

:\$ Scalar School

# Tecnologia Bitcoin

Fundamentos e  
Trilhas de Carreira  
para Desenvolvedoras



PARA TODOS OS CRÍTICOS E NEGADORES

QUE DIZEM QUE O BITCOIN É INÚTIL OU PERIGOSO

O BITCOIN ESTÁ LÁ FORA, TODOS OS DIAS, TODAS AS HORAS, EM ECONOMIAS COLAPSADAS E NOS CANTOS MAIS ESCUROS DO MUNDO, AJUDANDO PESSOAS QUE NINGUÉM MAIS ESTÁ DISPOSTO A AJUDAR. SENDO UM SALVA-VIDAS PARA \*QUALQUER UM\*

O DINHEIRO FIDUCIÁRIO FALHOU TERRIVELMENTE PARA A MAIORIA DAS PESSOAS NA TERRA. NOSSOS SISTEMAS MONETÁRIOS E DE "AJUDA" EXPLORAM E REPRIMEM EM VEZ DE ENTREGAR PROSPERIDADE E LIBERDADE

MAS O BITCOIN ESTÁ, LENTAMENTE E CONSTANTEMENTE, UNINDO, ENRIQUECENDO E LIBERTANDO O MUNDO

—ALEX GLADSTEIN

Dedico esta obra à Human Rights Foundation.

## 1. Por que o Bitcoin Importa

- 1.1 Introdução à Tecnologia Bitcoin
- 1.2 Atributos da Rede Bitcoin
- 1.3 Bitcoin e Direitos Humanos
- 1.4 O Problema dos Generais Bizantinos
- 1.5 Bitcoin Whitepaper
- 1.6 Origens Acadêmicas

## 2. Bitcoin e Criptografia

- 2.1 Blockchain: O Livro Razão do Bitcoin
- 2.2 Regras de Consenso
- 2.3 Modelo de Segurança do Bitcoin
- 2.4 Funções Hash
- 2.5 Chaves Digitais
- 2.6 Assinaturas Digitais
- 2.7 Endereços de Recebimento
- 2.8 Carteiras

## 3. Transações

- 3.1 Inputs, Outputs, UTXOs
- 3.2 SegWit—Segregated Witness e Maleabilidade de Transações
- 3.3 MultiSig: Transações Multi-assinatura (Multisig) no Bitcoin
- 3.4 Bitcoin Script
- 3.5 Miniscript
- 3.6 CoinJoin
- 3.7 Exploradores de Blocos
- 3.8 Taxas de Transação
- 3.9 Prática: Meu Primeiro Bitcoin On-Chain

## 4. Rede P2P

- 4.1 Nós de Bitcoin
- 4.2 Mempool
- 4.3 Mainnet
- 4.4 Regtest
- 4.5 Testnet
- 4.6 Signet
- 4.7 Forks

## 5. Mineração

- 5.1 Energia: Aproveitamento e Desenvolvimento de Infraestrutura
- 5.2 Prova-de-trabalho
- 5.3 Timechain
- 5.4 Oferta Inelástica

- [5.5 Mineração Solo e a Resiliência do Bitcoin](#)
- [5.6 Mineração em Pool](#)
- [5.7 Hardware de Mineração](#)
- [5.8 Ataque de 51%](#)
- [5.9 Stratum V2](#)
- [6. Bitcoin Core](#)
- [7. BIPS—Propostas de Melhoria do Bitcoin](#)
- [8. RPC API do Bitcoin Core](#)
- [9. Lightning Network](#)
  - [9.1 BOLTs—Basics of Lightning Technology](#)
  - [9.2 Canais de Pagamento](#)
  - [9.3 Nós Lightning](#)
  - [9.4 Exploradores de Rede](#)
  - [9.5 Prática: Meu Primeiro Bitcoin na Lightning Network](#)
- [10. Tecnologias de Liberdade](#)
  - [10.1 Cypherpunks](#)
  - [10.2 JoinMarket e Jam](#)
  - [10.3 E-cash—Federated Chaumian Mints](#)
  - [10.4 Nostr](#)
  - [10.5 Value4Value—Valor por Valor](#)
  - [10.6 Democratização da Ciência](#)
  - [10.7 Bitcoin Optech](#)
  - [10.8 The Bitcoin Dev Project](#)
- [11. Carreira em Desenvolvimento de Software Livre e Open Source](#)
  - [11.1 Filosofia do Desenvolvimento Bitcoin](#)
  - [11.2 Desenvolvimento Bitcoin FOSS](#)
  - [11.3 Chaincode Labs](#)
  - [11.4 Summer of Bitcoin](#)
  - [11.5 Scalar School](#)
- [12. Bitcoin é Para Todos](#)
- [13. Powered By Bitcoin](#)
- [14. Notas Finais](#)
  - [14.1 Isenção de Responsabilidade](#)
  - [14.2 Contato](#)
  - [14.3 Posfácio](#)

# 1. Por que o Bitcoin Importa

*“Uma nova tecnologia misteriosa surge, aparentemente do nada, mas na verdade é o resultado de duas décadas de intensa pesquisa e desenvolvimento por pesquisadores quase anônimos. Idealistas políticos projetam visões de libertação e revolução sobre ela; elites do establishment despejam desprezo e desdém sobre ela. Por outro lado, tecnólogos – nerds – ficam fascinados por ela. Eles veem um enorme potencial e passam suas noites e fins de semana mexendo com ela. Eventualmente, produtos, empresas e indústrias mainstream emergem para comercializá-la; seus efeitos tornam-se profundos; e mais tarde, muitas pessoas se perguntam por que sua poderosa promessa não era mais óbvia desde o início. De que tecnologia estou falando? Computadores pessoais em 1975, a Internet em 1993 e – acredito – o Bitcoin em 2014.”*

—Marc Andreessen, Fundador da Netscape e conhecido capitalista de risco, 2014

## 1.1 Introdução à Tecnologia Bitcoin

Uma maneira de pensar no Bitcoin é como uma sequência de transações atômicas. Cada transação é autenticada por um remetente com a solução para um quebra-cabeça criptográfico anterior que foi armazenado como um script, por meio da linguagem de programação Bitcoin Script.

A nova transação é bloqueada para o destinatário com um novo quebra-cabeça criptográfico que também é armazenado como um script, cujo novo dono é portador da solução para destravar transferências futuras.

Cada transação é registrada no livro razão global público e imutável, a blockchain. Somente o proprietário das chaves privadas que geraram o endereço onde estão os bitcoin consegue destrancar o valor para ser movido adiante.

Consideramos Bitcoin com letra maiúscula quando representamos a rede, o sistema em si. O bitcoin com letra minúscula é a moeda, os valores transferidos por meio deste sistema.

## 1.2 Atributos da Rede Bitcoin

**Segurança:** A rede Bitcoin é segura desde que mais de 50% dos nós participantes sejam honestos.

**Confiabilidade:** O estado da rede é mantido por todos os nós, que distribuem a cópia do livro-razão entre eles.

**Descentralização:** Todos os nós da rede replicam os registros de transações, garantindo a distribuição dos dados.

**Transações Peer-to-Peer:** Permite transações diretas entre usuários, sem a necessidade de intermediários ou autoridades centrais.

**Acessibilidade:** Qualquer pessoa pode ingressar ou sair da rede, validar transações ou minerar novas moedas a qualquer momento.

**Transparência:** Todas as transações são verificáveis publicamente e estão disponíveis para todos os operadores da rede.

**Ausência de Permissões:** Não são necessárias credenciais, identificações ou autorizações para participar da rede.

**Globalidade:** A rede opera sem restrições geográficas e pode ser acessada de praticamente qualquer lugar do mundo.

**Resistência à Censura:** Não há uma autoridade central que possa impedir a transferência de fundos entre usuários.

**Neutralidade:** A rede é indiferente a quem, o quê, quando, onde ou por que você está enviando e recebendo bitcoin.

**Oferta Inelástica e Distribuída:** A geração de bitcoins é autorregulada por algoritmos matemáticos e modelos de teoria dos jogos, garantindo que o processo seja justo e previsível.

## 1.3 Bitcoin e Direitos Humanos

Apesar da volatilidade do Bitcoin no curto prazo e da necessidade de letramento digital para seu uso pleno, o Bitcoin oferece benefícios significativos para os direitos humanos e a inclusão financeira, especialmente em contextos onde as alternativas tradicionais são limitadas ou ineficazes. Veja por que o Bitcoin importa para os direitos humanos.

### Alternativa ao sistema atual

A maior parte dos dramas da humanidade, como guerras infinitas, se devem ao fato de o dinheiro ser manipulável, impresso arbitrariamente, e alocado para tais fins sem o consentimento da população geral. O Bitcoin resolve isso com sua política monetária transparente e oferta inelástica definida pela comunidade a nível de código.

### Inclusão financeira para não bancarizados

Aproximadamente 1,7 bilhões de pessoas no mundo não têm acesso a serviços bancários tradicionais. O Bitcoin oferece uma alternativa viável, pois só é necessário acesso à internet e um dispositivo móvel para participar da rede financeira. Em regiões como a África subsaariana, onde a infraestrutura bancária é limitada, o uso do Bitcoin está crescendo como uma forma de acessar serviços financeiros.

### Liberdade financeira e proteção contra regimes opressores

Em alguns países, governos autoritários podem congelar contas bancárias ou confiscar bens arbitrariamente. O Bitcoin oferece uma forma de proteger ativos contra essas ações.

Em países com instabilidade política ou financeira, como a Venezuela, indivíduos têm usado Bitcoin para proteger seu patrimônio da hiperinflação e controle governamental.

### Facilitação de remessas internacionais com menores taxas

As remessas tradicionais de dinheiro, especialmente para países em desenvolvimento, podem ter taxas elevadas e demorar dias para serem processadas. Bitcoin permite transferências

quase instantâneas e com taxas muito menores. Trabalhadores migrantes que enviam dinheiro para suas famílias podem usar Bitcoin para evitar altas taxas de serviços como Western Union, aumentando a quantidade de dinheiro que chega aos destinatários finais.

### **Controle pessoal sobre os recursos financeiros**

Com Bitcoin, indivíduos têm controle total sobre seus fundos, sem necessidade de intermediários. Isso garante maior autonomia e segurança em suas transações financeiras. Em situações de crise, como desastres naturais ou conflitos, onde bancos podem estar inacessíveis, as pessoas ainda podem acessar e usar seus fundos com Bitcoin.

### **Transparência nas transações e segurança contra fraudes**

A blockchain do Bitcoin é um registro público imutável de todas as transações, o que reduz a possibilidade de fraude e aumenta a transparência. Organizações de direitos humanos podem utilizar Bitcoin para receber doações de forma transparente, permitindo que doadores vejam exatamente como os fundos são usados.

### **Incentivo ao uso de energias renováveis e desenvolvimento de comunidades**

A mineração de Bitcoin incentiva a construção de infraestrutura elétrica em locais pouco desenvolvidos ou de difícil acesso. O processo tem incentivado o uso de fontes de energia renovável e inovação em eficiência energética, pois os mineradores buscam formas mais baratas e sustentáveis de energia para maximizar seus lucros. Geralmente fontes limpas de energia podem entrar em períodos de preço negativo, quando a produção excede a demanda.

Nesses momentos, é possível ligar as mineradoras de Bitcoin para usar a energia excedente e regular os grids, aproveitando a energia e evitando prejuízos. A mineração de Bitcoin pode atuar como uma carga flexível, absorvendo o excesso de energia durante picos de produção e desligando-se quando a demanda aumenta.

### **Método de poupança**

O Bitcoin é o melhor investimento de todos os tempos, e a melhor forma de preservar o poder de compra no longo prazo enquanto as moedas fiduciárias são diluídas pela inflação. É uma ferramenta de poupança de longo prazo extremamente eficaz, pois é um ativo digital escasso. Ademais, a maioria das pessoas não tem acesso ao mercado de ações para preservar e multiplicar sua renda.

### **Dinheiro físico e privacidade de transações estão desaparecendo**

O que acontece quando toda nossa atividade financeira é rastreável por uma entidade centralizada, e perdemos a privacidade financeira do dinheiro físico? Que poderes os governos e corporações ganham quando trocamos nossa privacidade e liberdade por conveniência? Cada transação financeira revela enorme quantidade de informações sobre você. Isso acaba habilitando o controle por corporações e governos, censura das suas transações, e a viabilização da vigilância e a engenharia social.

**O Bitcoin tem sido considerado uma das principais ferramentas de garantia dos direitos humanos da atualidade.** Ele é, de fato, uma ferramenta de liberdade, sendo especialmente útil em países ditoriais com controle financeiro rígido das contas bancárias de seus habitantes.

O Bitcoin oferece aos humanos um dinheiro que não pode ser censurado pelas autoridades, que não pode ser desvalorizado pelos governos, que não pode ser monopolizado pelas corporações, que não pode ser facilmente monitorado em massa, que não pode ser parado pelas fronteiras e que pode ser acessado por qualquer pessoa. E é por isso que o Bitcoin é importante para os direitos humanos.

*"Poucas pessoas estão olhando para a intersecção entre liberdade monetária e liberdade real."*—Alex Li, Bitcoin Development Lead, Human Rights Foundation

*"O Bitcoin é colaborativo, descentralizado, e se alinha muito bem com o movimento dos direitos humanos."*—Alex Gladstein, CSO, Human Rights Foundation

*"O Bitcoin é terrível para ditadores."*—Alex Gladstein, CSO, Human Rights Foundation

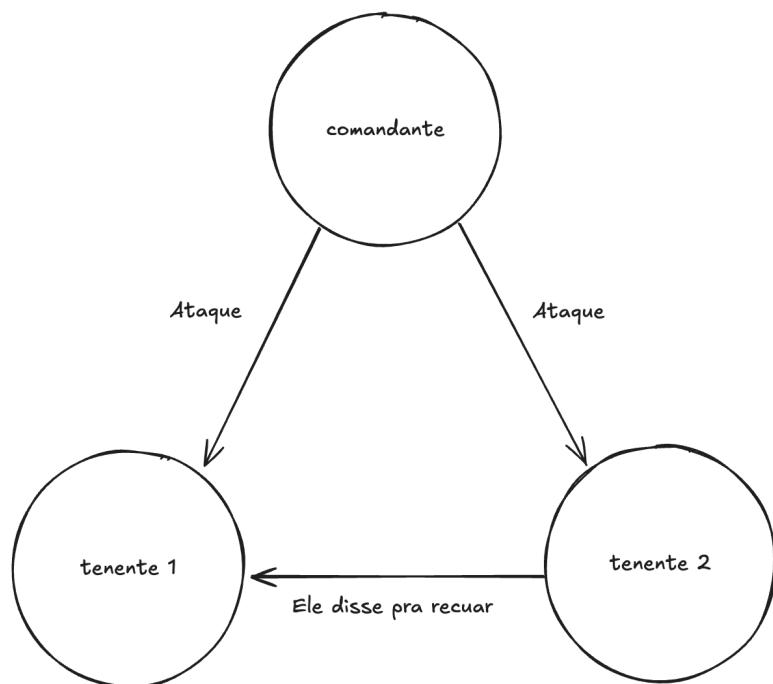
Leitura recomendada: [Verifique Seu Privilégio Financeiro.](#)

## 1.4 O Problema dos Generais Bizantinos

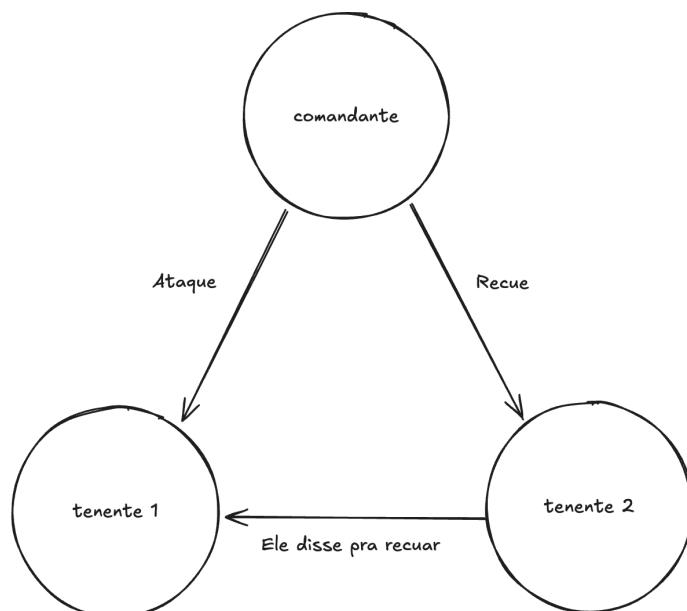
**O Bitcoin surgiu como solução, criada por Satoshi Nakamoto para o [Problema dos Generais Bizantinos](#).**

O Problema dos Generais Bizantinos é um problema clássico na ciência da computação na área de tolerância a falhas, especialmente no campo da computação distribuída e teoria dos sistemas distribuídos. Foi proposto pela primeira vez por Marshall Pease, Robert Shostak e Leslie Lamport em 1982, "expressado de forma abstrata em termos de um grupo de generais do exército bizantino acampados com suas tropas ao redor de uma cidade inimiga."

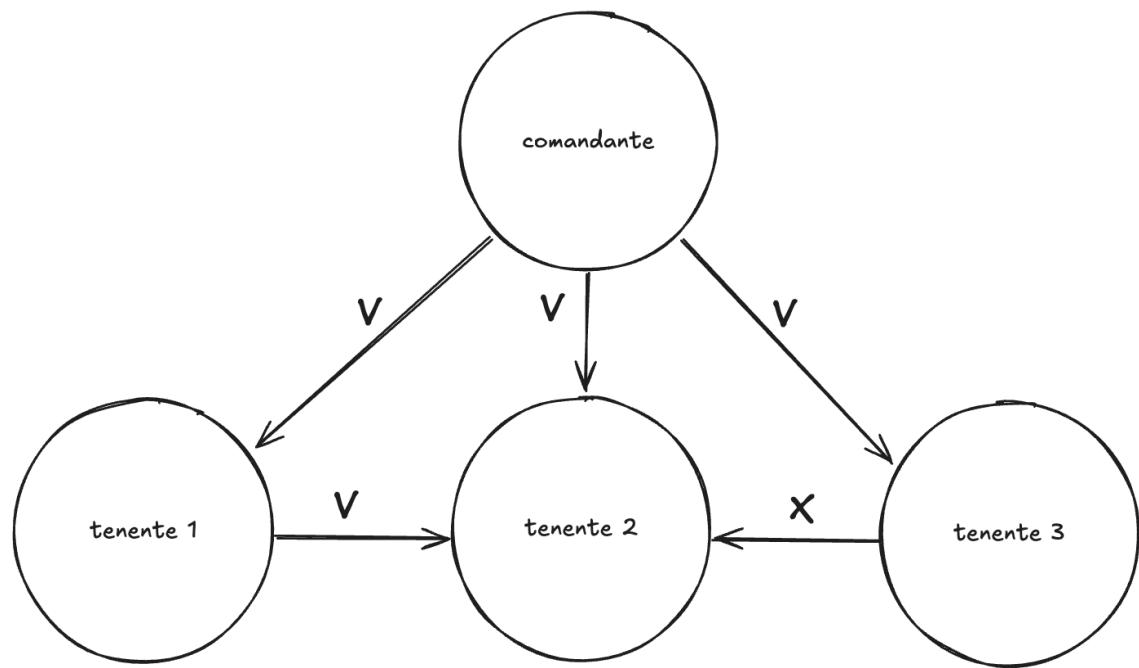
Neste cenário, um traidor (seja o Comandante ou o Tenente) impede o grupo de alcançar o consenso. Em um livro razão financeiro, pense no traidor como uma parte maliciosa que visa facilitar transações fraudulentas. À medida que o número de partes no sistema aumenta, o número de canais de comunicação (e oportunidades para desconfiança) aumenta exponencialmente. Imagine a complexidade de se construir um consenso com milhares ou milhões de partes envolvidas. Os esquemas a seguir são atribuídos a [Lamport, Shostak, Pease, 1982](#)



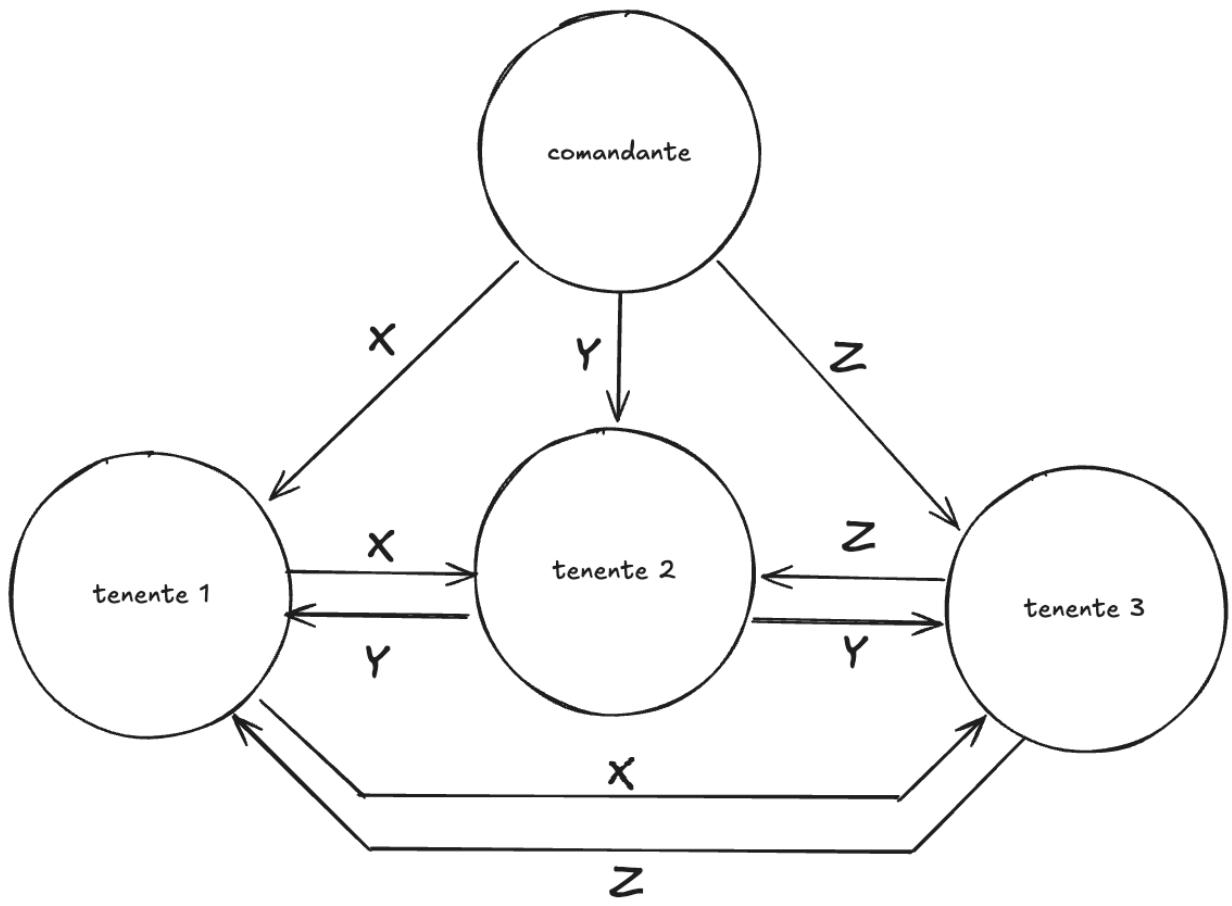
O tenente 2 é traidor



O comandante é traidor



Algoritmo OM(1) — O tenente 3 é traidor



A solução para o Problema dos Generais Bizantinos é composta pela combinação do trabalho probabilístico (tentativa e erro) de descoberta do nonce que gera um hash igual ou abaixo do nível de dificuldade definido no processo de mineração + a seleção da cadeia com a maior prova-de-trabalho cumulativa, ou seja, o maior poder computacional empregado para formá-la.

O Bitcoin resolve também o problema do gasto duplo, garantindo que um ativo digital (bits) não seja duplicável ou passível de copy-paste.

## 1.5 Bitcoin Whitepaper

### **Definição de Whitepaper**

Um whitepaper é um documento informativo e técnico que apresenta a visão, metodologia e detalhes de um projeto ou tecnologia, servindo como um guia para entender seus fundamentos e objetivos.

O whitepaper do Bitcoin, intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System", em Português Brasileiro, "[Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer](#)" foi lançado por Satoshi Nakamoto em 31 de outubro de 2008. Ele foi divulgado em uma lista de discussão sobre criptografia chamada "[The Cryptography Mailing List](#)" no site metzdowd.com, detalhando a estrutura e funcionamento de um sistema de pagamento eletrônico descentralizado.

Este documento introduziu os conceitos inovadores que revolucionaram o sistema financeiro global e que foram usados de formas diferentes para o desenvolvimento de milhares de outras criptomoedas e tecnologias blockchain.

**Tudo começou com o Bitcoin, que ainda é o projeto mais importante, mais descentralizado e o mais robusto candidato a sistema financeiro e de reserva de valor global sem uma autoridade central.** Muitos consideram todas as outras criptomoedas como tentativas centralizadas de falsificar o Bitcoin.

De fato, governos estão migrando seus sistemas financeiros para CBDCs (Central Bank Digital Currencies), sistemas inspirados na tecnologia do Bitcoin, mas que permitem um estado de extrema vigilância e controle orwelliano, pois operam por meio de um controle centralizado.

Como o Bitcoin é de código livre e aberto, qualquer pessoa pode copiar as ideias dele e construir novos sistemas. **Porém, somente o Bitcoin derivado da primeira versão de Satoshi Nakamoto é um sistema de dinheiro eletrônico ponto-a-ponto.**

O software Bitcoin foi lançado por Satoshi Nakamoto em 3 de janeiro de 2009. Nesse dia, Satoshi minerou o bloco gênesis, o primeiro bloco da blockchain do Bitcoin, marcando oficialmente o início da rede Bitcoin.

### **Mensagem no Bloco Gênesis**

No bloco gênesis, Satoshi Nakamoto deixou uma mensagem significativa: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

00000000	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	....;fíýz{.^zC,>
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.È.À~ŠQ2:Ý,a
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_IÝÝ...-+
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	.....ÿÿÿÿM.ÿÿ
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Times 03/
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ..ò.
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠý°þUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gn q0..`Ö`(`a9.
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaë.aþ`IÖ`?Lí8Ä
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.å.Á.p`8M+o..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00 00	ŠLp+kñ._-....

Esta mensagem é uma referência à manchete do jornal britânico "The Times" de 3 de janeiro de 2009, que destacava a crise financeira global e o iminente segundo resgate dos bancos pelo governo. A inclusão desta mensagem foi uma crítica implícita ao sistema financeiro tradicional e uma declaração de intenções sobre a necessidade de um sistema financeiro alternativo, descentralizado e resistente a manipulações e intervenções governamentais.

## **Consequências Negativas de um Segundo Resgate a Bancos**

## **Desigualdade econômica**

Resgates bancários frequentemente beneficiam grandes instituições financeiras e suas partes interessadas, enquanto a população em geral arca com os custos através de impostos e austeridade. Isso pode aumentar a desigualdade econômica, pois os recursos públicos são usados para salvar entidades privadas ricas.

## Risco moral

Resgates incentivam os bancos a tomar riscos excessivos, sabendo que serão salvos em caso de falência. Esse comportamento arriscado pode levar a práticas irresponsáveis, aumentando a probabilidade de futuras crises financeiras. [Oxford Academic](#)

## Aumento do déficit público

O uso de recursos públicos para resgates aumenta a dívida governamental, o que pode resultar em medidas de austeridade, cortes em serviços públicos essenciais e aumentos de impostos, afetando diretamente a qualidade de vida da população. [Kansas City Fed](#)

## Erosão da confiança pública

A percepção de que os bancos são favorecidos pelo governo pode erodir a confiança do público no sistema financeiro e na justiça econômica, gerando descontentamento social e uma possível perda de legitimidade das instituições. [Kansas City Fed](#)

### Impactos sociais

A impressão de dinheiro para financiar resgates pode levar à inflação, reduzindo o poder de compra da população. Medidas de austeridade e cortes em serviços públicos podem resultar em desemprego e uma crise econômica mais ampla, afetando diretamente a vida das pessoas.

Essas consequências ilustram como resgates bancários podem ter impactos profundos e duradouros na sociedade, exacerbando desigualdades e criando riscos adicionais para a estabilidade econômica a longo prazo.

## 1.6 Origens Acadêmicas

O Bitcoin tem um [pedigree acadêmico](#), sendo uma solução inovadora e criativa aos sistemas financeiros tradicionais. **É a culminação de décadas de pesquisa em criptografia e sistemas distribuídos.**

O conceito de Bitcoin integra descobertas e teorias de pesquisadores em criptografia, como David Chaum, e em sistemas distribuídos, como Nick Szabo e Wei Dai. Todos esse autores **enfatizaram a importância da privacidade e do anonimato** nas transações financeiras, conceitos que foram incorporados no design do Bitcoin.

Saiba mais sobre a origem do Bitcoin  
<https://nakamotoinstitute.org/literature/>

March 9, 1993: [A Cypherpunk's Manifesto](#)—Eric Hughes

November 1998: [b-money](#)—Wei Dai

August 1, 2002: [Hashcash - A Denial of Service Counter-Measure](#)—Adam Back

October 31, 2008: [Bitcoin: A Peer-to-Peer Electronic Cash System](#)—Satoshi Nakamoto

August 29, 2017: [O Pedigree Acadêmico do Bitcoin](#)—Arvind Narayanan and Jeremy Clark

O Bitcoin importa porque representa a primeira solução prática para criar uma moeda digital descentralizada, segura e sem a necessidade de intermediários. Ele resolve problemas fundamentais na segurança das transações digitais, como o gasto duplo e a necessidade de confiança em uma entidade central.

A tecnologia promove a liberdade financeira, a privacidade e a capacidade de transferir valor globalmente sem restrições, tornando-se uma alternativa revolucionária aos sistemas financeiros tradicionais.

## 2. Bitcoin e Criptografia

### 2.1 Blockchain: O Livro Razão do Bitcoin

Uma blockchain (corrente de blocos) é um banco de dados distribuído que armazena informações de maneira segura e transparente, funcionando como um livro-razão digital onde os dados são organizados em blocos interligados criptograficamente.

Cada bloco contém um registro de transações, um carimbo de data/hora e uma referência ao bloco anterior, garantindo a imutabilidade dos dados, pois qualquer alteração em um bloco afetaria toda a cadeia.

Para testemunhar e armazenar a blockchain do Bitcoin, o ponto de partida é baixar o software cliente de referência do Bitcoin—Bitcoin Core. Este software faz o download da blockchain completa, o livro-razão de todas as transações na história do Bitcoin. Cada cliente completo de Bitcoin armazena o registro completo de todas as transações de bitcoin desde sempre, sem um registrador central, apenas um conjunto de cópias distribuídas entre todos os clientes.

Após o download e validação do histórico da blockchain, surge a questão da sincronização: como manter essas cópias da blockchain sincronizadas umas com as outras e alcançar um consenso distribuído sem uma entidade central definitiva? Quando um cliente recebe mensagens conflitantes sobre uma transação, qual delas deve aceitar? A solução está na stack de tecnologias criptográficas e regras de consenso usadas no sistema.

Baixar o software cliente do Bitcoin não é obrigatório para usar bitcoin. Um simples software de carteira gratuito no celular é suficiente para começar. No entanto, instalar e manter nós é recomendado para usuários que desejam verificar suas transações de maneira privada e participar do processo de consenso. Nós completos também são ferramentas importantes para desenvolvedores e usuários avançados.

Leitura recomendada: <https://nakamotoinstitute.org/mempool/bitcoin-not-blockchain/>

### 2.2 Regras de Consenso

As regras de consenso definem o que o software do Bitcoin faz, e como. Estas regras são fundamentais para manter a integridade e a segurança da rede. Elas são usadas para garantir que todos os participantes da rede concordem sobre o estado atual do livro-razão distribuído (blockchain). Aqui estão as principais regras de consenso do Bitcoin:

#### **Prova de Trabalho (Proof of Work—PoW)**

O Bitcoin utiliza um mecanismo de consenso chamado Prova de Trabalho, que requer que os mineradores resolvam um problema matemático computacionalmente difícil para adicionar um novo bloco à blockchain. O primeiro minerador a resolver o problema ganha o direito de

adicionar o bloco e receber a recompensa do bloco em bitcoin, juntamente com as taxas de transação dos Bitcoins transferidos no bloco.

### **A cadeia com mais poder de hash acumulada**

A regra geral para a aceitação de uma cadeia de blocos é que os nós sempre consideram a cadeia de maior dificuldade cumulativa ou onde mais recursos computacionais foram gastos como a cadeia válida. Isso garante que a maioria do poder de processamento da rede concorda com o histórico de transações.

### **Limite de tamanho de bloco**

Cada bloco no Bitcoin é limitado a um tamanho máximo (atualmente 1 MB de tamanho de base com a possibilidade de até aproximadamente 4 MB de peso de bloco, devido ao SegWit). Isso limita o número de transações que podem ser incluídas em um bloco, afetando a taxa de transferências por segundo que a rede pode realizar.

### **Regras de formatação de transação**

As transações devem seguir um formato específico e incluir uma assinatura digital válida para serem consideradas válidas. Elas devem também se referir a saídas de transações anteriores não gastadas (UTXOs—Unspent Transaction Outputs).

### **Emissão de novos bitcoin**

A recompensa por bloco para os mineradores é reduzida pela metade a cada 210.000 blocos (aproximadamente a cada quatro anos) em um evento conhecido como "halving". Isso controla a emissão de novos bitcoins e é uma regra fundamental para a política monetária predefinida do Bitcoin. O dia do halving é um grande momento de celebração para a comunidade bitcoin.

Essa política monetária também inclui um limite máximo de 21 milhões de bitcoins que poderão ser emitidos. Esse teto absoluto garante que o Bitcoin seja uma moeda deflacionária, protegendo-a contra a inflação excessiva. Quando o último bitcoin for minerado, previsto para acontecer por volta do ano 2140, não haverá mais emissões, e os mineradores serão incentivados exclusivamente pelas taxas de transação.

### **Transações de tempo de bloqueio (timelock)**

Algumas transações incluem uma regra de tempo que impede que sejam adicionadas a um bloco até que um certo número de blocos ou um período de tempo tenha passado.

Essas regras são implementadas e aplicadas por meio do software que os participantes da rede (nós e mineradores) executam.

### **Validação de blocos**

Antes de um bloco ser adicionado à blockchain, ele deve ser validado pelos nós, garantindo que todas as transações dentro dele são válidas.

## **Reorganização de blocos**

Se dois blocos são encontrados quase simultaneamente, a rede eventualmente seguirá a cadeia que se torna mais longa primeiro, descartando o bloco órfão.

## **Ajuste de dificuldade**

Como a mineração é um processo probabilístico, de tentativa e erro, a velocidade de saída dos blocos é diretamente proporcional à quantidade de máquinas mineradoras participando do sistema (hash power) em determinado período. Para que o tempo de saída dos blocos seja mantido estável, a dificuldade do problema matemático ajusta-se aproximadamente a cada duas semanas (ou a cada 2016 blocos) para garantir que novos blocos sejam adicionados aproximadamente a cada 10 minutos.

## **Regras de formatação de blocos**

Blocos devem ter uma estrutura específica, incluindo um cabeçalho de bloco que contém o hash do bloco anterior, o timestamp, a dificuldade alvo e o nonce. O nonce é um número aleatório usado uma única vez para gerar variações no resumo de hash de um bloco. Os mineradores ajustam o nonce repetidamente até encontrar um valor de hash que esteja abaixo do valor-alvo definido pelo nível de dificuldade da rede. Essa operação é parte essencial do mecanismo de Prova de Trabalho (Proof of Work) no processo de mineração do Bitcoin.

## **Propagação de blocos**

Após um minerador encontrar um bloco válido, ele deve propagá-lo rapidamente pela rede para que outros nós possam validá-lo e começar a trabalhar no próximo bloco.

## **Transações Coinbase**

Cada bloco deve incluir uma transação coinbase, que é a primeira transação do bloco, criando novos bitcoin como recompensa para o minerador.

## **SegWit—Segregated Witness**

Uma atualização que separa a assinatura digital dos dados da transação, permitindo mais transações por bloco e corrigindo maleabilidade de transação.

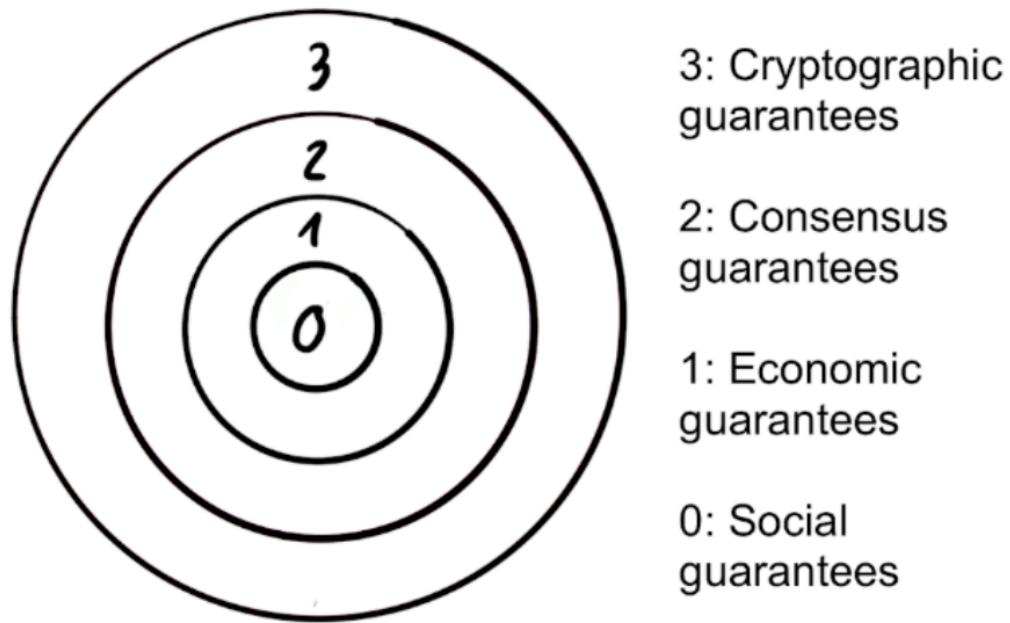
Qualquer tentativa de alterar essas regras requer um amplo consenso na comunidade e, muitas vezes, leva a um hard fork do software (divisão em duas blockchains compatíveis e incompatíveis, essencialmente duas moedas diferentes), como foi visto com a criação do Bitcoin Cash e outras variantes.

Alterar as regras de consenso do Bitcoin é um processo rigoroso que envolve propostas formais, discussões comunitárias, desenvolvimento de código, testes extensivos e métodos de ativação cuidadosamente planejados.

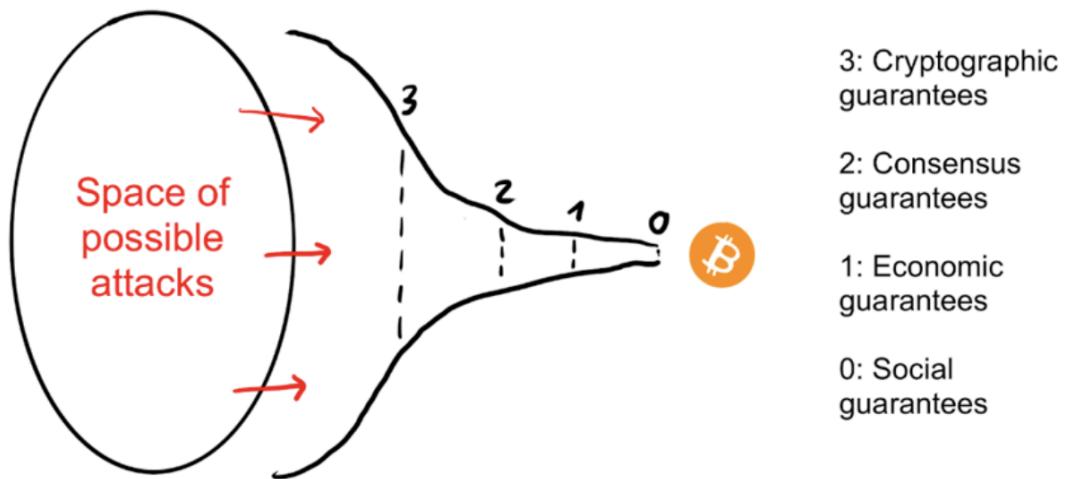
**Esse processo garante que qualquer mudança seja amplamente debatida, testada e aceita pela comunidade, preservando a segurança e descentralização da rede Bitcoin.**

## 2.3 Modelo de Segurança do Bitcoin

Blockchains públicas são seguras devido à combinação de várias camadas de proteção, incluindo garantias criptográficas, consenso e incentivos econômicos, além do suporte da comunidade. Esse modelo de cebola demonstra como cada camada adiciona segurança e impede ataques.



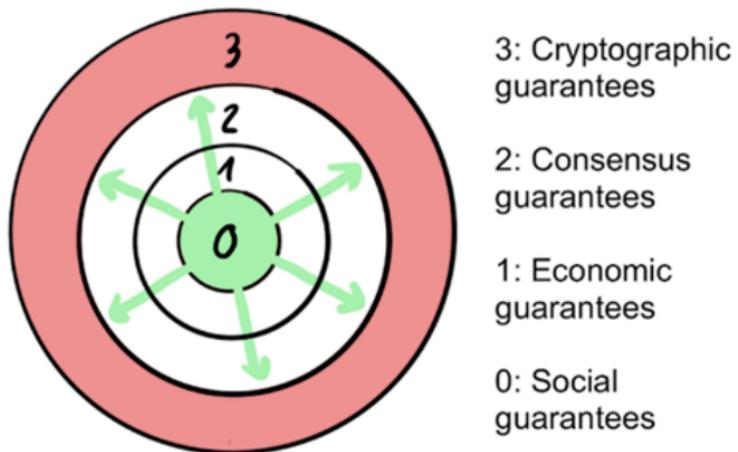
Para destruir permanentemente uma blockchain pública, é necessário destruir a fé dos usuários no estado do seu livro-razão (a lista de propriedade), bem como a capacidade de atualizar esse estado de forma confiável no futuro. Todas as camadas superiores servem para evitar que isso aconteça.



Mesmo se uma camada falhar, as outras ajudam a manter a integridade do sistema.

Uma blockchain aberta é apenas um meio para automatizar o processo de estabelecer um consenso social entre seus participantes, uma ferramenta para manter e atualizar uma base de dados compartilhada. O estado dessa base de dados tem valor para os participantes, e eles são fortemente incentivados a restaurar o sistema quando ele falha.

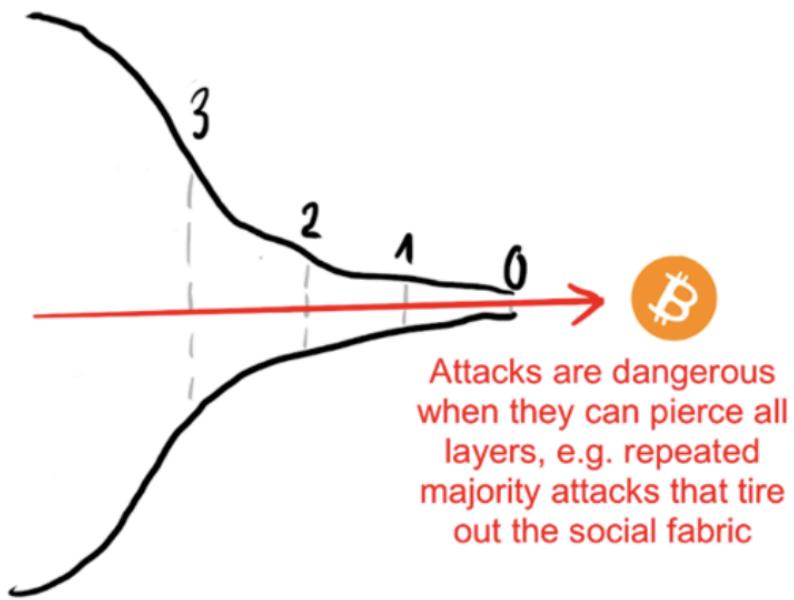
Por exemplo, se a função de hash criptográfica for quebrada, a camada social pode chegar a um consenso manual (orientado por especialistas técnicos) para substituir a parte danificada.



ECDSA breaks; a social intervention can mitigate the fallout and fork in a replacement

Da mesma forma, se um ataque ao consenso passar pela etapa das garantias econômicas, a camada social ainda pode rejeitá-lo manualmente. Se um atacante com a maioria do poder de hash começasse a realizar um ataque de negação de serviço (DOS) à rede minerando blocos vazios, aceitando totalmente o dano econômico para si mesmo, os usuários poderiam decidir mudar a função de Prova de Trabalho (PoW) e, assim, remover manualmente o controle desse minerador.

Os ataques são perigosos quando conseguem atravessar todas as camadas e, finalmente, desgastar o núcleo social do sistema até que ele não possa mais superar os danos nas camadas superiores e se recuperar.



Por exemplo, um ataque repetido de uma maioria que danifica e esgota a fábrica social.

Para que tanto a recuperação quanto a intervenção manual funcionem, as comunidades de cada projeto precisam de convenções sociais fortes em torno das principais propriedades do seu projeto. No caso do Bitcoin, esses valores fundamentais são a irreversibilidade das transações, resistência à censura, ausência de mudanças incompatíveis retroativamente e o limite de 21 milhões de tokens. Eles servem como roteiros de ação para quando a intervenção social se torna necessária e criam pontos focais em torno do que precisa ser corrigido e do que não precisa.

Esses valores fundamentais de um projeto são perpetuamente renegociados, e nem todos os usuários concordam com todas as propriedades. No entanto, quanto mais forte for o acordo em torno de um valor particular, mais provável é que ele seja mantido durante tempos de dificuldades.

**A segurança do Bitcoin depende da interação entre todas essas camadas e da forte base social e técnica que sustenta o sistema.**

Saiba mais em: [Modelo de Segurança das Blockchains](#)

## 2.4 Funções Hash

Bitcoin é uma coleção de conceitos e tecnologias que formam a base de um ecossistema de dinheiro digital, incluindo:

Uma rede descentralizada ponto-a-ponto—habilitada pelo protocolo Bitcoin.

Um livro-razão público de transações—a blockchain.  
Um mecanismo descentralizado, matemático e determinístico de emissão de moeda—mineração distribuída e o algoritmo de consenso “Prova de Trabalho”.  
Um sistema descentralizado de verificação de transações—script de transação.

Como tal, ele depende fortemente de tecnologias criptográficas, como:

### **Funções de hash**

SHA-256 e RIPEMD-160

### **Criptografia de Chave Pública**

ECDSA – o Algoritmo de Assinatura Digital de Curva Elíptica.

**A posse do bitcoin é estabelecida através da relação entre as chaves públicas e as assinaturas digitais produzidas a partir das chaves privadas correspondentes.**

Uma função de hash criptográfica é uma função matemática comumente usada para verificar a integridade dos dados, transformando dados idênticos em um resumo (código) único, representativo e de tamanho fixo. Qualquer modificação accidental ou intencional dos dados de entrada—como reorganização de caracteres—mudará completamente a saída do hash. Entradas diferentes nunca devem gerar o mesmo hash. Isso é conhecido como "colisão de hash."

Como as funções de hash são muito difíceis de serem revertidas, é quase impossível derivar o valor de entrada a partir de sua saída de hash. Isso é útil para esquemas de compromisso, ou seja, compartilhar um valor oculto que pode ser revelado autenticamente mais tarde.

O Bitcoin usa a função de hash SHA-256. A saída do hash é de 256 bits (32 bytes) de comprimento, pois 1 byte = 8 bits. Um hash SHA-256 é geralmente apresentado como uma sequência de 64 caracteres hexadecimais. Cada um dos 32 bytes é representado por 2 caracteres hexadecimais.

O primeiro algoritmo de hash foi apresentado pelo engenheiro sênior da IBM Hans Peter Luhn em 1958. Exemplo de saída de hash:

```
bitcoin → 6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b
```

```
bitcoins →  
b1e84e5753592ece4010051fab177773d917b0e788f7d25c74c5e0fc63903aa9
```

Note que apenas a inclusão da letra s gerou uma saída radicalmente diferente, tornando as funções hash extremamente eficientes na verificação da integridade de dados.  
As funções de hash criptográficas são amplamente utilizadas no bitcoin. No Bitcoin, o SHA-256 é utilizado em vários componentes críticos:

## **Endereços de bitcoin**

Os endereços de Bitcoin são derivados de chaves públicas usando SHA-256 e hashing RIPEMD-160. As funções hash são usadas na geração de diferentes tipos de endereços.

## **Identificador de transações (txid)**

As transações de Bitcoin são identificadas por um ID de transação (TXID), que é um hash SHA-256 dos dados da transação.

## **Mineração**

Quando as transações são transmitidas pela rede, a função de hash é usada para verificar a integridade dos dados, garantindo que não foram corrompidos ou modificados durante a transmissão. No mecanismo de prova de trabalho na mineração de Bitcoin, é usado hashing duplo SHA-256. Os mineradores devem encontrar um valor de hash que seja menor que um alvo especificado, repetindo o hashing dos cabeçalhos de bloco até encontrar o valor desejado.

## **Hash de blocos**

Cada bloco na blockchain do Bitcoin possui um hash único gerado usando SHA-256. Esse hash vincula cada bloco ao anterior, formando uma cadeia segura. Todas as transações de bitcoin são armazenadas em blocos, que são ligados em sequência, sempre referenciando (incluindo) o hash do bloco anterior. As funções de hash criptográficas verificam a integridade do bloco e estabelecem a ordem cronológica da blockchain.

## **Simulador de Hash**

Você pode praticar escrever algo e verificar como as saídas de hash se alteram neste simulador de hash. <https://academo.org/demos/SHA-256-hash-generator/>

## 2.5 Chaves Digitais

### **Criptografia Assimétrica**

Se a mesma chave fosse usada para ambas as etapas de criptografia e descriptografia, a relação seria simétrica. A criptografia assimétrica, por outro lado, envolve duas chaves, uma pública e uma privada. A chave pública criptografa a mensagem e a chave privada descriptografa. A chave pública pode ser derivada da chave privada, mas a chave privada não pode ser derivada da chave pública—isto é computacionalmente inviável.

Ao criptografar uma mensagem, o remetente criptografa a mensagem M usando a chave pública (derivada da chave privada) do destinatário para produzir a mensagem criptografada C. O destinatário descriptografa a mensagem criptografada C usando sua chave privada para ver a mensagem original M. C é o resultado da criptografia (também conhecido como "cifra"). M é a mensagem não criptografada / descriptografada (também conhecida como "texto plano"). Veja como a criptografia assimétrica é aplicada à tecnologia Bitcoin.

### **Chave Privada (Privkey)**

É um número gerado aleatoriamente que deve ser mantido em segredo. Usada para gerar chaves públicas e assinaturas digitais, confirmado a propriedade, e autorizando o gasto de bitcoin. Elas são criadas pelo software de carteira de Bitcoin. Deve ser armazenada em local seguro, preferencialmente escrita em papel ou placa de aço inoxidável e guardada em um cofre. **Quem possui a chave privada tem controle total sobre os bitcoin associados a ela.**

### **Chave Pública (Pubkey)**

A chave pública é gerada a partir da chave privada usando a multiplicação de curva elíptica no grupo da curva elíptica secp256k1. No Bitcoin, a chave pública é mascarada através de uma série de funções de hash, incluindo SHA-256 e RIPEMD-160, e é representada por um endereço de Bitcoin ao gastar e receber fundos.

### **Geração de endereços**

A chave pública é usada para gerar endereços de Bitcoin, que são compartilhados publicamente para receber bitcoins.

### **Verificação de assinaturas digitais**

A chave pública é usada para verificar assinaturas digitais. Quando uma transação é assinada com a chave privada, qualquer pessoa pode usar a chave pública correspondente para verificar a autenticidade da assinatura e confirmar que a transação foi autorizada pelo proprietário da chave privada.

A criptografia de chave pública é utilizada para produzir assinaturas digitais com o ECDSA (Algoritmo de Assinatura Digital de Curva Elíptica), especificamente a curva [secp256k1](#), para autorizar e validar transações.

A partir de janeiro de 2021, a versão v0.21 do Bitcoin Core passou a suportar o algoritmo de assinatura digital Schnorr. Após meses de testes e discussões sobre os métodos, a soft fork foi ativada na mainnet em novembro de 2021.

### **Links importantes:**

Bitcoin Core v0.21

<https://lists.linuxfoundation.org/pipermail/bitcoin-core-dev/2021-January/000097.html>

Taproot Activation Proposals

[https://en.bitcoin.it/wiki/Taproot\\_activation\\_proposals](https://en.bitcoin.it/wiki/Taproot_activation_proposals)

Taproot Locks In

<https://bitcoinmagazine.com/technical/taproot-locks-in>

Preparing for Taproot

<https://bitcoinops.org/en/preparing-for-taproot/>

Taproot: Script alternável preservador de privacidade

<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html>

O algoritmo de assinatura digital Schnorr foi projetado pelo criptógrafo alemão Claus-Peter Schnorr. Sua patente de 1991 expirou em fevereiro de 2010.

## 2.6 Assinaturas Digitais

Assinaturas digitais são usadas para autenticar transações válidas. Para fazer um pagamento em Bitcoin, uma transação de Bitcoin  $T$  é construída. Um subconjunto  $M$  das informações na transação  $T$  é assinado da seguinte forma:

### Assinando a Transação $T$

1. Criar a transação  $T$
2. Selecionar o subconjunto  $M$  da transação  $T$  (por exemplo, o identificador da transação, instruções da transação, etc.)
3. Calcular o hash  $H$  de  $M$ :  $H = \text{sha256}(M)$
4. Calcular uma assinatura  $S$  usando a saída desta função de hash  $F\text{hash}(M)$  com a chave privada do remetente, onde  $F\text{sig}$  é o algoritmo de assinatura:

$$S = F\text{sig}(F\text{hash}(M), K_{\text{priv}})$$

5. Enviar a assinatura  $S$  e a chave pública  $K_{\text{pub}}$  juntamente com a transação  $T$  para os mineradores de Bitcoin.

A **verificação** é o inverso da função de geração de assinatura, usando os valores  $R$ ,  $S$  e a chave pública para calcular um valor  $P$ , que é um ponto na curva elíptica. Para verificar uma transação recebida com a assinatura e a chave pública  $K_{\text{pub}}$ , um receptor deve:

### Verificar a transação $T$

$$P = S^{-1} \cdot F\text{hash}(M) \cdot G + S^{-1} \cdot R \cdot K_{\text{pub}}$$

Calcular:

Onde:

$R$  e  $S$  são os valores da assinatura

$K_{\text{pub}}$  é a chave pública

$M$  são os dados da transação que foram assinados

$G$  é o ponto gerador da curva elíptica

Se a coordenada  $x$  do ponto calculado  $P$  for igual a  $R$ , então o verificador pode concluir que a assinatura é válida. **Note que, ao verificar a assinatura, a chave privada não é conhecida nem revelada.**

O livro-razão público registra transferências de propriedade de uma quantidade de bitcoin de um proprietário para outro. (**Nota: Transações também podem ser 'auto-transferências,' ou seja, entre conjuntos de endereços e/ou chaves controlados pela mesma pessoa.**)

## 2.7 Endereços de Recebimento

Podemos encontrar diferentes tipos de endereços no Bitcoin.

**Legacy (P2PKH—Pay-to-Public-Key-Hash):** Formato original, começa com 1.

Exemplo: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa.

**SegWit (P2WPKH—Pay-to-Witness-Public-Key-Hash) P2SH (Pay-to-Script-Hash):**

Começam com 3.

Exemplo: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLY

No P2SH, o script é hash e só revelado ao gastar, permitindo transações mais complexas, como multisig. Por exemplo, um esquema 2-de-3 pode requerer duas de três assinaturas para validar uma transação, útil para serviços fiduciários ou de escrow (terceiros de confiança).

**SegWit Nativo (bech32):** Começa com bc1.

Exemplo: bc1qw508d6qejxtdg4y5r3zarvary0c5xw7kygt080

As transações na blockchain não registram as chaves públicas ou destinatários, mas em vez disso usam uma abstração chamada "endereço de Bitcoin" para registrar o beneficiário de cada quantia, permitindo maior flexibilidade.

Um endereço é um identificador único para o destino de um pagamento em bitcoin, gerado a partir de e correspondente a uma chave pública ou script.

Ele é geralmente gerado aplicando as funções de hash criptográficas SHA-256 e RIPEMD-160, em série, na chave pública. Esses endereços são codificados usando a codificação Base58, que representa um endereço em uma forma legível por humanos de 58 caracteres alfanuméricos. Os softwares de carteira geralmente codificam em formato QR Code, fazendo com que a experiência de transação financeira seja semelhante à do PIX.

Para criar um endereço de Bitcoin, o software de carteira de Bitcoin primeiro gera um par de chaves Pública-Privada ECDSA a partir de um número aleatório. O endereço de Bitcoin é gerado aplicando a seguinte sequência:

#### **Chave Privada, representação hexadecimal de um binário:**

```
C4bbeb1fbec99d65bf59d85c8cb62ee2db963f0fe106f483d9afa73bd4e39a8a
```

A chave pública é derivada pela multiplicação da chave privada por um ponto gerador predefinido na curva elíptica **secp256k1**. Esta operação é unidirecional, ou seja, é fácil calcular a chave pública a partir da chave privada, mas praticamente impossível calcular a chave privada a partir da chave pública devido à complexidade computacional (problema de logaritmo discreto). É computacionalmente simples para derivar a chave pública, mas impraticável para reverter.

Este ponto gerador é uma constante conhecida e bem definida.  
A operação é expressa matematicamente como:

```
Chave Pública = k * G
```

Onde  $k$  é a chave privada (um número inteiro), e  $G$  é o ponto gerador na curva elíptica.  
Após a multiplicação, a chave privada se transforma em chave pública:

```
0478d430274f8c5ec1321338151e9f27f4c676a008bdf8638d07c0b6be9ab35c71151806324  
3acd4dfe96b66e3f2ec8013c8e072cd09b3834a19f811659cc3455
```

Para chegarmos até um endereço de Bitcoin, essa chave pública é passada pelas funções hash SHA-256 e RIPEMD-160 na sequência. RIPEMD-160 sempre produz um hash de 160 bits (20 bytes) de comprimento. A saída correta deve ser um hash de 20 bytes (ou 40 caracteres hexadecimais). Vamos analisar primeiro a saída SHA-256.

```
SHA256(0478d430274f8c5ec1321338151e9f27f4c676a008bdf8638d07c0b6be9ab35c7115  
18063243acd4dfe96b66e3f2ec8013c8e072cd09b3834a19f811659cc3455)  
= c4c5d791fc4654a1ef5e03fe0ad3d9c598f9827
```

Agora a RIPEMD-160 do SHA-256.

```
RIPEMD160(c4c5d791fc4654a1ef5e03fe0ad3d9c598f9827) =  
448e53f6c8da1fcdea5f1812403db91d9867e305
```

Vamos adicionar o prefixo 00 para mainnet (rede principal).

```
00448e53f6c8da1fcdea5f1812403db91d9867e305
```

Agora é hora do SHA-256 duplo. Primeiro SHA-256.

```
SHA256(00448e53f6c8da1fcdea5f1812403db91d9867e305)  
= 3e417cec974b61aaa0ac2977ed4232f86da379782978d8e05ed3c378d1325a14
```

Segundo SHA-256.

```
SHA256(3e417cec974b61aaa0ac2977ed4232f86da379782978d8e05ed3c378d1325a14)  
= 7d6bc0cb60da0fb5081697c26c6b8913ee5ac609927d02c571cdacba486bb9d9
```

Os primeiros 4 bytes do segundo SHA são usados como [checksum](#).

```
7d6bc0cb
```

Agora vamos combinar o prefixo + RIPEMD + checksum.

```
00448e53f6c8da1fcdea5f1812403db91d9867e3057d6bc0cb
```

Agora vamos codificar esse número com Base58 para gerar o endereço de recebimento de bitcoin final.

```
Base58(00448e53f6c8da1fcdea5f1812403db91d9867e3057d6bc0cb)
```

O resultado é o endereço de recebimento de bitcoin.

```
17FVTAe4x93k79gT1ND3mk9sM4jUP2WFMt
```

Tecnicamente, o endereço é público, e a chave pública da qual ele é derivado não é exposta até que o bitcoin seja gasto.

**CURIOSIDADE:** Existem 52 caracteres no alfabeto, se incluirmos todas as letras maiúsculas e minúsculas. Existem também 10 números (de 0 a 9). Para evitar confusões e erros de cópia, Satoshi removeu 4 caracteres comumente confundidos do processo de geração de endereços: a letra maiúscula 'O' e o número '0', a letra maiúscula 'I' e a letra minúscula 'l.'

**Cuidado com Phishing:** Tenha cuidado com e-mails e sites falsos que tentam enganar você para roubar suas chaves privadas. Sempre verifique a autenticidade das fontes antes de inserir informações sensíveis. Se uma oportunidade parece boa demais para ser verdade, com certeza é golpe.

## 2.8 Carteiras

Uma carteira de Bitcoin é uma ferramenta digital que permite aos usuários armazenar suas chaves privadas, criar endereços de Bitcoin para recebimento, e assinar transações de saída de bitcoin. Embora o termo "carteira" sugira um local onde os bitcoin são armazenados, na realidade, as **carteiras de Bitcoin não armazenam os bitcoin em si**. Em vez disso, elas armazenam as chaves privadas necessárias para acessar e gerenciar os bitcoin registrados na blockchain.

Existem diferentes tipos de carteiras, cada uma com suas características específicas em termos de conveniência e segurança.

### **Carteiras Quentes (Hot Wallets)**

As carteiras quentes estão conectadas à internet e são geralmente mais fáceis de usar. Exemplos incluem aplicativos de carteira móvel, software de carteira em desktop e carteiras online. São consideradas carteiras quentes pois suas chaves privadas foram geradas em um aplicativo de celular ou dispositivo que fica em contato com a internet.

No geral, elas são seguras e uma forma perfeita de começar a comprar e vender ou trocar Bitcoin por serviços, mas não é recomendado deixar quantias muito altas de Bitcoin nelas. Uma sugestão de primeira carteira onchain é a [BlueWallet](#) e de primeira carteira Lightning, a [Phoenix](#). Vamos aprender mais sobre a rede lightning adiante.

### **Carteiras Fria (Cold Wallets)**

As carteiras frias podem ser de vários tipos e variar em sua superfície de contato com a internet. Exemplos incluem carteiras de hardware (dispositivos de assinatura), carteiras de papel e carteiras offline.

### **Dispositivos de Assinatura**

Criam e mantêm suas chaves privadas offline, servindo como uma camada extra de segurança. As carteiras frias não estão conectadas à internet, o que as torna muito mais seguras contra hacks e malware. Existem formas de criar esses dispositivos de assinatura de forma DIY, mas para iniciantes, existem marcas consolidadas no mercado. Uma opção popular é a [Jade Wallet](#).

**Nunca é recomendado deixar seus bitcoin em carteiras com suporte para outras criptomoedas. Procure sempre, pelo menos, instalar um firmware que seja Bitcoin-only—no caso da [Trezor](#), por exemplo.**

Existem algumas formas DIY de criar dispositivos de assinatura.

Seedsigner: <https://seedsigner.com/>

Krux: <https://selfcustody.github.io/krux/>

Jade: <https://github.com/Blockstream/Jade>

Specter: <https://github.com/cryptoadvance/specter-diy>

### **Carteiras de Aço Inoxidável (Steel Wallets)**

As carteiras de aço são métodos de backup físicos projetados para armazenar suas chaves privadas ou frases de recuperação de maneira segura e durável. Elas são feitas de metal, geralmente aço inoxidável, o que as torna resistentes a danos físicos, como fogo, água, corrosão e impactos mecânicos.

Ao contrário de papel ou dispositivos eletrônicos, as carteiras de aço são praticamente indestrutíveis e podem suportar condições extremas. Utilize a carteira de aço para gravar sua chave privada ou frase de recuperação. Algumas carteiras de aço vêm com kits de gravação, como letras e números estampados, ou placas que você pode marcar manualmente. Verifique se todas as informações foram registradas corretamente e são legíveis. Uma vez gravadas, essas informações são permanentes, então a precisão é crucial. Sempre teste instanciar suas chaves em um dispositivo de assinatura, para garantir que sua seed foi escrita corretamente.

Incorporando uma carteira de aço como parte de sua estratégia de segurança pode proporcionar uma tranquilidade adicional, garantindo que suas chaves privadas ou frases de recuperação estejam protegidas contra praticamente qualquer tipo de dano físico. É uma opção excelente para quem deseja um método de armazenamento robusto e a longo prazo para seus bitcoin.

Componentes de uma Carteira (dispositivos e aplicativos de assinatura) de Bitcoin

**Chave Privada:** Uma sequência secreta de números e letras que permite ao usuário acessar seus bitcoins. É essencial para assinar transações e deve ser mantida em segurança.

**Chave Pública:** Derivada da chave privada, a chave pública é usada para gerar endereços de Bitcoin.

**Endereço de Bitcoin:** Uma versão hash da chave pública, que é usada para receber bitcoins. Funciona como um número de conta bancária.

**Observação:** [BIPS—Bitcoin Improvement Proposals](#) ou Propostas de Melhorias no Bitcoin. É o mecanismo de comunicação da comunidade de desenvolvedores sobre as propostas de melhoria que passarão a fazer parte do código-fonte do Bitcoin. Algumas BIPs relevantes para a forma que nossas carteiras tem hoje incluem.

### **BIP 32: Carteiras Determinísticas Hierárquicas (HD Wallets)**

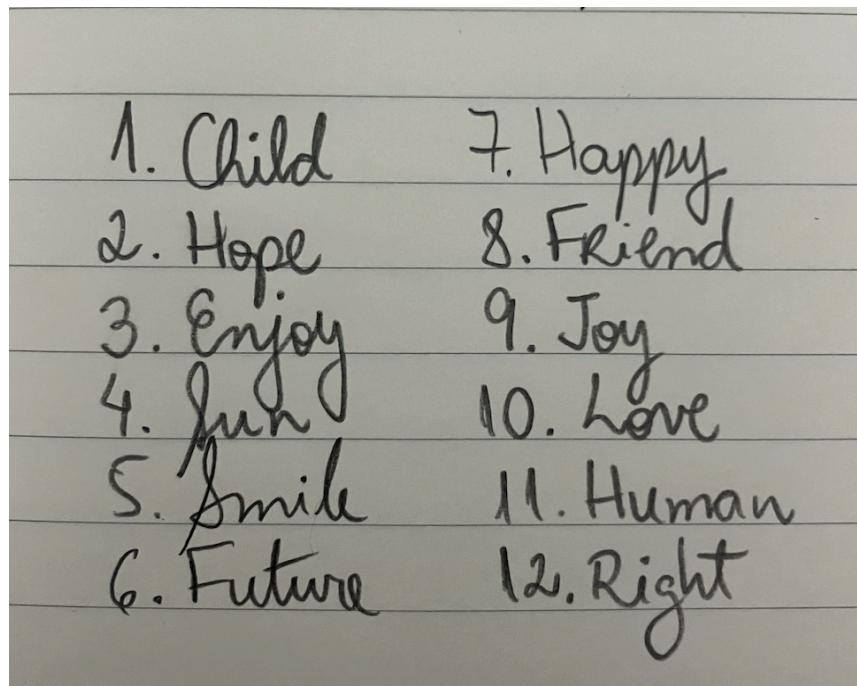
BIP 32 introduz o conceito de "carteiras determinísticas hierárquicas" ou HD wallets. Esse é um método de gerar e gerenciar chaves privadas e públicas de maneira mais organizada e segura. Antes do BIP 32, cada endereço de Bitcoin tinha sua própria chave privada. Gerenciar várias chaves era complicado e inseguro. Com BIP 32, você pode criar uma "semente" única (uma sequência de palavras) que pode gerar um número infinito de pares de chaves privadas e

públicas. Isso facilita o backup e a restauração de todas as suas chaves com apenas uma única semente.

### BIP 39: Frases Mnemônicas

BIP 39 define o padrão para criar uma "frase mnemônica" - uma sequência de 12 a 24 palavras comuns que representam uma semente criptográfica.

Essa frase mnemônica torna o processo de backup e restauração de carteiras muito mais simples e seguro. Em vez de lembrar uma longa e complicada sequência de números e letras (a chave privada), você só precisa lembrar ou anotar uma frase de palavras comuns. Por exemplo, uma frase mnemônica pode ser algo como "corredor chuva mesa sol viagem livro..."



Esta frase pode ser instanciada em qualquer dispositivo ou aplicativo de assinatura para acesso e assinatura de movimentações de Bitcoin. São essencialmente um símbolo da auto-soberania financeira e da necessidade de armazená-la em um local extremamente seguro e fora do alcance de atores mal-intencionados. Grandes poderes trazem consigo grandes responsabilidades.

### BIP 44: Estrutura de Endereços Multi-Conta

Recomendada para usuários mais avançados, a BIP 44 expande os conceitos do BIP 32, fornecendo uma maneira padronizada de organizar e gerenciar várias contas dentro de uma única carteira HD.

Com BIP 44, você pode criar várias contas (por exemplo, uma conta para gastos diários, outra para economias, etc.) dentro da mesma carteira, cada uma com seus próprios endereços. Isso traz uma camada adicional de organização e flexibilidade, facilitando a gestão de fundos para diferentes propósitos.

No aspecto de segurança de carteiras, temos um interessante projeto que verifica a integridade de binários sendo lançados ao público em lojas de software. O projeto é open source e chama-se [WalletScrutiny](#).

### 3. Transações

Cada transação associa uma quantidade de bitcoin com um endereço de bitcoin. Quando bitcoins são enviados para alguém, a transação registra a transferência de bitcoin do endereço do proprietário atual para o endereço do novo proprietário, autorizado por uma assinatura digital válida.

Quando essa transação é transmitida para a rede Bitcoin, todos os pares sabem que o novo proprietário desses bitcoin é o dono do novo endereço de recebimento.

O histórico completo de transações é mantido por todos os peers (pares, clientes completos, ou nós completos) na rede Bitcoin, para que qualquer pessoa possa verificar quem é o proprietário atual de qualquer quantidade de bitcoin, sem precisar conhecer suas chaves privadas.

Na maioria dos casos, tanto as chaves públicas quanto as privadas são armazenadas em uma carteira de Bitcoin. **Uma carteira de Bitcoin, assim como um cartão de crédito, não contém nenhum bitcoin, mas apenas os pares de chaves privada-pública, que são usados como mecanismos para acessar seus fundos, transferí-los para outro endereço, ou gerar novos endereços de recebimento.**

**Bitcoin Pizza Day:** comemorado anualmente no dia 22 de maio e marca a primeira transação comercial documentada usando Bitcoin. Em 2010, um programador chamado Laszlo Hanyecz fez história ao comprar duas pizzas por 10.000 bitcoins.

No dia 18 de maio de 2010, Laszlo Hanyecz postou uma mensagem no fórum Bitcointalk oferecendo 10.000 bitcoins em troca de duas pizzas. Quatro dias depois, em 22 de maio, ele conseguiu fechar a transação com um usuário que aceitou o pagamento e encomendou as pizzas para ele. Este evento é amplamente reconhecido como a primeira vez que Bitcoin foi usado para comprar um bem físico.

#### 3.1 Inputs, Outputs, UTXOs

Uma UTXO (Unspent Transaction Output, traduzido Saídas de Transações Não Gastas) é um conceito fundamental no funcionamento do protocolo Bitcoin. Para entender a UTXO, é importante primeiro compreender como as transações em Bitcoin são estruturadas e processadas.

Em uma transação Bitcoin, existem entradas (inputs) e saídas (outputs). Cada transação consome uma ou mais saídas não gastas de transações anteriores (inputs) e cria novas saídas

(outputs). Uma transação é considerada válida quando as saídas de todas as entradas são corretamente referenciadas e as somas de valores das entradas são iguais ou superiores às somas das saídas (com a diferença podendo ser a taxa de transação paga ao minerador).

Uma UTXO é uma saída de transação que ainda não foi gasta como entrada em uma transação subsequente. Essencialmente, é um registro no blockchain que indica a quantia de Bitcoin disponível para ser gasta por um endereço específico.

Quando uma transação é confirmada, suas saídas tornam-se UTXOs até serem usadas em uma nova transação. Quando uma nova transação é criada, ela referencia uma ou mais UTXOs como suas entradas. Essas UTXOs são então gastas e removidas do conjunto de UTXOs disponíveis. Cada UTXO é identificado exclusivamente pelo hash da transação que a criou e pelo índice da saída dentro dessa transação.

A estrutura básica de uma UTXO inclui:

**ID da Transação —txid:** O hash da transação que criou a UTXO.

**Index:** O índice específico da saída dentro da transação.

**Value:** O valor da UTXO em satoshis (unidade mínima de Bitcoin).

**ScriptPubKey:** Um script que define as condições necessárias para gastar a UTXO.

O modelo UTXO permite que o estado do blockchain seja facilmente verificável e mantém as transações paralelas independentes, facilitando a validação e a mineração. Além disso, o modelo melhora a escalabilidade, pois permite a validação paralela de transações e reduz a complexidade de rastrear a propriedade das moedas.

A utilização de UTXOs aumenta a segurança, pois cada transação deve referenciar saídas válidas de transações anteriores, evitando o gasto duplo e facilitando a detecção de tentativas de fraude. O modelo UTXO é um dos pilares que garante a segurança e a eficiência do Bitcoin, permitindo transações seguras e verificáveis em uma rede descentralizada. Esse modelo é crucial para o funcionamento do protocolo Bitcoin.

Podemos ver que as saídas de uma transação são as entradas para a próxima transação. Uma transação pode ter múltiplas saídas.

### **Os tipos de transações mais comuns**

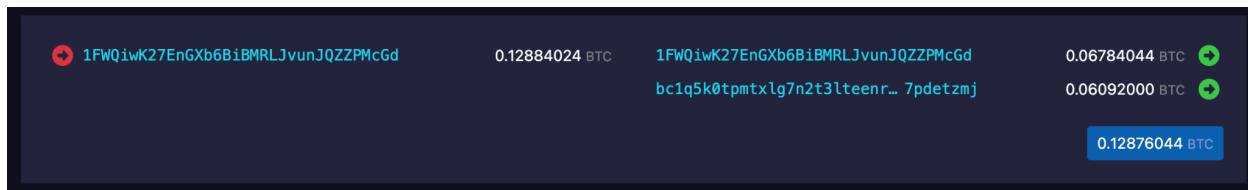
A forma mais comum de transação é um pagamento simples de um endereço Bitcoin para outro, que frequentemente inclui algum troco a ser retornado ao proprietário original. Esse tipo de transação possui uma entrada e duas saídas, conforme mostrado abaixo:

Entradas são debitadas do endereço Bitcoin do proprietário original.

Saídas são creditadas no endereço Bitcoin do novo proprietário; o troco é retornado ao proprietário original em uma segunda saída.

Input #0 Transação 1: Remetente	Output #0 Transação 1: Recipiente
	Output #1 Transação 2: Troco retornado ao remetente

Um exemplo real deste tipo de transação.



Em que o endereço 1FWQiwK27EnGXb6BiBMRLJvunJQZZPMcGd usa uma UTXO de 0.12884024 que é transformada no valor do pagamento 0.06092000 e no troco de 0.06784044 de volta para o endereço emissor. Nessa transformação, também é debitado um valor de taxa de rede.

Outra forma comum de transação é uma transação que agrupa várias entradas (3 no exemplo) em uma única saída. Isso representa o equivalente no mundo real a trocar uma pilha de moedas e notas de dinheiro por uma única nota de valor maior. Ou melhor, queimar essas notas antigas e criar uma única nova que represente o valor de todas elas.

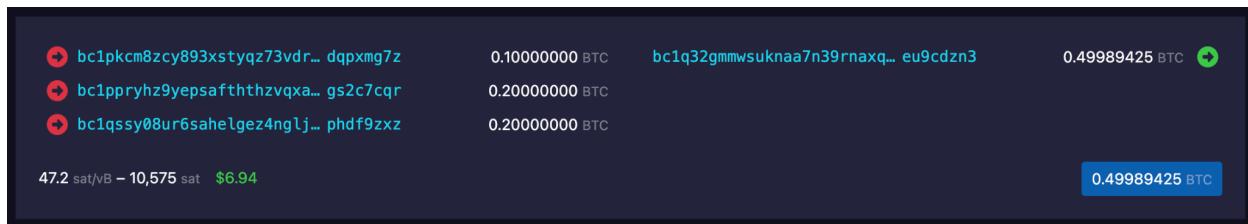
Transações como essas são às vezes geradas por aplicativos de carteira para limpar muitos pequenos valores que foram recebidos como troco, um processo chamado consolidação de transações. Geralmente uma transação de consolidação é feita quando as taxas de rede estão baixas.

Basicamente você cria uma transação para um endereço próprio, cujo valor é a soma de todas as suas UTXO menores. E voilá. O valor é consolidado em uma única UTXO de valor mais alto. Consolidar UTXOs em um período de taxas baixas ajuda a economizar em taxas em momentos futuros, quando você realmente estiver transacionando com outra pessoa. [Mais adiante](#) vamos entender melhor por que consolidar UTXOs em períodos de taxas baixas é uma prática importante.

Em uma transação deste tipo, múltiplas entradas são coletadas. Uma única saída é criada.

Input #0 Transação 1: Remetente	Output #0 Transação 1: Recipiente
Input #1 Transação 2: Remetente	
Input #2 Transação 3: Remetente	

### Um exemplo real deste tipo de transação



Outra forma de transação frequentemente observada no livro razão do Bitcoin distribui uma entrada para múltiplas saídas, que podem ou não representar múltiplos destinatários independentes. Esse tipo de transação é às vezes usado por entidades comerciais, como ao processar a folha de pagamento dos funcionários. De uma única entrada, múltiplas saídas são creditadas nos endereços Bitcoin dos novos proprietários.

Input #0 Transação 1: Remetente	Output #0 Transação 1: Recipiente 1
	Output #1 Transação 2: Recipiente 2
	Output #2 Transação 3: Recipiente 3

## Um exemplo real deste tipo de transação.

 bc1qgdq67upw5909ctmm3t54z... m5ggafcr	0.73060697 BTC	OP_RETURN x2[v 6 p[dW"7Wb43w ? dY UDZst]=@ N...	0.00000000 BTC 
		bc1p7l2cywf6qr9gwca3vsv6m... 6suc2lpk	0.00287500 BTC 
		bc1p7l2cywf6qr9gwca3vsv6m... 6suc2lpk	0.00287500 BTC 
		bc1qgdq67upw5909ctmm3t54z... m5ggafcr	0.72475706 BTC 
34.8 sat/vB – 9,991 sat  \$6.56			0.73050706 BTC

O campo OP\_RETURN em transações de Bitcoin é utilizado para incorporar dados arbitrários na blockchain. Este campo permite a inclusão de informações sem impactar a capacidade de gasto dos bitcoins. Existem serviços que passam documentos pelo SHA-256 e gravam o código resultando neste campo, de modo a registrar permanentemente a veracidade de um documento que pode ser posteriormente verificado. Essa prática não é amplamente aceita na comunidade Bitcoin, mas é uma das formas que a rede Bitcoin é usada.

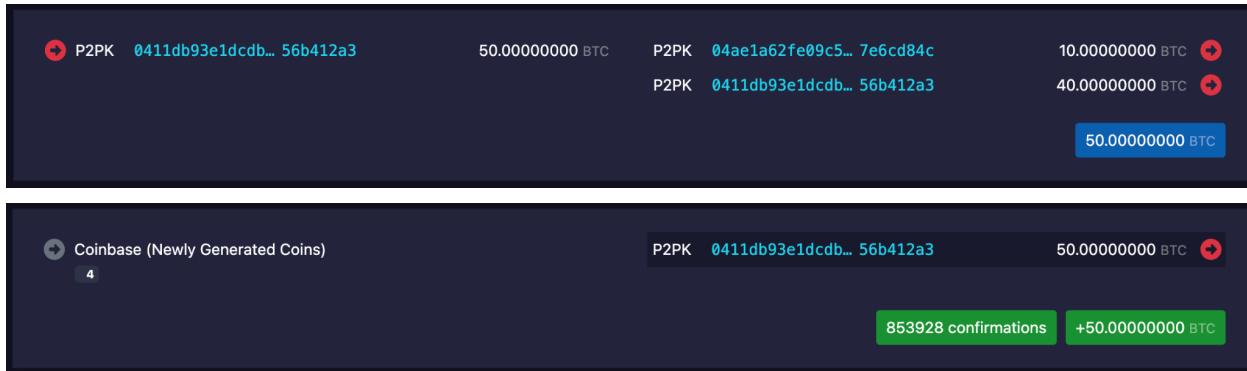
Outra forma de transação frequentemente observada no livro razão do Bitcoin é a transação coinbase. Diferente das transações comuns, a transação coinbase não possui entrada, pois representa moedas recém-geradas. Ela possui apenas uma saída, que é creditada nos endereços Bitcoin do minerador do bloco.

Sem input (apenas novas moedas geradas)	Output #0 Transação 1: Minerador
---	-------------------------------------

 Coinbase (Newly Generated Coins) I EligiusR/mmr>e +L0ocx(x8*) /ss311/kW	18d3HV2bm94UyY4a9DrP...XuiDQq2B	25.08660927 BTC 
		25.08660927 BTC

## Primeira Transação de Bitcoin

Abaixo está a primeira transação de bitcoin já realizada, entre Satoshi Nakamoto e Hal Finney. Nessa transação, Satoshi enviou 10 BTC para Hal Finney, com 40 BTC retornando como troco. Também podemos ver a transação coinbase do bloco em que essa transação foi incluída, que não possui entradas e inclui uma recompensa de bloco de 50 BTC.



### 3.2 SegWit—Segregated Witness e Maleabilidade de Transações

A maleabilidade de transações é uma vulnerabilidade que permitiria a um ator malicioso modificar ("maleabilizar") uma transação alterando os dados de testemunha de maneira que mude o ID da transação. (Lembre-se de que, após a confirmação, a assinatura digital e, portanto, o ID da transação são imutáveis).

O que foi produzido agora é uma segunda transação que assina o mesmo valor, para o mesmo endereço de destino, mas com um ID de transação alterado.

Este ataque não permite que o atacante roube fundos ou mude o destino do envio dos fundos. No entanto, pode ser usado para fraudar o remetente, enganando-o a enviar um segundo pagamento após a transação original parecer não ter sido confirmada.

[Maleabilidade de Transações Explicada](#)

**Curiosidade:** A Mt.Gox, a maior exchange do Japão, colapsou em fevereiro de 2014, suspendeu todos os saques e culpou a maleabilidade de transações pela suspensão dos saques.

#### SegWit surgiu para resolver o problema da maleabilidade de transações

Segregated Witness (SegWit) é uma mudança arquitetural que foi ativada no Bitcoin em 1º de agosto de 2017. Ela move os dados de testemunha das transações do campo scriptSig (script de desbloqueio) de uma transação para uma estrutura de dados de testemunha separada que acompanha a transação.

A maior parte do espaço em uma transação (cerca de 65% ou mais) pode ser ocupada pelos dados da assinatura. Movendo os dados de testemunha para fora da transação, o hash da transação usado como identificador não inclui mais os dados de testemunha.

O SegWit facilita e torna mais seguro a implementação de canais de pagamento, a Lightning Network e outras capacidades de script mais avançadas que serão introduzidas no futuro.

[SegWit Explicada](#)

#### Breve História

7 de dezembro de 2015: Pieter Wuille apresentou pela primeira vez a ideia do Segregated Witness nos workshops Scaling Bitcoin em Hong Kong como uma solução para os problemas de escalabilidade do Bitcoin.

23 de agosto de 2017: O Segregated Witness foi totalmente ativado como um soft fork na rede Bitcoin.

### **Benefícios**

SegWit aumenta a capacidade do bloco de 1MB para um teórico e maximamente eficiente 4MB, permitindo que mais transações caibam em cada bloco e reduzindo as taxas de transação.

Os nós podem podar os dados de testemunha após validar as assinaturas ou ignorá-los completamente ao realizar a verificação simplificada de pagamento. Ele impede ataques de maleabilidade de transações, possibilita scripts mais complexos e mantém a compatibilidade retroativa, sendo um soft fork.

### **Adoção do Segregated Witness desde sua ativação em 2017**

A maioria das carteiras e corretoras agora suporta SegWit. As versões do Bitcoin Core a partir da 0.16.0 incluem suporte completo ao SegWit. A porcentagem de transações de bitcoin usando SegWit excedeu 50% em setembro de 2019 e, em agosto de 2021, ultrapassou 75%.

### **Por que o SegWit não foi totalmente adotado?**

Como não foi uma atualização obrigatória, carteiras e exchanges adotam no seu próprio ritmo. Os usuários tiveram que se familiarizar com novos formatos de endereço (wrapped e native SegWit). Concepções errôneas sobre como o SegWit funcionava levaram a que seus benefícios de escalabilidade e taxas fossem ignorados.

## **3.3 MultiSig: Transações Multi-assinatura (Multisig) no Bitcoin**

O Bitcoin possui funcionalidade de multi-assinatura (abreviado como 'multisig'), na qual a movimentação de fundos pode ser configurada para exigir mais de uma assinatura—um quórum de assinaturas para autorizar transações, aumentando assim a segurança.

**Uso corporativo:** As carteiras MultiSig podem ser úteis em um ambiente corporativo, onde várias pessoas precisam aprovar a movimentação de fundos. Elas também podem ser usadas para facilitar serviços de custódia, especialmente em transações maiores com entidades desconhecidas.

**Configuração individual:** Um único indivíduo pode criar uma configuração MultiSig na qual ele possua todas as chaves, armazenando cada uma das chaves em diferentes dispositivos (por exemplo, celular, laptop e carteira de hardware), com a exigência de que assinaturas de duas das três chaves autorizem uma transação.

**Proteção contra ataques:** Configurações MultiSig podem ajudar a proteger os usuários contra ataques de phishing e infecções por malware. Mesmo que um dos dispositivos mencionados

seja perdido, roubado ou comprometido, uma chave não será suficiente para acessar os fundos; o proprietário original ainda pode acessar seus fundos usando as duas chaves restantes.

Essa funcionalidade é crucial para melhorar a segurança e a confiabilidade das transações de Bitcoin, fornecendo uma camada adicional de proteção e controle sobre os fundos.

A condição mais comum para transações multi-assinatura é usar um esquema *M-de-N*. Em um esquema 2-de-3, três chaves públicas são listadas como possíveis assinantes e pelo menos duas delas devem ser usadas para criar assinaturas para uma transação válida e gastar os fundos.

[MuSig](#): um novo esquema de multi-assinatura baseado em Schnorr que está em desenvolvimento, é projetado para tornar as transações multi-assinatura de Bitcoin menos complexas sem sacrificar a privacidade.

Devido à característica inovadora de agregação de chaves do MuSig, essa assinatura é uma assinatura Schnorr regular que pode ser processada pelo Bitcoin desde a ativação do Taproot. Quando usado para criar carteiras multisig, o MuSig reduz as taxas de transação e aumenta a privacidade em comparação com a forma tradicional de usar o opcode `CHECKMULTISIG` para assinaturas *n-de-n*, que requer *n* chaves públicas e *n* assinaturas ECDSA na blockchain.—Jonas Nick, Tim Ruffing

**Taproot**, ativado na rede Bitcoin em novembro de 2021, permite transações e scripts mais complexos, incluindo aqueles que utilizam assinaturas Schnorr e MuSig. Taproot melhora a privacidade ao tornar transações multisig indistinguíveis de transações regulares.

A BIP que define o Taproot é a [BIP 341](#). Esta proposta de melhoria do Bitcoin introduz o **Pay-to-Taproot (P2TR)**, que combina a funcionalidade dos scripts **Pay-to-PubKey (P2PK)** e **Pay-to-Script-Hash (P2SH)**, oferecendo aos usuários maior flexibilidade e benefícios de privacidade.

Além da [BIP 341](#), o Taproot também inclui:

[BIP 340](#): Implementa a tecnologia de assinatura Schnorr, que é mais segura e flexível, permitindo a agregação de chaves.

[BIP 342](#): Atualiza a linguagem de script do Bitcoin (Tapscript) para acomodar as assinaturas Schnorr e a tecnologia Taproot.

### 3.4 Bitcoin Script

Bitcoin Script é uma linguagem **baseada em pilha**, em **notação polonesa reversa**, e **Turing-incompleta** usada no protocolo Bitcoin para script de transações. É uma linguagem

**interpretada, e não compilada.** Ela é especificamente projetada para processar e validar transações Bitcoin.

O Bitcoin Script é diferente das linguagens de programação tradicionais que requerem um compilador por várias razões. Ela não é uma linguagem compilada, mas sim interpretada, projetada para processamento de transações específicas, seguras e determinísticas dentro da rede Bitcoin.

Os nós do Bitcoin interpretam o script no momento da verificação da transação. A linguagem é intencionalmente limitada em complexidade para evitar riscos de segurança e garantir que a verificação das transações permaneça rápida e determinística.

Ao ser Turing-incompleta, o Bitcoin Script evita loops e estruturas de controle mais complexas que poderiam levar a loops infinitos ou outros riscos computacionais, aumentando a segurança e previsibilidade.

Ela é projetada especificamente para definir condições sob as quais uma transação Bitcoin pode ocorrer, em vez de para computação de propósito geral. Se a saída final da interpretação é True, a transação acontece. Se é False, a transação é rejeitada e não acontece.

O Bitcoin Script opera usando um modelo de execução baseado em pilha, onde operações são empilhadas e desempilhadas durante a execução do script, similar à linguagem Assembly. A natureza determinística das operações baseadas em pilha garante resultados consistentes de validação de transações em todos os nós Bitcoin.

A linguagem inclui um conjunto de comandos básicos (**OPCODES**) para lidar com funções criptográficas, condicionais e outras operações simples necessárias para scripts de transação. A ausência de construtos complexos como funções ou classes reflete seu papel especializado no ecossistema Bitcoin.

Exemplos de uso do Bitcoin Script incluem:

P2PKH (Pay-to-PubKey-Hash): Tipo de script de transação padrão que bloqueia Bitcoin para um hash de chave pública específico.

P2SH (Pay-to-Script-Hash): Permite que scripts mais complexos sejam executados no momento do gasto, facilitando transações multi-assinatura e outros recursos avançados.

### **Script de Bloqueio: ScriptPubKey**

ScriptPubKey é um script que está incluído na saída de uma transação Bitcoin. Ele especifica as condições que devem ser atendidas para que essa saída (UTXO) possa ser gasta em uma transação futura. Basicamente, ele define 'quem' ou 'o que' pode gastar essa UTXO.

**Código de Operação (Opcode):** Scripts no Bitcoin são compostos por uma série de opcodes, que são instruções que a máquina virtual Bitcoin (Bitcoin Script) executa.

**Chave Pública (Public Key) ou Hash da Chave Pública (Public Key Hash):** O ScriptPubKey geralmente contém a chave pública ou o hash da chave pública do destinatário.

Um dos formatos mais comuns de ScriptPubKey é o P2PKH (Pay-to-PubKey-Hash). Vamos ver um exemplo para entender melhor.

#### Exemplo de P2PKH

Quando Alice envia Bitcoin para Bob, a transação cria uma saída que inclui um ScriptPubKey como este:

```
OP_DUP OP_HASH160 <Bob's Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG
```

**OP\_DUP:** Duplica a chave pública que será fornecida na transação de gasto (ou seja, cria uma cópia do item no topo da pilha de execução).

**OP\_HASH160:** Realiza um hash RIPEMD-160 seguido por um hash SHA-256 na chave pública duplicada.

**<Bob's Public Key Hash>:** Este é o hash da chave pública de Bob, que foi fornecido por Alice ao criar a transação.

**OP\_EQUALVERIFY:** Compara os dois valores no topo da pilha (o hash calculado da chave pública fornecida na transação de gasto e o hash da chave pública de Bob). Se eles forem iguais, a verificação continua; caso contrário, a transação falha.

**OP\_CHECKSIG:** Verifica se a assinatura fornecida na transação de gasto é válida para a chave pública fornecida.

#### Condições para Gastar a UTXO

Para gastar a UTXO protegida por este ScriptPubKey, Bob precisa criar uma transação de entrada que forneça:

**Chave pública:** Esta chave pública será usada no script de verificação (ScriptSig) da transação de entrada.

**Assinatura válida:** Esta assinatura deve corresponder à chave pública e à transação, provando que Bob possui a chave privada correspondente à chave pública especificada.

#### Script de Desbloqueio: ScriptSig

Fornece os dados necessários para satisfazer as condições do ScriptPubKey. Se no final da operação o resultado for True, o valor é liberado.

```
<Bob's Signature> <Bob's Public Key>
```

Quando essa transação de gasto é executada, o script combina o ScriptSig com o ScriptPubKey da seguinte maneira:

Chave pública de Bob é duplicada (OP\_DUP) e depois hashada (OP\_HASH160).

O hash resultante é comparado ao hash da chave pública armazenado na UTXO (OP\_EQUALVERIFY).

Se o hash é igual, a assinatura de Bob é verificada em relação à chave pública e à transação (OP\_CHECKSIG).

Se todas essas condições forem atendidas, a UTXO é considerada gasta, e a transação é validada.

O ScriptPubKey define as condições sob as quais uma UTXO pode ser gasta, garantindo que apenas o detentor da chave privada correspondente à chave pública (ou hash da chave pública) especificada possa gastar os fundos. Isso é fundamental para a segurança e integridade das transações Bitcoin.

### Assinatura MultiSig

A forma geral de um script de transação multi-assinatura *M-de-N* é a seguinte:

```
M <Chave Pública 1> <Chave Pública 2> ... <Chave Pública N> N  
OP_CHECKMULTISIG
```

No caso de uma transação multi-assinatura 2-de-3, o script de bloqueio é assim:

```
2 <Chave Pública A> <Chave Pública B> <Chave Pública C> 3 OP_CHECKMULTISIG
```

**2** significa que são necessárias 2 assinaturas.

<**Chave Pública A**> <**Chave Pública B**> <**Chave Pública C**> são as 3 chaves públicas envolvidas.

**3** indica que há 3 chaves públicas no total.

**OP\_CHECKMULTISIG** é o opcode que verifica múltiplas assinaturas.

### Script de Desbloqueio

O script acima forma um “script de bloqueio”, que só pode ser desbloqueado por um “script de desbloqueio” equivalente, contendo 2 ou mais assinaturas calculadas a partir das chaves privadas dos assinantes, correspondendo às chaves públicas listadas:

```
OP_0 <Assinatura B> <Assinatura C>
```

**OP\_0** é necessário devido a um bug histórico no Bitcoin que exige um zero adicional para o script MultiSig.

**<Assinatura B> <Assinatura C>** são duas assinaturas válidas correspondentes a duas das chaves públicas mencionadas no Script de Bloqueio.

### Script de Validação

Quando uma transação é verificada, o Script de Desbloqueio e o Script de Bloqueio são combinados para formar o Script de Validação:

```
OP_0 <Assinatura B> <Assinatura C> 2 <Chave Pública A> <Chave Pública B>
<Chave Pública C> 3 OP_CHECKMULTISIG
```

Essa configuração permite que uma transação multi-assinatura seja validada corretamente, garantindo que as assinaturas exigidas correspondam às chaves públicas listadas no script.

Aprenda mais sobre transações lendo o artigo [Desmembrando uma Transação Bitcoin P2PKH](#) por Rachel Rybarczyk—Board Member da Scalar School.

## 3.5 Miniscript

Miniscript é uma linguagem desenvolvida para escrever scripts Bitcoin de uma maneira estruturada, permitindo análise, composição, assinatura genérica e mais. Foi projetada e implementada por Pieter Wuille, Andrew Poelstra e Sanket Kanjalkar na Blockstream Research. O objetivo do Miniscript é facilitar a criação de condições de gasto complexas e garantir a segurança, eficiência e interoperabilidade dos scripts Bitcoin.

Miniscript oferece uma representação estruturada dos scripts Bitcoin, permitindo que o software analise automaticamente o script e determine quais dados de testemunha devem ser gerados para gastar os bitcoins protegidos por esse script.

A linguagem de script do Bitcoin permite que scripts sejam compostos a partir de expressões menores e válidas, facilitando a criação de condições de gasto complexas. Isso é especialmente útil para desenvolvedores de carteiras, que não precisam reescrever códigos ao mudar de um modelo de script para outro.

Miniscript otimiza a compilação de transações, o que pode resultar em uma pegada menor na blockchain, economizando taxas de transação. Além disso, a estrutura de Miniscript facilita a criação de contratos inteligentes mais complexos e seguros diretamente na blockchain base do Bitcoin.

**Multisig Decrescente:** Permite a criação de carteiras multisig onde o número de assinaturas necessárias pode diminuir ao longo do tempo ou após um determinado período, proporcionando flexibilidade adicional em casos como perda de chaves.

**Herança e Timelocks:** Facilita a criação de carteiras de herança onde os fundos podem ser acessados por herdeiros após um determinado período, funcionando como uma espécie de "switch" de herança automatizada.

O Bitcoin Script é uma linguagem baseada em pilha com muitos casos especiais, projetada para implementar condições de gasto que consistem em várias combinações de assinaturas, hash locks e time locks. No entanto, trabalhar diretamente com o Bitcoin Script pode ser difícil e sujeito a erros, especialmente para condições de gasto complexas. Miniscript resolve esses problemas ao fornecer uma maneira mais estruturada e fácil de entender e compilar scripts Bitcoin.

Miniscript promete facilitar o desenvolvimento de scripts Bitcoin mais seguros e eficientes, melhorando a usabilidade e a segurança para desenvolvedores e usuários finais. Embora a adoção possa levar algum tempo, suas vantagens em termos de segurança, flexibilidade e eficiência tornam-no uma ferramenta valiosa para o futuro do desenvolvimento de transações no Bitcoin.

Para saber mais sobre Bitcoin Miniscript, acesse <https://bitcoinops.org/en/topics/miniscript/>

### 3.6 CoinJoin

O CoinJoin é uma transação de Bitcoin onde múltiplos usuários combinam seus UTXOs, melhorando a privacidade. É uma das ferramentas essenciais para a preservação dos direitos humanos no contexto do uso do Bitcoin. Ele permite que transações sejam misturadas de forma a aumentar a privacidade dos usuários, tornando mais difícil rastrear a origem e o destino dos fundos. Em um mundo onde a vigilância financeira é crescente, proteger a privacidade das transações é crucial para garantir a liberdade individual e a segurança de ativistas, jornalistas e cidadãos comuns que vivem sob regimes opressivos.

Greg Maxwell escreveu no fórum Bitcointalk em 2013: "O Bitcoin é frequentemente promovido como uma ferramenta de privacidade, mas a única privacidade que existe no Bitcoin vem de endereços pseudônimos, que são frágeis e facilmente comprometidos por meio de reutilização, análise de "taint", rastreamento de pagamentos, monitoramento de nós de endereço IP, web-spidering e muitos outros mecanismos. Uma vez quebrada, essa privacidade é difícil e às vezes custosa de recuperar..."

Adotar o CoinJoin desde o início da trajetória como usuário de Bitcoin é vital. Isso não só protege a privacidade individual, mas também fortalece a rede como um todo, dificultando que entidades maliciosas rastreiem transações e identifiquem usuários. A privacidade financeira é um pilar para a liberdade e autonomia, e seu uso disseminado pode ser uma ferramenta poderosa para preservar um futuro onde os direitos humanos são respeitados e protegidos.

**Combinação de Transações:** CoinJoin é um método onde múltiplos usuários juntam suas transações em uma única transação Bitcoin. Isso significa que várias entradas e saídas de diferentes usuários são combinadas em um único bloco.

**Anonimato através da mistura (coin mixing):** Ao combinar transações de múltiplos usuários, fica difícil determinar qual saída pertence a qual entrada original. Isso aumenta a privacidade, pois observadores externos não conseguem facilmente traçar a origem e o destino dos fundos.

### Etapas do Processo

**Coordenação:** Um coordenador ou servidor CoinJoin junta as intenções de transação de vários participantes.

**Assinaturas Parciais:** Cada participante cria e assina parcialmente suas partes da transação.

**Combinação:** O coordenador combina todas as partes em uma única transação completa.

**Assinatura Final:** Cada participante assina a transação completa.

**Envio:** A transação finalizada é enviada para a rede Bitcoin.

### Ferramentas de Coin Join

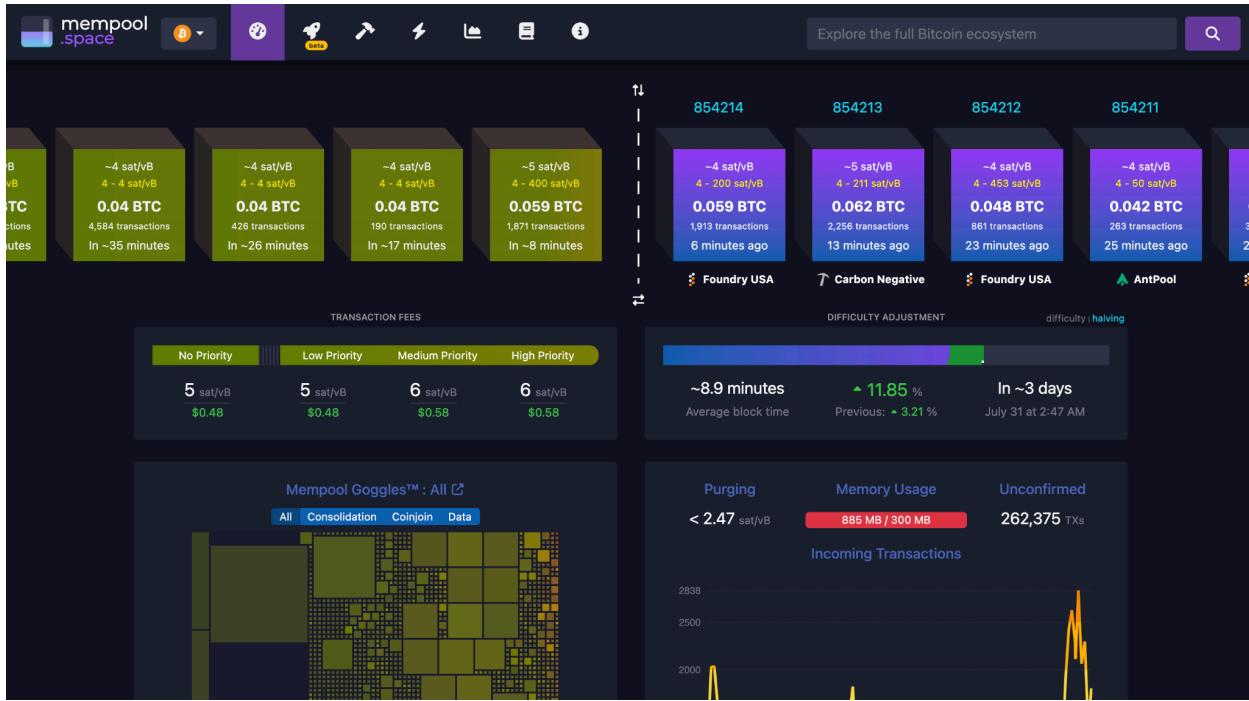
[Wasabi Wallet](#),

[Sparrow Wallet](#)

[Jam](#) que é uma interface UI para o software [JoinMarket](#)

## 3.7 Exploradores de Blocos

Um explorador de blocos é uma ferramenta indispensável para visualizar e interagir com a rede Bitcoin. Ele permite que você acesse uma vasta gama de informações detalhadas sobre transações, blocos e endereços. Veja um snapshot do explorador de blocos mempool.space.



## Informações sobre transações

Com um explorador de blocos, você pode consultar detalhes sobre transações, como entradas, saídas, taxas de rede e troco. Isso facilita a observação de como cada transação está conectada a transações anteriores, promovendo transparência e rastreabilidade.

Você pode verificar o número de confirmações de uma transação, indicando sua segurança e imutabilidade, bem como o tempo de inclusão de uma transação em um bloco específico.

Além disso, é possível visualizar os scripts de bloqueio (ScriptPubKey) e desbloqueio (ScriptSig) das transações e obter informações detalhadas sobre cada entrada e saída, incluindo endereços envolvidos e valores transferidos.

Os blocos minerados possuem informações detalhadas, como o minerador responsável, o tamanho do bloco, o número de transações incluídas e a recompensa total do bloco, que inclui a recompensa base e as taxas de transação coletadas.

Você pode visualizar o saldo atual de um endereço específico e seu histórico completo de transações, oferecendo uma visão clara das movimentações de fundos.

Exploradores de blocos também oferecem acesso a estatísticas da rede. Você pode ver a taxa de hash atual da rede, indicando o poder computacional total utilizado para minerar blocos, e a dificuldade de mineração, que ajusta periodicamente para manter o tempo de bloco constante.

## Funcionalidades adicionais

Alguns exploradores de blocos oferecem funcionalidades adicionais, como alertas e notificações. Você pode configurar alertas para ser notificado quando uma transação específica for confirmada ou quando um endereço receber ou enviar fundos. Isso ajuda a monitorar atividades relevantes na blockchain em tempo real.

### **APIs para desenvolvedores**

Exploradores de blocos também podem oferecer APIs de dados, permitindo que desenvolvedores accessem programaticamente informações da blockchain para integrar em seus aplicativos. Isso é essencial para o desenvolvimento de ferramentas e serviços que interagem diretamente com a blockchain Bitcoin.

### **Privacidade e segurança com um nó próprio**

Quando você acessa um explorador de blocos no navegador, ele faz uma solicitação a um nó da rede Bitcoin para obter dados específicos. O nó processa a solicitação, extrai os dados relevantes da blockchain e os envia de volta ao explorador, que então apresenta essas informações de forma amigável e acessível. Geralmente, esses nós são operados por terceiros, como empresas ou organizações. Embora conveniente, há riscos associados a confiar nesses nós, como problemas de privacidade, confiabilidade dos dados, censura e segurança.

Para mitigar esses riscos, é possível instalar um explorador de blocos em seu próprio nó Bitcoin. Isso oferece total controle sobre os dados consultados, evitando que terceiros monitorem suas atividades e garantindo que você esteja acessando informações diretamente de um nó de confiança.

### **Informações disponíveis em exploradores de blocos**

**Taxa de Hash:** Indica o poder computacional total que está sendo usado para minerar blocos.

**Dificuldade de Mineração:** Ajustada periodicamente para manter o tempo de bloco constante.

**Número Total de Nós:** Exibe a quantidade de nós ativos na rede Bitcoin.

**Altura do Bloco:** O número do bloco mais recente na blockchain.

**Volume de Transações:** Quantidade total de transações confirmadas em um determinado período.

**Tamanho da Blockchain:** O tamanho total da blockchain, em gigabytes.

**Confirmações de Transações:** Número de confirmações que uma transação recebeu, indicando sua segurança e imutabilidade.

**Tempo de Transação:** Carimbo de data/hora quando a transação foi incluída em um bloco.

**Script de Bloqueio e Desbloqueio:** Visualização dos scripts de bloqueio (ScriptPubKey) e desbloqueio (ScriptSig) das transações.

**Detalhes de Entrada e Saída:** Informações detalhadas sobre cada entrada e saída, incluindo endereços envolvidos e valores transferidos.

**Taxa de Transação:** Taxa paga para incluir a transação no bloco.

**Tamanho da Transação:** Tamanho total da transação em bytes.

**Mempool:** Transações pendentes que ainda não foram confirmadas e incluídas em um bloco.

**Minerador:** Identificação do minerador que minerou o bloco (quando disponível).

**Tamanho do Bloco:** O tamanho total do bloco em bytes.

**Número de Transações:** Quantidade de transações incluídas no bloco.

**Recompensa do Bloco:** A recompensa total recebida pelo minerador, incluindo a recompensa base e as taxas de transação.

**Tempo de Mineração:** O tempo que levou para minerar o bloco.

**Nonce:** Valor que os mineradores ajustam para encontrar um hash válido para o bloco.

**Versão do Bloco:** Número de versão do bloco.

**Saldo Atual de um Endereço:** O saldo total de um endereço específico.

**Histórico de Transações:** Todas as transações que envolveram o endereço, incluindo valores recebidos e enviados.

**Saldo Não Confirmado:** Saldo de transações que ainda não foram confirmadas.

**Primeira e Última Transação:** Datas da primeira e da última transação associada ao endereço.

**Taxas Médias de Transação:** Taxas de transação médias pagas em um determinado período.

**Estimativas de Taxas:** Estimativas de taxas recomendadas para que as transações sejam confirmadas dentro de um determinado número de blocos.

**Taxas Pagas por Bloco:** Taxas de transação totais pagas em cada bloco.

Exploradores de blocos são ferramentas versáteis que fornecem uma vasta gama de informações e funcionalidades, desde detalhes básicos de transações até análises avançadas e integrações API. Eles são essenciais para usuários que desejam entender melhor o funcionamento da blockchain Bitcoin, monitorar suas transações e desenvolver aplicações que interagem com a rede.

Você pode usar qualquer explorador de blocos para pesquisar por toda a blockchain, já que todas as transações são publicamente visíveis. Para começar, veja uma lista deles em <http://bit.ly/blockexplorers>. Os mais usados são [mempool.space](#) e [blockstream.info](#). Escolha qualquer transação, siga-a e veja o que você pode descobrir sobre as entradas, saídas, taxas de rede e troco. Observe como ela está conectada a transações anteriores.

Você pode pesquisar o ID da primeira transação e Bitcoin, ou seja, essencialmente, o primeiro txid já criado na rede.

Primeira transação de Bitcoin: Satoshi Nakamoto enviou a Hall Finney 10 BTC

f4184fc596403b9d638783cf57adfe4c75c605f6356fb91338530e9831e9e16

## Estrutura de Dados Blockchain

A ferramenta interativa de blockchain no site de Anders Brownworth é um recurso educacional projetado para ajudar usuários a entender os conceitos fundamentais da tecnologia blockchain. Ela simula como uma blockchain funciona, permitindo que você explore e visualize de maneira

prática os processos de criação de blocos, hash, encadeamento de blocos, e como as transações são registradas de forma segura e imutável.

<https://andersbrownworth.com/blockchain/blockchain>

### 3.8 Taxas de Transação

As taxas de transação são pequenas quantias de Bitcoin que os usuários pagam para que suas transações sejam processadas e confirmadas pelos mineradores. Essas taxas servem como um incentivo para os mineradores incluírem a transação no próximo bloco que minerarem.

Outro recurso importante nos exploradores de blocos é a análise das taxas de transação. Você pode consultar as taxas médias pagas em um determinado período e obter estimativas de taxas recomendadas para que as transações sejam confirmadas rapidamente. Isso é particularmente útil para usuários que desejam otimizar o custo de suas transações.

A taxa não é fixa e pode variar com base em vários fatores:

**Tamanho da Transação:** Transações maiores (em termos de tamanho de dados, não a quantia de Bitcoin) requerem mais espaço em um bloco, o que pode aumentar a taxa. O uso de várias UTXOs pequenas tem um custo maior que uma única UTXO de valor equivalente.

**Congestionamento da Rede:** Quando a rede está ocupada, as taxas tendem a subir à medida que os usuários competem para que suas transações sejam confirmadas rapidamente.

**Prioridade do Usuário:** Os usuários podem optar por pagar taxas mais altas para acelerar suas transações. Taxas mais altas geralmente resultam em confirmações mais rápidas.

As taxas de transação são geralmente calculadas por byte de dados na transação. O software da carteira frequentemente sugere uma taxa apropriada com base nas condições atuais da rede, garantindo que a transação seja confirmada dentro de um tempo razoável. Os usuários podem definir suas taxas manualmente, mas definir uma taxa muito baixa pode resultar em confirmações atrasadas.

Quando você envia Bitcoin pela rede, o software da carteira permite que você insira o valor da taxa que deseja pagar. Conhecer a taxa média no momento da transação e escolher um valor ligeiramente acima aumenta a probabilidade de que sua transação seja confirmada no tempo desejado.

#### Bytes Virtuais (vbytes)

Bytes virtuais (vbytes) são uma unidade de medida usada para calcular as taxas de transação no Bitcoin de maneira mais eficiente e justa, especialmente após a ativação do Segregated Witness (SegWit). Eles ajudam a refletir melhor o impacto real de uma transação na blockchain.

O SegWit foi uma atualização no protocolo Bitcoin que, entre outras coisas, separou a assinatura (witness) dos dados da transação. Esta atualização permitiu uma melhor utilização do espaço no bloco, aumentando a capacidade das transações sem alterar o tamanho máximo do bloco de 1 MB.

Antes do SegWit, as taxas de transação eram baseadas no tamanho total da transação em bytes. Após o SegWit, as transações possuem duas partes: dados regulares e dados de witness. Os dados de witness são menos críticos para a propagação da rede e validação, então, uma nova forma de medir o impacto das transações foi necessária.

### **Definição e cálculo dos vbytes**

Um vbyte é uma unidade de medida que ajusta o tamanho real de uma transação, considerando o peso diferenciado dos dados de witness. A fórmula básica para calcular vbytes é:

$$\text{vbytes} = \frac{\text{weight}}{4}$$

Onde weight (peso) é uma métrica que combina o tamanho dos dados regulares e dos dados de witness.

### **Weight units (WU)**

Cada byte de dados regulares da transação conta como 4 unidades de peso.

Cada byte de dados de witness conta como 1 unidade de peso.

Por exemplo, se uma transação tiver:

100 bytes de dados regulares:  $100 \times 4 = 400$  weight units

200 bytes de dados de witness:  $200 \times 1 = 200$  weight units.

Peso total:  $400 + 200 = 600$  weight units.

Então, os vbytes seriam:

$$\text{vbytes} = \frac{600}{4} = 150$$

Usar vbytes no cálculo das taxas de transação permite uma melhor correlação entre a taxa paga e o uso real do espaço no bloco, promovendo uma alocação mais eficiente dos recursos

da rede. Transações SegWit tendem a ser mais compactas em termos de vbytes, resultando em taxas mais baixas. Isso incentiva os usuários a adotarem SegWit, aumentando a capacidade efetiva da rede.

**Replace-by-Fee (RBF)** é uma funcionalidade no protocolo Bitcoin que permite ao remetente de uma transação substituir uma transação pendente (não confirmada) por uma nova transação com uma taxa de transação mais alta. O objetivo principal do RBF é aumentar a probabilidade de confirmação da transação em tempos de congestionamento da rede. Muitos softwares de carteira possuem essa funcionalidade embutida.

**Valor do Bitcoin:** Para saber quando isso vale equivalentemente na sua moeda local, você pode buscar 'preço do Bitcoin' no Google ou ferramentas de conversão de moedas. O Google geralmente tem uma função embutida de conversão quando você procura pelo preço, mas existem outras alternativas, como <https://cointradermonitor.com/>. É sempre bom checar de mais de uma fonte.

**Curiosidade Histórica:** A taxa de rede do Bitcoin atingiu seu valor máximo no dia do halving de 2024, em 19 de abril. Isso indica duas coisas. Primeiro, quando não houver mais subsídios de bloco disponíveis, os mineradores podem viver das taxas de rede. Segundo, as soluções de escalabilidade de camada 2, como a Lightning Network, são extremamente importantes para manter as taxas de transação baixas e a rede Bitcoin eficiente. Eu tirei um print do celular, pois nesse momento eu estava em uma aula de Matemática Discreta da [Fatec](#). 2832 sats/vB.

VIVO 5G 9:58 PM 58%

mempool.space

 mempool  
.space

Explore the full Bitcoin ecosystem

Block Subsidy has halved to 3.125 BTC per block

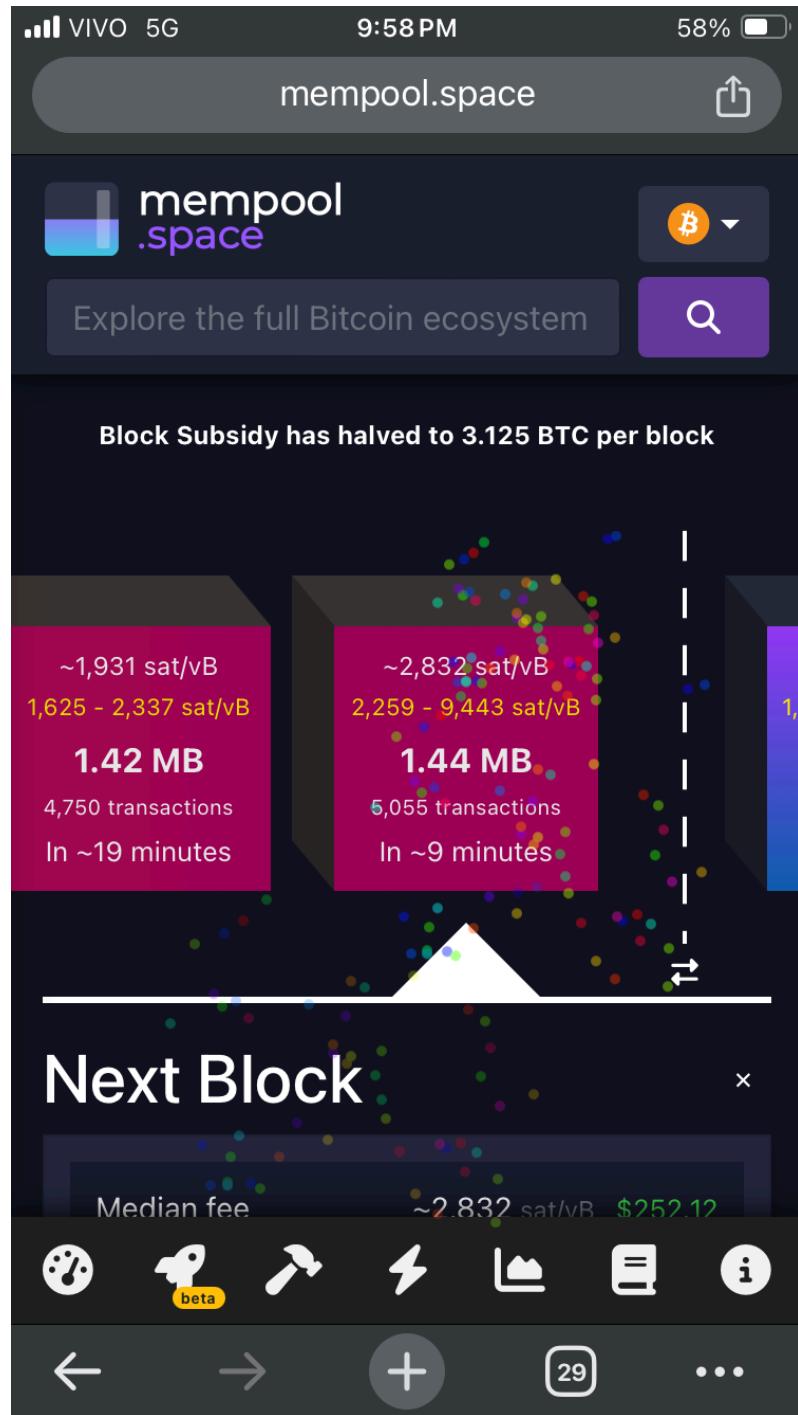
**1.42 MB**  
~1,931 sat/vB  
1,625 - 2,337 sat/vB  
4,750 transactions  
In ~19 minutes

**1.44 MB**  
~2,832 sat/vB  
2,259 - 9,443 sat/vB  
5,055 transactions  
In ~9 minutes

Median fee ~2.832 sat/vB \$252.12

Next Block

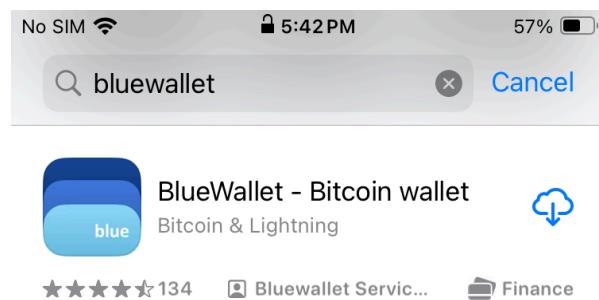
← → + 29 ...



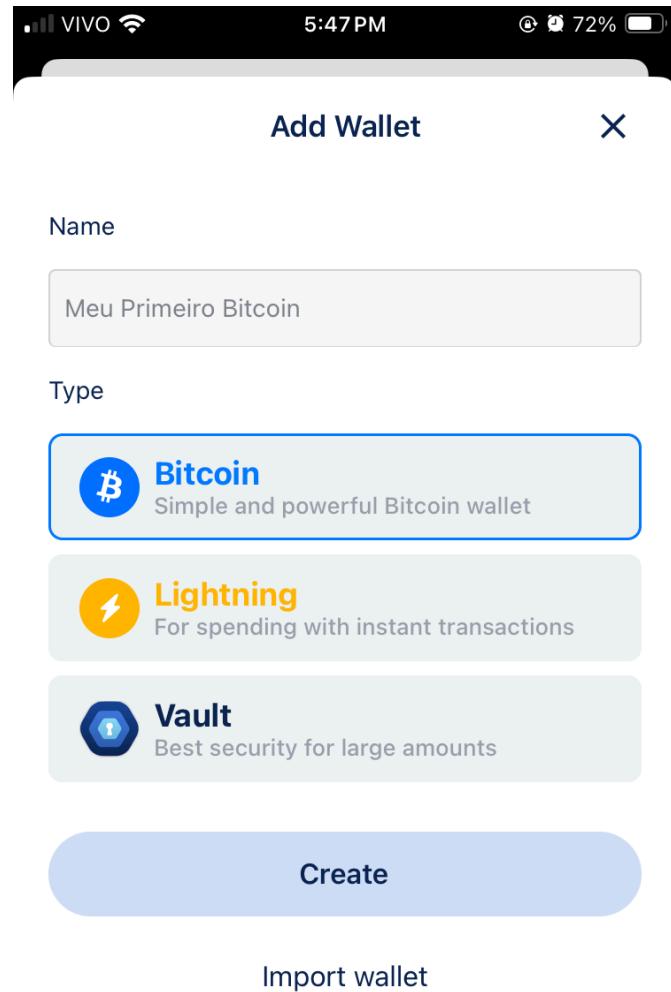
### 3.9 Prática: Meu Primeiro Bitcoin On-Chain

Vamos verificar a experiência de uma transação Bitcoin na prática. Dentro de um único aplicativo de carteiras Bitcoin, a [BlueWallet](#), é possível criar diversas carteiras. Então eu vou testar o envio de satoshis de uma carteira para outra que pertencem a mim mesma. O processo para envio à carteira de outra pessoa é exatamente igual. Vamos começar.

Primeiro você procura na App Store ou Play Store por BlueWallet.



Agora, no fluxo de acesso, você terá a opção de criar uma carteira. Escolha a primeira, Bitcoin—Simple and powerful Bitcoin wallet.



Anote sua seed, de preferência com lápis pois não sai com água nem álcool. Não tire print!

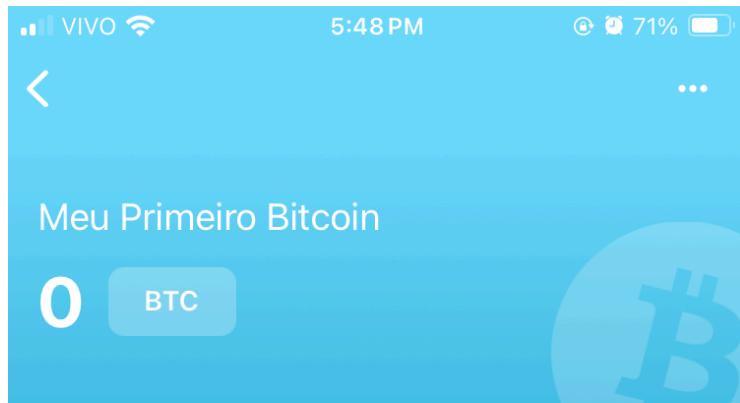


Please take a moment to write down this mnemonic phrase on a piece of paper. It's your backup and you can use it to recover the wallet.

- 1. return
- 2. cook
- 3. verify
- 4. quality
- 5. parade
- 6. forget
- 7. joy
- 8. stumble
- 9. flip
- 10. share
- 11. rescue
- 12. grab

OK, I wrote it down.

Depois de anotada, OK, I wrote it down vai te levar para a tela principal da sua carteira.



## Transactions

Your transactions will appear here.

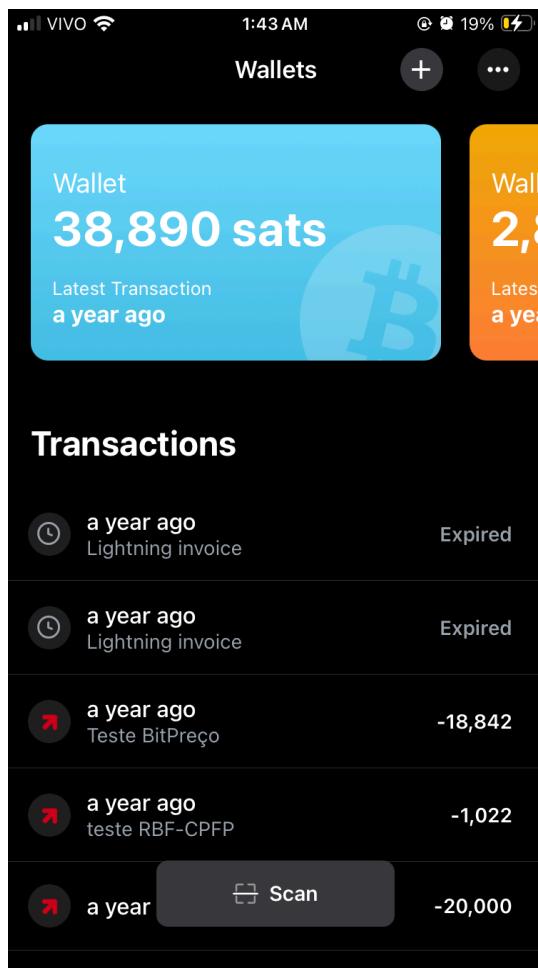
Receive

Send

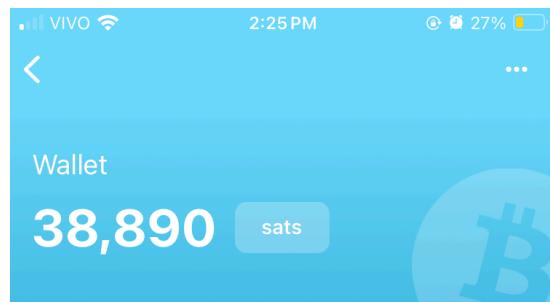
Como essa carteira está zerada, vamos usar ela pra receber uns satoshis. Clique em **Receive**. Um endereço de recebimento aparecerá na tela.



Clicando nesse endereço, ele vai para a área de transferência e consigo compartilhar com a pessoa que vai me pagar. Que no caso sou eu mesma. Agora, vamos para uma outra carteira, que tem uns satoshis, e tentar enviar pra esse endereço. No processo é copiar e colar, tomem cuidado, chequem bem se todos os caracteres estão batendo exatamente com o que foi gerado na carteira, especialmente se for entre vocês e corretoras. Existem malwares por aí que alteram esse endereço e, se você não tiver atenção, pode estar enviando Bitcoin para um mau ator. Além disso, sempre que adquirir Bitcoin, certifique-se de transferi-lo para um endereço gerado por uma carteira que seja sua. Tenha cuidado ao deixar Bitcoin em plataformas de terceiros, como corretoras. Não é seguro.



Entramos na outra carteira que tem o dinheiro, e vamos enviar para esse endereço da carteira Meu Primeiro Bitcoin.



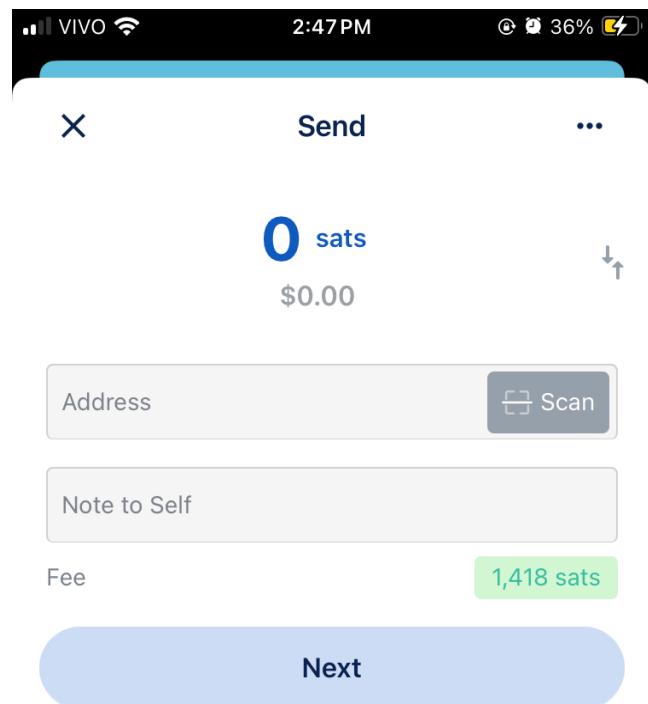
## Transactions

	a year ago Teste BitPreço	-18,842
	a year ago teste RBF-CPFP	-1,022
	a year ago	-20,000
	a year ago	7,885
	a year ago Child pays for parent (CPFP)	-2,352

Receive

Send

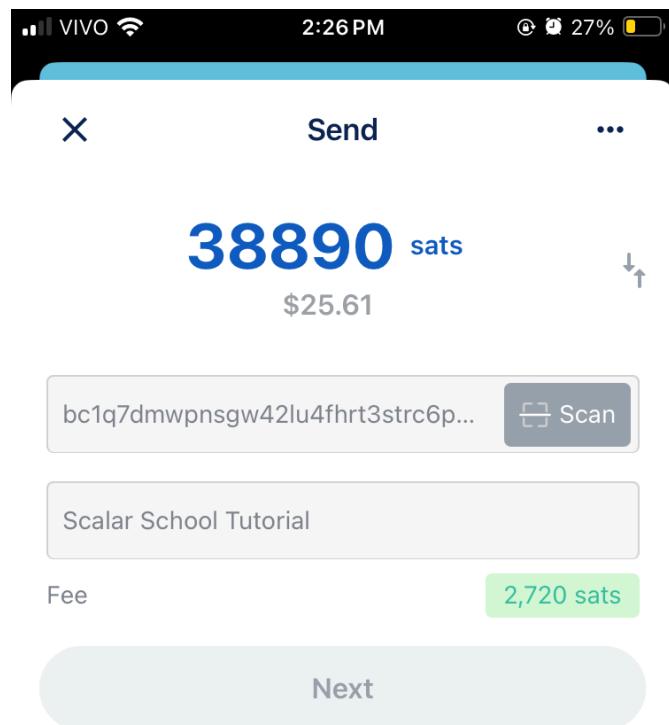
Para isso, clique em **Send**. Lembre-se que o endereço que vai receber já está na área de transferência, e é só colar no campo certo.



select wallet >

Wallet

No campo **Address**, cole o endereço. Em **Note to Self**, escreva um comentário identificador dessa transação (essas notas não vão para a blockchain, são metadados a nível do aplicativo de carteiras somente). Onde mostra o valor, coloque o valor que deseja enviar.

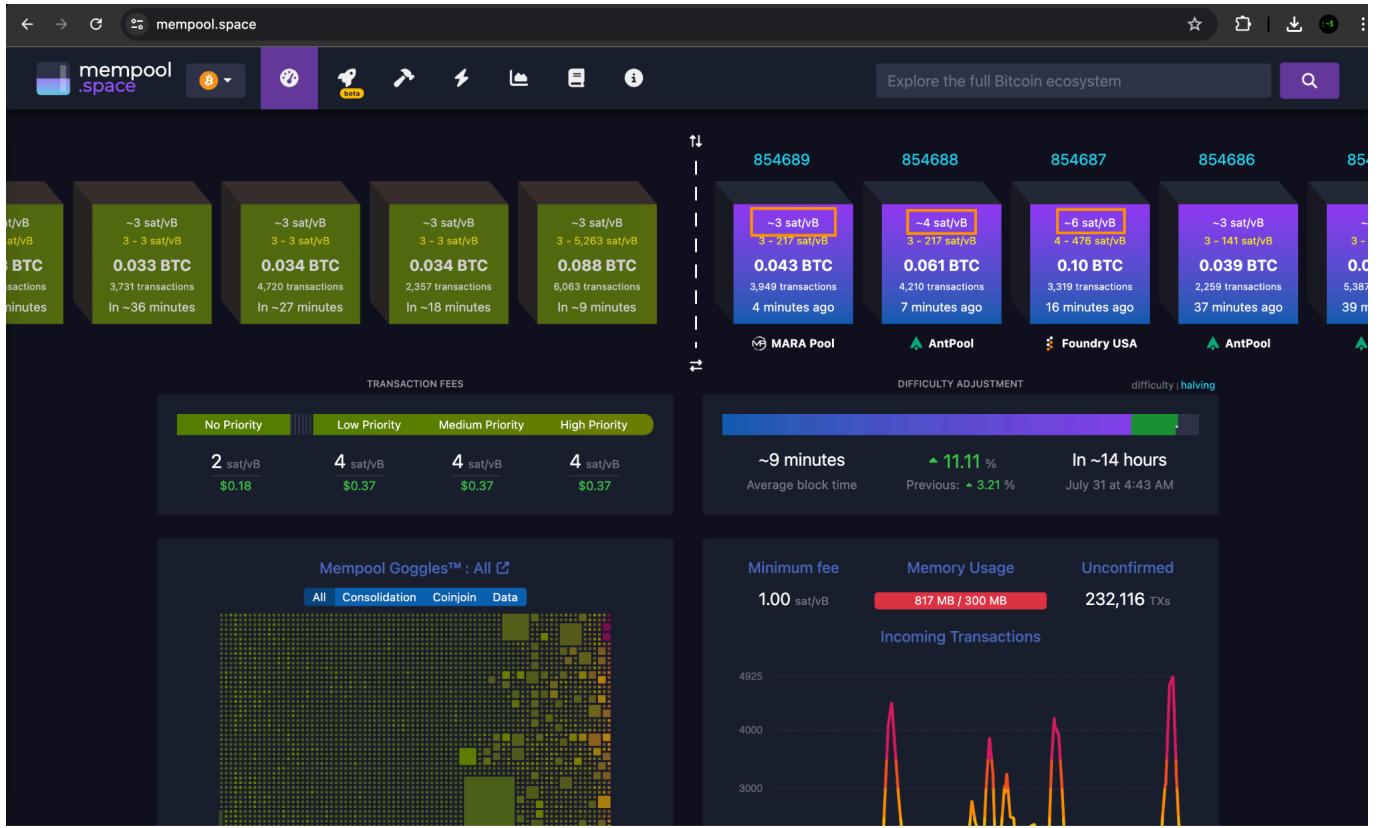


select wallet >

Wallet

No caso eu escrevi o valor total.

Mas veja que o botão **Next** ficou inativo! Isso é porque eu não considerei a taxa de rede que precisarei pagar para a transação ser processada, que é tirada da própria carteira. Vamos verificar o ambiente de taxas de rede. Acesse [mempool.space](https://mempool.space) e vamos ver qual a taxa média que está sendo suficiente para as transações serem incluídas em blocos.

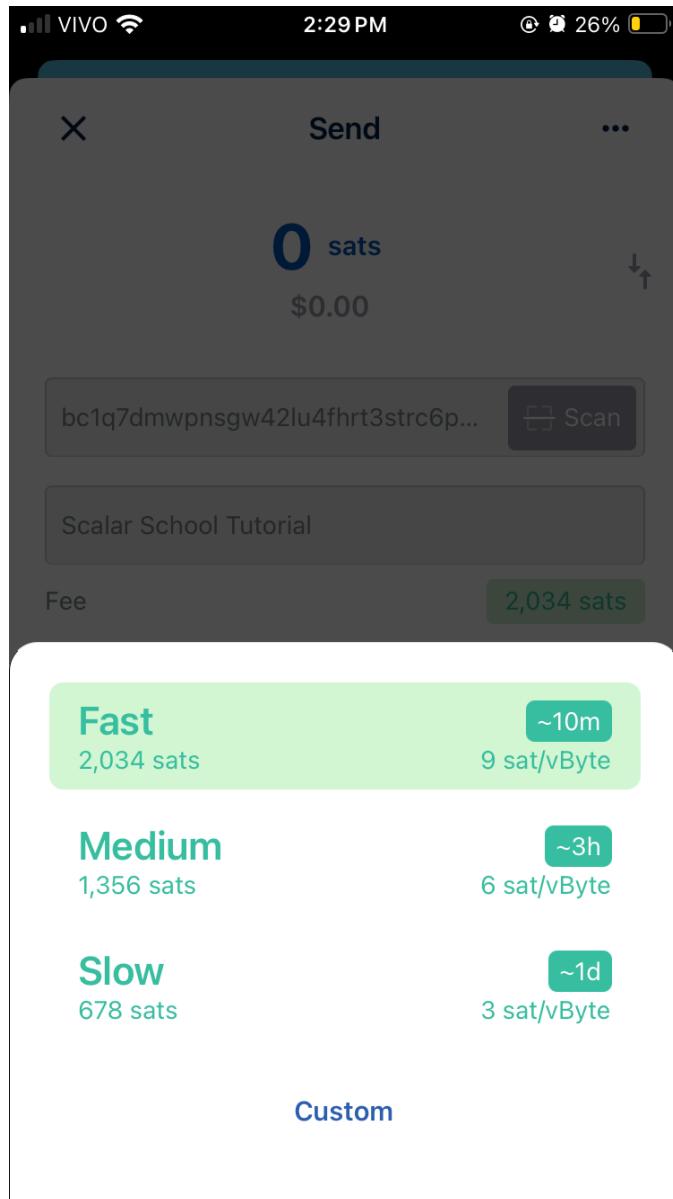


3 sats por bytes virtuais, 4 sats por bytes virtuais, 6 sats por bytes virtuais. Lembre-se que cada transação possui um conjunto de dados que precisam ser registrados na blockchain, e esses dados ocupam espaço em disco.

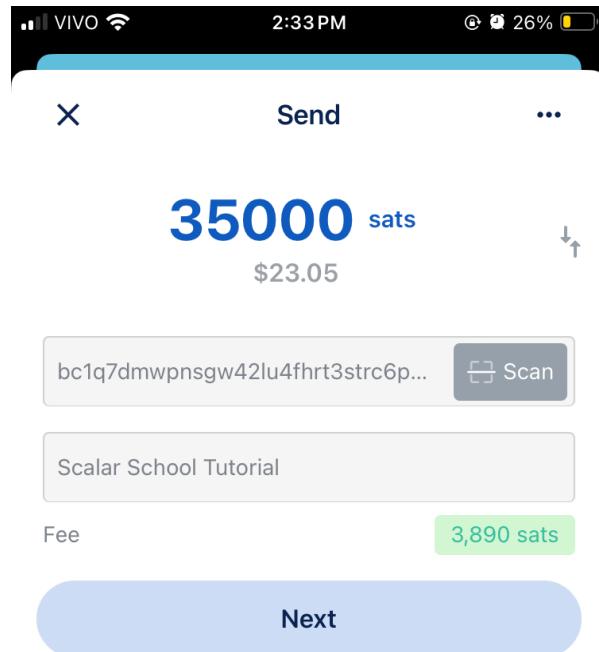
O valor total de uma transação depende do tanto de espaço que estamos demandando para a rede processar. Se eu fizer um pagamento de 38.000 sats que usa inúmeras UTXOs pequenas para somar o valor total, vai ser mais caro que realizar um pagamento de 38.000 sats com apenas uma UTXO de saída.

Por isso existe um processo chamado **consolidação de UTXOs**, que é quando um bitcoiner aproveita que as taxas de rede estão baixas para enviar o valor total de uma carteira pra outra, consolidando várias UTXOs menores em uma grande que será bem mais barata para transacionar no futuro.

Voltando à carteira, vamos clicar naquele campo em verde de definição de taxas.



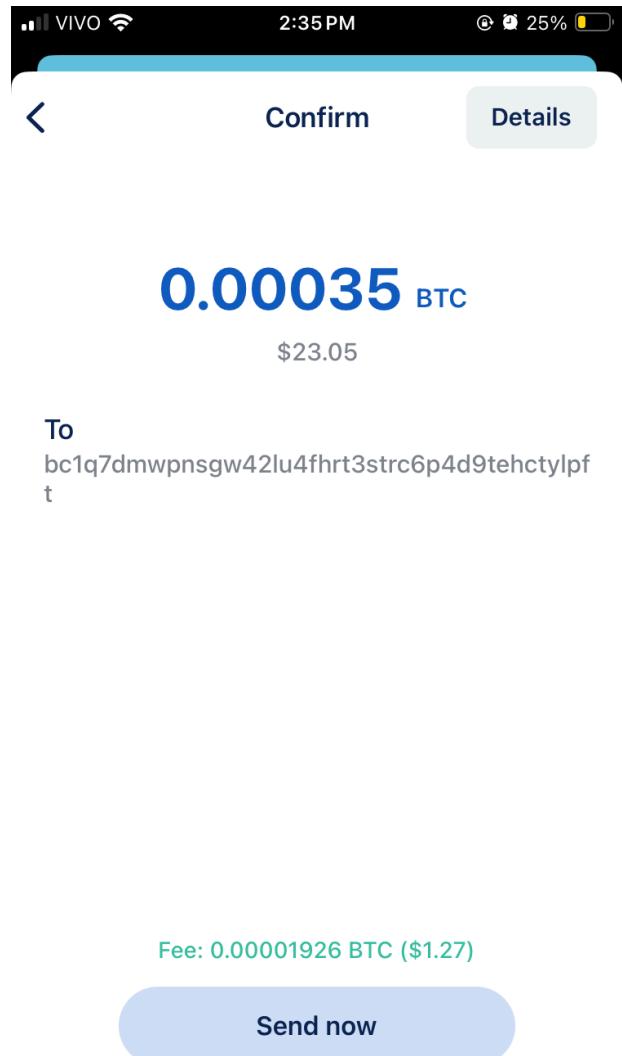
O aplicativo indica que, para nossa transação ser confirmada (incluída em bloco) rapidamente, devemos pagar em torno de 9 sats/vByte. Isso é bem acima do valor que verificamos no explorador de blocos, mas tudo bem, vou aceitar a sugestão. Note que eu fui baixando o valor manualmente até o botão **Next** ficar ativo, ou seja, até que o valor das taxas fossem cobertos.



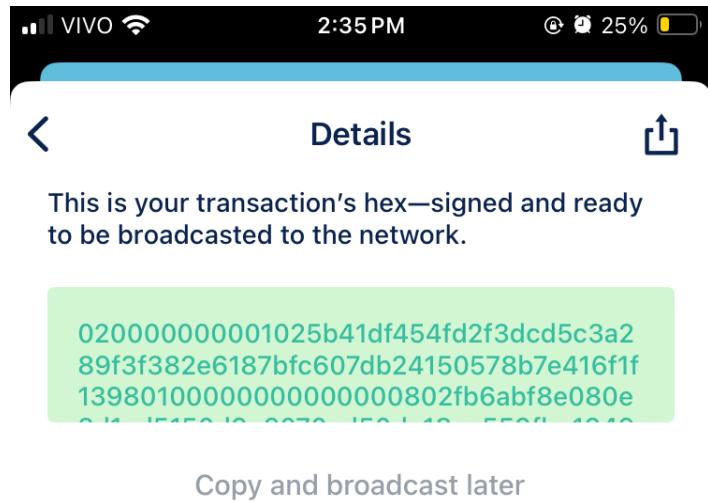
select wallet >

Wallet

Clicando em **Next**, entramos nessa tela. O app está mostrando o valor em BTC, mas você pode escolher sempre visualizar em sats. Lembrando que **1 Bitcoin = 100,000,000 Satoshi**



Clicando em **Details**, conseguimos acessar mais informações sobre a estrutura dessa transação.



Verify on coinb.in

To  
bc1q7dmwpnsgw42lu4fhrt3strc6p4d9tehcylpf  
t

Amount  
0.00035 BTC

Fee  
0.00001926 BTC

## Transaction Size

209 bytes

Transaction Size  
209 vbytes

Satoshi per vByte  
**9 Sat/vB**

Um hexadecimal de transação (hex) é uma representação serializada de uma transação Bitcoin. É essencialmente os dados brutos da transação codificados em formato hexadecimal. Esta string hex contém todas as informações necessárias sobre a transação, incluindo número da versão, entradas (hash da transação anterior, índice, scriptSig, sequência), saídas (valor, scriptPubKey), locktime e assinaturas, tornando possível transmiti-la para a rede Bitcoin.

Você pode decidir propagar a transação pela BlueWallet, ou copiar esse hex e propagar mais tarde usando outras ferramentas. Os exploradores de blocos geralmente possuem ferramentas de propagação, e você também pode propagar pela linha de comando do seu nó Bitcoin Core, usando o comando `sendrawtransaction`.

No caso, voltamos à tela anterior e clicamos em **Send now**.



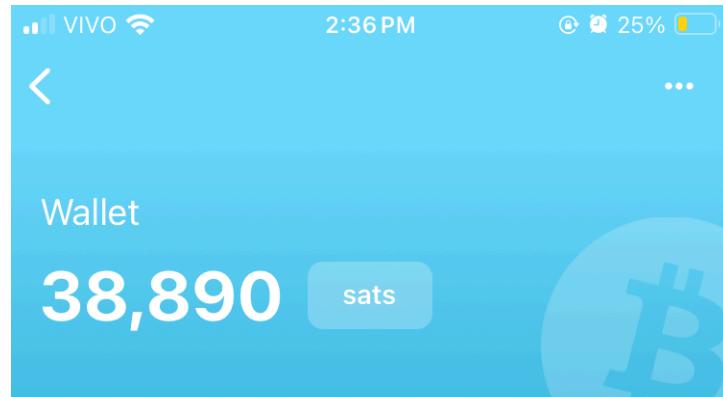
**0.00035 BTC**

Fee: 0.00001926 BTC



Done

Na tela principal, vemos a transação como Pending. Ela foi transmitida para a mempool, mas ainda não foi incluída em bloco.



## Transactions

<span>...</span>	Pending Conf: 0 Scalar School Tutorial	-36,926
<span>↗</span>	a year ago Teste BitPreço	-18,842
<span>↗</span>	a year ago teste RBF-CPFP	-1,022
<span>↗</span>	a year ago	-20,000
<span>↘</span>	a year ago	7,885
	<span>Receive</span>	<span>Send</span>
	Child pays for parent (CPFP)	

Clicando nela, vemos a opção de Bump fee, que é a função RBF. Vamos supor que a taxa de rede aumentou rapidamente, e você quer atualizar o valor e adicionar um extra de taxas para que sua transação acompanhe a média. É nesse momento que você usa a Bump fee. Também tem a opção de cancelar a transação. Mas após ela ser confirmada, ou incluída em bloco, ela se torna irreversível.

■■■ VIVO

2:36 PM

⌚ 25% 🔋



Details

**-36,926 sats**

Scalar School Tutorial



0 confirmations

ETA: In ~10 minutes

Bump Fee

Cancel Transaction

Clicando em details, conseguimos acessar o ID da transação.



## Transaction

Save

Scalar School Tutorial

## Input

[Copy](#)

```
bc1qymuu9ggspr5ayyy2m3e0pc8l09haydzm4  
meh4p,  
bc1qhcq7wpsutwwekm06exedfgypxcwtcdjdj2  
hc6
```

## Output

[Copy](#)

```
bc1q7dmwpnsgw42lu4fhr3strc6p4d9tehctylpf  
t,  
bc1qqchvvs2aun0kel393y33hwd0snj3vz30mg9  
lfs
```

## Transaction ID

[Copy](#)

```
c490e2e0ac7ac9ca8c33d05637494345240f510d  
8fd138a91f69dbf8a5ea115b
```

## Received

July 30, 2024 2:36 PM

## Inputs

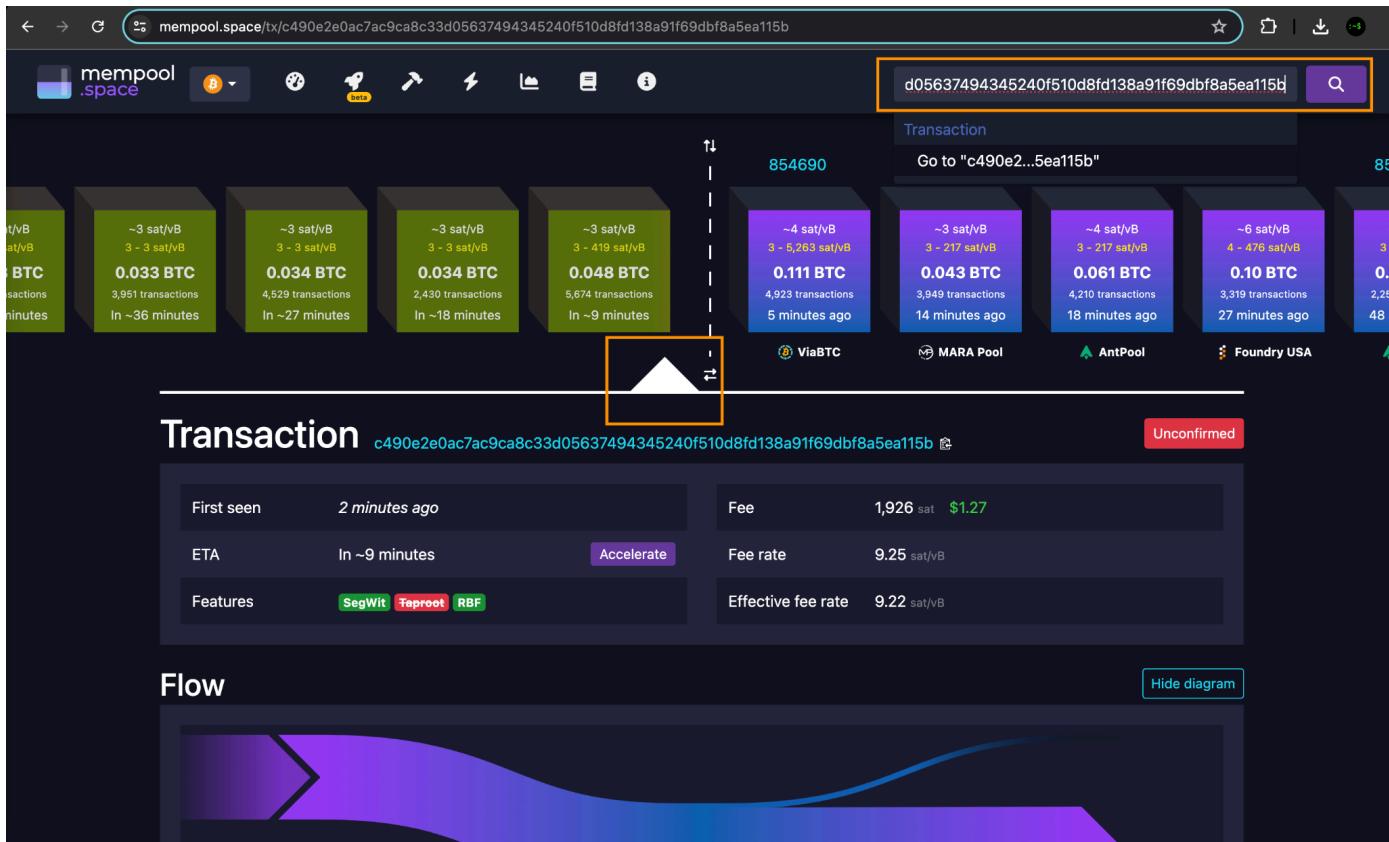
2

## Outputs

2

[View in Block Explorer](#)

Copie este ID e vamos acompanhar nossa transação até que seja confirmada. Você vai colar esse ID no campo de busca de um explorador de blocos. No caso eu usei [mempool.space](#).



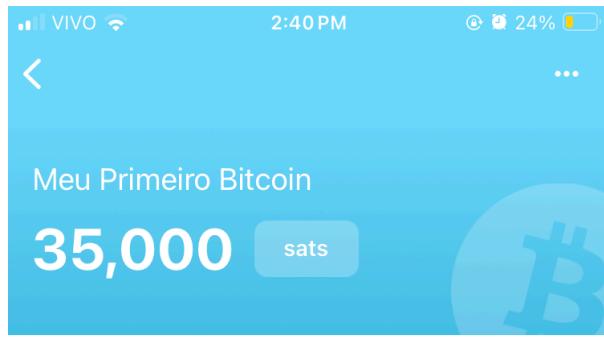
Note que há uma seta branca apontando para a região verde de blocos, que representa a mempool e um agrupamento de transações por valor de taxa—não são blocos reais ainda, mas as transações que estão sendo consideradas em blocos candidatos pelos mineradores. Somente quando essa transação for minerada que entramos em um bloco na parte roxa.

A confirmação dessa transação aconteceu quase em tempo real. Também, pudera, pagamos 3x mais que a taxa que era realmente necessária. Para ser realmente cauteloso em negociações de valores maiores, é recomendável esperar 6 confirmações. Isso garante que não possa haver nenhuma possível reorganização de blocos que coloque sua transação de volta na mempool.

The screenshot shows a dark-themed interface for mempool.space. At the top, there's a navigation bar with icons for search, refresh, and other functions. The main area displays a timeline of transactions. On the left, several green-colored boxes show recent transactions with details like fees (e.g., ~3 sat/vB), amounts (e.g., 0.033 BTC), and confirmation times (e.g., In ~36 minutes). On the right, a series of purple boxes show more recent transactions, with one highlighted in blue. Below this timeline is a section titled "Transaction" with a specific transaction ID: c490e2e0ac7ac9ca8c33d05637494345240f510d8fd138a91f69dbf8a5ea115b. This section includes a "1 confirmation" badge. It provides detailed information about the transaction, including:

Timestamp	2024-07-30 14:37:26 (1 minute ago)	Fee	1,926 sat \$1.27
Confirmed	After 1 minute	Fee rate	9.25 sat/vB
Features	SegWit Taproot RBF	Effective fee rate	9.22 sat/vB Overpaid 3x
Audit	Expected in Block	Miner	AntPool

Podemos verificar que o valor entrou na nova carteira. Hooray!



## Transactions

 3 minutes ago  
Conf: 1 Scalar School Tutorial  35,000

 Receive

 Send

## 4. Rede P2P

### 4.1 Nós de Bitcoin

O Bitcoin opera em uma rede ponto a ponto (P2P) de computadores. Qualquer computador conectado à rede é chamado de nó. Qualquer pessoa pode baixar e instalar o software Bitcoin de código aberto para se tornar um nó. Todos os nós são tratados igualmente, e nenhum nó é confiável por si só.

O sistema assume que a maioria dos nós (se forem nós de mineração, então o poder de hash) será honesta, ou seja, não retransmitirá transações e blocos falsos ou malformados. No entanto, em resposta a tal comportamento, um nó pode optar por desencorajar (marcar seu comportamento inadequado e talvez se desconectar em favor de novos pares), desconectar ou banir o par.

**Devido à arquitetura criptográfica da blockchain, o software Bitcoin consegue verificar se uma informação recebida sobre a rede é íntegra.** Cada bloco na blockchain contém um hash criptográfico do bloco anterior, criando uma cadeia de blocos interligados. Isso garante que qualquer alteração em um bloco anterior invalidaria todos os blocos subsequentes, tornando a falsificação impraticável.

Nós completos são responsáveis por verificar e manter todos os registros de propriedade de acordo com as regras de consenso. Nós de mineração também processam transações e adicionam novos blocos ao blockchain, em troca de uma recompensa. Nós podados verificam transações e blocos, mas não armazenam uma cópia completa da blockchain. Os nós SPV (Simple Verification Nodes) confiam em nós completos de terceiros para obter informações sobre endereços e transações específicas na rede. Softwares de carteira geralmente são nós SPV.

Os nós (nodes) são computadores que participam da rede Bitcoin, executando o software do Bitcoin. Eles desempenham várias funções essenciais para manter a rede segura, descentralizada e operando corretamente. Os principais papéis dos nós incluem:

**Verificação de Transações:** Nós verificam se as transações seguem todas as regras do protocolo Bitcoin, como a verificação de assinaturas criptográficas e a garantia de que os bitcoins não são gastos duas vezes.

**Propagação de Transações e Blocos:** Nós transmitem (ou retransmitem) transações e blocos para outros nós na rede, ajudando a disseminar informações de forma eficiente.

**Armazenamento da Blockchain:** Nós armazenam uma cópia completa ou parcial da blockchain, garantindo que os dados históricos sejam mantidos e acessíveis.

**Participação no Consenso:** Nós participam do processo de consenso, ajudando a validar novos blocos e manter a integridade do sistema.

Existem diferentes tipos de nós na rede Bitcoin, cada um com suas próprias funções e características:

**Nós Completos:** Um nó completo mantém uma cópia completa da blockchain e verifica todas as transações e blocos de acordo com as regras do Bitcoin. Eles são a espinha dorsal da rede, garantindo que todas as regras sejam seguidas e que a blockchain seja consistente em toda a rede.

Eles oferecem o mais alto nível de segurança e privacidade, pois não dependem de terceiros para verificar transações. Necessitam de mais recursos (espaço de armazenamento, largura de banda e poder de processamento) para operar eficientemente. Os nós completos garantem que

a rede Bitcoin permaneça segura e descentralizada. Quanto mais nós completos existirem, mais difícil se torna para qualquer entidade maliciosa comprometer a rede.

**Nós de Mineração:** Além de verificar transações e blocos, eles também participam do processo de mineração, adicionando novos blocos à blockchain e recebendo recompensas por isso.

**Nós Podados:** Verificam todo o histórico de transações e blocos, mas vão deletando os blocos verificados, e deste modo não armazenam uma cópia completa da blockchain, mantendo apenas os blocos mais recentes para economizar espaço em disco. No arquivo `bitcoin.conf` do Bitcoin Core você pode determinar quantos blocos deseja que o sistema mantenha em disco. O nó prunado (podado) limita um pouco as operações de RPC, pois você não tem a cópia indexada de todas as transações, mas, dependendo das suas necessidades, pode ser uma ótima opção.

**Nós SPV (Simplified Payment Verification):** Também conhecidos como "nós leves", eles não armazenam uma cópia completa da blockchain. Em vez disso, baixam apenas os cabeçalhos dos blocos e verificam as transações com base em provas de inclusão fornecidas por nós completos. Esses nós são ideais para dispositivos com recursos limitados, como smartphones, pois consomem menos recursos e largura de banda. A maioria das carteiras de Bitcoin possuem nós leves em sua composição. Eles dependem de nós completos para obter essas provas de inclusão e, portanto, precisam confiar nesses nós completos para a verificação correta das transações.

Você pode rodar um nó de Bitcoin usando o Bitcoin Core, que é a implementação de referência. No arquivo `bitcoin.conf`, você pode escolher as características deste nó, se vai ser completo, prunado, etc.

### Mapa da Rede Bitcoin

<https://medium.com/@gloriazhao/map-of-the-bitcoin-network-c6f2619a76f3>

Este site mostra algumas opções de projetos de full-nodes:

<https://bitcoiner.guide/node/diy/>

Há também formas de criar esses nós na nuvem, montados do zero ou por meio de sistemas que facilitam esse processo, como:

<https://voltage.cloud/>

<https://clovyr.app/>

## 4.2 Mempool

O Bitcoin opera usando dois conceitos principais de rede para a transmissão de dados. Uma rede para a transmissão (relay) de transações pendentes, chamada mempool, e outra para a transmissão (relay) de blocos minerados com transações confirmadas, que é a própria blockchain.

A mempool é um espaço onde as transações pendentes (não confirmadas) são armazenadas por cada nó da rede Bitcoin. Quando uma transação é transmitida para a rede, ela primeiro entra na mempool dos nós até ser incluída em um bloco minerado.

A mempool, abreviação de "memory pool" (pool de memória), é um componente crucial do sistema de Bitcoin. Ela funciona como uma área de espera para transações não confirmadas antes de serem incluídas em um bloco e adicionadas à blockchain. Quando um usuário realiza uma transação de Bitcoin, essa transação é inicialmente verificada por nós (computadores que participam da rede Bitcoin) e, em seguida, enviada para a mempool.

Aqui estão alguns pontos-chave sobre a mempool:

**Recepção de Transações:** Todas as transações que ainda não foram confirmadas por mineradores são armazenadas na mempool. Cada nó na rede Bitcoin possui sua própria versão da mempool, que pode variar ligeiramente entre os nós.

**Verificação Inicial:** Antes de uma transação ser adicionada à mempool, ela passa por uma verificação inicial para garantir que segue as regras do protocolo Bitcoin (por exemplo, se os inputs da transação são válidos e se a transação não tenta gastar Bitcoins inexistentes).

**Prioridade de Transação:** As transações na mempool são priorizadas com base nas taxas de transação. Transações com taxas mais altas são geralmente selecionadas primeiro pelos mineradores, pois os mineradores são incentivados a maximizar seus lucros incluindo transações com taxas mais elevadas nos blocos que mineram.

**Limitação de Espaço:** Cada nó pode configurar um limite de tamanho para sua mempool. Quando a mempool atinge esse limite, transações com taxas mais baixas podem ser descartadas para dar lugar a transações mais recentes com taxas mais altas.

**Confirmação:** Uma vez que um minerador inclui uma transação em um bloco e o bloco é adicionado à blockchain, a transação é removida da mempool. Esse processo confirma a transação, garantindo que ela não pode ser revertida ou duplicada.

A mempool é essencial para o funcionamento eficiente da rede Bitcoin, garantindo que as transações sejam verificadas e priorizadas antes de serem registradas permanentemente na blockchain.

## 4.3 Mainnet

A mainnet é a rede principal do Bitcoin, onde transações reais ocorrem e os bitcoin têm valor monetário. Desenvolvedores e empresas precisam usar a mainnet para operações de produção e lançamentos finais de seus produtos.

As transações são confirmadas por mineradores e registradas permanentemente na blockchain, garantindo alta segurança e imutabilidade. Desenvolvedores e usuários interagem através de nós completos, carteiras e APIs de terceiros para realizar e monitorar transações reais.

Veja alguns casos de uso para desenvolvedores.

### **Cenário 1: Lançamento de uma Nova Carteira Bitcoin**

Uma empresa de fintech desenvolveu uma nova carteira Bitcoin com recursos avançados de segurança e privacidade. Após extensivos testes na Testnet e Signet, eles estão prontos para lançar a carteira ao público.

A empresa lança a nova carteira na Mainnet, permitindo que os usuários começem a realizar transações reais com bitcoins reais. A equipe de marketing promove a carteira, e os desenvolvedores monitoram o feedback dos usuários para adaptar e melhorar a experiência do usuário com base em interações reais. A empresa fornece suporte ao cliente para resolver quaisquer problemas que possam surgir durante o uso da carteira na Mainnet.

### **Cenário 2: Implementação de um Serviço de Pagamento Bitcoin**

Uma plataforma de e-commerce decide aceitar Bitcoin como método de pagamento e precisa integrar um serviço de pagamento Bitcoin seguro e eficiente. A equipe técnica integra um serviço de pagamento Bitcoin que permite aos clientes pagar por bens e serviços usando bitcoins reais.

A plataforma começa a processar transações reais na Mainnet, recebendo pagamentos de clientes e verificando a confirmação das transações na blockchain. A empresa implementa sistemas de contabilidade e relatórios para rastrear os pagamentos em Bitcoin, garantindo conformidade com as regulamentações financeiras.

### **Cenário 3: Implementação de um Sistema de Remessas Internacionais**

Uma empresa de serviços financeiros lança um sistema de remessas internacionais que utiliza Bitcoin para transferir dinheiro entre países de forma rápida e com baixas taxas. A empresa processa remessas de clientes, utilizando Bitcoin para transferir fundos de um país para outro. Os bitcoins reais são usados para realizar as transações na Mainnet.

A plataforma converte automaticamente as moedas fiat dos clientes em Bitcoin para transferência e, em seguida, converte de volta para a moeda fiat do destinatário após a

transação. A empresa mantém registros detalhados de todas as transações de remessa, garantindo conformidade com as regulamentações internacionais de transferência de dinheiro.

## 4.4 Regtest

Regtest (Regression Test) é uma rede de teste local que permite aos desenvolvedores criar um ambiente de teste totalmente controlado. Não é uma rede pública e é controlada pelo usuário. Totalmente configurável pelo usuário, permitindo ajustes na dificuldade de mineração e no tempo entre blocos.

Ideal para desenvolvimento inicial, testes de regressão e ajustes finos de funcionalidades sem esperar por confirmações de rede. As moedas na Regtest não têm valor monetário, facilitando testes seguros e rápidos. Desenvolvedores configuram um nó Bitcoin em modo Regtest e utilizam comandos RPC para criar e manipular blocos e transações de forma manual.

### **Cenário 1: Desenvolvimento Inicial de um Novo Protocolo ou Funcionalidade**

Uma equipe de desenvolvedores está trabalhando na implementação de um novo protocolo para o Bitcoin, como uma nova forma de assinatura digital ou uma sugestão de atualização no sistema de consenso. A equipe pode criar blocos instantaneamente na Regtest, permitindo testes rápidos sem a necessidade de esperar pela confirmação dos blocos, como aconteceria na Testnet ou Mainnet.

A Regtest permite que os desenvolvedores ajustem a dificuldade de mineração e o tempo entre os blocos, criando condições específicas para testar a nova funcionalidade em diferentes cenários. Como a Regtest é uma rede local, não há interferência de transações ou blocos de outros desenvolvedores. Isso permite testes mais focados e controlados.

Permite um ciclo de desenvolvimento rápido com feedback imediato. Possibilita a simulação de diferentes condições de rede de forma controlada. Ideal para testes iniciais e ajustes finos de novas funcionalidades.

### **Cenário 2: Teste de Integração e Automatização**

Uma empresa de software está desenvolvendo um conjunto de ferramentas automatizadas para monitorar e gerenciar transações Bitcoin, incluindo detecção de fraudes e auditorias de conformidade.

A empresa pode automatizar a criação e verificação de transações na Regtest, garantindo que seus scripts de monitoramento funcionem corretamente em diversas situações. É possível criar transações específicas e blocos para testar as respostas do sistema de monitoramento, verificando se ele detecta corretamente comportamentos anômalos ou suspeitos.

Desenvolvedores podem simular ataques ou tentativas de fraude na Regtest sem qualquer risco, testando a eficácia de seus sistemas de detecção. A rede facilita a criação de um ambiente de teste automatizado para integração contínua, permite testes detalhados de

sistemas de monitoramento e segurança, e proporciona um ambiente seguro para simulação de ataques e respostas.

### **Cenário 3: Desenvolvimento de Aplicações Personalizadas**

Uma startup está desenvolvendo uma aplicação personalizada de micropagamentos que utiliza transações Bitcoin para facilitar pagamentos entre usuários. A startup pode simular milhares de transações em um curto período de tempo, testando a capacidade de sua aplicação de lidar com um grande volume de micropagamentos.

Permite testar a experiência do usuário (UX) ao realizar transações, ajustando o tempo de confirmação e a dificuldade de mineração para avaliar diferentes cenários de uso. A Regtest facilita um ciclo de desenvolvimento iterativo, permitindo que a startup faça mudanças rápidas e veja imediatamente os efeitos dessas mudanças.

### **Cenário 4: Testes de Regressão**

Uma equipe de desenvolvimento está implementando atualizações em um software existente de carteira Bitcoin e precisa garantir que as novas mudanças não introduzam bugs ou falhas. A equipe pode criar um conjunto de testes automatizados que executam transações, criam blocos e verificam o estado da blockchain para garantir que tudo funcione como esperado após as atualizações.

A Regtest proporciona um ambiente de teste consistente onde os mesmos testes podem ser repetidos várias vezes, garantindo que as novas mudanças não afetem negativamente as funcionalidades existentes. Permite a criação de condições específicas que podem ser difíceis de reproduzir na Testnet ou Mainnet, como falhas de rede ou ataques específicos.

## **4.5 Testnet**

Testnet (Test Network) é uma rede pública de teste que imita o comportamento da Mainnet. Bitcoins na Testnet não têm valor monetário, permitindo testes sem risco financeiro. Qualquer pessoa pode minerar blocos e realizar transações na Testnet. A Testnet simula as condições da Mainnet, oferecendo um ambiente realista para desenvolvimento e testes. Moedas da Testnet não têm valor financeiro, permitindo testes seguros. Desenvolvedores utilizam nós completos, carteiras e APIs especificando a Testnet para simular operações reais sem risco financeiro.

### **Cenário 1: Desenvolvimento de Carteira Bitcoin com Suporte para Transações Multisig**

Uma startup de fintech está desenvolvendo uma nova carteira Bitcoin com suporte para transações multisig. Eles querem testar a funcionalidade de criar e gastar uma transação multisig para garantir que tudo funcione conforme o esperado antes de lançar o produto ao público.

Desenvolvedores podem criar endereços multisig na Testnet sem o risco de perder fundos reais. Eles podem experimentar diferentes configurações de M-de-N (por exemplo, 2-de-3 ou 3-de-5). Usando a Testnet, a equipe pode enviar e receber transações de teste para e dos

endereços multisig. Como os bitcoins da Testnet não têm valor real, não há risco financeiro envolvido.

A Testnet permite que a equipe simule condições reais da rede, como a propagação de transações, taxas de transação variáveis e tempos de confirmação. Eles podem ajustar as taxas de transação para ver como isso afeta a velocidade de confirmação.

A equipe pode facilmente obter bitcoins de Testnet de faucets para financiar suas transações de teste, o que permite testes extensivos sem custos financeiros reais.

### **Cenário 2: Desenvolvimento de uma Nova Função de Carteira**

Uma empresa de software está desenvolvendo uma nova função para sua carteira Bitcoin que permite a conversão automática de transações de uma moeda fiat para Bitcoin.

Desenvolvedores podem testar a funcionalidade de conversão automática, verificando se as taxas de câmbio são aplicadas corretamente e se as transações em Bitcoin são enviadas e recebidas sem problemas.

Utilizando a Testnet, a equipe pode ajustar e testar diferentes níveis de taxas de transação para garantir que a carteira selecione automaticamente a taxa mais apropriada em diferentes condições de rede. A empresa pode simular vários cenários de uso real, como altas e baixas frequências de transações, para garantir que a nova função funcione de forma eficiente e estável.

### **Cenário 3: Implementação de Suporte para Transações SegWit**

Uma equipe de desenvolvimento está implementando suporte para transações Segregated Witness (SegWit) em sua aplicação de pagamento Bitcoin. Desenvolvedores podem criar e enviar transações SegWit na Testnet para garantir que a implementação esteja correta e que as transações sejam válidas. A equipe pode verificar se sua aplicação é compatível com outras carteiras e serviços que suportam SegWit, garantindo a interoperabilidade.

Utilizando a Testnet, a equipe pode medir o desempenho das transações SegWit em comparação com as transações não SegWit, analisando aspectos como velocidade de confirmação e uso de espaço no bloco.

## **4.6 Signet**

Signet é uma rede de teste proposta para Bitcoin que utiliza assinaturas digitais em vez de Proof-of-Work (PoW) para validação de blocos. Essa abordagem melhora a previsibilidade e a estabilidade, proporcionando um ambiente ideal para os desenvolvedores testarem recursos e protocolos.

As redes de teste existentes, como Testnet e Regtest, têm limitações. A Testnet é notoriamente pouco confiável devido a frequentes grandes reorganizações e geração irregular de blocos. Regtest permite que qualquer participante crie blocos livremente, o que prejudica sua

adequação para testes de longo prazo com múltiplas partes. A Signet visa fornecer um ambiente mais previsível e controlado, abordando essas questões.

**Validação de Blocos:** A Signet exige que os blocos incluam uma assinatura digital baseada em um desafio específico (scriptPubKey). Essa assinatura garante que apenas entidades autorizadas possam criar blocos válidos.

**Compatibilidade com Proof-of-Work:** Embora a Signet use assinaturas para validação de blocos, ela mantém os cabeçalhos de blocos PoW, permitindo compatibilidade com softwares existentes que suportam PoW.

**Redes Personalizadas:** Os usuários podem criar suas próprias redes Signet gerando um par de chaves e um scriptPubKey de desafio. Essa flexibilidade permite ambientes de teste personalizados para diversos protocolos e recursos.

**Validação Baseada em Assinatura:** Cada bloco inclui uma assinatura que deve ser verificada para validar o bloco. Esse processo envolve a criação de transações virtuais que garantem que o bloco atenda aos requisitos do desafio.

**Mineração Simplificada:** O processo de assinatura não se compromete com o valor do nonce, permitindo que os mineradores gerem PoW sem assinar repetidamente o bloco.

**Bloco Gênesis e Início da Mensagem:** Um bloco gênesis e um início de mensagem padronizados garantem consistência entre diferentes redes Signet.

**Compatibilidade:** A Signet foi projetada para funcionar com o software Bitcoin existente com modificações mínimas. Pode ser integrada aos sistemas atuais adicionando parâmetros de rede sem alterar a lógica fundamental de validação de blocos.

**Teste de Protocolos:** A Signet é ideal para testar novos protocolos como Eltoo ou Taproot, fornecendo um ambiente estável para testes de integração ao longo de períodos prolongados.

**Teste de Exchanges:** Exchanges podem usar a Signet para testar seus sistemas contra cenários realistas de reorganização, garantindo que seu software lide corretamente com esses eventos.

**Teste de Carteiras:** A Signet permite que os desenvolvedores de carteiras testem seu software em um ambiente controlado, verificando a manipulação de reorganizações e outras funcionalidades críticas.

**Controle Centralizado:** A natureza centralizada da Signet permite a execução fácil de testes globais, como reorganizações programadas, tornando-a mais previsível do que a Testnet.

**Uso pela Comunidade:** Embora qualquer pessoa possa criar uma Signet personalizada, ter uma rede Signet padrão e confiável pode fomentar um terreno comum para testes, reduzindo a fragmentação e aumentando a eficácia dos esforços de teste da comunidade.

A Signet oferece uma alternativa robusta e previsível às redes de teste existentes, abordando suas limitações e fornecendo um ambiente flexível e controlado para testes extensivos de recursos e protocolos do Bitcoin.

### **Cenário 1: Implementação de Sistema de Gerenciamento de Risco para uma Grande Exchange**

Uma grande exchange está implementando um novo sistema de gerenciamento de risco que envolve transações complexas e contratos inteligentes. A confiabilidade e a previsibilidade do ambiente de teste são cruciais para garantir que o sistema funcione sem falhas. A Signet permite que a exchange realize testes com transações complexas e contratos inteligentes em um ambiente controlado.

As transações podem incluir scripts personalizados ou funcionalidades avançadas que precisam ser validadas rigorosamente. Como os blocos na Signet são assinados por entidades confiáveis, a exchange pode ter certeza de que o ambiente de teste será estável e livre de comportamentos inesperados, como ataques de spam ou mudanças bruscas na dificuldade de mineração.

A Signet garante que as transações de teste sejam confirmadas de maneira previsível, permitindo à equipe de desenvolvimento focar na validação das funcionalidades sem se preocupar com falhas na rede de teste. Ela oferece um ambiente onde auditorias de segurança e verificações de conformidade podem ser realizadas de forma confiável, garantindo que o sistema de gerenciamento de risco atenda aos padrões necessários antes do lançamento.

### **Cenário 2: Testes de Segurança e Resiliência**

Uma empresa de segurança cibernética está desenvolvendo uma nova solução de segurança para transações Bitcoin e precisa realizar testes extensivos para garantir que sua solução resista a diversos tipos de ataques. Na Signet, a empresa pode simular ataques como double spending, replay attacks e outros, sabendo que o ambiente é controlado e previsível.

A solução de segurança pode ser testada contra os ataques simulados para garantir que todas as defesas funcionem corretamente. A Signet permite um monitoramento detalhado e logging de todas as atividades, facilitando a análise de como a solução de segurança responde a diferentes ameaças.

### **Cenário 3: Desenvolvimento de Smart Contracts Avançados**

Uma empresa de blockchain está desenvolvendo contratos inteligentes (smart contracts) avançados para aplicações financeiras complexas, como empréstimos descentralizados e derivativos. A empresa pode desenvolver e testar smart contracts complexos na Signet, garantindo que todas as funções e condições sejam executadas corretamente.

A Signet proporciona um ambiente onde as condições de teste são estáveis e previsíveis, permitindo testes rigorosos de lógica de contrato e segurança. Desenvolvedores podem validar que os contratos inteligentes interagem corretamente com outras partes do sistema e que todas as transações são registradas conforme esperado.

## 4.7 Forks

Um fork é uma mudança ou divergência no software, na blockchain ou no consenso de rede. Forks podem ser categorizados em dois tipos principais: hard forks e soft forks.

Forks referem-se a mudanças no protocolo Bitcoin que resultam em uma divisão na blockchain, levando à criação de um novo caminho ou nova blockchain. Essas alterações podem ser classificadas como hard forks ou soft forks, dependendo da compatibilidade com versões anteriores. Soft forks são compatíveis com versões anteriores (backwards compatible). Hard forks geram outro tipo de criptomoeda incompatível com o Bitcoin original.

### Hard Forks

Hard Forks são divergências não compatíveis com versões anteriores no protocolo Bitcoin ou na história dos blocos. Em um hard fork, os nós devem adotar novas regras de consenso, que podem ser mais frouxas ou diferentes das regras anteriores. Nós que não atualizarem seu software verão os blocos produzidos sob as novas regras como inválidos. Um hard fork é uma mudança permanente nas regras de consenso que os nós antigos não podem seguir.

Em 1 de agosto de 2017, enquanto a rede Bitcoin estava prestes a ativar o Segregated Witness (SegWit), uma parte da rede seguiu um caminho alternativo de escalonamento não compatível com versões anteriores, aumentando o tamanho base do bloco sem SegWit. Isso resultou na criação da criptomoeda de fork conhecida como Bitcoin Cash (BCH).

### Soft Forks

Soft Forks são mudanças compatíveis com versões anteriores no protocolo Bitcoin. Em um soft fork, os nós optam por um aperto ou restrição das regras de consenso. Os nós que não atualizarem continuarão recebendo novos blocos e os reconhecendo como válidos, desde que esses blocos sigam as regras antigas.

### Exemplos de Soft Forks

**Segregated Witness (SegWit):** Introduzido como um soft fork, SegWit altera a forma como os dados de transação são armazenados, aumentando a capacidade de transação sem aumentar o tamanho do bloco.

**Pay to Script Hash (P2SH):** Um soft fork que resultou na implementação de carteiras multi-assinatura na rede Bitcoin.

Atualizações de soft fork podem causar divisões temporárias na blockchain, mas a aplicação por uma maioria de poder de hash garante a eventual convergência na mesma história de transações.

### **Tipos de Soft Forks**

**Miner Activated Soft Fork (MASF):** Um soft fork ativado pelo poder de hash dos mineradores. Os mineradores sinalizam seu apoio à mudança e, quando um determinado limiar de suporte é alcançado, a mudança é ativada.

**User Activated Soft Fork (UASF):** Um soft fork ativado por usuários. Os nós que desejam impor as novas regras de consenso optam por implementar a atualização, independentemente do suporte dos mineradores. Um exemplo notável é a ativação do SegWit através de um UASF.

### **Importância do UASF**

O User Activated Soft Fork (UASF), ou Soft Fork Ativado Por Usuários, é significativo porque demonstra o poder dos usuários de Bitcoin em influenciar mudanças no protocolo, independentemente do apoio dos mineradores.

Em 1º de agosto de 2017, o UASF foi utilizado para ativar o SegWit na rede Bitcoin. Apesar da resistência inicial de alguns mineradores, a pressão dos usuários levou à implementação bem-sucedida do SegWit, mostrando que os usuários entrando em consenso podem desencadear mudanças importantes no protocolo.

### **Detectção de Hard Forks ou Redes Erradas**

Para garantir que você está na rede correta e não em um hard fork ou rede errada, existem algumas práticas e verificações que os nós executam:

**Cabeçalhos de Bloco:** Nós verificam a cadeia de cabeçalhos de bloco para garantir que estão na cadeia mais longa e válida. A cadeia mais longa é aquela com o maior trabalho acumulado (proof-of-work).

**Pontos de Verificação (Checkpoints):** Certos nós utilizam pontos de verificação, que são blocos de altura específica que são bem conhecidos e aceitos pela comunidade Bitcoin. Isso ajuda a garantir que o nó esteja na cadeia correta.

**Versão do Software:** Utilizar a versão mais recente do software Bitcoin Core (ou outra implementação confiável) garante que o nó esteja seguindo as regras de consenso mais atualizadas.

**Conexões de Rede:** Conectar-se a nós conhecidos e confiáveis na rede Bitcoin ajuda a garantir que você esteja na rede correta. Muitos clientes Bitcoin vêm com uma lista de nós confiáveis pré-configurados.

Suponha que você configure um nó Bitcoin usando o software Bitcoin Core. Quando o nó se conecta à rede, ele:

Começa a baixar e verificar a cadeia de blocos desde o bloco gênesis. Valida cada bloco e transação de acordo com as regras de consenso. Se conecta a outros nós e recebe cabeçalhos de blocos para garantir que está na cadeia mais longa. Usa pontos de verificação para garantir que não está seguindo um fork incorreto.

O sistema Bitcoin é projetado para operar de maneira descentralizada e segura, assumindo que a maioria dos nós será honesta devido aos incentivos econômicos e à verificação mútua das regras de consenso. Embora nenhum nó individual seja confiável por si só, a rede como um todo mantém sua integridade através da verificação contínua e da descentralização.

Para garantir que você está usando uma versão legítima e segura do software Bitcoin Core, baixe-o apenas do repositório oficial no [GitHub](#).

## 5. Mineração

### 5.1 Energia: Aproveitamento e Desenvolvimento de Infraestrutura

A mineração de Bitcoin pode aproveitar energia excedente que, de outra forma, seria desperdiçada, como a energia gerada por fontes renováveis em momentos de baixa demanda.

Isso cria incentivos para o desenvolvimento de infraestrutura de eletricidade em áreas pouco desenvolvidas, pois a presença de operações de mineração pode tornar projetos de geração de energia economicamente viáveis.

Além disso, a demanda constante por eletricidade estável e barata para a mineração pode estimular investimentos em tecnologias de energia renovável e eficiência energética, beneficiando comunidades locais e promovendo um uso mais sustentável dos recursos energéticos.

Existem alguns projetos notáveis de infraestrutura elétrica em países africanos que envolvem a mineração de Bitcoin. Aqui estão alguns exemplos:

#### **Gridless Compute**

Localizado no Quênia e outras regiões da África Oriental, a Gridless Compute utiliza microgrids hidroelétricos para alimentar operações de mineração de Bitcoin em comunidades rurais. Esse modelo aproveita a energia excedente que seria desperdiçada, garantindo uma demanda constante e confiável por eletricidade, o que, por sua vez, ajuda a financiar a expansão da infraestrutura elétrica nessas áreas. Esse projeto recebeu financiamento de Jack Dorsey's Block e da empresa de capital de risco Stillmark ([CoinDesk](#)) ([Finbold](#)).

#### **Virunga National Park**

Localizado na República Democrática do Congo, no Parque Nacional de Virunga, a mineração de Bitcoin é alimentada por hidrelétricas, gerando renda crucial para a reserva biológica e para as comunidades locais. O calor gerado pelos equipamentos de mineração também está sendo utilizado para secar grãos de cacau, proporcionando uma solução econômica e sustentável para processos industriais locais ([Bitcoin Magazine](#)).

Esses projetos demonstram como a mineração de Bitcoin pode ser integrada com iniciativas de infraestrutura de energia renovável para promover o desenvolvimento econômico e a sustentabilidade em regiões subdesenvolvidas.

## 5.2 Prova-de-trabalho

A mineração é o processo de adição de novos blocos à blockchain e a emissão de novas unidades de bitcoin.

A integridade das transações e blocos é garantida pela contribuição de poder computacional, um processo chamado prova-de-trabalho. Os dados do bloco candidato são hashados repetidamente até que o valor do hash seja menor que um valor padrão determinado pela dificuldade atual. O valor de um hash é considerado 'menor' se tiver mais zeros à esquerda que o número que determina a dificuldade da rodada.

Embora possa parecer complicado, não se preocupe, pois o processo é automatizado. A configuração e manutenção das máquinas de mineração são frequentemente o único trabalho manual necessário. As máquinas de mineração são especialmente projetadas para realizar cálculos de hash de maneira eficiente, utilizando hardware especializado como ASICs (Application-Specific Integrated Circuits).

A prova de trabalho—PoW—é um protocolo que requer um esforço computacional significativo para ser realizado, mas é fácil de verificar. No contexto do Bitcoin, o PoW é utilizado para assegurar que todos os participantes concordem com o estado atual da blockchain.

Neste processo, os mineradores competem para encontrar um hash válido que atenda ao critério de dificuldade.

A mineração de Bitcoin envolve vários passos contínuos e cíclicos, realizados pelos mineradores para adicionar novos blocos à blockchain.

Abaixo, o processo é detalhado de forma lógica:

### **Coleta e agrupamento de transações da mempool**

Os mineradores coletam transações não confirmadas da mempool, que é uma espécie de 'sala de espera' para transações que ainda não foram incluídas em um bloco.

### **Organização em um bloco candidato**

Essas transações transmitidas na rede peer-to-peer são organizadas em um bloco candidato. Os mineradores podem escolher arbitrariamente quais transações incluir, geralmente optando por aquelas com a maior taxa por byte, gerando maior lucratividade por bloco minerado. Eles também verificam se todas as transações no bloco são válidas, garantindo que não haja duplicações ou transações inválidas.

### **Seleção do bloco anterior**

Seleciona-se o bloco mais recente no caminho mais longo da blockchain e insere-se um hash de seu cabeçalho no novo bloco.

Esse bloco candidato inclui:

**Hash do bloco anterior:** Este hash aponta para o bloco anterior na blockchain, garantindo que os blocos estejam encadeados em uma sequência imutável, mantendo a estrutura de dados da timechain (o nome original da blockchain).

**Merkle root:** Uma estrutura de árvore de hashes que representa todas as transações do bloco. O Merkle root é colocado no header do bloco.

**Timestamp:** Um carimbo de data/hora que registra o momento em que o bloco foi minerado.

**Nonce:** Um número que os mineradores alteram para encontrar um hash válido que satisfaça as condições da rede (isto é, começa com um certo número de zeros). Cada nonce diferente gera um hash diferente que é comparado ao nível de dificuldade até que o hash resultante esteja abaixo do mesmo—representando que o bloco tem os atributos necessários para fazer parte da blockchain.

### **O header do bloco contém:**

Hash do bloco anterior.

Merkle root das transações.

Timestamp.

Nonce.

A versão do software do Bitcoin.

O alvo de dificuldade, que determina a dificuldade do problema de hashing.

### **Prova de Trabalho**

Os mineradores ajustam o nonce repetidamente e re-hash o header do bloco até encontrar um hash que esteja abaixo do alvo de dificuldade estabelecido pela rede. Esse processo envolve:

#### a. Incrementação do Nonce

Incrementar (adicionar 1 a) um número arbitrário no cabeçalho do bloco chamado nonce.

#### b. Cálculo do Hash

Calcular o hash do cabeçalho do bloco resultante.

### c. Verificação do Hash

Verificar se o hash do cabeçalho do bloco, quando expresso como um número, é menor que um valor-alvo predeterminado.

Os mineradores repetem os passos de incrementação do nonce, cálculo do hash e verificação do hash milhões de vezes por segundo até encontrar um hash válido. Esse ciclo rápido e contínuo é essencial para a segurança e a integridade da rede Bitcoin.

### **Validação e inclusão na blockchain**

Uma vez encontrado um hash válido, o bloco é transmitido para a rede, onde outros nós verificam a validade das transações e a solução do PoW (Proof-of-Work). Se o bloco for aceito, ele é adicionado à blockchain.

O minerador vencedor é recompensado com uma quantidade predefinida de bitcoins (subsídio de bloco da época) e as taxas de transação incluídas no bloco. Lembrando que a mineração é uma corrida, então a velocidade de propagação de um bloco válido também é importante para garantir que ela seja efetivada.

### **Rejeição de blocos inválidos**

Se o hash do cabeçalho do bloco não for menor que o valor-alvo, o bloco é rejeitado pela rede.

O desempenho da mineração é medido em hashes por segundo, atualmente calculado em gigahashes (GH/s) ou terahashes (TH/s).

### **Nova rodada**

Depois disso, todos os mineradores começam a trabalhar na busca pelo próximo bloco, incorporando o novo hash do bloco anterior como seu ponto de partida.

## 5.3 Timechain

Embora o termo *timechain* não tenha se popularizado, ele destaca a visão de Satoshi sobre a importância do tempo na estrutura de uma blockchain. O termo timechain aparece nos primeiros comentários no código-fonte do Bitcoin e em algumas das comunicações de Satoshi, embora blockchain tenha se tornado o termo mais amplamente adotado.

### **Ajuste de dificuldade**

Como a mineração é um processo de tentativa e erro realizado por computadores, quanto maior o poder computacional, mais rápido se encontra um hash válido, e vice-versa. A dificuldade é ajustada regularmente para garantir que novos blocos sejam minerados aproximadamente a cada [10 minutos](#), mantendo assim a estabilidade e a segurança da rede.

Para garantir que novos blocos sejam minerados aproximadamente a cada 10 minutos, a rede Bitcoin ajusta automaticamente a dificuldade de mineração a cada 2016 blocos (aproximadamente a cada duas semanas).

Se o tempo médio de bloco for maior que 10 minutos, a dificuldade é diminuída; se for menor, a dificuldade é aumentada.

Esse ajuste considera a quantidade de poder computacional contribuído, garantindo que a mineração continue eficiente e equilibrada, independentemente do número de mineradores e do poder de seus equipamentos.

Em junho de 2021, o governo chinês impôs restrições severas às operações de mineração, forçando muitos mineradores a desligarem suas máquinas ou relocarem suas operações. Como resultado, a taxa de hash global caiu drasticamente, levando a um ajuste de dificuldade de cerca de -28% no início de julho de 2021, o maior ajuste para baixo registrado até então.

## 5.4 Oferta Inelástica

A geração de novas unidades de bitcoin segue um cronograma de emissão determinístico, com um suprimento total finito de aproximadamente 21 milhões de bitcoins. Essa é uma das principais regras de consenso do sistema, o que garante que ele seja uma alternativa aos sistemas financeiros atuais, que são obscuros, inflacionários, e com impressão arbitrária de moeda.

Você pode encontrar o trecho do código com a função GetBlockSubsidy direto no [GitHub repository do Bitcoin Core](#).

```
1918
1919    CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
1920    {
1921        int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
1922        // Force block reward to zero when right shift is undefined.
1923        if (halvings >= 64)
1924            return 0;
1925
1926        CAmount nSubsidy = 50 * COIN;
1927        // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
1928        nSubsidy >>= halvings;
1929        return nSubsidy;
1930    }
1931
```

### Histórico dos [Halvings](#) do Bitcoin

**Recompensa Inicial, 2009:** Em 3 de janeiro de 2009, Satoshi Nakamoto minerou o bloco gênese, com uma recompensa de 50 bitcoins por bloco.

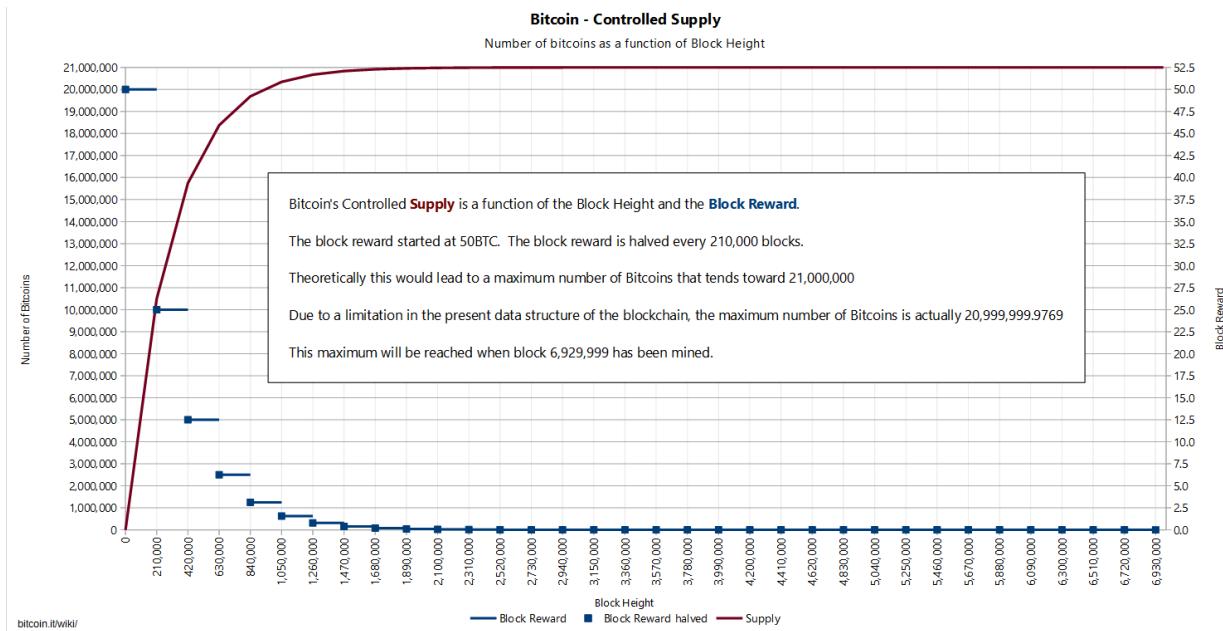
**Primeiro Halving, 2012:** Em 28 de novembro de 2012, ocorreu o primeiro halving, reduzindo a recompensa de bloco de 50 para 25 bitcoins.

**Segundo Halving, 2016:** Em 9 de julho de 2016, ocorreu o segundo halving, reduzindo a recompensa de bloco de 25 para 12,5 bitcoins.

**Terceiro Halving, 2020:** Em 11 de maio de 2020, ocorreu o terceiro halving, reduzindo a recompensa de bloco de 12,5 para 6,25 bitcoins.

**Quarto Halving, 2024:** Em 19 de abril de 2024 ocorreu o quarto halving, reduzindo a recompensa de bloco de 6,25 para 3,125 bitcoins.

Mais de 19 milhões de bitcoins (mais de 90% do total da oferta de bitcoins) já foram emitidos até agora através das recompensas de bloco. A taxa de emissão continuará diminuindo até que a emissão final ocorra em 2140.



## 5.5 Mineração Solo e a Resiliência do Bitcoin

A mineração solo envolve o uso de computadores próprios ou hardware especializado para procurar blocos. Os mineradores solo são pagos apenas se resolverem um bloco de forma independente, o que torna essa prática altamente competitiva nos tempos atuais, exigindo um investimento significativo.

No entanto, a capacidade de realizar mineração solo é uma decisão de design fundamental que contribui significativamente para a resiliência e indestrutibilidade do Bitcoin. Esta abordagem descentralizada permite que qualquer pessoa, em qualquer lugar do mundo, participe do processo de mineração usando seu próprio hardware. Isso traz várias vantagens:

**Descentralização:** A mineração solo ajuda a evitar a concentração de poder de mineração em mãos de poucos grandes players. Qualquer indivíduo pode potencialmente encontrar um bloco, o que distribui o poder de mineração globalmente.

**Segurança:** Com uma rede altamente distribuída de mineradores individuais, torna-se extremamente difícil para qualquer entidade controlar a maioria do poder de hash. Isso protege a rede contra ataques de 51%, onde um atacante tenta reverter transações ou impedir novas transações de serem confirmadas.

**Resiliência:** A natureza distribuída da mineração solo significa que a rede Bitcoin pode sobreviver a interrupções regionais. Mesmo que uma grande quantidade de poder de hash seja perdida devido a um problema geopolítico ou desastre natural, pequenos mineradores individuais ao redor do mundo podem continuar operando e garantindo a continuidade da rede.

**Inclusividade:** Permitir que qualquer pessoa participe da mineração promove um ecossistema mais inclusivo, onde novos mineradores podem contribuir para a segurança da rede, independentemente de sua localização ou acesso a recursos.

**Redução do Risco de Censura:** Uma rede de mineração descentralizada torna mais difícil para governos ou outras entidades censurar transações ou mineradores, já que não há um ponto único de falha ou controle.

#### **Taxa de Hash da rede Bitcoin ao Longo do Tempo:**

Setembro de 2019: 90.000.000 TH/s

Setembro de 2020: 140.000.000 TH/s

Fevereiro de 2021: 150.000.000 TH/s

Agosto de 2021: 129.000.000 TH/s ([queda após repressão à mineração na China](#))

Para uma pessoa comum, a mineração solo não é ideal devido à alta competitividade e ao investimento significativo necessário.

Porém, mesmo que a mineração solo possa não ser economicamente viável para a maioria dos indivíduos hoje, a possibilidade de realizá-la é crucial. Essa capacidade garante que a rede permaneça descentralizada e acessível, evitando a centralização excessiva e mantendo a robustez e a segurança do Bitcoin.

Ao permitir a mineração solo, o design do Bitcoin fortalece sua estrutura descentralizada, tornando a rede mais segura, resiliente e resistente a ataques e censura. Isso assegura que o

Bitcoin continua operando de forma robusta, mesmo em cenários adversos, contribuindo para sua indestrutibilidade.

## 5.6 Mineração em Pool

A mineração em pool é o método principal usado hoje, onde mineradores combinam seu poder de hash para resolver a prova de trabalho coletivamente.

### Funcionamento

O servidor do pool prepara um bloco com a transação coinbase para o endereço da pool.

Mineradores fazem uma solicitação `getwork/getblocktemplate` ao servidor da pool.

Cada minerador tenta resolver o problema de PoW, incrementando o nonce e calculando o hash do cabeçalho do bloco.

Quando um minerador encontra um hash abaixo do alvo de dificuldade, submete-o ao servidor.

O servidor verifica e acompanha as participações enviadas.

Ao encontrar uma solução, o servidor paga a recompensa proporcionalmente ao número de participações de cada minerador.

Mineradores periodicamente atualizam o servidor sobre novos blocos descobertos.

### Distribuição de recompensas

Na mineração em pool, os mineradores combinam seu poder de hash para resolver a prova de trabalho coletivamente. Cada minerador recebe uma parte proporcional da recompensa com base em sua contribuição de poder de hash. Se um minerador contribuiu com metade do poder de hash do pool, ele recebe metade da recompensa.

### Esquemas de Distribuição de Recompensas

**PPS (Pay Per Share):** Cada minerador é pago uma quantia garantida por cada participação submetida, com dificuldades personalizadas.

**PPLNS (Pay Per Last Number of Shares):** Os pagamentos são baseados no último número x de participações após um bloco ser encontrado.

**Proporcional:** Pagamentos baseados na proporção de participações desde o último bloco, contando todas as participações.

## 5.7 Hardware de Mineração

### Mineração com CPU

Inicialmente, a mineração de Bitcoin era feita usando CPUs, mas essas foram superadas por hardware mais eficiente.

### Mineração com GPU

As GPUs são projetadas para realizar muitos cálculos paralelos, sendo ordens de magnitude mais rápidas que as CPUs.

### FPGA (Field Programmable Gate Arrays)

FPGAs foram um passo intermediário entre CPUs e ASICs, usados até que os ASICs dominassem a mineração de Bitcoin.

### Mineração com ASIC

ASICs são construídos especificamente para uma aplicação e são muito mais rápidos que GPUs. Eles são personalizados para executar apenas o hashing SHA-256, tornando-se a única técnica de mineração economicamente eficiente atualmente. Veja como elas são:

<https://m.bitmain.com/>

## 5.8 Ataque de 51%

O poder de hashing está distribuído globalmente entre milhares de mineradores. Para controlar 51% da rede, um ator malicioso precisaria adquirir e operar uma quantidade de hardware maior do que a soma do que está atualmente distribuído entre todos esses mineradores. Essa operação não passaria despercebida pela comunidade, pois ela fere as regras de consenso.

### Ações Possíveis em um Ataque de 51%

**Reversão de Transações:** O atacante pode reverter transações recentemente confirmadas, permitindo o gasto duplo de moedas. Isso significa que o atacante pode gastar as mesmas moedas duas vezes, uma vez em uma transação legítima e novamente em uma transação fraudulenta.

**Impedir a Confirmação de Novas Transações:** O atacante pode impedir que novas transações sejam confirmadas, efetivamente congelando a atividade da rede. Eles podem excluir ou atrasar transações específicas ou todas as transações. Isso causa uma negação de serviço (DoS) na rede, interrompendo a operação normal da blockchain.

**Monopolização da Mineração:** O atacante pode controlar a mineração de novos blocos, recusando-se a incluir transações de outros mineradores e coletando todas as recompensas de

bloco. Isso centraliza a mineração, reduz a descentralização da rede e pode levar à manipulação de transações.

**Manipulação da Ordem das Transações:** O atacante pode reorganizar a ordem das transações nos blocos, alterando a sequência de transações. Isso pode ser usado para beneficiar certas transações ou mineradores, causando desigualdade e favorecimento dentro da rede.

### **Limitações de um Ataque de 51%**

Apesar das ações prejudiciais possíveis, um atacante não pode fazer tudo.

Eles **não** podem:

**Criar novas moedas do nada.**

**Reverter transações antigas (além das mais recentes).**

**Modificar as regras de consenso ou as propriedades fundamentais da blockchain.**

**Caso histórico:** Em 2014, o pool de mineração GHash.io chegou perto de controlar 51% do poder de hashing da rede, atingindo cerca de 42% em um ponto. Isso gerou grande preocupação na comunidade, levando a uma **descentralização voluntária dos mineradores para reduzir o risco**.

Desde então, a rede se tornou ainda mais distribuída. Controlar o poder de hashing da rede Bitcoin não é apenas uma questão de adquirir hardware e energia; é também sobre a logística de manter essa operação massiva em escala global.

**O custo, a necessidade de infraestrutura e a vigilância contínua da comunidade tornam essa tarefa extremamente difícil e impraticável para qualquer entidade isolada.**

## 5.9 Stratum V2

Stratum V2 é uma versão atualizada do protocolo de mineração Stratum, amplamente utilizado na mineração de Bitcoin. Ele foi desenvolvido para resolver várias limitações e problemas presentes no Stratum V1, melhorando a eficiência, a segurança e a flexibilidade do processo de mineração. Aqui estão os principais aspectos e problemas que o Stratum V2 visa resolver:

**Autenticação e Criptografia:** O Stratum V2 oferece autenticação e criptografia de ponta a ponta, protegendo as comunicações entre o minerador e a pool de mineração contra ataques de interceptação (man-in-the-middle) e espionagem. Isso é particularmente importante para proteger dados sensíveis e evitar que atacantes possam alterar ou monitorar o tráfego.

**Redução do Overhead:** O Stratum V2 é projetado para reduzir a quantidade de dados transmitidos entre os mineradores e a pool, melhorando a eficiência da comunicação. Ele usa um formato de mensagem binária compacta, em vez de um formato de texto, o que economiza largura de banda e acelera a transmissão de dados.

**Distribuição de Trabalho:** Diferente do Stratum V1, onde a pool de mineração controla completamente o trabalho distribuído aos mineradores, o Stratum V2 permite que os mineradores selezionem transações e construam blocos de forma mais independente. Isso aumenta a descentralização e dá mais autonomia aos mineradores.

**Priorização de Transações:** Com o Stratum V2, os mineradores têm mais controle sobre quais transações incluir nos blocos, permitindo que eles priorizem transações com taxas mais altas, o que pode aumentar a lucratividade.

**Failover e Reconexão Automática:** O Stratum V2 inclui melhorias no gerenciamento de conexões, como failover automático e reconexão rápida, o que aumenta a robustez e a resiliência das operações de mineração em caso de falhas de rede ou desconexões.

O Stratum V2 visa resolver problemas de segurança, eficiência e centralização presentes na versão anterior do protocolo, proporcionando uma solução mais robusta e adaptável para o futuro da mineração.

O Stratum V2 é um dos projetos open-source que oferecem grants para desenvolvedores do ecossistema Bitcoin. Saiba mais em [11. Carreira em Desenvolvimento Open-Source](#)

## 6. Bitcoin Core

Desde que Satoshi Nakamoto lançou o Bitcoin v0.1 em janeiro de 2009, sob a licença de software livre MIT, centenas de desenvolvedores ao redor do mundo têm contribuído para o daemon e o cliente de referência, além de diversos clientes alternativos. Estes desenvolvedores, que colaboram no desenvolvimento do software principal, são coletivamente conhecidos como "Bitcoin Core". Hoje a implementação de referência do software está em <https://github.com/bitcoin>

As discussões e novos lançamentos eram frequentemente compartilhados através da lista de discussão pública 'bitcoin-dev', que agora está sendo descontinuada em favor de novas plataformas como os fóruns <https://groups.google.com/g/bitcoindev> e [Delving Bitcoin](#).

A maioria desses colaboradores trabalha de forma voluntária, embora alguns sejam patrocinados por seus empregadores ou recebam subsídios de empresas do setor. Recentemente, o financiamento se tornou mais diversificado graças a iniciativas como GitHub Sponsors, Human Rights Foundation (HRF) Bitcoin Development Fund, Bitcoin Donation Portal e Open Sats.

Os mantenedores do projeto, liderados atualmente por Wladimir van der Laan, desempenham um papel crucial que inclui equilibrar tarefas reativas (interações com a comunidade) com

tarefas proativas, como a escrita e revisão de código, similar ao papel de "zelador" em outros projetos de software de código aberto.

Além disso, há um clube semanal de revisão de código, onde são discutidos conceitos importantes e pull-requests, promovendo uma colaboração contínua e a melhoria do projeto. É o Bitcoin Core PR Review Club—<https://bitcoincore.reviews/>

## 7. BIPS—Propostas de Melhoria do Bitcoin

Desde 2011, mudanças no Bitcoin, além das tarefas de manutenção, são introduzidas e organizadas através de um processo chamado Propostas de Melhoria do Bitcoin, ou BIPs (Bitcoin Improvement Proposals). As BIPs são uma maneira formal de documentar, discutir e implementar mudanças e melhorias no protocolo Bitcoin.

A ideia das BIPs foi inspirada pelo processo de Propostas de Melhoria da Python (PEPs), utilizado para melhorar a linguagem de programação Python. A intenção é fornecer uma estrutura clara e transparente para a introdução de mudanças no Bitcoin.

A primeira BIP (BIP 0001) foi proposta por Amir Taaki e define o processo pelo qual as BIPs devem ser submetidas, discutidas e aprovadas.

### **Processo de Criação, Avaliação e Aceitação de uma BIP**

A ideia para uma nova BIP é inicialmente formulada e discutida organicamente em vários canais de comunicação, como IRC, listas de discussão, fóruns e redes sociais.

Após a ideia ser amadurecida, o autor escreve um rascunho da BIP. Este rascunho é submetido para revisão e comentários pela comunidade.

O rascunho é submetido ao repositório de BIPs, onde passa por um processo formal de revisão. Durante essa fase, o autor pode fazer ajustes com base no feedback recebido.

A BIP é amplamente discutida e avaliada pela comunidade e por desenvolvedores principais. Essa etapa pode envolver vários ciclos de revisão e modificação.

Uma vez que a BIP é aceita em princípio, uma implementação de referência é criada. Esta implementação é um exemplo prático de como a mudança deve ser incorporada ao Bitcoin.

A implementação de referência é testada pela comunidade. Se for aceita e considerada estável, a BIP é promovida ao status "Final".

Várias BIPs tiveram impactos significativos no desenvolvimento e aprimoramento do Bitcoin. Aqui estão algumas das mais importantes:

**BIP 0016 (P2SH):** Introduzida por Gavin Andresen, essa BIP implementou o "Pay to Script Hash" (P2SH), permitindo transações mais complexas, como carteiras multisig.

**BIP 0032 (Hierarchical Deterministic Wallets):** Proposta por Pieter Wuille, essa BIP introduziu carteiras determinísticas hierárquicas, facilitando a gestão e backup de carteiras com múltiplos endereços.

**BIP 0065 (CheckLockTimeVerify):** Proposta por Peter Todd, essa BIP adicionou uma nova função de script que permite bloquear uma transação até um determinado momento, habilitando contratos inteligentes mais avançados.

**BIP 0141 (Segregated Witness - SegWit):** Introduzida por Pieter Wuille, essa BIP corrigiu a maleabilidade das transações e aumentou a capacidade de transação, permitindo soluções de escalabilidade como a Lightning Network.

**BIP 0144 (Compact Block Relay):** Também parte da implementação do SegWit, essa BIP melhorou a eficiência da propagação de blocos na rede.

**BIP 0173 (Bech32 Address Format):** Proposta por Pieter Wuille e Greg Maxwell, essa BIP introduziu um novo formato de endereço, que é mais eficiente e menos propenso a erros de digitação.

O Segregated Witness, ou SegWit, é um exemplo notável de uma BIP que teve um grande impacto no Bitcoin. Ele foi definido pelas BIPs 141 e 144 e introduziu mudanças no consenso para corrigir a maleabilidade das transações e melhorar a escalabilidade. Após meses de testes e discussões, SegWit foi ativado na mainnet em 2017.

As BIPs são fundamentais para o processo de evolução do Bitcoin, permitindo uma abordagem estruturada e colaborativa para a implementação de mudanças. Elas garantem que qualquer melhoria ou alteração no protocolo seja bem documentada, discutida e testada antes de ser adotada.

Para desenvolvedores e entusiastas do Bitcoin, compreender o processo das BIPs e conhecer as mais importantes é essencial para participar ativamente na comunidade e no desenvolvimento contínuo do Bitcoin. Você pode conhecer todas as BIPs do Bitcoin acessando o repositório oficial do Bitcoin Core: <https://github.com/bitcoin/bips>

## 8. RPC API do Bitcoin Core

O Bitcoin Core implementa uma interface JSON-RPC que pode ser acessada usando a ferramenta de linha de comando `bitcoin-cli`. Esta interface permite experimentar interativamente as funcionalidades disponíveis programaticamente via API.

Após instalar o Core e iniciá-lo com o comando `bitcoind -daemon`, você consegue começar a chamar comandos RPC (Remote Procedure Call). É possível acessar diretamente via HTTP usando `curl`.

## Comandos Básicos de RPC

Os comandos RPC do Bitcoin Core permitem explorar interativamente a blockchain, verificar transações, e obter informações detalhadas sobre o estado da rede e da carteira. Para ver uma lista dos comandos disponíveis, use:

```
bitcoin-cli help
```

Veja alguns comandos úteis.

`bitcoin-cli getbestblockhash`: Retorna o hash do melhor bloco na cadeia de blocos.

`bitcoin-cli getblock "blockhash"`: Obtém informações sobre um bloco específico dado seu hash.

`bitcoin-cli getblockchaininfo`: Exibe informações detalhadas sobre o estado da blockchain.

`bitcoin-cli getnetworkinfo`: Exibe informações básicas sobre o status do nó da rede Bitcoin.

`bitcoin-cli getrawtransaction "txid"`: Retorna uma transação não processada em notação hexadecimal.

`bitcoin-cli decoderawtransaction "hex"`: Decodifica uma transação não processada de hexadecimal para JSON.

`bitcoin-cli walletpassphrase "passphrase" timeout`: Desbloqueia a carteira e a mantém desbloqueada por um período de tempo específico.

`bitcoin-cli walletpassphrasetchange "oldpassphrase" "newpassphrase"`: Muda a senha da carteira.

`bitcoin-cli walletprocesspsbt "psbt"`: Processa uma PSBT (Partially Signed Bitcoin Transaction).

`bitcoin-cli getblockhash 1000`: Para obter o hash do bloco na altura 1000.

`bitcoin-cli getblock "blockhash"`: Para obter detalhes de um bloco usando seu hash.

`bitcoin-cli getrawtransaction "txid"`: Para obter e decodificar uma transação usando seu ID.

`bitcoin-cli decoderawtransaction "hex"`: Decodifica uma transação não processada de hexadecimal para JSON.

`bitcoin-cli getnetworkinfo`: Para obter informações sobre o status do nó da rede.

Usar esses comandos através da linha de comando ou programaticamente via API permite que desenvolvedores e entusiastas do Bitcoin interajam diretamente com a rede, validando e explorando dados de maneira independente e segura. Veja mais em

<https://developer.bitcoin.org/reference/rpc/>

## 9. Lightning Network

Você encontra o livro-texto Mastering the Lightning Network traduzido para pt-BR neste repositório: <https://github.com/biohazel/lntbook-pt-br>

A Rede Lightning é um sistema descentralizado para micropagamentos instantâneos e de alto volume que elimina o risco de delegar a custódia de fundos a terceiros confiáveis. O Bitcoin, a moeda digital mais amplamente utilizada e valiosa do mundo, permite que qualquer pessoa envie valor sem um intermediário ou depósito confiável. O Bitcoin contém um sistema de script avançado que permite aos usuários programar instruções para fundos. No entanto, há algumas desvantagens no design descentralizado do Bitcoin.

As transações confirmadas na blockchain do Bitcoin levam até uma hora para serem irreversíveis (aproximadamente 6 confirmações, ou 6 blocos de profundidade).

Micropagamentos, ou pagamentos menores que alguns centavos, são inconsistentes e as taxas tornam essas transações inviáveis na rede atualmente.

A Rede Lightning resolve vários problemas de escalabilidade e custo do Bitcoin. É uma das primeiras implementações de um contrato inteligente multipartidário (dinheiro programável) usando o script embutido do Bitcoin. A Rede Lightning está liderando o desenvolvimento tecnológico em transações financeiras multipartidárias com Bitcoin, permitindo transações rápidas, de baixo custo e fora da cadeia (off-chain).

**Pagamentos Instantâneos:** O Bitcoin agrupa transações em blocos espaçados de dez minutos. Os pagamentos são amplamente considerados seguros no Bitcoin após a confirmação de seis blocos, ou cerca de uma hora. Na Rede Lightning, os pagamentos não precisam de confirmações de bloco e são instantâneos e atômicos. A Lightning pode ser usada em terminais

de ponto de venda no varejo, com transações de dispositivo para dispositivo, ou em qualquer lugar onde pagamentos instantâneos são necessários.

**Micropagamentos:** Novos mercados podem ser abertos com a possibilidade de micropagamentos. A Lightning permite enviar fundos até 0,00000001 bitcoin sem risco de custódia. A blockchain do Bitcoin atualmente impõe um tamanho mínimo de saída muitas centenas de vezes maior e uma taxa fixa por transação, o que torna os micropagamentos impraticáveis. A Lightning permite pagamentos mínimos denominados em bitcoin, usando transações reais de bitcoin.

**Escalabilidade:** A rede Bitcoin precisará suportar ordens de magnitude maior volume de transações para atender à demanda por pagamentos automatizados. O aumento iminente de dispositivos conectados à internet precisa de uma plataforma para pagamentos de máquina para máquina e serviços de micropagamento automatizados. As transações da Rede Lightning são conduzidas fora da blockchain sem delegação de confiança e propriedade, permitindo que os usuários realizem transações quase ilimitadas entre outros dispositivos.

**Como Funciona:** Os fundos são colocados em um endereço "canal" de bitcoin com múltiplas assinaturas de duas partes. Esse canal é representado como uma entrada no livro-razão público do Bitcoin. Para gastar fundos do canal, ambas as partes devem concordar com o novo saldo. O saldo atual é armazenado como a transação mais recente assinada por ambas as partes, gastando do endereço do canal. Para fazer um pagamento, ambas as partes assinam uma nova transação de saída gastando do endereço do canal. Todas as transações de saída antigas são invalidadas ao fazer isso.

A Rede Lightning não requer cooperação da contraparte para sair do canal.

Ambas as partes têm a opção de fechar unilateralmente o canal, encerrando seu relacionamento. Como todas as partes têm múltiplos canais com múltiplos usuários diferentes nesta rede, é possível enviar um pagamento para qualquer outra parte através desta rede. Ao embutir o pagamento condicionado ao conhecimento de um hash criptográfico seguro, os pagamentos podem ser feitos através de uma rede de canais sem a necessidade de qualquer parte ter propriedade unilateral dos fundos.

A Rede Lightning permite o que anteriormente não era possível com sistemas financeiros confiáveis vulneráveis a — sem a necessidade de confiança e custódia, a participação na rede pode ser dinâmica e aberta para todos.

A escalabilidade é um dos principais desafios enfrentados pela rede Bitcoin. Este termo refere-se à capacidade do Bitcoin de processar um grande número de transações de forma rápida e eficiente. Aqui estão alguns dos desafios específicos:

**Limite de Tamanho do Bloco:** Cada bloco na blockchain do Bitcoin tem um tamanho máximo de 1 megabyte. Isso limita o número de transações que podem ser incluídas em cada bloco,

resultando em uma capacidade máxima de aproximadamente 7 transações por segundo. Este é um número relativamente pequeno comparado a sistemas de pagamento tradicionais, como as redes de cartões de crédito, que podem processar milhares de transações por segundo.

**Tempo de Confirmação:** O tempo médio para minerar um bloco é de cerca de 10 minutos. Durante períodos de alta demanda, as transações podem levar muito tempo para serem confirmadas, causando atrasos significativos.

**Taxas de Transação:** Quando a rede está congestionada, as taxas de transação aumentam à medida que os usuários competem para que suas transações sejam incluídas nos próximos blocos. Isso pode tornar o uso do Bitcoin caro, especialmente para transações de menor valor.

A Lightning Network é uma solução de camada 2 projetada para resolver os problemas de escalabilidade do Bitcoin. Ela permite transações rápidas e de baixo custo, movendo-as fora da blockchain principal (off-chain). Aqui está como a Lightning Network funciona e como ela aborda os desafios de escalabilidade.

**Canais de Pagamento:** A Lightning Network utiliza canais de pagamento entre pares. Dois usuários podem abrir um canal de pagamento estabelecendo uma transação inicial na blockchain do Bitcoin. Uma vez que o canal está aberto, eles podem realizar um número ilimitado de transações entre si sem ter que registrar cada transação individualmente na blockchain.

**Transações Off-Chain:** As transações realizadas dentro de um canal de pagamento são registradas apenas pelos dois participantes do canal, não sobrecarregando a blockchain do Bitcoin. Apenas a abertura e o fechamento do canal são registrados on-chain, o que reduz significativamente a quantidade de dados processados na blockchain.

**Baixas Taxas e Alta Velocidade:** Como as transações na Lightning Network não requerem confirmação dos mineradores, elas são quase instantâneas e têm taxas muito mais baixas. Isso torna viável o uso do Bitcoin para pequenas transações cotidianas, como comprar um café ou pagar por um serviço online.

**Rede de Canais:** A Lightning Network é composta por uma rede de canais de pagamento interconectados. Mesmo que dois usuários não tenham um canal direto entre si, eles podem enviar transações através de múltiplos canais intermediários, desde que exista um caminho disponível. Isso amplia significativamente a utilidade da Lightning Network.

**Segurança:** Apesar de operar off-chain, a Lightning Network ainda se beneficia da segurança da blockchain principal do Bitcoin. Se houver qualquer tentativa de fraude ou desentendimento entre os participantes, as regras da Lightning Network permitem que os usuários revertam para a blockchain principal para resolver disputas.

A Lightning Network resolve os problemas de escalabilidade do Bitcoin ao mover a maior parte das transações fora da blockchain principal, permitindo transações rápidas, baratas e seguras. Isso aumenta a capacidade da rede de Bitcoin e torna o sistema mais eficiente e escalável para um uso mais amplo.

## 9.1 BOLTs—Basics of Lightning Technology

Os Fundamentos da Tecnologia Lightning (BOLT) são as especificações técnicas padronizadas para a Lightning Network, definindo como várias implementações podem interoperar entre si na mesma rede.

O processo de criação, avaliação, desenvolvimento e testes de uma BOLT é colaborativo e rigoroso, envolvendo múltiplas etapas de revisão, testes e refinamentos. Esse processo garante que as melhorias propostas para a Lightning Network sejam tecnicamente sólidas, seguras e benéficas para a comunidade como um todo.

O processo de submissão e aprovação de um BOLT é análogo ao processo nas BIPs do Bitcoin. Conheça as BOLTS que estão implementadas atualmente.

### BOLT 1: Conceitos Básicos da Tecnologia Lightning (BOLTs)

**Descrição:** Este BOLT fornece uma visão geral da Lightning Network, explicando os conceitos fundamentais e objetivos. Define a estrutura e o propósito dos BOLTs, que servem como documentos padronizados para especificações do protocolo.

**Exemplo de Aplicação:** Um desenvolvedor novo na Lightning Network pode consultar este BOLT para entender a arquitetura geral e o propósito, orientando seus esforços iniciais de desenvolvimento.

### BOLT 2: Protocolo de Par para Gerenciamento de Canal

**Descrição:** Especifica o protocolo para gerenciar canais entre pares, incluindo estabelecimento, fechamento e troca de mensagens.

**Exemplo de Aplicação:** Implementação de um nó Lightning que pode abrir e fechar canais de pagamento com pares, garantindo conformidade com o protocolo da rede.

### BOLT 3: Formatos de Transações e Scripts Bitcoin

**Descrição:** Detalha os formatos de transação e scripts usados na Lightning Network, incluindo os detalhes das transações de financiamento e a estrutura das transações de compromisso.

**Exemplo de Aplicação:** Criação de transações ou scripts personalizados para recursos avançados, como tempos de bloqueio personalizados ou pagamentos condicionais.

### BOLT 4: Protocolo de Roteamento Onion

**Descrição:** Descreve o protocolo de roteamento onion usado para pagamentos multi-hop privados e seguros. Inclui detalhes sobre estrutura de pacotes, criptografia e o processo de roteamento.

**Exemplo de Aplicação:** Desenvolvimento de lógica de roteamento de pagamentos seguros em uma carteira ou serviço Lightning, garantindo que os pagamentos dos usuários sejam roteados de forma confidencial pela rede.

#### **BOLT 5: Manuseio On-chain da Lightning Network**

**Descrição:** Fornece diretrizes para lidar com transações on-chain (fechamento de canais cooperativo ou forçado), incluindo monitoramento de canais e transações de remediação de violação.

**Exemplo de Aplicação:** Implementação de serviços de "watchtower" que monitoram a blockchain para fraudes potenciais ou violações e tomam ações corretivas.

#### **BOLT 6: Especificação de Transações de Compromisso**

**Descrição:** Define a estrutura e as regras para transações de compromisso, que são o núcleo das atualizações de estado do canal.

**Exemplo de Aplicação:** Garantir que um nó Lightning manipule corretamente as transações de compromisso para manter a integridade do canal e prevenir perdas.

#### **BOLT 7: Descoberta de Nós e Canais P2P**

**Descrição:** Descreve os protocolos para descoberta de nós e canais, permitindo que os nós encontrem pares e aprendam sobre a topologia da rede.

**Exemplo de Aplicação:** Aprimorar a capacidade de um nó Lightning de descobrir e conectar-se dinamicamente a novos pares, melhorando a conectividade e robustez da rede.

#### **BOLT 8: Transporte Criptografado e Autenticado**

**Descrição:** Especifica o protocolo de camada de transporte criptografado e autenticado para comunicação segura entre nós.

**Exemplo de Aplicação:** Garantir a segurança dos canais de comunicação em uma implementação de nó Lightning, assegurando que todas as mensagens sejam criptografadas e autenticadas.

#### **BOLT 9: Flags de Recursos Atribuídos**

**Descrição:** Lista as flags de recursos usadas na Lightning Network para sinalizar recursos opcionais do protocolo que um nó suporta.

**Exemplo de Aplicação:** Desenvolvimento de aplicações Lightning que possam negociar recursos suportados com pares, garantindo compatibilidade e interações ricas em funcionalidades.

#### **BOLT 10: Inicialização de DNS e Localização Assistida de Nós**

**Descrição:** Define o uso de DNS para inicializar a conexão inicial do nó e auxiliar na localização de nós.

**Exemplo de Aplicação:** Implementação de lógica de conexão inicial em uma carteira Lightning que usa DNS para encontrar e conectar-se à Lightning Network.

#### **BOLT 11: Protocolo de Fatura para Pagamentos Lightning**

**Descrição:** Especifica o formato para faturas de pagamento Lightning, incluindo detalhes como valor, hash de pagamento e tempo de expiração.

**Exemplo de Aplicação:** Geração e decodificação de faturas de pagamento em um processador de pagamento Lightning, permitindo que os usuários façam e recebam pagamentos facilmente.

<https://www.bolt11.org/>

Embora o **BOLT 12** ainda esteja em desenvolvimento ativo e não tenha sido formalmente integrado ao repositório principal das BOLTs, ele traz diversas melhorias sobre o BOLT 11, incluindo suporte a ofertas estáticas (o que significa que um único código QR pode ser gerado e usado repetidamente para pagamentos. Isso contrasta com o BOLT 11, onde cada pagamento exigia um código QR único), pagamentos recorrentes, caminhos blindados e mensageria onion. Para detalhes mais específicos e atualizações, é recomendável acompanhar as discussões na [lightning-dev mailing list](#) e nos repositórios de desenvolvimento relevantes.

Esses BOLTs garantem que a Lightning Network opere de maneira eficiente, segura e interoperável, proporcionando aos desenvolvedores os padrões necessários para criar aplicações robustas e ricas em funcionalidades.

Os BOLTs (Basis of Lightning Technology) são gerenciados de forma colaborativa pelos desenvolvedores da comunidade Lightning Network. Desenvolvedores de vários clientes da Lightning Network, como LND (Lightning Network Daemon), Éclair e Core Lightning, contribuem e asseguram a compatibilidade de seus softwares com esses padrões.

Discussões e propostas de desenvolvimento ocorrem na lightning-dev-mailing-list e redes sociais como Nostr e X.

## 9.2 Canais de Pagamento

A Lightning Network é uma solução inovadora para os problemas de escalabilidade e custo das transações on-chain no Bitcoin. Ela permite que transações rápidas e de baixo custo sejam realizadas off-chain através de canais de pagamento. Esses canais são construídos sobre endereços multisig 2-de-2, timelocks e saídas de transações Segregated Witness, proporcionando uma maneira segura e eficiente de movimentar bitcoins entre usuários sem a necessidade de registrar cada transação na blockchain principal.

Para entender melhor como gerenciar e otimizar a capacidade desses canais, é importante conhecer as várias opções disponíveis, incluindo a abertura de novos canais, técnicas de splicing, rebalancamento de canais, swaps submarinos, fábricas de canais e canais dual-funded. Além disso, provedores de liquidez terceirizados podem ser utilizados para adicionar fundos aos seus canais, aumentando a flexibilidade e a eficiência das suas transações na Lightning Network.

Para aumentar a capacidade de um canal na Lightning Network, você tem várias opções, incluindo splicing. Aqui estão as principais opções:

## **Abrir um Novo Canal**

Abrir um novo canal com a quantidade adicional de bitcoins que você deseja ter disponível. Isso pode ser feito independentemente ou com o mesmo parceiro de canal, aumentando a capacidade total disponível para suas transações na Lightning Network.

## **Splicing**

Splicing é uma técnica que permite adicionar ou remover fundos de um canal existente sem fechá-lo. Existem dois tipos principais de splicing:

**Splice-In:** Adicionar fundos ao canal existente. Isso envolve uma transação on-chain que adiciona mais bitcoin ao canal, aumentando sua capacidade.

**Splice-Out:** Remover fundos do canal, permitindo que você retire parte do saldo do canal sem fechar o canal completamente.

## **Rebalanceamento de Canais**

Rebalancear o canal significa mover fundos entre seus canais existentes para otimizar a liquidez sem a necessidade de fechar ou abrir novos canais. Isso pode ser feito enviando pagamentos para si mesmo através da rede Lightning para redistribuir o saldo entre os canais.

## **Loop In/Loop Out (Submarine Swaps)**

Utilizando swaps submarinos, você pode mover fundos entre a rede Lightning e a blockchain principal sem fechar os canais. Existem dois tipos:

**Loop In:** Mover fundos da blockchain principal para um canal Lightning.

**Loop Out:** Mover fundos de um canal Lightning para a blockchain principal.

## **Fábricas de Canais**

Channel Factories permitem a criação de canais de pagamento múltiplos entre várias partes usando uma única transação on-chain inicial. Isso pode aumentar a eficiência e a capacidade geral dos canais.

## **Canais de Financiamento Duplo**

Os canais dual-funded permitem que ambas as partes contribuam com fundos na abertura do canal, aumentando a capacidade inicial sem a necessidade de uma única parte financiar o canal inteiro.

## **Provedores de Liquidez Terceirizados**

Você pode usar provedores de liquidez terceirizados, que podem adicionar fundos aos seus canais em troca de uma taxa. Isso é particularmente útil para usuários que necessitam de capacidade adicional sem querer abrir novos canais diretamente.

Essas opções proporcionam flexibilidade para gerenciar e otimizar a capacidade de seus canais na Lightning Network, garantindo que você tenha a liquidez necessária para realizar transações eficientes e rápidas.

Um canal de pagamento é simplesmente um endereço multisig 2-de-2 no Bitcoin, para o qual você possui uma chave, e seu parceiro de canal possui a outra chave. Para abrir um canal na lightning, o canal efetivamente lhe dará acesso à toda a rede, você precisa primeiro enviar bitcoin on-chain para seu endereço de abertura de canal.

O valor da transação que você fizer on-chain será seu crédito de gasto. Para realizar um pagamento maior que essa primeira transação on-chain, você precisaria abrir outro canal ou aumentar a liquidez do seu canal.

Reforçando a memória, os canais de pagamento são construídos sobre endereços multi-assinatura 2-de-2, timelocks e saídas de transações Segregated Witness.

**Abertura de Canal:** Um canal é aberto após o endereço multi-assinatura receber uma transação inicial de financiamento na cadeia (on-chain).

**Pagamentos Off-Chain:** As partes no canal podem fazer pagamentos off-chain entre si, atualizando o saldo do canal ao longo do tempo, tanto quanto desejarem.

**Fechamento de Canal:** Qualquer um dos participantes pode decidir fechar o canal, de forma cooperativa ou não cooperativa, a qualquer momento.

**Liquidação do Saldo:** Quando o canal é fechado, o saldo será liquidado através de uma transação registrada na cadeia (on-chain).

### **Exemplo Hipotético com Três Partes (A, B, C) em Roteamento**

Cenário Inicial:

Participantes: A, B, e C.

Canais de Pagamento:

A possui um canal de pagamento com B.

B possui um canal de pagamento com C.

Pagamento de A para C:

A atualiza seu saldo com B:

A deseja enviar 1 BTC para C.

A e B atualizam seu canal de pagamento: A diminui seu saldo em 1 BTC e B aumenta seu saldo em 1 BTC.

Esse processo é realizado através de um contrato de hash bloqueado por tempo (HTLC), garantindo que a transação só seja concluída se todos os participantes concordarem.

B atualiza seu saldo com C:

B, agora com 1 BTC a mais, envia esse 1 BTC para C. B e C atualizam seu canal de pagamento: B diminui seu saldo em 1 BTC e C aumenta seu saldo em 1 BTC. Novamente, isso é feito usando um HTLC para garantir segurança e sincronização.

Pagamento de C para A:

C paga B:

Se C deseja enviar 1 BTC para A, o processo é similar, mas na direção oposta.

C e B atualizam seu canal de pagamento: C diminui seu saldo em 1 BTC e B aumenta seu saldo em 1 BTC, utilizando um HTLC.

B paga A:

B, agora com 1 BTC a mais, envia esse 1 BTC para A.

B e A atualizam seu canal de pagamento: B diminui seu saldo em 1 BTC e A aumenta seu saldo em 1 BTC, também utilizando um HTLC.

#### **Como Funciona o HTLC (Hash Time-Locked Contract):**

HTLC é um tipo de contrato inteligente que garante a segurança das transações na Lightning Network. Ele permite que um pagamento seja realizado apenas se uma determinada condição for satisfeita, como a apresentação de um segredo (hash pré-imagem) ou o cumprimento de um prazo de tempo. Isso impede que fundos sejam perdidos ou roubados durante o roteamento do pagamento.

Esta estrutura permite transações rápidas e baratas, utilizando a segurança da rede Bitcoin, mas sem a necessidade de registrar cada transação individualmente na blockchain, aumentando a escalabilidade e eficiência do sistema.

Saiba mais em <https://lightning.network/>

### 9.3 Nós Lightning

Abaixo estão as diferentes formas de interagir com a Lightning Network e os aplicativos principais que fornecem esses serviços. Essa variedade de opções permite que os desenvolvedores e usuários escolham a abordagem que melhor se adapta às suas necessidades e preferências.

#### **Full Node**

Operar um nó completo da Lightning Network envolve executar um nó Bitcoin completo e um nó Lightning ancorado a ele. Isso oferece a máxima segurança e controle, mas requer mais recursos de hardware e conhecimento técnico. Para gerenciar nós Lightning completos, ferramentas como [Ride The Lightning](#) são extremamente úteis. Veja abaixo algumas implementações populares de nós lightning.

*LND (Lightning Network Daemon):* Desenvolvido pela Lightning Labs, é uma das implementações mais populares para operar um nó completo. Ele oferece uma ampla gama de funcionalidades e APIs para desenvolvedores.

*c-lightning:* Desenvolvido pela Blockstream, é uma implementação leve e modular do protocolo Lightning, oferecendo flexibilidade para customizações.

*Eclair:* Desenvolvido pela ACINQ, é uma implementação robusta da Lightning Network voltada para nós completos, com suporte a várias funcionalidades avançadas.

### **Light Node**

Nós leves não requerem a execução de um nó Bitcoin completo. Eles dependem de nós completos terceirizados para verificar as transações e blocos, tornando-os mais fáceis de configurar e operar.

### **Carteiras Custodiadas**

Carteiras custodiadas são gerenciadas por terceiros, o que significa que a responsabilidade pelos fundos é transferida para a empresa que fornece o serviço. Elas são fáceis de usar e ideais para iniciantes.

**Wallet of Satoshi:** Uma carteira custodiada que oferece uma interface amigável e simplificada para transações na Lightning Network. <https://www.walletofsatoshi.com/>

### **Carteiras Não-Custodiadas—100% controladas pelos usuários**

Carteiras não custodiadas permitem que os usuários mantenham o controle total sobre suas chaves privadas e fundos, oferecendo maior segurança e privacidade.

**Phoenix Wallet:** Desenvolvido pela ACINQ, é uma carteira móvel que atua como um nó leve, permitindo transações rápidas e seguras na Lightning Network. Quando você cria uma carteira pela Phoenix, ela automaticamente abre um canal com a ACINQ, o nó mais bem conectado e com maior liquidez de toda a rede. <https://phoenix.acinq.co/>

**Zeus Wallet:** Permite aos usuários conectar-se a seus próprios nós LND, c-lightning, ou Electrum, oferecendo controle total sobre os fundos e transações. É realmente empoderante poder estar em qualquer lugar do mundo e transacionar por meio de uma conexão VPN diretamente do seu nó completo na sua casa. É a auto-soberania financeira completa. Saiba mais em: <https://zeusln.com/>

## 9.4 Exploradores de Rede

Exploradores de rede da Lightning Network permitem aos usuários verificar o estado dos canais, transações e outros dados relevantes de forma pública.

[1ML](#): Um explorador de rede e diretório de nós para a Lightning Network, oferecendo visualizações de canais, capacidades e informações sobre nós.

[Amboss](#): Outro explorador que fornece uma interface amigável para explorar a topologia da rede Lightning e informações detalhadas sobre nós e canais.

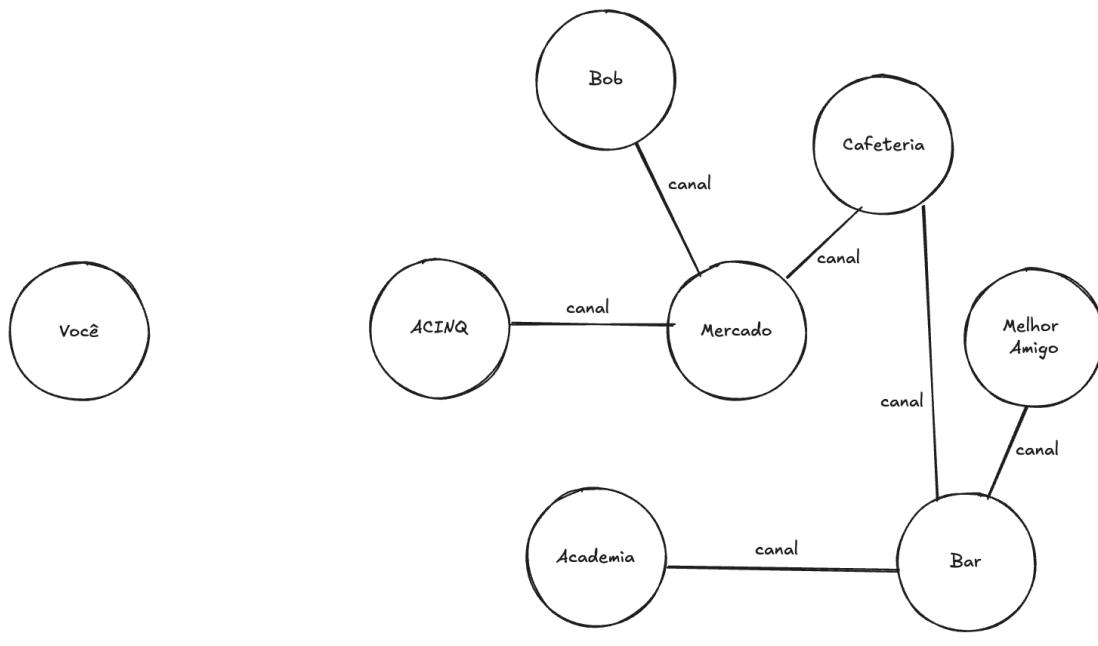
Essas diversas formas de interagir com a Lightning Network fornecem uma gama de opções adaptáveis a diferentes níveis de conhecimento técnico e requisitos de segurança. Com essas ferramentas, tanto desenvolvedores quanto usuários podem se engajar de maneira eficiente e segura com a Lightning Network.

## 9.5 Prática: Meu Primeiro Bitcoin na Lightning Network

Hora de experimentar uma transação de Bitcoin via Lightning. Quando transacionamos Bitcoin on-chain, como fizemos anteriormente, o termo usado é "transação". No caso da Lightning Network, o termo usado é "pagamento", pois essencialmente realizamos pagamentos de faturas (invoices). Por meio da função `keysend`, conseguimos enviar valores arbitrários para as pessoas, mas ainda assim continuamos chamando de pagamentos.

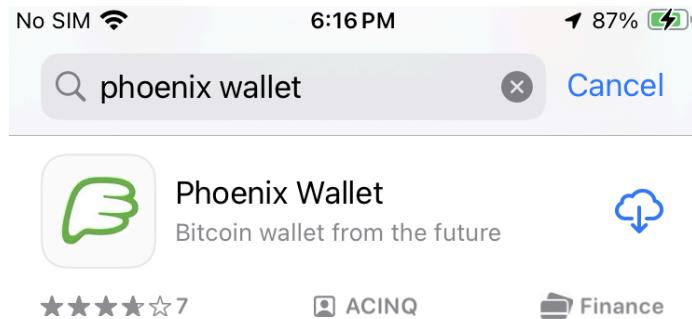
Para interagir com a Lightning Network, você precisa abrir um primeiro canal que lhe dará acesso potencialmente a todos os nós da rede, dependendo de quão bem conectado ele é. O nó ACINQ é um dos mais bem conectados e também um dos maiores em termos de liquidez (quantidade de bitcoins alocados).

A carteira Phoenix, desenvolvida pela ACINQ, facilita esse processo de abertura de canal com eles, permitindo que você usufrua de pagamentos instantâneos e de baixas taxas na Lightning Network. Antes de termos nosso primeiro canal aberto, nós não conseguimos realizar e receber pagamentos pela Lightning. A situação está ilustrada abaixo.

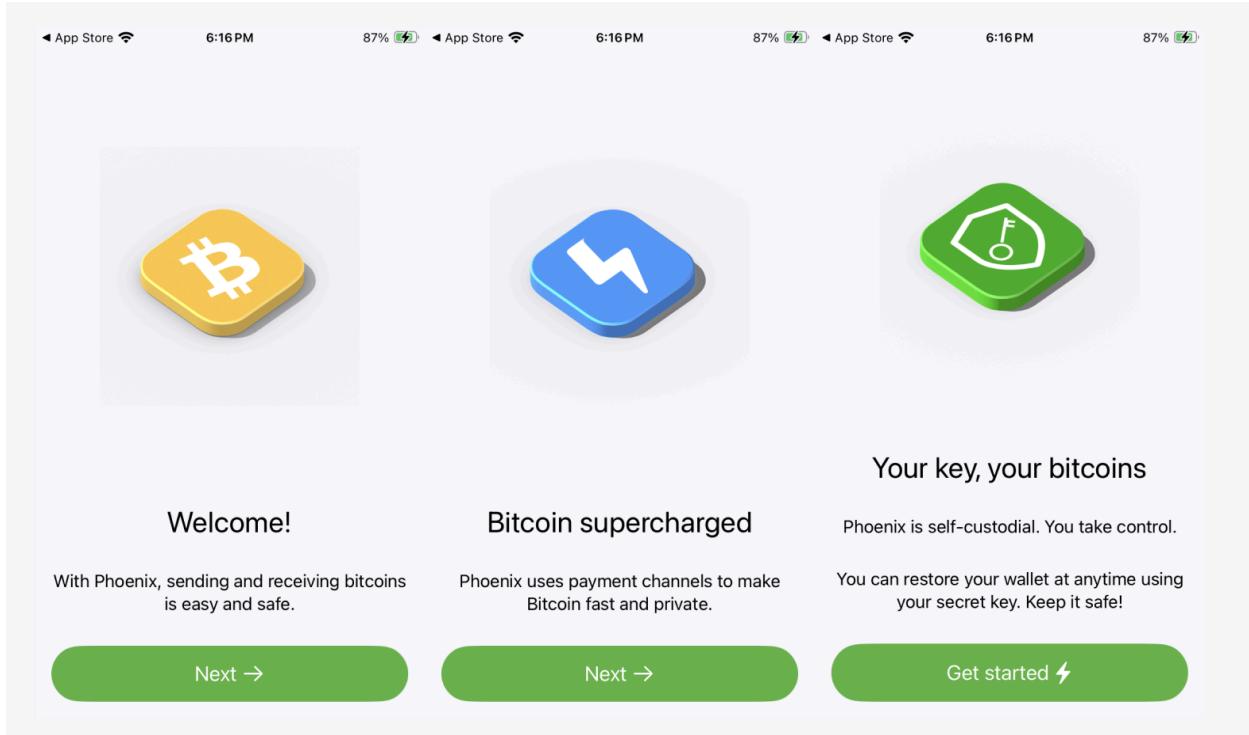


Rede Lightning

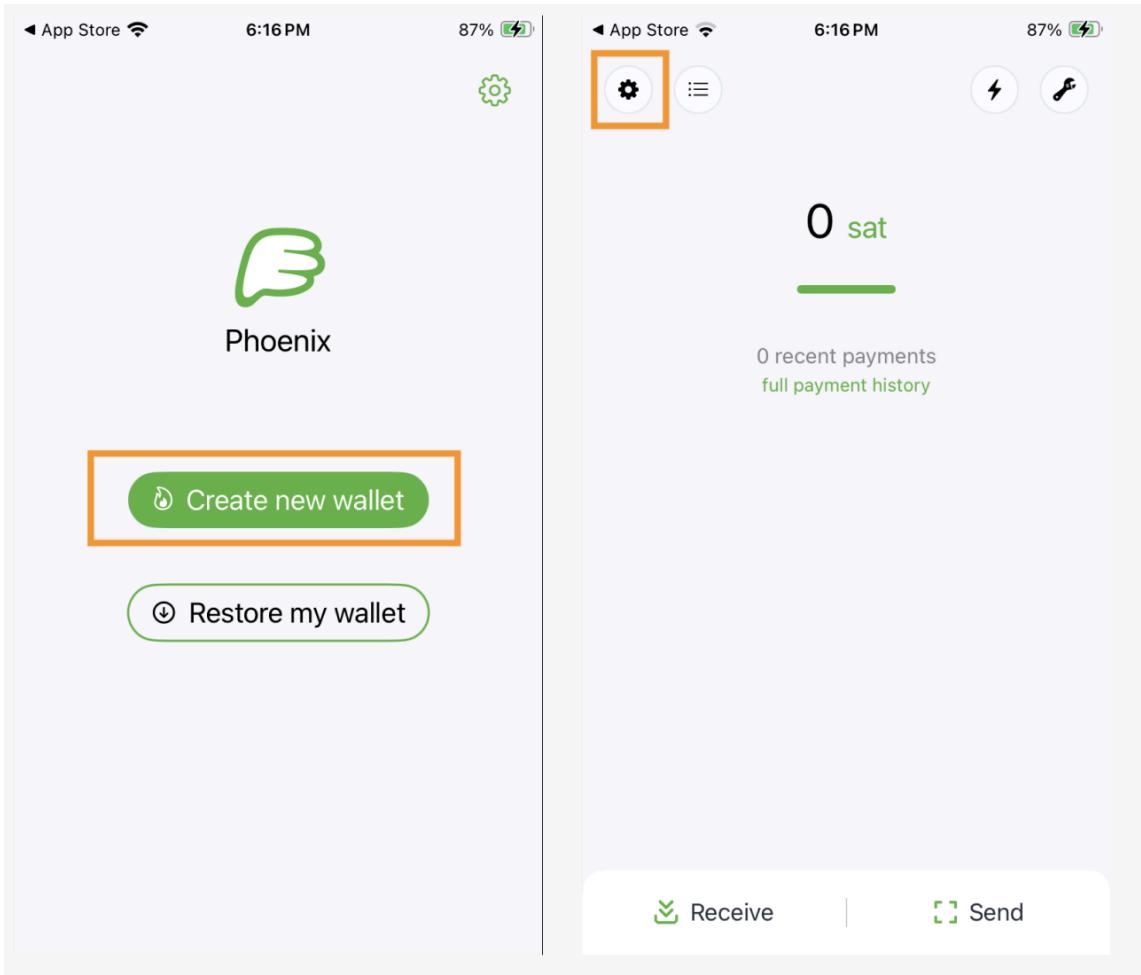
Para fazer nossa primeira transação na Lightning, vamos utilizar a carteira Phoenix.



Vão ter 3 telas iniciais, você clica em **Next**, **Next** e **Get started**.



Agora escolha **Create new wallet**. Em seguida, clique no ícone de **Configurações** para encontrarmos e anotarmos nossa frase mnemônica de recuperação de carteira.



Clique em **Recovery phrase** e em seguida em **Display seed**.

The image shows two screenshots of the Phoenix wallet app interface on an iPhone.

**Left Screenshot: Settings**

- Top bar: App Store, 6:17 PM, 87% battery.
- Section: FEES
  - Channel management
  - Add liquidity
- Section: PRIVACY & SECURITY
  - App access
  - Recovery phrase** (highlighted with an orange border)
  - Electrum server
  - Tor
  - Payments backup

**Right Screenshot: Recovery Phrase**

- Top bar: App Store, 6:17 PM, 87% battery.
- Text: "Beware of phishing. The developers of Phoenix will never ask for your seed."
- Text: "Do not lose this seed. Save it somewhere safe (not on this phone). If you lose your seed and your phone, you've lost your funds."
- Section: Display seed (button highlighted with an orange border)
- Section: LEGAL
  - I have saved my recovery phrase somewhere safe.
  - I understand that if I lose my phone & my recovery phrase, then I will lose the funds in my wallet.
- Cloud icon: iCloud backup

Anote bem sua seed.



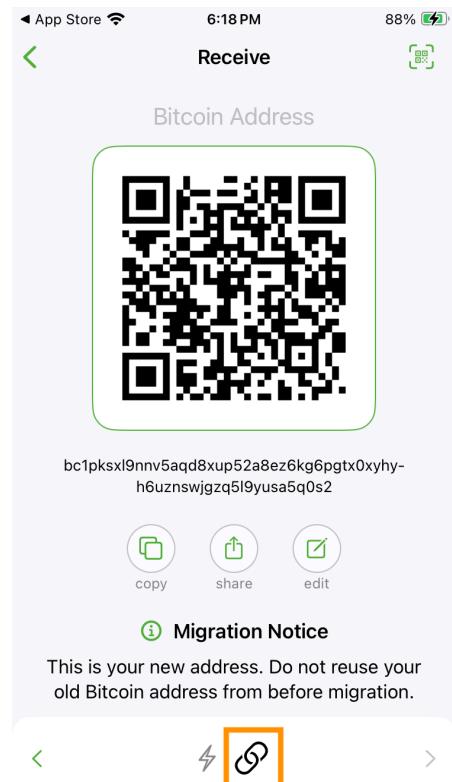
KEEP THIS SEED SAFE.  
DO NOT SHARE.

```
#1 fork  
#2 roast  
#3 deputy  
#4 vendor  
#5 seek  
#6 myth  
#7 decide  
#8 ten  
#9 prepare  
#10 diet  
#11 over  
#12 gas
```

[Copy](#)

BIP39 seed with standard BIP84 derivation path

Agora, clique no x, depois em **Receive**, e clique no ícone de corrente.



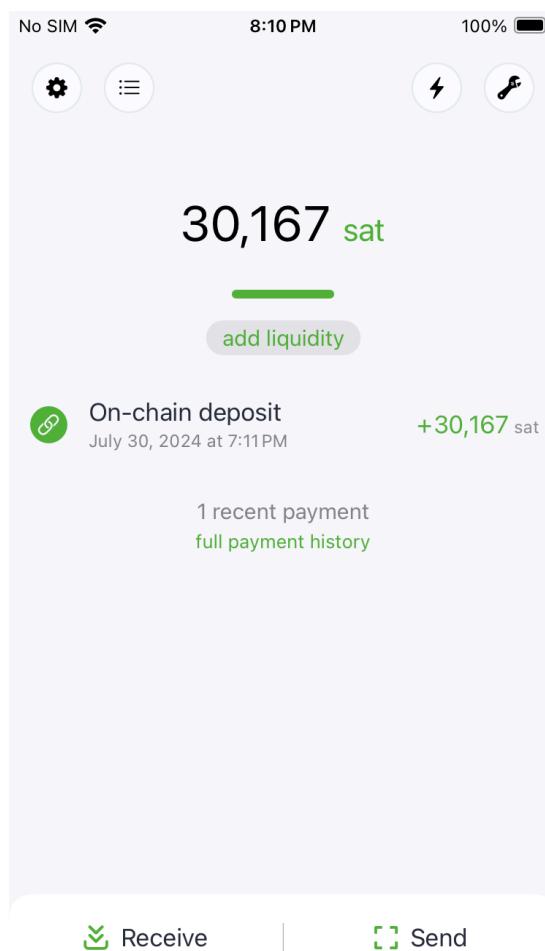
Esse endereço na tela é um endereço on-chain para sua carteira. Agora que você já sabe como fazer transações on-chain, pode abrir sua carteira BlueWallet e enviar uma quantia para esse endereço. Essa quantia será a capacidade do seu canal na Lightning Network.

Pense nisso como uma conta pré-paga, uma quantia de bitcoin que fica 'travada' no canal, mas que você pode usar para enviar e receber bitcoin com taxas muito baixas e em velocidade instantânea.

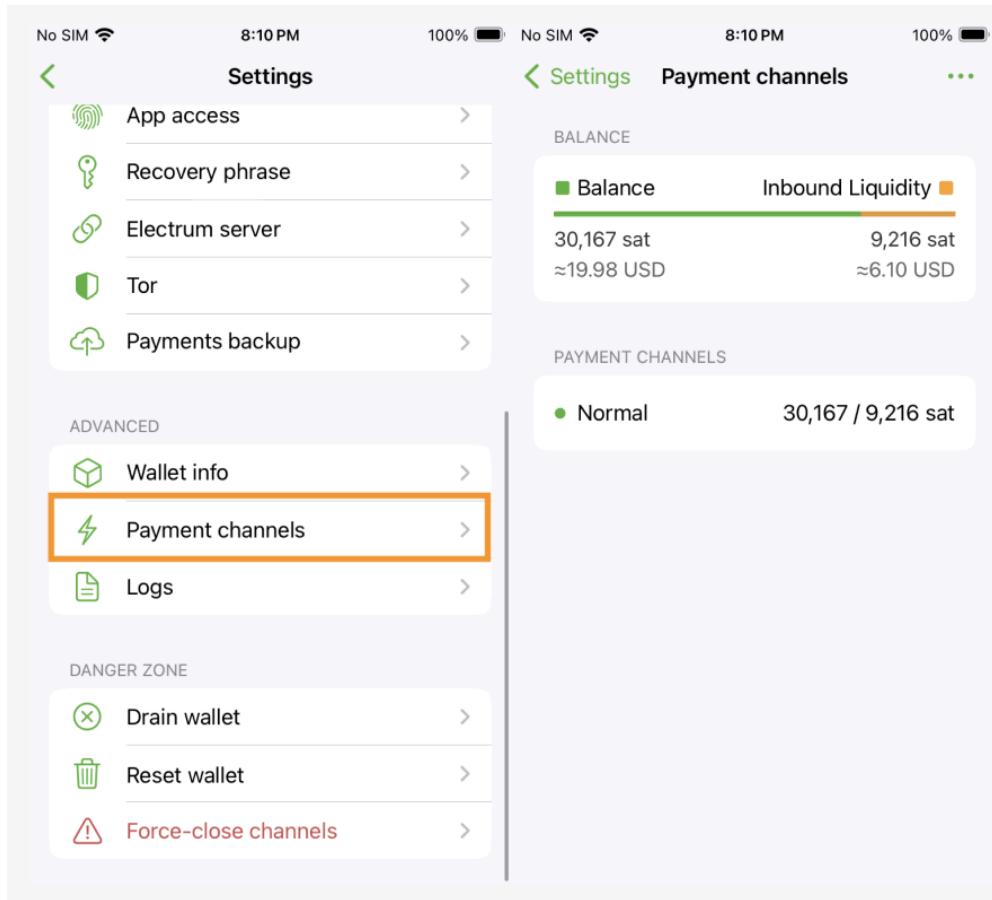
**Em um mundo onde o Bitcoin é uma moeda de troca, você pode vir a abrir um canal na Lightning e nunca mais fechar. Agora que você sabe quase tudo sobre Bitcoin, monte uma economia circular na sua comunidade e essa realidade chegará antes que imagina.**

A priori, quando você abre um canal na Lightning Network, você só tem capacidade outbound, ou seja, para enviar bitcoins, e não para receber. Existem ferramentas que ajudam a balancear os canais para que você consiga tanto enviar quanto receber. A carteira Phoenix gerencia isso automaticamente.

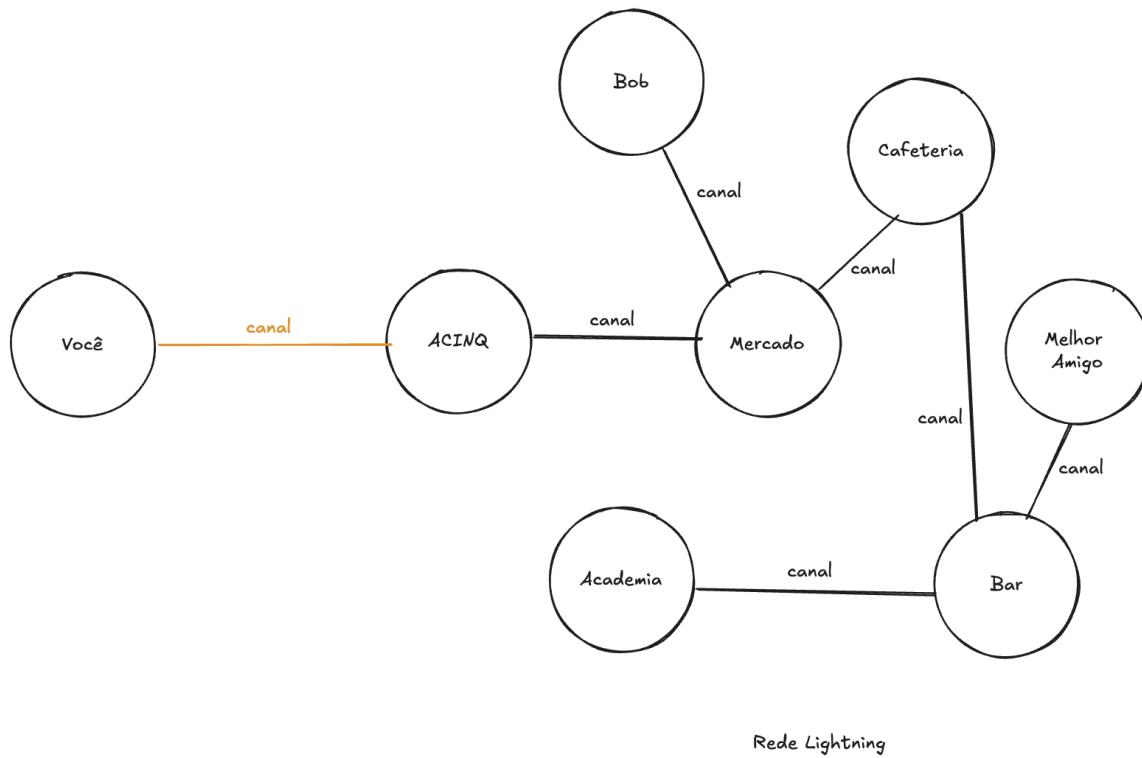
Após enviados os satoshis da sua outra carteira, você verá o valor na tela principal.



Novamente em **Configurações**, procure **Payment channels** e você verá seu primeiro canal aberto na Lightning.



Parabéns! Agora você está usando a melhor solução de camada L2 (Layer 2, camada 2, fora da camada 1 que é on-chain) do Bitcoin. O procedimento de pagar ou gerar invoices Lightning é completamente intuitivo, pelos botões **Send** e **Receive**, com opções de QR Code e código por escrito. O importante é que agora você está operando via Lightning por intermédio da Phoenix. Agora se alguém for lhe pagar em Bitcoin e perguntar "on-chain ou via Lightning", você já sabe a resposta.



## 10. Tecnologias de Liberdade

### 10.1 Cypherpunks

O Bitcoin foi criado como uma resposta às limitações do sistema financeiro tradicional e surgiu de uma busca pela liberdade humana. Este movimento foi fortemente influenciado pela comunidade de cypherpunks, um grupo de ativistas tecnológicos que defendem o uso da criptografia para proteger a privacidade e promover a liberdade individual.

Os cypherpunks são conhecidos por sua defesa vigorosa do uso da criptografia para assegurar a privacidade e a liberdade de expressão na era digital. Formada nos anos 1990, esta comunidade é composta por programadores, criptógrafos e defensores da privacidade que acreditam que a criptografia é uma ferramenta essencial para manter a liberdade pessoal contra a vigilância e o controle governamental.

A filosofia dos cypherpunks está enraizada na crença de que a privacidade é fundamental para a liberdade humana. Eles defendem a criação e o uso de tecnologias que possam proteger as comunicações e transações pessoais de qualquer forma de vigilância ou censura.

A criação do Bitcoin por Satoshi Nakamoto em 2008 foi fortemente influenciada pelos ideais cypherpunk. Nakamoto estava envolvido em discussões sobre criptografia e moedas digitais, e o Bitcoin representa uma implementação prática das ideias defendidas pelos cypherpunks: um sistema financeiro descentralizado e anônimo.

O movimento cypherpunk começou no final dos anos 1980 e início dos anos 1990. Foi fundado por pessoas como Eric Hughes, Timothy C. May, e John Gilmore.

Em 1993, Eric Hughes publicou o "[Manifesto Cypherpunk](#)", que delineou os princípios e objetivos do movimento. Ele enfatizou a importância da privacidade e o uso da criptografia para alcançá-la.

Os cypherpunks acreditam que a privacidade é essencial para uma sociedade livre e que ela deve ser protegida contra intrusões, usam e promovem o uso da criptografia forte como meio de proteger comunicações e dados pessoais, e defendem sistemas descentralizados que não dependem de autoridades centrais, pois esses sistemas são menos suscetíveis à censura e controle.

### **Tecnologias e Contribuições da Comunidade Cypherpunk**

**PGP (Pretty Good Privacy):** Um dos primeiros e mais conhecidos softwares de criptografia, criado por Phil Zimmermann, um membro da comunidade cypherpunk. Desenvolvido em 1991, o PGP permitiu a qualquer pessoa proteger suas comunicações eletrônicas de maneira eficaz. Zimmermann se tornou um símbolo da luta pela privacidade digital, recebendo diversos prêmios e reconhecimentos por suas contribuições à segurança da informação.

A luta de Zimmermann, que enfrentou retaliações do governo americano na década de 1990, ajudou a solidificar a importância da privacidade digital como um direito fundamental. Em 1993, ele foi alvo de uma investigação criminal por suposta violação das leis de exportação de munições, uma vez que o PGP era considerado tecnologia de criptografia de grau militar. No entanto, após intensa pressão pública e campanhas de apoio, o caso foi encerrado sem acusações formais em 1996.

A defesa de Zimmermann pela criptografia forte influenciou políticas e regulamentações em todo o mundo, promovendo a adoção de tecnologias de segurança digital tanto por indivíduos quanto por empresas. Seu trabalho continua a impactar a segurança digital até hoje, estabelecendo a criptografia como uma ferramenta essencial para a proteção da privacidade e da liberdade de expressão na era digital.

No contexto do desenvolvimento Bitcoin, por exemplo, é boa prática que os desenvolvedores envolvidos assinem seus commits com suas chaves PGP. Saiba mais em <https://docs.github.com/en/authentication/managing-commit-signature-verification/signing-commits>

**Tor:** O movimento cypherpunk influenciou diretamente os criadores do Tor. A rede Tor (The Onion Router) foi originalmente desenvolvida pelo Laboratório de Pesquisa Naval dos Estados Unidos em meados da década de 1990. O projeto começou com a necessidade de proteger as comunicações online do governo dos EUA. Em 2002, Tor foi lançado ao público para fornecer anonimato na internet.

**Bitcoin:** Embora Satoshi Nakamoto, o criador do Bitcoin, não tenha sido um membro declarado da comunidade cypherpunk, muitos dos princípios e ideias do Bitcoin foram influenciados pela filosofia cypherpunk.

**Lightning Network:** Embora a Lightning Network não tenha sido criada explicitamente pelos cypherpunks, ela incorpora muitos dos valores fundamentais da filosofia cypherpunk, como a privacidade, a descentralização e a eficiência. Essas características são refletidas nas decisões de design que permitem transações rápidas e privadas, mantendo a segurança e a descentralização do Bitcoin. A LN continua a evoluir como uma solução crucial para escalar o Bitcoin, mantendo seus princípios fundamentais.

Muitos cypherpunks são ativistas que lutam contra a vigilância em massa e a censura na internet, defendendo políticas que protejam a privacidade e a liberdade digital. A filosofia e as tecnologias desenvolvidas pela comunidade cypherpunk têm tido uma influência significativa na segurança digital e na proteção da privacidade online. Eles têm desempenhado um papel crucial no desenvolvimento de muitas das tecnologias de segurança digital que usamos hoje.

A influência dos cypherpunks continua a ser sentida no desenvolvimento de novas tecnologias de privacidade e segurança. Projetos que seguem os princípios cypherpunk continuam a surgir, buscando sempre proteger a liberdade individual no mundo digital.

### **O ecossistema de desenvolvimento open-source Bitcoin é atrelado à filosofia de proteção da privacidade e da liberdade humana.**

Muitos aplicativos integrados com o Bitcoin seguem essa lógica de design, e é especialmente gratificante saber que seu talento está sendo usado para construir ferramentas relevantes para libertar a humanidade. Veja alguns exemplos de projetos importantes no ecossistema, muitos dos quais oferecem oportunidades remuneradas para desenvolvedores.

## 10.2 JoinMarket e Jam

JoinMarket é uma ferramenta poderosa que permite aos usuários de Bitcoin aumentar significativamente a privacidade de suas transações através de um processo chamado CoinJoin. Desenvolvido para facilitar a mistura de transações de Bitcoin, JoinMarket conecta usuários que desejam anonimizar suas transações com aqueles que fornecem liquidez para o processo.

JoinMarket utiliza o conceito de CoinJoin, onde várias transações são combinadas em uma única transação conjunta, dificultando a rastreabilidade dos fundos. Aqui está um passo a passo de como o JoinMarket funciona. Existem dois tipos principais de usuários no JoinMarket:

**Makers:** Fornecem liquidez para o CoinJoin, oferecendo seus fundos para serem misturados. Em troca, eles recebem uma pequena taxa.

**Takers:** Iniciam a transação CoinJoin e pagam uma taxa aos Makers para misturar suas moedas.

Os usuários precisam configurar uma carteira JoinMarket, que pode ser feita através da interface de linha de comando ou da interface gráfica opcional. A carteira se conecta à rede Bitcoin para realizar as transações.

### Processo de CoinJoin

Makers anunciam suas ofertas de liquidez na rede JoinMarket.

Takers selecionam as ofertas dos Makers e iniciam uma transação CoinJoin.

A transação combinada é criada, assinada por todos os participantes e enviada à rede Bitcoin.

Use o modo de "daemon" para executar JoinMarket em segundo plano, facilitando a execução contínua de processos CoinJoin. Participe regularmente em CoinJoins para aumentar a privacidade de suas transações. Combine JoinMarket com outras práticas de privacidade, como o uso de endereços novos para cada transação.

Para instalar o JoinMarket, você pode clonar o repositório oficial do GitHub e seguir as instruções de instalação. Aqui estão os passos detalhados:

Clone o repositório JoinMarket:

```
git clone https://github.com/JoinMarket-Org/joinmarket-clientserver.git
```

```
cd joinmarket-clientserver
```

Execute o script de instalação:

```
./install.sh
```

Configurando a Carteira. Crie o arquivo de configuração:

```
cp cfg/joinmarket.cfg.example cfg/joinmarket.cfg
```

Edite o arquivo joinmarket.cfg conforme necessário, especialmente a seção de configuração da conexão com o Bitcoin Core.

Inicie o daemon do JoinMarket:

```
jmwalletd
```

**Veja o [guia de instalação](#) do JoinMarket, bem como seu [guia de uso](#).**

### **Contribuição ao Projeto**

Familiarize-se com o repositório do JoinMarket no GitHub, onde você pode encontrar o código-fonte e abrir pull requests para contribuir com melhorias. Participe de discussões na comunidade para entender as necessidades e prioridades dos usuários. Trabalhe em melhorias de interface de usuário para tornar o JoinMarket mais acessível a usuários não técnicos. Contribua para a documentação, ajudando novos usuários a configurar e utilizar JoinMarket de maneira eficaz.

Diferente de outros mixers centralizados, JoinMarket é descentralizado, eliminando a necessidade de confiar em um serviço intermediário. Makers são incentivados economicamente a fornecer liquidez, recebendo taxas dos Takers.

JoinMarket permite que os usuários escolham suas próprias taxas e ofertas, proporcionando flexibilidade no uso do serviço.

Ele representa uma ferramenta crucial para aqueles que valorizam a privacidade no uso do Bitcoin. Com uma comunidade ativa de desenvolvedores e usuários, a plataforma continua a evoluir, oferecendo métodos eficazes para anonimizar transações e proteger a privacidade financeira dos usuários.

### **JAM (Joinmarket-API-Interface)**

É uma interface de usuário (UX) avançada e amigável para JoinMarket, projetada para facilitar o uso do CoinJoin e melhorar a experiência do usuário, especialmente para aqueles que não são tecnicamente inclinados.

JAM é uma aplicação baseada em navegador que oferece uma interface gráfica (GUI) para interagir com o JoinMarket. Desenvolvida para ser intuitiva e acessível, ela permite que os usuários configurem e gerenciem suas carteiras JoinMarket, participem de CoinJoins e monitorem suas transações com facilidade.

O JAM representa um avanço significativo na usabilidade do JoinMarket, oferecendo uma interface amigável e acessível que facilita a participação em transações CoinJoin e melhora a privacidade dos usuários de Bitcoin. Tanto usuários quanto desenvolvedores são encorajados a

explorar e contribuir para o projeto, ajudando a construir uma ferramenta mais robusta e segura para todos.

Para mais informações e instruções detalhadas sobre como começar, visite o repositório oficial do [JAM no GitHub](#).

## 10.3 E-cash—Federated Chaumian Mints

O Chaumian e-cash é uma tecnologia essencial para a preservação da privacidade em transações digitais, concebida pelo [criptógrafo David Chaum](#). Ele permite a criação de moedas digitais que são anônimas e não rastreáveis, utilizando técnicas de criptografia avançadas, como assinaturas cegas (blind signatures). Esta tecnologia é de particular interesse para desenvolvedores que buscam criar sistemas de pagamento privados e seguros.

Embora o Bitcoin utilize um modelo diferente para garantir a segurança e a privacidade das transações, a ideia de assinaturas cegas de Chaum contribuiu significativamente para a compreensão de transações anônimas e descentralizadas que deram origem ao Bitcoin. A combinação dos dois sistemas favorece a escala do Bitcoin como um sistema financeiro que realmente preserve a privacidade dos usuários.

### Funcionamento do Chaumian E-cash

Chaumian e-cash é um sistema que utiliza assinaturas cegas para garantir que a entidade que emite o dinheiro não possa vincular a identidade do usuário às transações subsequentes. Isso é alcançado através de um processo onde os tokens digitais são assinados de forma cega pelo emissor, e somente o portador dos tokens pode gastá-los sem revelar sua identidade.

Ele é composto por duas partes principais: a casa da moeda (mint) e a carteira de e-cash. A tecnologia permite que qualquer pessoa opere uma casa da moeda para sua aplicação, que pode variar de carteiras digitais a sistemas de vouchers e recompensas.

Os tokens de e-cash emitidos pela casa da moeda têm paridade 1:1 com Bitcoin. Isso significa que para cada token de e-cash emitido, há uma quantidade equivalente de bitcoin mantido em reserva. Usuários podem facilmente converter seus tokens de e-cash de volta em Bitcoin, garantindo a liquidez e usabilidade dos fundos.

Chaumian e-cash combina a privacidade das assinaturas cegas com a eficiência e escalabilidade da Lightning Network. Essa combinação de privacidade, segurança e eficiência faz do Chaumian e-cash uma solução robusta para transações financeiras anônimas. Saiba mais sobre os componentes de um sistema E-cash.

**Casa da Moeda (Mint):** É responsável pela emissão dos tokens de e-cash. Quando um usuário deposita Bitcoin, a casa da moeda cria tokens equivalentes de e-cash usando assinaturas cegas. Este processo garante que a casa da moeda não possa rastrear as transações futuras desses tokens. Uma casa da moeda não armazena um banco de dados de contas de usuários

e suas atividades, o que protege os usuários de um sistema de E-cash contra vazamentos de seus dados privados para hackers e pode fornecer uma resistência à censura mais forte do que os sistemas de pagamento tradicionais.

**Carteira de e-cash:** Os usuários mantêm seus tokens de e-cash em carteiras digitais, que podem ser usadas para realizar transações. Estas transações respeitam a privacidade dos usuários, pois os tokens são gastos de maneira anônima.

As transações de e-cash entre usuários, ou de usuários para prestadores de serviços, são realizadas de maneira que a identidade do remetente e do destinatário é protegida. Qualquer pessoa pode operar uma casa da moeda para sua aplicação, seja uma carteira, um paywall na web, serviços de streaming pagos, ou um sistema de vouchers e recompensas.

O e-cash Chaumiano representa uma peça crucial na construção de tecnologias de liberdade financeira junto com o Bitcoin. Projetos como Cashu e Fedimint exemplificam como essa tecnologia pode ser aplicada para criar sistemas de pagamento privados e seguros, oferecendo amplas oportunidades para desenvolvedores dispostos a contribuir para o avanço do ecossistema Bitcoin de código aberto e de liberdade financeira.

### **Cashu**

Cashu é um protocolo de e-cash integrado ao protocolo Bitcoin. É um projeto que implementa o Chaumian e-cash para criar uma plataforma de transações Bitcoin privada e fácil de usar. Os usuários podem depositar Bitcoin e receber tokens de e-cash equivalentes que podem ser gastos anonimamente dentro do sistema. O principal benefício do Cashu é a proteção da privacidade do usuário, pois as transações realizadas com os tokens de e-cash não podem ser rastreadas.

O Cashu é focado principalmente em fornecer uma maneira simplificada e privada de usar Bitcoin, enfatizando a facilidade de uso e a privacidade das transações. É projetado para ser leve e fácil de implementar, tornando-o acessível para desenvolvedores que desejam integrar transações privadas de Bitcoin em seus aplicativos.

Desenvolvedores interessados em contribuir para o Cashu encontrarão várias oportunidades de trabalho open source. Eles podem se envolver na implementação de protocolos de privacidade, melhorar a eficiência das assinaturas cegas e criar interfaces de usuário que facilitam a adoção da tecnologia por um público mais amplo.

Saiba mais em: <https://docs.cashu.space/>

### **Fedimint**

Fedimint é outro projeto inovador que utiliza o Chaumian e-cash, mas com uma abordagem federada para a custódia e gestão de Bitcoin. Neste sistema, uma federação de entidades confiáveis colabora para emitir e gerenciar tokens de e-cash.

A federação utiliza assinaturas múltiplas (multi-sig) para aprovar a emissão e o resgate dos tokens, distribuindo a confiança entre vários participantes e mitigando riscos de segurança. A descentralização da federação assegura que não haja um único ponto de falha no gerenciamento da casa da moeda.

Para desenvolvedores, o Fedimint oferece um campo fértil para contribuir com a segurança descentralizada e a privacidade financeira. Oportunidades incluem a implementação de esquemas de multi-sig mais robustos, a otimização da comunicação entre os membros da federação e o desenvolvimento de ferramentas que facilitam a criação de federações em diferentes comunidades.

A implementação e o aprimoramento de tecnologias como o Chaumian e-cash em projetos como Cashu e Fedimint abrem um leque de oportunidades para desenvolvedores. Contribuir para esses projetos não só ajuda a fortalecer a privacidade e a segurança das transações financeiras, mas também posiciona os desenvolvedores na vanguarda da inovação tecnológica no espaço Bitcoin.

Participar desses projetos oferece a chance de trabalhar com tecnologias de ponta, colaborar com uma comunidade global de desenvolvedores e contribuir para a construção de sistemas financeiros mais justos e privados.

Seja aprimorando algoritmos criptográficos, desenvolvendo interfaces intuitivas ou implementando soluções de custódia descentralizadas, as possibilidades são vastas e impactantes.

Saiba mais em: <https://fedimint.org/>

## 10.4 Nostr

Tim Berners-Lee, um cientista da computação britânico, inventou a World Wide Web (WWW) em 1989 enquanto trabalhava no CERN, o laboratório de física de partículas na Suíça. Berners-Lee queria criar um sistema que facilitasse a troca de informações entre cientistas de diferentes universidades e instituições ao redor do mundo. Em 1991, ele lançou a primeira página web e o primeiro servidor web, tornando a web pública.

A visão original de Berners-Lee para a internet era uma rede descentralizada e incensurável, onde qualquer pessoa pudesse compartilhar e acessar informações livremente. Ele projetou a web como um espaço aberto, baseado em padrões universais e gratuitos, que promoveriam a comunicação e a colaboração global sem barreiras.

Com o tempo, empresas de tecnologia como Google, Facebook, Amazon e outras se tornaram dominantes na internet. Essas Big Techs e provedores de serviços de nuvem centralizaram grande parte do tráfego e dos dados da internet. Embora essas empresas tenham facilitado o acesso a informações e serviços, elas também introduziram novos desafios.

As grandes plataformas têm o poder de censurar conteúdos e controlar o que pode ou não ser compartilhado. A coleta massiva de dados pessoais para fins de monetização compromete a privacidade dos usuários. A dependência de servidores centralizados torna a rede vulnerável a falhas e ataques.

### O Problema que o Nostr Resolve

Nostr (Notes and Other Stuff Transmitted by Relays) é um protocolo criado para superar os problemas de centralização e censura na internet. Diferente das redes sociais e plataformas tradicionais, Nostr foi projetado para ser distribuído e resistente à censura.

Nostr é uma camada de protocolo simples de mensagens assíncronas. O protocolo opera de forma descentralizada e resistente à censura para garantir a liberdade de expressão. Portanto, não é um aplicativo ou serviço para o qual você se inscreve. É um protocolo, um padrão aberto sobre o qual qualquer pessoa pode construir.

O protocolo é baseado em objetos de eventos muito simples e flexíveis e utiliza criptografia de curva elíptica padrão para chaves e assinaturas. Como o Nostr não depende de alguns poucos servidores centrais para mover ou armazenar dados, ele é muito resiliente e permite comunicação resistente à censura entre seus clientes.

Nostr é um protocolo descentralizado, o que significa que não é controlado por nenhuma autoridade central. Em vez disso, a rede é apenas uma coleção de relays de dados (servidores) operados de forma independente. Uma pessoa pode usar sua máquina pessoal para servir como relay, garantindo que suas mensagens postadas estarão sempre disponíveis (pelo menos, pelo seu servidor doméstico) e voluntariar-se para armazenar e propagar eventos de outras chaves Nostr. Isso significa que o Nostr como um todo não é vulnerável à censura ou manipulação por qualquer entidade única.

Diferentemente de muitas plataformas de mídia social, o Nostr não coleta dados do usuário para vendê-los a anunciantes de terceiros. Nenhum endereço de e-mail, número de telefone ou identidade governamental está associado à sua conta Nostr. Assim como no Bitcoin, o sistema conhece apenas chaves públicas e assinaturas criptográficas para autenticação.

O Nostr oferece um sistema de monetização único para criadores de conteúdo. Ele é facilmente integrável com a Lightning Network. Diferente de outras plataformas de mídia social, que dependem da receita de publicidade para pagar os criadores de conteúdo, o Nostr permite que os criadores monetizem seu conteúdo diretamente com Bitcoin. Imagine que em cada post seu tem um botão que se as pessoas clicarem, elas estarão enviando satoshis de apreciação. Bem melhor que likes e o sequestro da nossa atenção no processo. Esses são os famosos Nostr Zaps.

O código do Nostr é open source, estando disponível para qualquer pessoa visualizar, usar e modificar. Isso permite transparência e colaboração no desenvolvimento do protocolo. Qualquer pessoa pode contribuir com o Nostr.

### Como o Nostr funciona

Cada conta Nostr é baseada em um par de chaves pública/privada. Uma maneira simples de pensar sobre isso é que sua chave pública é seu nome de usuário e sua chave privada é sua senha, com uma ressalva importante: ao contrário de uma senha, sua chave privada não pode ser redefinida se for perdida. Sua chave pública geralmente é apresentada como uma string com o prefixo *npub1* e a chave privada com o prefixo *nsec1*: Certifique-se de armazenar sua chave privada em um lugar seguro e não compartilhá-la com ninguém.

Por meio do compartilhamento de sua chave pública, outros podem encontrá-lo. Sua chave privada permite que você publique notas, interaja com outros e verifique que é você que está fazendo isso por meio de assinaturas criptográficas. A posse da chave também permite que você migre para outros clientes. Imagine que você tem uma conta no Twitter e quer mudar para o TikTok. Usando o Nostr, você pode fazer isso sem precisar avisar ninguém. Você simplesmente usa o novo cliente fazendo login com sua chave privada.

No Nostr, todos usam um cliente (Primal, Damus, Coracle, Amethyst, Iris, Snort, etc), a janela através da qual você olha para o protocolo Nostr. Para publicar algo, você escreve uma nota, assina-a com sua chave privada (ao apertar send, isso acontece automaticamente) e a envia para vários relays com redundância de cópias (servidores hospedados por outra pessoa, ou por você mesmo). Para obter atualizações de outros, você pergunta a vários relays se eles sabem algo sobre essas outras pessoas. Muito simples.

Nota: Se todos os relays que você usou no passado ficarem offline, todas as suas postagens serão irrecuperáveis. Esta é uma das razões pelas quais o Nostr permite que os usuários se conectem a muitos relays – isso garante algum maior grau de backup.

Embora um relay possa bloquear um usuário de publicar qualquer coisa nele, eles não podem impedir que alguém publique em outros relays ou de você executar seu próprio relay e transmitir suas próprias mensagens. Como os usuários são identificados por uma chave pública, eles não perdem suas identidades e sua rede de seguidores se forem banidos de um relay porque simplesmente podem se conectar a outro ou executar um por conta própria. Isso é exatamente o que torna o Nostr descentralizado e resistente à censura.

Se você deseja garantir que sua fala seja absolutamente incensurável, você pode e deve executar seu próprio relay. Isso garante que você sempre tenha uma cópia de todas as suas postagens e interações no Nostr para sempre. Se você estiver executando seu próprio nó Bitcoin com Umbrel, você pode facilmente executar seu próprio relay Nostr junto com seu nó Bitcoin.

Nota: Se você perceber que seu cliente Nostr está lento, é mais provável que seja devido aos relays que você está usando. Pode valer a pena adicionar alguns relays adicionais ao seu cliente para tornar a experiência mais agradável.

Veja um [vídeo do Uncle Bob Martin](#), que escreveu os conceituados livros Clean Code e Clean Architecture, falar sobre a importância do protocolo Nostr para preservar nossa liberdade de discurso (freedom of speech).

Saiba mais em: <https://nostr.com/>

Um ótimo cliente Nostr para iniciantes é o <https://primal.net/home>

Para devs é essencial que se familiarizem com as NIPs, ou Nostr Implementation Possibilities <https://github.com/nostr-protocol/nips>.

E esta é uma lista de relays bem conectados. O uptime dos relays é importante para manter a redundância e incensurabilidade das mensagens propagadas: <https://nostr.watch/relays/find>

Embora Nostr e Bitcoin operem em domínios diferentes, suas bases tecnológicas e filosóficas compartilham muitos princípios. A interoperabilidade entre as duas tecnologias pode levar a novos casos de uso inovadores que combinam comunicação segura e descentralizada com transações financeiras privadas e resistem a censura.

**O ecossistema de desenvolvimento Bitcoin + Nostr está em franco crescimento, há inclusive hackathons especializados para Nostr.**

Veja um snapshot do Primal

The screenshot shows the Primal Nostr app interface. On the left is a sidebar with icons for Home, Explore, Messages, Bookmarks, Notifications, Downloads, Settings (with a red notification badge), Help, and a New Note button. Below the sidebar is a circular profile icon for 'Scalar School' with the handle ':~\$'. The main content area features a large note from 'Scalar School' with the title ':~\$ Scalar School'. The note content includes the text 'Inspiring the next generation of Bitcoin developers.' and 'Inspirando a próxima geração de desenvolvedores Bitcoin.', followed by the URL 'scalarschool.org'. Below this are statistics: 4 notes, 0 replies, 0 zaps, 4 following, 3 followers, and 10 relays. A reply from 'Jonas' is shown, linking to 'https://bitcoindevphilosophy.com'. Another note from 'Scalar School' follows, quoting Adam Jonas: '"We are here to change the world!" —Adam Jonas'. The bottom of the screen shows a footer with the handle ':~\$ Scalar School' and a search bar at the top right.

Esta é nossa chave Nostr. Crie sua conta e nos siga por lá.

npub1jf9mxsndnwupaergsyat0myst8pygpz2pyx032dz62pefmz22esrcjf2t

## 10.5 Value4Value—Valor por Valor

A internet moderna é amplamente monetizada através de um modelo baseado em publicidade, onde algoritmos complexos e interesses empresariais desempenham um papel central. As plataformas de mídia social, mecanismos de busca e outros serviços online coletam vastas quantidades de dados dos usuários para personalizar anúncios e maximizar o engajamento.

Este modelo é alimentado por algoritmos que analisam comportamentos e preferências dos usuários, muitas vezes promovendo conteúdos que aumentam a retenção e o tempo de uso.

Embora eficaz para gerar receita, este sistema levanta preocupações significativas sobre privacidade, manipulação de informações e censura.

As plataformas coletam dados pessoais, históricos de navegação e interações dos usuários.

Utilizando esses dados, os algoritmos personalizam anúncios para aumentar a probabilidade de cliques e conversões. Os algoritmos promovem conteúdos que aumentam o tempo de uso, muitas vezes priorizando conteúdos polarizantes ou sensacionalistas para manter os usuários engajados.

A vigilância comercial é usada para entender melhor os comportamentos dos consumidores e direcionar produtos e serviços específicos. As empresas podem censurar conteúdos que não se alinham com seus interesses comerciais ou políticos, manipulando a percepção pública e influenciando opiniões.

### **Filosofia Value 4 Value (V4V)**

A filosofia Value 4 Value (V4V) propõe uma abordagem diferente, onde o conteúdo digital é monetizado diretamente pelos usuários através de micropagamentos, promovendo um ecossistema mais aberto e justo. Este modelo é facilitado pelo Bitcoin e pela Lightning Network, permitindo transações rápidas e de baixo custo.

Utilizando o Bitcoin e a Lightning Network, os criadores de conteúdo podem receber pagamentos diretos de seus usuários, eliminando a necessidade de intermediários.

As transações são transparentes e respeitam a privacidade dos usuários, evitando a coleta excessiva de dados. Os usuários são incentivados a apoiar diretamente os conteúdos e criadores que valorizam, criando uma relação mais direta e honesta.

O feedback dos usuários é valorizado e integrado no processo de criação, promovendo uma maior conexão e participação comunitária.

### **Nostr + Zaps**

Zaps são micropagamentos feitos através da Lightning Network que integram diretamente com a rede Nostr para apoiar conteúdos e criadores. Eles representam uma implementação prática da filosofia Value 4 Value (V4V).

Nostr / Zaps: <https://github.com/aljazceru/awesome-nostr>, <https://www.nostrapps.com/>

Outros exemplos de plataformas que habilitam uma cultura v4v.

Crowdfunding: <https://geyser.fund/>

Podcasting: <https://www.fountain.fm/>

Agendar Reuniões: <https://lncal.com/>

A filosofia Value 4 Value representa uma transição importante da monetização baseada em publicidade e vigilância para um modelo mais justo e aberto. Ao promover a transparência, a privacidade e o engajamento direto dos usuários, o V4V busca criar um ecossistema digital onde o valor é diretamente trocado entre criadores e consumidores, sem a interferência de intermediários.

Essa abordagem não só empodera os criadores de conteúdo, mas também promove a liberdade de expressão e a resistência à censura, alinhando-se com os princípios de descentralização e autonomia financeira promovidos pelo Bitcoin. Saiba mais em <https://value4value.info/>.

## 10.6 Democratização da Ciência

O sistema acadêmico tradicional é altamente estruturado, hierarquizado e burocrático, baseado em instituições como universidades, centros de pesquisa, e revistas científicas. Pesquisadores, para progredirem em suas carreiras, precisam publicar seus trabalhos em periódicos de alto impacto, que são frequentemente indexados em bases de dados como o Web of Science, Scopus, e Google Scholar.

Esse sistema de indexação é fundamental para a visibilidade e citação dos trabalhos científicos, o que, por sua vez, é crucial para a reputação e financiamento dos pesquisadores e instituições.

Os artigos são submetidos a periódicos, onde passam por um processo de revisão por pares antes de serem aceitos para publicação. Este processo pode ser demorado e muitas vezes sujeito a viés.

A proteção da propriedade intelectual é crucial para muitas universidades e centros de pesquisa, que frequentemente registram patentes para proteger suas inovações. Este processo pode ser demorado e caro, muitas vezes levando anos para ser concluído e limitando a evolução livre desses achados e tecnologias. Muitas pesquisas, especialmente aquelas financiadas por corporações, são realizadas sob acordos de não divulgação, limitando a transparência e a colaboração acadêmica.

Corporações frequentemente financiam pesquisas com o objetivo de obter resultados que beneficiem seus interesses comerciais. Isso pode levar a um viés nas conclusões e na publicação seletiva dos resultados. O processo de revisão por pares, publicação, e obtenção de patentes pode ser muito lento, beneficiando empresas que desejam controlar o ritmo de inovação para proteger seus próprios interesses.

Os editores de revistas científicas lucram com a venda de assinaturas e artigos individuais, muitas vezes a preços elevados e inacessíveis para o público geral. Empresas que financiam pesquisas podem controlar quando e como os resultados são divulgados, protegendo suas patentes e estratégias de mercado.

Esse paradoxo — onde a ciência, idealmente destinada a beneficiar a população, acaba servindo interesses privados — atrasa significativamente a evolução de soluções e tecnologias que poderiam beneficiar a humanidade. Ao priorizar a proteção de interesses comerciais e a manutenção do status quo, o sistema acadêmico tradicional impede a disseminação rápida e aberta de conhecimentos inovadores, limitando o progresso científico e tecnológico global.

## **Novo Paradigma Científico**

A introdução de novas plataformas e tecnologias descentralizadas, como Bitcoin e Nostr, oferece uma alternativa promissora, promovendo transparência e acessibilidade, e potencialmente acelerando o ritmo da inovação científica.

Essas tecnologias abrem novas possibilidades de se realizar e financiar pesquisas científicas. A transparência, rastreabilidade e alta disponibilidade global dos protocolos Bitcoin e Nostr permite que formas revolucionárias de pesquisa e desenvolvimento se formem, sem dependência direta de agências governamentais e processos competitivos e burocráticos de arrecadação de fundos para diversos tipos de projetos sociais e científicos.

Qualquer pessoa pode participar e contribuir para projetos científicos, facilitando a implementação de iniciativas de ciência cidadã em uma economia verdadeiramente global.

O novo paradigma científico oferece uma abordagem mais democrática para a pesquisa e desenvolvimento. Em vez de depender de instituições centralizadas e corporações que frequentemente controlam a agenda científica de acordo com seus interesses financeiros, tecnologias descentralizadas como Bitcoin e Nostr permitem uma distribuição mais equitativa de recursos e oportunidades.

Plataformas descentralizadas democratizam a ciência ao permitir que qualquer pessoa, independentemente de sua localização geográfica ou condição financeira, possa contribuir com a pesquisa e desenvolvimento. Isso é particularmente importante para cientistas e pesquisadores de países em desenvolvimento que, muitas vezes, enfrentam barreiras significativas para obter financiamento e publicar seus trabalhos.

Ao promover a transparência, a acessibilidade e a participação global, esse novo paradigma permite que iniciativas de pesquisa e desenvolvimento sejam mais abertas, justas e acessíveis, beneficiando toda a humanidade.

Iniciativas globais de citizen science se tornam fáceis de ser implementadas com uma economia livre e verdadeiramente global. Ferramentas como [Bitpac](#) favorecem a gestão democrática dos recursos em projetos e organizações.

Plataformas de crowdfunding como [Geyser Fund](#) permitem que você publique seu projeto e peça doações em Bitcoin para executá-lo.

O céu é o limite quando temos um sistema financeiro realmente livre.

## **Sci-Hub: um projeto notável**

O Sci-Hub—<https://sci-hub.se/>—é um repositório online que oferece acesso gratuito a milhões de artigos acadêmicos e de pesquisa. Fundado por Alexandra Elbakyan em 2011, o site surgiu como uma resposta ao alto custo de acesso a publicações científicas, que frequentemente

estão fora do alcance de pesquisadores e estudantes, especialmente em países em desenvolvimento.

Uma forma interessante de usar o potencial do Sci-Hub é procurando as publicações de interesse no [Google Scholar](#), e então realizando a busca no Sci-Hub para superar possíveis paywalls.

Para manter suas operações e evitar a interferência governamental, o Sci-Hub aceita doações em Bitcoin. Isso permite que o site continue fornecendo acesso gratuito a artigos científicos, financiando seus custos operacionais e combatendo ações judiciais.

## 10.7 Bitcoin Optech

Bitcoin Optech (Bitcoin Operations Technology Group) é uma organização dedicada a ajudar empresas de Bitcoin a adotarem tecnologias de escalabilidade e otimizarem sua eficiência operacional. O principal objetivo do Bitcoin Optech é fornecer recursos abrangentes, orientação técnica e melhores práticas para melhorar a funcionalidade e a escalabilidade da rede Bitcoin. Acompanhe suas atividades e newsletter em <https://bitcoinops.org/>

## 10.8 The Bitcoin Dev Project

Da seção Sobre no site <https://bitcoindevs.xyz/>:

*"Nosso objetivo é fornecer aos recém-chegados recursos e suporte para sua jornada de desenvolvimento de código aberto no Bitcoin. Estamos aqui para convencê-lo a contribuir para projetos de código aberto no Bitcoin. Medimos nosso sucesso pela ação, não pelo consumo passivo de materiais educativos.*

*Existe um sentimento repetido na comunidade de que o Bitcoin não precisa de você. Embora o Bitcoin seja projetado para ser resiliente, nós precisamos de você. O Bitcoin precisa de todo o talento e energia que puder reunir para resolver alguns dos problemas técnicos mais difíceis do nosso tempo. O Bitcoin em suas mãos muda tudo."*

O Bitcoin Dev Project é uma excelente iniciativa de Adam Jonas para compilar o caminho para se tornar um colaborador no ecossistema Bitcoin. O projeto oferece um conjunto robusto de ferramentas projetadas para ajudar os desenvolvedores em sua jornada de aprendizado, incluindo ferramentas de IA e de busca especializadas, e um jogo incrível chamado [Saving Satoshi](#), onde os desenvolvedores podem praticar conceitos de Bitcoin. Há também uma lista compilada de [Good First Issues](#) que os desenvolvedores podem tentar resolver assim que se sentirem prontas.

## 11. Carreira em Desenvolvimento de Software Livre e Open Source

*"Se um vídeo do YouTube sai do ar, podemos lamentar a perda de um conhecimento valioso, mas se um projeto open source sai do ar, isso pode literalmente quebrar a internet."*

— Nadia Eghbal, *Working in Public, The Making and Maintenance of Open Source Software*

O software livre e de código aberto é um pilar fundamental da sociedade digital moderna, promovendo a inovação, a segurança e a inclusão. Ele oferece uma alternativa sustentável e ética ao software proprietário, ao mesmo tempo que abre novas possibilidades de carreira e desenvolvimento profissional para indivíduos ao redor do mundo.

Nos dias de hoje, trabalhar em projetos de FOSS (Free and Open Source Software) se tornou uma opção de carreira viável e distinta do sistema corporativo tradicional. A importância do FOSS para a humanidade é imensa. Ele permite que qualquer pessoa, independentemente de recursos financeiros, tenha acesso a ferramentas de alta qualidade, promovendo a inclusão digital e a igualdade de oportunidades.

Além disso, a transparência do código aberto aumenta a segurança, pois qualquer pessoa pode inspecionar e melhorar o código, reduzindo a dependência de soluções proprietárias e aumentando a confiança no software utilizado.

Na comunidade open source, encontram-se alguns dos melhores programadores do mundo, trabalhando nos problemas de software mais complexos e desafiadores. Participar dessa comunidade é extremamente benéfico para o currículo de um desenvolvedor por várias razões.

Primeiramente, a natureza colaborativa dos projetos open source exige que os desenvolvedores possuam habilidades técnicas avançadas e uma capacidade de resolver problemas complexos de maneira eficaz. Contribuir para esses projetos demonstra que um desenvolvedor é capaz de trabalhar em equipe, comunicar-se bem e resolver problemas difíceis — habilidades altamente valorizadas por empregadores.

Os projetos open source são muitas vezes responsáveis por algumas das inovações tecnológicas mais significativas. Participar e contribuir para esses projetos permite que os desenvolvedores trabalhem com as tecnologias mais recentes e avanços na área de software. Isso não só aumenta a experiência prática do desenvolvedor, mas também mantém suas habilidades atualizadas com as tendências do setor.

Além disso, a visibilidade que vem com a contribuição para projetos open source é inestimável. O código e as contribuições de um desenvolvedor são publicamente acessíveis, permitindo que potenciais empregadores vejam diretamente a qualidade do trabalho e o nível de

comprometimento do desenvolvedor. Isso pode levar a oportunidades de carreira, já que muitas empresas de tecnologia monitoram ativamente essas comunidades em busca de talentos.

Participar da comunidade open source também oferece oportunidades de networking com outros desenvolvedores experientes e influentes na indústria. Essas conexões podem levar a colaborações futuras, recomendações de trabalho e mentoria, todas as quais podem ser extremamente valiosas para o desenvolvimento da carreira.

Ao contrário da ideia errônea de que os desenvolvedores open source são apenas voluntários, muitos começam como voluntários para demonstrar sua ética de trabalho e fazer networking. No entanto, existem muitas oportunidades para trabalhar em posições que são verdadeiramente rentáveis.

A maioria dos projetos open source são, de fato, precificados em dólares. Isso ocorre porque o dólar americano é a moeda mais amplamente aceita e utilizada internacionalmente, especialmente em transações online e em plataformas de financiamento coletivo. Esse padrão facilita a coordenação de projetos e pagamentos entre desenvolvedores de diferentes países.

Contribuir voluntariamente para projetos open source permite que os desenvolvedores construam um portfólio público, ganhem visibilidade na comunidade e estabeleçam conexões valiosas. Essas contribuições iniciais muitas vezes abrem portas para posições pagas dentro do mesmo projeto ou em outras iniciativas de código aberto.

Uma carreira como desenvolvedor open source pode ser gratificante e cheia de oportunidades, tanto para o crescimento profissional quanto para o impacto positivo na comunidade global. Em primeiro lugar, oferece uma grande flexibilidade e autonomia.

Desenvolvedores open source podem trabalhar em projetos de qualquer lugar do mundo, sem a necessidade de estarem fisicamente presentes em um escritório ou de seguirem horários rígidos. A colaboração remota é uma prática comum, permitindo que trabalhem nos horários que melhor se ajustem ao seu estilo de vida.

Contribuir para projetos open source também permite que desenvolvedores impactem positivamente a comunidade global. Eles podem resolver problemas reais e melhorar tecnologias usadas por muitas pessoas diariamente.

Participar desses projetos também proporciona um desenvolvimento contínuo de habilidades, já que os desenvolvedores trabalham com as mais recentes tecnologias e padrões da indústria, recebendo feedback direto de outros profissionais experientes, o que acelera seu aprendizado.

Uma das grandes vantagens de uma carreira open source é o reconhecimento e as oportunidades de carreira que ela pode proporcionar. Contribuições significativas para projetos open source aumentam a visibilidade e a reputação do desenvolvedor na comunidade

tecnológica. Existem diversas oportunidades de financiamento através de grants e patrocínios de empresas que suportam projetos de código aberto.

Os profissionais que mais se destacam nessa área geralmente possuem um perfil proativo e autodidata. Eles são capazes de aprender novas tecnologias e ferramentas por conta própria e demonstram iniciativa para identificar problemas e criar soluções. Habilidades de comunicação são vitais, pois a maior parte do trabalho envolve colaborar com outros desenvolvedores globalmente. Documentar o trabalho e comunicar ideias claramente em discussões e pull requests é essencial.

Desenvolvedores open source precisam ter habilidades técnicas sólidas, sendo proficientes em linguagens de programação relevantes e ferramentas de desenvolvimento. A familiaridade com sistemas de controle de versão, especialmente Git, é crucial. A paixão pela tecnologia e inovação é outro fator que diferencia esses profissionais. Eles são motivados pelo desejo de criar software de alta qualidade que resolva problemas reais e melhore a vida das pessoas.

Adaptabilidade e resiliência também são qualidades importantes, pois o ambiente de desenvolvimento open source pode ser dinâmico e desafiador. Os desenvolvedores precisam estar preparados para lidar com feedbacks constantes e mudanças rápidas.

Existem muitos exemplos de sucesso que ilustram a importância e o potencial de uma carreira open source. Linus Torvalds, criador do Linux, começou com um projeto open source que se tornou um dos sistemas operacionais mais importantes do mundo. Guido van Rossum, criador da linguagem de programação Python, também lançou seu projeto como open source, que hoje é amplamente utilizado.

**Trabalhar em projetos open source é a maneira perfeita de construir um portfólio. Quando você trabalha como desenvolvedor de software em empresas privadas, geralmente não pode colocar os projetos no seu portfólio devido a acordos de confidencialidade e propriedade intelectual. Em contraste, projetos open source são públicos por natureza, permitindo que você mostre seu trabalho, contribuições e habilidades de forma transparente para potenciais empregadores e colaboradores.**

**Ademais, uma carreira construída em software open source é meritocrática. Se você se destaca, é porque está realmente gerando valor. Isso pode se tornar uma defesa contra sistemas corporativos arbitrários que, em uma situação de layoff, por exemplo, acabam descartando excelentes profissionais por motivos de força maior.**

## 11.1 Filosofia do Desenvolvimento Bitcoin

Ser um desenvolvedor Bitcoin envolve uma grande responsabilidade ética e social. O Bitcoin é uma das melhores ferramentas já criadas para libertar a humanidade da tirania de governos opressivos e de políticas monetárias restritivas.

Para guiar esse compromisso ético, a comunidade Bitcoin compilou um documento que lista os principais aspectos filosóficos do desenvolvimento Bitcoin. Saiba mais em <https://rosenbaum.se/btcphil/>

## 11.2 Desenvolvimento Bitcoin FOSS

O Bitcoin exemplifica o poder e a importância do FOSS em criar sistemas descentralizados e inovadores que promovem a liberdade, a segurança e a inclusão financeira. O ecossistema do Bitcoin, com suas diversas aplicações de código aberto, continua a crescer e a evoluir, oferecendo vastas oportunidades para desenvolvedores e usuários ao redor do mundo.

---

Tradução do texto em <https://bitcoindevs.xyz/career>

Por que considerar uma carreira no desenvolvimento open source de bitcoin?  
Se você aspira a ter liberdade profissional, trabalhar em algo que impactará a vida de inúmeras pessoas ao redor do mundo, escrever código que atravessará gerações e colaborar com alguns dos desenvolvedores mais talentosos do planeta para resolver alguns dos problemas técnicos mais difíceis da nossa era, então você está no lugar certo.

Obtendo uma bolsa para trabalho open source em bitcoin em tempo integral  
O suporte financeiro para trabalho open source em bitcoin geralmente vem na forma de uma bolsa. As bolsas normalmente duram um ano e muitas são renovadas.  
O financiamento de bitcoin é diferente de outros projetos open source e de outras criptomoedas. Conseguir uma bolsa em bitcoin é bem direto. Você precisa de alguém que te recomende ou precisa fazer o trabalho – de preferência ambos.

Embora os programas de bolsas muitas vezes tenham inscrições abertas, o segredo para conseguir financiamento não é muito secreto. Comece fazendo o trabalho de graça. É assim que você constrói seu portfolio de contribuições. Isso estabelece você como um colaborador e prova sua motivação. Mostra que você é um bom investimento.

Os candidatos terão muito mais sucesso se fizerem o trabalho e depois se inscreverem. Para a maioria dos empregos, o candidato tenta convencer o empregador de que é capaz de fazer o trabalho. Mas o candidato não tem ideia de como é o trabalho ou o ambiente de verdade. No open source, não é necessário adivinhar. **Faça o trabalho. Demonstre a capacidade. Então peça apoio.**

Fazer o trabalho também significa demonstrar seu trabalho. Nem todo trabalho no open source é tão visível quanto escrever código. O trabalho menos visível não é menos valioso, mas é do seu interesse criar artefatos do seu esforço. A transparência é sua amiga. Se você aprender algo, é útil codificar isso escrevendo um post em um blog ou mantendo um registro contínuo.

Eu já vi algumas pessoas escreverem um e-mail resumindo seu progresso a cada duas semanas. Revisões de código costumavam ser difíceis de rastrear, mas agora o GitHub faz um trabalho melhor creditando um quadrado verde. Fazer longas caminhadas para refletir sobre como abordar um problema é necessário, mas escrever suas conclusões em um local público é um colateral valioso que pode servir para sempre como prova de seu progresso. (Trecho de [Um guia para buscadores de bolsas open-source de bitcoin](#))

### Organizações de Financiamento

[Spiral](#) é o braço de P&D de bitcoin da Block, que distribui bolsas desde 2019.

[Brink](#) é uma 501c3, focada principalmente em financiar desenvolvedores do Bitcoin Core, estabelecida em 2020.

[OpenSats](#) é uma 501c3, estabelecida em 2021.

A [Human Rights Foundation](#) é uma 501c3 que distribui bolsas desde 2020. Várias exchanges e indivíduos já patrocinaram desenvolvedores no passado, mas as organizações acima se tornaram as principais distribuidoras de bolsas nos últimos anos.

---

Iniciativas como a [Scalar School](#) recebem financiamento da Human Rights Foundation para criar comunidade de estudos em desenvolvimento open-source voltadas para mulheres e preparar as próximas gerações de bolsistas.

Veja neste repositório uma lista de projetos que oferecem oportunidades para desenvolvedores open source no ecossistema Bitcoin. <https://github.com/biohazel/freedom-devs>

**Mas antes, leia este [artigo da contribuidora do BDK](#), Daniela Brozzoni, dando dicas de como interagir e contribuir com o ambiente open source.**

## 11.3 Chaincode Labs

Chaincode Labs é uma organização de pesquisa e desenvolvimento dedicada ao avanço do Bitcoin e seu ecossistema de software. Fundada por membros respeitados da comunidade Bitcoin, Chaincode Labs se concentra em contribuir para o desenvolvimento do Bitcoin Core, bem como em educar e apoiar novos desenvolvedores na área. Os programas da Chaincode Labs também funcionam como on-ramps para outros projetos do ecossistema. Saiba mais em <https://bitcoindevs.xyz/>

### Programas de Treinamento da Chaincode Labs

Chaincode Labs oferece programas de treinamento para desenvolvedores que desejam se aprofundar no desenvolvimento do Bitcoin e contribuir para a rede. Esses programas são projetados para fornecer uma compreensão profunda dos conceitos técnicos subjacentes ao Bitcoin e para oferecer experiência prática no desenvolvimento do Bitcoin Core.

### Chaincode Residency Program

O Chaincode Residency Program é um dos programas de treinamento mais conhecidos oferecidos pela Chaincode Labs. Este programa é intensivo e geralmente dura várias semanas, durante as quais os participantes recebem orientação e suporte de desenvolvedores experientes do Bitcoin Core. Aqui estão alguns dos principais componentes do programa:

Os residentes participam de workshops e palestras que cobrem uma ampla gama de tópicos técnicos, desde a estrutura do Bitcoin Core até conceitos avançados de criptografia.

Os participantes trabalham em projetos práticos, contribuindo diretamente para o Bitcoin Core ou desenvolvendo ferramentas e melhorias relacionadas. Cada residente é emparelhado com um mentor experiente que oferece orientação e feedback contínuos ao longo do programa. O programa promove um ambiente colaborativo, onde os residentes podem trabalhar em conjunto, trocar ideias e resolver problemas técnicos.

### **Chaincode Labs Seminar Series**

Além do Residency Program, a Chaincode Labs também organiza uma série de seminários. Esses seminários são menos intensivos que o programa de residência, mas ainda oferecem uma oportunidade valiosa para desenvolvedores aprenderem sobre tópicos específicos relacionados ao Bitcoin e à criptografia.

Cada seminário foca em um tópico específico, como segurança da rede, design de sistemas descentralizados, ou protocolos de segunda camada. Os seminários geralmente incluem sessões interativas onde os participantes podem fazer perguntas e discutir ideias com especialistas da Chaincode Labs.

Muitos dos seminários são oferecidos online, permitindo a participação de desenvolvedores de todo o mundo. Participar dos programas de treinamento da Chaincode Labs oferece várias oportunidades para desenvolvedores:

Os programas fornecem uma formação técnica aprofundada e prática, ajudando os desenvolvedores a aprimorar suas habilidades e entender melhor o funcionamento do Bitcoin. Participantes têm a oportunidade de conhecer e colaborar com desenvolvedores experientes e outros participantes, construindo uma rede de contatos valiosa na comunidade de desenvolvimento do Bitcoin.

Através dos projetos práticos, os participantes podem fazer contribuições diretas para o ecossistema Bitcoin, ganhando experiência prática e reconhecimento na comunidade.

A experiência e as conexões feitas durante esses programas podem abrir portas para oportunidades de carreira em empresas de tecnologia financeira, startups de blockchain, e organizações de pesquisa.

A Chaincode Labs desempenha um papel crucial no avanço do desenvolvimento do Bitcoin e na formação de novos desenvolvedores na área. Seus programas de treinamento oferecem

uma oportunidade inestimável para desenvolvedores aprenderem com os melhores, contribuírem para o projeto Bitcoin e avançarem em suas carreiras.

## 11.4 Summer of Bitcoin

O Summer of Bitcoin é um programa global de estágio online realizado durante o verão no hemisfério norte. Este período corresponde aos meses de junho, julho e agosto, quando muitas universidades do hemisfério norte estão em recesso, permitindo que os estudantes participem do programa de estágio online de forma mais intensa e dedicada.

Focado em introduzir estudantes universitários ao desenvolvimento e design de código aberto do Bitcoin, este programa oferece uma oportunidade única para estudantes adquirirem experiência prática e conhecimento profundo sobre o funcionamento do Bitcoin, ao mesmo tempo em que contribuem para projetos significativos no ecossistema de código aberto.

O programa identifica e forma novos talentos no campo do desenvolvimento e design de Bitcoin, preparando os estudantes para futuras carreiras na indústria. Ao envolver estudantes em projetos de código aberto, o Summer of Bitcoin promove a inovação contínua no ecossistema do Bitcoin. As contribuições dos estudantes ajudam a resolver problemas reais e a melhorar a funcionalidade e a usabilidade do Bitcoin.

Estudantes que se destacam no programa têm a oportunidade de se conectar com líderes da indústria e potenciais empregadores. Recomendações e reconhecimentos obtidos durante o programa podem abrir portas para carreiras no setor. Participar do programa permite que os estudantes desenvolvam habilidades técnicas avançadas em programação, design e segurança, bem como habilidades de colaboração e comunicação, que são essenciais no ambiente de desenvolvimento de código aberto.

### **Funcionamento do Summer of Bitcoin**

Estudantes universitários interessados se inscrevem no programa através de um processo de aplicação online, onde devem demonstrar suas experiências anteriores e seu interesse no Bitcoin.

As inscrições passam por uma triagem rigorosa para selecionar os candidatos mais promissores com base em suas habilidades, motivação e potencial de contribuição para projetos de código aberto.

Os estudantes selecionados aprendem como o Bitcoin funciona através de um conjunto de recursos cuidadosamente selecionados e de alto rigor técnico.

Após o treinamento inicial, os estudantes submetem propostas de projeto, detalhando como planejam contribuir para um projeto específico de código aberto relacionado ao Bitcoin.

Estudantes que escolhem a trilha de desenvolvedor trabalham em tarefas de programação e desenvolvimento de software, contribuindo diretamente para a base de código dos projetos de Bitcoin.

Estudantes que escolhem a trilha de designer focam em criar experiências de usuário intuitivas e atraentes para produtos e serviços de Bitcoin de código aberto.

Os estudantes recebem mentoria de desenvolvedores e designers experientes no ecossistema Bitcoin. Mentores fornecem orientação técnica, feedback sobre o progresso do projeto e suporte contínuo durante todo o programa.

No final do programa, os projetos dos estudantes são avaliados com base na qualidade, impacto e contribuição para a comunidade de código aberto do Bitcoin. Estudantes que se destacam recebem recomendações e reconhecimentos, aumentando sua visibilidade na comunidade de desenvolvedores e designers de Bitcoin e abrindo oportunidades de carreira no setor.

O Summer of Bitcoin é uma excelente plataforma para estudantes universitários que desejam se envolver no desenvolvimento de código aberto e fazer contribuições significativas para o ecossistema do Bitcoin, enquanto desenvolvem habilidades valiosas e constroem uma rede de contatos profissionais.

Existe uma [remuneração](#) pela participação no programa.

## 11.5 Scalar School

Scalar School é uma escola de treinamento para futuros desenvolvedores de Bitcoin no Brasil, financiada pela Human Rights Foundation.

As mulheres estão sendo sistematicamente negadas a oportunidades de se desenvolverem plenamente como desenvolvedoras no ecossistema do Bitcoin. O ecossistema open source, especialmente no desenvolvimento de Bitcoin, tem se mostrado um ambiente hostil para as mulheres. Assédios, microagressões e exclusão são problemas recorrentes que dificultam a participação e o progresso das mulheres nessa área. A falta de um ambiente seguro e acolhedor impede que muitas mulheres aproveitem as oportunidades de aprendizado e crescimento técnico.

Microagressões verbais, tratamento diferencial, ostracismo social, e passivo-agressividade atrapalham o processo de aprendizado das mulheres, além de danificar sua saúde mental e performance intelectual. Queremos evitar esses obstáculos intelectuais e oferecer uma comunidade onde as mulheres se sintam seguras e apoiadas para estudar e explorar a tecnologia Bitcoin sem ocorrências hostis.

Para combater essa hostilidade, decidimos transformar a Scalar School em um programa exclusivamente para mulheres. Queremos criar um espaço seguro e de apoio onde as mulheres possam se concentrar em estudar tópicos técnicos complexos sem interrupções e sem ninguém questionando o potencial intelectual delas.

Esses espaços seguros são essenciais para proteger o bem-estar mental das mulheres e sua capacidade de aprender e crescer. Embora a presença de homens tecnicamente qualificados possa ser benéfica, o maior problema é que as mulheres, no momento de encontrar uma comunidade de estudos e pertencer a ela plenamente, estão sendo privadas de oportunidades de aprendizado devido ao assédio, à diminuição de seus esforços, e à exclusão. Isso é um problema sério que deve ser abordado por toda a comunidade Bitcoin, nacional e internacionalmente.

**Inicialmente, tínhamos considerado educar e controlar a comunidade aberta com códigos de conduta rigorosos.** No entanto, percebemos que um programa aberto levaria a ocorrências frequentes. Atualmente, grande parte da comunidade aberta de desenvolvedores Bitcoin no Brasil é, essencialmente, um grupo de ódio organizado contra mulheres. Para saber mais, visite: [biohazel.github.io](https://biohazel.github.io) e leia <https://bitfeminist.substack.com/p/empoderando-a-misoginia-extrema-atraves>.

Pensamos nos ambientes exclusivos para mulheres pela lógica de um avião que está caindo. Nossa sociedade está colapsando, e temos a obrigação de colocar a máscara de oxigênio em nós primeiro. Estamos cientes de que é ingênuo acreditar que podemos mudar toda uma estrutura social da noite para o dia. Para isso, precisamos primeiro nos fortalecer como minoria, criando um espaço exclusivamente para mulheres. Inspiramo-nos no sucesso do projeto [Bitcoin Dada](#) em trazer mulheres para o Bitcoin e esperamos replicar esse sucesso no contexto brasileiro.

Nosso currículo é baseado nos melhores programas técnicos do mundo, como Base58, Chaincode Labs, Bitshala, "Aprendendo Bitcoin pela Linha de Comando", e os livros técnicos canônicos da área. Além disso, promovemosativamente o crescimento e fortalecimento da comunidade, e esperamos em breve retomar o Bitdevs Ribeirão Preto com uma versão para mulheres.

A Scalar School desempenha um papel vital no ecossistema open source, criando uma comunidade de construtoras e oferecendo treinamento para desenvolvedoras iniciantes que serão as futuras líderes em programas de fomento em pesquisa e desenvolvimento do Bitcoin FOSS.

Nosso sonho é nos tornar uma referência global, um grupo de pesquisa e desenvolvimento independente e focado nos valores de inclusão, liberdade, e superação de barreiras artificiais impostas pela sociedade. Queremos vivenciar a democratização da ciência e do conhecimento no ecossistema Bitcoin.

As mulheres são um grupo historicamente marginalizado em áreas de altos salários como a tecnologia. Nossa escola é o primeiro projeto para devs open source Bitcoin liderado por uma mulher no Brasil, tornando a Scalar School uma iniciativa histórica no cenário tecnológico nacional.

Estamos orgulhosas de anunciar que temos suporte e financiamento da Human Rights Foundation (HRF) para construir nossa comunidade. Este apoio nos permite oferecer treinamento de alta qualidade e criar um ambiente seguro para todas.

Para as mulheres desenvolvedoras, ou que almejam sê-lo, convidamos você a fazer parte dessa jornada transformadora preenchendo nosso [formulário de interesse](#) para a primeira trilha Full-Stack Bitcoin: Da Mineração à Lightning.

Se você é um desenvolvedor bem-intencionado e experiente no ecossistema Bitcoin—de qualquer gênero— e gostaria de voluntariar como professor nesse programa somente para mulheres, por favor entre em contato via scalarbitcoin@gmail.com

## 12. Bitcoin é Para Todos

O Bitcoin, como tecnologia open source, representa muito mais do que uma revolução financeira; é um símbolo de inclusão, transparência e inovação. Desde o seu lançamento em 2009 por Satoshi Nakamoto, o Bitcoin tem promovido uma nova era de liberdade financeira e acesso democrático ao conhecimento técnico.

A natureza do código aberto do Bitcoin permite que qualquer pessoa, em qualquer lugar, participe do desenvolvimento e aprimoramento desta tecnologia. Isso cria um ambiente onde a colaboração é incentivada e a inovação é constante.

Para muitos, o desenvolvimento open source em Bitcoin não é apenas uma oportunidade de carreira, mas uma missão. É uma forma de trabalhar em algo significativo, com impacto global e duradouro.

No entanto, é crucial reconhecer e enfrentar os desafios sociais que acompanham essa liberdade. Infelizmente, a **misoginia** ainda é prevalente em muitas comunidades técnicas, especialmente na do Bitcoin.

Mulheres e minorias frequentemente enfrentam preconceitos e barreiras significativas, desde microagressões até assédio explícito, o que limita sua participação e contribuições. Nossa comunidade e escola surge como uma estratégia para aumentar a voz das mulheres no ecossistema.

**Na Scalar School of Bitcoin Developers, acreditamos que o Bitcoin deve ser para todos. Mas, principalmente, acreditamos que é uma ferramenta poderosa para diminuir a**

**desigualdade social, de oportunidades, de salários e de independência financeira entre homens e mulheres. Também acreditamos que comunidades com balanço de gênero—perto de uma distribuição de 50-50—são mais justas, saudáveis e criativas.**

Portanto, nosso compromisso inicial é criar um ambiente seguro, inclusivo e respeitoso para mulheres. Lutar contra a misoginia social pode parecer uma tarefa impossível, porém, temos o sonho de um dia podermos abrir nossa comunidade para todos os gêneros no futuro.

Acreditamos que, ao promover uma cultura de respeito e inclusão, podemos não apenas melhorar a tecnologia do Bitcoin, mas também criar uma sociedade mais justa e equitativa.

Ademais, nós também queremos experienciar a liberdade. Nós também queremos anunciar eventos públicos em locais que não exigem KYC e saber que estamos seguras, que não seremos perseguidas e assediadas. Queremos conhecer a liberdade, não apenas ouvir histórias sobre ela.

Acreditamos que é muito importante que os homens desenvolvedores do ecossistema criem consciência das implicações desta guerra contra as mulheres nos espaços de oportunidades técnicas e criem iniciativas paralelas para que, no futuro, consigamos juntar os gêneros de maneira saudável e respeitosa, colocando a comunidade de desenvolvedores open source Bitcoin no eixo 50-50. Só então saberemos o verdadeiro potencial de transformação social do Bitcoin.

Juntos, podemos construir um futuro onde o conhecimento e o Bitcoin sejam de fato para qualquer um, e onde essa forma de financiamento traga prosperidade para iniciativas que realmente gerem valor para a humanidade.

## 13. Powered By Bitcoin

Até hoje, valeu tudo para que fosse construída qualquer coisa desde que envolvesse a infraestrutura do Bitcoin, inclusive a normalização e a propagação da misoginia extrema. Como disse o rapper Projota.

*"As obras serão construídas. Aprendi com meu pai que é pedreiro."*

Para o bem ou para o mal, o Bitcoin será construído. No cenário atual, precisamos lidar com um débito social persistente deixado pelas comunidades de desenvolvedores mais antigos do ecossistema, que infelizmente ainda atuam até hoje. Felizmente, a situação está começando a mudar, permitindo-nos interagir com o ecossistema de desenvolvimento sem a necessidade de passar por eles. Além disso, alguns dos desenvolvedores mais antigos são pessoas respeitosas e bem-intencionadas. Só precisamos encontrá-los.

Pois bem. Temos nossos problemas expostos, e temos o Bitcoin como ferramenta poderosa de liberdade financeira e construção de uma nova sociedade. Há pessoas que vão se interessar em desenvolvimento de código, mas paralelamente, alguns vão desejar construir um mundo melhor e vão buscar formas criativas de fazê-lo.

E agora, o que vamos construir com todo esse conhecimento, poder de compra e liberdade financeira que o Bitcoin nos trás?

Eu vou dar uma sugestão, mas também sugiro que você quebre a cabeça e sugira muito mais—desde que não seja construir algo que favoreça um mundo retrógrado, anti-feminista, misógino e red pill, por favor. Sem mais dos mesmos erros de sempre da humanidade.

**Precisamos de mais feminismo e defesa dos direitos das mulheres e crianças, não menos.**

Sabia que o mercado global de produtos para bebês foi estimado em aproximadamente USD 320,65 bilhões em 2023 e espera-se que cresça a uma taxa de crescimento anual composta (CAGR) de 5,9% de 2024 a 2030? Os principais segmentos de produtos incluem alimentos para bebês, cosméticos e produtos de higiene para bebês, produtos de segurança e conveniência para bebês, e roupas e acessórios para bebês.

No meio desses produtos estão uma miríade de parafernálias que os bebês não precisam, mas que são vendidos para famílias inocentes que obtém seus conhecimentos sobre as melhores formas de criar bebês de influencers do instagram que estão exatamente vendendo produtos. Nada pode ser mais padrão fiat que isso.

Bebês não tem poder de compra, mas são cooptados para convencer seus pais a gastarem. Sendo que um entendimento de seu funcionamento biológico deixa claro que os investimentos em "coisas para seu desenvolvimento" são basicamente desnecessários.

Porém, é preciso educar famílias sobre como funciona um bebê. Biologicamente e em termos comportamentais, e quais as melhores formas de lidar e interagir com eles. Isso, claro, não rende lucros. Leva tempo, pais interessados, e cuidadores que são treinadores atenciosos para demonstrar e explicar o porquê das interações e intervenções, bem como o por quê das preparações dos ambientes de formas específicas—com menos, não mais.

A realidade é semelhante à de web3 e memecoins distraindo as pessoas do Bitcoin. O verdadeiro tratamento padrão Bitcoin que os bebês merecem está longe de ser alcançado, porque o sistema fiduciário é manipulável para construir coisas que não precisamos. Mas e se o Bitcoin resolver isso?

Emmi Pikler foi uma pediatra húngara cujas observações e práticas revolucionaram o cuidado infantil. Trabalhando em um orfanato em Budapeste, Pikler desenvolveu métodos que enfatizavam a autonomia e a liberdade de movimento das crianças. Sua abordagem visava

respeitar o ritmo natural de desenvolvimento de cada criança, promovendo um crescimento saudável tanto físico quanto emocional.

Nos orfanatos tradicionais, as crianças frequentemente sofriam de falta de estímulo, pouca interação e cuidados padronizados, resultando em problemas de desenvolvimento físico e emocional, e dificuldade de se encaixarem na sociedade na vida pós orfanato.

Pikler observou que esses métodos falhavam em proporcionar um ambiente que suportasse o desenvolvimento saudável das crianças. Ela se propôs a criar um sistema de cuidado que atendesse às necessidades individuais das crianças e promovesse sua saúde mental. Imagine um mundo em que mesmo crianças muito pobres são perfeitamente bem ajustadas e aproveitadas do máximo de seu material neurológico.

Pikler desenvolveu uma rotina e práticas específicas que promoviam a independência e o desenvolvimento natural das crianças, bem como a comunicação respeitosa entre cuidador e criança, com limites bem delimitados desde bem pequenas.

**Liberdade de Movimento:** As crianças eram colocadas no chão em uma posição de costas e incentivadas a se mover livremente. Isso permitia que desenvolvessem habilidades motoras de forma natural, sem intervenção direta dos cuidadores, e no tempo delas.

**Intervenção Mínima:** Cuidadores evitavam manipular ou forçar posições nas crianças, como sentá-las ou colocá-las de bruços antes que estivessem prontas para esses movimentos por conta própria.

**Ambiente Seguro e Estimulante:** Pikler introduziu móveis baixos e estruturas como o Triângulo de Pikler, que incentivavam a exploração segura e o desenvolvimento físico.

**Observação Atenta:** Cuidadores observavam cuidadosamente cada criança para entender suas necessidades e responder de maneira adequada, sem superestimulação ou subestimação.

**Respeito pelo Tempo da Criança:** Cada criança tinha seu próprio ritmo de desenvolvimento respeitado, promovendo confiança e segurança emocional.

As crianças cuidadas segundo os métodos de Pikler saíam do orfanato com posturas espinais impecáveis, habilidades motoras bem desenvolvidas e um forte senso de autonomia. Elas demonstravam maior resiliência, confiança e capacidade de interação social saudável.

O sucesso das crianças no orfanato de Pikler evidenciou que um cuidado respeitoso e baseado na autonomia e no conhecimento da biologia humana podia resultar em adultos bem ajustados e saudáveis, mesmo em condições precárias como em orfanatos de guerra. Magda Gerber foi sua aluna e trouxe esse conhecimento para os Estados Unidos, sendo bem conhecida entre as

famílias de alta renda da Califórnia. As babás com formações no método Pikler são as mais bem pagas do Vale do Silício, e eu já fui uma delas.

Mas essa ideia não movimenta a indústria de produtos para bebês, tampouco viraliza para as massas pelo mesmo motivo. Só um novo sistema econômico e de valores poderia fazer com que esses valores básicos se tornassem a norma. **Temos confiança que o padrão Bitcoin vai ajustar, também, nossa percepção de valores sobre desenvolvimento humano, e não apenas de código.**

Porém, antes de tudo, precisamos focar no desenvolvimento do Bitcoin como software e na implementação do Bitcoin em si. Por meio do Bitcoin, temos a chance de construir um futuro melhor, onde a liberdade financeira, a liberdade real e a ética caminham juntas, criando um impacto positivo duradouro para a humanidade.

Estude Bitcoin, construa o Bitcoin, viva o Bitcoin. Mas saiba que a vida humana vai para além do Bitcoin, e que o que fazemos e construímos com Bitcoin também importa.

## 14. Notas Finais

### 14.1 Isenção de Responsabilidade

A SCALAR SCHOOL NÃO FORNECE CONSULTORIA DE INVESTIMENTOS. SOMOS UM GRUPO DE EDUCAÇÃO, PESQUISA E DESENVOLVIMENTO DE TECNOLOGIA BITCOIN.

As informações contidas neste livro são fornecidas apenas para fins educacionais e informativos. Embora a autora tenha feito esforços para garantir a precisão das informações apresentadas, não há garantias, explícitas ou implícitas, sobre a exatidão, completude ou adequação das mesmas.

Investir e transacionar em Bitcoin envolve riscos significativos. Antes de tomar qualquer decisão financeira, os leitores são incentivados a realizar sua própria pesquisa e, se necessário, consultar um profissional financeiro qualificado.

A autora não será responsável por qualquer perda ou dano, incluindo, sem limitação, perdas ou danos indiretos ou consequentes, ou qualquer perda ou dano decorrente da perda de dados ou lucros, resultantes do uso ou dependência das informações contidas neste livro.

## 14.2 Contato

Dúvidas, sugestões e correções podem ser enviadas para scalarbitcoin@gmail.com, aos cuidados de Luciana. Ou via issue no repositório:

<https://github.com/biohazel/scalar-school-handbook>

Nostr: npub1jfk9mxsndnwupaergsyat0myst8pygpz2pyx032dz62pefmz22esrcjf2t

Instagram: @scalar.school

X: @scalarschool

## 14.3 Posfácio

Um mundo melhor é possível. Absolutamente tudo é inventado na nossa sociedade, o que significa que como humanidade temos o potencial orquestrar uma ação conjunta e construir um mundo melhor em 24 horas.

Nunca deixe de sonhar, nem de se divertir estudando, codificando, e trabalhando com Bitcoin. Que o universo lhe dê sabedoria e prosperidade por meio do conhecimento. Bons estudos.