NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 20: Limitations of PoW: Forking and Security

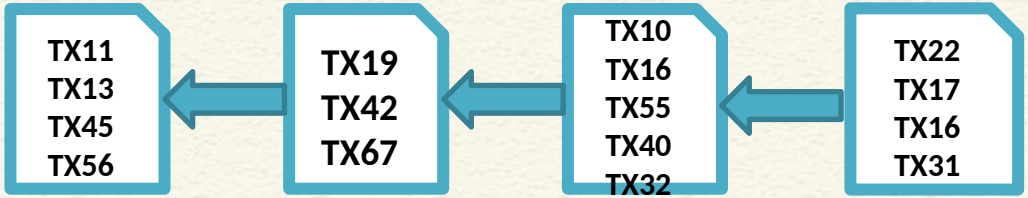
CONCEPTS COVERED

- PoW Forks
- Attacks on PoW
- The Monopoly Problem

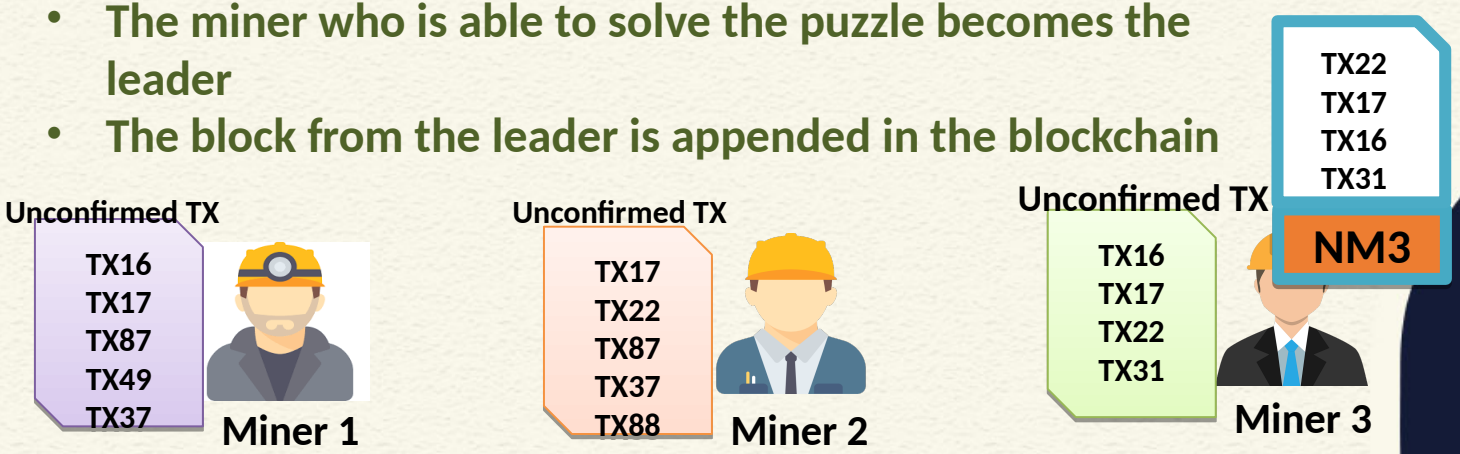
KEYWORDS

- Forks
- Security
- 51% attack

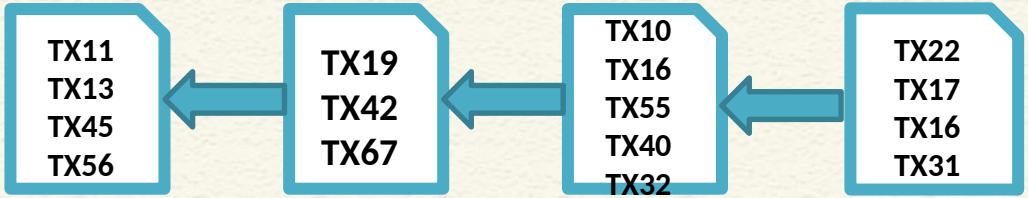
PoW: Mining a New Block



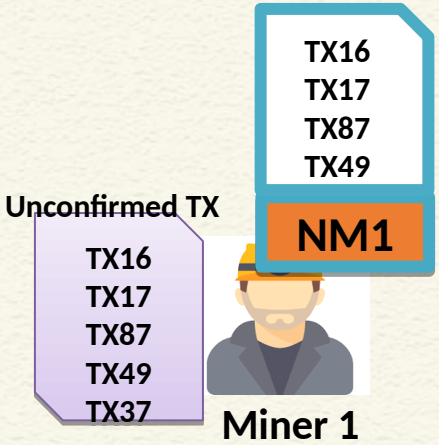
- The miner who is able to solve the puzzle becomes the leader
- The block from the leader is appended in the blockchain

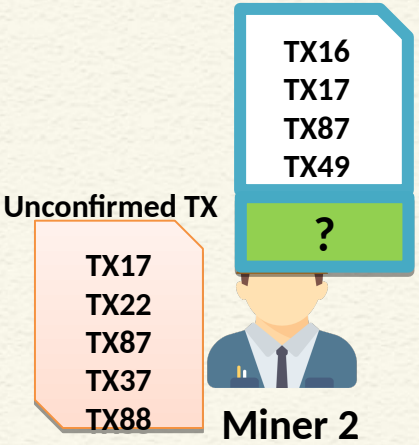


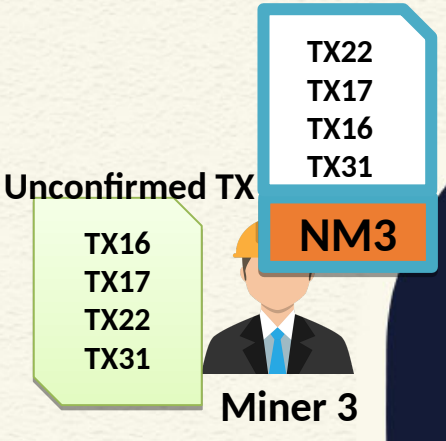
PoW: Mining a New Block



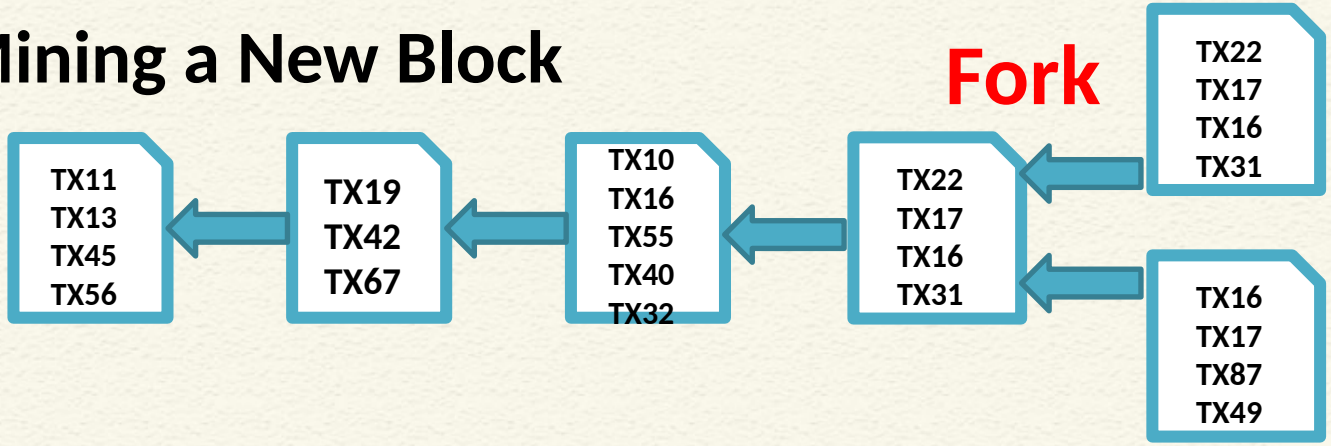
What if two miners solve the puzzle simultaneously?







PoW: Mining a New Block



Unconfirmed TX

TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

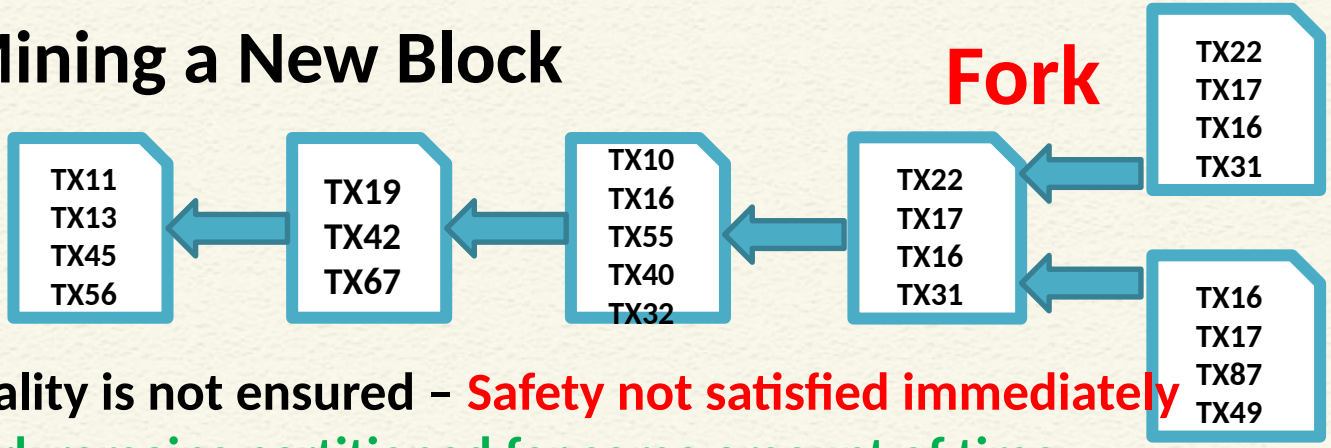
Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

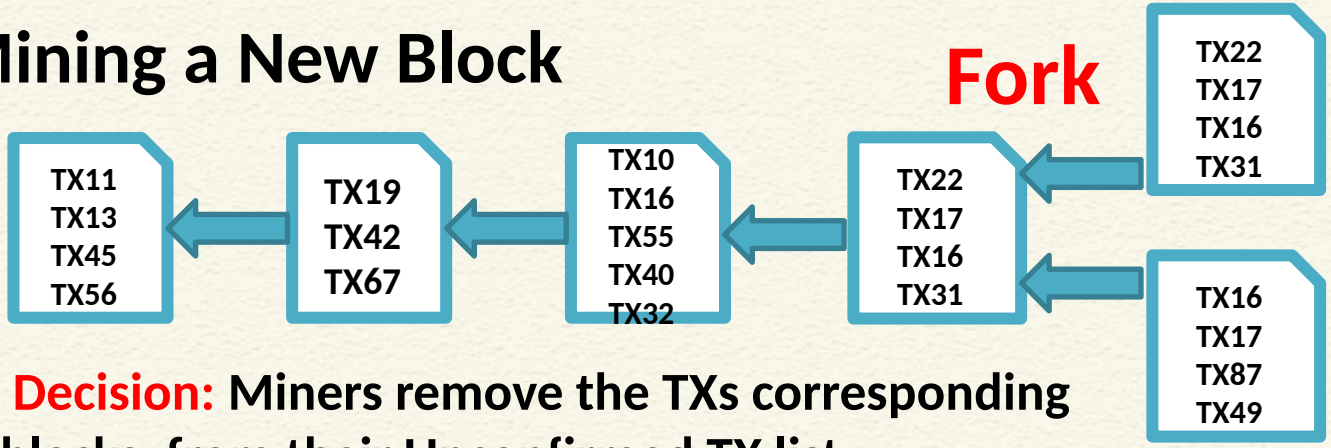
PoW: Mining a New Block



Consensus finality is not ensured – Safety not satisfied immediately

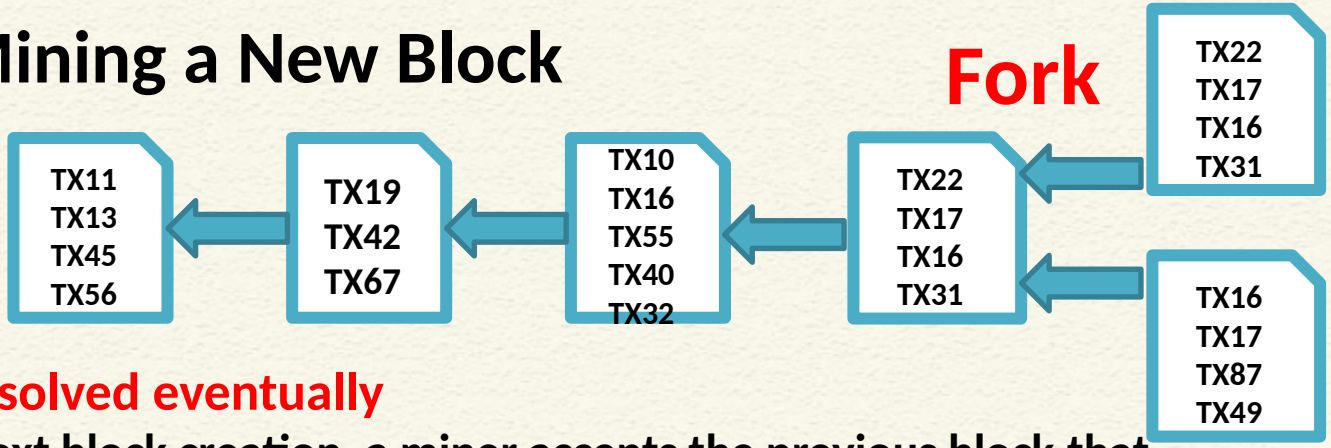
- **The network remains partitioned for some amount of time**

PoW: Mining a New Block



Momentary Decision: Miners remove the TXs corresponding to both the blocks, from their Unconfirmed TX list

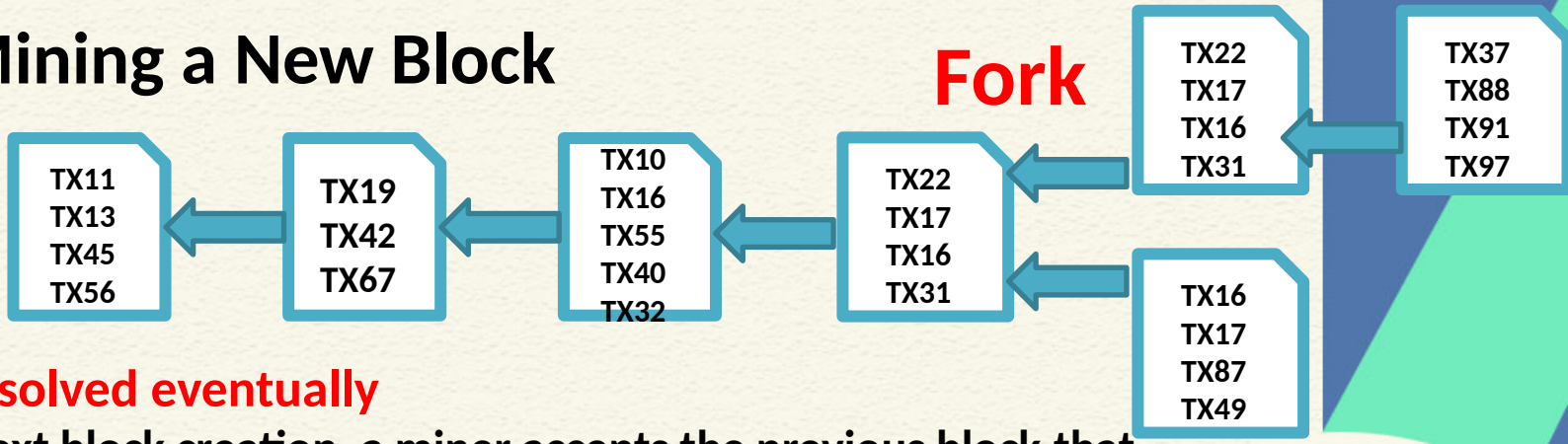
PoW: Mining a New Block



Forks are resolved eventually

- For the next block creation, a miner accepts the previous block that it hears from the majority of the neighbor

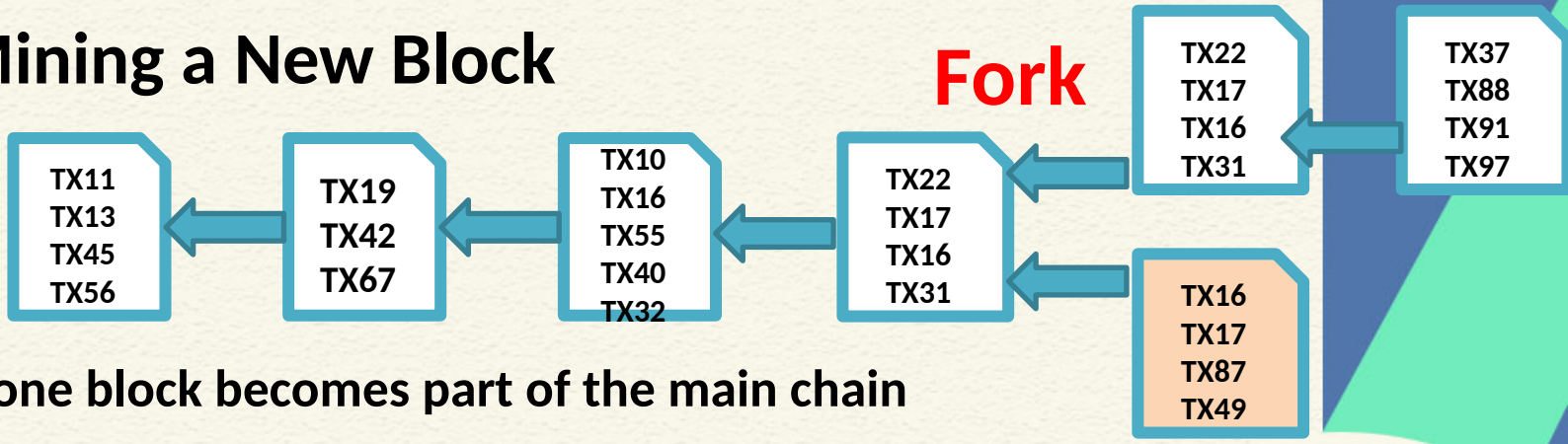
PoW: Mining a New Block



Forks are resolved eventually

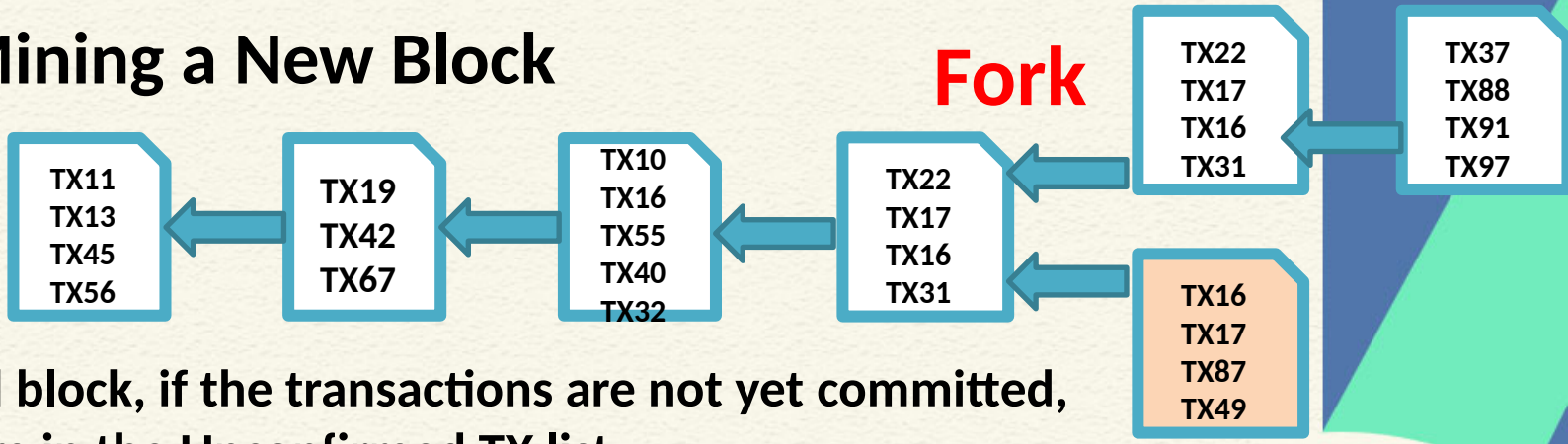
- For the next block creation, a miner accepts the previous block that it hears from the majority of the neighbor

PoW: Mining a New Block



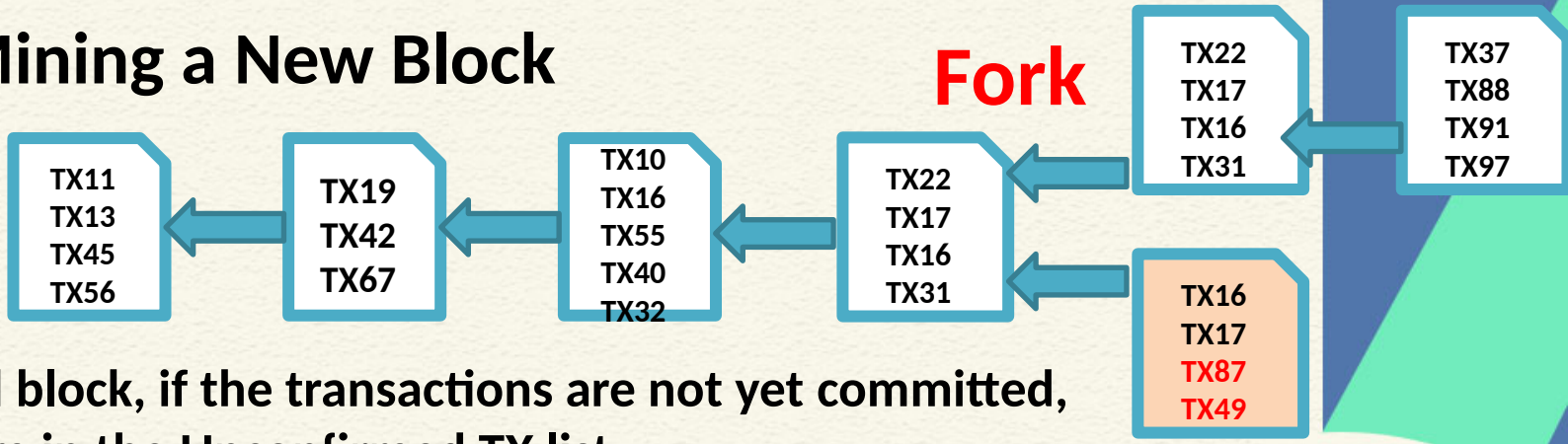
Eventually, one block becomes part of the main chain

PoW: Mining a New Block

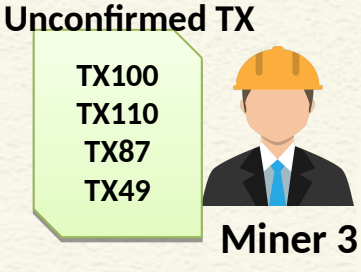


For a forked block, if the transactions are not yet committed, include them in the Unconfirmed TX list

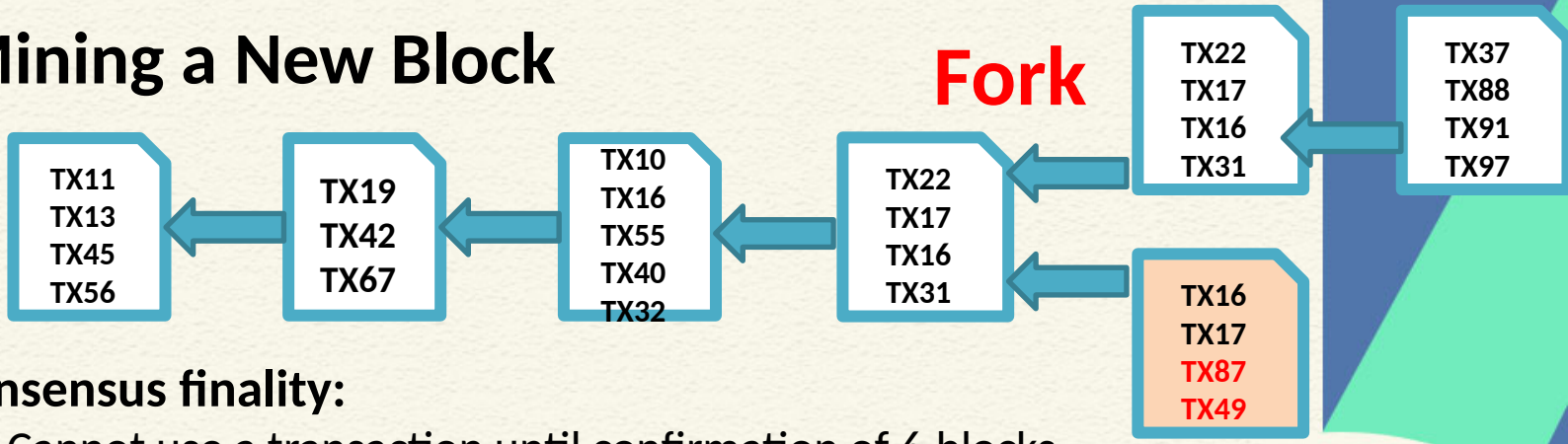
PoW: Mining a New Block



For a forked block, if the transactions are not yet committed, include them in the Unconfirmed TX list



PoW: Mining a New Block



Eventual consensus finality:

- (Bitcoin) Cannot use a transaction until confirmation of 6 blocks – ensured through scripts

Security Measures for PoW

- **Sybil Attacks**
  - Attacker attempts to fill the network with the clients under its control
  - Create multiple identities (multiple public key addresses) to control the network – refuse to relay valid blocks or relay attacked blocks
  - **Solution:** Diversify the connections – Bitcoin allows one outbound connection to per /16 block of IP addresses – cannot make both 202.141.81.2/16 and 202.141.80.18/16 as the peers

Security Measures for PoW

- **Denial of Service (DoS)**
  - Send a lot of data to a node – block the processing power
  - **Solution:** Limit forwarding of blocks, disconnect a peer that sends too many transactions

Breaking PoW

- Bitcoin PoW is **computationally difficult** to break, but not **impossible**

- Attackers can deploy high power servers to do more work than the total work of the blockchain

Breaking PoW

- A known case of successful double-spending
  - (November 2013) “it was discovered that the GHash.io mining pool appeared to be engaging in repeated payment fraud against *BetCoin Dice*, a gambling site” [Source: https://en.bitcoin.it/]

The Monopoly Problem

- PoW depends on the computing resources available to a miner
  - Miners having more resources have more probability to complete the work

The Monopoly Problem

- Monopoly can increase over time (*Tragedy of the Commons*)
  - Miners will get less reward over time
  - Users will get discouraged to join as the miner
  - Few miners with large computing resources may get control over the network

The Monopoly Problem

- **51% Attack:** A group of miners control more than 50% of the hash rate of the network
  - Hypothetical as of now for Bitcoin (as the network is large), but not impossible (happened for Kryptom – Ethereum based blockchain, in August, 2016)

Conclusion

- PoW may result a fork – consensus finality is not ensured
- The security of PoW is ensured with the condition that attackers cannot gain more than 50% of the hash power


Thank you