

Bitcoin

Leonardo Araújo

UFSJ

Bitcoin: A Interseção entre Tecnologia e Economia

Explorando suas Inovações e Impactos

Introdução

- **Criptografia, Internet e Dinheiro Digital**
- Propriedades desejadas de uma moeda digital:
 - Distribuído, sem autoridade central
 - Prevenir duplo gasto
 - Anonimato
 - Pagamentos offline

O que é Dinheiro? (Perspectiva de Rothbard)

- Definição: Dinheiro é um meio de troca amplamente aceito em uma sociedade para bens, serviços e pagamento de dívidas.
- Visão de Murray Rothbard:
 - O dinheiro surge espontaneamente por processos de mercado, não por decreto estatal.
 - Resolve o problema da “coincidência dupla de desejos” no sistema de troca direta.
- Funções Principais:
 - Meio de troca
 - Reserva de valor
 - Unidade de conta
- Por que Importa: Compreender as origens do dinheiro ajuda a explicar o papel do Bitcoin como moeda descentralizada.

Exemplos Históricos de Dinheiro

■ Conchas:

- Usadas por tribos nativas americanas (ex.: contas wampum).
- Valorizadas por raridade, portabilidade e significado cultural.
- Exemplo: Wampum usado no comércio na América do Norte.

■ Sal:

- Valorizado em sociedades antigas (ex.: soldados romanos pagos com sal, origem de “salário”).
- Durável, divisível e essencial para preservação.
- Exemplo: Sal como moeda em rotas comerciais africanas.

■ Ouro:

- Dinheiro universal por séculos devido à escassez, durabilidade e divisibilidade.
- O valor do ouro vem da escolha do mercado.
- Exemplo: Moedas de ouro na Europa medieval e América do século XIX.

Do Dinheiro-Commodity aos Bancos

- Dinheiro-Commodity:
 - Bens físicos (ex.: ouro, prata) usados como dinheiro.
 - Rothbard: O mercado seleciona commodities por sua utilidade e escassez.
- Surgimento dos Bancos:
 - Ourives guardavam ouro e emitiam recibos de depósito (primeiras notas bancárias).
 - Recibos tornaram-se substitutos confiáveis para o ouro físico.
- Certificados de Depósito:
 - Reivindicações em papel para ouro armazenado em cofres.
 - Exemplo: Notas de ourives de Londres no século XVII, resgatáveis sob demanda.
- Problema: Certificados permitiram que bancos influenciassem a oferta monetária.

Sistema de Reservas Fracionárias

- O que é:
 - Bancos emitem mais certificados de depósito do que o ouro em reserva.
 - Exemplo: Banco possui 100 onças de ouro, mas emite recibos para 1.000 onças.
 - Reservas fracionárias criam “dinheiro do nada”, inflando a oferta monetária.
 - Viola direitos de propriedade, pois nem todos os depositantes podem resgatar ouro simultaneamente.
- Consequências:
 - Ciclos de expansão e colapso (ex.: pânico bancários do século XIX).
 - Erosão do poder de compra do dinheiro.
- Conexão com Bitcoin: Oferta fixa (21M moedas) impede manipulação por reservas fracionárias.

Emissão de Dinheiro e Bancos Centrais

- Emissão de Dinheiro:
 - Criação de novo dinheiro, historicamente ligado a depósitos de ouro, agora fiat (fiduciário) por bancos centrais.
 - Bancos centrais (ex.: Federal Reserve) monopolizam a emissão, causando inflação.
- **Exemplo de Banco Central:**
 - Federal Reserve imprime dólares, não lastreados por ouro desde 1971 (fim de Bretton Woods).
 - 2020–2022: Oferta monetária M2 cresceu, alimentando inflação.
 - De acordo com dados do Federal Reserve, a oferta monetária M2 nos EUA cresceu aproximadamente 40% entre fevereiro de 2020 e fevereiro de 2022 (de ~\$15,5 trilhões para ~\$21,8 trilhões).
 - Essa foi uma taxa de expansão sem precedentes em comparação com tendências históricas, nas quais o M2 geralmente cresce de 5 a 7% ao ano.
- Solução de Rothbard:
 - Bancos livres e retorno ao padrão-ouro para limitar criação arbitrária de dinheiro.
- Papel do Bitcoin: Emissão descentralizada (mineração) com oferta limitada contraria inflação fiat

Entendendo a Oferta Monetária M2

- O que é M2?:
 - Medida da oferta monetária incluindo dinheiro, contas correntes, poupança e fundos de mercado monetário.
 - Exemplo: M2 dos EUA foi ~\$21 trilhões em 2023.
- Visão de Rothbard:
 - Crescimento do M2 reflete políticas inflacionárias de bancos centrais e reservas fracionárias.
 - Dilui o poder de compra, prejudicando poupadores.
- Impacto:
 - 1971–2025: Dólar americano perdeu ~85% de seu valor devido à expansão do M2.
- Alternativa Bitcoin: Cronograma de emissão previsível, imune à manipulação de bancos centrais.

Lições de Rothbard para o Bitcoin

- Dinheiro deve ser guiado pelo mercado, não pelo Estado (conchas, ouro → Bitcoin).
- Reservas fracionárias e emissão fiat causam instabilidade; a oferta fixa do Bitcoin evita isso.
- Inflação do M2 erode riqueza; Bitcoin oferece proteção.
- Bitcoin:
 - Descentralizado, como dinheiro-commodity histórico.
 - Resiste à inflação, ao contrário da expansão do M2 fiat.
 - Sem reservas fracionárias no protocolo do Bitcoin.

“O sistema bitcoin, diferente de bancos tradicionais e sistemas de pagamento, baseia-se na confiança descentralizada. Em vez de uma autoridade central confiável, no bitcoin, a confiança é alcançada como uma propriedade emergente das interações dos diferentes participantes no sistema bitcoin.” (Mastering Bitcoin, de Andreas M. Antonopoulos e David A. Harding)

Uma Proposta Revolucionária

- **Origem do Bitcoin**

- Introduzido em 2008 por Satoshi Nakamoto
 - Documento: *Bitcoin: A Peer-to-Peer Electronic Cash System*
- Satoshi Nakamoto retirou-se em 2011.

Base Tecnológica

- Sistema descentralizado (peer-to-peer).
- Livro público: *Blockchain*.
 - Cada nó possui uma cópia.
- Transparência: Todas as contas e transações são públicas.
- Integridade por meio de funções de hash criptográficas.

Visão Geral da Blockchain

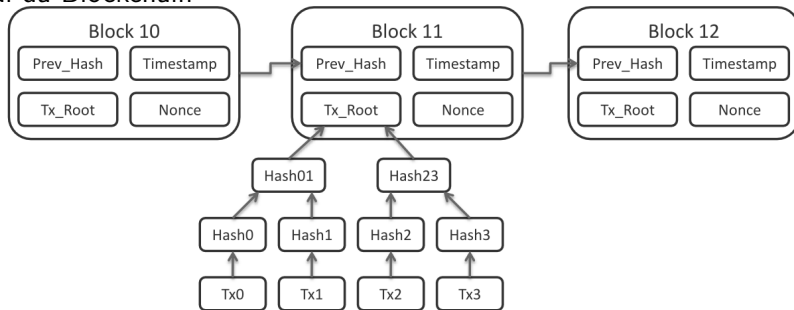


Figure 1: Dados de um Bloco do Bitcoin (wikimedia)

Cada bloco usa uma estrutura de árvore de Merkle. Uma árvore de hash permite uma verificação eficiente e segura do conteúdo de uma estrutura de dados grande.

Visão Geral da Blockchain

■ Blocos e Transações

- Tamanho dos blocos: 1 MB (4 MB desde 2017).
- Tempo para adicionar um bloco: ~10 minutos.
- Provisão máxima: 21 milhões de bitcoins.
- Halving: A recompensa de mineração cai pela metade a cada 4 years.
 - 2009 (50), 2012 (25), 2016 (12.5), 2020 (6.25), 2024 (3.125), ...

Mineração e Prova de Trabalho (PoW)

- **Prova de Trabalho (Proof-of-Work)**

- Resolve quebra-cabeças de hash criptográfico.
- Recompensas por encontrar um hash válido abaixo de um alvo.

- **Pools de Mineração**

- Colaboração para aumentar as chances de recompensas.

Hash Puzzle: O Núcleo da Mineração

- **Objetivo:** Encontrar um *nonce* que produza um hash que atenda a um alvo específico.
- **Função Hash:**
 - Entrada: Dados do bloco (transações + nonce).
 - Saída: Hash criptográfico.
- **Condição Alvo:** O hash deve ter um certo número de zeros à esquerda.

Processo

- 1 O minerador seleciona um valor de nonce.
- 2 Calcula o hash do bloco.
- 3 Compara o hash com o alvo:
 - Se válido, o bloco é adicionado à blockchain.
 - Caso contrário, o minerador incrementa o nonce e tenta novamente.

Ajuste de Dificuldade

- A dificuldade é ajustada a cada **2.016 blocos** (~2 semanas).
- Objetivo: Manter uma média de **1 bloco a cada 10 minutos**.
- Maior poder de hash na rede → Aumento da dificuldade.
- Menor poder de hash na rede → Redução da dificuldade.

Exemplo

- Alvo: 000000... (zeros à esquerda).
- Hash calculado: 000000a1b2c3... (válido).

Por que Zeros à esquerda?

- Reflete dificuldade: Mais zeros à esquerda exigem mais esforço computacional.

Consenso e Resiliência

■ Problema dos Generais Bizantinos

- Desafio: Como partes independentes (que não podem confiar umas nas outras) podem concordar sobre um estado compartilhado sem depender de uma terceira parte confiável?
- Abordagem do Bitcoin: Prova de Trabalho (PoW) serve como uma solução prática.

Como Funciona

- Os nós do Bitcoin sempre selecionam a blockchain com o **maior trabalho cumulativo** (ou seja, a cadeia válida mais longa).
- A **blockchain mais pesada** é considerada válida, resolvendo conflitos e prevenindo duplo gasto.

Principais recursos

- **Incentivos para jogar limpo:** Jogadores malcomportados incorrem em custos (computação desperdiçada) sem recompensas.
- **Importância de executar seu próprio nó:**
 - Garante validação pessoal de transações e privacidade.
 - Evita dependência de terceiros para dados de blockchain.

Aprenda mais sobre o problema dos Generais Bizantinos

Hashcash: A Base da Prova de Trabalho

- O mecanismo de Prova de Trabalho (PoW) do Bitcoin é inspirado no Hashcash.
- **Hashcash foi introduzido em 1997 por Adam Back**
 - Um sistema de prova de trabalho projetado para combater **spam de e-mail** e **ataques de negação de serviço (DoS)**.

Como Funciona

- O remetente deve calcular um hash com um número específico de zeros à esquerda.
- Esse cálculo requer esforço, mas a verificação pelo destinatário é rápida.
- Caso de uso: Adicionar um pequeno custo computacional para cada e-mail desestimula o envio de spam.

Criptografia no Bitcoin

- **Público, mas Seguro:**

- As transações são visíveis publicamente, mas protegidas por mecanismos criptográficos.

Assinaturas Digitais

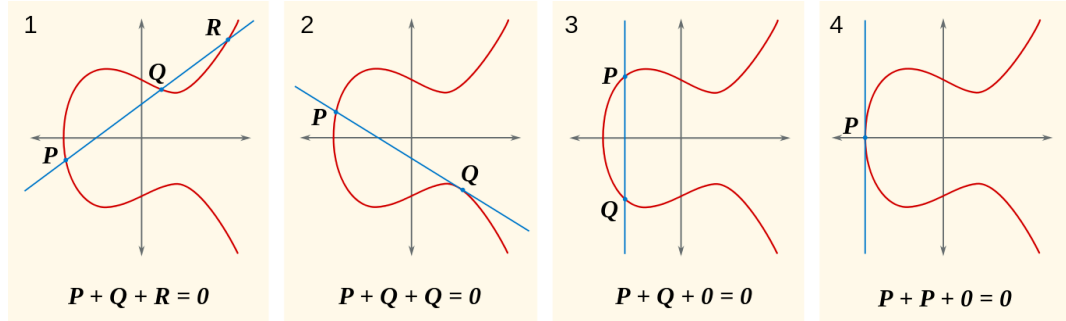
- **Prova de Propriedade:**

- As chaves privadas são usadas para assinar transações.
- As chaves públicas validam essas assinaturas.

- **Criptografia de Curvas Elípticas (ECC):**

- O Bitcoin usa a curva elíptica secp256k1 para gerar pares de chaves.
- Benefícios: Alta segurança com tamanhos de chave menores.

Aritmética da Curva Elíptica



Fonte: <https://bitcoin.stackexchange.com>

- Um (relativamente fácil de entender) manual sobre criptografia de curva elíptica
- Criptografia de curva elíptica para aqueles que têm medo de matemática

Endereços Bitcoin

- Derivados de chaves públicas usando:
 - SHA256 → RIPEMD160 → Endereço.
 - Resistência à Colisão Aumentada usando duas funções hash diferentes.
 - Atraso na Exposição da Chave Pública: Endereços Bitcoin são derivados de chaves públicas com hash, então a chave pública em si não é visível no blockchain até que os fundos sejam gastos do endereço.
- Codificado em Base58Check para legibilidade.
 - Soma de verificação: Quatro bytes adicionais.

Chaves e Endereços do Bitcoin

Estrutura

- 1 **Dados Brutos:** Chave criptográfica ou hash.
- 2 **Prefixo:** Identifica o tipo de dado.
- 3 **Soma de verificação:** Detecta erros na entrada de dados.

Exemplos

Endereço Bitcoin (Legado)

- **Derivado de:** Chave pública.
- **Prefixo:** 0x00 (mainnet).
- **Exemplo:** 1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs.

Endereço SegWit (Bech32)

- **Derivado de:** Hash de chave pública.
- **Prefixo:** bc1 (formato Bech32 da mainnet).
- **Exemplo:** bc1qw508d6qe...skjc.

Chave privada (formato WIF)

- **Dados brutos:** Chave privada.
- **Prefixo:** 0x80 (mainnet).
- **Exemplo:** 5J76fRXQYWkPtMoWx2DvX1ZWyaXHZA v9UvUjwsCbnHL2GuThU6q.

Codificação

- Todas as chaves e endereços são codificados usando métodos apropriados:
- **Base58Check**: Para endereços legados e chaves privadas.
- **Bech32**: Para endereços SegWit.

Tabela de resumo de prefixos

Tipo de dados	Prefixo	Exemplo
Endereço legado	0x00	1PMycacnJa...UAs
Endereço SegWit	bc1	bc1qw508d6q...
Endereço Testnet	0x6F	mhPo5P2RVu5...rEo
Chave privada (WIF)	0x80	5J76fRXQYWk...U6q

Base58Check

- Conjunto de caracteres: 1 2 3 4 5 6 7 8 9 A B C D E F G H J K L M N P Q R S T U V W X Y Z a b c d e f g h i j k m n o p q r s t u v w x y z.
 - a-z, A-Z, e 0-9, com os caracteres visualmente ambíguos removidos (0, O, l, I).

exemplo

- 3 bytes: 0xFFFFFFFF
- Base 58: 2UzHL
- Passos:
 - $0xFFFFFFFF = 16777215$
 - $16777215 \bmod 58 = 19 = L$
 - $289262 \bmod 58 = 16 = H$
 - $4987 \bmod 58 = 57 = z$
 - $85 \bmod 58 = 27 = U$
 - $1 \bmod 58 = 1 = 2$

Bech32

- Conjunto de caracteres: q p z r y 9 x 8 g f 2 t v d w 0 s 3 j n 5 4 k h c e 6 m u a 7 l.
 - a-z e 0-9, sem os seguintes caracteres: 1, b, i e o (b, i e o podem ser facilmente confundidos com 8, 1 e 0, especialmente em caligrafia ou certas fontes).
 - Caracteres comumente confundidos (por exemplo, 5 vs S, 2 vs Z, p vs q vs g, etc.) são sempre um bit diferentes.
 - Códigos BCH, GF(32), polinômio $g(x) = x^6 + 29x^5 + 22x^4 + 20x^3 + 21x^2 + 29x + 18$.
 - Detecção de erro de 4 erros em até 89 caracteres.

Palestra - Pieter Wuille: New Address Type for SegWit Addresses
(Some of) the math behind Bech32 addresses

Funções criptográficas em Bitcoin

Funções hash

- **Funções principais:**

- Derivação de endereço.
- Proteger cabeçalhos de bloco e dados.
- Garantir a imutabilidade do blockchain.
- Criar identidades únicas e quebra-cabeças criptográficos.

Assinaturas Digitais

- **Propósito:**

- Provar a propriedade de ativos digitais.
- Validar e assinar transações.

- **Como Funciona:**

- A propriedade está vinculada a chaves privadas e públicas.
- Uma assinatura válida é necessária para que uma transação seja incluída no blockchain.

Impactos Econômicos e Sociais

■ Aspectos Econômicos

- Fornecimento limitado garante tendências deflacionárias.
- Descentralização desafia sistemas financeiros tradicionais.

■ Aspectos Sociais

- Promove inclusão financeira.
- Levanta preocupações sobre atividades ilegais e uso de energia.

Desafios e Limitações

- Alto consumo de energia (PoW).
- Problemas de escalabilidade.
- Incertezas regulatórias.

Forks no Bitcoin: Evolução por Consenso

- Um **fork** ocorre quando o blockchain diverge em dois caminhos, normalmente devido a mudanças nas regras do protocolo.

Tipos de Forks

1. **Soft Fork**

- **Compatibilidade com versões anteriores:**
 - Nós antigos (seguindo regras anteriores) ainda podem reconhecer novos blocos como válidos.
- **Resultado:**
 - Se a maioria dos mineradores adotar as novas regras, o soft fork se torna a cadeia dominante.
 - Se não, as novas regras falham.

Exemplo:

- Segregated Witness (SegWit) em 2017, que melhorou a eficiência do espaço do bloco.

2. Hard Fork

- **Não compatível com versões anteriores:**

- Nós antigos rejeitam blocos criados sob as novas regras.

- **Resultado:**

- Uma divisão permanente em duas cadeias separadas se o consenso não for alcançado.

Exemplo:

- Bitcoin Cash (2017) se separou do Bitcoin para permitir tamanhos de bloco maiores.

Importância dos Forks

- Permitir inovação e atualizações de protocolo.
- Risco de fragmentação e perda de consenso se mal coordenado.

Propostas de Melhoria do Bitcoin (BIPs)

■ O que são BIPs?

- Propostas de Melhoria do Bitcoin são documentos de design que propõem novos recursos, processos ou mudanças no Bitcoin.
- Visam padronizar o desenvolvimento e garantir transparência no processo de tomada de decisão.

Tipos de BIPs

- 1 **Standards Track:** Propostas que afetam o protocolo do Bitcoin, validação de bloco ou formatos de carteira.
- 2 **Informativo:** Diretrizes ou explicações gerais sem adoção obrigatória.
- 3 **Processo:** Propostas relacionadas a processos como fluxos de trabalho BIP.

Exemplos de BIPs notáveis

- **BIP 16:** Pay-to-Script-Hash (P2SH) – Introduziu scripts flexíveis para transações.
- **BIP 39:** Frases de Semente Mnemônicas – Padrão para gerar frases de recuperação de carteira legíveis por humanos.
- **BIP 141:** Segregated Witness (SegWit) – Capacidade de bloco melhorada e maleabilidade de transação resolvida.
- **BIP 32:** Hierarchical Deterministic (HD) Wallets – Geração de semente única habilitada para múltiplas chaves.

Importância

- Garante que o desenvolvimento do Bitcoin permaneça aberto e orientado pela comunidade.
- Fornece uma abordagem estruturada para atualizar a rede.

Bitcoin e Altcoins

■ **Criptomoedas alternativas**

- Diferentes políticas monetárias e mecanismos de consenso.
- Exemplos:
 - Litecoin (Scrypt PoW).
 - Ethereum (Contratos inteligentes, Turing-complete).

Perspectivas futuras

- Avanços em tecnologias de blockchain.
- Mudança para mecanismos de consenso ecologicamente corretos.
- Adoção mais ampla em setores e comunidades.

Considerações finais

- Bitcoin como um experimento tecnológico e econômico.
- Evolução contínua moldando o futuro dos ativos digitais.

Capitalização de mercado























Top Assets by Market Cap						
All assets, including public companies, precious metals, cryptocurrencies, ETFs						
Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	 Gold	\$17.855 T	\$2,659	0.40%		
2	 Apple	\$3.673 T	\$243.04	0.01%		USA
3	 NVIDIA	\$3.552 T	\$145.06	-0.05%		USA
4	 Microsoft	\$3.290 T	\$442.62	1.19%		USA
5	 Amazon	\$2.319 T	\$220.55	1.10%		USA
6	 Alphabet (Google)	\$2.122 T	\$174.31	-1.01%		USA
7	 Bitcoin	\$1.954 T	\$98,716	-4.17%		
8	 Saudi Aramco	\$1.801 T	\$7.45	0.18%		S. Arabia
9	 Silver	\$1.783 T	\$31.68	0.46%		
10	 Meta Platforms (Facebook)	\$1.537 T	\$608.93	-0.79%		USA
11	 Tesla	\$1.186 T	\$369.49	3.23%		USA

Figure 2: Principais ativos por capitalização de mercado (6 de dezembro de 2024).

Fonte: <https://companiesmarketcap.com/>