NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty
Department of Computer Science & Engineering

Lecture 08: Distributed Systems for Decentralization – The Beginning

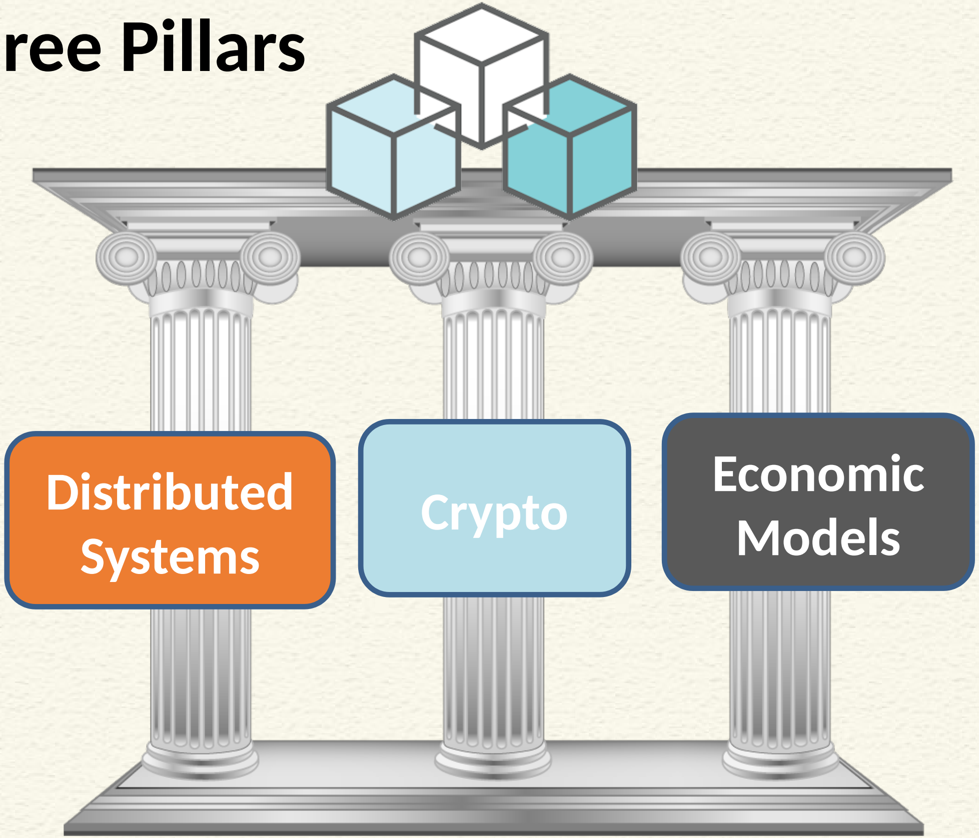
CONCEPTS COVERED

- Distributed Systems
- Blockchain as a Distributed System
- Distributed Consensus – A History

KEYWORDS

- **Distributed System**
- **Consensus**

The Three Pillars

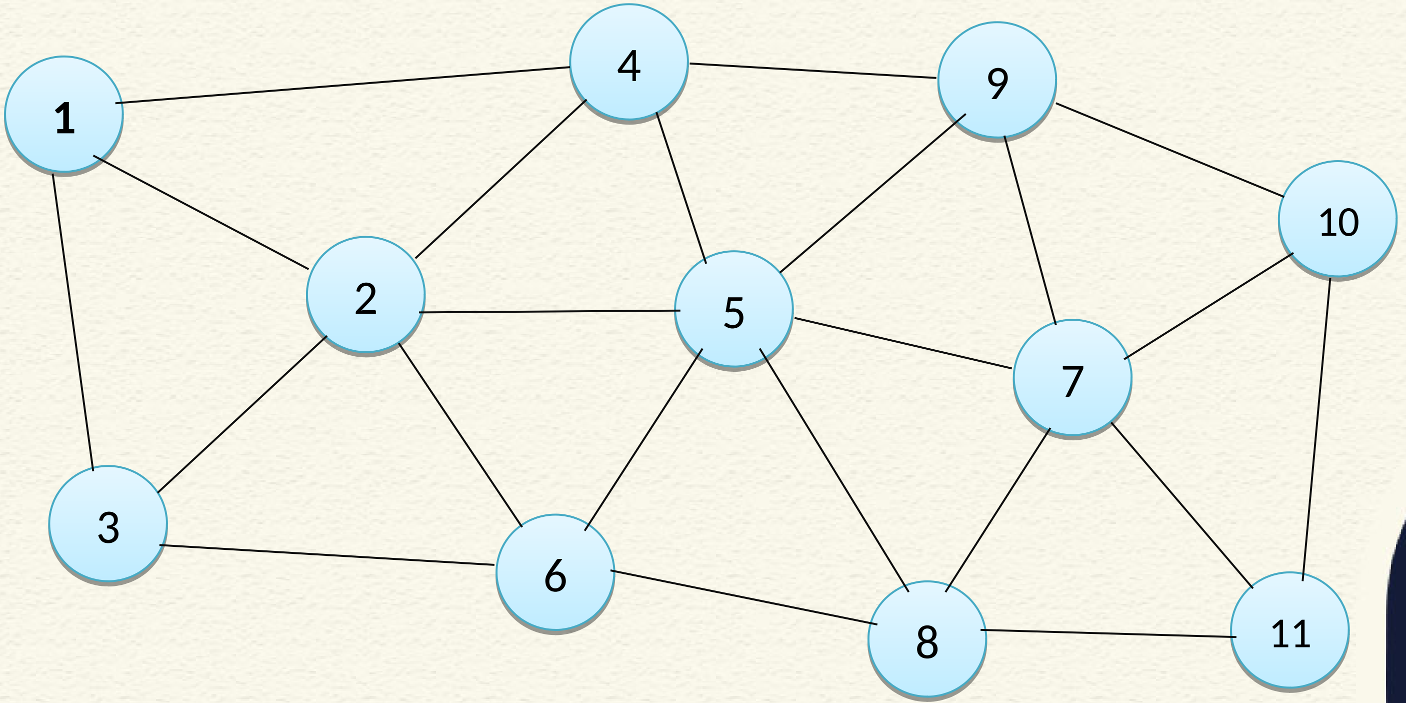


Distributed Systems

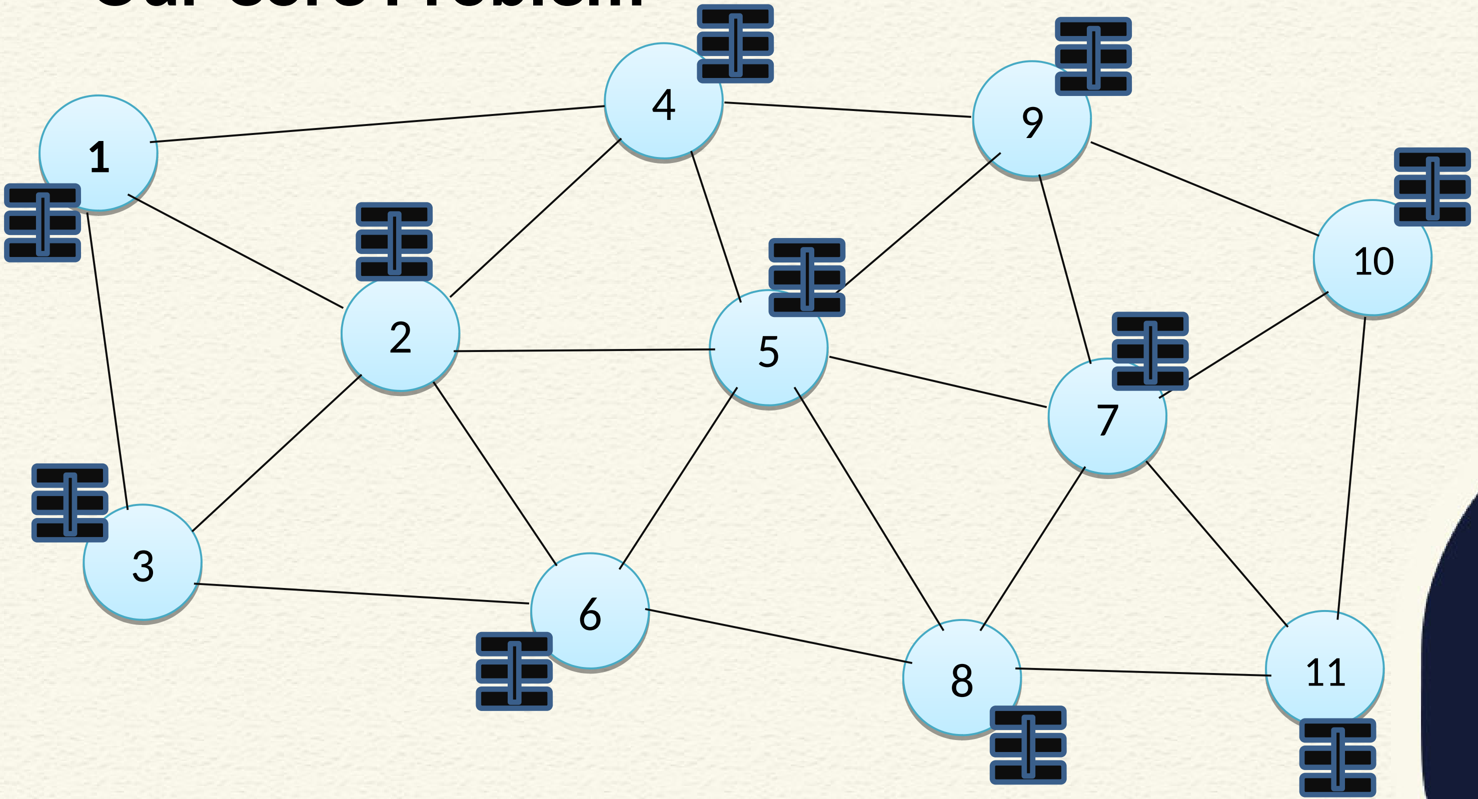
Crypto

Economic Models

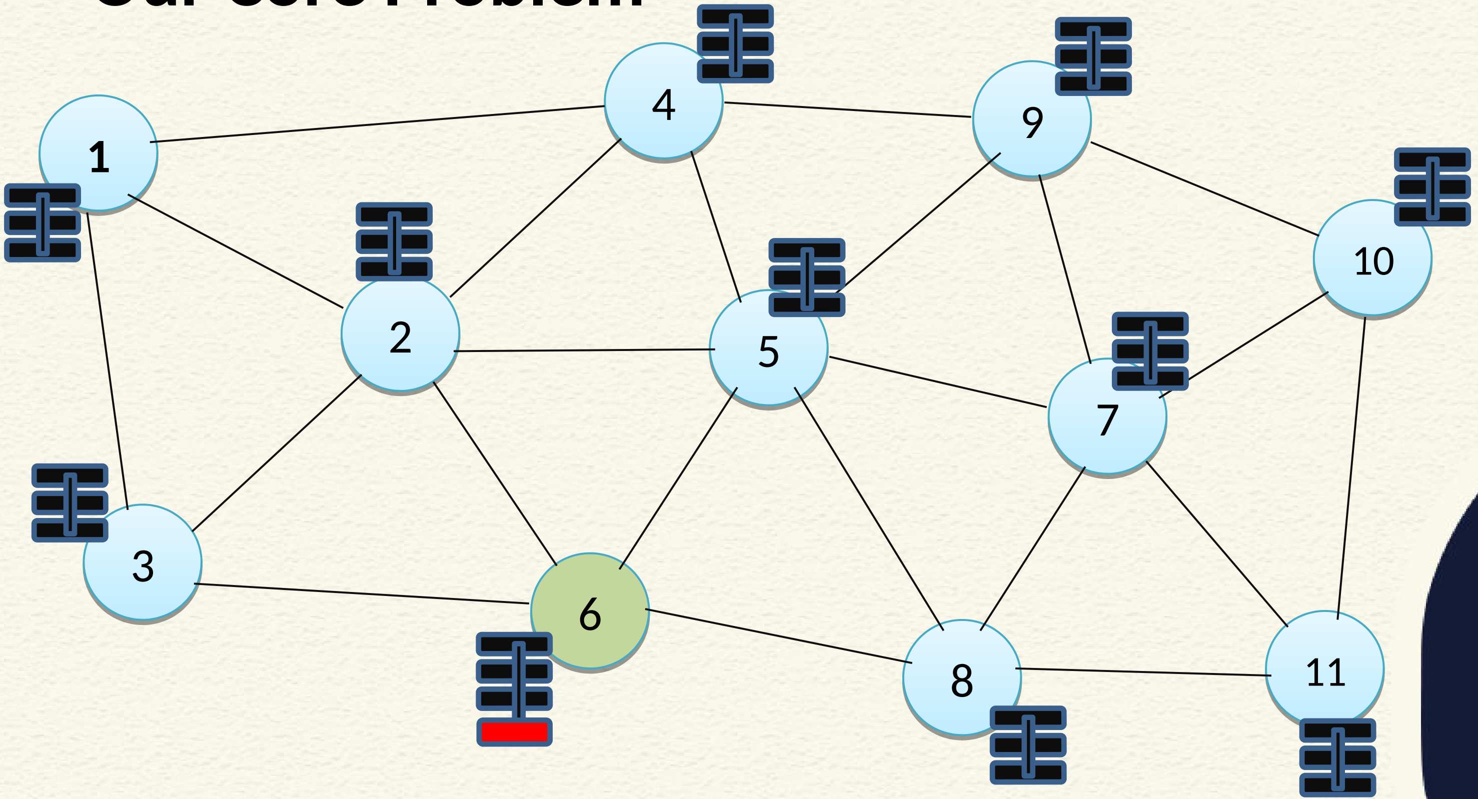
Our Core Problem



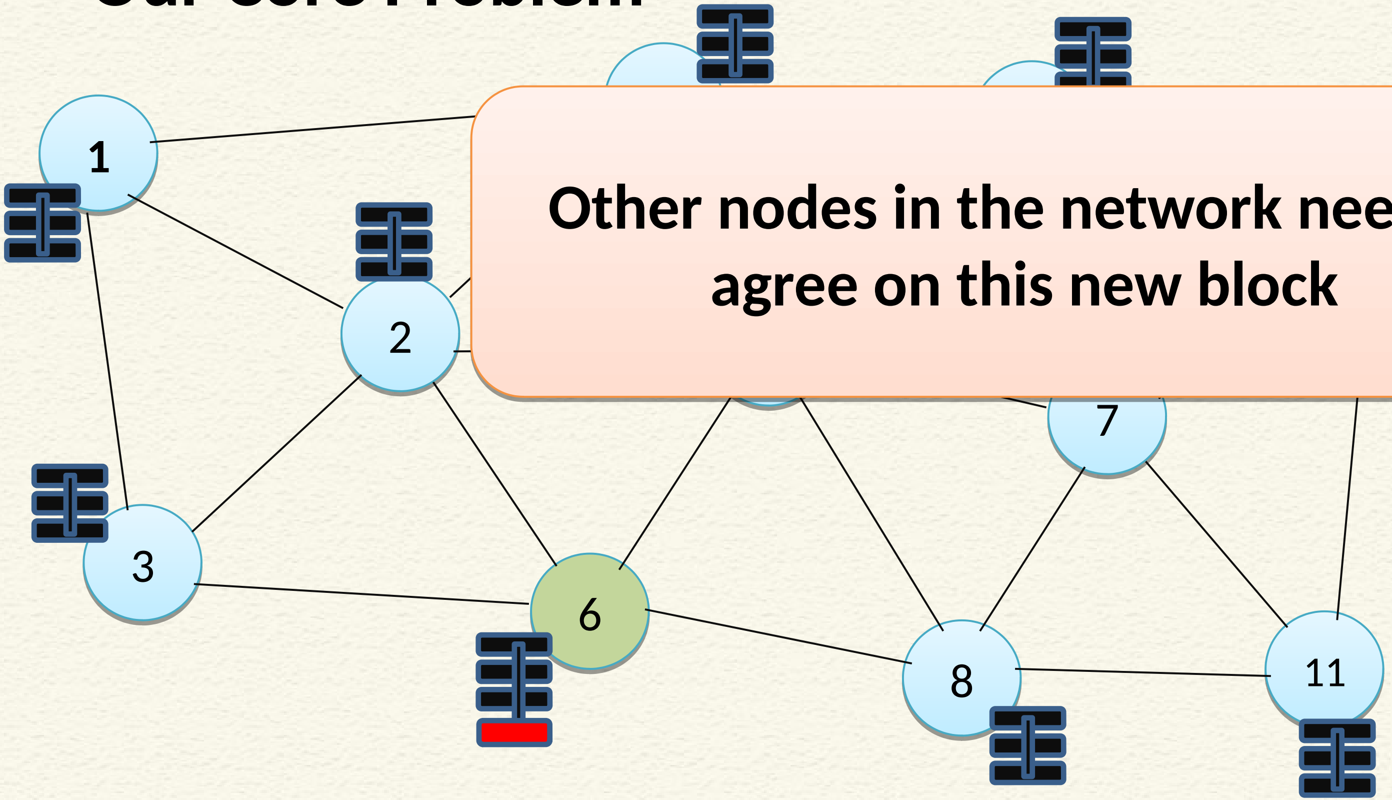
Our Core Problem



Our Core Problem

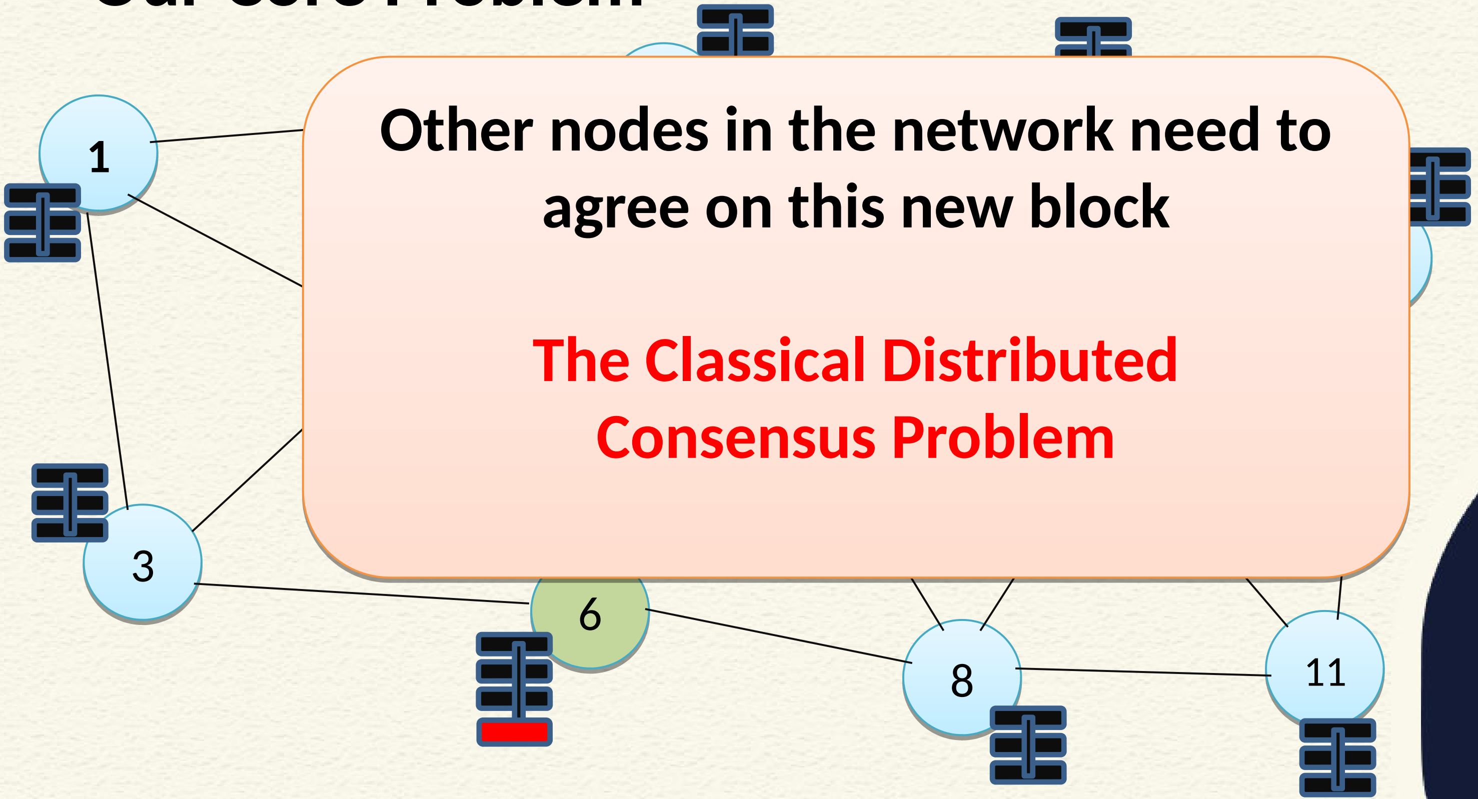


Our Core Problem



Other nodes in the network need to agree on this new block

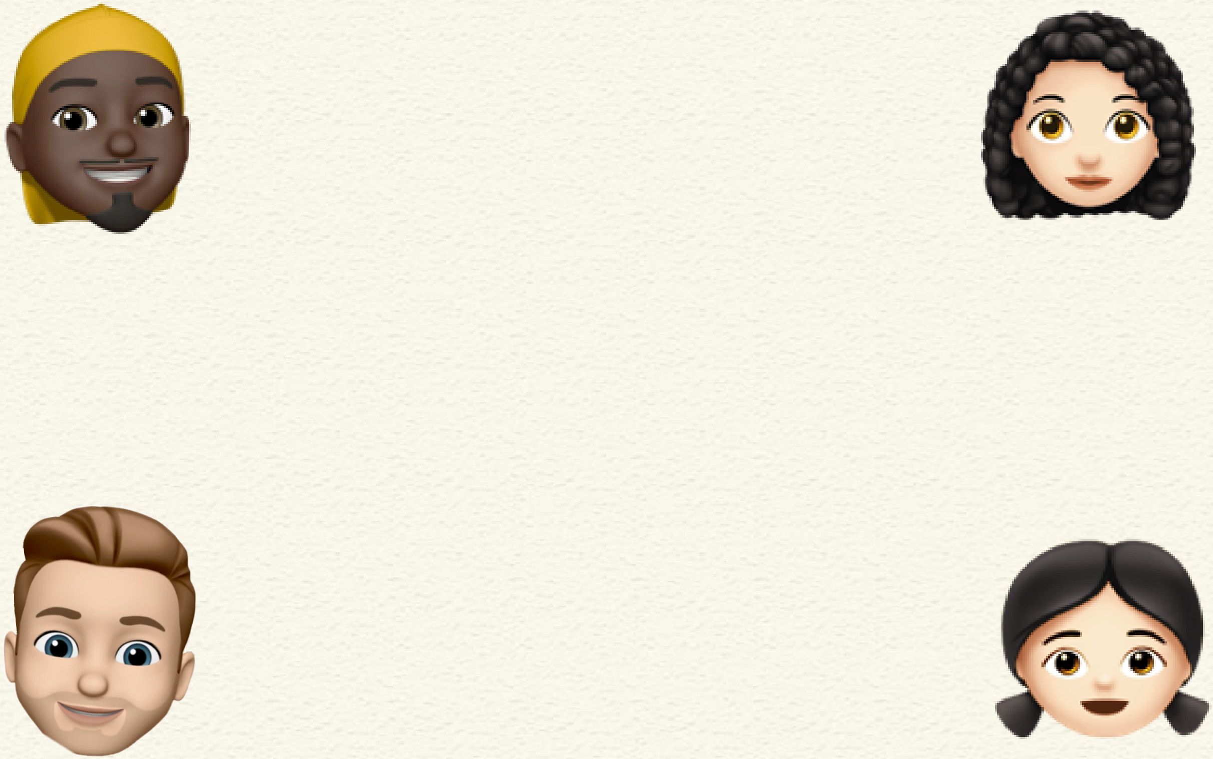
Our Core Problem



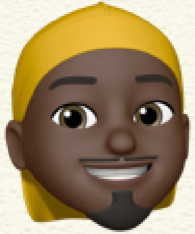
Other nodes in the network need to agree on this new block

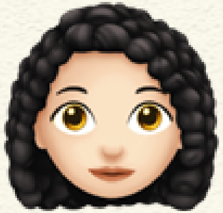
The Classical Distributed Consensus Problem

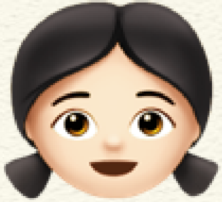
Distributed Consensus



Distributed Consensus





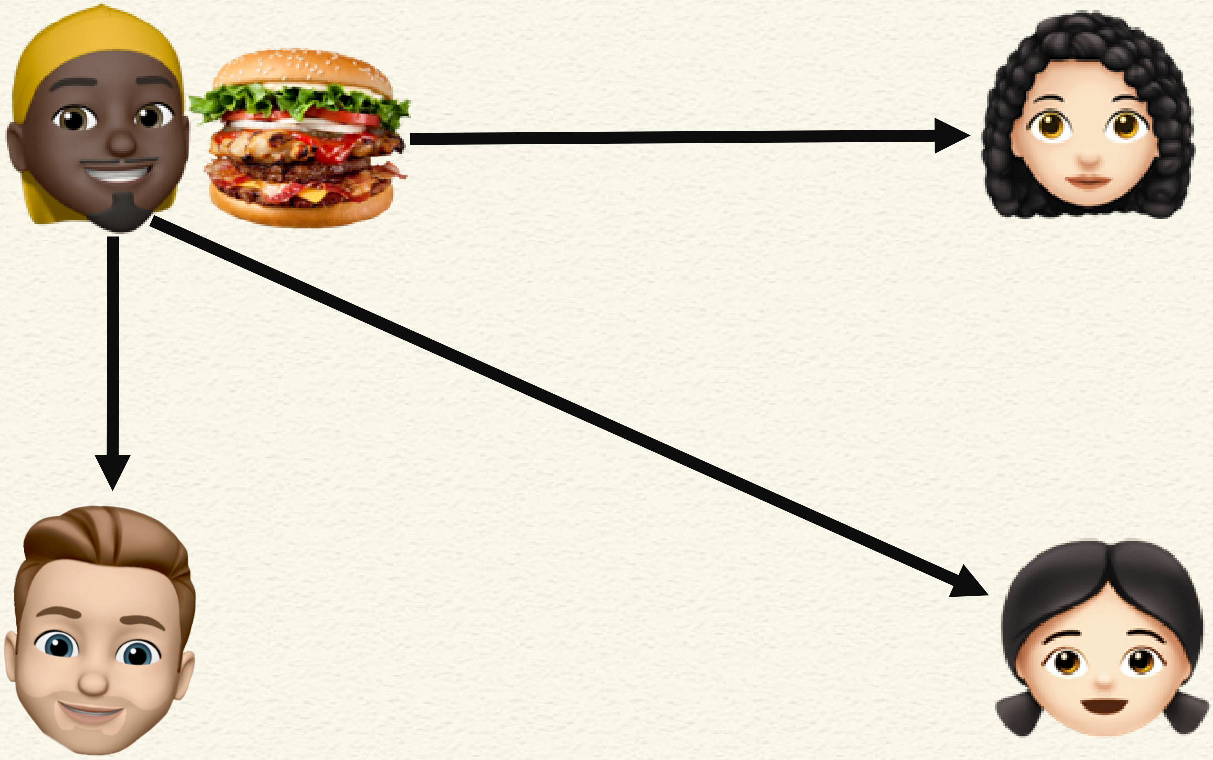


Distributed Consensus

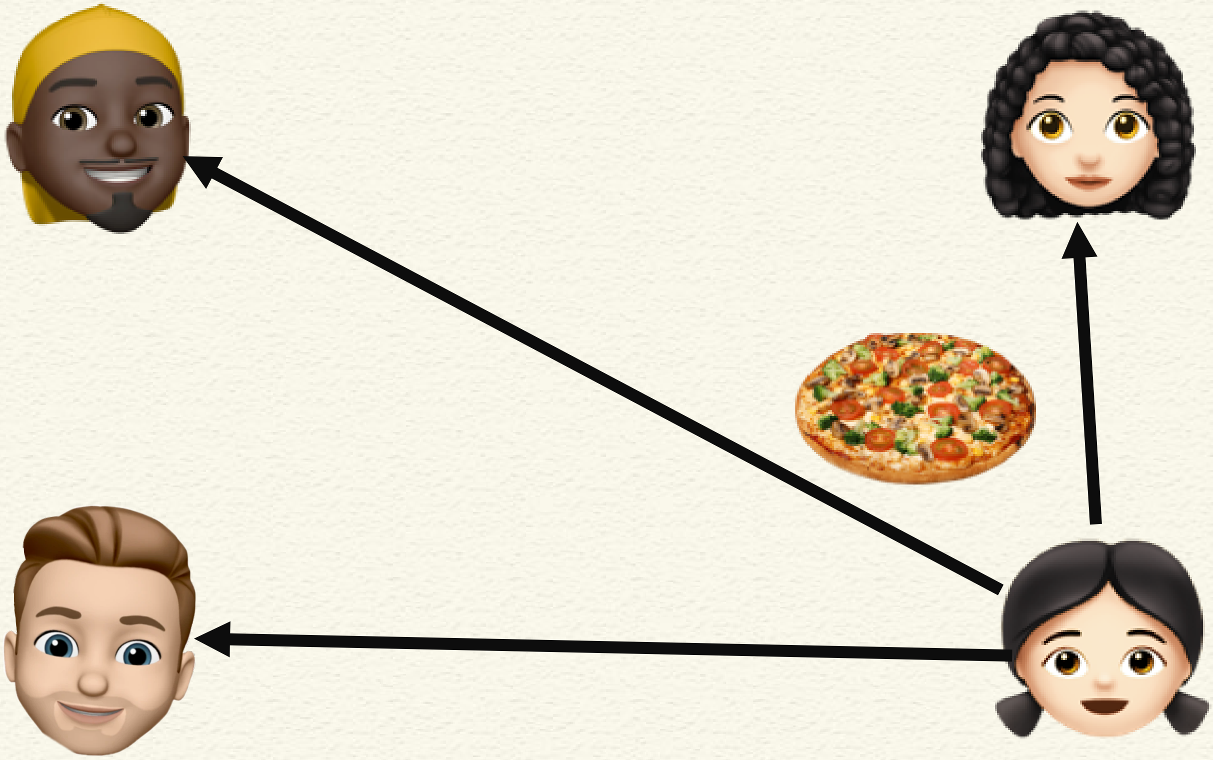
Distributed Consensus

How can we make this decision in a distributed way?

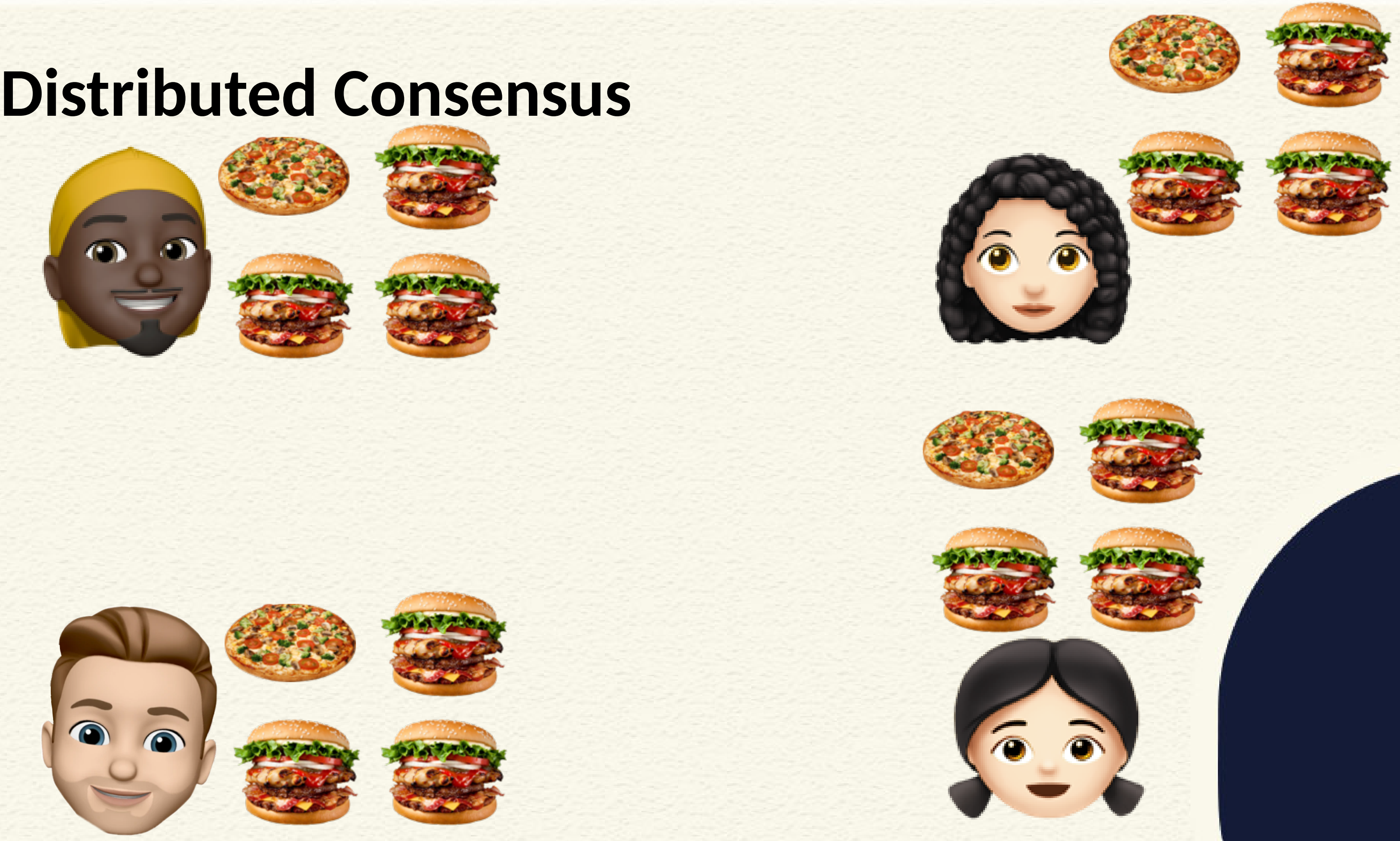
Distributed Consensus



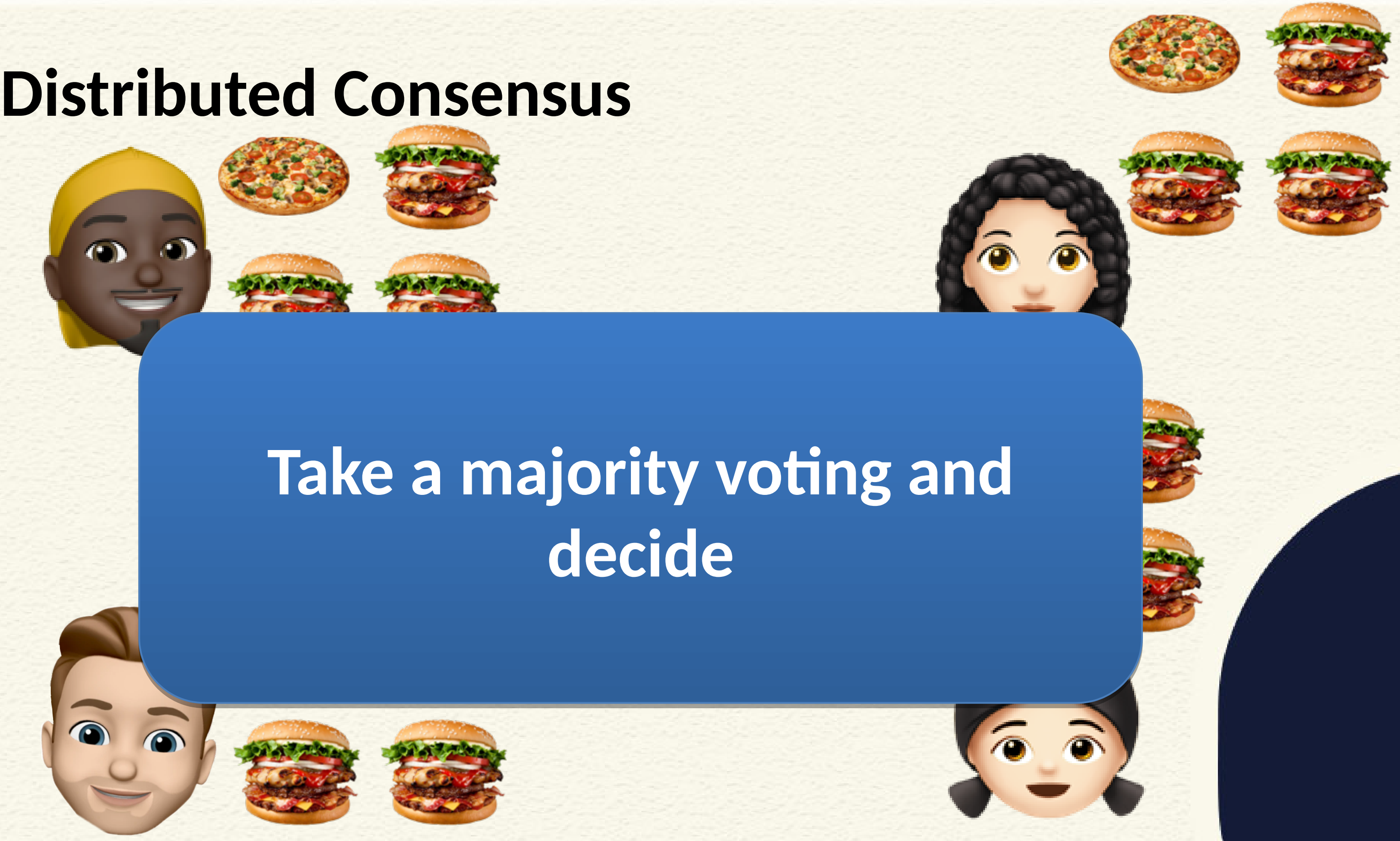
Distributed Consensus



Distributed Consensus

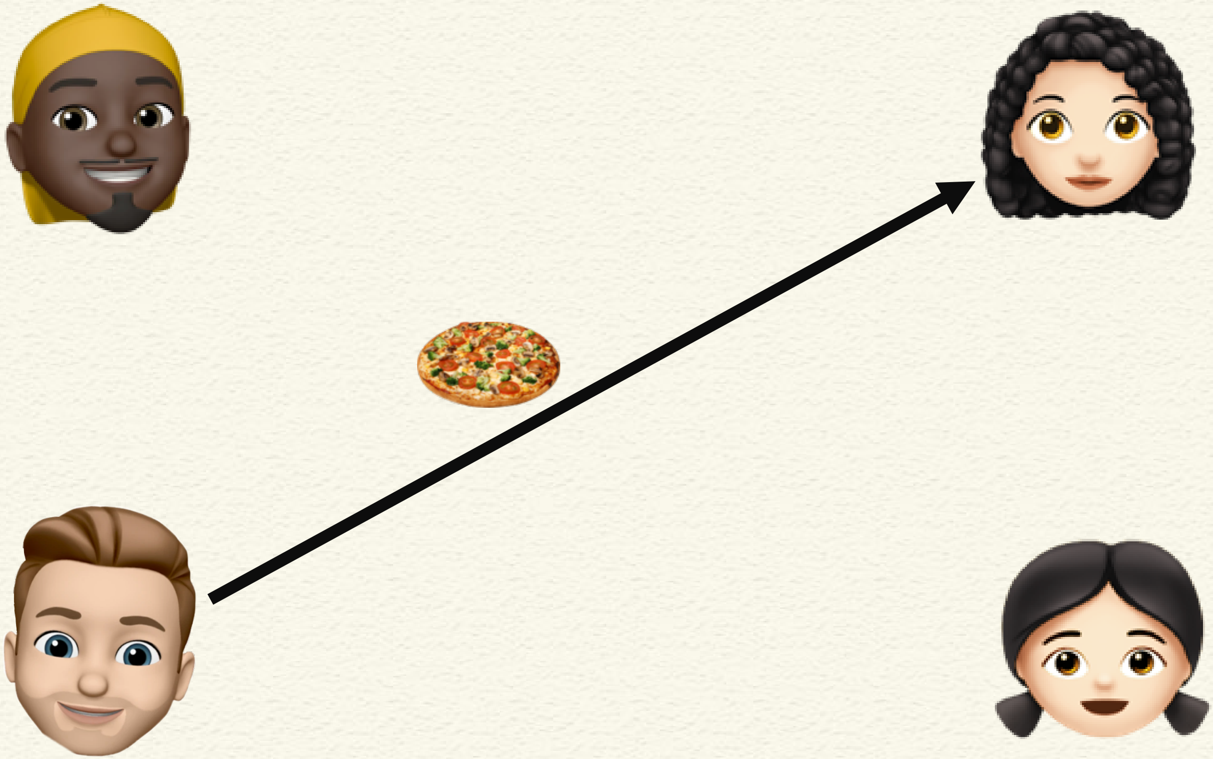


Distributed Consensus

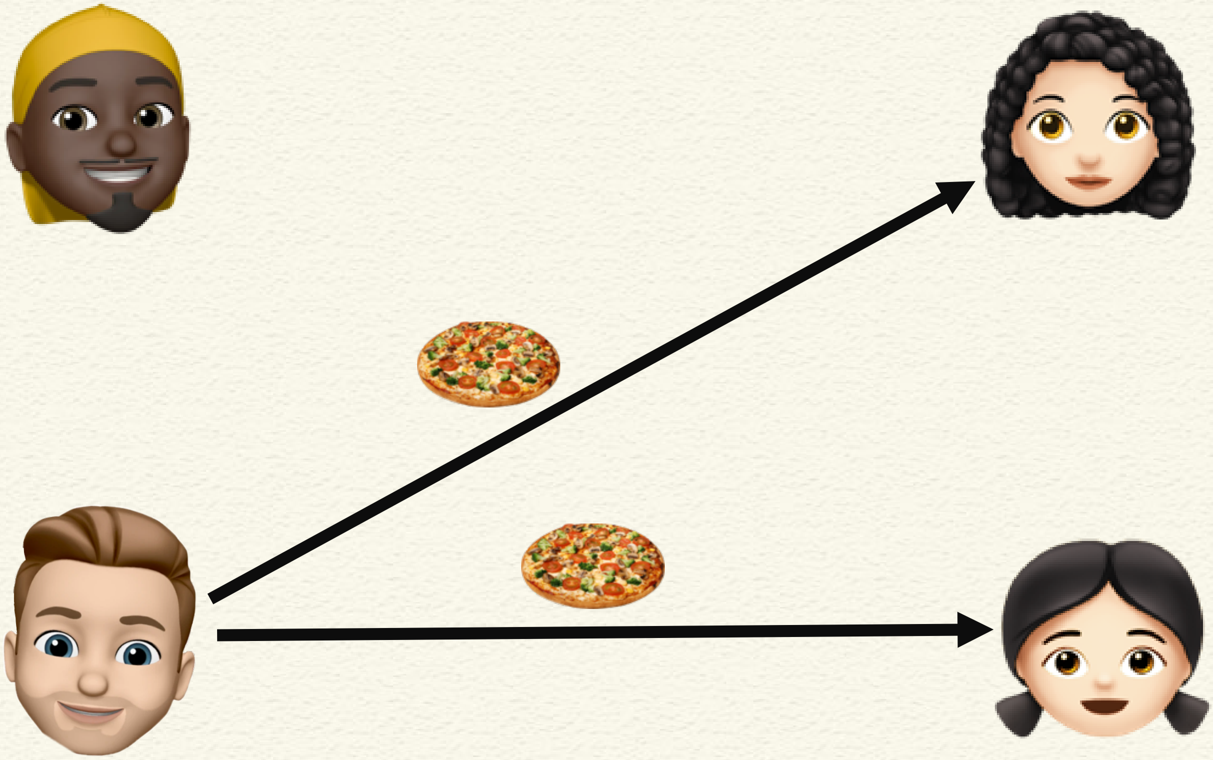


Take a majority voting and decide

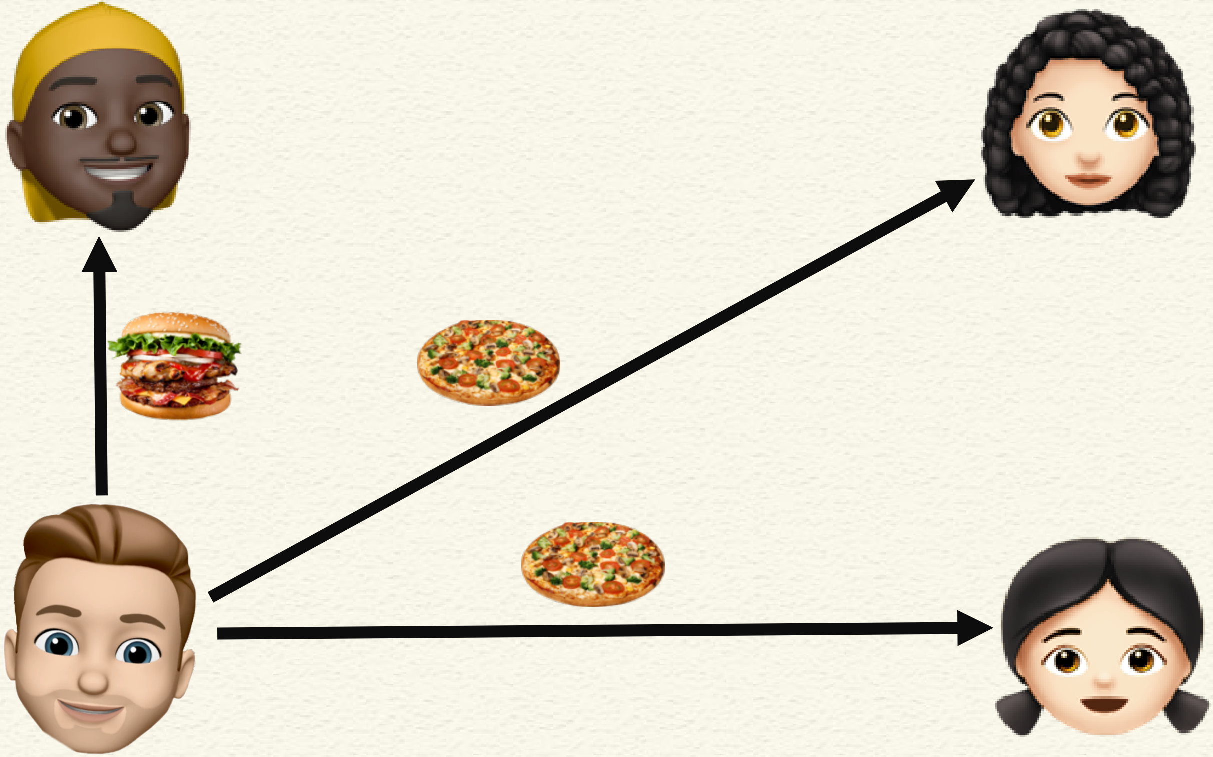
Distributed Consensus



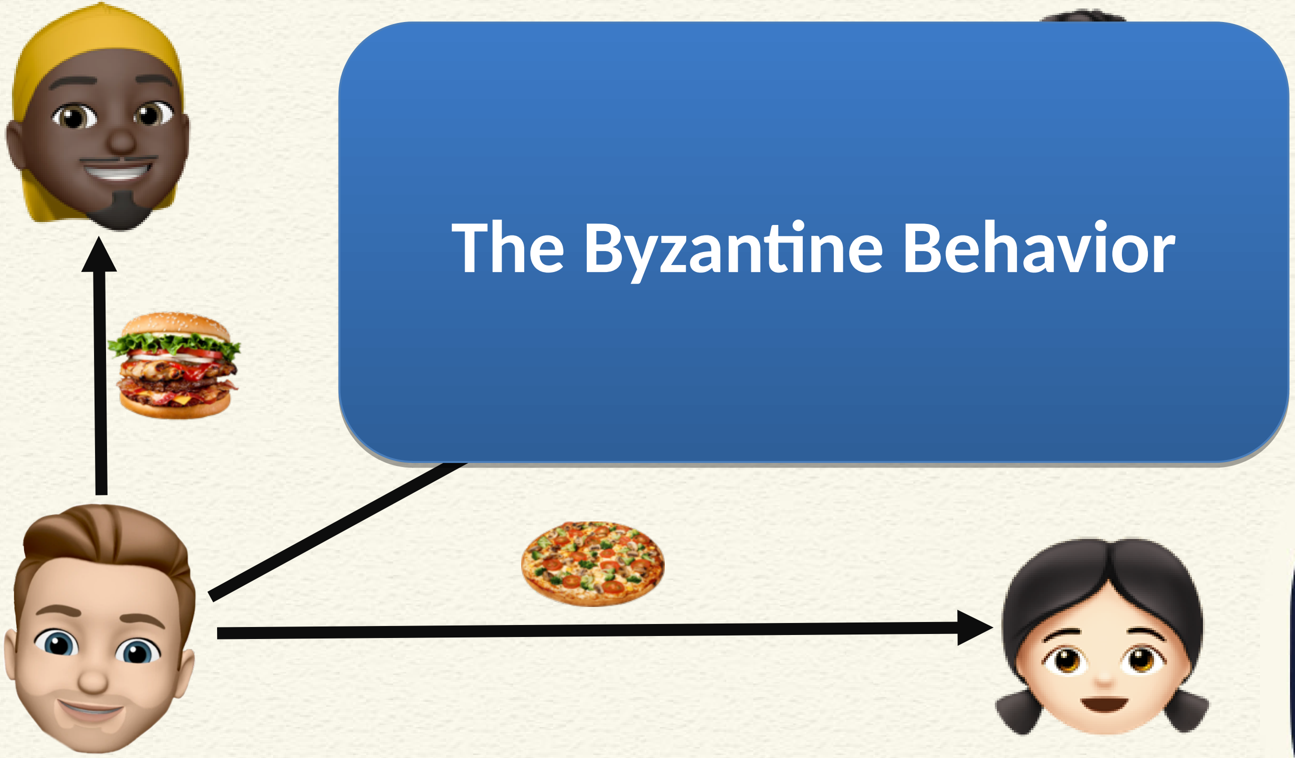
Distributed Consensus



Distributed Consensus



Distributed Consensus



The Byzantine Behavior

Distributed Consensus – The Literature

- 1985: **FLP Impossibility Theorem** – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault

Distributed Consensus – The Literature

- 1985: **FLP Impossibility Theorem** – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together

Distributed Consensus – The Literature

- 1985: **FLP Impossibility Theorem** – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together

Correct processes will yield the correct output

The output will be produced within a finite amount of time (eventual termination)

Distributed Consensus – The Literature

- 1985: **FLP Impossibility Theorem** – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together

- 1989: Lamport started talking about "Paxos"
  - Supports safety but not the liveness

Distributed Consensus – The Literature

- 1985: **FLP Impossibility Theorem** – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**<u>Safety</u>**" and "**<u>Liveness</u>**" together
- 1989: Lamport started talking about "Paxos"
  - Supports safety but not the liveness
- 1990's: Everyone were confused about the correctness of Paxos

Distributed Consensus – The Literature

- 1998: Paxos got published in ACM Transactions on Computer Systems
- 2001: FLP Impossibility paper wins Dijkstra Prize
  - People starts talking about Distributed Systems
- 2009: Zookeeper released
  - Service for managing distributed applications

Distributed Consensus – The Literature

- 2010's onward: Different types of consensus algorithms released
  - Multi-Paxos
  - Raft
  - Byzantine Fault Tolerance
  - PBFT
  - …

Conclusion

- Blockchain needs consensus at its back
- There is a vast literature on distributed consensus
- Can we use them for blockchain?

Thank you