O Que é o Bitcoin

Bitcoin é a **primeira moeda digital descentralizada** do mundo, criada em 2009 por um programador (ou grupo) sob o pseudônimo **Satoshi Nakamoto**.

A grande inovação do Bitcoin foi resolver o problema da **confiança e do gasto duplo** (double-spending) *sem a necessidade de um banco ou instituição central.*

🔒 1. Oferta Limitada – Por que o Bitcoin é Escasso

Bitcoin tem um código aberto que define uma **oferta máxima de 21 milhões de unidades**.

- Essa regra está **programada no protocolo** e não pode ser alterada sem consenso global.
- Novos bitcoins são emitidos como **recompensa aos mineradores** (já vamos falar disso) — esse processo é chamado de **halving**: a cada 210 mil blocos (~4 anos), a recompensa é cortada pela metade.

Ano	Recompensa por Bloco	Emissão diária (~)	Total em circulação
2009	50 BTC	~7200 BTC	Poucos milhares
2012	25 BTC	~3600 BTC	~10 milhões
2016	12.5 BTC	~1800 BTC	~15 milhões
2020	6.25 BTC	~900 BTC	~18.5 milhões
2024	3.125 BTC	~450 BTC	+19.8 milhões

🔚 **Em 2140**, a recompensa chegará a zero, e nenhum novo BTC será emitido. Isso transforma o Bitcoin num **ativo deflacionário**, como o ouro — mas com portabilidade digital.

📌 **Exemplo:** Imagine um terreno raríssimo em uma ilha isolada. Ninguém pode criar mais terra ali. O Bitcoin funciona da mesma forma: só existirão 21 milhões — nunca mais.

⚙️ 2. PoW (Prova de Trabalho) – Como o Bitcoin se Mantém Seguro

O **Proof of Work (PoW)** é o mecanismo de consenso do Bitcoin. Ele garante que todas as transações são válidas e que ninguém pode enganar o sistema.

Como funciona?

- Os **mineradores** competem para resolver **quebra-cabeças matemáticos** (hashes complexos).
- O primeiro que encontra a solução "**ganha o direito de validar um bloco**" (incluindo transações) e recebe uma **recompensa em BTC** + taxas.
- Esse processo demanda **poder computacional** e **energia elétrica** — por isso é chamado de *trabalho*.

🔐 Cada novo bloco validado reforça a **segurança da rede**.

📌 **Exemplo prático:** Um minerador tenta encontrar um número que, quando combinado com os dados de transações e passado por uma função hash (SHA-256), resulte em um valor com, por exemplo, 20 zeros no início. Isso exige **milhões ou bilhões de tentativas por segundo**.

⛏️ 3. Mineração – O Motor do Bitcoin

Mineração é o processo pelo qual os blocos são validados e novos bitcoins são emitidos.

Máquinas Especializadas

Máquinas (ASICs) especializadas processam hashes 24/7.

Formação de Blocos

Mineradores agrupam transações, formam blocos e tentam resolver o hash.

Recompensa

O minerador vencedor: - Valida o bloco - Ganha **BTCs novos** + **taxas de transação** - O bloco é adicionado à blockchain

⚡ A mineração também impede fraudes: para alterar uma transação passada, alguém teria que **refazer todo o trabalho de todos os blocos subsequentes**, o que é praticamente impossível.

📌 **Exemplo real:** A maior fazenda de mineração do mundo está na Islândia, onde há energia barata e clima frio (evita superaquecimento dos ASICs).

🟢 4. PoS (Prova de Participação) – Comparação com Outras Criptos

Bitcoin usa PoW, mas muitas criptomoedas modernas, como Ethereum (desde 2022), usam **PoS (Proof of Stake)**.

Como funciona o PoS:

- Em vez de gastar energia, os validadores **trancam moedas como garantia** (stake).
- São escolhidos para validar blocos com base em **quantidade apostada** e tempo.
- Se agirem de má-fé, **perdem parte do stake** (slashing).

Comparativo

	PoW (Bitcoin)	PoS (Ethereum, Solana)
Energia	Alta	Baixa
Segurança	Alta (muito caro atacar)	Alta, mas depende do stake
Centralização	Risco via grandes mineradores	Risco via baleias com muito stake
Custo de entrada	Caro (ASICs, energia)	Mais barato (moedas)

🧠 Resumo Final: Bitcoin é uma Inovação em Economia e Engenharia

1. Uma **moeda digital escassa**, imutável e fora do alcance de censura.
2. Baseada em **código aberto, criptografia e consenso distribuído**.
3. Ganha segurança através da **mineração PoW**, mas inspirou outros modelos (como PoS).
4. É **o ativo mais descentralizado e auditável** da história monetária.