# Consensus Algorithms

Administrivia

- HW1 due tonight!

- HW2 out ~tonight (will be due in 2 weeks)

  - Spoilers: it's about hashing

  - MUST be done in pairs

  - Tonight's clinic will cover more hashing stuff

- Quiz 2 also out today (will be due Friday night)

  - Covers Thurs lecture on hashing and Tues lecture on consensus algorithms (not today!)
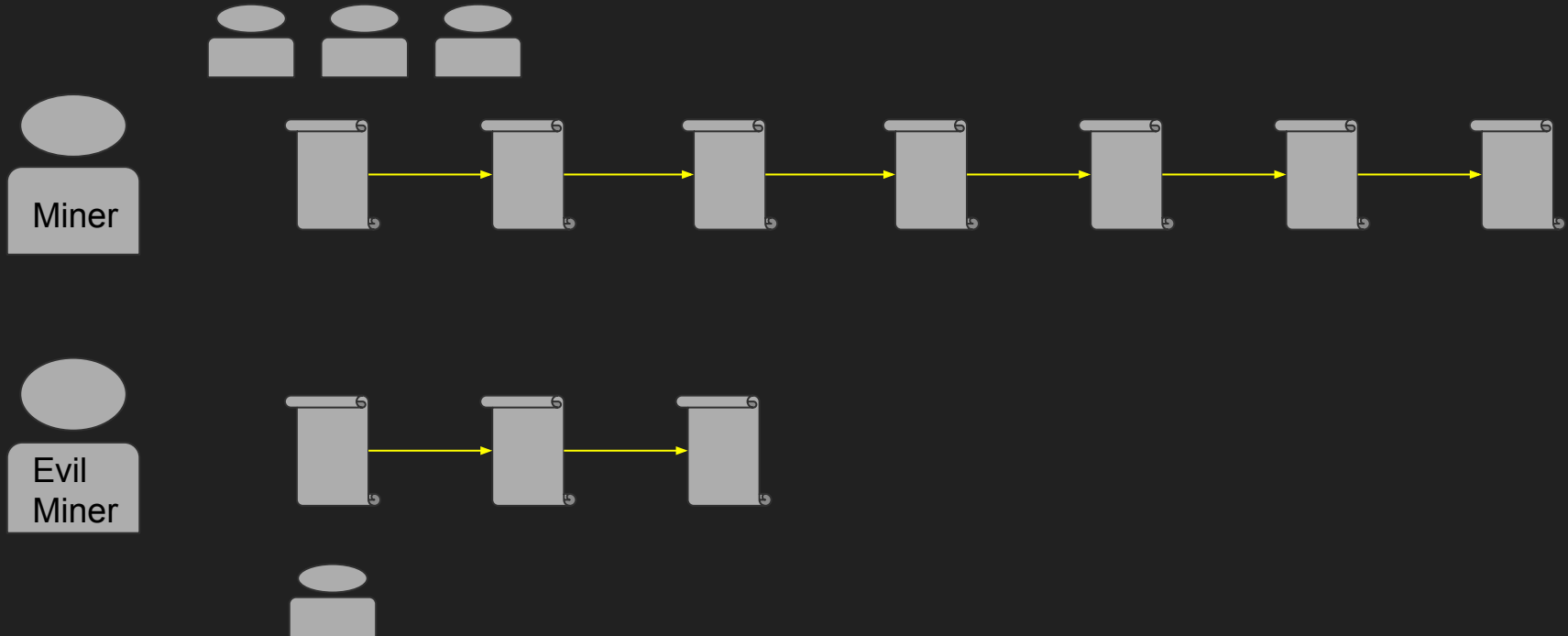
- Regular office hours schedule coming soon

Proof of Work (cont.)
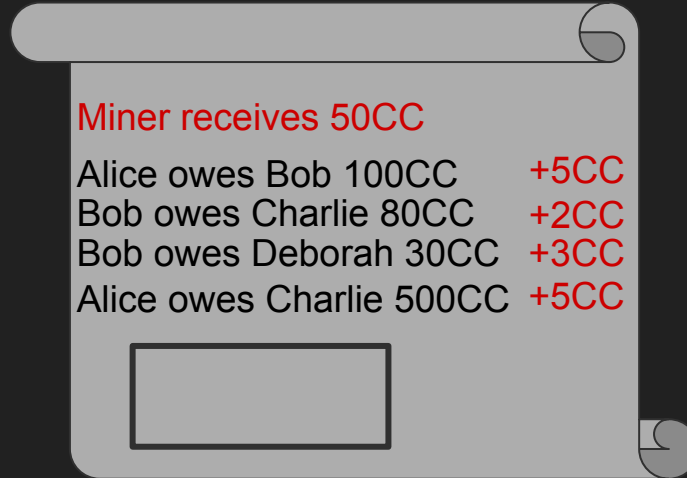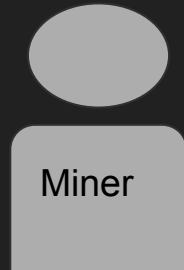
Proof of Work
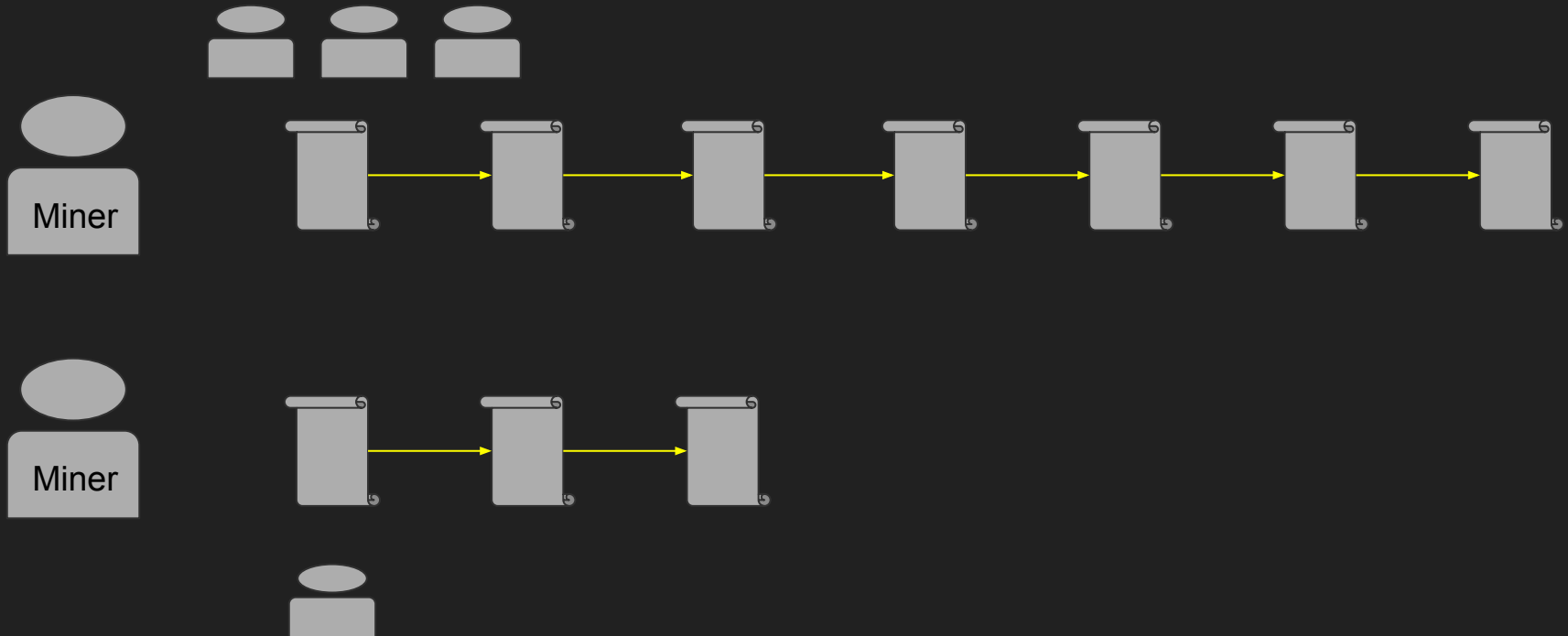
Proof of Work

- Also protection against fraud!
  - (So long as you don't have 51% of computation power)

Proof of Work

- Is the Miner incentive actually all that incentivizing?
  - What's the expected time for any individual Miner to win the race?
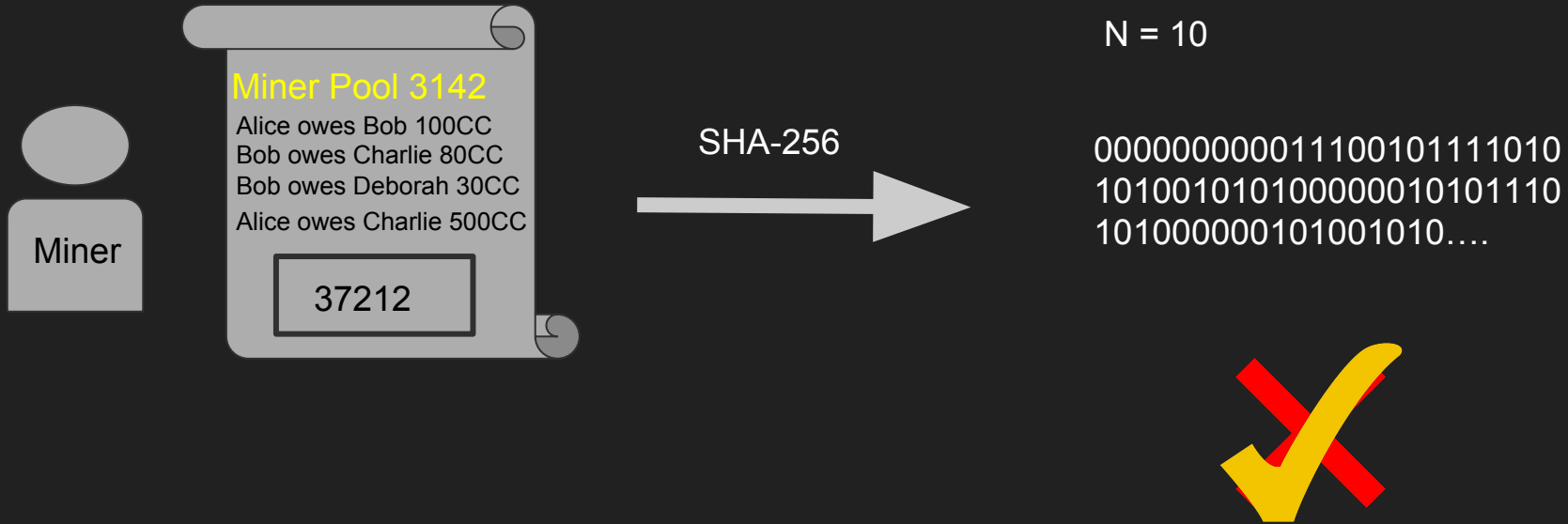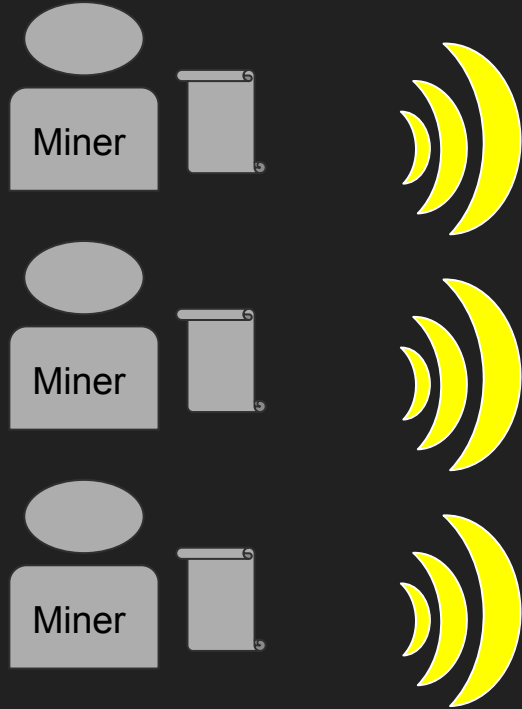
Miner

Miner receives 50CC

Alice owes Bob 100CC   +5CC
Bob owes Charlie 80CC   +2CC
Bob owes Deborah 30CC   +3CC
Alice owes Charlie 500CC +5CC

Proof of Work: Miner Pools

Miner

Miner Pool 3142
Alice owes Bob 100CC
Bob owes Charlie 80CC
Bob owes Deborah 30CC
Alice owes Charlie 500CC

37212

SHA-256

N = 10

0000000000111001011111010
1010010101000000101011100
101000000101001010….

Proof of Work: Miner Pools

Miner

Miner
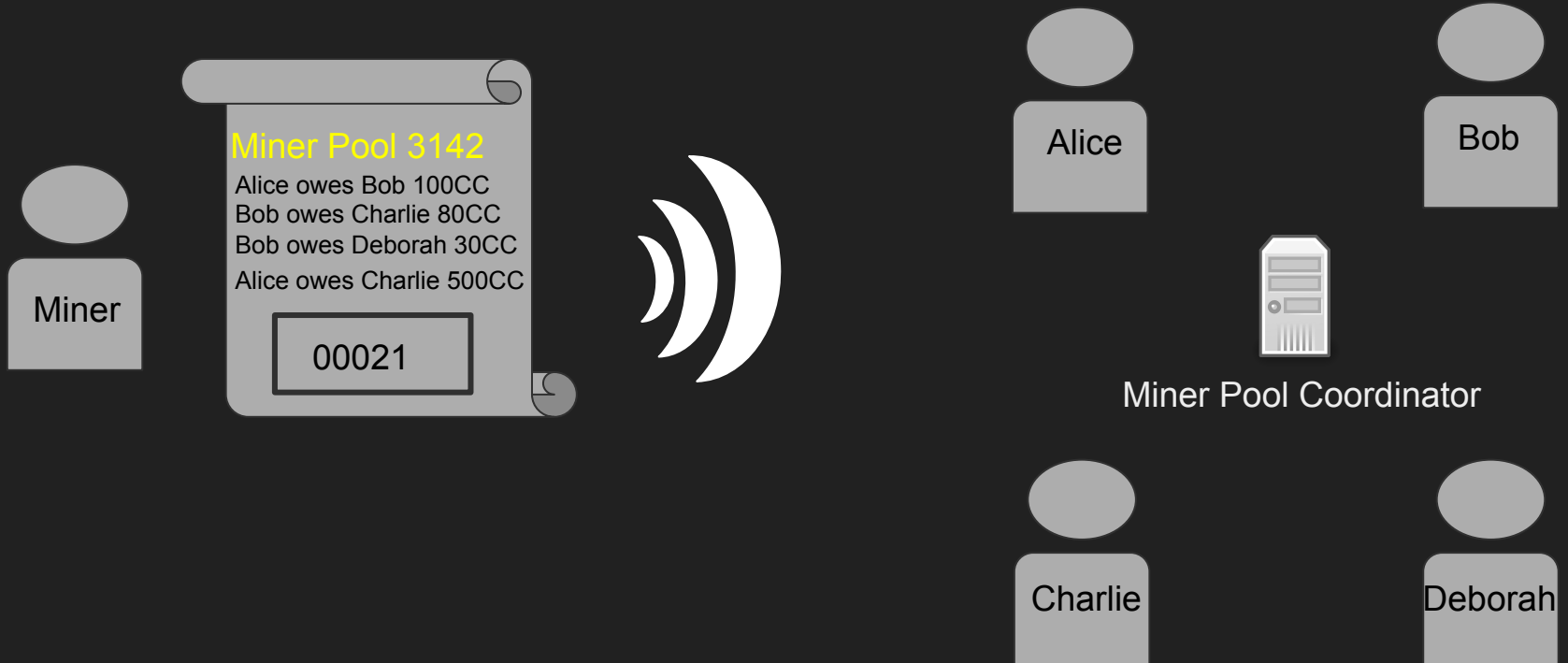
Miner

Miner Pool Coordinator

Proof of Work: Miner Pools

Proof of Work: Miner Pools

- Miners do work on behalf of the pool

- As long as they can show that they're helping, they get a cut
  - Very roughly like tip sharing at a diner

- But… is there anything stopping you from being in multiple pools?
  - Potential for abuse: can broadcast near misses but save actual hits for your "real" pool
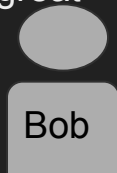
Paxos

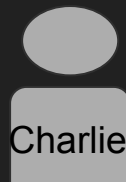# Paxos

What do we mean by consensus?

- Consensus is on **<u>one</u>** value.
- Consensus is reached once a **<u>majority</u>** of participants agree.
- Once a consensus is reached, everyone can **<u>eventually</u>** know the result.
- Participants are happy to reach consensus on **<u>any</u>** result, not just the one they propose.
- Communication channels are **<u>not</u>** perfect (messages may be lost).

Paxos

Paxos