Blockchain Structure 🧱

P2P Network
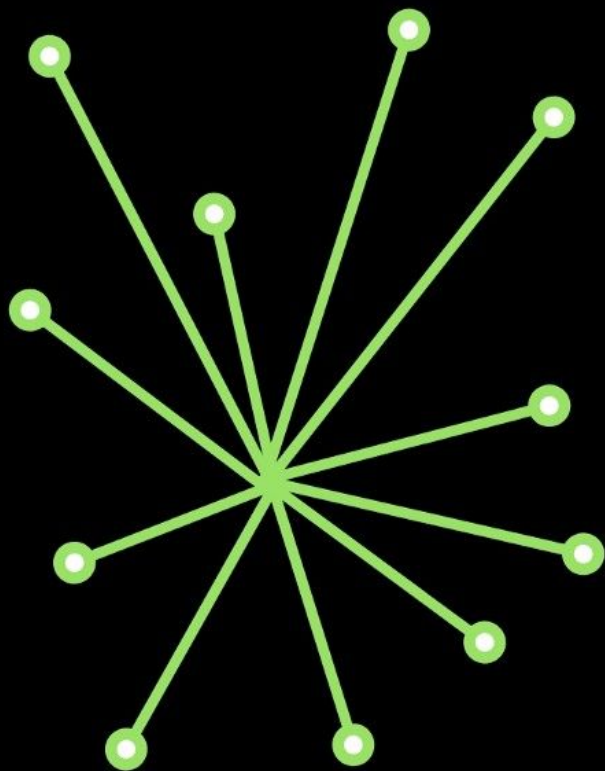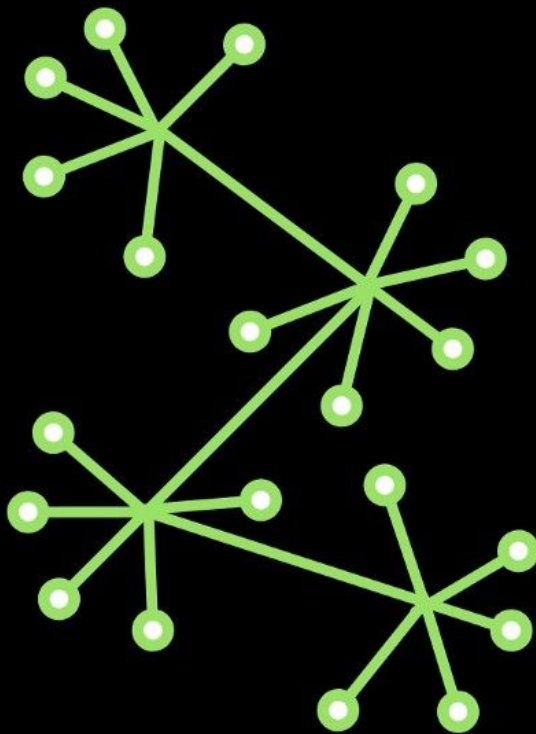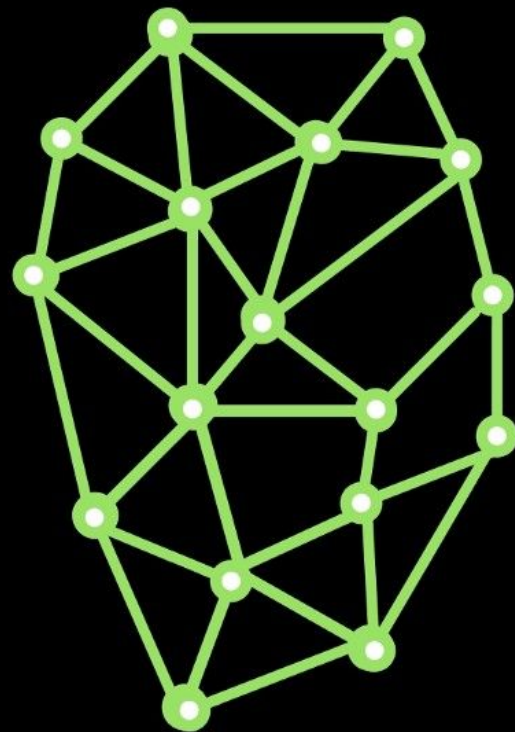
Blockchain Network Architecture

🏛️

Centralized   Decentralized   Distributed

nakamo·to

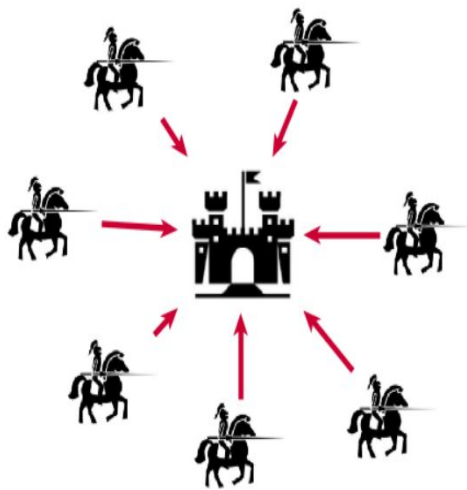A **server** based network | A **peer-to-peer** based network.

Q&A: Review #1

- **Q:** How do distributed p2p networks agree on what data is valid *without* a central administrator running the show? 🤔

Byzantine Generals' Problem

- Problem = **coordination in a decentralized environment**
- Solution?
  - **Proof of Work**
- Game Theory
  - Losing Strategy = Traitor Wins
  - Winning Strategy = Consensus

Coordinated attack leading to victory

Traitor

Traitor

Uncoordinated attack leading to defeat

Byzantine Generals' Problem

- Problem = **coordination in a decentralized environment**
- Solution?
  - **Proof of Work**
- Game Theory
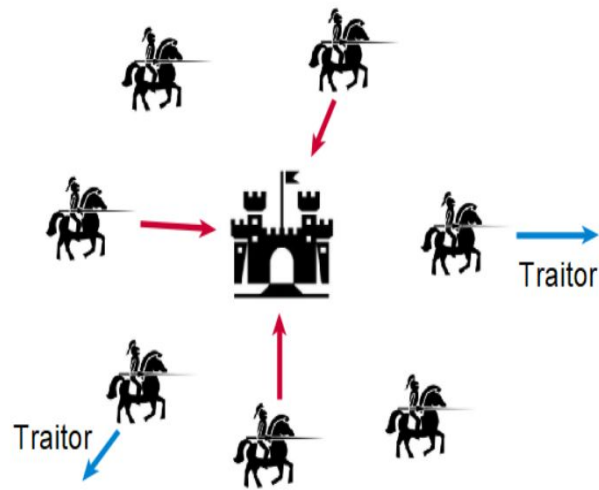 - Losing Strategy = Traitor Wins
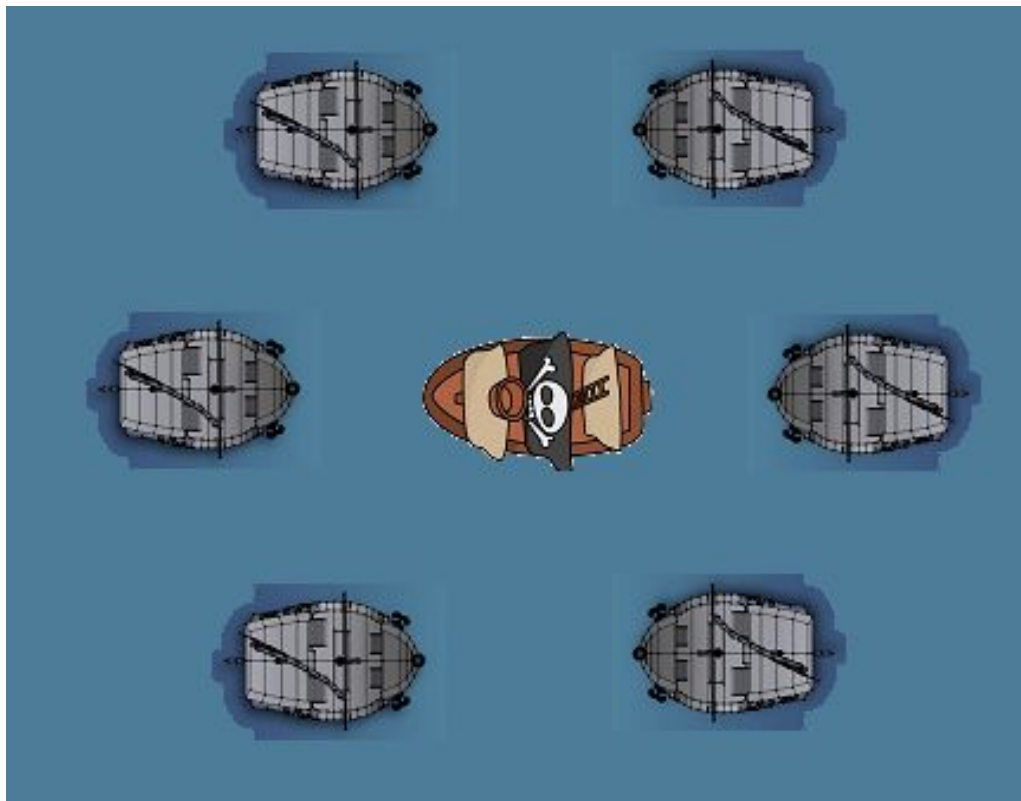 - Winning Strategy = Consensus

Q&A: Review #1

- **Q: How do distributed p2p networks agree on what data is valid without a central administrator running the show? 🤔**
  - **A:** Consensus mechanisms!
    - The Bitcoin network decides validity of new data based on who is able to produce a valid proof-of-work.

Q&A: Review #2

- **Q:** How is the block hash calculated?

Q&A: Review #2

- **Q:** **How is the block hash calculated?**
  - **A:** A [hashing function](#) takes data as input, and returns a unique hash.

Q&A: Review #3

- **Q:** What is a "valid" hash?

Q&A: Review #3

- **Q: What is a "valid" hash?**
  - **A:** A valid hash for a blockchain is a hash that meets certain requirements.
    - Ie:
      1. Block index is one greater than latest block index.
      2. Block previous hash equal to latest block hash.
      3. Block hash meets difficulty requirement.
      4. Block hash is correctly calculated.

[Blockchain Demo](#)

Next:

UTXO & Account Models