NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 18: Permissionless Model and Open Consensus

CONCEPTS COVERED

- **Permissionless Model**
- **Consensus Requirements for Open Networks**
- **FLP Impossibility and Open Consensus**

KEYWORDS

- Permissionless Models
- Synchronous and Asynchronous
- Failures in distributed system
- Safety vs Liveness

Permissionless Model

- Open network
  - Anyone can join in the network and initiate transactions
  - Participants are free to leave the network, and can join later again

Permissionless Model

- Open network
  - Anyone can join in the network and initiate transactions
  - Participants are free to leave the network, and can join later again

- **Assumption: More than 50% of the participants are honest**
  - A society cannot run if majority of its participants are dishonest !!

Permissionless Blockchain

BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
TROYOZ 999 FINE COPPER MJB MONETARY METALS

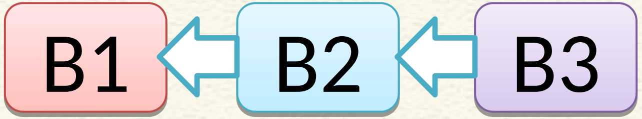
Consensus Challenges

- **Participants do not know others**
  - Cannot use message passing !!

- **Anyone can propose** a new block
  - Who is going to add the next block in the blockchain?

- The network is **asynchronous**
  - We do not have any global clock
  - A node may see the blocks in different orders

Consensus Challenges

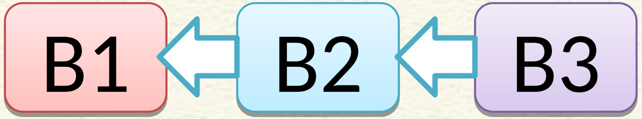


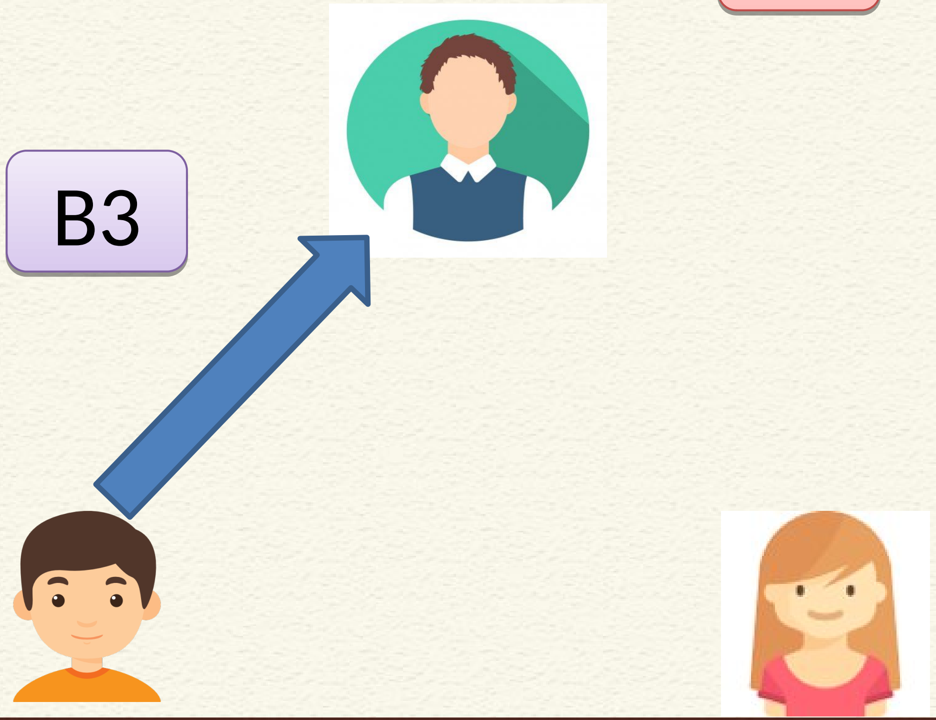
B1

B2

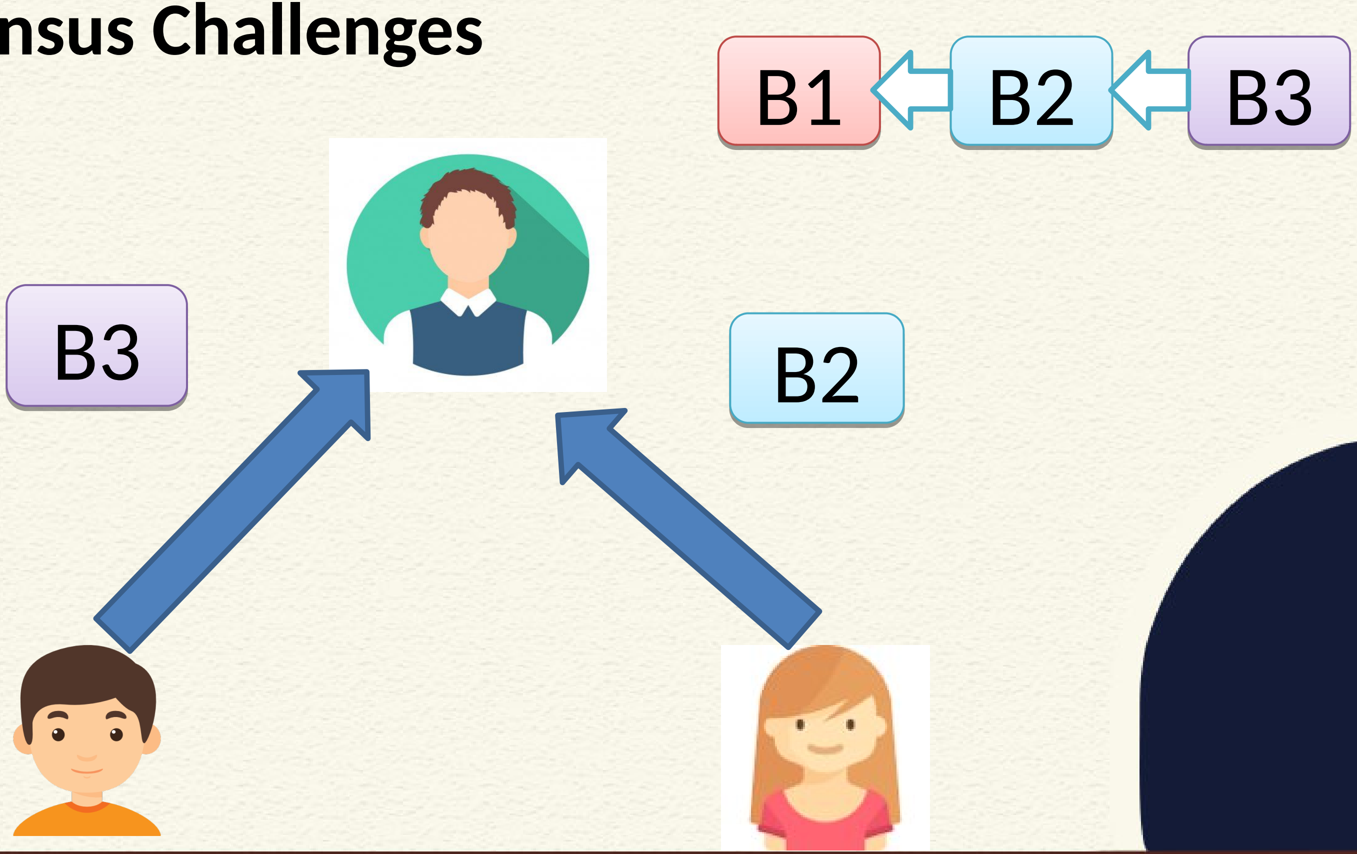
B3

Consensus Challenges





Consensus Challenges



Consensus Challenges

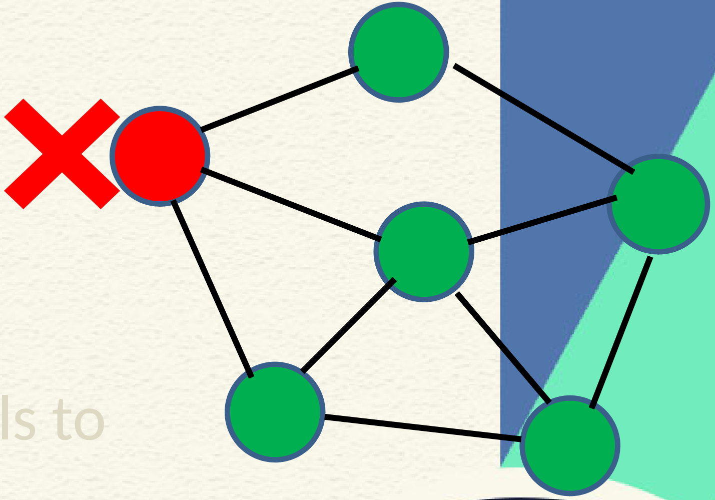
- Any types of **monopoly needs to be prevented**
  - A single user or a group of users should not gain the control – we don't trust anyone

Synchronous vs Asynchronous

- Synchronous vs Asynchronous Networks
  - **Synchronous**: I am sure that I'll get the message in real time (theoretically no delay or minimum delay)
  - **Asynchronous**: I am not sure whether and when the message will arrive

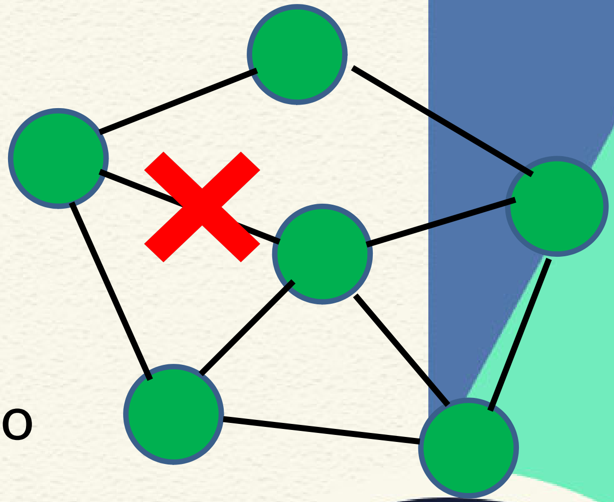
Failure in a Network

- **Crash Fault**: A node stops responding
- **Link Fault** (or Network Fault): A link fails to deliver the message
- **Byzantine Fault**: A node starts behaving maliciously



Failure in a Network

- **Crash Fault**: A node stops responding
- **Link Fault** (or Network Fault): A link fails to deliver the message
- **Byzantine Fault**: A node starts behaving maliciously

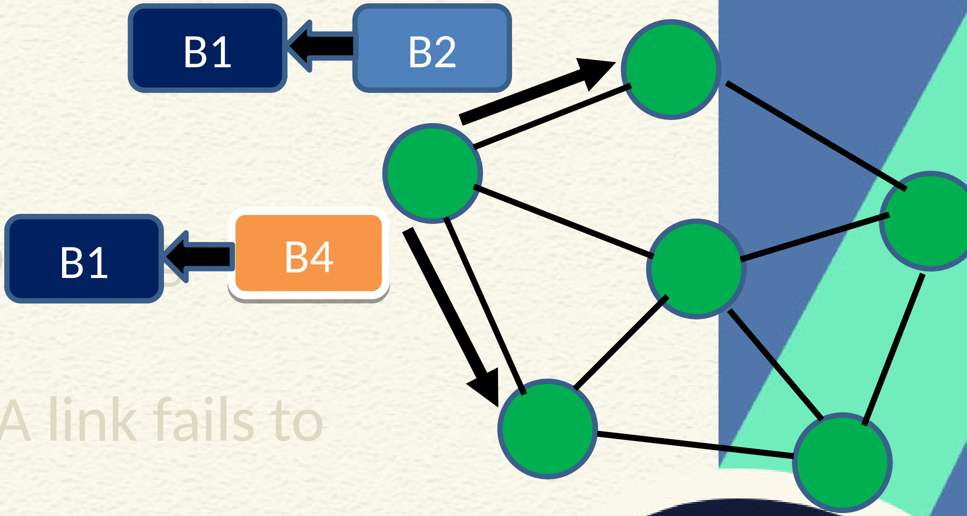


Failure in a Network

- **Crash Fault**: A node stops resp

- **Link Fault** (or Network Fault): A link fails to deliver the message

- **Byzantine Fault**: A node starts behaving maliciously



Remember FLP Impossibility?

- **The Impossibility Theorem**: Consensus is not possible in a perfect asynchronous network even with a single crash failure
  - Cannot ensure safety and liveness simultaneously

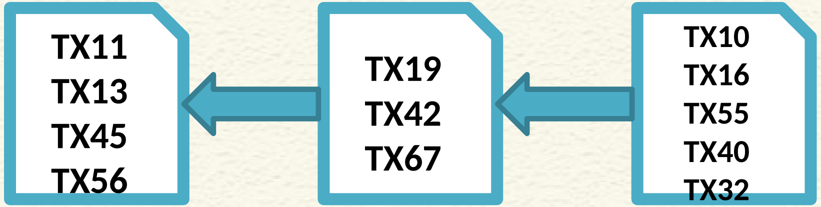
The Safety vs Liveness Dilemma

The Nakamoto Consensus (Proof of Work)

Liveness is more important than Safety

Immediate focus is on liveness with a minimum safety guarantee, full safety will be ensured eventually

The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

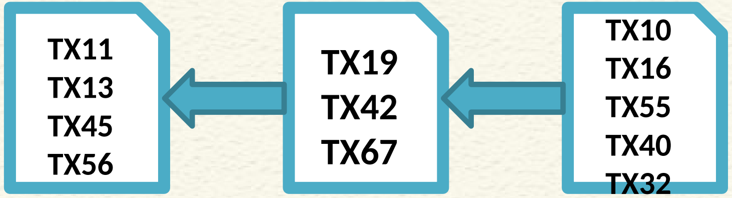
TX10
TX16
TX55
TX40
TX32

Miner 1

Miner 2

Miner 3

The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

TX10
TX16
TX55
TX40
TX32

Bitcoin Unconfirmed TX : https://www.blockchain.com/btc/unconfirmed-transactions

Unconfirmed TX

Miner 1

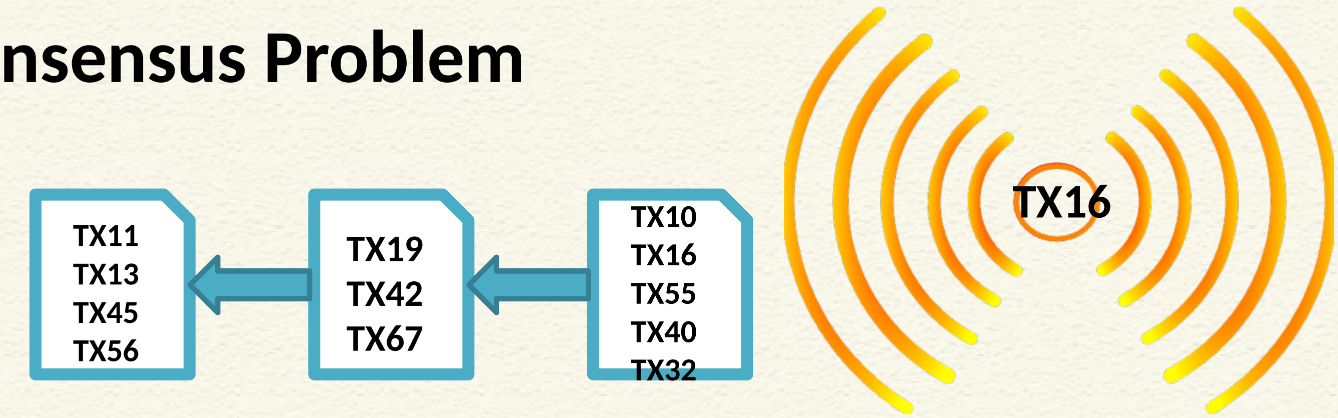
Unconfirmed TX

Miner 2

Unconfirmed TX

Miner 3

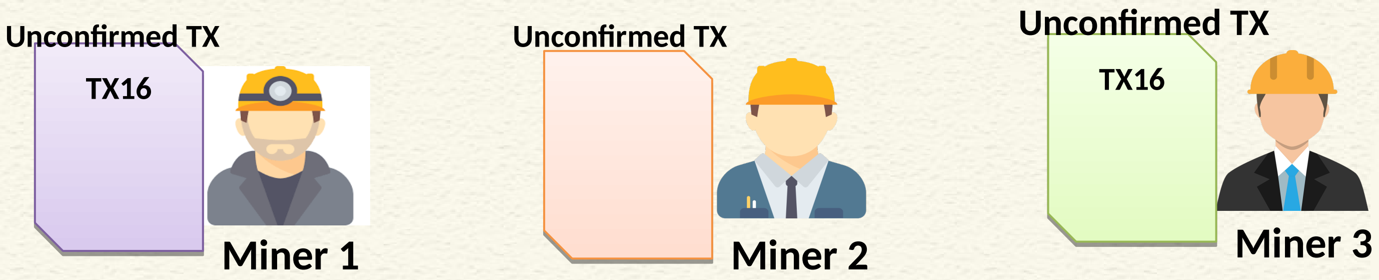
The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

TX10
TX16
TX55
TX40
TX32



Unconfirmed TX

TX16

Miner 1

Unconfirmed TX

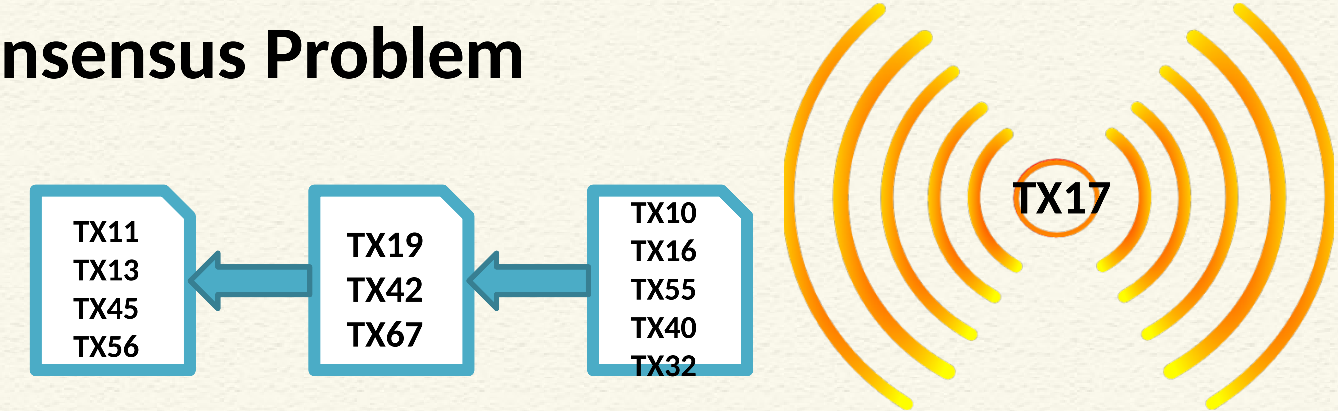
Miner 2

Unconfirmed TX

TX16

Miner 3

The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

TX10
TX16
TX55
TX40
TX32

TX17

Unconfirmed TX

TX16
TX17

Miner 1

Unconfirmed TX

TX17

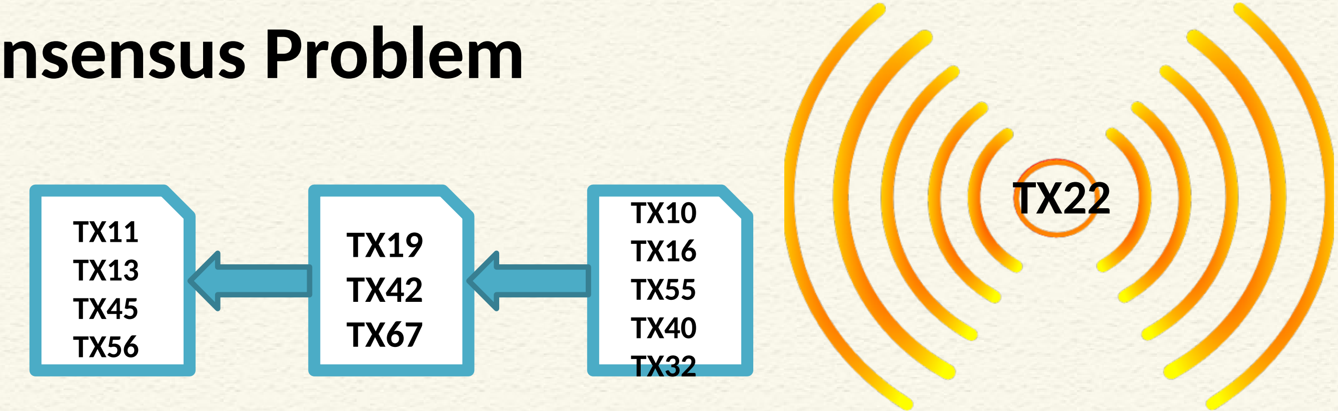
Miner 2

Unconfirmed TX

TX16
TX17

Miner 3

The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

TX10
TX16
TX55
TX40
TX32

TX22

Unconfirmed TX

TX16
TX17

Miner 1

Unconfirmed TX

TX17
TX22

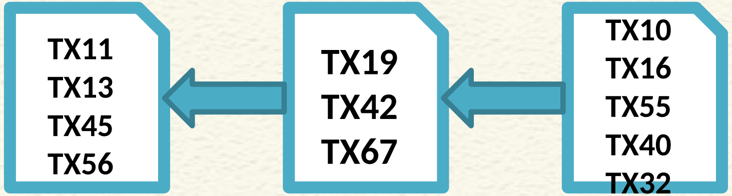
Miner 2

Unconfirmed TX

TX16
TX17
TX22

Miner 3

The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

TX10
TX16
TX55
TX40
TX32

Unconfirmed TX

TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

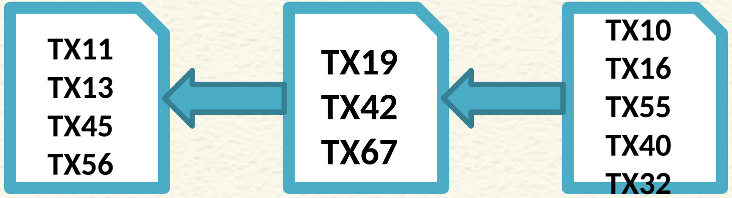
Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

The Consensus Problem



TX11
TX13
TX45
TX56

TX19
TX42
TX67

TX10
TX16
TX55
TX40
TX32

Which one would be the next block?

Unconfirmed TX

TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

Conclusion

- Message passing is not possible over an open network

- FLP Impossibility: Safety vs Liveness

- Priority over Liveness
  - More suitable for Blockchain? Include the correct block – whether it is final, think later

- Different miners see different blocks
  - Which one to add?

Thank
you