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

Miner

SHA-256

N = 10
000000000011100101111010
10100101010000010101110
101000000101001010101010
Proof of Work: Miner Pools
Proof of Work: Miner Pools

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

Miner Pool Coordinator

Miner

Alice

Bob

Charlie

Deborah
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

Citation: Google Tech Talks video on Paxos
Paxos

What do we mean by consensus?

- Consensus is on one value.
- Consensus is reached once a majority of participants agree.
- Once a consensus is reached, everyone can eventually know the result.
- Participants are happy to reach consensus on any result, not just the one they propose.
- Communication channels are not perfect (messages may be lost).
“Let’s see Finding Nemo”

“Sure, Finding Nemo is great”

“Finding Nemooooooooo”

“OK, I guess it’s Finding Nemo”

“What about Mission Impossible”

“Ugh, OK fine”
“Hey guys, wanna watch the Star Wars Holiday Special”

“NO. We already decided Finding Nemo”