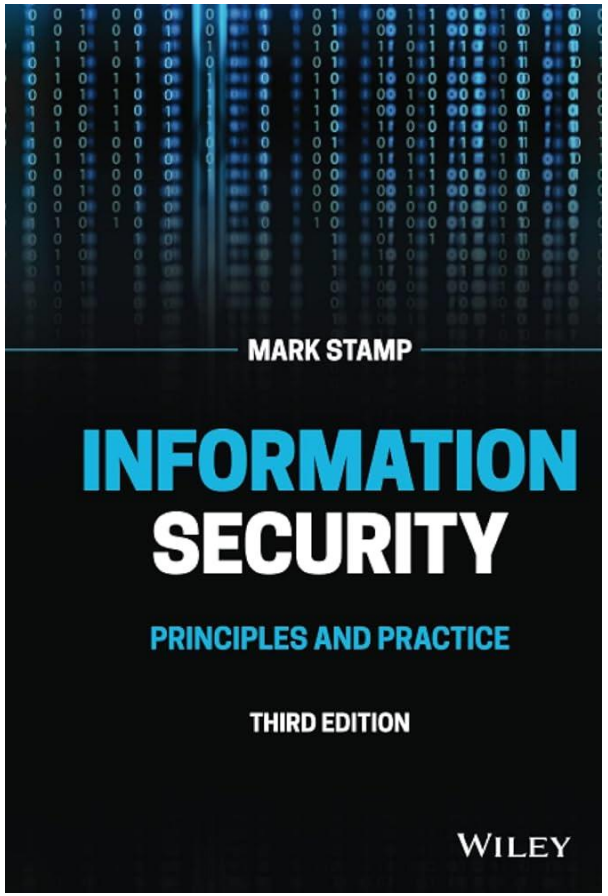
بسم الله الرحمن الرحیم

# مبانی رایانش امن

## جلسه ۱۳

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان


MARK STAMP
INFORMATION SECURITY
PRINCIPLES AND PRACTICE
THIRD EDITION
WILEY

- فصل ؟ استمپ

# Blockchain

# Preliminaries: Work

- How to measure (digital) ***work*** ?
- Our unit of work will be 1 hash
- Suppose that we have a hash function h(x) that generates an N-bit output
- Then randomly chosen input generates one of $2^N$ equally likely outputs
  - For any input R, have, $0 \leq h(R) < 2^N$
  - Different R yield uncorrelated hashes

# Work and Hashing

- For 16-bit hash, how many hashes until

  $h(R) = y = (0000000000y_5y_4y_3y_2y_1y_0)$ ?

- For random R, we have a 1/2 chance that

  $y = (0y_{14}y_{13}y_{12}y_{11}y_{10}y_9y_8y_7y_6y_5y_4y_3y_2y_1y_0)$

- And 1/4 chance that

  $y = (00y_{13}y_{12}y_{11}y_{10}y_9y_8y_7y_6y_5y_4y_3y_2y_1y_0)$

- And 1/8 chance that

  $y = (000y_{12}y_{11}y_{10}y_9y_8y_7y_6y_5y_4y_3y_2y_1y_0)$

- And so on…

# Work and Hashing

- For 16-bit hash, if someone gives us an R such that h(R) < 64
  - Then expected number of hashes computed is $2^{10}$ ("expected" means average case)
  - That is, they have done 1,000 units of work
- We use hashing to show work was done
- Why this obsession with work?
  - That will become clear later…

# Work and Hashing

- We can adjust parameter so more work (or less) is required
  - For N-bit hash, if we require $h(R) < 2^n$ then expected work is $2^{N-n}$ hashes
- ***Note***: We can easily verify that the expected amount of work was done
  - Only requires one single hash
  - No matter how much work to find R

# Distributed Ledger and Work

- Every ledger will have some amount of work associated with it
- Ledger with most work always "wins"
  - That is, everyone accepts ledger that has the most work put into it
- Recall, work is measured in hashes
- So, more hashes is "more better"

# Blocks and Hashes

- Each transaction is signed
- Transactions grouped into ***blocks***
  - Let B be one such block
- Find (nonce) R so that $h(B,R) < 2^n$
  - Equivalent to saying h(B,R) starts with a specified number of 0s
- Work required to find R?
  - On average $2^{N-n}$ hashes for N-bit hash

# Chain

- Don't want to revalidate each block, want to order blocks, and so on
- We'll ***chain*** blocks together
  - Put hash of previous block in header of current block before computing hash
- So, must find R so that $h(Y,B,R) < 2^n$
  - Where Y is hash of previous block

# Blockchain

- We now have

$$Y_{i+1} = h(Y_i, B_i, R_i) < 2^n$$

$$Y_{i+2} = h(Y_{i+1}, B_{i+1}, R_{i+1}) < 2^n$$

$$Y_{i+3} = h(Y_{i+2}, B_{i+2}, R_{i+2}) < 2^n$$

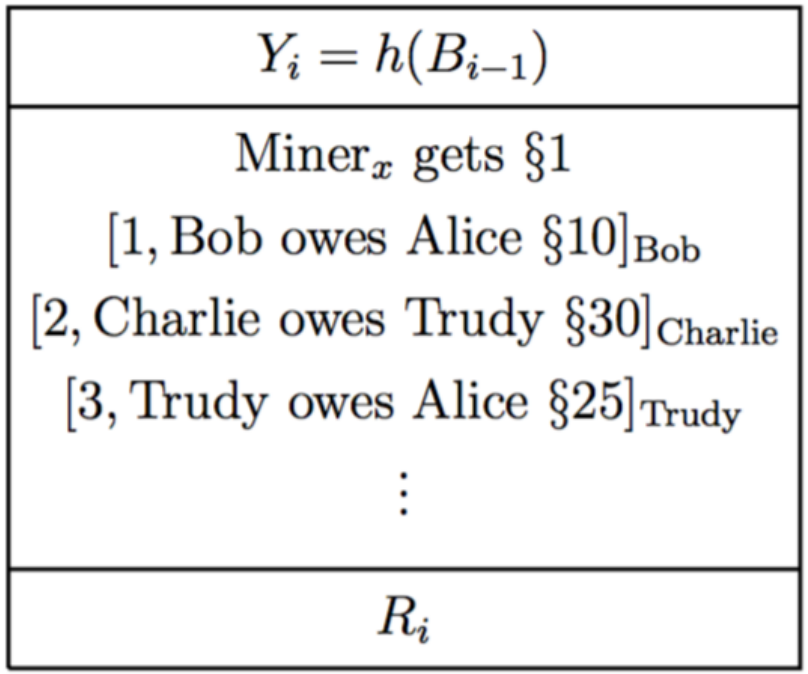
- Each B is a block
  - Block is a group of signed transactions
- Each R is chosen so inequality holds
  - Lot of work to find R, easy to verify $Y < 2^n$

# Mining?

- Anyone can create a new block
- But lots of work to find a valid hash
- So what is the incentive to do work?
- "Free" money!
  - Get (new) money for doing work, say, § 1
  - Put this info at start of block, does not need to be signed (since new money)

# One Block

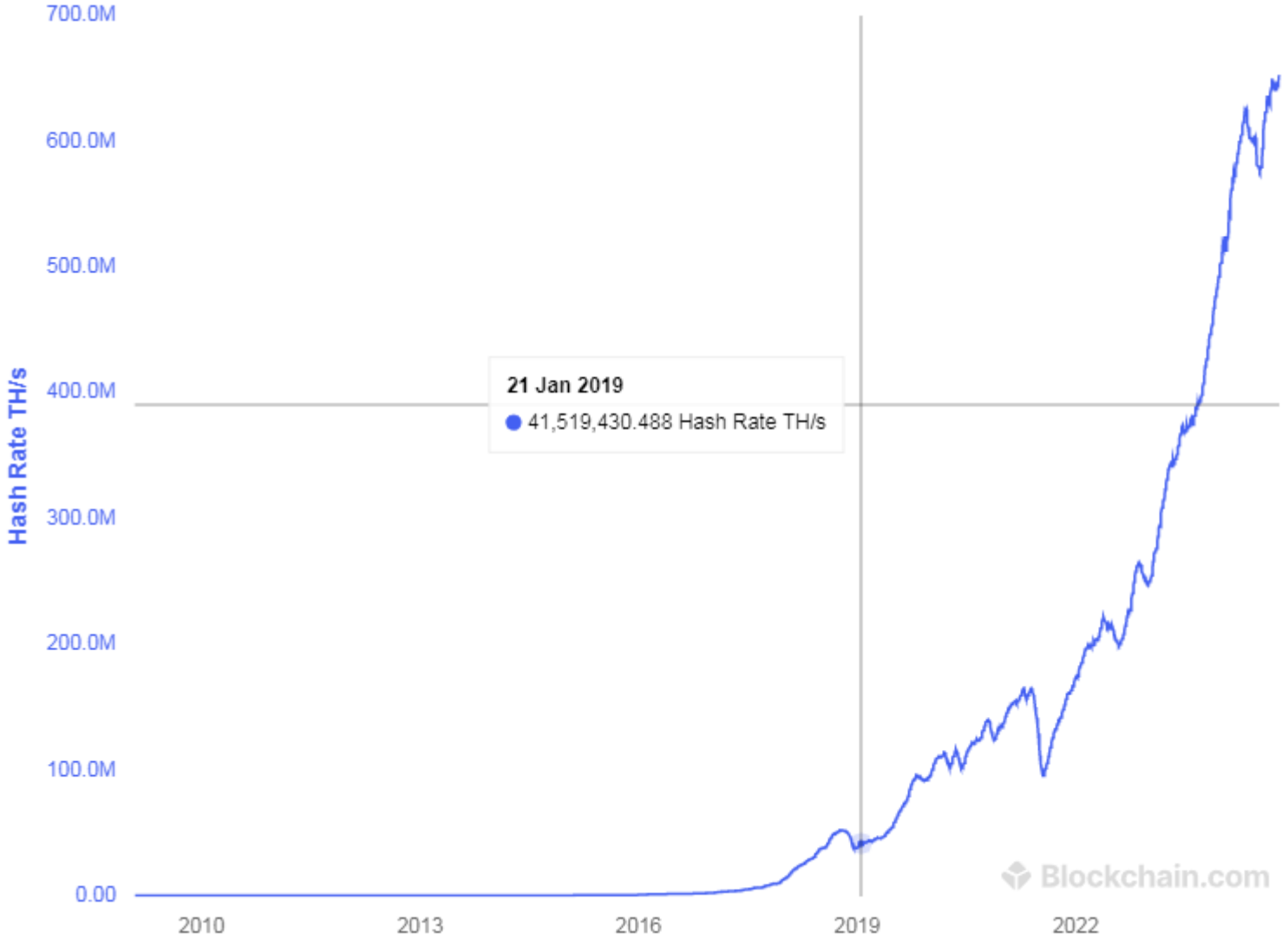
- Block $B_i$ looks like...




Block $B_i$

# Mining

- Free money, so miners are in a race to find hashes that yield valid blocks
- The more computing power a miner has, the better chance to win race
- Once a valid hash is found, miner sends the block out to everybody
- Again, easy to verify hash is correct


700.0M
600.0M
500.0M
400.0M
300.0M
200.0M
100.0M
0.00
Hash Rate TH/s
21 Jan 2019
41,519,430.488 Hash Rate TH/s
2010
2013
2016
2019
2022
Blockchain.com

# Mining Hardware

IUT-ECE

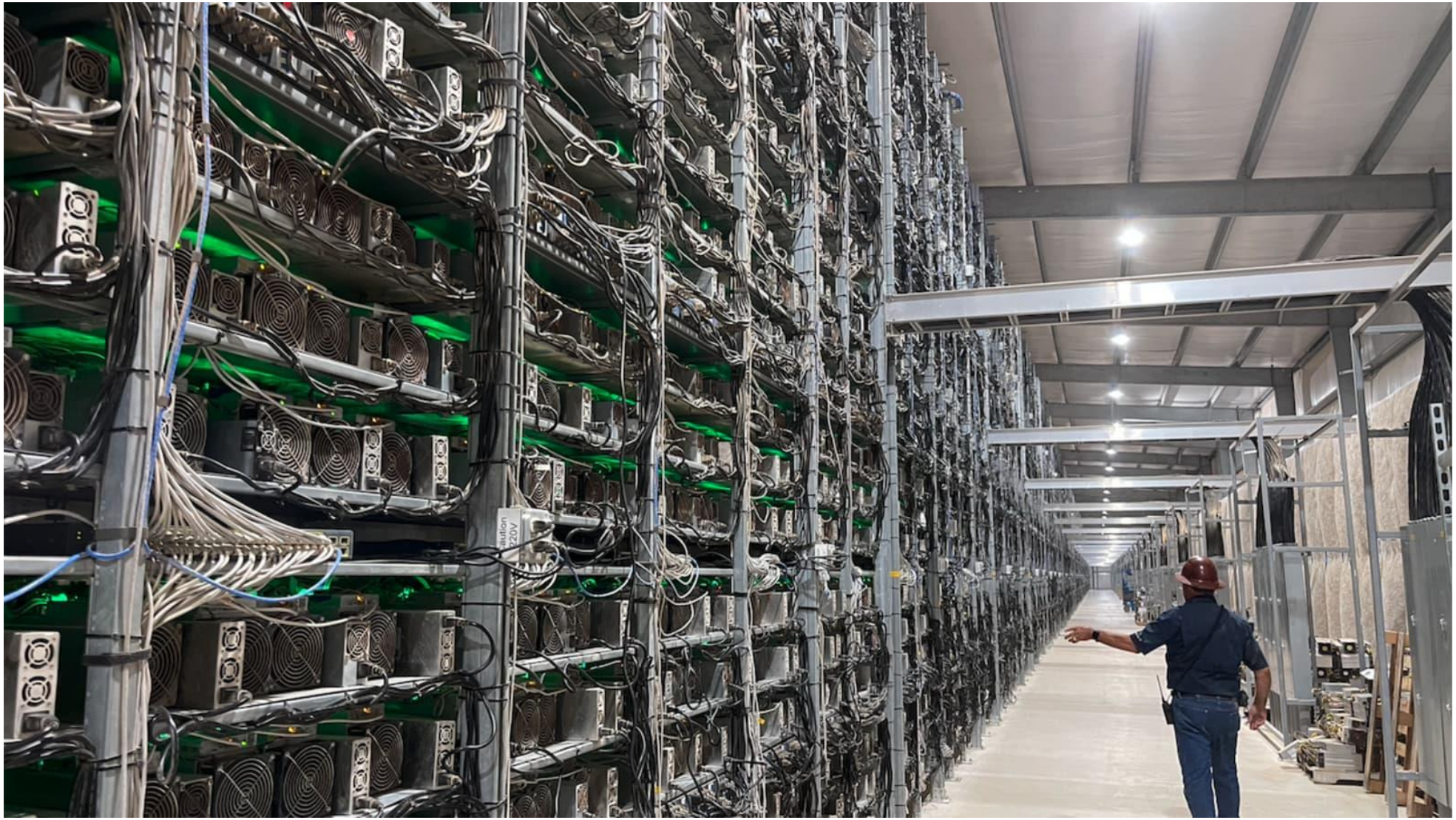
GPU

FPGA

ASIC

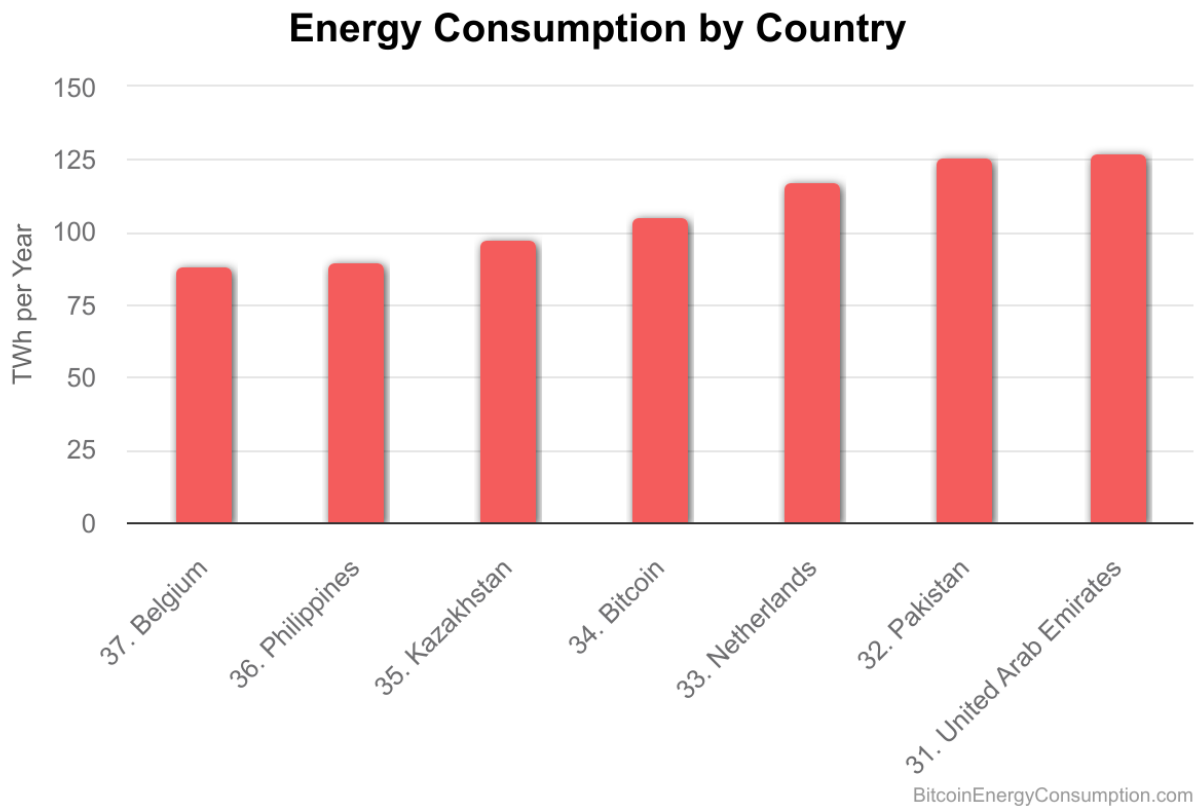
# Mining Hardware





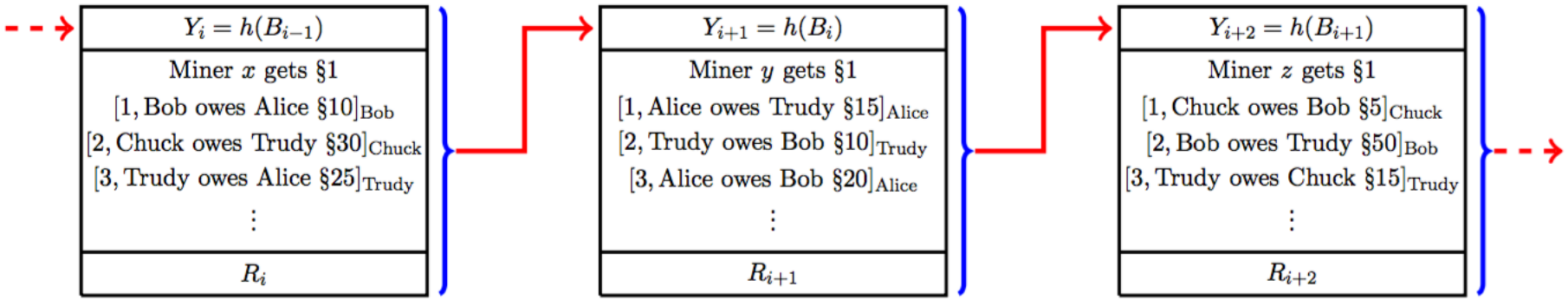
# Mining Hardware





# Blockchain

- Blockchain looks like...




- Require that $h(Y_i, B_i, R_i) < 2^n$ and so on

# Mining

- Why is "mining" called mining ?
  - Really, just finding a valid block hash
- Miner is doing work, and creating new money that did not previously exist
  - In a sense, this is comparable to mining gold or silver (for example)
- This may be the most misunderstood part of cryptocurrency protocols