endereço** de Eliana.

**5.** Eliana pode então usar sua **chave privada** para acessar os fundos transferidos em sua carteira.

É importante observar que, uma vez que a **transação** é concluída, ela não pode ser revertida.

## Agora, com um pouco mais de detalhes:

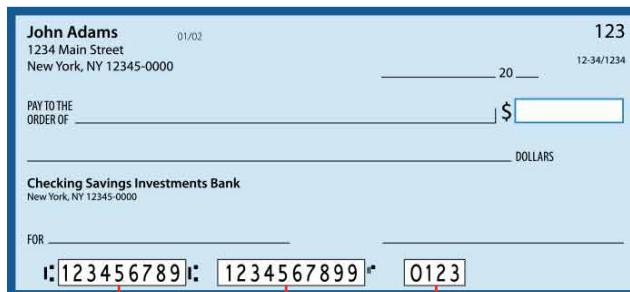
Após abrir sua carteira digital, Jim, através de seu próprio **endereço**, inicia a **transação** solicitando e incluindo o **endereço de bitcoin** de Eliana (semelhante a escrever um número de roteamento para uma transferência bancária tradicional) e a quantidade de **bitcoin** a ser enviada. Jim **assina** a **transação** com sua **chave privada** (semelhante a acessar uma conta com uma senha privada) para validar a transferência.

**My Wallet** Be Your Own Bank.

Wallet Home My Transactions Send Money Receive Money Import / Export

Total Transactions	0	
Total Received	0.00 BTC	
Total Sent	0.00 BTC	
Final Balance	0.00 BTC	

This Is Your Bitcoin Address  
19emjx4vqHPn6ZTsh1ZNbBD7uFZFqWA5Cq  
Share this with anyone and they can send you payments.



Número de roteamento do banco Número da conta Número do cheque



## Capítulo #5



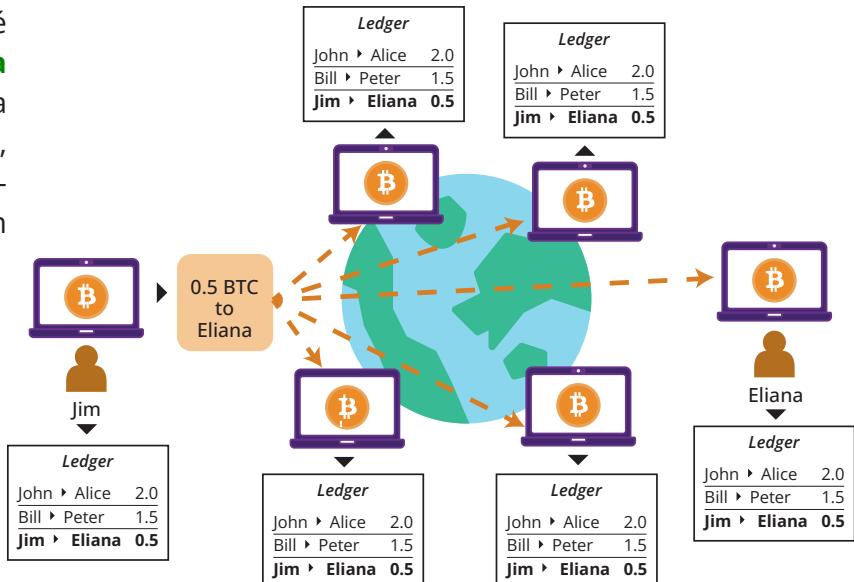
Em seguida, a **transação** é transmitida para a rede com apenas um clique de botão.

Uma **transação** na **blockchain** pode ser comparada a um processo de entrega de pacotes. Quando um pacote é enviado pela primeira vez, ele é apenas um pacote em **um** correio (uma **transação** enviada para um primeiro nó). O correio (nó) **verifica** a autenticidade do pacote e, se for válido, o envia para outros correios (nós) para verificação adicional. O pacote é passado de correio para correio até chegar a todos os correios da rede (todos os nós na **blockchain**). A autenticidade e validade do pacote são confirmadas em cada parada, assim como uma **transação** é verificada por vários **nós** na blockchain. **blockchain**.

- O **endereço** único de Eliana é gerado usando sua **chave pública** para garantir que apenas ela possa acessar e desbloquear os fundos, semelhante a resolver um quebra-cabeça em que apenas aqueles com as peças corretas podem abri-lo.



Para **verificar** a autenticidade da transação, é usado uma **assinatura digital** e uma **chave pública**.



A **assinatura digital** e a **chave pública** são duas peças importantes do quebra-cabeça. A **chave pública** atua como um cartão de identificação, garantindo que Jim é o legítimo proprietário do **bitcoin**. A **assinatura digital** comprova que Jim autorizou a **transação**, assim como assinar um cheque.

	Assinatura Manuscrita	Assinatura Digital
Conceito		Assinatura digital usando criptografia assimétrica // Método de descriptografia 73207079591743137199 61288414545595292784 33060039936533846924
Problema	Reutilizável	Impossível de reutilizar



prove  
justify  
check  
inspect  
confirm  
substantiate  
clarify  
verify  
attest  
authenticate

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

Os **nós** na **Rede Bitcoin** são como verificadores de quebra-cabeça. Eles devem verificar se todas as peças se encaixam corretamente. Eles garantem que Jim seja o proprietário do **bitcoin** e tenha autorizado a **transação**.

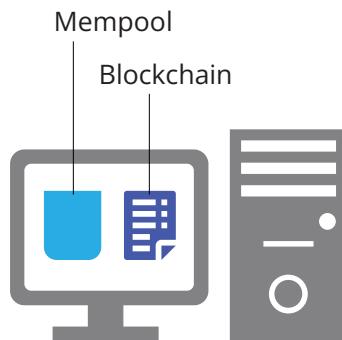
Uma vez que a maioria dos nós esteja em consenso de que o quebra-cabeça foi resolvido corretamente, a **transação** é considerada legítima e adicionada a uma **fila**.



Essa fila de transações pendentes é chamada de "**mempool**".

O **mempool** é como uma área de espera para quebra-cabeças que foram resolvidos corretamente, mas ainda não foram adicionados (encadeados) ao quebra-cabeça permanente (**blockchain**). Ele está localizado em uma seção diferente do armazenamento de memória de um nó em comparação com o **blockchain**, que registra permanentemente as **transações** confirmadas.

## Um Nó na Rede Bitcoin



Uma vez que as transações são verificadas, elas devem ser registradas permanentemente no **blockchain**. Um grupo de **nós** chamados "**mineradores**" compete para ser o primeiro a adicioná-las ao **blockchain**, a fim de receber uma recompensa.

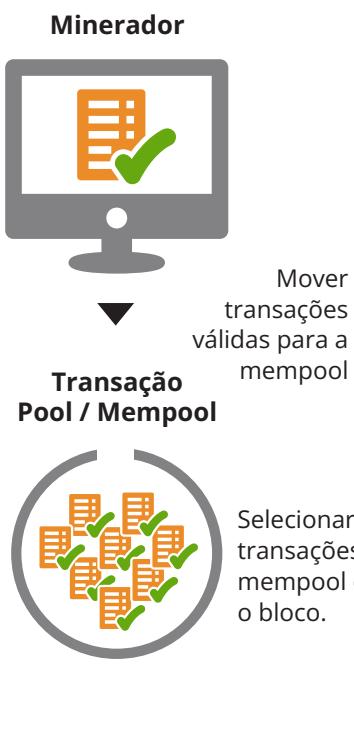
Conheça os super-heróis do **Bitcoin**: **os mineradores!** Esses computadores especiais usam seu software superpoderoso para verificar se ninguém está **gastando duas vezes**, roubando ou enviando acidentalmente fundos que não possuem e garantem que todos os outros mineradores estejam fazendo o mesmo.

- **Os mineradores** são como curadores de quebra-cabeças, eles selecionam quais quebra-cabeças da fila adicionar à exposição final, esse processo garante que o mesmo bitcoin não possa ser gasto duas vezes pela mesma pessoa e que as **transações** sejam processadas rapidamente.

Os mineradores mantêm uma cópia do **blockchain**, e verificam cada **transação** em relação ao blockchain para **confirmar** que o mesmo **bitcoin** não foi gasto antes. Apenas **transações** legítimas que atendem a certos critérios, como ter a **assinatura digital** correta e fundos suficientes, são adicionadas ao **blockchain** pelos mineradores.

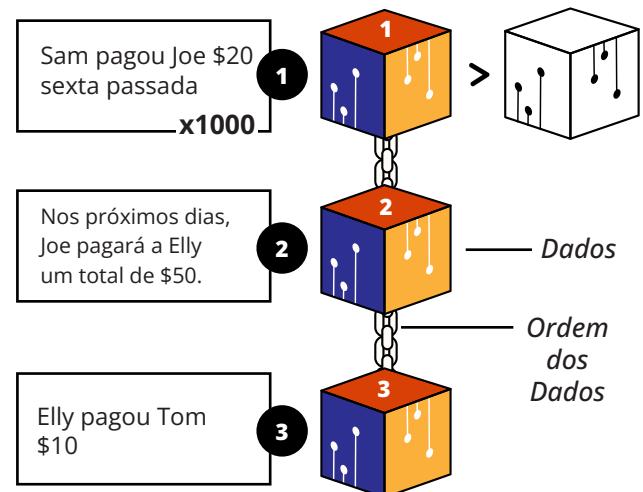


Uma vez no **blockchain**, as transações incluídas no bloco são consideradas completas e irreversíveis. A troca de **bitcoin** de um **endereço** para outro é liquidada.



Em resumo, o uso do **Bitcoin** envolve a criação de uma **transação**, sua transmissão para a rede e a validação e confirmação da mesma. Esse processo garante que a **transação** seja segura e não possa ser alterada, permitindo que as pessoas confiem no sistema sem a necessidade de uma autoridade central.

#### Exemplo de uma Transação em uma Blockchain



#### Como uma transação de Bitcoin funciona



#### 5.3.1 Exercício em sala de aula: Transações de Bitcoin em Ação

Os mineradores são responsáveis por adicionar novas **transações** à **blockchain**. Full nodes validam as **transações** e armazenam uma cópia completa da **blockchain**. Light nodes permitem que as pessoas validem **transações** usando menos armazenamento e recursos computacionais.

**Exercício em sala de aula.** Vamos assumir que o remetente e o destinatário são light nodes. Na realidade, nem todas as carteiras são light nodes.

*Entenda o seu papel. Você foi designado para um dos seguintes papéis: remetente, destinatário, nó ou minerador.*

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

- Os remetentes serão responsáveis por criar e transmitir transações.
- Os destinatários serão responsáveis por receber e verificar as transações.
- Os nós serão responsáveis por validar as transações, verificando se a transação é válida. Eles farão isso comparando-a com as regras do protocolo e o mecanismo de consenso.
- Os mineradores serão responsáveis por adicionar as transações à blockchain.

**1. Como remetente:** Crie uma transação. Para criar uma transação, siga estes passos:

- Pegue uma nota de transação e escreva a quantidade de moedas que deseja enviar e o nome ou iniciais do destinatário.
- Assine a nota com o seu nome ou iniciais, simulando uma **chave privada**.
- Passe a nota de transação e a quantidade correspondente de **moedas** para o destinatário.

**Tanto os nós quanto os destinatários devem verificar as transações:**

**2. Como destinatário:** Você é responsável por verificar as transações. Siga estes passos:

- Verifique a nota de transação para garantir que a quantidade correta de moedas e o nome ou iniciais do destinatário estejam escritos.
- Conte as moedas recebidas e compare-as com a quantidade de moedas escrita na nota.
- Se as moedas coincidirem, marque a caixa de aprovação.
- Se as moedas não coincidirem ou se tiver dúvidas, rejeite a transação.

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

**3. Como um nó:** Verifique e valide as transações. Você é responsável por verificar se a transação é válida.

- Verifique se o endereço do remetente é válido e se o endereço do destinatário é válido.
- Verifique se o remetente possui fundos suficientes para concluir a transação e se a transação não está gastando duas vezes as mesmas moedas.

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

**4. Adicionar transações à blockchain:** **Como minerador**, você é responsável por adicionar as transações à blockchain. Siga estes passos:

- Verifique as transações que foram aprovadas pelos destinatários e validadas pelos nós.



- Role o dado e compare os números com o outro minerador. O minerador com o número menor irá adicionar a **transação** à blockchain.
- Pelo seu tempo, energia e esforço, você receberá uma recompensa. Vá escolher um doce de sua escolha.
- Uma vez que uma **transação** é adicionada à **blockchain**, ela não pode ser alterada ou revertida.

**5.** Mantenha o controle do seu saldo de **moedas**: Ao longo da atividade, acompanhe seu saldo de moedas contando as moedas em sua carteira digital.

Moeda Enviada	Remetente	Assinatura do Remetente	Destinatário	Data e Hora	Aprovação

**6.** Discuta os conceitos aprendidos com sua turma.

#### **5.4 O que dá valor ao bitcoin ?**

Ao contrário das formas tradicionais de moeda, como ouro ou dinheiro fiduciário, o **bitcoin** é digital, descentralizado e escasso. Essas características conferem a ele várias vantagens em relação às formas tradicionais de dinheiro, tornando-o uma valiosa reserva de valor e meio de troca.

O **Bitcoin** obtém seu valor a partir de uma combinação de fatores, incluindo:

- Sua escassez, uma vez que a quantidade total de **bitcoins** que podem ser criados é limitada a 21 milhões, o que o diferencia do dinheiro regular que pode ser impresso pelos governos.
- Sua utilidade como uma moeda digital descentralizada, o que significa que não é controlada por nenhum governo ou instituição e pode ser usada para **transações** em qualquer lugar do mundo.
- Valor percebido por investidores e usuários, já que algumas pessoas veem o **bitcoin** como um bom investimento, uma forma de guardar dinheiro ou uma proteção contra a inflação.

#### **Qual é a demanda de mercado pelo bitcoin e como ela influencia seu preço?**

A demanda de mercado pelo **bitcoin** se refere à quantidade de pessoas dispostas a comprar Bitcoin a um determinado preço. O preço do **bitcoin** é influenciado pela demanda de mercado, assim como pela oferta e outros fatores econômicos. Quando a demanda é alta e a oferta é limitada, o preço do **bitcoin** tende a aumentar. Por outro lado, quando a demanda é baixa e a oferta é grande, o preço do **bitcoin** tende a diminuir.

Um dos principais argumentos contra o **bitcoin** é que ele não é respaldado por nenhum ativo físico ou garantias governamentais, tornando-o intrinsecamente sem valor. No entanto, esse argumento

# Revelando o Futuro do Dinheiro: Uma Introdução ao Bitcoin

compreende erroneamente a natureza do dinheiro. **O dinheiro não precisa ser respaldado por ativos físicos ou garantias governamentais para ser valioso; ele simplesmente precisa ser amplamente aceito como meio de troca e reserva de valor. O Bitcoin atende a esses critérios e vai além.**

O status virtualmente intocável do **Bitcoin**, que torna difícil sua apreensão, é um fator importante em seu valor para aqueles que temem regimes autoritários ou tirânicos. Essa característica é vista como mais valiosa do que as características físicas de um ativo por alguns.

Por fim, o **Bitcoin** também é versátil, com sua tecnologia subjacente, o blockchain, sendo aplicada em diversas indústrias, como cadeia de suprimentos, identidade digital e muito mais, tornando-o uma mercadoria valiosa em muitas áreas diferentes.

- O **Bitcoin** está sendo visto como uma solução para os problemas econômicos do mundo, pois é justo, seguro e incorruptível.
- O **Bitcoin** está sendo chamado de ouro digital, e espera-se que sua demanda continue a crescer à medida que mais pessoas assumem o controle de sua riqueza.
- Embora possa haver debates em curso sobre o papel do **bitcoin** como meio de troca, é importante reconhecer o progresso significativo que foi feito nos últimos anos para aumentar sua aceitação como uma opção viável para **transações**. Com o surgimento de novas tecnologias e soluções de pagamento inovadoras, o **bitcoin** está sendo cada vez mais visto como um meio de troca prático e eficiente, especialmente no âmbito das **transações** internacionais. À medida que mais empresas e indivíduos reconhecem as vantagens de usar o **bitcoin** para **transações** cotidianas, seu potencial de se tornar um meio de troca amplamente aceito continua a crescer.



## *Capítulo #5*





## *Capítulo #6*

# *Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras*

**6.0** De Novato a Profissional: Navegando pelo Mundo da Carteira Bitcoin

**6.1** O Processo de Integração e Segurança da sua bitcoin

**6.1.1** Exercício em Sala de Aula: Dominando a Autocustódia e Usando Sua Carteira com Confiança

**6.1.2** Exercício em Sala de Aula: Como Receber bitcoin (em detalhes)

**6.1.3** Exercício em Sala de Aula: Como Enviar bitcoin e Pagar por Bens e Serviços (em detalhes)

**6.2** On-Chain vs. Off-Chain

**6.3** A Lightning Network

**6.3.1** Uma Transação Lightning

**6.3.2** Exercício em Sala de Aula: Corrida de Revezamento de Carteiras Lightning

**6.3.3** Exercício em Sala de Aula: Demonstração Interativa Online da Lightning

# Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras

## 6.0 De Novato a Profissional: Navegando pelo Mundo da Carteira de Bitcoin

Quando os Sats são comprados pela primeira vez, eles serão creditados em uma conta virtual, semelhante à forma como os fundos são depositados em uma conta bancária.



A diferença fundamental é que, enquanto uma conta bancária é centralizada e está sujeita a regulamentações governamentais, uma **carteira de Bitcoin** é descentralizada e opera em uma rede **ponto a ponto**.

- O **Bitcoin** não possui um ponto central de falha, mas é importante ter cautela, pois os **bitcoins** de alguém podem estar nas mãos de terceiros que os estão gerenciando.

• Esta conta virtual, frequentemente chamada de “carteira”, é protegida por uma **chave privada mestra**, assim como uma conta bancária é protegida por um PIN pessoal ou senha. Assim como você tem controle sobre os fundos em sua conta bancária, você pode controlar os Sats em sua carteira e usá-los para fazer compras ou transferi-los para outras contas.

• Assim como um chaveiro pode criar qualquer número de chaves que podem ser usadas para abrir fechaduras, uma **frase de recuperação ou backup** (ou chave privada mestra) pode ser usada para gerar qualquer número de **chaves privadas** que podem ser usadas para acessar sua carteira de Bitcoin. Pode-se dizer que uma **frase de recuperação** é como um chaveiro, e as **chaves privadas** são as chaves criadas pelo chaveiro.

12-Word Backup Phrase	PRIVATE KEYS
dog cat human elephant bird dolphin snake rat snail zebra leopard ant	Bitcoin 8u924fua9x9vz9e...
	Litecoin f7ag9vc89x7as9d...
	Ethereum 54as76d5f7aos8fe...
	DASH 54as76d5f7aos8fe...
	Decred 87f298f7987dsf24f...



Esta tabela inclui os dois principais tipos de carteiras de bitcoin, **auto custodial** e **custodial**. Você pode ver os benefícios e riscos de usar cada tipo de carteira e quem controla o bitcoin em cada caso. Auto custodial significa que o usuário possui as **chaves privadas**, o que significa que eles estão verdadeiramente em posse de seu bitcoin, enquanto no segundo tipo, um terceiro as possui.

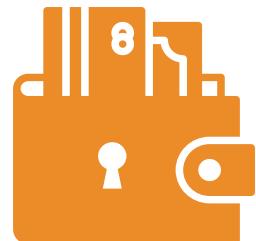
Tipo de Carteira	Quem controla meus bitcoins?	Benefícios	Riscos
<b>Carteiras auto custodiadas</b>	O usuário	Controle total sobre os fundos e transações, sem processo de aprovação ou congelamento de conta, sem controle corporativo ou governamental, proteção contra confisco arbitrário, como manter dinheiro em casa.	Sem recuperação possível se a frase de recuperação for perdida, suporte ao cliente limitado, toda a responsabilidade recai sobre o usuário.
<b>Carteiras custodiadas</b>	O provedor de terceiros	Recuperação fácil em caso de perda de acesso, suporte ao cliente mais fácil.	Os fundos estão sempre conectados à internet, o que os torna mais vulneráveis a ataques de hackers e violações de segurança.



## Capítulo #6

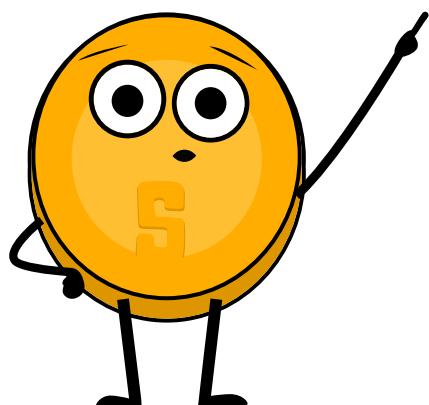
Em uma **carteira de auto custódia** (também chamada de **carteira não custodial**) você é o único com as **chaves** da carteira e **tem controle total sobre o que entra e sai**. Por outro lado, em uma carteira custodial, outra pessoa detém a chave e pode acessar e gerenciar o conteúdo da carteira em seu nome.

- A auto custódia é como ser seu próprio banco. As **transações** não estão sujeitas a controle ou autoridade de qualquer governo ou empresa, mas também significa que você assume total responsabilidade por manter seu **bitcoin** seguro.
- A auto custódia garante que terceiros não possam confiscar seu **bitcoin** sem o seu consentimento.
- A auto custódia oferece tranquilidade em tempos de incerteza, sabendo que seu **bitcoin** está seguro.



É importante escolher o tipo certo de carteira para atender às necessidades individuais de cada pessoa. Às vezes, as pessoas têm dificuldade em distinguir se estão instalando uma carteira custodial ou uma carteira de auto custódia. Esta tabela mostra as diferenças no processo de instalação.

Tipo de Carteira	Passo 1: Escolha uma carteira	Passo 2: Instale a carteira	Passo 3: Crie uma nova carteira	Passo 4: Proteja sua frase de recuperação	Passo 5: Comece a usar sua carteira
<b>Carteiras auto custodiadas</b>	Escolha um provedor de carteira auto custodial.	Siga as instruções do provedor de carteira.	Gere uma <b>frase de recuperação</b> e pelo menos uma <b>chave privada</b>	Guarde a <b>frase de recuperação</b> em um local seguro	Comece a usar a carteira para receber e enviar <b>bitcoin</b>
<b>Carteiras custodiadas</b>	Escolha um provedor de carteira custodial.	Siga as instruções do provedor de carteira.	Crie uma conta com o provedor de carteira.	N/A (o provedor de carteira detém as <b>chaves privadas</b> )	Comece a usar a carteira para receber e enviar <b>bitcoin</b>



Quando se trata de armazenar seus **bitcoin**, não se trata apenas de quem tem o controle sobre eles - há muitos outros riscos a serem considerados também. Por isso, é importante encontrar uma solução de armazenamento que seja ao mesmo tempo segura e conveniente.

# Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras

Tipo de Carteira	Descrição	Vantagens	Desvantagens	Exemplo de usuário
<b>Carteira Online</b>	Uma carteira que é acessada por meio de um navegador da web.	Acessível a partir de qualquer dispositivo com conexão à internet. Fácil de usar.	Menos seguro. Pode ser invadido ou comprometido.	Alguém que precisa acessar sua carteira com frequência e não possui muitos fundos para armazenar.
<b>Carteira Mobile</b>	Uma carteira instalada em um dispositivo móvel.	Conveniente. Pode ser acessada de qualquer lugar.	Pode ser perdida se o dispositivo for extraviado, roubado ou invadido.	Alguém que precisa fazer <b>transações</b> em movimento e não possui muitos fundos para armazenar.
<b>Carteira Desktop</b>	Uma carteira instalada em um computador desktop.	Mais seguro do que as carteiras online. Pode ser usado offline.	Pode ser invadido se o computador estiver infectado por malware.	Alguém que deseja armazenar uma grande quantidade de <b>bitcoins</b> e está confortável em usar um computador desktop.
<b>Hardware Wallet</b>	Um dispositivo físico que armazena <b>bitcoin</b> offline.	Muito seguro. Pode ser usado offline.	Os fundos podem se tornar irreparáveis se o dispositivo for perdido ou roubado.	Alguém que deseja armazenar uma grande quantidade de <b>bitcoins</b> e está disposto a pagar pela segurança adicional de uma carteira de hardware.
<b>Paper Wallet</b>	Um registro físico das chaves privadas e públicas de uma carteira de bitcoin.	Muito seguro. Pode ser usado offline.	Pode ser perdido ou roubado se o registro físico for perdido ou roubado.	Alguém que deseja armazenar uma grande quantidade de <b>bitcoins</b> e está disposto a tomar as precauções adicionais para garantir sua segurança.

Analizar as compensações das carteiras e entender que não há uma carteira ideal que atenda a todas as necessidades.

- Ao escolher uma carteira de bitcoin, existem várias coisas que você deve considerar:
- **Segurança:** Certifique-se de que a carteira possui medidas de segurança sólidas, como autenticação de dois fatores e políticas de senha seguras.
- **Privacidade:** Considere se a carteira permite que você permaneça anônimo ou se requer informações pessoais para configurar uma conta.
- **Facilidade de Uso:** Escolha uma carteira que seja fácil de usar e navegar, especialmente se você é novo no uso de **bitcoin**.
- **Compatibilidade:** Verifique se a carteira é compatível com seu dispositivo e sistema operacional.
- **Taxas:** Compare as taxas cobradas por diferentes carteiras para garantir que você esteja obtendo a melhor oferta.



- **Reputação:** Pesquise a reputação da carteira e de sua equipe para garantir que seja confiável.
- **Controle:** Algumas carteiras oferecem mais controle sobre suas chaves privadas, o que pode ser uma vantagem em termos de segurança. Considere se você deseja uma carteira que lhe dê controle total ou uma que seja mais amigável ao usuário, mas possa ter menos controle.

Você sempre pode transferir seus fundos para uma carteira diferente posteriormente.

## 6.1 O Processo de Onboarding e Segurança do Seu **bitcoin**



Onboarding no **Bitcoin** se refere ao processo de adquirir e usar **bitcoin**.

Antes de prosseguirmos, é importante que aprendamos os passos para o **onboarding** e nos familiarizemos com o processo de **comprar** e **guardar bitcoin** com segurança.

- 1. Escolha uma exchange ou corretora de bitcoin:** Existem várias plataformas diferentes que permitem comprar e vender **bitcoin**. Escolha uma plataforma que atenda às suas necessidades e seja confiável.
- 2. Crie uma conta:** Siga as instruções da plataforma para criar uma nova conta. Isso pode envolver fornecer informações pessoais e verificar sua identidade.
- 3. Conecte um método de pagamento:** A maioria das plataformas permite conectar uma conta bancária, cartão de crédito ou cartão de débito para financiar sua conta. Siga as instruções da plataforma para adicionar seu método de pagamento.
- 4. Faça um pedido:** Depois de configurar e financiar sua conta, você pode fazer um pedido para comprar **bitcoin**. A plataforma fornecerá uma cotação de preço e você poderá especificar a quantidade de **bitcoin** que deseja comprar.
- 5. Confirme a transação:** Revise os detalhes da **transação** e **confirme a compra**. A plataforma processará a **transação** e o **bitcoin** será transferido para sua conta na plataforma.
- 6. Saque o bitcoin:** Se você deseja transferir o bitcoin para uma carteira de auto-custódia, precisará sacar o **bitcoin** da plataforma e enviá-lo para sua carteira. A plataforma fornecerá instruções de como fazer isso.

*"Não são suas chaves, não são suas moedas"*

Esta é uma expressão popular entre os detentores de **bitcoin**. Ela se refere à ideia de que se você não tem controle direto sobre as chaves privadas associadas à sua carteira de bitcoin, você não possui a verdadeira propriedade das moedas.

A **chave privada** é um código secreto que permite acessar e gastar seus **bitcoins**. Quando você armazena seus **bitcoins** em um serviço de terceiros, como uma exchange ou carteira online, você

# **Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras**

está confiando nesse serviço para manter sua chave privada segura. Se o serviço for invadido ou encerrar suas atividades, você pode perder o acesso aos seus **bitcoins**.

Portanto, a expressão “**Not your keys, not your coins**” é um lembrete de que é importante assumir o controle de suas próprias **chaves privadas** e armazená-las de forma segura. Ao fazer isso, você pode garantir que tenha controle total sobre seus **bitcoins** e possa acessá-los quando desejar.



## ***6.1.1 Exercício em sala de aula: Dominando a Autocustódia e Usando sua Carteira com Confiança***

Se os alunos não tiverem celulares, o professor fornecerá um para cada aluno emprestar. Existem duas opções para essa atividade:

**Exercício em Classe. Opção 1. Baixe uma nova carteira.** Guie os estudantes passo a passo:

**Como criar e usar uma carteira de bitcoin.**

- 1.** Procure o aplicativo na App Store (iOS) ou Google Play Store (Android).
- 2.** Abra o aplicativo e digite sua **frase de recuperação** de 12 ou 24 palavras.  
**Certifique-se de anotá-la.** Mantenha-a em um local seguro. Lembre-se de que se você perder ou esquecer essa sequência de palavras, não poderá acessar seus bitcoins se perder o acesso à sua carteira.
- 3.** Em seguida, você deve **confirmar** se realmente salvou sua frase de recuperação ou **seed phrase**. Para fazer isso, você deve **digitar**, na mesma ordem, as **palavras** da sua seed phrase.
- 4.** Como medida adicional de segurança, algumas carteiras permitem que você **escolha** uma senha segura.
  - Sua **chave privada** e primeiro endereço de bitcoin são criados automaticamente pela sua carteira.
- 5.** Use seu endereço de “**receber**” para receber **bitcoin**.  
**Transfira bitcoin para sua carteira.**
  - Com uma carteira de autocustódia, nem sempre é possível comprar **bitcoin** diretamente com moeda fiduciária, então você pode precisar comprá-los e transferi-los de uma exchange primeiro.

**Exercício em sala de aula. Opção 2. Restaurar Carteira (Tempo Limitado).**

**Baixe** uma carteira de bitcoin e adicione alguns sats para cada aluno. Dê a cada aluno uma folha com uma seed phrase para recuperar uma carteira. Guie os alunos passo a passo:



- 1.** Quando você abrir sua carteira pela primeira vez, verá três métodos de criação de carteira. Toque em **[Importar uma carteira existente]**
  - Você verá uma tela de introdução, toque em **[Restaurar com frase de recuperação]**
- 2.** Digite sua frase de recuperação de 12/18/24 palavras uma por uma, na ordem correta.
- 3.** Toque em **[Restaurar/Restaurar]** quando terminar.
- 4.** Você verá um modo “Importação Bem-sucedida” quando sua carteira tiver sido importada com sucesso.

#### *6.1.2 Exercício em sala: Como Receber Bitcoin (detalhadamente)*

Para receber **bitcoin**, você precisará fornecer ao remetente o **endereço** da sua carteira de bitcoin. Esse é um conjunto único de letras e números que representa sua carteira e é usado para identificá-la na **Rede Bitcoin**. Você pode encontrar o **endereço** da sua carteira acessando sua carteira de bitcoin e procurando por uma opção de “Receber” ou “Depositar” **bitcoin**.

Em seguida, você pode compartilhar o **endereço** de bitcoin com o remetente de várias maneiras:

- **Copiar e colar o endereço:** Você pode copiar o **endereço** destacando-o e pressionando “Copiar” no seu teclado e, em seguida, colá-lo em um e-mail ou mensagem para o remetente.
- **Compartilhar um link para sua carteira de bitcoin:** Algumas carteiras de bitcoin permitem que você crie um link para sua carteira que você pode compartilhar com o remetente. Eles podem clicar no link para acessar sua carteira e enviar o bitcoin.
- **Compartilhar um código QR:** Se o remetente tiver um smartphone com um aplicativo de carteira de bitcoin, eles podem escanear o código QR para obter o **endereço** do seu bitcoin.

Depois que o remetente tiver o endereço do seu bitcoin, eles podem enviar o **bitcoin** para você, digitando seu endereço e a quantidade que desejam enviar e iniciando a **transação**. O **bitcoin** será então enviado para sua carteira e ficará visível assim que a **transação** for confirmada na **Rede Bitcoin**. Isso geralmente leva alguns minutos.

#### *6.1.3 Exercício em sala: Como Enviar bitcoin e Pagar por Bens e Serviços (detalhadamente)*

Para enviar **bitcoin**, você precisará de algumas coisas: uma carteira de bitcoin, o **endereço** de bitcoin do destinatário e a quantidade de **bitcoin** que deseja enviar.

- 1.** Abra sua carteira de bitcoin.
- Um código SMS será enviado para o seu número de telefone e você precisará inseri-lo na caixa de diálogo. Alternativamente, se você tiver ativado a autenticação em duas etapas do Google (Google 2FA), você precisará inserir o código de seis dígitos do aplicativo Google Authenticator.
- 2.** Acesse a opção “Enviar” ou “Retirar” e copie o endereço do destinatário.

# Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras

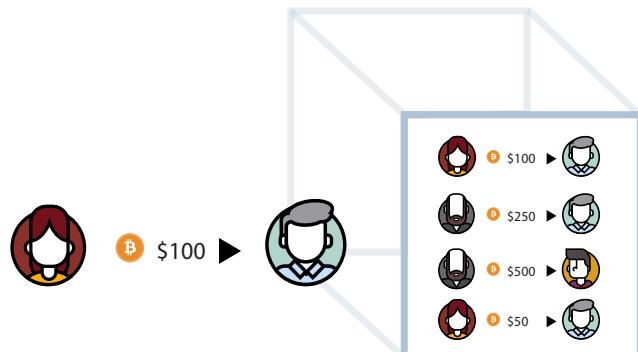
3. Cole o **endereço bitcoin** do destinatário no campo “Para”.
4. Insira a quantidade de **bitcoin** que deseja enviar no campo “Quantidade”.
5. Verifique novamente o **endereço** do destinatário e a quantidade a ser enviada.
6. Antes de clicar em **Confirmar e Enviar**, recomendamos que você verifique novamente os detalhes da **transação** para garantir que está enviando a quantidade correta de **bitcoin** para o endereço da carteira correto.
7. Confirme a **transação** e aguarde a confirmação da rede.
  - Vamos praticar!!! Vá até a cafeteria e **compre** lanches com **bitcoin**.

## 6.2 On-Chain vs. Off-Chain

É importante observar que nem todas as **transações** de **bitcoin** são registradas na **blockchain** principal do **Bitcoin**. Algumas redes utilizam **blockchains** diferentes chamadas sidechains para registrar **transações**.

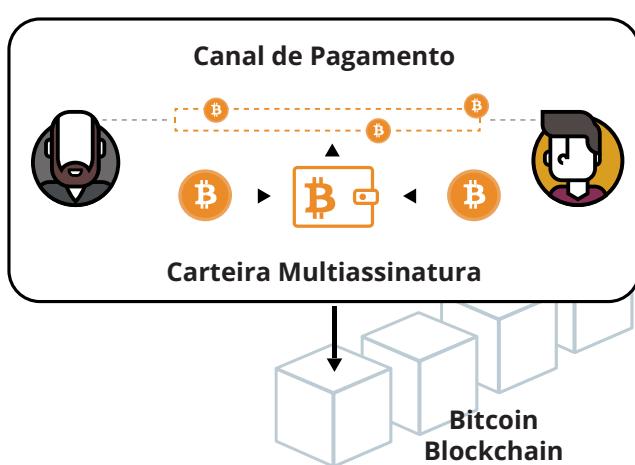
### Transações on-chain:

- Essas são **transações** que ocorrem diretamente na **blockchain** do **Bitcoin**.
- Elas levam cerca de 10 minutos para serem confirmadas e as taxas dependem do tamanho da **transação** em bytes.
- Elas são seguras, mas podem ser mais lentas.



### Transações off-chain (Rede Lightning):

- Essas **transações** ocorrem em uma rede separada construída sobre a **blockchain** do **Bitcoin**.
- Elas são liquidadas mais rapidamente e com taxas mais baixas.
- Elas são comumente usadas em locais onde as regulamentações e leis apoiam sua adoção e onde a velocidade e o custo das **transações** são mais importantes.
- Em comparação com as **transações** on-chain, elas são menos seguras.

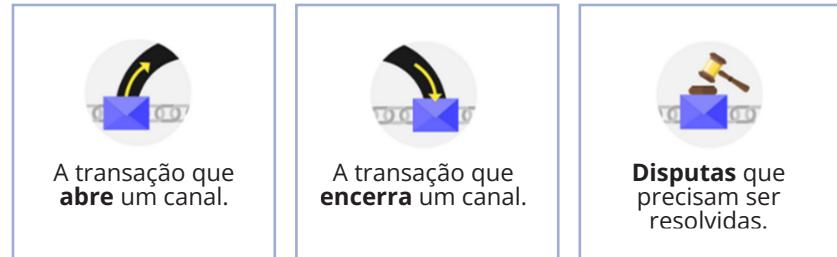




Se estiver utilizando a rede Lightning apenas **três tipos de transações** precisam ser transmitidas para a *blockchain*.

A **Rede Lightning** é uma **abordagem** de escalabilidade para o **Bitcoin**.

Trata-se realmente de mover muitas transações de **Bitcoin** para **fora da blockchain e para canais privados** entre usuários, mas ainda contando com a segurança da blockchain.



Rede de Pagamento	Bitcoin Network	Rede Lightning
<b>Definição</b>	Uma rede digital descentralizada que utiliza criptografia para garantir transações financeiras.	Um protocolo de pagamento de segunda camada que opera em cima da <i>blockchain</i> do <b>Bitcoin</b> , permitindo transações mais rápidas e baratas.
<b>Vantagens</b>	- Descentralizado e seguro - Sem chargebacks ou fraudes - Pode ser usado anonimamente - Aceitação global	- Transações mais rápidas e baratas - Maior escalabilidade - Transações fora da cadeia não congestionam a <i>blockchain</i>
<b>Desvantagens</b>	- Tempos de transação lentos - Altas taxas para certos tipos de transações - Complexo para iniciantes	- Requer confiança nos operadores de canal - Ainda experimental e não amplamente adotado - Requer transação on-chain para abrir e fechar canais

### 6.3 A **Rede Lightning**

O **Bitcoin** é conhecido por seu registro público imutável, mas pode não ser a melhor escolha para transações do dia a dia, como comprar café. O processo de transmitir essas transações para muitos nós e armazená-las em um banco de dados compartilhado pode ser lento e complicado. Para transações pessoais ou privadas, é melhor usar canais de pagamento ponto a ponto.

Uma solução melhor é uma abordagem em camadas para escalabilidade, como a combinação de **Bitcoin** e **Rede Lightning**. Isso permite que os usuários escolham a camada que atende às suas necessidades. O **Bitcoin** é uma moeda digital descentralizada, enquanto a **Rede Lightning** oferece pagamentos rápidos, baratos e confidenciais.

# Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras



A Rede Lightning é um sistema de pagamento que permite aos usuários enviar e receber pagamentos de forma rápida e econômica usando **bitcoin**. Funciona configurando uma carteira compartilhada onde ambas as partes armazenam seus **bitcoin**, e, em seguida, realizam transações ilimitadas entre si sem interagir com a **blockchain** principal. Ao concluir, o saldo final é registrado na **blockchain** principal.

A Rede Lightning opera como uma rede separada conectada à **blockchain** do **Bitcoin** e foi projetada para funcionar perfeitamente com o **Bitcoin**. O Taro, que é uma adição recente à **Lightning**, agora permite que a rede seja usada para outros tipos de ativos, como stablecoins, permitindo que os usuários realizem pagamentos quase instantâneos e de baixo custo em uma moeda vinculada ao fiat tradicional, como o dólar americano. Os pagamentos podem ser feitos diretamente ao destinatário, contornando intermediários, e convertendo o pagamento para a moeda original antes de chegar à loja.

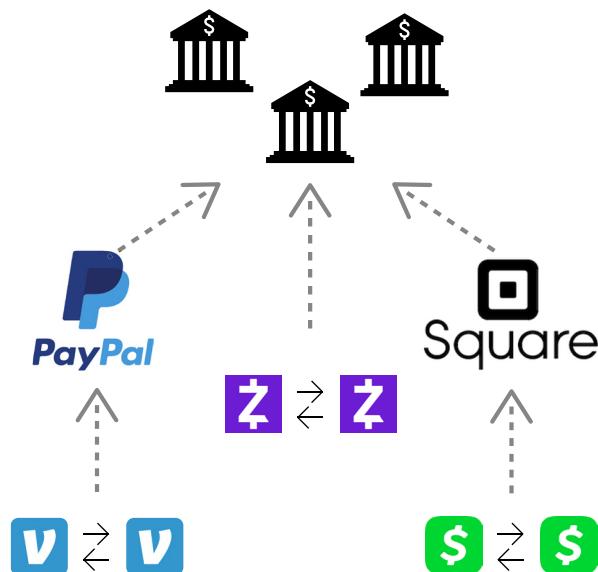
O uso de stablecoins na **Rede Lightning** para transações internacionais, como remessas, oferece várias vantagens:

**1. Redução de custos:** As transações transfronteiriças podem ser caras devido às taxas cobradas por bancos ou outros intermediários. Ao usar stablecoins na Rede Lightning, essas taxas podem ser reduzidas ou eliminadas, tornando os pagamentos transfronteiriços mais acessíveis.

**2. Aumento da velocidade:** As transações transfronteiriças podem levar vários dias para serem concluídas quando se utiliza métodos

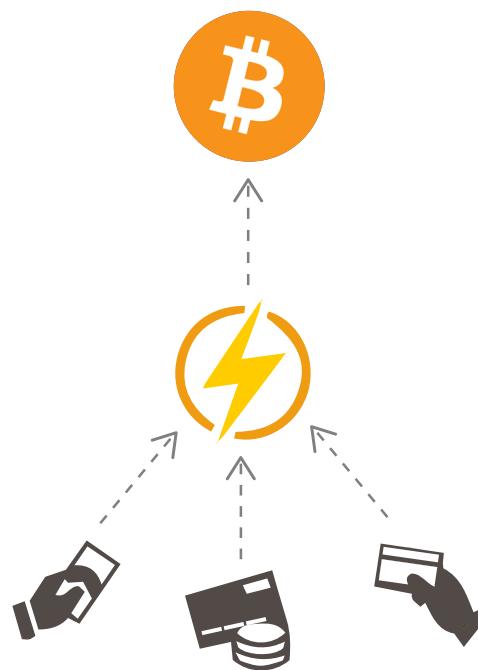
## Sistema Monetário Moderno = Redes Fechadas

Bancos Mantêm a Finalidade



## Sistema Monetário do Bitcoin = Rede Aberta

O Bitcoin Mantém a Finalidade



A **Rede Lightning** oferece os benefícios das carteiras digitais, como o Apple Pay, sem a volatilidade de preço associada ao **bitcoin**.



tradicionais. Ao usar stablecoins na **Rede Lightning**, as **transações** internacionais podem ser processadas rapidamente, reduzindo o tempo necessário para concluir a **transação**.

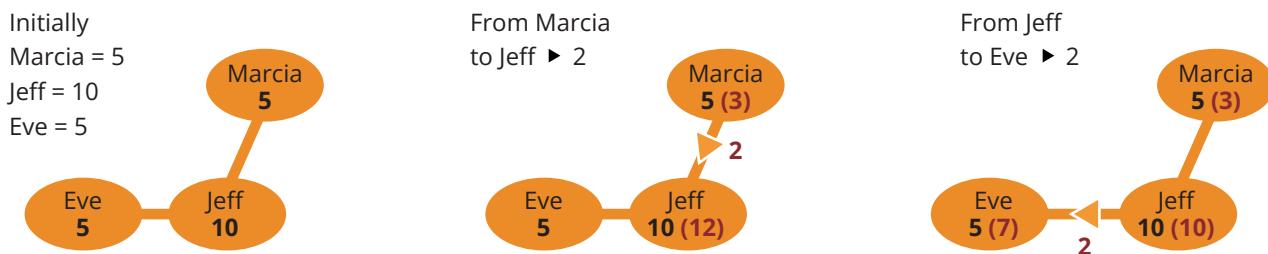
**3. Melhoria no acesso:** Para pessoas físicas ou empresas em países com acesso limitado a serviços bancários tradicionais, o uso de stablecoins na **Rede Lightning** pode fornecer um meio de realizar pagamentos internacionais, melhorando assim o acesso a serviços financeiros.

### 6.3.1 Uma **Transação Lightning**

#### ► Exemplo#1

- A seguir, Marcia possui 5 unidades de uma determinada moeda e Eve também possui 5 unidades. Marcia deseja enviar 2 de suas unidades para Eve, então ela envia 2 unidades para Jeff. Jeff, então, repassa as 2 unidades para Eve, que agora possui 7 unidades. Marcia agora tem 3 unidades. E é isso! A **transação** está concluída.

O ponto-chave aqui é que Marcia e Eve não precisam passar por um banco ou outro intermediário para realizar a **transação**.



- Jeff age como um intermediário ou um “**terceiro confiável**” nesse cenário, onde Marcia e Eve não confiam diretamente uma na outra. Jeff recebe as 2 unidades de Marcia e depois as repassa para Eve, concluindo assim a **transação**. Ao usar Jeff como intermediário, Marcia e Eve podem concluir a **transação** sem a necessidade de um banco ou outra instituição centralizada, o que pode tornar a **transação** mais rápida, mais barata e mais segura. Jeff é um elemento-chave nesse processo de **transação** peer-to-peer.

Como operador de nó em uma **transação** da **Rede Lightning**, Jeff se beneficia de várias maneiras:

- 1. Taxas de transação:** Jeff recebe uma pequena taxa por cada **transação** que passa por seu nó, o que o compensa pelo tempo e esforço dedicados à manutenção e operação de seu nó.
- 2. Participação na rede:** Ao executar um nó **Lightning**, Jeff está participando da rede e ajudando a aumentar sua descentralização, segurança e estabilidade. Isso pode aumentar a reputação e a credibilidade de Jeff como um operador de nó confiável, tornando-o um intermediário mais atraente para **transações** futuras.

# Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras

**3. Crescimento da rede:** À medida que a **Rede Lightning** cresce e mais pessoas a utilizam, é provável que o número de **transações** que passam pelo nó de Jeff aumente, o que pode resultar em um aumento de receita proveniente das **taxas de transação**.

**4. Aumento da segurança da rede:** O papel de Jeff como intermediário ajuda a aumentar a segurança da rede, adicionando uma camada adicional de proteção entre Marcia e Eve. Isso pode aumentar a confiança dos usuários na rede, tornando-a mais atraente para novos usuários e ajudando a impulsionar o crescimento.

Em geral, ser um operador de nó na **Rede Lightning** pode fornecer a Jeff uma fonte estável de renda, além da oportunidade de contribuir para o crescimento e desenvolvimento da rede.

Resumindo, as **transações** on-chain são mais lentas, porém mais seguras, enquanto as **transações off-chain (Rede Lightning)** são mais rápidas, porém menos seguras. Você deve considerar o equilíbrio entre segurança e velocidade, dependendo das suas necessidades.

## ► Exemplo#2

Mina tem um amor sério pelo McDonald's. Ela vai lá para o café da manhã, almoço e jantar todos os dias! Mas com tantas opções de pagamento disponíveis, ela não tem certeza de qual é a melhor escolha. Felizmente, ela aprendeu um pouco sobre o **Bitcoin** e a **Rede Lightning**. Depois de comparar as tabelas abaixo, Mina não tem dúvida de que usar um método de pagamento **Lightning** é o caminho certo a seguir.

Benefícios	Lightning	Sistema Bancário Tradicional
<b>Velocidade</b>	Rápida	Lenta
<b>Transparência</b>	Transparente	Opaco
<b>Segurança</b>	Seguro	Vulnerável
<b>Taxas de Transação</b>	Baixa	Alta
<b>Inclusão Financeira</b>	Alta	Limitada

Benefícios	Lightning	On-Chain
<b>Escalabilidade</b>	Alta	Baixa
<b>Privacidade</b>	Alta	Moderada
<b>Interoperabilidade</b>	Alta	Baixa
<b>Conformidade Legal</b>	Moderada	Alta
<b>Eficiência de custos</b>	Alta	Moderada

**Visa, Inc.**

Em média, 1.700 transações por segundo.



Capacidade de 65.000 transações por segundo.

**Bitcoin On-chain**



Capacidade de 7 transações por segundo.

**Bitcoin  
Rede Lightning**



Milhões de transações por segundo.



Mina também é fã de **transações** rápidas, seguras e com custo efetivo, então ela decidiu usar a **Lightning** para suas compras no McDonald's. Com a **Lightning**, ela pode desfrutar ainda mais de suas refeições sabendo que seus pagamentos são processados instantaneamente, de forma segura e com baixas taxas. Além disso, como a **Rede Lightning** oferece inclusão financeira, Mina agora pode pagar por suas refeições mesmo se estiver em uma área remota em El Salvador.

Para começar com a **Lightning**, Mina primeiro faz o download de uma carteira **Lightning** em seu celular. Em seguida, ela financia sua carteira **Lightning** enviando alguns bitcoins de sua carteira de bitcoin regular para sua nova carteira **Lightning**. Esse processo é chamado de “financiamento da carteira” ou “financiamento de um canal de pagamento”. Mina pode financiar sua carteira com qualquer quantidade de bitcoin com a qual se sinta confortável, mas é importante observar que a quantidade de bitcoin que ela bloqueia em sua carteira **Lightning** não pode ser usada em suas **transações** on-chain.

Uma vez que sua carteira **Lightning** está financiada, ela pode usá-la para fazer pagamentos no McDonald's. O McDonald's possui um nó **Lightning**, então Mina pode abrir um canal de pagamento com eles enviando alguns de seus bitcoins de sua carteira **Lightning** para um endereço específico fornecido pelo McDonald's. Isso move seus **bitcoins** da blockchain do Bitcoin para uma **transação** off-chain na **Rede Lightning**.



Com o canal de pagamento aberto, Mina agora pode fazer compras no McDonald's sem precisar abrir um novo canal ou pagar altas taxas a cada vez. O canal permanece aberto enquanto Mina e o McDonald's desejarem usá-lo. Por exemplo, se Mina compra um hambúrguer por 0,0005 **bitcoin**, o canal registra que Mina agora tem 0.9995 **bitcoin**. E se ela compra um milkshake por 0.0003 **bitcoin** no dia seguinte, o canal registra que Mina agora tem 0.9992 **bitcoin**.

Quando Mina decide que deseja usar seu saldo de **bitcoin** para outra finalidade, ela fecha o canal ao transmitir uma **transação** de fechamento para a **blockchain** do **Bitcoin**. Isso é feito iniciando uma **transação** de fechamento em sua carteira **Lightning**, e a **transação** contém o saldo final do canal acordado por ambas as partes. A **transação** é então transmitida para a **blockchain** do **Bitcoin** e confirmada por um minerador. Uma vez que a **transação** é confirmada, o canal é fechado e o **bitcoin** restante no canal será devolvido a Mina e ao McDonald's.

É importante observar que o fechamento de um canal pode levar algum tempo para ser confirmado na **blockchain**. Durante esse período de espera, os fundos ainda estão bloqueados no canal e não podem ser usados para **transações** on-chain. Mina receberá uma notificação assim que a **transação** de fechamento for confirmada.

# **Carteiras de Bitcoin: Navegando na Autocustódia e na Lightning Network para Transações Seguras**

## **6.3.2 Exercício em Sala: Revezamento de Carteira Lightning**

- 1.** Primeiro, você precisará baixar uma carteira Lightning em seu telefone ou computador. Existem várias opções para escolher, incluindo Muun, Blue Wallet, Bitcoin Beach Wallet e Eclair para telefones celulares, e Lightning App e Zap para computadores desktop.
- 2.** Siga as instruções para instalar a carteira em seu dispositivo. Isso pode envolver baixar o aplicativo da App Store ou Google Play, ou baixar e instalar o software do site da carteira.
- 3.** Uma vez que a carteira estiver instalada, abra-a e siga as instruções para configurá-la. Isso pode envolver a criação de uma nova carteira ou a restauração de uma existente, e a proteção com uma senha ou outra forma de autenticação.
- 4.** Certifique-se de ter uma maneira de receber satoshis. Isso pode envolver fornecer à sua carteira um endereço de recebimento, ou escanear um código QR fornecido pelo seu professor ou outro membro do seu grupo.
- 5.** Quando sua carteira estiver configurada e você estiver pronto para receber satoshis, seu professor dará a você e ao seu grupo uma quantidade inicial de satoshis enviando-os diretamente para sua carteira.
  - A.** O objetivo do seu grupo é passar os satoshis de uma carteira para outra, usando a **Rede Lightning**, até que eles cheguem à última pessoa do grupo.
  - B.** Para enviar satoshis para outra pessoa, abra sua carteira e siga as instruções para fazer um pagamento. Você precisará fornecer o endereço da carteira do destinatário ou escanear um código QR, e digitar a quantidade de satoshis que deseja enviar.
  - C.** Se o seu grupo for o primeiro a enviar com sucesso os satoshis para a última pessoa, vocês ganham! (E ficam com os sats e alguns doces.)

**Exercício em Sala.** Comece explorando um dos sites interativos fornecidos pelo professor. Em seguida, siga as instruções na próxima página.

- <https://lnrouter.app/graph/zero-base-fee>
- <https://www.robtex.com/lneulator.html?conf=A5-5B,B5-5C&send=A2C>





### 6.3.3 Exercício em Sala: Demonstração Interativa Online do Lightning

- 1.** Concentre-se nos conceitos-chave discutidos em sala, incluindo canais de pagamento, rotas e taxas.
- 2.** Faça anotações de quaisquer perguntas ou dificuldades que você encontrar ao explorar o site.
- 3.** Trabalhe com seu grupo para compartilhar suas descobertas e discutir quaisquer perguntas ou dificuldades com a turma.
- 4.** Esteja preparado para participar de discussões em sala sobre a Rede Lightning e seu potencial como solução de escala para transações de bitcoin.



## *Capítulo #7*

# *Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs*

**7.0** Colocando a Questão do Gasto Duplo para Descansar: Compreendendo a Solução do Bitcoin

**7.1** Rastreando a Jornada da sua Moeda

**7.2** Segurança e Sigilo

**7.3** A “Mempool” ou Pool de Memória: Compreendendo o Reservatório de Transações do Bitcoin

**7.3.1** Exercício em Sala: Em Espera: Examinando as Transações Não Confirmadas da Rede Bitcoin

**7.4** Por Trás dos Blocos: O Mistério da Programação do Bitcoin

**7.4.1** Uma Exploração Técnica das Transações do Bitcoin

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

0000110011100010100010101010110010001010100110011000011101000101000111110  
011010111100100110110001100101110010011010011100010100100110110111010001100101  
101010001101100000101110101000100011100000000111010110111100001010110011110010  
1010000101000011

Você vê aquela longa sequência de uns e zeros lá em cima? Isso é chamado de número aleatório e, se o convertermos para o nosso sistema decimal regular, ele se torna um número com mais de 70 dígitos, o que é ainda mais átomos do que existem em nosso universo! Mas podemos usar um sistema diferente para representar esse número de forma mais curta, e chamamos de **chave privada**.

Algo realmente legal sobre esta **chave privada** em particular é que ela é única, o que significa que nunca foi usada antes e nunca aparecerá novamente uma vez que você saia desta página ou gere uma nova. É como jogar 256 moedas seguidas e obter o mesmo resultado duas vezes - impossível!

A segurança do **Bitcoin** depende dessa **chave privada** ser privada e difícil de ser adivinhada. Se outra pessoa colocar as mãos nela, ou se você a perder, perderá todo o seu dinheiro para sempre. Então, mantenha-a em segurança!



Mas como o **Bitcoin** realmente funciona? Assista ao vídeo a seguir para entender melhor.



Até agora, aprendemos sobre a história do dinheiro e a ideia revolucionária da tecnologia **blockchain**, e exploramos os conceitos básicos do **Bitcoin** - a primeira moeda digital descentralizada do mundo. Mas como o **Bitcoin** evita fraudes e garante que as pessoas não possam **gastar o mesmo dinheiro duas vezes?**

A verdade é que, quando você envia alguns **bitcoins** para outra pessoa, você precisa dizer "sim, eu aprovo isso" com sua **chave privada**. Em seguida, a rede verifica se está tudo certo e confirma que a **transação** é legítima antes de enviar os **bitcoins**.

Sign a transaction  
Transaction + Private Key -> Signature

Transaction

Me → Dalia 3

Public Key: b47c062afef30a2297 ...

Your Private Key

dfdbd55a1e6edaab10e57df84ced5d3231d7ae2667ab5e14c69ae8a44557c5

Digital Signature

304402206e3cd262c156ee1983190fa6e0d5dfeb1e0f281253a958c4a8  
905f85320414e022033e747a84e717585c9a0a533e7d56339017497b02  
6bd79b582b6a8e26b73769fc

Sign transaction with your Private Key

Verify a transaction  
Transaction + Signature + Public Key -> Valid?

Transaction

Me → Dalia 3 BTC

Public Key: b47c062afef30a2297 ...

Digital Signature

304402206e3cd262c156ee1983190fa6e0d5dfeb1e0f281253a958c4a8  
c4a8905f85320414e022033e747a84e717585c9a0a533e7d56339017497b02  
7497b026bd79b582b6a8e26b73769fc

Public Key

b47c062afef30a229704c3bbe34a5ac9363c962f6add47c692b1ff26323877

Verify signature with Public Key



É aí que a magia dos **UTXOs**, **criptografia de chave pública**, **hashing**, **scripting**, e o **mempool** entram em jogo. Assim como uma impressão digital garante que ninguém mais possa usar sua identidade, os **hashes** no **Bitcoin** garantem que as **transações** não possam ser alteradas. Os **Scripts** são como as regras de um jogo, garantindo que as **transações** sigam condições específicas. Os **UTXOs** são como os blocos de construção de um quebra-cabeça, mantendo o controle de todo o dinheiro em sua carteira virtual. E o **mempool** funciona como uma área de espera, garantindo que todas as **transações** sejam verificadas antes de serem adicionadas ao **blockchain**. Então, vamos mergulhar e descobrir como o **Bitcoin** resolve o **problema de gasto duplo** e garante a integridade de cada **transação** em sua rede.

## 7.0 Colocando o Problema de Duplo Gasto para Descansar: Entendendo a Solução do Bitcoin

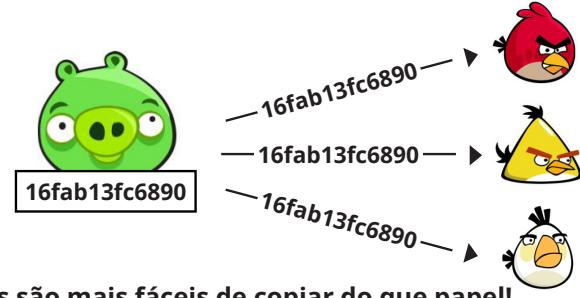
Lembre-me, qual é o “problema de gasto duplo”?

As **chaves privadas**, **públicas** e as **transações** de **bitcoin**, como já vimos, são representadas por uma série de números e letras aleatórios que podem ser visualizados em qualquer dispositivo com acesso à internet.



Além disso, grande parte das informações relacionadas a essas transações é normalmente comunicada usando um sistema de notação numérica conhecido como **números hexadecimais**.

Gasto duplo ...



Bits são mais fáceis de copiar do que papel!

Isso significa que é comum ver sequências de números hexadecimais de 64 caracteres, compostas por letras (A-F) e números (0-9), como:

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

Então, como realmente impedimos alguém de copiar e colar seu bitcoin e gastá-lo várias vezes, como eles fariam com um e-mail ou foto?

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16.  
f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16.

Como chegamos a um consenso sobre quem possui qual dinheiro sem uma autoridade central?

**Hashing** e código. Vamos explicar.

Imagine que você tem 1 **bitcoin** e quer enviá-lo como presente de aniversário para seu amigo.

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

Você envia o **bitcoin** para o **endereço**, do seu amigo, mas então percebe que deve dinheiro ao seu ex-namorado e deveria ter enviado o **bitcoin** para ele em vez disso. Em um momento de pânico, você decide ser esperto(a) e criar uma nova transação para enviar o mesmo 1 **bitcoin** para o seu ex-namorado. Isso é o que chamamos de “**double spend**” (**gasto duplo**).

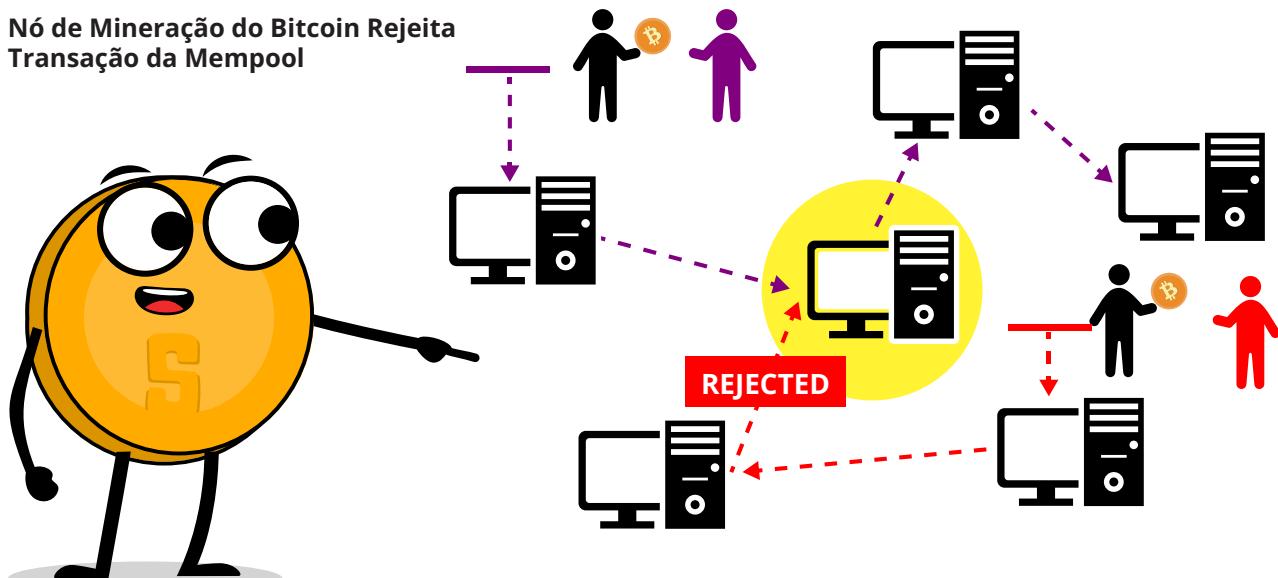
Mas espere, como a rede impede que isso aconteça? É simples. Os nós na rede detectam **transações** conflitantes e permitem apenas que uma delas seja confirmada com base em um conjunto de regras conhecidas como “**regras de consenso**”. Nesse caso, é provável que a **transação** para o seu ex-namorado seja rejeitada, pois foi enviada após a **transação** original para seu amigo. No entanto, é apenas uma questão de sorte qual **transação** é escolhida primeiro por um minerador.

Graças à **blockchain**, todos na rede conseguem concordar com o estado atual do livro-razão. Isso ajuda a evitar o **double-spending** e a fraude, tornando-o um sistema seguro e confiável, assim como uma versão digital do “sistema de honra”. Então, da próxima vez que você enviar **bitcoin**, pode relaxar sabendo que a rede está te protegendo.

Então, como o **Bitcoin** realmente resolve isso? Bem, vamos descobrir.

• O **Bitcoin** evita o double spending ao implementar um mecanismo de confirmação e manter um livro-razão universal (**blockchain**).

- As **transações** são adicionadas à **blockchain** de forma cronologicamente ordenada e com registro de data e hora.
- Para evitar o double spending, apenas a primeira **transação** a receber confirmações suficientes (geralmente 6) é incluída na **blockchain**, enquanto as outras são descartadas.
- As **transações** na **blockchain** são irreversíveis e impossíveis de serem alteradas.





Quando qualquer **transação** é iniciada, qualquer **nó** pode verificá-la na rede em alguns passos simples:

1. Primeiro, o nó **verificará se a transação está corretamente assinada** pela **chave privada do remetente**, o que garante que a **transação** seja legítima e não tenha sido adulterada.
2. Em seguida, o nó **verificará se o remetente possui fundos suficientes** para concluir a **transação**. Isso é feito examinando o saldo do remetente no livro-razão da **blockchain**.
3. Por fim, o nó também validará as **entradas e saídas** da **transação**, verificando se as entradas gastos na **transação** não foram gastos em outra **transação** e se as saídas não excedem o fornecimento total.

Como veremos, a combinação de **criptografia de chave pública** e o sistema **UTXO** (Unspent Transaction Output) são usados no **Bitcoin** para verificar a autenticidade das **transações** e prevenir fraudes sem uma autoridade central. A **criptografia de chave pública** garante comunicação segura e transferências de fundos, enquanto o UTXO mantém um registro de todos os fundos na rede e previne gastos duplos.



**UTXO**, que significa “Unspent Transaction Output” (Saída de Transação Não Gasta), é simplesmente um registro de todos os fundos disponíveis na rede que ainda não foram gastos.

## 7.1 Rastreando a Jornada da sua Moeda

No **Bitcoin**, as **transações** funcionam como dividir uma nota grande em notas menores e entregá-las a pessoas diferentes. O troco que você recebe de uma **transação** é chamado de saída não gasta e pode ser usado como entrada para uma nova transação. As saídas nas **transações** do **Bitcoin** podem estar **gastas ou não gastas**, e as saídas não gastos são consideradas valiosas porque podem ser usadas em novas **transações**.

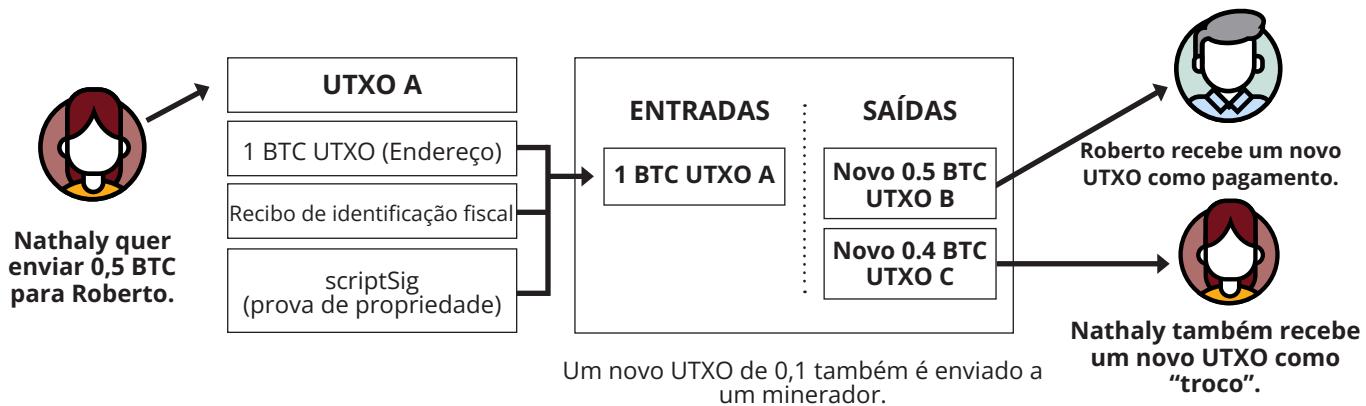
- Pense nisso como usar vários cartões-presente para pagar uma compra. Os cartões-presente de **transações** anteriores atuam como entradas, e o troco que você recebe é representado por um novo cartão-presente com o valor restante. Isso é semelhante à forma como as **transações** do **Bitcoin** funcionam com UTXOs.

### O que são UTXOs?

O saldo de uma carteira é a soma de todos os UTXOs de um usuário. Os UTXOs são usados para rastrear a propriedade do **bitcoin** na rede. Quando uma transação é feita, ela cria novos UTXOs, e quando uma transação é gasta, ela consome os UTXOs existentes.

- Os UTXOs são como moedas digitais no mundo do **Bitcoin**. É o troco que você recebe depois de gastar alguns **bitcoins**.

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs



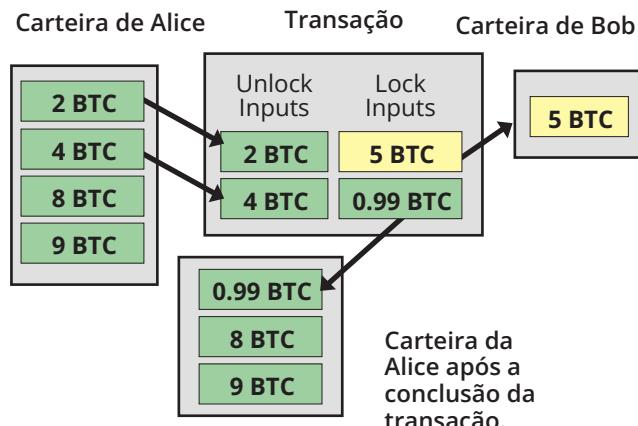
## Como funcionam os UTXOs nas transações de Bitcoin

Quando uma **transação** é feita, a quantidade de **bitcoin** que é enviada é dividida em várias saídas, cada uma associada a um endereço específico.

- Ao enviar **bitcoin** para alguém, você usará uma ou mais Unspent Transaction Outputs (UTXOs) como fonte dos fundos. Esses UTXOs serão combinados, se necessário, para criar uma nova saída que pertença ao destinatário da **transação**. Essa nova saída, ou UTXO, então se torna propriedade do destinatário e pode ser usada como fonte de fundos em uma **transação** futura. Essa cadeia de UTXOs cria um histórico transparente e rastreável de todas as transações de **bitcoin** na **blockchain**, a partir do primeiro bloco.

- Por exemplo, se alguém quer enviar 2 **bitcoins**, mas tem um UTXO no valor de 5 **bitcoins**, a diferença de 3 **bitcoins** é enviada de volta para o remetente como "troco". Esse troco é um novo UTXO para o remetente e pode ser gasto em uma **transação** futura.

- No exemplo, Alice envia 5 BTC para Bob, mantendo uma parte para si mesma. Ela combina 6 **bitcoins** de seus quatro UTXOs, totalizando 23 **bitcoins**, e envia 5 para Bob e 0,99 de volta para si mesma, com uma taxa de 0,01 para processamento. A **transação** é então adicionada à **blockchain**, atualizando todos os nós com uma cópia do registro de UTXO atualizado. Se Alice tentar enviar 23 BTC para Ximena em uma **transação** separada, os nós irão rejeitá-la, pois parte da saída já foi gasta.



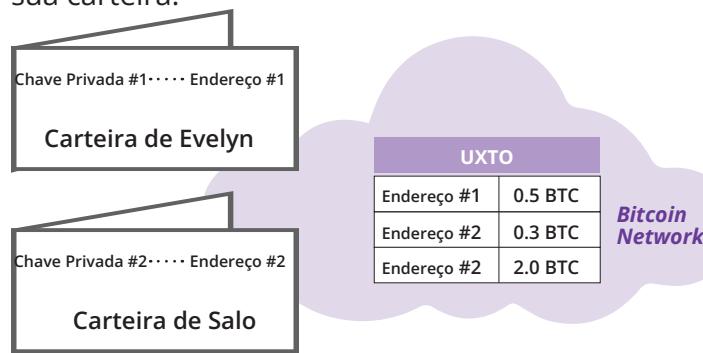
Se alguém tentasse usar uma saída de **transação** já gasta em sua **transação**, é provável que seja rejeitada pelos nós da rede. Isso ocorre porque esses nós mantêm uma cópia do mesmo conjunto de banco de dados e podem facilmente chegar a um consenso verificando o saldo de cada endereço antes de validar qualquer nova **transação**. Isso garante a integridade e validade das transações na rede.



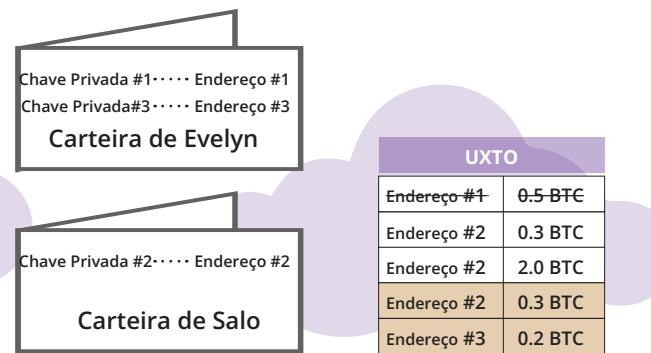
## Capítulo #7

Vamos dar uma olhada em outro exemplo:

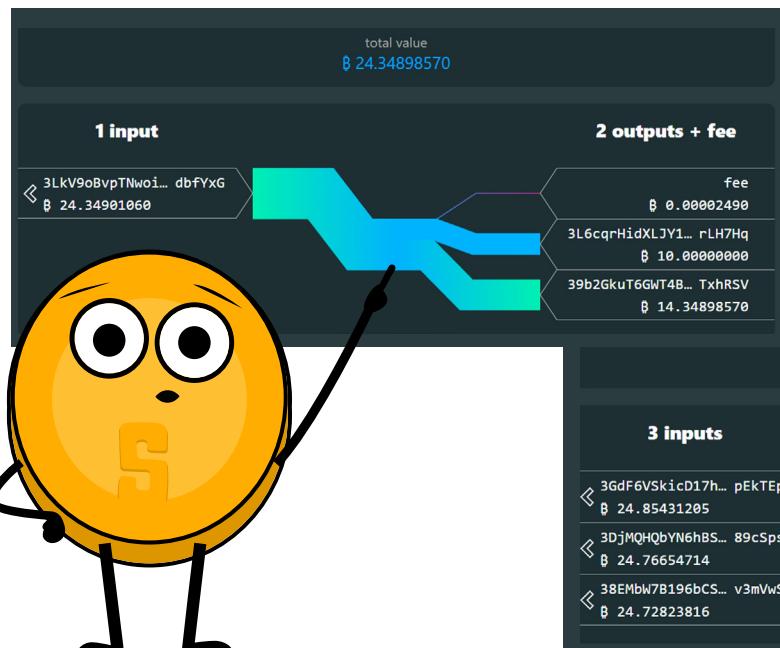
Apenas a pessoa que possui a **chave privada** de um **endereço** pode acessar os UTXOs armazenados nesse endereço. Por exemplo, se a Evelyn possui a **chave privada** para o **endereço** #1, ela verá 0.5 **bitcoin** em sua carteira. Se o Salo possui a **chave privada** para o **endereço** #2, ele verá 2.3 **bitcoin** em sua carteira.



Quando Evelyn envia 0.3 **bitcoin** para o Salo, sua carteira gera uma nova **chave privada** e endereço (#3). O UTXO original no **endereço** #1 é gasto e dois novos UTXOs são criados: um para o endereço do Salo com 0.3 **bitcoin** e outro para o novo **endereço** da Evelyn com 0.2 **bitcoin**. Após essa **transação** ser registrada no livro-razão, a carteira do Salo mostra 2,6 **bitcoin** e a carteira da Evelyn mostra 0.2 **bitcoin**.



Abaixo está uma captura de tela real de uma **transação** em que há apenas uma entrada. No entanto, em um caso mais geral, o saldo inicial pode ser a soma de vários UTXOs que uma pessoa acumulou de transações anteriores.



Quais observações podem ser feitas?  
Os inputs correspondem aos outputs?  
É possível descrever os detalhes da **transação**? Existe alguma conexão entre as duas capturas de tela? E qual **transação** ocorreu primeiro?

The screenshot shows a transaction with the following details:

- total value**: ฿ 74.34901060
- 3 inputs**: 3GdF6VSkicD17h... pEkTEp, ฿ 24.85431205; 3DjM0HQbYN6h8S... 89cSpS, ฿ 24.76654714; 38EMbw7B196bCS... v3mVws, ฿ 24.72823816
- 2 outputs + fee**:
  - fee: ฿ 0.00008675
  - 3LkV9oBvpTNwoi... dbfYxG, ฿ 24.34901060
  - bc1qqshu7uelwf... ajze6f, ฿ 50.00000000

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs



Geralmente, as **saídas gastas** são exibidas em vermelho e as **saídas não gastas** em verde. Essa codificação de cores fornece uma maneira visual de identificar rapidamente saídas gastas e não gastas, o que pode ser útil para rastrear **transações** e entender o fluxo de fundos em uma blockchain.

## 7.2 Segurança e Sigilo

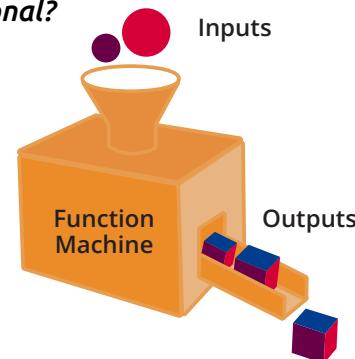
Por favor, não se intimide com os termos técnicos e conceitos matemáticos a seguir. Entendemos que nem todos são aficionados por matemática, mas você pode se surpreender e perceber que até mesmo as ideias mais complexas podem ser compreendidas com um pouco de esforço.

*O que é uma função, mais especificamente, o que é uma função unidirecional?*



Uma **função** é como uma máquina que recebe algumas informações e as transforma em algo novo. As informações que você fornece à função são chamadas de **entrada**. As novas informações criadas pela função são chamadas de **saída**. As funções ajudam os computadores a realizar tarefas e resolver problemas.

Pense nisso como uma receita para fazer uma salada. A receita (ou função) diz quais ingredientes usar e como misturá-los para fazer a salada. Você pode colocar ingredientes diferentes, mas a receita sempre resultará na salada como saída. As funções podem ser usadas para facilitar e tornar as coisas mais eficientes.



Essa receita, portanto, é uma **função** que recebe os **ingredientes** como **entrada** e gera a **salada mista** como **saída**.



No **Bitcoin**, **funções** são utilizadas para **executar transações**. Já sabemos que as **transações** no **Bitcoin** são essencialmente transferências de valor de um endereço para outro. Para realizar uma **transação**, várias funções criptográficas são utilizadas para validar a **transação** e atualizar o estado da blockchain do **Bitcoin**, que é um livro-razão descentralizado que registra todas as **transações**.

As funções usadas em uma **transação** de **Bitcoin** incluem verificar a autenticidade das entradas da **transação**, verificar se o remetente possui fundos suficientes e atualizar os saldos dos endereços relevantes. Uma vez que uma **transação** é verificada e adicionada à blockchain, ela se torna parte do registro permanente de todas as **transações** na rede.

- Uma **função unidirecional** utiliza um conjunto de instruções para processar as informações

e transformá-las em algo **novo**, assim como uma receita de smoothie transforma ingredientes em uma nova bebida. No entanto, assim como **não é possível desfazer a mistura de um smoothie** para obter os ingredientes originais de volta, **não é possível reverter uma função unidirecional para recuperar as informações originais**.



A **criptografia de chave pública**, da qual a **chave pública** é uma parte, depende do uso de **funções unidireccionais**, o que torna difícil determinar a **chave privada** a partir da **chave pública**. Não é exatamente “impossível” encontrar a chave privada a partir da **chave pública**, mas é extremamente difícil fazê-lo e demandaria uma quantidade desproporcional de tempo e poder computacional para realizar essa tarefa.

- Encontrar uma **chave privada** a partir de uma **chave pública** no **Bitcoin** é como tentar encontrar uma agulha em um palheiro do tamanho de um campo de futebol. A agulha representa a **chave privada** e o palheiro representa todas as possíveis **chaves privadas**.



Da mesma forma, as funções unidireccionais são projetadas para serem irreversíveis e não podem ser descriptografadas.

### O que é uma função de hash?



O **Hashing** é como uma impressão digital para dados digitais. É um processo de pegar uma mensagem digital e transformá-la em um código de comprimento fixo, que serve como um identificador único.

Assim como uma impressão digital pode identificar uma pessoa, um hash pode identificar uma mensagem digital. Hashes são usados em muitas aplicações, incluindo **transações** em **Bitcoin**.

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

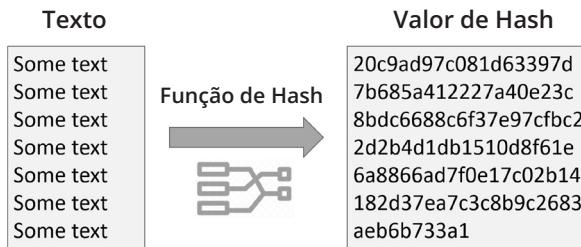
## Como o Hashing é usado em transações de Bitcoin

No **Bitcoin**, cada **transação** é hashada antes de ser adicionada à **blockchain**. O hash atua como uma assinatura para a **transação**, verificando se a **transação** é válida e não foi adulterada. Se alguém tentar alterar até mesmo uma única letra na **transação**, o hash será completamente diferente, alertando outros sobre a alteração.

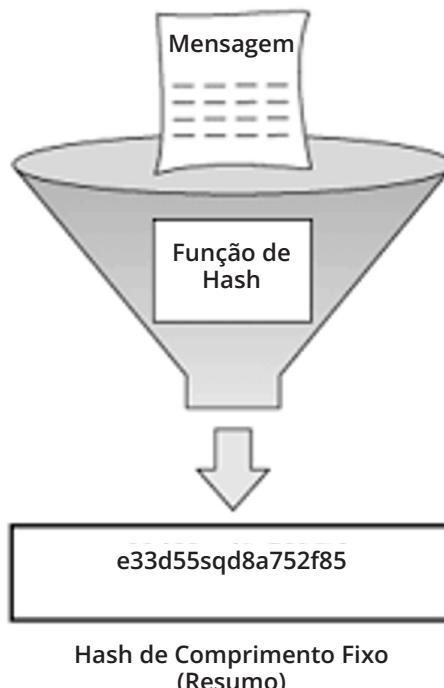
## O papel do Hashing em fornecer segurança

O Hashing é essencial para a segurança da **Rede Bitcoin**. Ao usar hashes para identificar transações, a rede pode detectar qualquer tentativa de alterar ou manipular uma **transação**. Isso ajuda a prevenir fraudes e garantir que todas as transações sejam registradas corretamente na **blockchain**.

Uma função de hash é um tipo de **função unidirecional** que recebe uma **entrada** (referida como “mensagem” ou “dados”) e a converte em uma representação numérica chamada “**hash**.” O hash de **saída** é único para os dados de **entrada**, então mesmo uma pequena alteração nos dados de entrada resulta em um hash completamente diferente.



## Dados de Comprimento Arbitrário



Uma **função de hash** é como uma máquina de código secreto. Ela recebe uma **mensagem** e a transforma em um código.

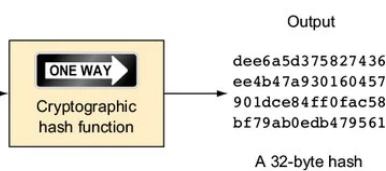
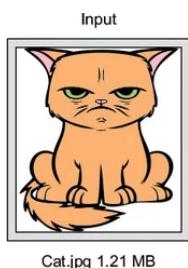
- O código sempre parece o mesmo para a mesma mensagem. Se você alterar a mensagem mesmo que seja um pouco, o código será completamente diferente. Isso ajuda os computadores a lembrarem as coisas e verificar se algo foi alterado.



Instantaneamente gere um hash SHA256 de qualquer string ou valor de entrada. Funções de hash são usadas como métodos unidirecionais.

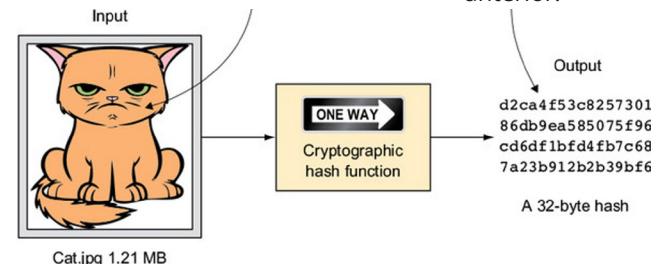


## Capítulo #7



Falta um bigode! Agora ela tem motivo para ficar rabugenta.

Completamente diferente do hash anterior.



A 32-byte hash

A **saída**, ou **hash**, tem sempre o mesmo comprimento, não importa quanto longa seja a informação original.

O **Bitcoin** utiliza alguns tipos específicos de **função** de hash chamados **SHA-256** e **RIPEMD160**. Seguem abaixo alguns exemplos:

- Observe que um ponto no segundo input altera completamente a saída em comparação com o primeiro.
- O terceiro input é um arquivo enorme, mas a saída ainda tem o mesmo comprimento fixo que os outros dois.

- SHA256 hash da string **hello world**  
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- SHA256 hash da string **hello world.**  
7ddb227315f423250fc67f3be69c544628dff41752af91c50ae0a9c49faeb87
- SHA256 hash do arquivo ISO para download do **Ubuntu 18.10**  
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

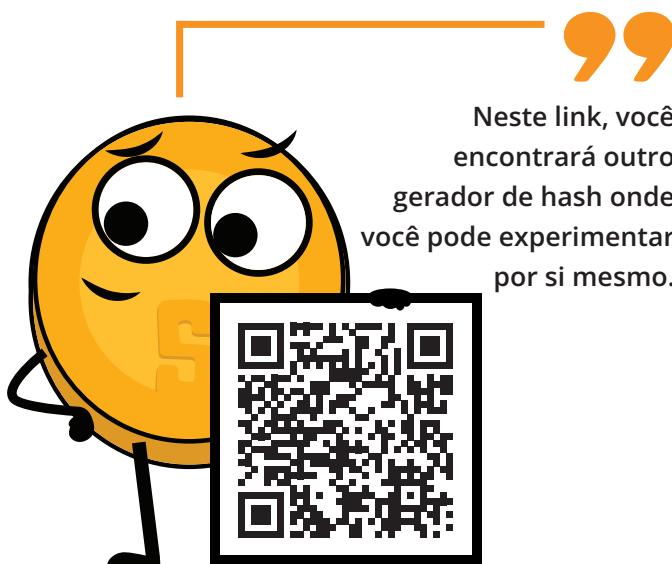
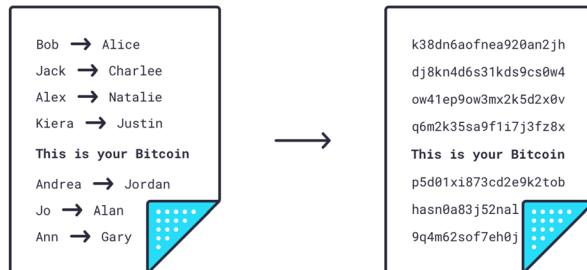
O **hashing** também pode ser comparado a uma partitura musical que captura a essência de uma peça de música. Assim como uma partitura musical é uma representação única de uma melodia, um valor de hash é uma representação única de um conjunto de dados. Ao comparar a partitura de uma peça musical com a performance real, um músico pode determinar se a performance é precisa. Da mesma forma, ao comparar o valor de hash dos dados recebidos com o valor de hash original, pode-se determinar se os dados foram alterados durante a transmissão.



# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

- Assim como uma leve variação em uma performance musical pode fazer com que ela soe diferente, mesmo a menor alteração nos dados originais resultará em um valor de hash diferente. Isso torna o hashing uma ferramenta poderosa para garantir a integridade e autenticidade das informações digitais.

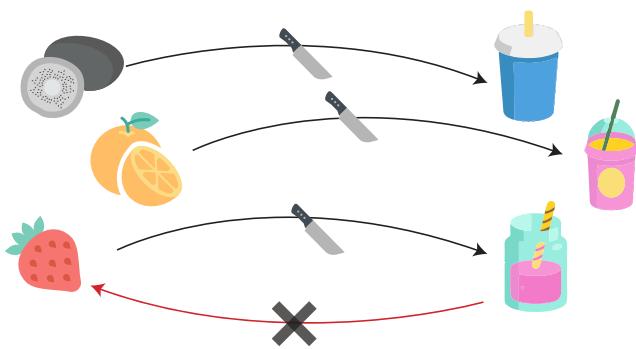
O processo de codificar a **chave pública** por meio do hashing é usado para melhorar a segurança das informações, convertendo-as em um formato fixo e ilegível. O Bitcoin utiliza os algoritmos SHA-256 e Ripemd-160 para produzir **endereços públicos**. A saída resultante serve como um identificador único para a **chave pública** e ajuda a garantir a integridade e segurança das transações armazenadas na *blockchain*. Ao **codificar** as informações dessa maneira, torna-se mais difícil para indivíduos não autorizados acessarem e manipularem os dados.



## Hashing

Uma função de hash recebe qualquer entrada e produz uma saída de comprimento fixo (hash).

### Ingredientes      Função de Hash      Smoothies



- **Determinístico.** Os mesmos ingredientes sempre resultam no mesmo smoothie.

- **Resistência a Pré-Imagem.** Você não consegue juntar uma morango de volta quando tem apenas o smoothie.

- **Resistência à Correlação.** Mudar um pouco os ingredientes resulta em um smoothie completamente diferente.

- **Resistência a Colisões.** É difícil encontrar ingredientes diferentes para um smoothie que resultem no mesmo resultado.

- **Velocidade e Verificabilidade.** Jogue frutas no liquidificador. É rápido e o que sai com certeza é um smoothie.



### 7.3 A “Mempool” ou Pool de Memória: Entendendo o Tanque de Espera das Transações do Bitcoin

#### O que é o Mempool?

O mempool é como uma sala de espera para transações na **Rede Bitcoin**. Quando uma transação é feita, ela é primeiro adicionada ao mempool de um nó antes de ser verificada e adicionada à **blockchain**.

O **mempool** é onde as transações aguardam para serem confirmadas em um bloco.



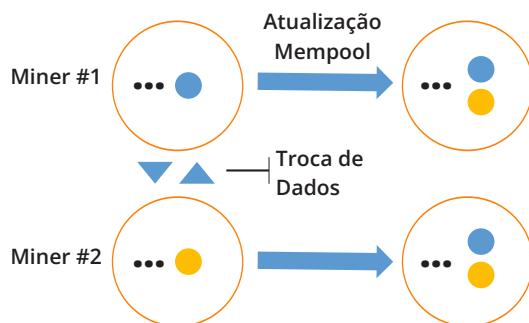
- tx hsh 6053b699...  
fee rate: 3 sat/vB
- tx hsh bb3b8clf...  
fee rate: 1 sat/vB
- tx hsh d7c2532a9...  
fee rate: 15 sat/vB
- tx hsh 0ecdd9c6...  
fee rate: 2 sat/vB



Quando um nó recebe uma transação de um outro nó, ele precisa verificar se a transação é legítima. Ninguém quer transações defeituosas ou enganosas.



A **sincronização do mempool** permite que os nós compartilhem suas transações com outros nós, enviando uma mensagem contendo uma lista de transações **verificadas** no mempool.



O principal objetivo de um mempool é:

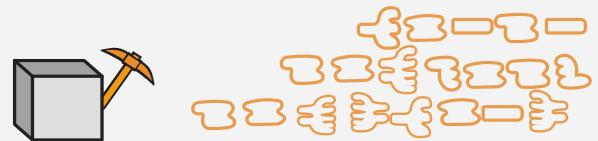
1

Repassar transações não confirmadas.



2

Fornecer transações aos mineradores para serem incluídas em blocos.



O processo de “Accept To Memory Pool” (ATMP)

envolve a verificação de coisas como:

- Já posso essa transação?
- Existe algum conflito com outra transação no mempool?
- Os **bitcoins** recebidos são suficientes para cobrir os **bitcoins** enviados?
- As assinaturas provam que as saídas anteriores podem ser gastas?
- Há taxas suficientes anexadas à transação?

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

## Como as Transações São Verificadas e Adicionadas ao Mempool

Um **nó completo** verifica todas as **transações** para garantir que sejam válidas e não tenham sido usadas anteriormente. Se uma **transação** for válida, o nó a verifica e a adiciona ao seu mempool de memória. Em seguida, ele a compartilha com outros nós para uma verificação dupla. Por fim, se a maioria concordar, a **transação** será removida do mempool de todos para se tornar uma parte permanente da **blockchain**.

As **transações** na **Rede Bitcoin** são retiradas do mempool e confirmadas quando são incluídas em um bloco, que é então adicionado à **blockchain**. No entanto, existem várias razões pelas quais uma **transação** pode não ser confirmada após 72 horas:

- 1. Baixa taxa:** Transações com uma taxa baixa podem não ser processadas rapidamente, pois os mineradores têm mais probabilidade de escolher transações com taxas mais altas para incluir em seus blocos.
- 2. Congestionamento da rede:** Se a rede estiver congestionada, pode haver um atraso na confirmação das transações, mesmo que tenham uma taxa alta.
- 3. Tentativa de gasto duplo:** Se um agente malicioso tentar gastar duas vezes, sua transação pode ser rejeitada pela rede.
- 4. Dados incorretos ou incompletos:** Se uma transação contiver dados incorretos ou incompletos, ela pode ser rejeitada pela rede.
- 5. Transação malformada:** Se uma transação estiver malformada, ela pode ser rejeitada pela rede.

Para evitar que as **transações** sejam rejeitadas, é recomendado incluir uma taxa alta o suficiente para garantir que a **transação** seja processada de forma oportuna, e verificar novamente se todos os dados da **transação** estão corretos antes de enviá-la.

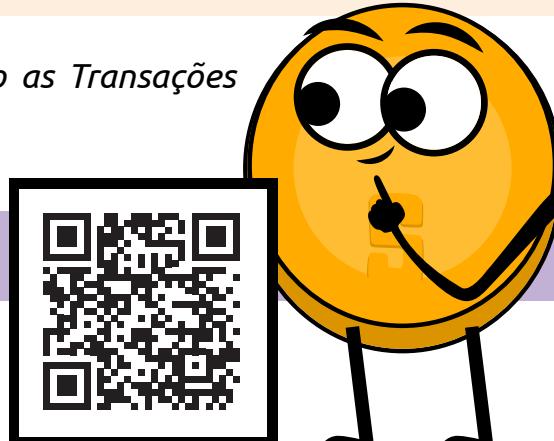


Um ataque **DDoS** (Distributed Denial of Service) é uma tentativa de tornar a rede indisponível para os usuários, sobrecarregando-a com um tráfego excessivo vindo de múltiplas fontes. Esse ataque tem como objetivo perturbar o tráfego normal de um site ou serviço, sobrecarregando-o com tráfego falso, tornando difícil ou impossível para usuários reais acessá-lo.

### 7.3.1 Exercício em Classe: Em Espera: Examinando as Transações Não Confirmadas da Rede Bitcoin.

**Exercício em Classe.** Siga as seguintes instruções:

- Visite o website <https://bits.monospace.live/>





**2.** Localize uma **transação** não confirmada e clique nela.

- Que informações você pode encontrar?
- É possível acompanhar a origem dos bitcoins?
- Quantos endereços você vê? O que significa entrada (input) e saída (output)?
- É possível acompanhar as UTXOs? Você consegue identificar quais BTCs foram gastos?
- A entrada corresponde à saída?
- Toda **transação** tem uma taxa?
- Para quem vai a taxa? É justa?
- Quem paga a taxa?
- É possível identificar a quantidade de bitcoins transferidos de um endereço para outro?

**3.** Anote o TxID, taxa de **transação**, taxa e valor total da **transação** em um caderno.

**4.** Analise outras **transações**, se desejar, e compare-as com a primeira em termos de valor, taxa paga e probabilidade de ser incluída no próximo bloco.

**5.** Considere o que significa para um bloco ser “minerado” e para uma **transação** ser “não confirmada”.

**6.** Esteja preparado para discutir essas observações e perguntas na próxima aula.

#### 7.4 Por Trás dos Blocos: O Mistério do Scripting do Bitcoin

O **Script** é uma **linguagem de programação** usada no **Bitcoin** para criar **contratos inteligentes** e **automatizar transações**. Para entender o script, é útil pensar nele como um conjunto de instruções que dizem à **Rede Bitcoin** o que fazer com uma **transação** específica.



Um **contrato inteligente** é um contrato autoexecutável em que os termos do acordo entre comprador e vendedor são escritos diretamente em linhas de código. O código e os acordos contidos nele existem em uma rede blockchain e são aplicados automaticamente.

• Pense nisso como uma máquina de venda automática. Você coloca dinheiro, faz uma seleção e a máquina dispensa o item automaticamente. Da mesma forma, um contrato inteligente executa automaticamente os termos do acordo entre duas partes, sem a necessidade de intermediários como advogados ou bancos.

Por exemplo, um contrato inteligente poderia ser usado para representar um acordo financeiro, como um empréstimo ou um título. Os termos do acordo, como a taxa de juros e o cronograma de pagamento, são codificados no contrato. Quando as condições acordadas são atendidas, o contrato executa automaticamente os termos e transfere os fundos.

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

Os principais benefícios dos contratos inteligentes são que eles são transparentes, seguros e autoexecutáveis, o que pode ajudar a reduzir os custos e riscos associados aos processos contratuais tradicionais. Além disso, por existirem em uma rede descentralizada, eles são resistentes a adulterações ou interferências, tornando-os uma forma mais segura e confiável de realizar transações.

De maneira semelhante, o **Bitcoin** utiliza o script para garantir que condições específicas sejam atendidas antes que uma transação seja processada.

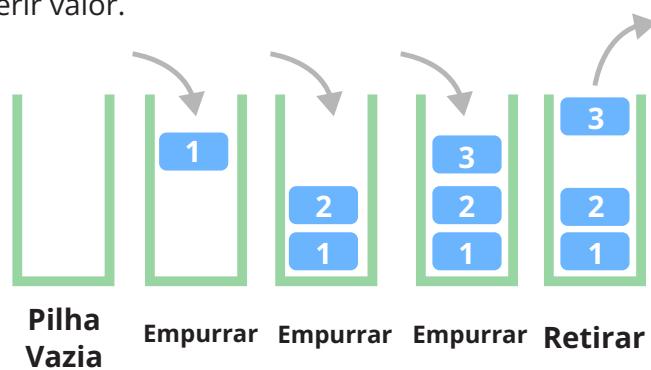
Enquanto outras redes **blockchain**, como o Ethereum, também suportam contratos inteligentes e transações programáveis, elas utilizam linguagens de programação e abordagens diferentes para impor as regras e condições das transações. Apenas o Bitcoin utiliza o script.

O script é uma linguagem de programação muito básica, mas é poderosa o suficiente para lidar com uma ampla variedade de transações. Por exemplo, ele pode ser usado para criar transações multiassinadas, onde várias pessoas devem aprovar uma transação antes que ela possa ser processada, ou para criar um contrato inteligente, onde uma transação é executada automaticamente quando certas condições são atendidas.

Embora o script possa parecer complexo, a ideia básica por trás dele é na verdade bastante simples. Ao usar o script, a rede Bitcoin pode automaticamente impor as regras e condições das transações, tornando-a uma forma segura e eficiente de transferir valor.

## Como o Script é Usado em Transações Bitcoin

- Imagine que você tenha uma fileira de moedas e queira classificá-las em compartimentos diferentes, como colocar moedas em diferentes cofrinhos. A ordem em que você coloca as moedas nos compartimentos é importante. Isso é semelhante à forma como os satoshis são transferidos em uma transação. As

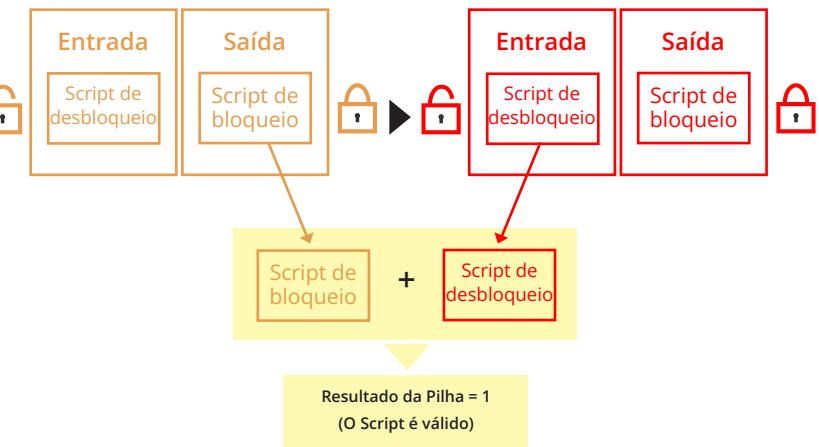


entradas são como uma fileira de moedas e as saídas são os compartimentos esperando para receber uma moeda. Para atribuir as moedas aos compartimentos, você passa por cada moeda na fileira, em ordem, e coloca cada uma no primeiro compartimento disponível. Isso é chamado de “primeiro a entrar, primeiro a sair” ou FIFO, o que significa que a primeira moeda na fileira vai para o primeiro compartimento disponível, e assim por diante.

- Os scripts operam em um **sistema baseado em pilha**, onde as instruções são processadas na ordem em que aparecem, de cima para baixo. O conceito é semelhante a uma pilha de pratos, onde você só pode acessar o prato que está no topo da pilha.



Uma transação básica de **bitcoin** utiliza pelo menos um “**script de bloqueio**” e um “**script de desbloqueio**” para determinar quem pode acessar os fundos em um determinado endereço de carteira. O script de bloqueio pode ser considerado como uma **lista de instruções que descreve como o destinatário dos fundos pode acessá-los**, enquanto o script de desbloqueio **desbloqueia os fundos**.



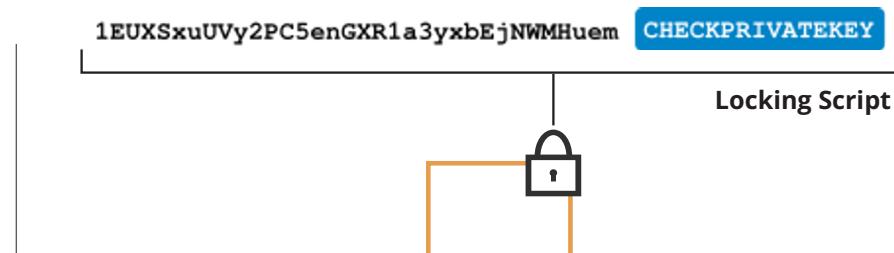
- Pense no Script como uma receita para assar um bolo. Assim como você precisa seguir os passos na receita para fazer o bolo, o computador precisa seguir as instruções do Script em uma ordem específica para transferir a propriedade do **bitcoin**.

Ao utilizar scripts de bloqueio e desbloqueio, juntamente com chaves privadas e públicas, a propriedade e a transferência de UTXOs podem ser rastreadas e verificadas com segurança.

#### 7.4.1 Uma Imersão Técnica nas Transações do *Bitcoin*

O script de bloqueio contém o **endereço do destinatário** e verifica se a **chave privada** correta foi utilizada. Isso garante que as **chaves privadas** permaneçam confidenciais e possam ser protegidas com segurança.

Para desbloquear os fundos, o remetente deve comprovar a propriedade gerando uma **assinatura** com sua **chave privada**, confirmindo assim a posse do **endereço**.

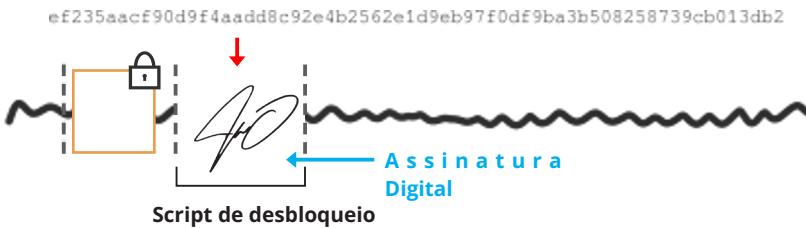


A saída (**bitcoin UTXO**) foi bloqueada para este **endereço** (1EUX...) e apenas a **chave privada** correta poderá desbloqueá-la.

# Desvendando os Segredos do Funcionamento Interno do Bitcoin: A Matemática, a Mempool e os UTXOs

Por exemplo, digamos que você queira enviar alguns **bitcoins** para o seu amigo, mas deseja garantir que seu amigo só possa gastá-los após uma determinada data. Você pode usar o **Bitcoin** script para definir essa condição, conhecida como **"bloqueio por tempo"**. Ao criar a **transação**, você inclui um script que especifica a condição de bloqueio por tempo. Quando seu amigo recebe os **bitcoin**, ele só pode gastá-los após a data especificada ter passado.

O script do **Bitcoin** também pode ser usado para criar condições mais complexas para gastar **bitcoins**, como transações de múltiplas assinaturas, que exigem que várias partes autentiquem uma **transação** antes que ela possa ser gasta. Isso pode ser útil em situações em que várias partes precisam aprovar uma **transação**.



**CHECKPRIVATEKEY** é uma função que verifica se o **endereço** corresponde à **chave privada** correta.



**CHECKSIG** verifica se a **transação** foi aprovada pelo proprietário da **chave privada** que corresponde à **chave pública** usada para assinar a **transação**.

Em termos simples, o script ajuda a garantir a segurança e confiabilidade das **transações** do **Bitcoin** ao usar chaves privadas e públicas para verificar a propriedade e a transferência dos fundos. Métodos diferentes de **transações** têm níveis de segurança variados. Alguns revelam a **chave**



## Capítulo #7



**pública** do destinatário durante a **transação**, tornando-a vulnerável a roubo se a **chave privada** for comprometida. Outros mantêm a **chave pública** oculta, proporcionando um nível mais alto de segurança.

No próximo capítulo, iremos aprofundar o processo de mineração e o papel dos mineradores na **Rede Bitcoin**. Exploraremos como eles validam as **transações**, criam novos blocos e recebem recompensas por seus esforços.

Fique atento para obter uma compreensão abrangente de como a **Rede Bitcoin** opera!



## *Capítulo #8*



# *Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain*

- 8.0** Revelando as Joias da Blockchain: Conheça os Mineradores e o Processo de Mineração
- 8.1** Sistema de Recompensas Dinâmicas da Mineração do Bitcoin: Recompensas em Blocos, Taxas de Transação e Halvings
- 8.2** A Tarefa Vital da Mineração do Bitcoin: Segurança da Blockchain
- 8.3** Dissecando o Bloco
- 8.4** Rehashing das Hashes - Sem trocadilhos
- 8.5** O Processo Passo a Passo da Mineração de um Bloco
  - 8.5.1** Exercício em Sala de Aula: Exercício Interativo de Mineração
  - 8.5.2** Resumo da transação do início ao fim
  - 8.5.3** Não confie, verifique
- 8.6** Exercício em Sala de Aula: Transação com UTXOs

# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

## 8.0 Descobrindo as Joias da Blockchain: Conheça os Mineradores e o Processo de Mineração

Os mineradores são os contadores.

- Em sistemas centralizados, os contadores são pagos pelas empresas para acompanhar e manter a precisão e integridade de seus registros financeiros.

Da mesma forma, os **mineradores** são pagos em **bitcoin** pelo seu trabalho de verificar e adicionar **transações** à **blockchain**, ajudando a manter a segurança e o funcionamento suave da rede. Esse trabalho envolve o uso de **poder computacional** e hardware especializado. O objetivo da mineração é adicionar novos blocos à **blockchain** e manter sua segurança, descentralização e viabilidade a longo prazo.

### O que é a mineração de Bitcoin?



A mineração de **Bitcoin** é um processo de adicionar informações de transações ao registro público de transações passadas do **Bitcoin**, conhecido como blockchain.

Este registro de transações passadas é chamado de blockchain, pois é uma cadeia de blocos. Essa cadeia serve para validar as transações de todas as outras redes como tendo ocorrido.

Os nós de **Bitcoin** utilizam essa cadeia tecnológica para distinguir uma transação genuína do **Bitcoin** de tentativas de gastar novamente moedas que já podem ter sido gastos em outro lugar.



Os mineradores coletam transações não confirmadas e formam um bloco, em seguida, embarcam em uma busca pela valiosa chave que **garantirá o lugar do bloco na blockchain**.

A chave é um “**hash de bloco válido**”, que está oculto entre bilhões de outros e só pode ser desbloqueado por uma chave específica definida pela rede.

- Imagine um grande monte de feno cheio de milhões de chaves, cada uma representando um hash de bloco único. A rede definiu uma chave específica que desbloqueará um prêmio valioso. Os mineradores procuram no monte de feno, testando cada chave na fechadura, mas apenas um minerador terá a sorte de encontrar a correspondência correta.

O primeiro minerador que encontrar o hash de bloco correto o transmite para a rede juntamente com o bloco de **transações**. Outros mineradores então verificam a solução para garantir que ela se encaixe corretamente na fechadura. Se a solução for precisa, o bloco é adicionado ao blockchain, criando um registro seguro e público.

Pelo seu trabalho árduo, os mineradores são recompensados de duas maneiras: recompensas em bloco e taxas de **transação**. As **recompensas em bloco** são **bitcoins** recém-gerados que são colocados em circulação a cada bloco adicionado ao blockchain. Já as **taxas de transação** são pequenas quantias de **bitcoins** que os usuários pagam para ter suas **transações** processadas mais rapidamente e priorizadas no bloco pelo minerador. Os mineradores têm liberdade para escolher quais **transações** incluir no bloco que estão minerando, e frequentemente priorizam aquelas com as maiores taxas de **transação**.



## 8.1 O Sistema Dinâmico de Recompensas da Mineração de Bitcoin: Recompensas em Blocos, Taxas de Transação e Halvings

Satoshi Nakamoto, o criador do **Bitcoin**, desenvolveu uma solução inteligente para distribuir novos **bitcoins** por meio de um sistema de recompensas em blocos de maneira descentralizada.



O **cronograma de fornecimento de bitcoin** é o seu plano para a criação e liberação de novos bitcoins em circulação, projetado para manter a escassez de bitcoins ao longo do tempo.

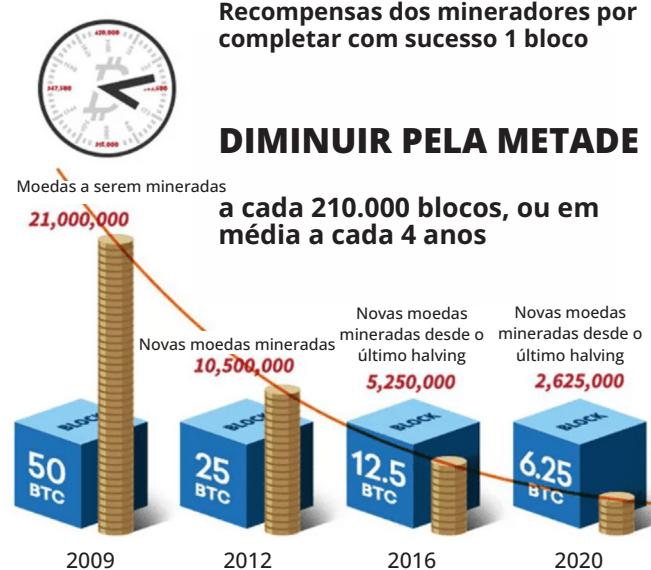
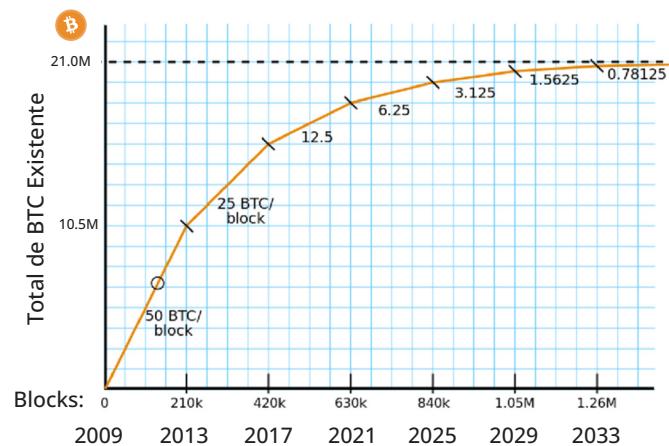
Nos primeiros dias do **Bitcoin**, os mineradores recebiam uma recompensa de 50 **bitcoins** por cada bloco que mineravam. Essa recompensa em bloco serve como uma motivação financeira para os mineradores investirem em hardware poderoso e eletricidade para suas operações de mineração.

No entanto, para controlar o fornecimento de novos **bitcoins** e manter a estabilidade na rede, a recompensa em bloco é **reduzida pela metade** aproximadamente a cada 210.000 blocos. Esse processo, conhecido como "**halving**", reduz a quantidade de novos **bitcoins** lançados em circulação e continua a incentivar os mineradores a garantir a segurança da rede e garantir sua descentralização.

- Vamos supor que você tenha um pote que só pode conter 1000 doces. Todos os dias, você pode adicionar 10 doces ao pote. Isso é como os novos **bitcoins** são criados e adicionados ao fornecimento por meio do processo de mineração. No entanto, a cada quatro anos, a quantidade de doces que você pode adicionar ao pote é cortada pela metade.

Isso é semelhante ao **halving** do **Bitcoin**, que **desacelera a taxa** de criação de novos bitcoins. O objetivo final é manter a escassez e limitar o **número total de bitcoins** a **21 milhões de unidades**, assim como o pote pode conter apenas uma quantidade limitada de doces.

**Cronograma de Fornecimento do Bitcoin**



# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

O **processo de halving** é semelhante à forma como as minas de ouro têm um suprimento limitado e eventualmente se tornam mais difíceis de encontrar. Atualmente, o protocolo do **Bitcoin** libera aproximadamente 6,25 novos BTC para os mineradores a cada 10 minutos quando um bloco é minerado.

A tabela mostra os detalhes dos **próximos** eventos de halving para o **Bitcoin**, incluindo a **porcentagem do suprimento total** que será minerado até aquela data, a data esperada do próximo evento de halving e o número do bloco em que se espera que o evento de halving ocorra.

Evento	Data Esperada	Bloco	Recompensa do Bloco	Porcentagem 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 %



A **oferta circulante** se refere à **quantidade de bitcoin** que está atualmente em circulação e disponível para negociação. Essa medida representa o número total de moedas que foram mineradas e estão em circulação em determinado momento, excluindo quaisquer moedas que possam estar bloqueadas ou perdidas permanentemente.

À medida que mais bitcoins são minerados, a oferta circulante e a porcentagem do suprimento total que foi minerada continuarão a aumentar até que o suprimento total de 21 milhões seja alcançado.

## Bitcoin: Porcentagem do Suprimento de 21 Milhões Minerada





**A Taxa de Inflação** é a taxa pela qual a oferta em circulação de uma criptomoeda está aumentando ao longo do tempo, **expressa como uma porcentagem da oferta máxima total**. Essa taxa é calculada como a diferença entre a oferta em circulação e a oferta máxima total (21 milhões), dividida pela oferta máxima total e multiplicada por 100.

Durante cada **evento de halving**, a recompensa em bloco para os mineradores é reduzida, diminuindo a **taxa de emissão** de novos **bitcoins**. Como resultado, a **taxa de inflação** do **bitcoin** diminui ao longo do tempo, o que pode levar a um aumento no preço do **bitcoin**.

A **redução na oferta**, combinada com o **aumento da demanda**, pode impulsionar o preço do **bitcoin**. Isso beneficia não apenas os primeiros adotantes da tecnologia, mas também serve como um incentivo para os mineradores continuarem a garantir a segurança da rede e contribuírem com seu poder de computação e recursos.

## 8.2 A Tarefa Vital da Mineração do Bitcoin: Garantir a Segurança da Blockchain

### O que é um Hash de Bloco Válido na Blockchain?

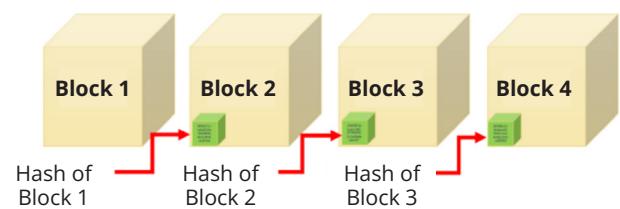
Um hash de bloco serve como um identificador único para cada bloco na **blockchain** e ajuda a detectar qualquer tentativa de alterar **transações** passadas. **Os blocos na blockchain armazenam transações e formam uma cadeia de blocos**, começando pelo **bloco gênese** até o mais recente, criando um registro público e transparente de todas as **transações**. O hash de bloco vincula cada bloco ao anterior, permitindo que qualquer pessoa visualize o histórico de qualquer **transação** e garanta a precisão e segurança dos dados armazenados na rede. Assim como uma **impressão digital** identifica um indivíduo, o hash de bloco identifica cada bloco único na **blockchain**.



O primeiro bloco de **bitcoin**, já minerado, contendo um total de 50 **bitcoins** foi minerado pelo criador do **bitcoin**, Satoshi Nakamoto.



Os blocos são “vinculados” uns aos outros por meio da aplicação de uma relação específica entre eles. Ou seja, um bloco deve conter uma “impressão digital”, que é um valor hash dos dados do bloco anterior. Uma função hash pode condensar uma mensagem arbitrária (as informações do bloco) para um tamanho fixo (por exemplo, 160 bits) e produzir uma impressão digital da mensagem.



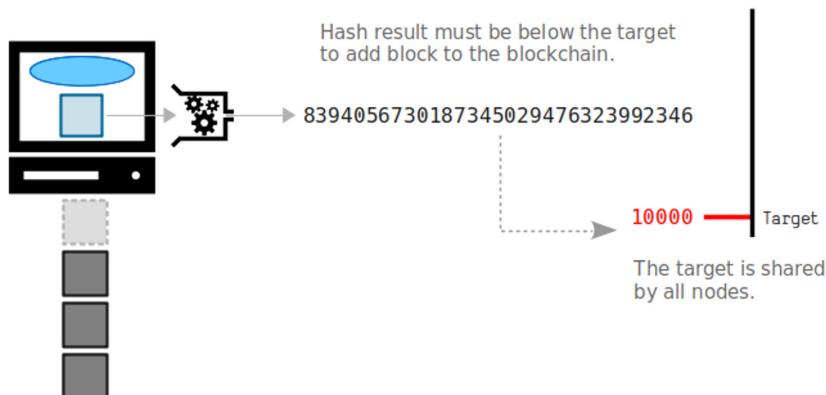
# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

Embora um hash de bloco **possa ser usado para verificar a integridade** dos dados no bloco, ele **não revela todas as informações** dentro do bloco. As informações dentro do bloco só podem ser acessadas usando as chaves criptográficas necessárias para decodificá-las. O hash do bloco simplesmente fornece um meio de verificar que os dados no bloco não foram alterados.

## A Corrida para Minerar um Bloco

Os mineradores se envolvem em uma competição para descobrir o hash de bloco que corresponde ao alvo (um número especial) definido pela rede. O minerador que descobre com sucesso o hash de bloco correto recebe a oportunidade de adicionar esse bloco à blockchain e atribuir a ele o respectivo ID de hash. Essa solução serve como validação da autenticidade do bloco.

- A mineração pode ser comparada a uma corrida onde o objetivo é alcançar a linha de chegada o mais rápido possível. O **alvo de dificuldade** na corrida é ajustado periodicamente, tornando mais difícil minerar um bloco à medida que mais mineradores se juntam à corrida.



- Digamos que o alvo definido pela rede em uma *blockchain* seja 1000. Os mineradores teriam que usar seus computadores para procurar por um número especial, chamado de hash de bloco, que seja menor que 1000. O primeiro minerador que encontrar um hash de bloco menor que 1000 pode adicionar um grupo de transações à blockchain e é recompensado com alguns **bitcoins**.



O **nível de dificuldade** é uma medida de quão difícil é encontrar um hash de bloco válido que atenda ao alvo definido pela rede. Ele é ajustado periodicamente para garantir que os blocos sejam adicionados à blockchain em uma taxa consistente. O nível de dificuldade é expresso como um número, e quanto maior o nível de dificuldade, mais difícil é encontrar um hash de bloco que atinja o alvo.

- Por exemplo, considere dois hashes diferentes:
  - Hash 1: **0000A1mINgF0RbL0cK5wItHth3hAy5tAcK**  
Nível de dificuldade: 1
  - Hash 2: **00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK**  
Nível de dificuldade: 2



Neste exemplo, o Hash 2 tem um nível de dificuldade maior do que o Hash 1 porque requer mais zeros no início. Isso significa que é mais difícil encontrar um hash de bloco que atenda ao alvo definido pela rede quando o nível de dificuldade é maior.

Encontrar um hash de bloco válido envolve **muito trabalho computacional**.



Ao encontrar um hash de bloco válido, um **minerador demonstra que realizou o trabalho necessário** para adicionar o novo bloco à blockchain e ser remunerado em bitcoin por seu esforço. **Prova de trabalho (PoW)** é o método que o **Bitcoin** utiliza para validar transações e adicionar novos blocos à blockchain.

A PoW mantém a *blockchain* segura, dificultando que qualquer pessoa com intenções maliciosas assuma o controle. O alvo é ajustado para que um bloco seja minerado a cada 10 minutos, tornando a rede ainda mais segura à medida que o alvo se torna mais difícil de ser alcançado.

Como exemplo, o alvo estabelecido pela rede para minerar um bloco específico pode ser:

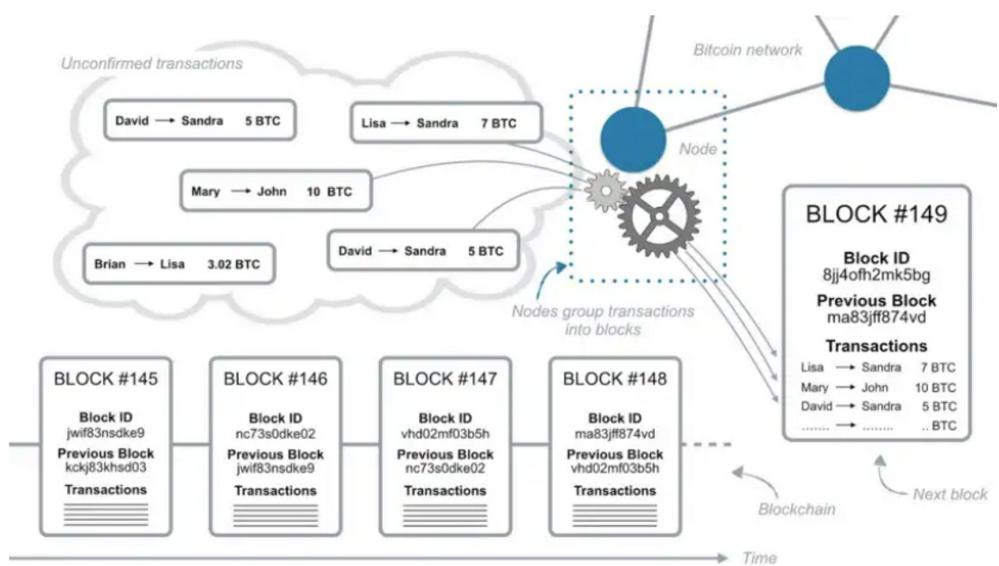
**00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK**

Isso significa que o primeiro minerador a encontrar um hash com oito zeros iniciais atingirá esse alvo e poderá adicionar o bloco à blockchain, além de receber uma compensação em bitcoin.

### O Papel dos Mineradores

Os mineradores têm duas tarefas em uma rede *blockchain*:  
**1) verificar transações** e **2) adicionar novos blocos**.

Eles coletam **transações** não confirmadas em sua **mempool**, selecionam um subconjunto delas para incluir em seu **bloco candidato** e, em seguida, procuram pelo hash do bloco.



# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

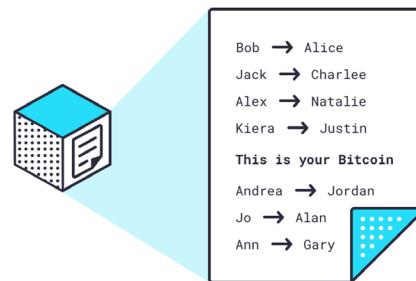
Vários mineradores podem estar trabalhando simultaneamente na criação de novos blocos. O primeiro minerador que descobrir um hash de bloco que atenda ao alvo definido pela rede o anuncia à rede, e os outros mineradores então **verificam** as **transações** no bloco candidato desse minerador para garantir que sejam válidas. Se as **transações** forem realmente válidas, o bloco é adicionado à blockchain. Os outros blocos criados pelos outros mineradores naquele momento não são adicionados e são descartados. Esse processo ajuda a manter o consenso dentro da rede e evita gastos duplos.



Um **bloco candidato** é um bloco de transações que está sendo considerado para ser adicionado à blockchain, mas ainda não foi adicionado.

## 8.3 Dissecando o Bloco

Uma **blockchain** é composta por blocos, semelhantes a páginas em um livro-razão, que armazenam novas **transações**. Cada bloco possui um **cabeçalho** com um resumo dos dados, um link para o bloco anterior, e um número único chamado **nonce**, ou um **número usado apenas uma vez**, e alguns outros detalhes. A tarefa dos mineradores é preencher corretamente as informações do cabeçalho ao criar blocos candidatos.

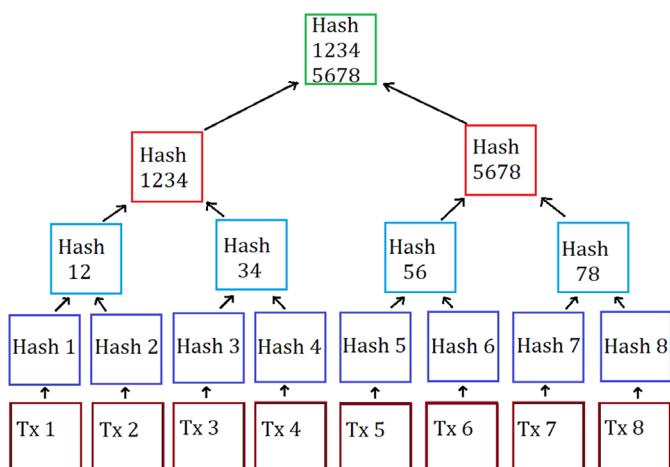


### A Organização das Transações

Os mineradores devem organizar as **transações** em seus blocos candidatos em um formato específico, no qual apenas algumas informações são incluídas no cabeçalho.



As transações formam a base da **Rede Bitcoin** e são organizadas de forma eficiente e segura por meio do uso de **Árvores de Merkle**. Essas árvores condensam grandes quantidades de dados em uma representação compacta, melhorando a segurança e eficiência geral da rede.





O **Merkle Root Hash**, que é o dado incluído no cabeçalho, é um **único valor de hash** que atua como uma impressão digital para todas as **transações** em um bloco. Isso permite a verificação eficiente das **transações** sem ter que examinar cada uma individualmente, tornando-o um componente importante da segurança e escalabilidade da rede Bitcoin.

Se uma **transação** estiver incluída em um bloco, seu hash será incluído no **Merkle Root Hash**. Se qualquer parte dos dados for alterada, o código final será diferente, tornando fácil detectar quaisquer alterações maliciosas nos dados. Isso ajuda a manter a privacidade e proteger informações sensíveis contidas em cada **transação** na rede.

Se um hacker tentar alterar um único caractere em uma **transação**, as verificações subsequentes do bloco falharão, pois cada bloco depende das informações do bloco anterior. O Merkle Root atua como uma cadeia segura que vincula todas as **transações** em um bloco, garantindo a precisão e integridade dos dados na rede.



Uma **transação Coinbase** no **Bitcoin** é um tipo especial de **transação** incluída em cada bloco da blockchain. Ela serve para dois propósitos: primeiro, recompensar o minerador que conseguiu minerar com sucesso o bloco e, segundo, fornecer um endereço para receber taxas de **transação** como comissão.

Essa **transação** também é incluída na Árvore de Merkle. Ao contrário de outras **transações**, a **transação Coinbase** não possui uma entrada, pois ela gera novas moedas por meio do algoritmo de software. Em vez disso, ela cria uma nova saída de **transação** não utilizada (UTXO), que pode ser usada como entrada para **transações** futuras.

#### **Os Blocos de Construção de um Bloco: Entendendo o Cabeçalho do Bloco na Blockchain**



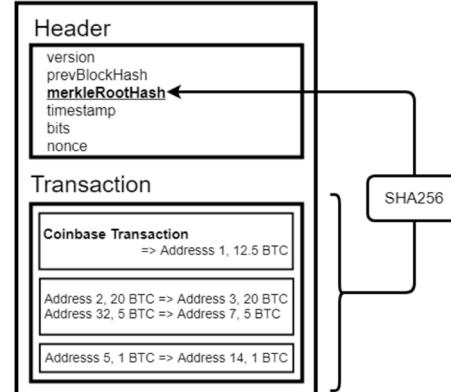
Um **cabeçalho de bloco** é como a capa de um livro; ele fornece um resumo do seu conteúdo e detalhes importantes de um bloco.

- **O Hash do Bloco:** O código único e válido do bloco pelo qual ele é identificado. **Um hash de bloco** pode ser usado para verificar a consistência das informações em um bloco cada vez que ele ou as informações nele são verificadas.
- **Versão:** Isso é como uma etiqueta que indica qual versão do software foi usada pela pessoa que criou o bloco.
- **Hash do Bloco Anterior:** Este é o hash válido do bloco que veio antes do que você está olhando. Ele garante que os blocos estejam na ordem correta e que ninguém possa alterar os blocos anteriores sem afetar o bloco atual e todos os blocos que vêm depois dele.

# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

## Cabeçalho do Bloco

Versão	1
Bloco anterior	00000000000002efa96db4fd543284c4b8bdc21daaac75c9f311af6312da87d
Raiz de Merkle	ba3ffef2b2b29e6ae2fd4f7188c5c2ad13fce618aa2cde86adacb6229e75b762
Carimbo de tempo	2012-08-31 11:32:28
Bits	436658110
Nonce	538012418



- **Hash da raiz de Merkle:** **SHA256** (**Hash(H(1,2),H(3,4))**, **Hash(H(5,6),H(7,8)).....**). Isso atualiza UTXOs específicos na cadeia.

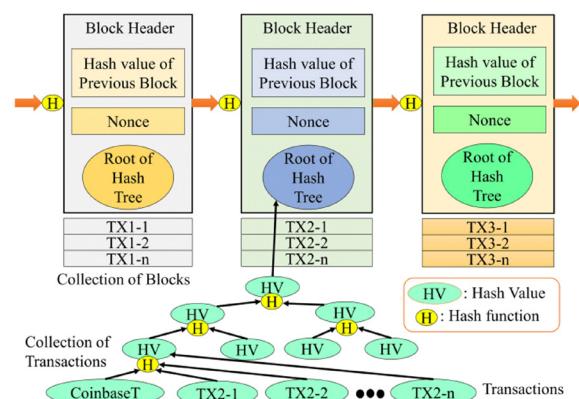
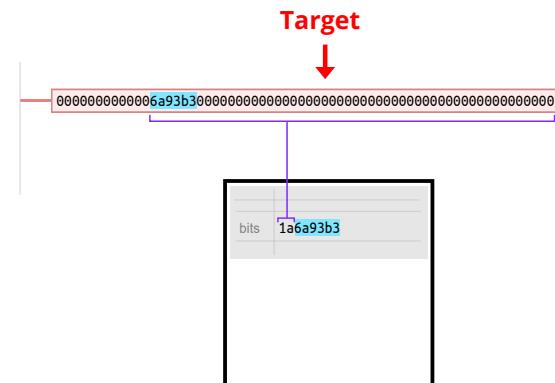
- **Tempo:** Este é o momento em que a pessoa que criou o bloco começou a trabalhar nele.

- **Bits:** Isso é como um código que indica o quanto difícil foi criar este bloco. Também é chamado de "**valor alvo**".

- **Nonce:** Um nonce é um número único usado pelos mineradores para criar um novo bloco em uma blockchain. Os mineradores tentam diferentes nonces até encontrar um que lhes dê o valor de hash correto para o bloco, o que comprova que eles fizeram o trabalho necessário para validar o bloco e adicioná-lo à **blockchain**.

## A Busca pelo Nonce: Encontrando o Número Mágico na Corrida da Blockchain

No mundo da **blockchain**, cada bloco possui informações únicas e medidas de segurança para evitar adulteração. Uma dessas medidas é o **nonce**, um número usado uma vez para criar um **hash de bloco candidato** único.



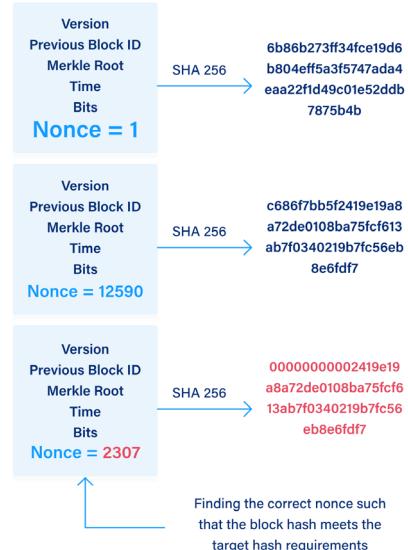
Quando um minerador está tentando adicionar um novo bloco à **blockchain**, ele precisa **encontrar o nonce correto** que **produzirá um valor de hash que atenda ao alvo estabelecido pela rede**. Isso é feito tentando diferentes valores de nonce e passando-os pela função de hash até encontrar o correto.



## Capítulo #8

Lembre-se de que as funções de hash são altamente sensíveis a qualquer alteração na entrada, o que significa que mesmo uma pequena mudança na **entrada** resultará em uma **saída** completamente diferente. Portanto, ao usar um valor de nonce diferente, os mineradores podem garantir que cada bloco que eles mineram tenha um **valor de hash único**.

O nonce é apenas um dos componentes no cabeçalho do bloco, juntamente com outras informações importantes, como o carimbo de data e hora e o hash do bloco anterior. Depois que todas as informações do cabeçalho do bloco são combinadas em um único hash, é criado o **hash do bloco candidato**. O minerador que encontra o valor de hash que atende ao alvo estabelecido pela rede é aquele que vence a corrida e pode adicionar o bloco à blockchain.



Conforme vemos abaixo, para o Bloco #7, **Mi Primer Bitcoin** foi recompensado com 1 BTC por calcular o hash de bloco correto exigido pela rede na época (21/1/23). Além disso, MPB recebeu taxas das **transações** incluídas no bloco. O **nonce** que finalmente produziu o **hash vencedor** foi 354.

Block 7 21/1/23 07:50:54			
Miner: MiPrimerBitcoin			
Set as 'Last Block' (only if you know what you do)			
longest chain			
2 Transactions			
New Block Reward	→ MiPrimerBitcoin 7a38ab902a...	1 BTC	
MiPrimerBitcoin	→ Marc 7a38ab902a...	0.2 BTC	
Hash of the previous Block 00d695226ec071b3182c94182014f0a7956b5040b2c0930f271e1a47ccb2f187			
Nonce: 354			
Hash	0029aa9c719bb1861bdb7c194583c3c7666a45ffcf14d6cfb410bbd6337f8e7		

Block 8 21/1/23 07:53:09			
Miner: MiPrimerBitcoin			
longest chain			
4 Transactions			
MiPrimerBitcoin	→ jim 7a38ab902a...	0.03 BTC	
MiPrimerBitcoin	→ Roby 7a38ab902a...	0.04 BTC	
MiPrimerBitcoin	→ Dalia 7a38ab902a...	0.003 BTC	
Hash of the previous Block 0029aa9c719bb1861bdb7c194583c3c7666a45ffcf14d6cfb410bbd6337f8e7			
Nonce: 271			
Hash	000a5d0388ca848147ed884571a8e8c9113746569f394cc40544e37507ed1af7		



Uma nova transação -  
foi transmitida para a  
Blockchain.



Um número de  
transações é  
selecionado.



O bloco será  
hashado.



O minerador receberá sua  
recompensa após várias  
confirmações.

O bloco é adicionado  
à cadeia.

TRUE

O quebra-cabeça  
foi resolvido.

FALSE

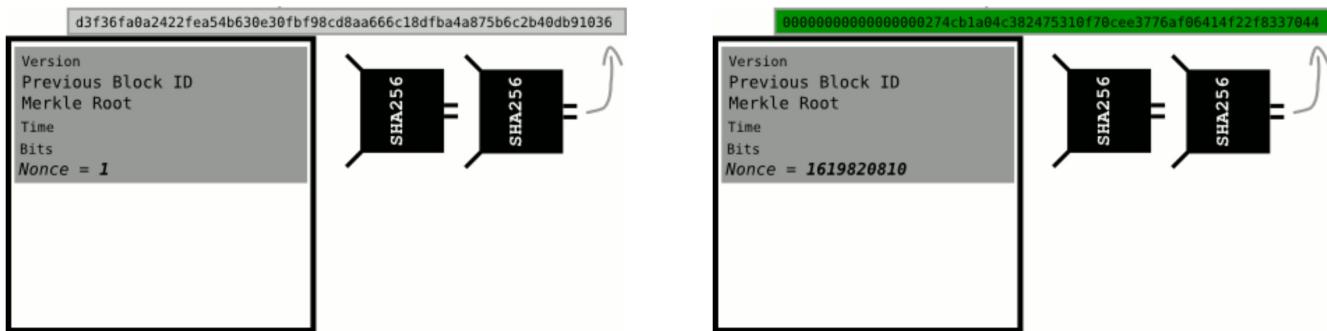
O bloco é novamente hash até que  
outro nó resolva o quebra-cabeça.

# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

## 8.4 Re-hashing dos Hashes - Sem trocadilhos

Quanto tempo os mineradores levam para descobrir um hash válido? E quanto rapidamente eles podem modificar os valores de nonce durante o processo de cálculo?

No exemplo abaixo, um minerador levou 1619820810 iterações para encontrar um valor de hash com o número necessário de zeros. O minerador que conseguiu encontrar o valor de nonce correto adicionou o bloco à blockchain, formando uma parte segura e inalterável da cadeia.



A **taxa de hash** é uma medida do poder computacional da rede e da **velocidade com que os mineradores podem fazer cálculos de nonce**, que são usados para encontrar o hash de bloco correto.

Quanto mais poder computacional um minerador tem, mais rápido eles podem fazer esses cálculos, o que lhes dá uma vantagem no processo de mineração. No entanto, à medida que a taxa de hash da rede aumenta, a dificuldade de minerar novos **bitcoins** também aumenta, tornando mais desafiador para todos os mineradores encontrarem o **hash de bloco** correto.

- Assim como os atletas atualizam seu equipamento para correr mais rápido, os mineradores de Bitcoin investem em hardware de computador especializado para aumentar sua **taxa de hash** e minerar blocos de forma mais eficiente. Quanto mais recursos eles investem, melhores são suas chances de chegar à linha de chegada primeiro.

- A taxa de hash pode ser comparada à velocidade do corredor. Quanto mais poderosa for a máquina do minerador, maior será a taxa de hash e mais rápido eles podem minerar. No entanto, assim como em uma corrida, ter uma alta velocidade não garante uma vitória se o alvo de dificuldade foi ajustado para um nível mais alto. Os mineradores devem constantemente atualizar seu equipamento e melhorar sua taxa de hash para se manterem à frente da concorrência e terem a chance de minerar um bloco e vencer a corrida.



O processo de encontrar o **valor de hash** correto ao alterar o **nonce** é o que chamamos de **mineração**!



Quando falamos sobre mineradores individuais e o tamanho da rede como um todo, usamos prefixos SI diferentes, o que pode ser confuso.

As principais denotações de hash são as seguintes:

- As máquinas de mineração de **Bitcoin** possuem uma taxa de hash em Terahashes por segundo (**TH/s**).
- A **taxa total de hash** da rede é descrita em Exahashes por segundo (**EH/s**)

### Taxa de Hash do Bitcoin:

#### 1.1 Exahash / segundo

Um hash / segundo

Um **Kilohash** = 1,000 hashes

Um **Megahash** = 1,000,000 hashes

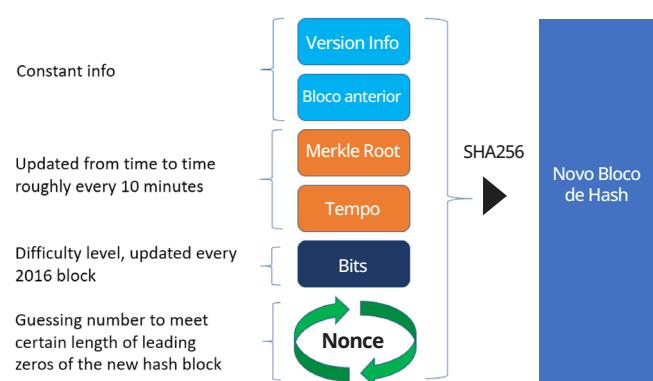
Um **Gigahash** = 1,000,000,000 hashes

Um **Terahash** = 1,000,000,000,000 hashes

Um **Petahash** = 1,000,000,000,000,000 hashes

Um **Exahash** = 1,000,000,000,000,000,000 hashes

### Hashing de Blocos do Bitcoin

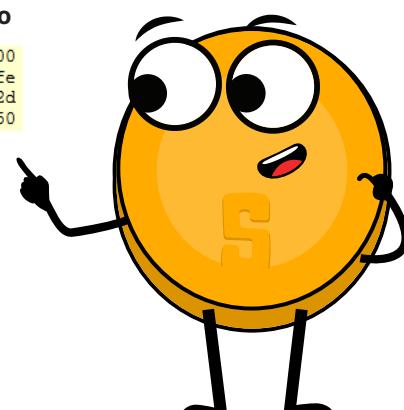


**O Hash do Bloco pode ser referido como a Prova de Trabalho.**

Em resumo, a cada cerca de dez minutos, os mineradores entram em uma corrida para encontrar um hash de bloco válido. Eles começam pegando todos os dados de seus blocos candidatos (que são resumidos de forma organizada nos cabeçalhos dos blocos), fazendo um duplo hash desses dados em um único hash e comparando o resultado com um valor de hash alvo estabelecido pela rede. Se o hash do bloco produzido for muito alto, o minerador ajusta o nonce e tenta novamente, repetindo esse processo trilhões de vezes por segundo até que um minerador sortudo finalmente encontre um hash que atenda ao alvo da rede.

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf29759b55 330edad87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

**Hash do Bloco**  
  
 0000000000000000  
 e067a478024adfe  
 cdc93628978aa52d  
 91fabd4292982a50



# **Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain**



Não importa quanto pouco ou quanto grande seja o poder de hash aplicado à mineração, em média, um bloco é minerado a cada 10 minutos.

- Quando a **taxa total de hash** diminui, o **nível de dificuldade** também diminui para facilitar a mineração de novos bitcoins.
  - Isso ajuda a manter constante a taxa na qual novos **bitcoins** são minerados.
- O ajuste de dificuldade é feito usando uma fórmula que leva em consideração o tempo médio necessário para minerar os 2016 blocos anteriores.
  - Se o tempo médio para minerar 2016 blocos for inferior a 14 dias, o nível de dificuldade é aumentado.
  - Se o tempo médio para completar 2016 blocos for superior a 14 dias, o nível de dificuldade é diminuído.



**A Taxa de Emissão** refere-se à velocidade com que novas moedas estão sendo adicionadas à oferta em circulação, geralmente por meio da mineração. Essa taxa pode ser afetada por vários fatores, incluindo mudanças na taxa total de hash da rede, o número de blocos minerados, e eventos de halving, que reduzem a quantidade de moedas que podem ser mineradas por bloco.

## **8.5 O Processo Passo a Passo da Mineração de um Bloco**

Minerar um bloco na **Rede Bitcoin** envolve várias etapas:

1. Novas **transações** são transmitidas para a rede, coletadas e verificadas pelos nós.
2. As **transações** são coletadas a partir das **transações** não confirmadas na **Mempool**. Transações com taxas mais altas têm prioridade.
3. Essas **transações** são então organizadas em uma **Árvore de Merkle** e incluídas em um **bloco candidato**, juntamente com o **Hash do Bloco anterior**, um **timestamp** e um **nonce**.
4. Os mineradores competem para resolver um quebra-cabeça matemático com base nas informações do bloco, incluindo as **transações** e um número aleatório.
5. O quebra-cabeça envolve encontrar um número específico (o “hash”) que, quando combinado com os dados do bloco, resulta em um valor menor que um número alvo.



Em outras palavras, os mineradores utilizam a **prova de trabalho** para ajustar o valor do **nonce** até obterem um hash que atenda aos **requisitos de dificuldade especificados**.

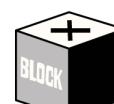
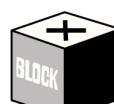


## Capítulo #8

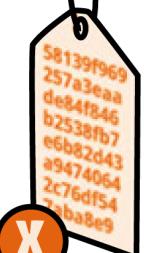
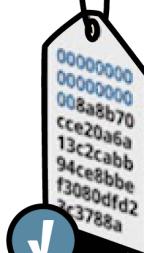
**OS MINERADORES** – Os nós que trabalham para manter e atualizar o registro - reúnem todos os dados das transações mais recentes.



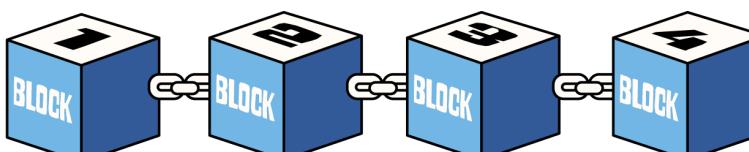
Eles agrupam tudo em um **BLOCO** para adicionar à cadeia.



Em seguida, eles calculam um **HASH** para aquele bloco: eles passam todos os dados por um algoritmo que produz uma sequência única. Eles fazem isso novamente. E de novo. Eles estão procurando por um hash válido - um que comece com uma longa sequência de zeros. O primeiro minerador a encontrar um ganha bitcoin recém-criado, e seu bloco é adicionado à cadeia.



Este hash garante que ninguém adultere o livro-razão. Alterar um único número ou letra em qualquer parte da cadeia tornará cada hash de cada bloco subsequente **irreconhecivelmente diferente**. Nesse caso, os outros nós rejeitarão o livro-razão comprometido.



**6.** O minerador que primeiro encontra o hash correto o transmite para a rede, e os outros mineradores verificam a solução para garantir que ela seja realmente correta.

**7.** Se a solução for verificada, o bloco é adicionado à *blockchain*.



O **bloco minerado** é transmitido para a rede para **verificação** e, uma vez verificado por outros mineradores e alcançado o consenso na rede, o bloco é adicionado à *blockchain* como o último bloco na cadeia.



# **Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain**

8. O minerador que conseguiu minerar com sucesso o bloco é recompensado com **bitcoins** recém-criados a partir da transação **coinbase** e com as taxas de transação das transações incluídas.
9. O novo bloco se torna parte do registro imutável e transparente de todas as transações na **blockchain**. O hash do bloco e as informações nele são usados para atualizar a **blockchain** e o processo recomeça com o próximo bloco.

## *8.5.1 Exercício em Classe: Exercício Interativo de Mineração*

**Exercício em Classe.** Siga as seguintes instruções:

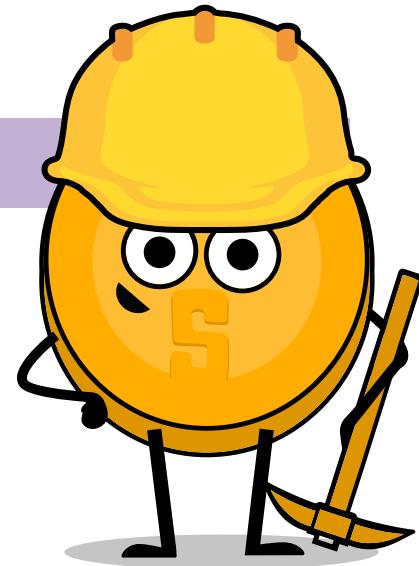
1. Visite o website  
<https://chainflyer.bitflyer.jp/>

2. Revise os vários elementos exibidos na página, incluindo os últimos blocos, transações confirmadas, o número de transações, uso de memória e o valor aproximado do bloco inteiro.

a. Responda às perguntas:

i. Qual foi o último bloco minerado?

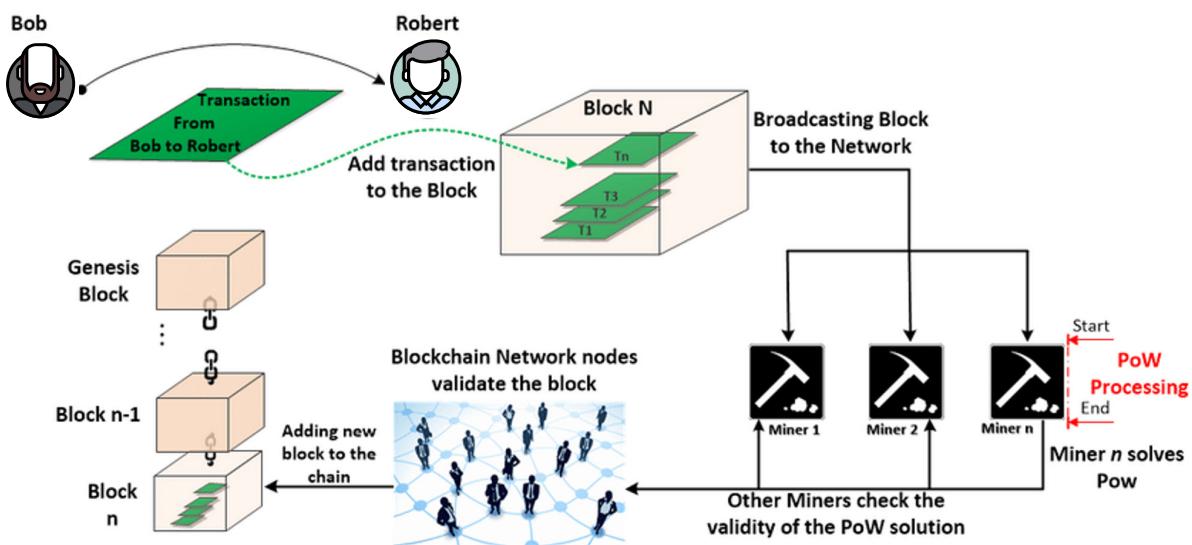
- Quantas transações foram incluídas nesse bloco?
- Qual é o valor total negociado em **bitcoin**?
- Qual foi o tamanho em megabytes do bloco?
- Com quantos zeros o nonce do bloco começa?
- Quanto o minerador ganhou no total?
- Qual foi o valor total das taxas recebidas pelo minerador por adicionar as transações à rede?
- Escolha uma das transações de maior valor no bloco. Para quantas carteiras de BTC o valor foi distribuído.





### 8.5.2 Resumo da Transação do Início ao Fim

1. Um usuário deseja enviar alguns **bitcoins** para outro usuário. Eles criam uma **transação** com os detalhes do envio, incluindo a quantidade de **bitcoins** sendo enviada, o endereço do remetente e o endereço do destinatário.
2. O usuário então usa sua **chave privada** para criptografar a **transação**. Essa chave privada é como um código secreto que apenas o usuário conhece e é usada para provar que o usuário é quem diz ser.
3. A **transação** criptografada é transmitida para a rede de nós do **Bitcoin**.



4. Os nós verificam a **transação** usando a **chave pública** do remetente, que está disponível no **blockchain**. Eles verificam se a assinatura é válida e se o remetente possui **bitcoins** suficientes para concluir a **transação**.
5. Os nós então agrupam as **transações** verificadas em um bloco.
6. O bloco é transmitido para a rede de mineradores do **Bitcoin**.
7. Os mineradores usam um algoritmo matemático complexo para resolver um quebra-cabeça, conhecido como "mineração". Uma vez que o quebra-cabeça é resolvido, ele é adicionado ao **blockchain** e o bloco é adicionado à cadeia.
8. Uma vez que o bloco é adicionado ao **blockchain**, a **transação** é considerada completa e o destinatário pode acessar os **bitcoins** usando sua própria **private key**.



Resumidamente, o remetente cria e criptografa a transação com sua chave privada, os nós verificam as UTXOs da transação usando a chave pública do remetente, e os mineradores adicionam a transação verificada ao blockchain. O destinatário pode então acessar os **bitcoins** usando sua chave privada. Uma vez que um bloco é minerado, todas as **transações** nele incluídas são consideradas confirmadas, e as UTXOs usadas como entradas nessas **transações** são consideradas gastas e não serão utilizadas novamente.

# Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain

## 8.5.3 Não confie, verifique

No mundo das criptomoedas, a frase “**Não confie, verifique**” é um lembrete para sempre verificar as transações por conta própria em vez de confiar em terceiros, como uma autoridade centralizada ou intermediário. A rede Bitcoin é composta por uma rede descentralizada de nós, o que permite aos usuários verificar as transações por si mesmos.

No entanto, existem cenários que podem fazer com que as transações sejam revertidas, como **gastos duplos**, **blocos órfãos** e **reorganização**. Para aumentar a segurança das transações, é recomendável aguardar 6 confirmações, ou seja, 6 blocos que contenham a transação específica, antes de considerá-la como finalizada. Quanto mais confirmações uma transação tiver, mais segura ela se torna, pois a probabilidade de ser revertida diminui. O número de confirmações necessárias pode variar dependendo do caso de uso e do nível desejado de segurança.

- **Gastos duplos:** Em um ataque de gasto duplo, um ator malicioso tenta gastar o mesmo bitcoin duas vezes manipulando a rede para que ela aceite sua segunda transação do mesmo bitcoin como válida. Se um minerador ou grupo de mineradores que controla mais de 50% do **poder computacional da rede** (conhecido como ataque de 51%) confirmar uma transação de gasto duplo, ela poderá ser adicionada a um bloco e considerada válida, revertendo efetivamente a transação original.
- **Blocos órfãos:** Quando dois mineradores encontram um novo bloco ao mesmo tempo, a rede pode aceitar temporariamente ambos. Quando um dos blocos é posteriormente estendido por blocos adicionais, a rede reconhecerá essa cadeia como a cadeia principal e o outro bloco se tornará órfão, não fazendo mais parte do *blockchain* principal. As transações incluídas no bloco órfão não são perdidas e serão incluídas em um bloco posterior se continuarem válidas.



Um bloco órfão no **Bitcoin** é um bloco válido que não está incluído na cadeia mais longa, que é considerada a cadeia principal.

- **Reorganização:** Isso poderia teoricamente acontecer se um novo bloco fosse adicionado à blockchain e isso causasse a substituição da cadeia existente por outra. Se uma transação foi incluída em um bloco que não está mais na cadeia principal, ela seria considerada inválida e a transação seria revertida.

TRANSACTION

ogdao6f8dbzdc5b9ea5ce9d3d3df1028679fe29091fa9410d6fc3be78052c7a6

Pending (5 Confirmations)

Received Time 2023-04-24 10:12:21 UTC

Amount sent 6.42932021 ₿

Block Height 773373

TRANSACTION

3748e734657f7f8112b0dc85a1351d9aabef6263f76b6a636f382e13b393730

8 Confirmations

Received Time 2023-04-24 09:38:03 UTC

Amount sent 6.27633464 ₿

Block Height 773374



## 8.6 Exercício em Sala de Aula: Transação com UTXOs

**Exercício em Classe.** Siga as seguintes instruções:

**1.** Entenda seu papel: Você foi designado para um dos seguintes papéis: remetente, destinatário, nó ou minerador.

- Como **remetente**, você será responsável por criar e transmitir transações.
- Como **destinatário**, você será responsável por receber e verificar transações.
- Como **nó**, você será responsável por validar as transações e seguir as regras.
- Como **minerador**, você será responsável por verificar, adicionar as transações à *blockchain* e coletar recompensas pelo seu trabalho árduo.

**2.** Se você é o **remetente**, crie uma transação: Para criar uma transação, siga estas etapas:

- Pegue um formulário de transação e preencha os seguintes campos:
  - UTXO de entrada: 20BTC
  - UTXO de saída: 10BTC para o endereço do destinatário
  - UTXO de saída: 1BTC para o endereço do minerador
  - UTXO de troco: 9BTC para o seu endereço
  - Assinatura: Sua assinatura simulando uma chave privada.
- Passe o formulário de transação e a quantidade correspondente de moedas para o destinatário.

**3.** Se você é o **destinatário**, verifique as transações: Siga estas etapas:

- Verifique o formulário de transação para garantir que o número correto de moedas e o nome ou iniciais do destinatário estejam escritos.
- Conte as moedas que você recebeu e compare-as com o número de moedas escritas no formulário de transação.
- Se as moedas corresponderem, marque a caixa de aprovação no gráfico de UTXOs que é compartilhado e acessível a todos na sala de aula.
- Se as moedas não corresponderem ou se você tiver dúvidas, rejeite a transação e escreva o motivo no gráfico de UTXOs.

**4.** Se você é um **nó**, valide as transações: Como nó, você é responsável por validar as transações verificando se a transação é válida, seguindo as regras do protocolo e o mecanismo de consenso.

- Verifique se o endereço do remetente é válido e se o endereço do destinatário é válido.
- Verifique se o remetente tem fundos suficientes para concluir a transação, verificando se a UTXO usada como entrada na transação realmente existe e não foi gasta anteriormente, olhando para o gráfico de UTXOs.
- Verifique se a transação não duplica o gasto de moedas, olhando para o gráfico de UTXOs.

# **Construindo a Cadeia de Segurança: Compreendendo o Processo de Mineração do Bitcoin e seu Papel na Blockchain**

**5.** Se você é um **minerador**, adicione as **transações** à **blockchain**: Como minerador, você é responsável por adicionar as **transações** à **blockchain**. Siga estas etapas:

- Verifique as **transações** que foram aprovadas pelos destinatários e validadas pelos nós.
- Jogue o dado e compare os números com o outro minerador. O minerador com o menor número (abaixo de 25) adicionará a **transação** à **blockchain**.
- Por seu tempo, energia e esforço, você receberá uma recompensa... 1BTC.
- Uma vez que uma **transação** é adicionada à blockchain, ela não pode ser alterada ou revertida.

**6.** Acompanhe o saldo de suas moedas: Ao longo da atividade, acompanhe o saldo de suas moedas contando as moedas em sua carteira digital.

**7.** Discuta com seus colegas de classe e professor os conceitos-chave aprendidos.



*Capítulo #8*





# *Capítulo #9*



## ***Por que o valor intrínseco do Bitcoin vai além da superfície***

**9.0** Por que o Bitcoin?

**9.1** O Futuro do Bitcoin

**9.1.1** O Efeito Lindy

**9.2** Usando o Bitcoin para Mais do que Apenas Dinheiro Digital

**9.3** Os Desafios

**9.3.1** O Ambiente Regulatório para o Bitcoin

**9.3.2** Compreendendo o Consumo de Energia da Mineração de Bitcoin

**9.4** Os Riscos

**9.5** Negociação e Investimento em Bitcoin



# *Por que o valor intrínseco do Bitcoin vai além da superfície*

## **9.0 Por que o Bitcoin?**

O **Bitcoin** é um agente transformador no mundo financeiro, especialmente em partes do mundo onde o sistema bancário tradicional é ineficaz. Em comunidades carentes, os bancos tradicionais muitas vezes não estão dispostos a atender às necessidades das pessoas devido aos altos custos de conformidade impostos por regulamentações. Como resultado, uma parcela significativa da população fica sem acesso a serviços financeiros essenciais. Além disso, as remessas transfronteiriças para países como El Salvador não apenas são caras, mas também demoram muito tempo. As taxas associadas a essas transações e a demora no processamento podem ser devastadoras para aqueles que dependem desses fundos para suas necessidades diárias. Além disso, as pessoas em comunidades sem acesso a serviços bancários não conseguem acessar investimentos e ativos para proteger-se contra a inflação, o que aumenta ainda mais a insegurança financeira. Diante dessas questões, o **Bitcoin** oferece uma solução que aborda as necessidades imediatas dessas comunidades. Ele permite a transferência rápida e eficiente de fundos, sem a necessidade de intermediários e a um custo muito menor. Além disso, oferece uma maneira para as pessoas em comunidades sem acesso a serviços bancários armazenarem valor e se protegerem contra a inflação.

## **9.1 O Futuro do Bitcoin**



"A hiperbitcoinização" é um futuro teórico em que o **Bitcoin** se torna a moeda dominante em escala global. Isso significaria que o bitcoin seria utilizado por todos, em todos os lugares e para tudo - desde comprar café até pagar contas e até mesmo adquirir uma casa.

O crescente interesse pelo **Bitcoin** por parte de bilionários, países e governos destaca o impacto potencial de sua adoção generalizada na economia e na sociedade. Aqui estão alguns dos benefícios de um mundo com hiper-bitcoinização:

**1. Uma Revolução no Mercado de Remessas:** O mercado de remessas envolve a transferência de fundos de uma parte para outra, muitas vezes atravessando fronteiras internacionais. Apesar da redução dos custos, as remessas continuam sendo relativamente caras em comparação com transferências bancárias domésticas, especialmente para quantias menores. O **Bitcoin** tem o potencial de revolucionar o mercado de remessas, reduzindo os custos quase a zero por meio de seu protocolo de camada 2, a **Rede Lightning**. A Lightning Network oferece transações rápidas e de baixo custo, sendo adequada para o mercado de remessas e abordando os altos custos e outros desafios associados às remessas, como tempos lentos de liquidação e restrições de horário comercial.

**2. Um Futuro de Autossuficiência:** Um futuro de autossuficiência é aquele em que os indivíduos têm controle total sobre sua própria identidade digital e ativos. Isso pode levar a uma maior inclusão financeira, privacidade e segurança, e aumentar o valor atribuído à privacidade nas transações.



**3. Mudanças na Política Monetária:** Se o **Bitcoin** se tornasse amplamente adotado, poderia desafiar a capacidade dos governos de controlar a oferta monetária por meio de ferramentas tradicionais de política monetária, levando a mudanças na gestão e implementação da política monetária. Isso também poderia aumentar a inclusão financeira, a igualdade e as oportunidades, além de reduzir a capacidade dos governos e das instituições financeiras de manipular a economia.

**4. Uma Reserva de Valor Confiável:** A escassez digital do **Bitcoin** faz dele uma reserva de valor confiável, o que poderia incentivar mais pessoas a usá-lo como meio de poupança para o futuro.

**5. Transparência e Rastreabilidade Aprimoradas:** O registro à prova de adulteração e imutável de todas as **transações** na blockchain pode aumentar a transparência e a responsabilidade em diversas indústrias e setores.

**6. Melhoria da Segurança Cibernética:** A estrutura descentralizada do Bitcoin o torna menos vulnerável a ataques hackers e violações de dados, melhorando a segurança geral.

**7. Redução da Pegada de Carbono e Promoção de Energias Renováveis:** Ao tornar o processo de mineração de bitcoin mais sustentável e ecologicamente correto, os mineradores podem ajudar a reduzir sua pegada de carbono e promover o uso de fontes de energia renovável. Isso está alinhado com importantes considerações ambientais, sociais e de governança (ESG).

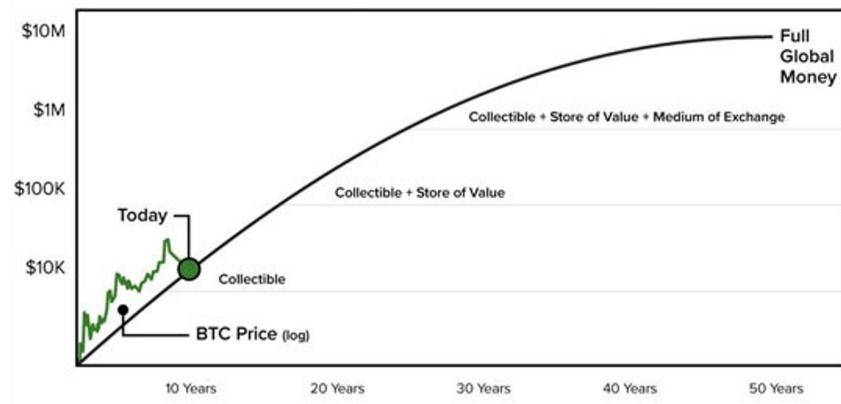
## 9.1.1 O Efeito Lindy



O Efeito Lindy é uma teoria simples que afirma que quanto mais tempo algo existe, maior a probabilidade de continuar existindo no futuro. Essa teoria pode ser aplicada a muitas coisas, incluindo o **Bitcoin**.

O **Bitcoin**, uma moeda digital descentralizada que existe desde 2009, é um exemplo perfeito do Efeito Lindy em ação. Apesar de enfrentar inúmeros desafios ao longo dos anos, incluindo mudanças tecnológicas, violações de segurança e regulamentações governamentais, o Bitcoin continuou a crescer em popularidade e foi adotado por um número cada vez maior de empresas como meio de pagamento.

### Passando no Teste do Tempo



# *Por que o valor intrínseco do Bitcoin vai além da superfície*

Uma das principais razões para a longevidade e uso contínuo do **Bitcoin** é sua natureza descentralizada. Isso significa que ele opera como um sistema financeiro seguro e transparente, sem a necessidade de intermediários, o que o torna atraente para pessoas que valorizam a privacidade e o controle financeiro. Além disso, a capacidade do **Bitcoin** de funcionar como uma reserva segura de valor também contribuiu para sua crescente popularidade e aceitação.

Outro fator que contribui para a longevidade do **Bitcoin** é sua resistência a mudanças e competição. Alterações nas regras de consenso da rede requerem que a maioria dos usuários concorde com a atualização, tornando difícil alcançar o consenso e levando apenas às atualizações que a maioria esmagadora dos participantes da rede concorda em implementar. Além disso, apesar da existência de muitas criptomoedas concorrentes, nenhuma delas foi capaz de igualar a longevidade do **Bitcoin** ou alcançar o mesmo nível de efeitos de rede.

A taxa de hash do **Bitcoin** tem aumentado exponencialmente ao longo dos anos e a distribuição da mineração também está se tornando mais ampla. O número de usuários que ingressam na **Rede Bitcoin** também aumentou em taxa exponencial, com uma estimativa de 140-190 milhões de usuários agora fazendo parte dela. Esses fatores, combinados com sua popularidade e utilidade contínuas, sugerem que o **Bitcoin** provavelmente continuará sendo usado e confiável no futuro.

## **9.2 Utilizando o Bitcoin para mais do que apenas dinheiro digital**

O **Bitcoin** ganhou popularidade por várias razões além de ser apenas um meio de ganhar dinheiro. Alguns usuários são motivados pela ideia de criar um sistema financeiro livre de controle central, enquanto outros simplesmente desejam se beneficiar financeiramente.

O **Bitcoin** também permite a criação de **artefatos digitais** únicos conhecidos como **inscrições de Satoshi**. Essas inscrições, que podem incluir texto, imagens, vídeos, áudio e software, são armazenadas na **blockchain** do **Bitcoin**, tornando-as imutáveis, seguras e descentralizadas. A identificação única de cada Satoshi é possibilitada por **Ordinais**. Ao contrário dos NFTs tradicionais, essas inscrições não exigem uma infraestrutura ou token separado, o que aumenta ainda mais sua segurança e descentralização.

A combinação de **Bitcoin** e IA pode ser utilizada para várias aplicações, como negociação de criptomoedas, segurança e análise de mercado.

A **rede lightning** do **Bitcoin** tornou possíveis pagamentos financeiros mais rápidos e seguros. Por exemplo, as trocas atômicas permitem que as pessoas troquem uma criptomoeda por outra sem a necessidade de um intermediário. A RSK, uma plataforma construída em cima da **blockchain** do **Bitcoin**, também permite a criação de contratos inteligentes e aplicativos descentralizados, o que abre novas possibilidades para o que pode ser construído em cima do **Bitcoin**.

À medida que essas tecnologias continuam sendo desenvolvidas e aprimoradas, espera-se que coisas emocionantes aconteçam no futuro.



### 9.3 Os Desafios

O **Bitcoin Core** é uma implementação poderosa e amplamente utilizada do protocolo **Bitcoin**. No entanto, existem algumas áreas em que ele poderia ser aprimorado:

**1. Escalabilidade:** À medida que o número de usuários e **transações** na rede cresce, a quantidade de dados que precisa ser armazenada e processada pelos nós pode se tornar bastante grande. Isso pode retardar a validação das **transações** e tornar mais difícil para novos usuários ingressarem na rede.

**2. Privacidade:** Embora as **transações** de **bitcoin** sejam pseudônimas, a blockchain é publicamente acessível, o que significa que é possível para terceiros rastrearem o fluxo de fundos e identificar os usuários. Existem algumas soluções propostas para esse problema, como o uso de **mistura de moedas** e endereços ocultos, mas elas ainda não são amplamente adotadas.

**3. Usabilidade:** Para o usuário médio, o processo de configuração e uso de um nó completo pode ser bastante técnico e intimidador. Simplificar a experiência do usuário e torná-la mais acessível a um público mais amplo poderia ajudar a aumentar a adoção.

**4. Descentralização:** O algoritmo de consenso atual do **Bitcoin** é o Proof-of-Work, que pode ser minerado por fazendas de mineração especializadas e grandes. Isso pode levar a uma concentração de poder de mineração e representar uma ameaça à descentralização e segurança do sistema.

**5. Segurança:** Embora o **Bitcoin Core** seja de código aberto, o que significa que seu código pode ser auditado por qualquer pessoa, ainda é possível introduzir bugs ou vulnerabilidades no código. Auditorias e melhorias contínuas na segurança do software podem ajudar a proteger os usuários de possíveis ataques. Por exemplo, se um atacante conseguisse gerar uma chave privada que corresponda a uma grande quantidade de bitcoins, ele poderia roubar esses bitcoins.

Em geral, embora o **Bitcoin Core** seja um software sólido, o desenvolvimento e a pesquisa contínuos são essenciais para abordar essas áreas de melhoria e garantir que a rede permaneça segura, descentralizada e amplamente adotada.

#### 9.3.1 O Ambiente Regulatório do **Bitcoin**

O mercado de criptomoedas tem enfrentado inúmeros desafios nos últimos anos, incluindo o colapso da FTX em 2022 e a queda das stablecoins TerraUSD e LUNA no mesmo ano, resultando em perdas significativas e uma queda na confiança dos investidores. Os riscos associados ao investimento em criptomoedas incluem volatilidade, dificuldade na avaliação de ativos, riscos de custódia, ativos não registrados e provedores operando fora dos quadros regulatórios e regulamentações imprevisíveis.

A regulamentação das criptomoedas, incluindo o **Bitcoin**, tem sido um tema de debate entre governos e reguladores financeiros em todo o mundo. Enquanto alguns proibiram as criptomoedas, outros buscam regulá-las de forma a equilibrar a inovação e a proteção ao consumidor. O presidente da SEC dos EUA, Gary Gensler, afirmou recentemente que a regulamentação do mercado de criptomoedas

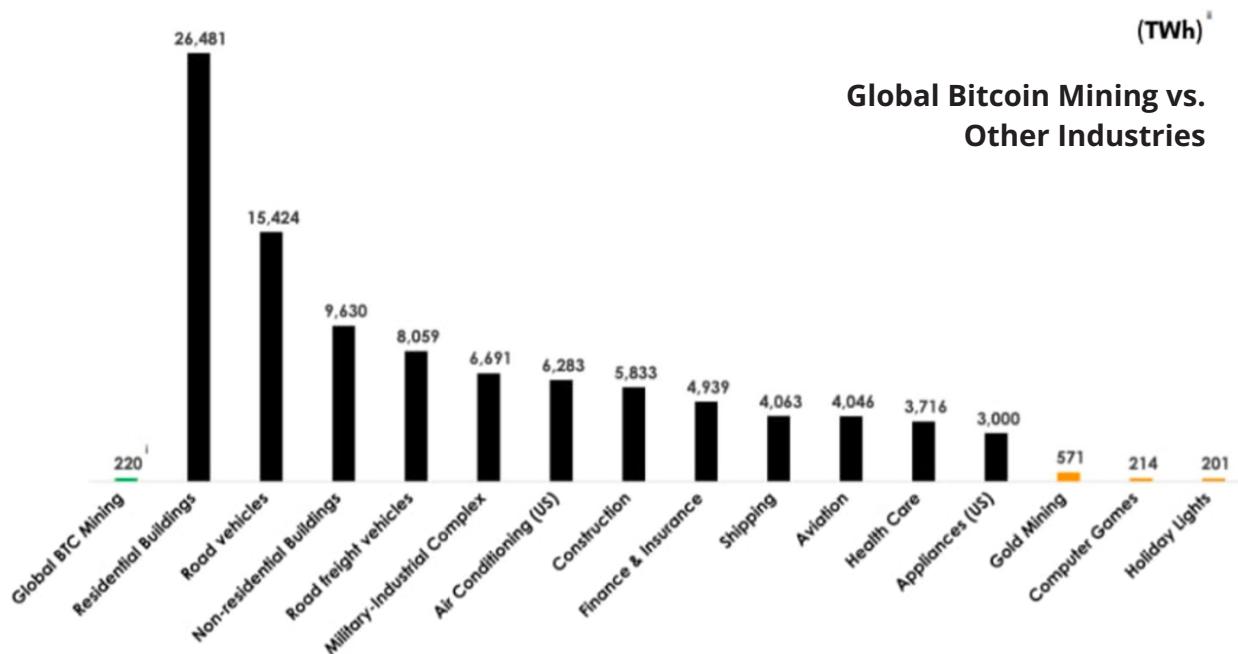
# Por que o valor intrínseco do Bitcoin vai além da superfície

está se aproximando e que o **Bitcoin** será considerado uma mercadoria. De acordo com a SEC, muitos tokens no mercado têm os principais atributos de títulos e estarão sujeitos à jurisdição da SEC, enquanto o **Bitcoin** está sob a supervisão da Commodity Futures Trading Commission (CFTC) como uma mercadoria. A SEC ainda tem trabalho a fazer para introduzir leis abrangentes que protejam os investidores, e essa decisão do presidente da SEC é vista como positiva por alguns investidores, levando à expectativa de preços gradualmente crescentes. Apesar da atual volatilidade do mercado, alguns investidores veem isso como uma oportunidade de compra e acreditam no futuro das moedas digitais como uma forma de dinheiro sem fronteiras, descentralizada, à prova de adulteração e inconfiscável.

## 9.3.2 Compreender o Uso de Energia na Mineração do **Bitcoin**

A mineração do **Bitcoin** consome muita energia, cerca de 79 terawatts-hora por ano. No entanto, isso não significa necessariamente que seja um desperdício de energia ou prejudicial ao meio ambiente. A mineração do **Bitcoin** pode ajudar a utilizar a capacidade de energia não utilizada, especialmente em lugares remotos ou inacessíveis. Além disso, a maior parte da mineração do Bitcoin é feita com energia renovável, como hidrelétrica, solar, eólica e geotérmica. Isso ajuda a tornar a produção e a pesquisa dessas fontes de energia mais lucrativas. Além disso, a mineração do Bitcoin proporciona segurança para a rede do Bitcoin, permitindo que as pessoas tenham acesso a um dinheiro seguro e acessível.

No entanto, é importante observar que o consumo de energia é determinado pela competição entre os mineradores, não pelo número de transações. O processo de validação de assinaturas digitais, que é uma pequena parte da mineração, consome energia mínima. O consumo de energia na mineração do **Bitcoin** é alto, mas não é tão alto quanto em outras indústrias, como o sistema financeiro tradicional ou a mineração e reciclagem de ouro. Os mineradores também estão cada vez mais utilizando fontes de energia limpa e renovável, como energia geotérmica e hidrelétrica, para alimentar suas operações de mineração.





A chave para reduzir o impacto ambiental é impulsionar a demanda por energia verde, e à medida que a indústria cresce, isso está levando à inovação na produção de energia limpa e à diminuição da poluição. É importante ressaltar também que a fonte de energia utilizada pelos mineradores tem um grande impacto ecológico. Conforme a tecnologia e a indústria evoluem, cada vez mais mineradores estão utilizando fontes de energia renovável, como hidrelétrica, solar e eólica, o que reduz significativamente o impacto ambiental.

#### 9.4 Os Riscos

O **Bitcoin** pode oferecer grande liberdade, mas é importante lembrar que com grande poder vem grande responsabilidade. Existem riscos envolvidos no uso do **bitcoin**, portanto, é essencial entender esses riscos e tomar medidas proativas para proteger seus fundos.

- 1. Volatilidade:** O valor do **bitcoin** pode ser altamente volátil e pode mudar muito em um curto período de tempo, o que pode levar a perdas significativas para os investidores.
- 2. Falta de regulamentação:** O **Bitcoin** não é regulamentado por governos ou instituições financeiras, o que significa que há pouca supervisão para proteger os consumidores.
- 3. Riscos de segurança:** As exchanges e carteiras de Bitcoin podem estar sujeitas a invasões e roubo, o que pode resultar na perda de fundos para os usuários.
- 4. Golpes:** Existem muitos golpes relacionados ao **Bitcoin** que podem levar à perda de fundos para os investidores.
- 5. Atividades ilícitas:** O **Bitcoin** tem sido usado para atividades ilegais, como lavagem de dinheiro e compra de bens ilegais na dark web.
- 6. Falta de compreensão:** O **Bitcoin** é complexo e pode ser difícil de entender para a pessoa comum, o que pode levar a decisões equivocadas e perdas potenciais.
- 7. Falta de aceitação:** O **Bitcoin** não é amplamente aceito como meio de pagamento, o que limita sua utilidade na vida cotidiana.
- 8. Riscos técnicos:** O **Bitcoin** está sujeito a riscos técnicos, como bugs e erros, que podem levar a problemas e potencialmente a perda de valor.
- 9. Computação quântica:** A computação quântica poderia potencialmente comprometer a segurança do **Bitcoin** ao quebrar a criptografia usada para proteger **transações** e carteiras.



A **computação quântica** é uma forma de realizar cálculos computacionais que é diferente do funcionamento da maioria dos computadores atualmente. Em vez de usar apenas estados "ligado" e "desligado" como os computadores tradicionais, os computadores quânticos usam "**qubits**" que podem estar em muitos estados ao mesmo tempo. Isso faz com que os computadores quânticos possam ser potencialmente muito mais rápidos em certos tipos de cálculos do que os computadores regulares.

# *Por que o valor intrínseco do Bitcoin vai além da superfície*

**10. Ameaças Digitais:** Hackers podem explorar a sua conexão com a internet para acessar suas **chaves privadas** e dados sensíveis, o que inclui hackear carteiras de software, clicar em links maliciosos e cair em golpes de spyware.

**11. Golpes de Engenharia Social:** Golpistas podem manipulá-lo para confirmar **transações** fingindo ser agentes de atendimento ao cliente ou criando uma falsa sensação de confiança, portanto, é importante ter cautela e não compartilhar sua frase de recuperação.

**12. Assinatura Cega:** A falta de transparência pode levar a uma assinatura cega, na qual você concorda com **transações** sem entender completamente os detalhes, por isso é importante se informar sobre os golpes mais recentes e escolher uma carteira que exiba todos os detalhes da **transação**.

**13. Um ataque de 51%** é uma ameaça potencial à segurança da **Rede Bitcoin** e ocorre quando um único minerador ou grupo de mineradores controla mais de 50% do poder computacional total ou taxa de hash da rede. Isso permite que eles assumam o controle da rede e potencialmente manipulem o blockchain, seja impedindo a adição de novas **transações** ou modificando **transações** a seu favor.

Se um atacante conseguisse realizar com sucesso um ataque de 51%, eles poderiam realizar gastos duplos de **bitcoin**, o que significa que poderiam gastar o mesmo bitcoin mais de uma vez. Isso lhes permitiria efetivamente roubar bitcoins ou cometer fraudes na rede. No entanto, executar um ataque de 51% é extremamente difícil e custoso, pois exigiria o controle de uma quantidade significativa de poder computacional, e os custos envolvidos em obter tal poder poderiam superar quaisquer ganhos potenciais do ataque.

É importante ressaltar que a **Rede Bitcoin** nunca foi atacada com sucesso dessa maneira, mas a possibilidade de um ataque de 51% está sempre presente, e isso destaca a importância de garantir que a rede permaneça descentralizada e segura.

Para proteger sua segurança no **Bitcoin**, use uma carteira offline, leia todos os detalhes da **transação** e continue se informando sobre as ameaças mais recentes. Não permita que a ignorância e uma falsa sensação de confiança comprometam seus ativos suados.

Embora o risco da computação quântica para a segurança do **Bitcoin** seja real, é importante lembrar que ainda é uma ameaça especulativa e incerta quanto ou se ela se tornará realidade. Um ataque de 51% ao **Bitcoin** é uma preocupação, mas seria caro e não muito benéfico para o atacante. Métodos de ataque mais eficientes e econômicos, como DDoS, seriam mais prováveis para um ator racional buscando cometer fraude.

## **9.5 Negociar e investir em **bitcoin****

Quando se trata de investir em criptomoedas, o **bitcoin** é a escolha segura e confiável, e aquela que está alinhada com os valores e princípios de um futuro descentralizado.

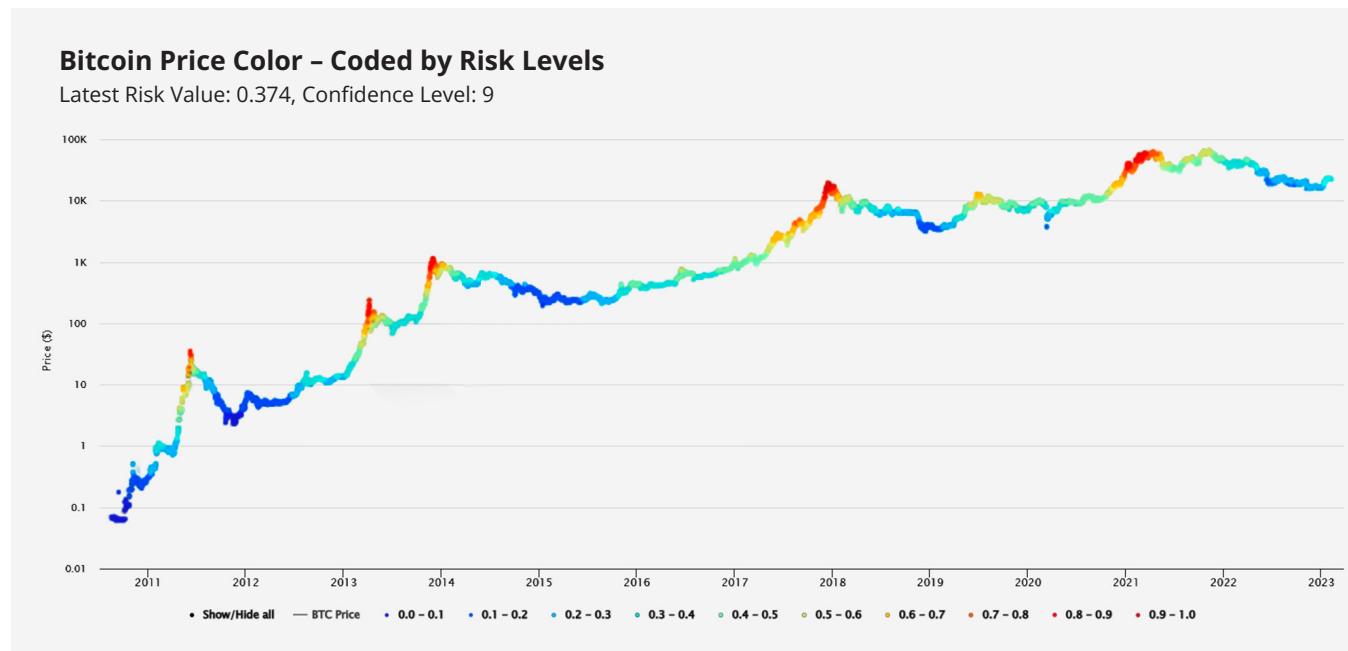


**Tendências de mercado** se referem à direção geral em que o mercado está se movendo. Uma tendência de alta ocorre quando o mercado está em uma trajetória ascendente, enquanto uma tendência de baixa ocorre quando o mercado está em uma trajetória descendente. Isso geralmente está associado ao otimismo dos investidores e à expectativa de que os preços continuem a subir. Em contraste, uma tendência de baixa ocorre quando o mercado está em uma trajetória descendente, caracterizada por máximas e mínimas mais baixas. Isso geralmente está associado ao pessimismo dos investidores e à expectativa de que os preços continuem a cair.

A análise técnica não é uma ciência perfeita, e o desempenho passado nem sempre é indicativo de resultados futuros. Ela deve ser usada em conjunto com outras formas de análise, como análise fundamentalista e sentimento de mercado, para tomar decisões de negociação e investimento informadas.

O gráfico de **Métrica de Risco**, criado por Benjamin Cohen, é uma maneira rápida e intuitiva de entender o sentimento do mercado e avaliar possíveis oportunidades de compra ou venda de bitcoin. Esse gráfico exibe o preço dos ativos e atribui um valor codificado por cores para representar o risco associado a esse preço. Os valores de risco variam de 0 a 1, com cores vermelhas mais escuras indicando maior risco e cores azuis mais escuras indicando menor risco.

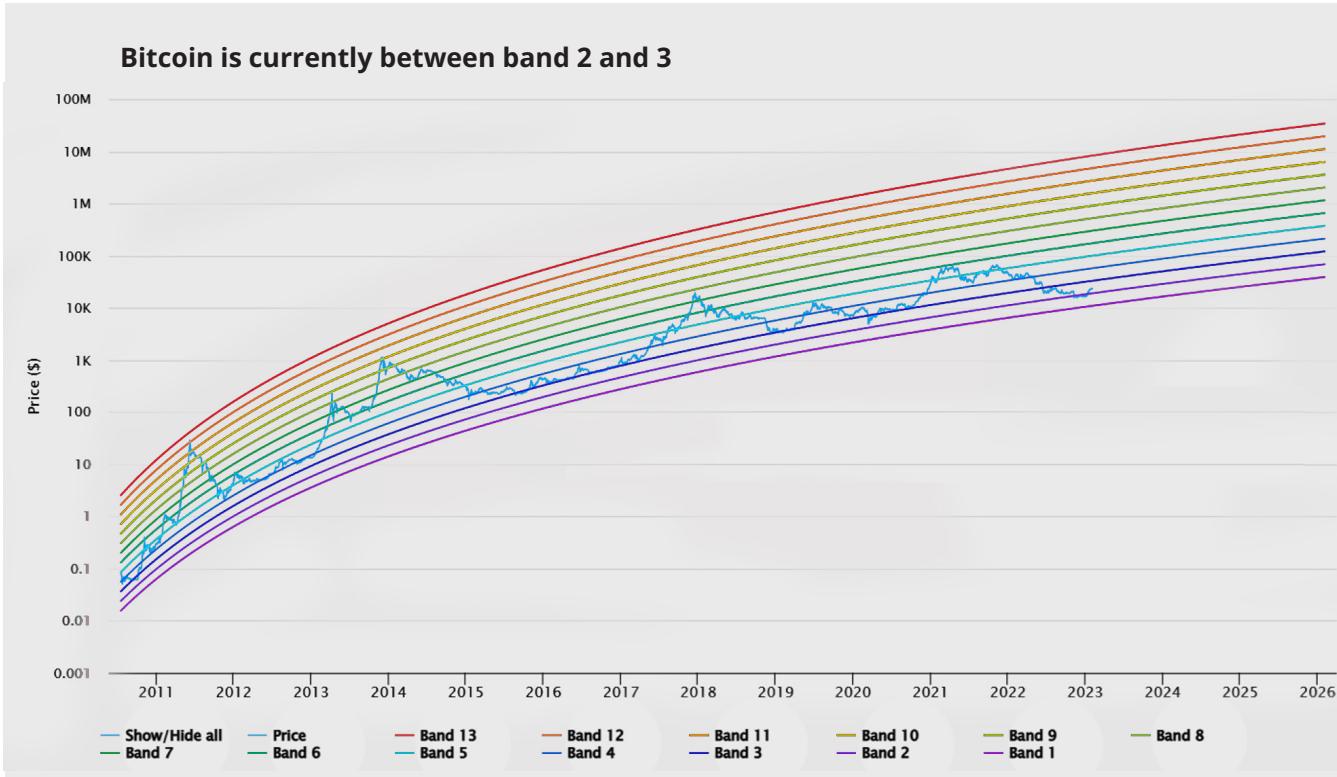
O objetivo da **Métrica de Risco** não é prever os topes ou fundos do mercado, mas sim identificar áreas que possam ser atraentes para compra ou venda no longo prazo. Uma pontuação de baixo risco sugere que o bitcoin pode estar subvalorizado e pode representar uma oportunidade de compra, enquanto uma pontuação de alto risco sugere que ele pode estar sobrevalorizado e pode representar uma oportunidade de venda.



O **preço de mercado logarítmico** é um método de visualização dos movimentos de preço de um ativo, como o bitcoin, ao longo do tempo. Essa abordagem utiliza uma escala logarítmica no eixo y para melhor refletir o crescimento exponencial que frequentemente ocorre nos preços dos ativos.

# Por que o valor intrínseco do Bitcoin vai além da superfície

O preço de mercado logarítmico está sendo usado para acompanhar os movimentos de preço do bitcoin ao longo do tempo e identificar possíveis picos e zonas de acumulação. Os ciclos de mercado mencionados no exemplo são períodos de aumento e queda de preço, e as faixas arco-íris são usadas para ilustrar a magnitude relativa desses movimentos de preço.



O preço de mercado logarítmico pode ser útil para identificar zonas de acumulação potenciais, ou períodos em que o preço pode estar relativamente baixo e oferecer uma boa oportunidade de compra. No exemplo, as zonas entre a faixa 3 e 4 são identificadas como bons períodos de acumulação para os ciclos de mercado 3 e 4.



Os **ciclos de mercado** no **Bitcoin** se referem ao padrão recorrente de crescimento e contração em seu preço e atividade de mercado. Eles são caracterizados por períodos de especulação e hype, seguidos por correção e consolidação. Alguns analistas argumentam que os ciclos estão fortemente correlacionados aos eventos de halving.

É importante ressaltar que, embora o preço de mercado logarítmico possa fornecer informações valiosas, ele é apenas uma das muitas ferramentas que podem ser usadas para analisar tendências de mercado e movimentos de preços, e deve ser usado em conjunto com outros métodos de análise para formar uma compreensão mais completa do mercado. Além disso, as condições de mercado estão em constante mudança, e o desempenho passado não é uma garantia de resultados futuros.



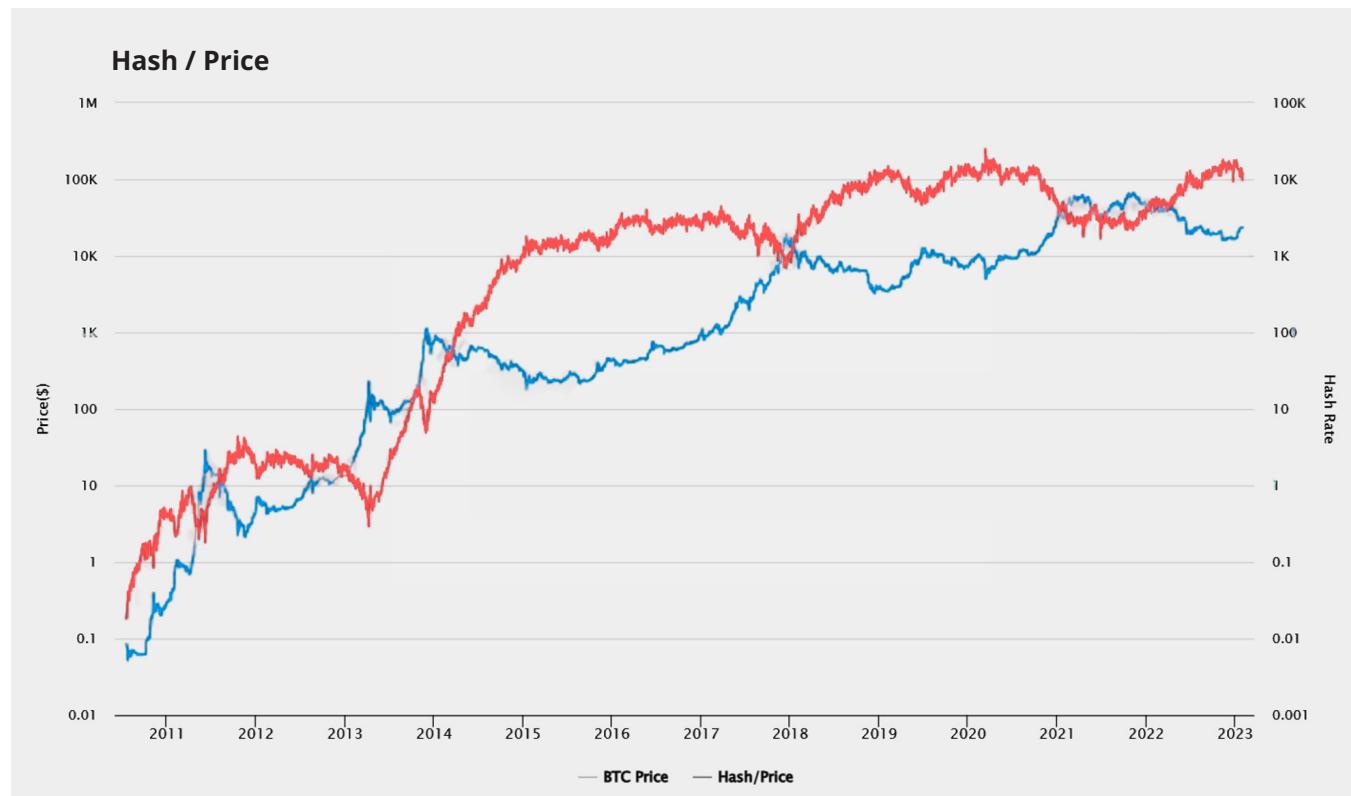
## Capítulo #9

A **relação Hash/Preço** e a relação Preço/Hash são métricas usadas para comparar o crescimento do preço do **Bitcoin** e o crescimento do poder computacional da **Rede Bitcoin**, ou taxa de hash. Essas métricas são utilizadas para entender a relação entre os dois e como mudanças em um podem afetar o outro.

Quando o preço do **bitcoin** aumenta em um ritmo mais rápido do que a taxa de hash, a relação Hash/Preço diminui e a relação Preço/Hash aumenta. Isso significa que o preço do **bitcoin** está crescendo mais rapidamente do que o poder computacional da rede, o que pode indicar um aumento na demanda por **bitcoin**.

No entanto, próximo aos picos locais, quando o preço do **bitcoin** está aumentando rapidamente, pode haver quedas repentinhas na relação Hash/Preço. Isso ocorre porque o crescimento do preço ultrapassa o crescimento do poder computacional, levando a uma diminuição na relação Hash/Preço.

Por outro lado, se tanto a taxa de hash quanto o preço do **bitcoin** diminuem ou aumentam nas mesmas taxas relativas, as relações permanecerão constantes. Isso significa que o poder computacional da rede e o preço do **Bitcoin** estão crescendo na mesma proporção.



# Por que o valor intrínseco do Bitcoin vai além da superfície

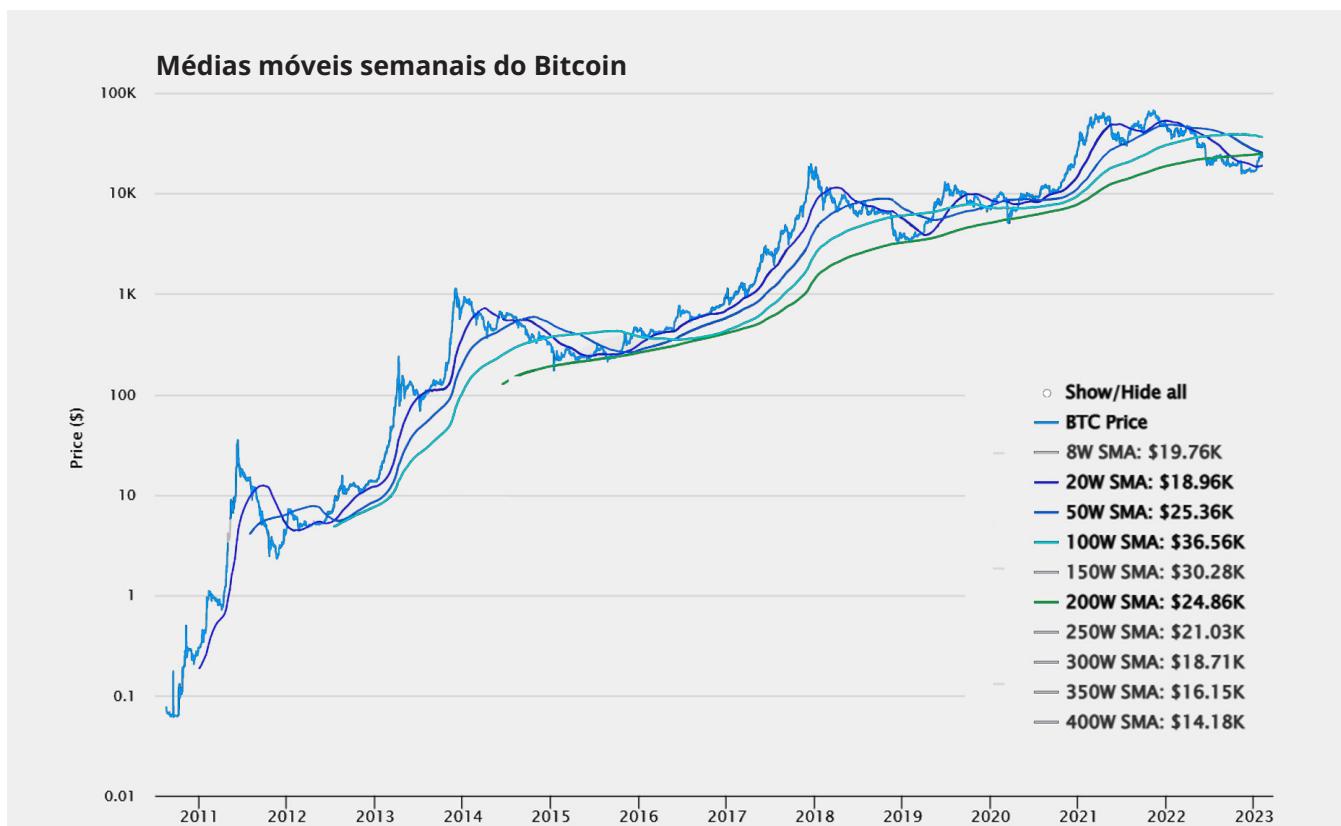
Se a taxa de hash da **Rede Bitcoin** está aumentando em um ritmo mais rápido do que o preço do **bitcoin**, a relação Hash/Preço aumentará e a relação Preço/Hash diminuirá. Isso pode indicar que a rede está se tornando mais segura e mais capaz de processar transações, o que pode ter um impacto positivo no preço do **bitcoin** no futuro.

As **linhas de tendência** são usadas para identificar uma tendência atual no mercado. Elas são formadas ao conectar dois ou mais pontos de preço e são usadas para indicar um nível de suporte ou resistência. Uma linha de tendência inclinada para cima é considerada altista, enquanto uma linha de tendência inclinada para baixo é considerada baixista.

As **médias móveis** são usadas para suavizar a volatilidade do preço de um ativo ao longo de um período específico. Elas são calculadas somando os preços de fechamento de um ativo ao longo de um número específico de períodos e, em seguida, dividindo pelo número de períodos. Uma média móvel pode ser usada para identificar a direção de uma tendência e também pode ser usada para gerar sinais de compra e venda. Fazer uma média de custo em dólar (DCA) abaixo de médias móveis de curto prazo, como a média móvel de 100 semanas e 50 semanas, pode fornecer mais pontos de entrada, mas pode resultar em perdas a curto prazo.



O método do **dollar-cost averaging** (DCA) é uma estratégia de investimento em que uma quantia fixa de dinheiro é investida regularmente em um determinado ativo, independentemente do preço.





O objetivo do DCA é reduzir o impacto da volatilidade do mercado em uma carteira de investimentos, distribuindo as compras ao longo do tempo, em vez de comprar tudo de uma vez.

- Por exemplo, um investidor pode decidir investir \$100 em um ativo de criptomoeda a cada mês. Se o preço do ativo estiver alto, o investidor comprará menos unidades, e se o preço estiver baixo, o investidor comprará mais unidades. Ao longo do tempo, essa abordagem pode resultar em um custo médio menor por unidade do ativo, reduzindo assim o impacto das flutuações de preço de curto prazo.

O **DCA** pode ser usado em uma variedade de investimentos, incluindo ações, títulos e commodities, e é frequentemente recomendado para indivíduos que estão começando a investir e desejam minimizar o risco da volatilidade do mercado.

É importante destacar que o DCA não garante lucro ou protege contra perdas em um mercado em declínio, e deve ser combinado com uma pesquisa completa e análise de mercado. Além disso, os investidores devem considerar seus próprios objetivos financeiros e tolerância ao risco ao decidir sobre a melhor estratégia de investimento.

Indicadores como o **RSI** e o **MACD** são usados para identificar condições de sobrecompra e sobrevenda, bem como possíveis mudanças de tendência. O RSI compara a magnitude dos ganhos recentes com as perdas recentes para determinar as condições de sobrecompra e sobrevenda. O MACD é calculado subtraindo a média móvel exponencial de 26 períodos (EMA) da EMA de 12 períodos e, em seguida, traçando uma EMA de 9 dias do resultado. Ele é usado para identificar mudanças no momentum e na tendência.

É importante observar que essas métricas são apenas uma das muitas ferramentas que podem ser usadas para analisar tendências de mercado e movimentos de preços, e devem ser usadas em conjunto com outros métodos de análise para obter uma compreensão mais completa do mercado. Além disso, as condições de mercado estão em constante mudança, e o desempenho passado não garante resultados futuros.



## *Capítulo #10*



# *De Bits ao Bitcoin: Montando o Quebra-Cabeça*

**10.0** Apenas Alguns Fatos, Algumas Piadas... e a Linguagem Específica.

**10.1** Submissão do Projeto Final Mi Primer Bitcoin e Diretrizes de Avaliação.



# De Bits ao Bitcoin: Montando o Quebra-Cabeça

## 10.0 Apenas alguns fatos, algumas piadas... e o vocabulário

**CRYPTOCURRENCY SLANG**

**WHALE**  
Someone who owns a lot of cryptocurrency – usually 5% of any given coin.

"THIS GUY BOUGHT BITCOIN BACK IN 2011, AND NOW HE'S A HUGE WHALE"

**HODL**  
A by-word for not panicking. HODL began with a typo for 'hold' and came to mean hold on for dear life (i.e. don't sell your coins).

"KEEP CALM AND HODL DURING THIS SLUMP; YOU'LL BE REWARDED WITH BIG GAINS"

**BAG HOLDER**  
Someone who is holding onto a currency that drops in price to the point of being worthless.

"THEY CALL ME A BAG HOLDER, BUT I'M SURE IT'S GOING TO GO BACK UP..."

**REKT**  
A phrase from the gaming world, it means when a cryptocurrency plummets in value and wipes out investors.

"LET'S HAVE A MOMENT OF SILENCE FOR ALL THOSE #REKT ON MARGIN CALLS"

**FUD**  
An acronym for 'fear, uncertainty and doubt' which are especially common negative rumours spread in the media.

"DON'T LISTEN TO THOSE RUMORS: THEY'RE JUST SPREADING FUD"

**BEARWHALE**  
A cross between a whale and a bear – that is, a trader who believes prices will fall. A BearWhale's sell-off can temporarily flatten the whole market.

"THAT BEARWHALE CAUSED INVESTORS A BIT OF HAVOC"

**TO THE MOON!**  
The rallying cry of Bitcoin investors, it's the most common way to celebrate when a coin is on the up and up.

"BITCOIN JUST HIT \$50,000! TO THE MOON!"



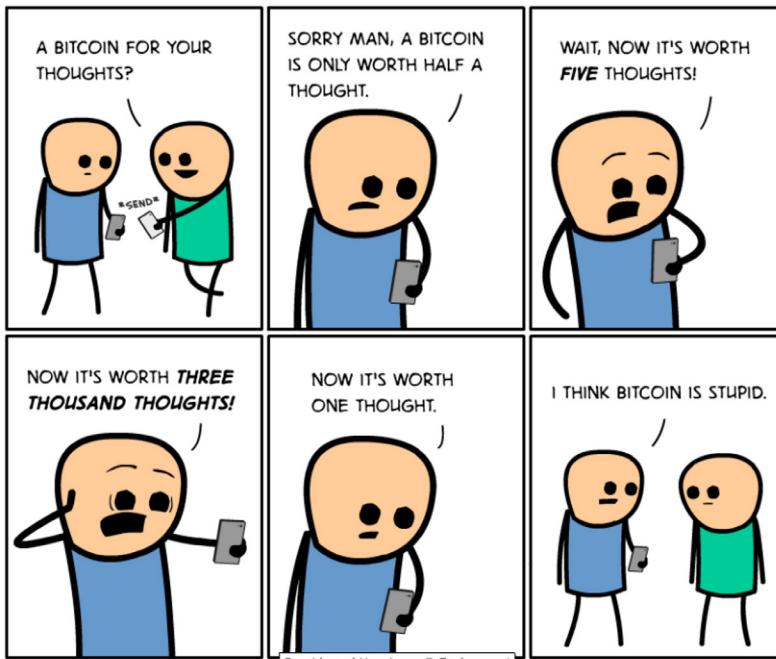
A **Rede Bitcoin** é mais poderosa do que 500 supercomputadores juntos.



**Reembolsos** não são possíveis em transações de **bitcoin**.



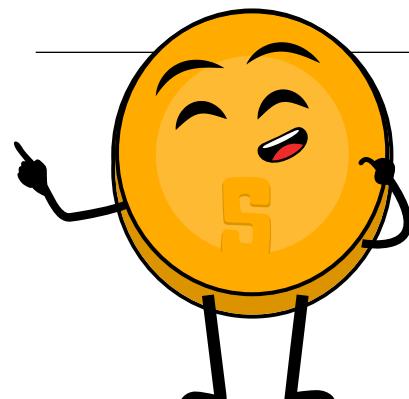
## Capítulo #10



Quantos mineradores são necessários para trocar uma lâmpada?

- Um milhão.

***Um minerador para trocá-la e 999.999 mineradores correndo em círculos para determinar quem fará isso.***



# De Bits ao Bitcoin: Montando o Quebra-Cabeça

## 10.1 Envio do Projeto Final Meu Primeiro Bitcoin e Diretrizes de Avaliação

### Introdução:

O projeto final do curso **Mi Primer Bitcoin** consiste em um ensaio de 1 a 2 páginas intitulado “Por que Bitcoin?”, no qual você será solicitado a explicar o que é o **Bitcoin**, como ele funciona e de que maneira ele está transformando o mundo hoje.

### Requisitos:

- O ensaio deve ter no mínimo 1 página e no máximo 2 páginas, com espaçamento duplo e fonte tamanho 12.
- O ensaio deve ser escrito em português correto e estar livre de erros gramaticais e ortográficos.
- O ensaio deve incluir introdução, desenvolvimento e conclusão.

### Tópicos a serem abordados:

- Explique o que é o **Bitcoin** e sua história.
- Explique como o **Bitcoin** funciona, incluindo suas características principais, como descentralização, transações e mineração.
- Discuta pelo menos duas maneiras pelas quais o **Bitcoin** está mudando a forma como o mundo opera hoje. Forneça exemplos e evidências para apoiar sua resposta.

### Projeto Alternativo:

Para aqueles que preferem uma experiência prática, você pode participar da Atividade Final (Simulador de Blockchain Bitcoin) usando a *Ferramenta de Simulação de Blockchain Bitcoin*:

<https://www.bitcoinsimulator.tk/>.

Aqui você criará uma nova carteira e receberá uma chave privada, que permitirá que você mine um bloco, assine transações, crie uma blockchain privada e execute um ataque de 51%.



### Critérios de Avaliação:

Os seguintes critérios serão usados para avaliar seu projeto final:

- Clareza na explicação do que é o **Bitcoin** e como ele funciona.
- Uso de exemplos e evidências para apoiar sua resposta.
- Coerência e organização do ensaio.
- Uso adequado de gramática e ortografia.
- Relevância e profundidade da discussão sobre o tópico.



**Envio:**

O projeto final deve ser enviado em formato Word ou PDF por e-mail ao instrutor do curso até a data limite especificada no programa do curso. Submissões tardias não serão aceitas.

**Conclusão:**

O projeto final é uma oportunidade para você mostrar seu entendimento sobre o **Bitcoin** e seu impacto no mundo. O ensaio deve demonstrar sua capacidade de analisar e sintetizar informações e apresentá-las de forma clara e concisa. Boa sorte com seu projeto final!





# *Recursos Adicionais*



# Recursos Adicionais

## *Por que usar o bitcoin?*

- **Filme “Hard Money” (30 minutos):**

Este filme explora a história do dinheiro e como o bitcoin se encaixa no sistema financeiro atual. Ele aborda os problemas das moedas fiduciárias tradicionais e como o bitcoin oferece uma solução.

- **“Why Bitcoin” por Wiz:**

Este artigo fornece uma visão geral dos benefícios de usar o bitcoin como moeda e reserva de valor. Destaca a natureza descentralizada do bitcoin e como isso permite maior liberdade financeira e segurança.

- **“The Bullish Case for Bitcoin” por Vijay Boyapati:**

Este artigo argumenta por que o bitcoin é um ativo valioso e por que tem potencial para se tornar uma moeda global dominante. O autor aborda os aspectos técnicos e econômicos do bitcoin que o tornam uma sólida oportunidade de investimento.

- **“Why Bitcoin Matters” por Aleks Svetski (1 hora):**

Este vídeo aborda a importância do bitcoin como um ativo digital descentralizado e como pode impactar o sistema financeiro atual. O palestrante explora o potencial do bitcoin para trazer liberdade financeira às pessoas ao redor do mundo.

## *O que é o Bitcoin?*

- **“What Is Bitcoin” por Greg Walker:**

Este artigo oferece uma explicação abrangente do que é o bitcoin, incluindo sua história, tecnologia e como difere das moedas tradicionais.

- **“Bitcoin - The Genesis” por RT (30 minutos):**

Este vídeo aborda a criação e os primeiros dias do bitcoin. Ele explora as motivações do misterioso criador, Satoshi Nakamoto, e como o conceito de bitcoin evoluiu.

- **“Understanding Bitcoin” por BJ Dweck (1 hora e 30 minutos):**

Este vídeo oferece uma explicação detalhada dos aspectos técnicos do bitcoin e como ele funciona. O palestrante aborda tópicos como blockchain, mineração e a natureza descentralizada do bitcoin.

## *Aprendizado Adicional*

- **The Bitcoin Standard (1 hora e 40 minutos):**

Este audiolivro explora o contexto econômico e histórico que levou à criação do bitcoin. Ele aborda os benefícios de uma moeda descentralizada e o potencial do bitcoin para se tornar um padrão global.

- **“Intro to Bitcoin Austrian Thought” (1 hora):**

Esta palestra em áudio aborda a Escola Austríaca de economia e como ela se relaciona com o conceito de bitcoin. Fornece uma análise profunda dos princípios econômicos por trás do bitcoin e como eles se alinham ao pensamento austríaco.



<b>Alex Gladstein</b>	Check Your Financial Privilege
<b>Alex Swan</b>	Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications
<b>Amanda Cavaleri</b>	Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide
<b>Anita Posch</b>	Learn Bitcoin: Become Financially Sovereign
<b>Eric Yakes</b>	The 7th Property: Bitcoin and the Monetary Revolution
<b>Jeff Booth</b>	The Price of Tomorrow: Why Deflation is the Key to an Abundant Future
<b>Jimmy Song</b>	The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future
<b>Nik Bhatia</b>	Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies
<b>Robert Breedlove</b>	Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money





# *Glossário*

# Glossário

**Altcoins:** Moedas digitais excluindo o Bitcoin.

**Armazenamento a frio:** Um método de armazenamento de bitcoins offline, longe 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 eficientemente a integridade de grandes conjuntos de dados.

**Assinatura:** Um mecanismo matemático que permite que alguém prove a propriedade de algo.

**Ataque de 51%:** Um tipo de ataque em uma rede blockchain no qual uma única entidade ou grupo controla a maioria do poder de computação da rede, permitindo manipular transações e potencialmente interromper a rede.

**Ativo Digital:** Uma representação digital de valor que pode ser negociada ou usada como reserva de valor, como o Bitcoin.

**Atomic Swap:** Uma troca peer-to-peer de uma criptomoeda por outra sem a necessidade de uma exchange centralizada ou intermediário.

**Autenticação em Dois Fatores (2FA):** Uma medida de segurança que exige dois métodos de autenticação, normalmente uma senha e um código ou dispositivo separado, para acessar uma conta ou concluir uma transação.

**Backup da Carteira:** Uma cópia das chaves privadas e da frase de recuperação/palavras-chave de uma carteira de Bitcoin, que pode ser usada para restaurar o acesso à carteira no caso de perda ou roubo da original.

**Baleia:** Um indivíduo ou organização que possui uma quantidade significativa de criptomoeda, capaz de influenciar os preços de mercado por meio de grandes negociações.

**Bancário Restritivo:** Restrições ou limitações nos serviços bancários ou no acesso a serviços bancários.

**Banco Central (Fed):** Uma instituição de propriedade governamental que gerencia a política monetária de um país.

**Bitcoin:** Uma moeda digital/sistema que permite que as pessoas enviem dinheiroumas para as outras sem usar um banco.

**Blockchain:** Um registro público de todas as transações de Bitcoin que ocorreram.



**Blockchain Privada:** Uma blockchain que é controlada por uma única organização, em vez de ser descentralizada.

**Blockchain Pública:** Uma blockchain aberta para qualquer pessoa participar e verificar transações, tornando-a descentralizada.

**Bloco Órfão:** Um bloco que não é incluído na cadeia principal da blockchain devido a ser invalidado por uma cadeia concorrente mais longa.

**BTC:** A unidade usada para bitcoin. Uma moeda digital que pode ser usada para fazer compras ou ser negociada.

**Carteira:** Um contêiner virtual para bitcoin, semelhante a uma carteira física, que contém chave(s) privada(s) que permitem gastar os bitcoins alocados a ela na blockchain.

**Carteira de criptomoedas:** Um programa de software que armazena chaves privadas e permite aos usuários enviar, receber e gerenciar suas criptomoedas.

**Carteira Multiassinatura (Multisig):** Uma carteira que requer múltiplas assinaturas ou aprovações antes que uma transação possa ser executada, fornecendo segurança e controle adicionais.

**Carteira Online:** Uma carteira de Bitcoin que está conectada à internet, permitindo fácil acesso aos bitcoins.

**Centralização:** A concentração de poder ou controle em uma única entidade.

**Cesta de bens:** Uma coleção de bens ou serviços usada para medir as mudanças no custo de vida.

**Chave Privada:** Um dado secreto que comprova o direito de uma pessoa gastar bitcoins de uma carteira específica por meio de uma assinatura criptográfica.

**Chave Pública:** Um identificador único usado para receber bitcoins, derivado da chave privada de um usuário por meio de um processo matemático.

**Chave Pública / Endereço Bitcoin:** Uma senha/número público usado para receber bitcoins.

**Confirmação:** O processo de uma transação sendo processada pela rede e com pouca probabilidade de ser revertida. Os “mineradores” verificam a autenticidade das transações com seu hardware e software de computador. É recomendado esperar pelo menos 6 confirmações para evitar gastos duplos.

**Contrato Inteligente:** Um contrato autoexecutável cujos termos são escritos em código.

# Glossário

**Controles de capital:** Restrições sobre o movimento de dinheiro através das fronteiras.

**Criptografia:** Um ramo da matemática que ajuda a criar sistemas seguros.

**Desbancarizados:** Indivíduos ou comunidades sem acesso a serviços bancários tradicionais.

**Descentralização:** A distribuição de poder e controle em uma rede, em vez de ter uma autoridade central.

**Desvalorização:** A redução no valor de uma moeda, muitas vezes pela redução da quantidade de metal precioso em uma moeda.

**Dívida:** Dinheiro que é devido a outra pessoa.

**Dupla coincidência de desejos:** O fenômeno em que duas partes em uma economia de troca têm o que a outra parte deseja e desejam o que a outra parte tem.

**Endereço da Carteira:** Um identificador único usado para enviar e receber bitcoin na rede Bitcoin, normalmente representado como uma sequência de letras e números.

**Exchange de criptomoedas:** Uma plataforma onde os usuários podem comprar, vender e negociar criptomoedas por outros ativos, como moeda fiduciária ou outras criptomoedas.

**Explorador de blocos:** Uma ferramenta usada para visualizar e explorar a blockchain, permitindo que os usuários vejam blocos individuais, transações e endereços de carteira.

**Fiduciário:** Cujo valor depende somente da confiança a ele dispensada (diz-se de papel-moeda).

**Finanças Descentralizadas (DeFi):** Um movimento dentro da indústria de criptomoedas para criar produtos e serviços financeiros descentralizados que operam em uma blockchain.

**FOMO:** Medo de ficar de fora, um termo usado para descrever a sensação de ansiedade ou arrependimento de que se pode perder uma oportunidade lucrativa no mercado de criptomoedas.

**Frase de Recuperação / Palavra-chave de Restauração:** uma sequência de 12, 18 ou 24 palavras que podem ser usadas para gerar múltiplos pares de chaves privadas e públicas. Elas podem ser usadas para restaurar uma carteira de Bitcoin.

**FUD:** Medo, incerteza e dúvida, um termo usado para descrever rumores ou informações negativas que podem causar pânico ou queda no mercado.

**Função de Hash:** Uma função matemática que recebe dados de entrada de qualquer tamanho e



produz uma string de caracteres de tamanho fixo, comumente usada em criptografia e tecnologia blockchain.

**Gasto duplo:** Quando uma pessoa tenta gastar seu bitcoin para dois destinatários diferentes ao mesmo tempo.

**Hacker Ético (White Hat Hacker):** Um hacker ético que usa suas habilidades para identificar e corrigir vulnerabilidades em sistemas e redes de computadores.

**Hard Fork:** Uma mudança no protocolo do Bitcoin que cria uma nova versão da blockchain, que não é compatível com a versão anterior. (por exemplo, Bitcoin Cash)

**Hardware Wallet:** Um dispositivo físico usado para armazenar chaves privadas e gerenciar criptomoedas, proporcionando segurança aprimorada em relação às carteiras de software.

**HODL:** Um termo usado na comunidade de criptomoedas para descrever a estratégia de manter a posse de criptomoedas a longo prazo, em vez de vendê-las ou negociá-las.

**ID de Transação:** uma sequência de números e letras que mostra os detalhes de uma transferência de bitcoin (como a quantia enviada, os endereços do remetente e do destinatário e a data da transferência) na blockchain do Bitcoin.

**Importações:** Bens e serviços produzidos em outro país e vendidos no mercado doméstico.

**Inflação:** Um aumento no nível geral de preços de bens e serviços em uma economia.

**Leilão:** Um processo pelo qual bens ou ativos são vendidos ao maior licitante.

**Lightning Network:** Um protocolo de pagamento de camada 2 que permite transações mais rápidas e baratas de Bitcoin, utilizando canais fora da cadeia para transações menores.

**Lightweight Node:** Um cliente Bitcoin que armazena apenas uma quantidade limitada de dados da blockchain, em vez de toda a cadeia.

**Livro Razão:** Um registro de transações financeiras.

**Livro-razão Público:** Um banco de dados descentralizado que mantém um registro público de todas as transações na rede Bitcoin.

**Mecanismo de consenso:** Um método usado na tecnologia blockchain para validar transações e garantir a integridade da blockchain.

**Meios de Troca:** Objetos ou sistemas amplamente aceitos em troca de bens e serviços.

# Glossário

**Mineração:** O processo de usar hardware de computador para realizar cálculos matemáticos para a rede Bitcoin, a fim 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.

**Multiassinatura:** Um recurso de segurança que requer mais de uma chave privada para autorizar uma transação de Bitcoin.

**Nó:** Um computador ou dispositivo conectado à rede Bitcoin que participa da verificação e transmissão de transações.

**Nonce:** Um número aleatório adicionado ao cabeçalho de um bloco para criar um hash que atenda ao alvo de dificuldade.

**Oferta e Demanda:** O princípio econômico de que o preço de um bem ou serviço é determinado pela interação da quantidade do bem ou serviço fornecido e a quantidade demandada.

**Oferta Inicial de Moedas (ICO):** Um método de captação de recursos no qual uma nova criptomoeda é vendida para investidores em troca de uma criptomoeda mais estabelecida, como o Bitcoin.

**Oferta Monetária:** A quantidade total de dinheiro em circulação em uma economia.

**Organização Autônoma Descentralizada (DAO):** Uma organização ou rede governada por contratos inteligentes e executada em uma blockchain, sem uma autoridade central ou estrutura de gestão.

**Paper Wallet:** Uma cópia impressa das chaves privadas e públicas de um usuário usadas para armazenar e gerenciar criptomoedas offline.

**Par de Negociação:** Um conjunto de duas moedas ou ativos que podem ser negociados entre si em uma exchange de criptomoedas.

**Peer-to-Peer (P2P):** Uma rede descentralizada na qual os participantes interagem diretamente entre si, em vez de passar por uma autoridade central.

**Pegar (Peg):** Uma taxa de câmbio fixa entre duas moedas, onde uma está vinculada ao valor da outra.

**PIB:** Produto Interno Bruto, o valor total de bens e serviços produzidos em um país em um determinado período de tempo.



**Poder de Compra:** A capacidade do dinheiro de comprar bens e serviços.

**Política Monetária e Fiscal:** As políticas de um banco central e do governo, respectivamente, que influenciam a oferta de dinheiro e as taxas de juros em uma economia.

**Pool de Mineração:** Um grupo de mineradores que trabalham juntos para aumentar suas chances de encontrar novos blocos e ganhar bitcoins.

**Proof of Stake (PoS):** Um mecanismo de consenso usado em algumas redes blockchain que exige que os usuários possuam uma certa quantidade de criptomoeda para participar da validação de transações.

**Proof of Work:** Um mecanismo de consenso que exige que os usuários realizem uma determinada quantidade de trabalho computacional para participar da rede.

**Protocolo de Camada 1:** A camada subjacente de uma rede blockchain que lida com os aspectos fundamentais de consenso, validação de transações e armazenamento de dados.

**Protocolo de Camada 2:** Uma camada secundária construída sobre uma rede blockchain de camada 1, geralmente usada para melhorar escalabilidade, velocidade e funcionalidade.

**Recompensa por bloco:** A quantidade de novos bitcoins que são concedidos aos mineradores por adicionar 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.

**Registro Distribuído:** Um banco de dados que está espalhado por uma rede de computadores, em vez de ser armazenado em um local central.

**Reutilização de endereço:** A prática de usar o mesmo endereço de Bitcoin para várias transações.

**Satoshi:** A menor unidade de Bitcoin, equivalente a 1/100.000.000 de um bitcoin. Ela recebe o nome do criador do Bitcoin, Satoshi Nakamoto.

**Satoshi Nakamoto:** O pseudônimo usado pelo(s) criador(es) anônimo(s) do Bitcoin.

**Satoshis por byte (sat/b):** Uma unidade usada para medir a quantidade de taxa de transação de bitcoin paga por byte de dados de transação.

**SegWit (Testemunha Separada):** Uma atualização do protocolo Bitcoin que muda a forma como os dados são armazenados na blockchain, permitindo maior capacidade e taxas de transação mais baixas.

**Sem Confiança:** Um sistema ou transação que não requer confiança em terceiros ou intermediários, mas sim depende da segurança e transparência da tecnologia subjacente.

**Sidechain:** Uma blockchain que está conectada a outra blockchain, permitindo a transferência de ativos ou informações entre as duas cadeias.

**Sistema Centralizado:** Um sistema no qual o poder ou controle é concentrado em uma única entidade.

**Sistema Descentralizado:** Um sistema no qual o poder ou controle é distribuído entre várias entidades.

**Soft Fork:** Uma mudança no protocolo Bitcoin que é compatível com versões mais antigas do software.

**Stablecoin:** Um tipo de criptomoeda projetada para manter um valor estável, muitas vezes sendo ancorada a uma moeda fiduciária ou 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.

**Taxa de Reserva:** A proporção de depósitos que um banco deve manter como reserva.

**Taxa de Transação:** Uma pequena quantidade de bitcoin paga pelo remetente de uma transação para incentivar os mineradores a incluir a transação em um bloco e adicioná-la à blockchain.

**Temporada de altcoins:** Um período de tempo em que as criptomoedas alternativas experimentam aumentos significativos de preço, frequentemente devido ao aumento do interesse e adoção por investidores.

**Token:** Uma unidade de valor criada em uma blockchain, frequentemente usada para representar um ativo específico ou utilidade dentro de um ecossistema específico.

**Token Não Fungível (NFT):** 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 criar uma representação digital de um ativo ou classe de ativos em



uma blockchain, permitindo a propriedade fracionada e transferibilidade.

**Transação:** A transferência de bitcoin de um endereço para outro na rede Bitcoin.

**Transação em pó:** Uma transação que envia uma quantia muito pequena de Bitcoin que é muito pequena para ser economicamente viável.

**Troca:** A troca de bens e serviços sem o uso de dinheiro.

**Unidade de Conta:** Uma unidade de medida padrão usada para expressar o valor de bens e serviços.

**Valor do Dinheiro ao Longo do Tempo:** O princípio de que o dinheiro tem mais valor no presente do que no futuro.

**Volatilidade:** O grau de variação no preço de um ativo ao longo do tempo.

**Whitepaper:** um relatório que explica o problema e a solução que um projeto de blockchain ou criptomoeda está tentando abordar.

**XBT and BTC:** abreviações para bitcoin.



## ***Por que é importante aprender sobre o Bitcoin?***

### ***1. O que é o **Bitcoin** e como ele funciona?***

O Bitcoin é uma moeda digital descentralizada que opera independentemente de um banco central. Ele permite transações entre pares sem a necessidade de intermediários, tornando-se uma tecnologia revolucionária na indústria financeira. Compreender como ele funciona é crucial para compreender suas possíveis implicações e uso.

### ***2. O que torna o **bitcoin** único e valioso?***

O Bitcoin é único porque opera em uma rede descentralizada, tornando-se resistente à interferência e manipulação governamental. Ele também possui um suprimento finito, limitado a 21 milhões, tornando-se escasso e valioso, assim como o ouro. Aprender sobre essas qualidades ajuda a entender seu potencial como reserva de valor e investimento.

### ***3. Qual impacto o **Bitcoin** pode ter na indústria financeira?***

A ampla adoção do **Bitcoin** tem o potencial de perturbar os sistemas financeiros tradicionais e desafiar o monopólio dos bancos centrais. Também oferece novas oportunidades de investimento e inclusão financeira, especialmente para indivíduos em países com moedas instáveis. Compreender o impacto potencial do Bitcoin na indústria financeira é crucial para qualquer pessoa interessada em finanças e tecnologia.





