Mineração na blockchain

PUC Minas

Aplicações Descentralizadas e Blockchain

Prof. Carlos Leonardo dos S. Mendes

Qual o objetivo da mineração?

- **Sistemas descentralizados** precisam de alguma forma de consenso para determinar o **estado corrente válido** do sistema.
- O **consenso** é um mecanismo fundamental em sistemas distribuídos e serve para proteger todo o sistema de componentes que enviam informações inválidas.
- Informações inválidas podem ser originárias de componentes com mau funcionamento (*bugs*) ou *hackeados*.
- A **mineração** é uma forma de consenso que garante **segurança** às redes de blockchain que adotam algoritmos de **prova de trabalho**.

O processo de mineração no Bitcoin

- A mineração é uma corrida entre nós da rede para resolver um **problema matemático** usando força computacional.
- O nó mais rápido a calcular a resposta correta para o problema matemático ganha o direito de gravar um novo bloco na rede.
- O vencedor recebe como recompensa:
  - novos bitcoins que são gerados pelo protocolo da rede e
  - as taxas de transações pagas pelos usuários.

O problema matemático

PUC Minas

O problema matemático

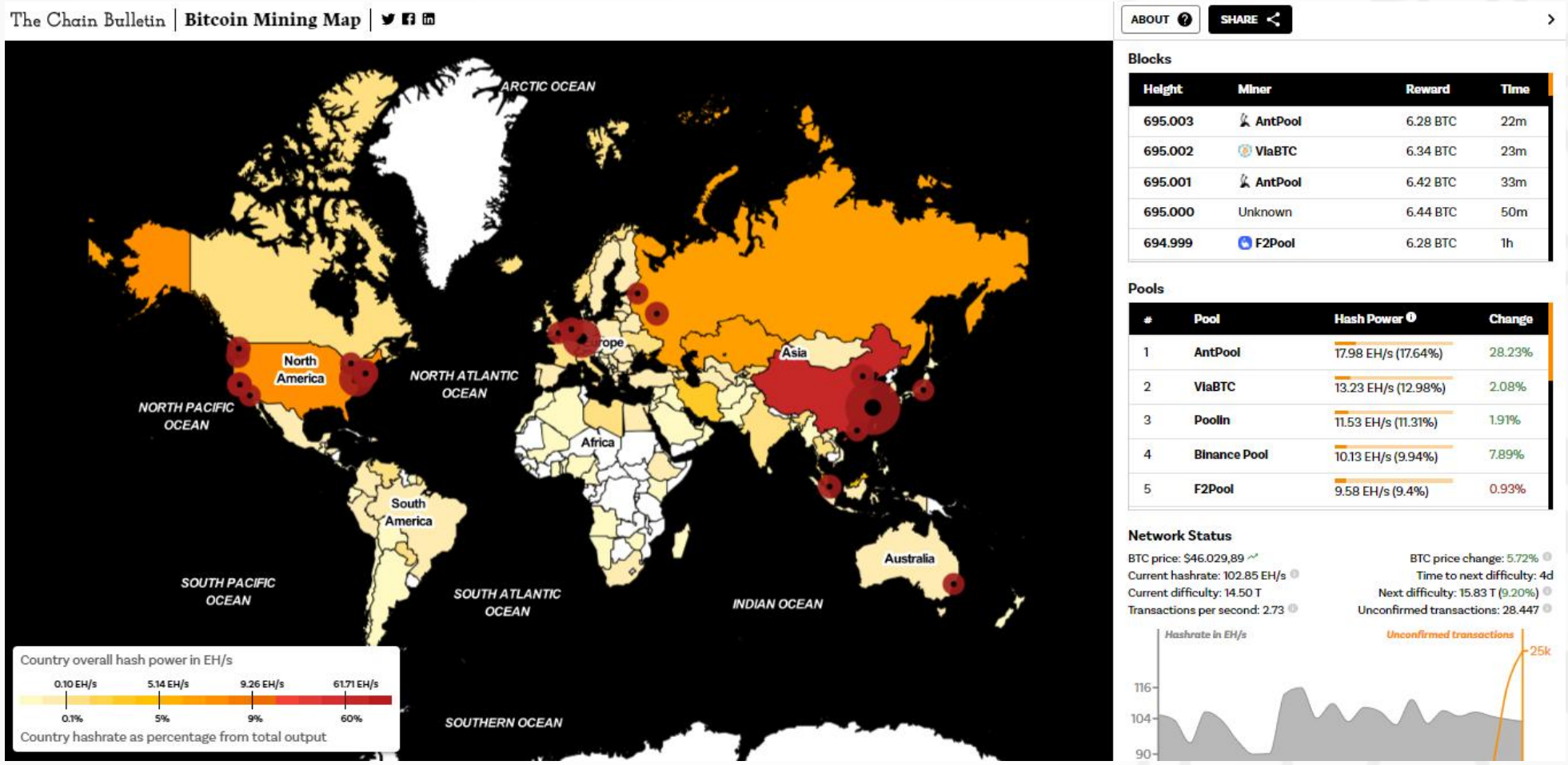
- O **hash** de um bloco do bitcoin tem 256 bits e é calculado pelo algoritmo SHA-256.
- O hash é calculado tendo como entrada os dados de transações do bloco e campos de controle.
- O desafio imposto (**problema matemático**) consiste em encontrar um determinado campo de controle da entrada (conhecido como **nounce**) que irá fazer a **saída da função hash** começar com um **determinado número de zeros**.
- Como a função hash é uma função de excelente distribuição, mínimas variações na entrada produzem grandes variações no hash.
- Basicamente, encontrar a solução significa determinar um **número inteiro para o campo nounce** que produza um hash com as condições impostas.

A dificuldade do problema matemático

- A dificuldade do problema matemático é ajustada pelo protocolo da rede para manter uma produção constante de blocos a cada 10 minutos.
- A dificuldade do problema matemático no bitcoin é conhecida como **hash rate**.
- Se há muito poder computacional na rede, os mineradores tendem a resolver o problema matemático mais rapidamente.
- Se há menos poder computacional, o problema tende a ser resolvido com mais tempo.
- O ajuste da dificuldade é um fator importante para manter a taxa aproximada de um bloco a cada 10 minutos, o que é importante para a **escalabilidade** do bitcoin.

Mapa de mineradores

(hash power)



Fonte: https://chainbulletin.com/bitcoin-mining-map/

PUC Minas

Mineração de forma resumida

Resumidamente, **minerar no blockchain** significa resolver um problema matemático de **difícil solução**, mas de **fácil verificação**.

A emissão de criptomoedas na mineração

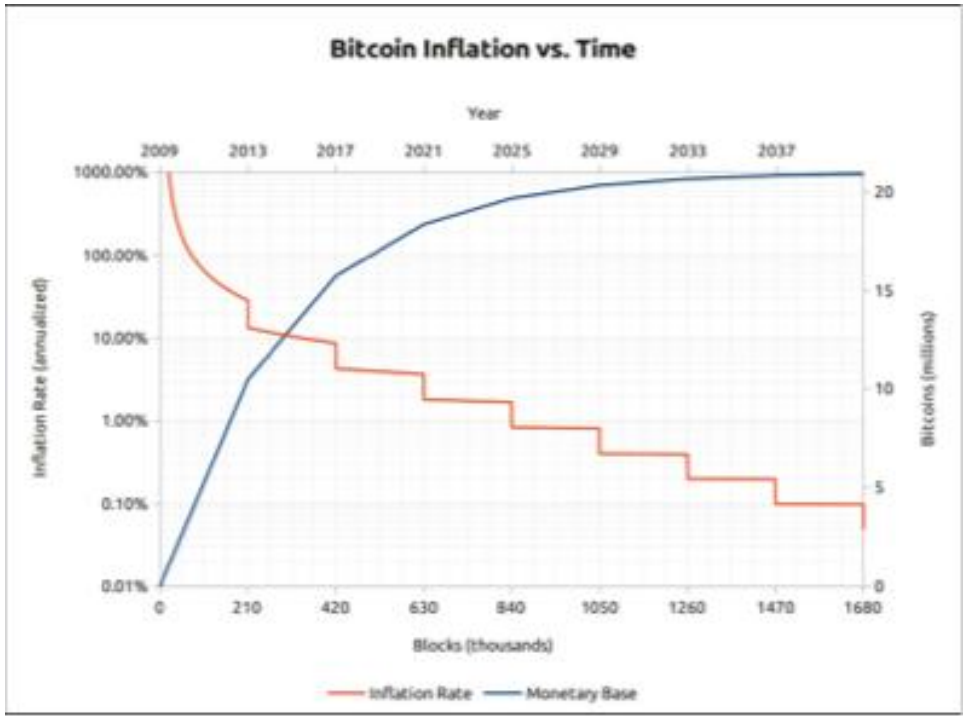
- **Criptomoedas**, como o bitcoin, **não são emitidas por uma autoridade** ou instituição central.
- No Bitcoin, elas são **geradas pelo protocolo** da rede de blockchain no processo de **mineração**.
- As criptomoedas geradas são **repassadas ao minerador** como forma de recompensá-lo por ter empregado **recurso computacional** como forma de **consenso e proteção** da rede.

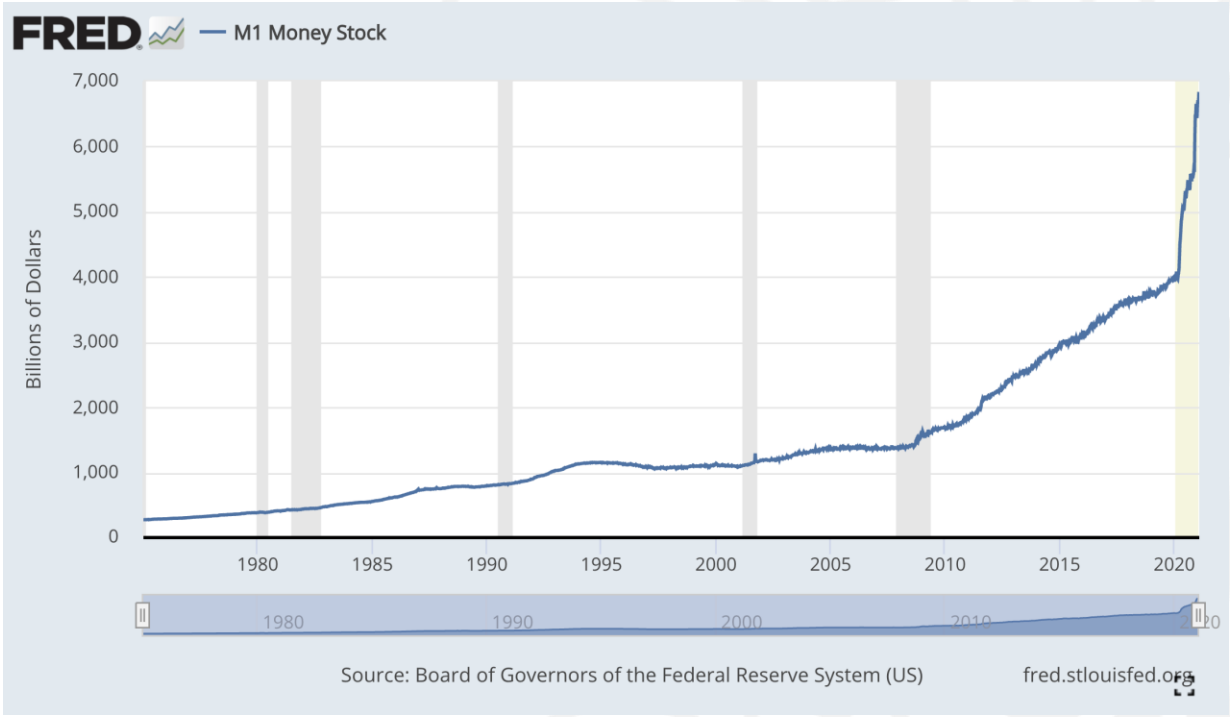
Bitcoin Halving

- O bitcoin possui um estoque total finito e pré-determinado (21 milhões).
- A quantidade de bitcoins gerada a cada novo bloco minerado cai pela metada a cada 4 anos (210.000 blocos).
- A geração iniciou com 50 BTC e atualmente (2021) está em 6.25 BTC.
- Em 2032, mais de 99% de BTC estará gerado. A emissão de novos bitcoins está estimada até 2140.

PUC Minas

Emissão de Bitcoin X US$



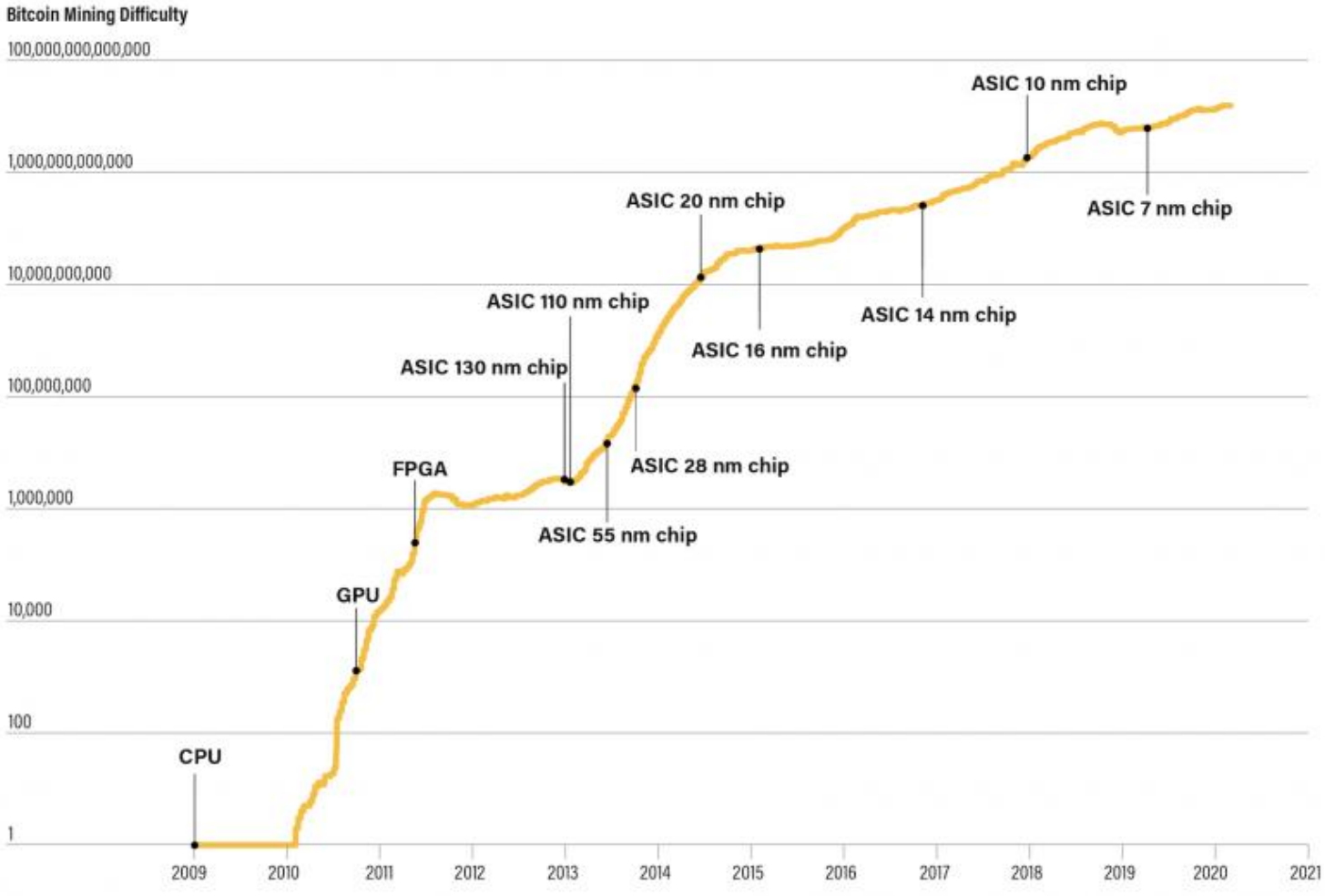


PUC Minas

A história da mineração no Bitcoin

- Em 3 de janeiro de 2009, Satoshi Nakamoto minerou o primeiro bloco do bitcoin usando seu computador pessoal.
- Esse bloco é conhecido como **genesis block**.
- Atualmente, devido ao grande uso da rede, é impossível minerar blocos usando computadores pessoais.
- A mineração se tornou um processo demandante de altos recursos computacionais.
- As tecnologias de processamento usadas na mineração evoluíram de CPUs para GPUs, FPGAs e ASIC.

A evolução dos hardwares de mineração



Bitcoin mining difficulty vs. time and approximate introduction dates of new mining technology
Source: "The Evolution of Bitcoin Hardware" by Michael Bedford Taylor (University of Washington), CoinDesk Research

PUC Minas

PUC Minas