# What is mining?

A bird’s eye view of Bitcoin mining

Meni Rosenfeld

# Introduction

- Bitcoin mining consists in using computers to perform specific calculations, and obtaining bitcoins in return

- **Bitcoin is not about mining!**
  - Bitcoin is a decentralized digital currency
  - Mining is the means to that end
  - A Bitcoin user does not need to do mining

- This talk will touch on key concepts in mining

# Why does Bitcoin need mining?

- Mining is a system that serves two distinct purposes:
  - Determining the initial distribution of coins
  - Synchronizing Bitcoin transactions

# Initial distribution of bitcoins

- Bitcoins are property; someone needs to own them when created.
  - The inventor of Bitcoin? Not fair
  - Equally to each person? Requires physical authority
  - By software instances? Can be cloned/gamed
  - By IP addresses? Centralized and arbitrary
  - …?
- Distribution according to proof of computational work is fair, measurable, "pure" and has low overhead
- Long term, initial distribution doesn't matter that much

# Synchronizing transactions

- Digital currencies have a problem called “double spending”
  - The owner of a coin can try to use the same coin to pay two people simultaneously
- Centralized solutions are known
- The first decentralized solution is the blockchain (mining), invented in 2008 by “Satoshi Nakamoto”
- This talk is not about how mining works to synchronize transactions

# Mining hardware

- Mining involves a specific calculation – SHA-256

- Mining performance is measured in MH/s
  - (Mega hashes per second)

- Types of hardware (performance per $1K)
  - CPU: 10 MH/s
  - GPU: 1,000 MH/s
  - FPGA: 2,000 MH/s
  - ASIC: 40,000 MH/s

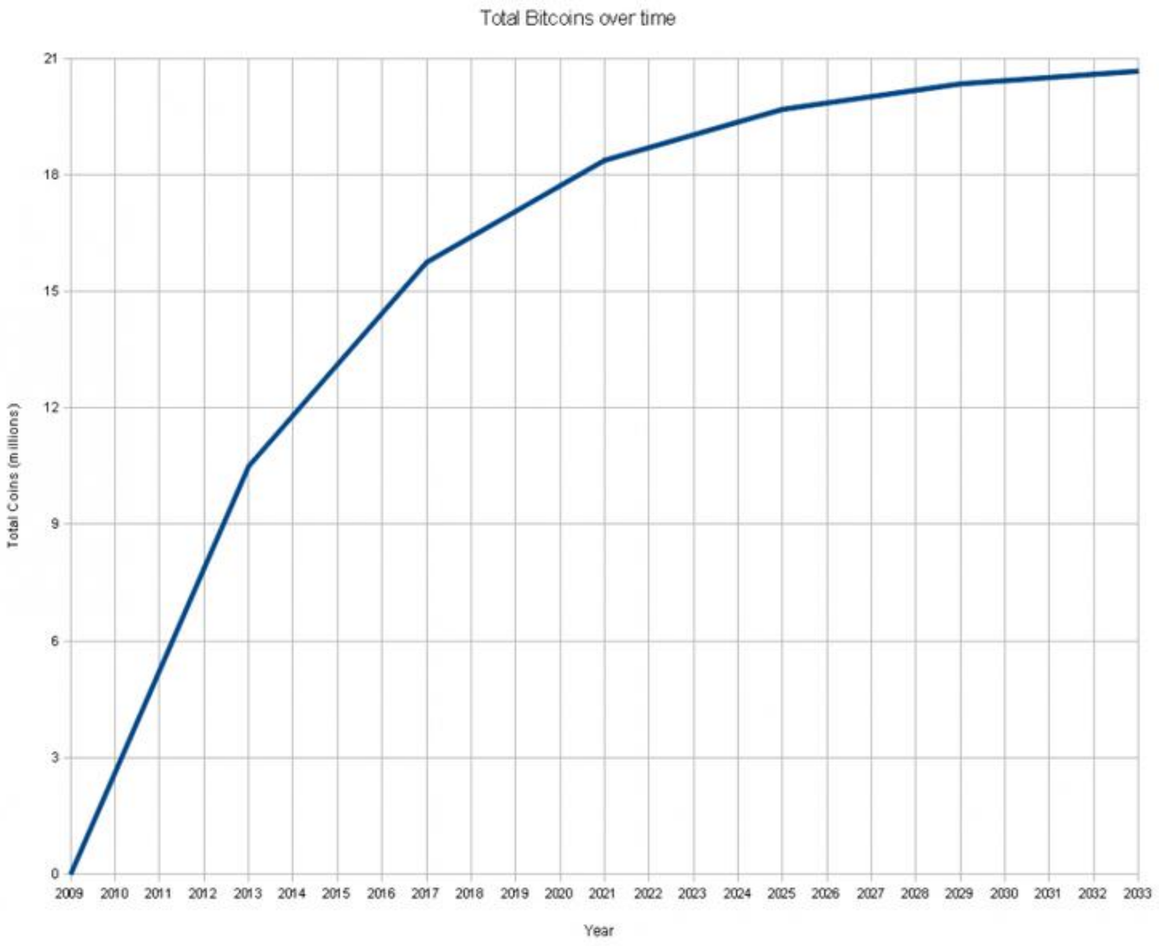
# Mining rewards

- Miners work & try to find blocks

- For each block found they get:
  - Newly generated coins (currently 25 BTC per block)
    - New coins gradually enter circulation
    - New coins per block are reduced by half every 4 years
    - There will never be more than 21M bitcoins

  - Transaction fees (currently ~0.3 BTC per block)
    - Bitcoin users pay them out of existing coins
    - Help the transaction to execute faster
    - Will become more significant going forward

# Inflation Schedule



# Mining difficulty

- “Difficulty” controls the number of hashes required to find a block
- Difficulty is adjusted every 2 weeks to keep the rate of finding blocks at one per 10 minutes on average
- Difficulty increases as more people mine – BTC generation rate is fixed, distributed in proportion to mining performance.

# Mining pools

- Finding blocks is discrete, random and highly variable
  - A miner expecting to find 1 block on average per month (~$360) will actually find 0-3 blocks
  - Not good for cash flow or mental health

- Most miners join a mining pool, mine together and share the rewards
  - Mining rewards in a pool are very close to average
  - Many pools with different size, reward method and other features. Some good, some not so good

# Mining as an investment

- Buying mining hardware is a risky investment
  - Future BTC price is unknown
  - Future difficulty is unknown
  - Might never reach positive ROI
- Running a mining operation requires technical expertise
- Capital markets help separate the two

# The ASIC arms race

- Multiple companies are working on dedicated Bitcoin mining chips
  - Butterfly Labs (multiple delays)
  - bASIC (scrapped due to internal conflicts)
  - Avalon (shipped yesterday!)
  - ASICMINER (will mine itself, not sell hardware)
  - DeepBit
- The advent of ASIC chips will be very disruptive
- Investing in mining now is even riskier than usual
- Seeing this transition unfold will be interesting

# Questions?