NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 16: Blockchain Elements - IV

CONCEPTS COVERED

- Joining a Bitcoin Network
- Transaction Flooding
- Block Mining
- Block Propagation
- Forking and Propagation of Longest Chain

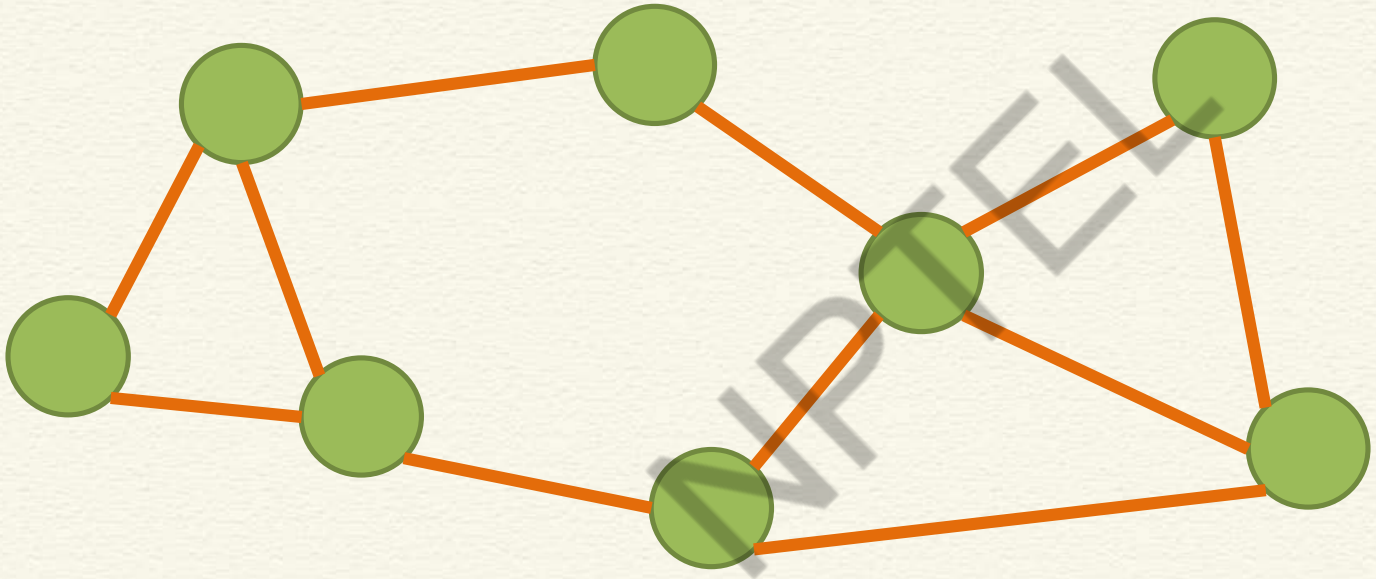
KEYWORDS

- Bitcoin Node
- Transaction Flooding
- Block Reward
- Block Propagation
- Fork in Blockchain

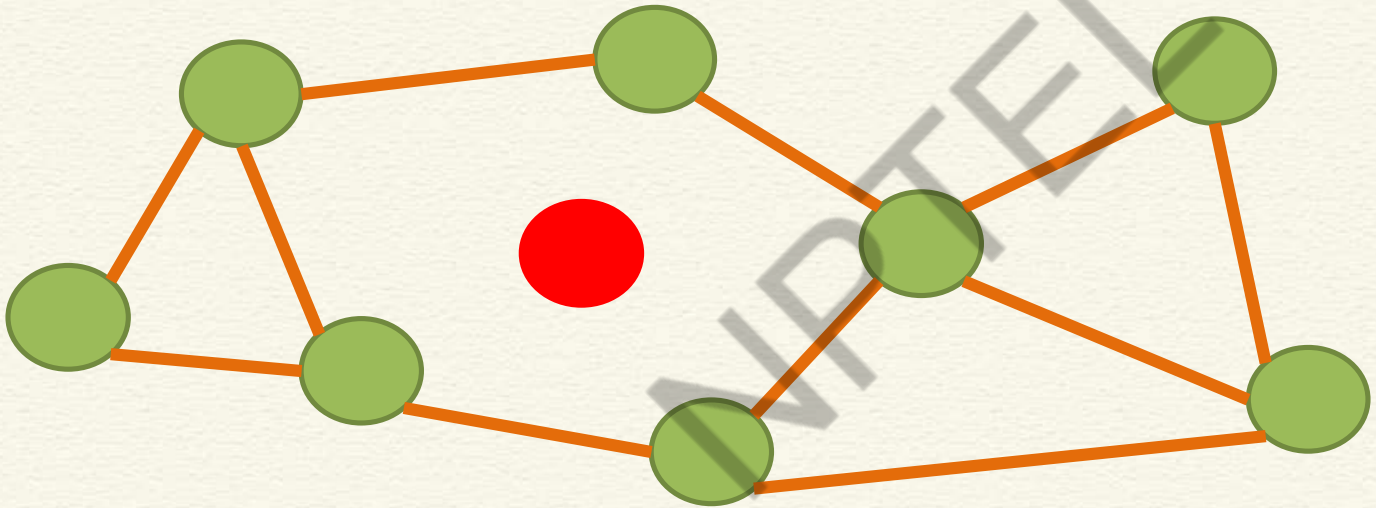
Bitcoin P2P Network

- An ad-hoc network with random topology, Bitcoin protocol runs over TCP
- All nodes (users) in the bitcoin network are treated equally
- New nodes can join any time, non-responding nodes are removed after 3 hours

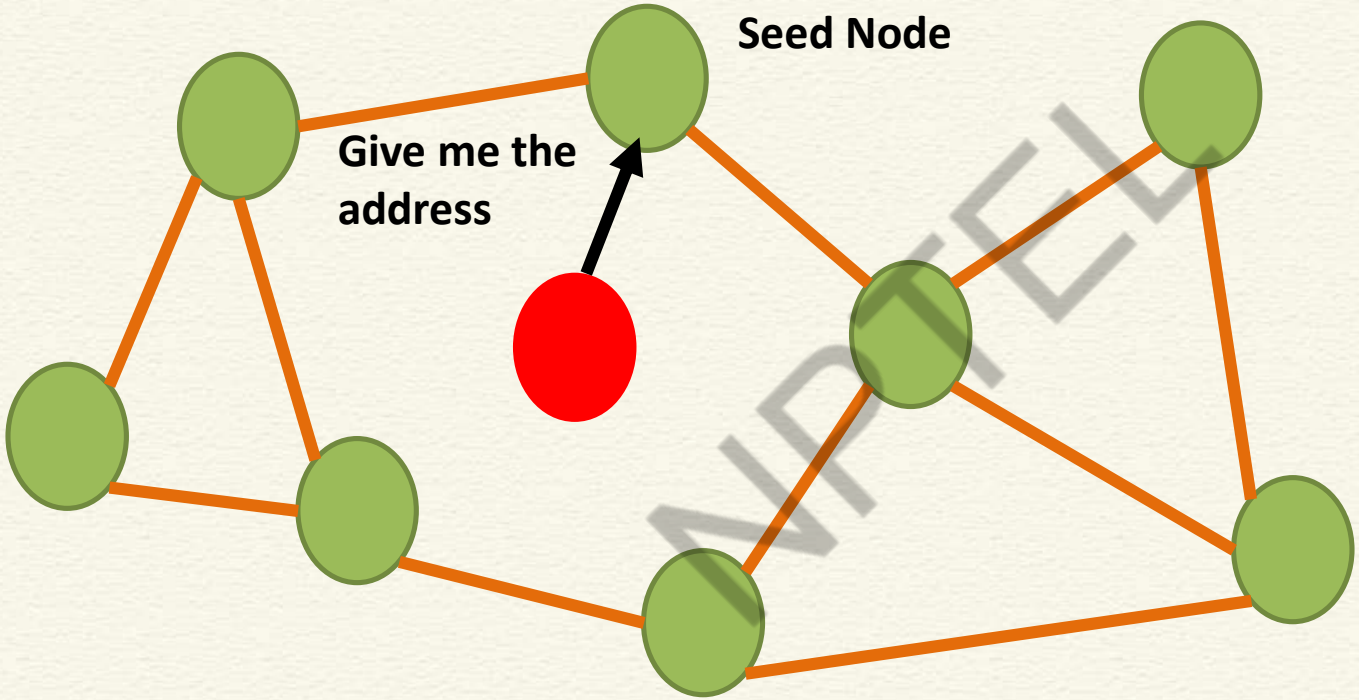
Joining in a Bitcoin P2P Network



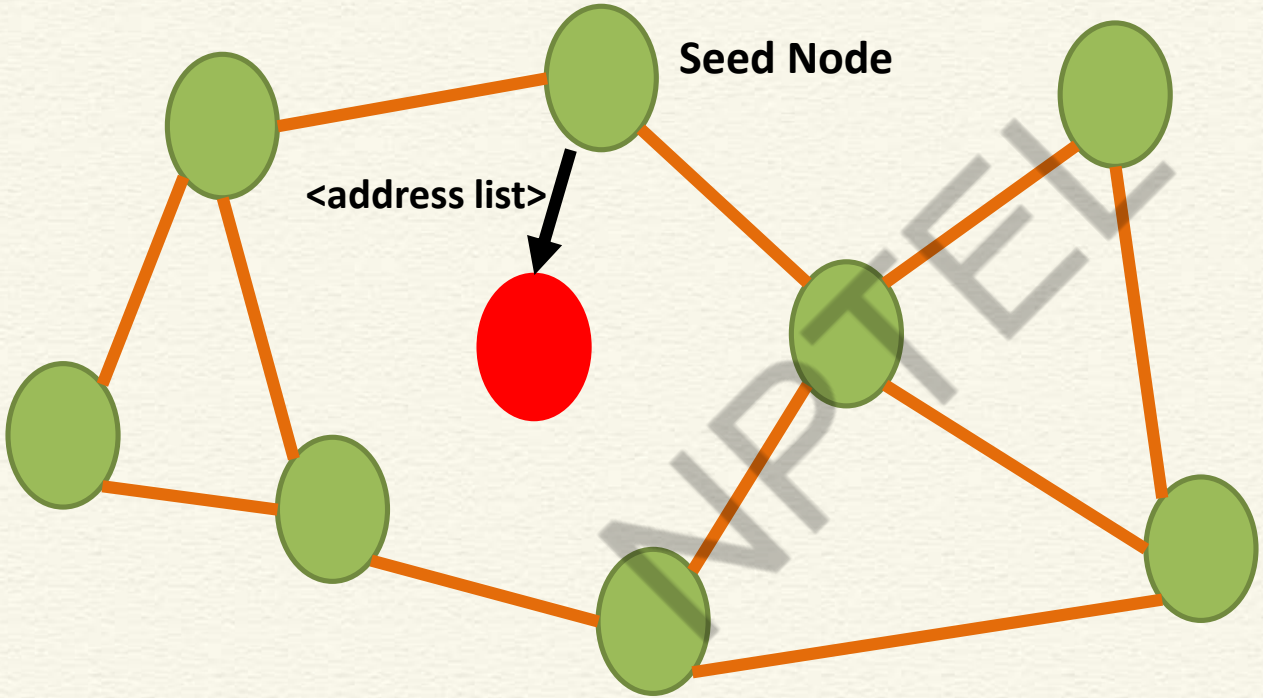
Joining in a Bitcoin P2P Network



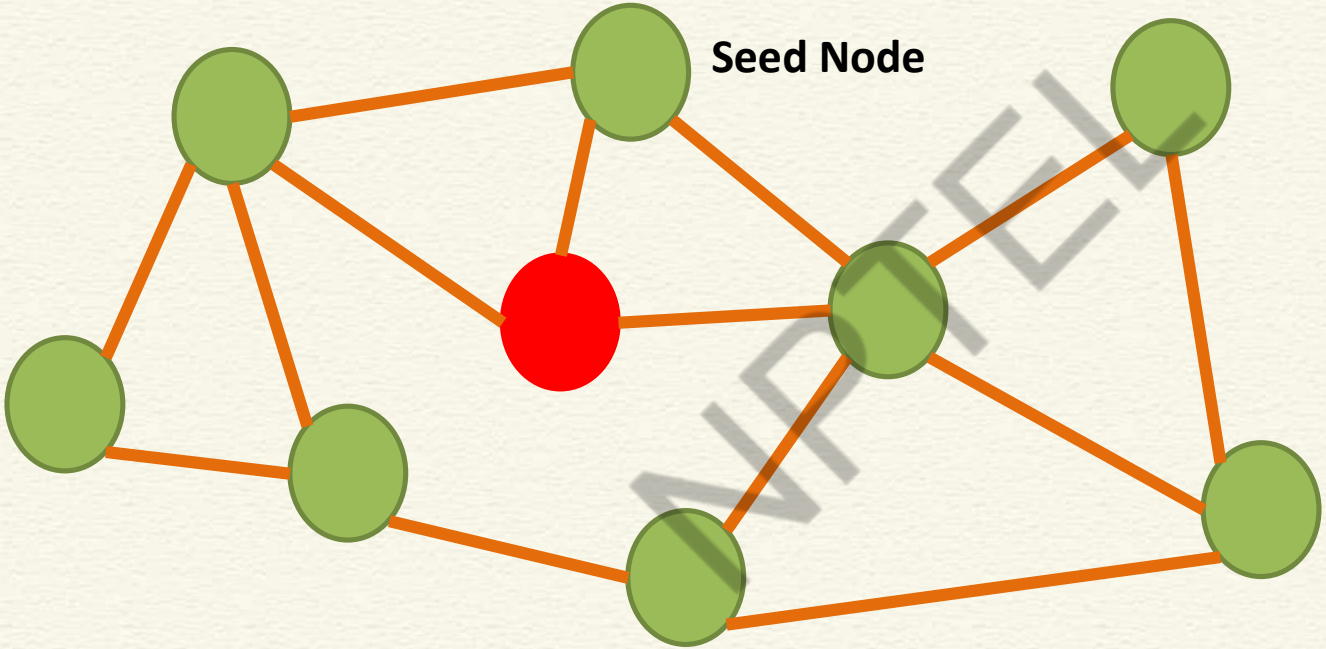
Joining in a Bitcoin P2P Network



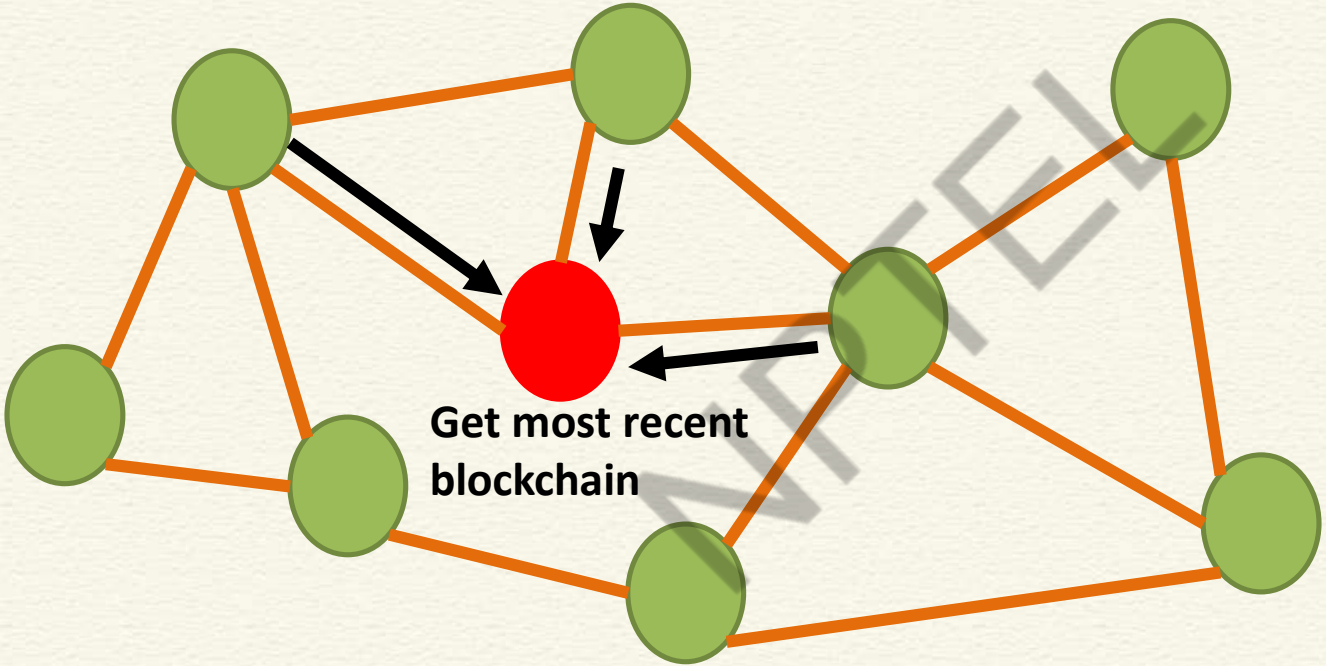
Joining in a Bitcoin P2P Network



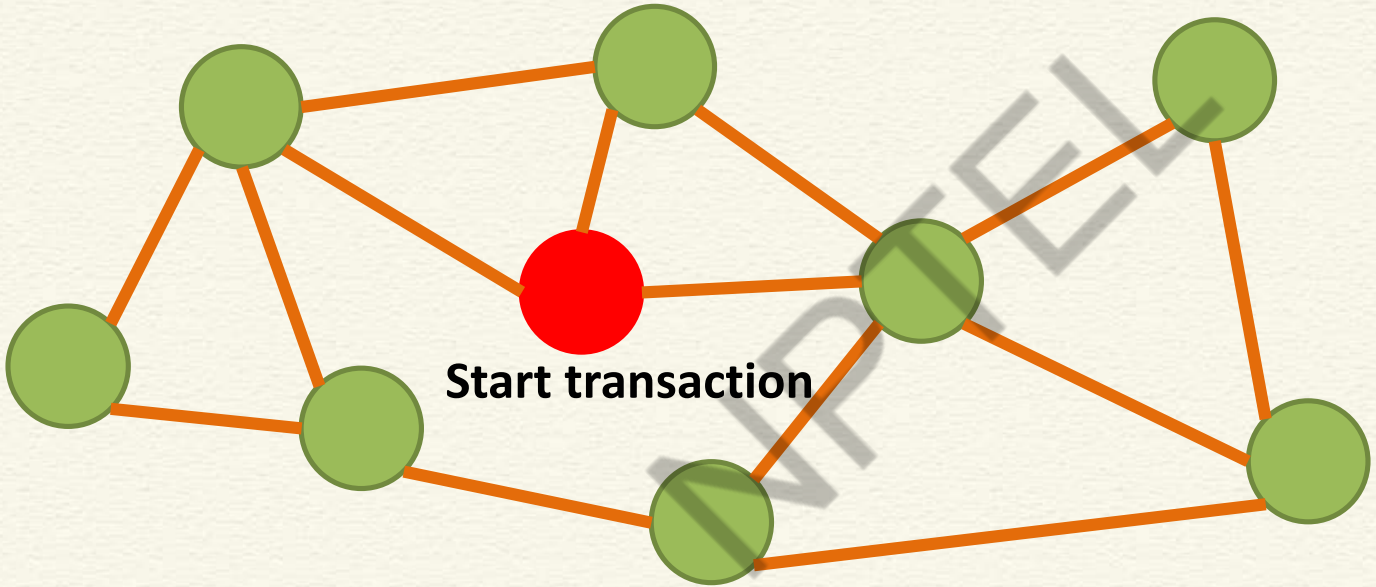
Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network



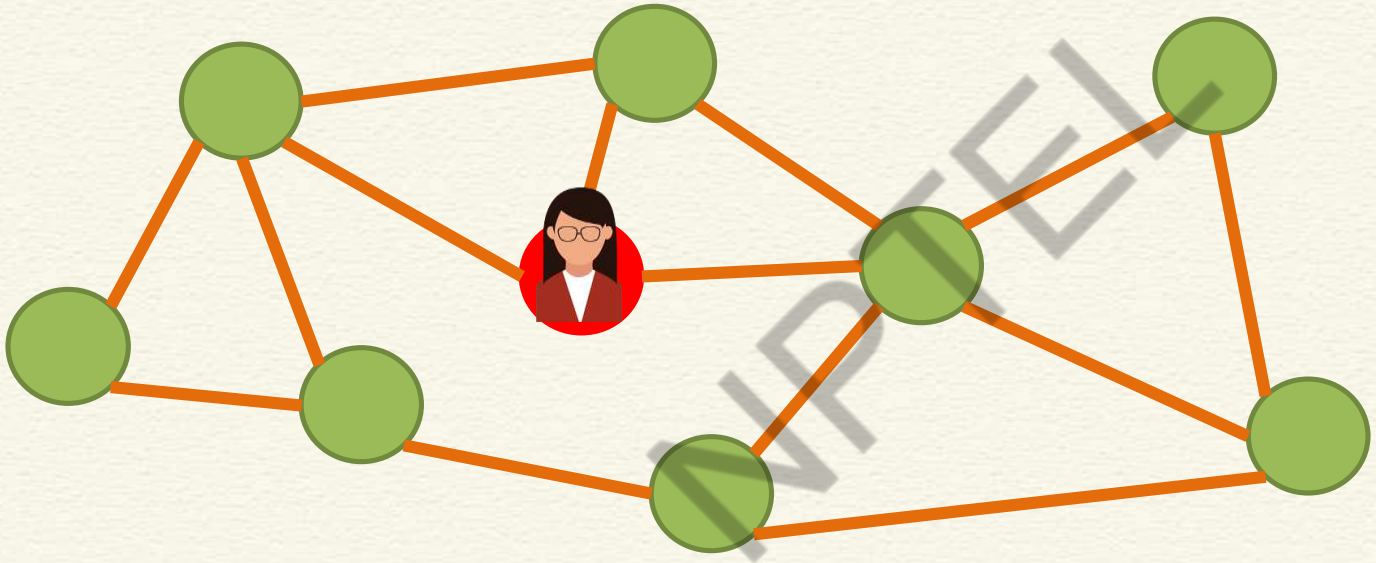
Joining in a Bitcoin P2P Network



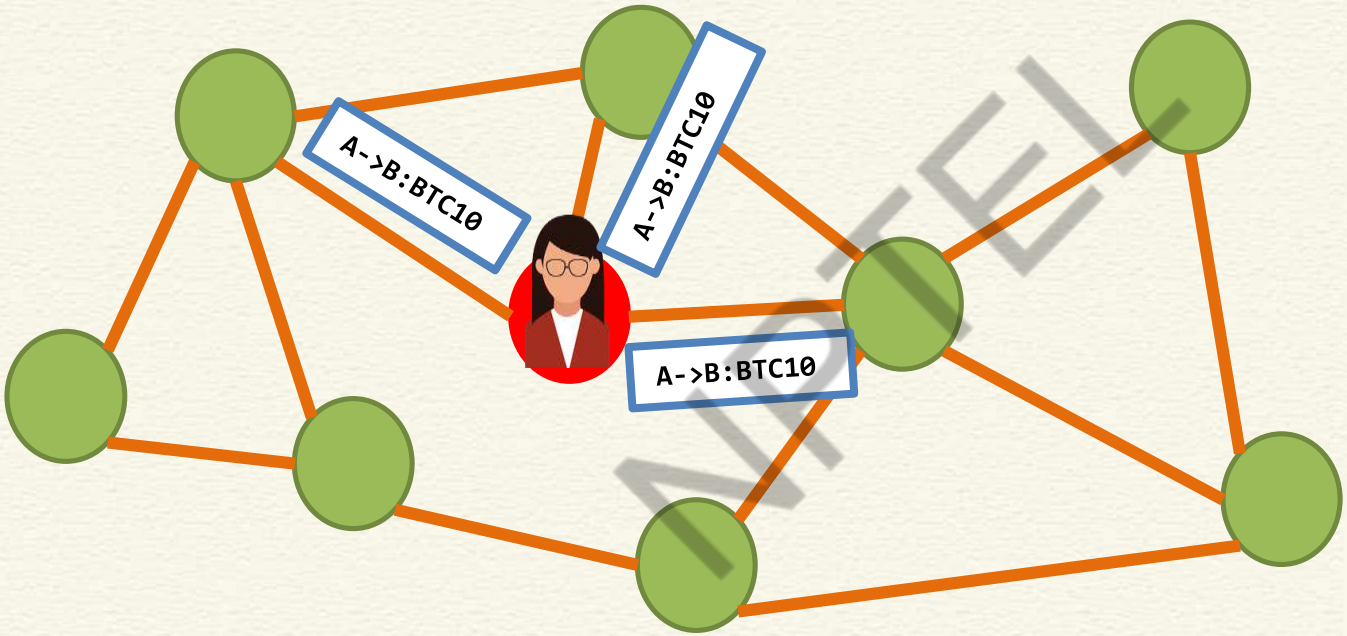
Transactions in a Bitcoin Network

- Alice joins the Bitcoin network by opening her applet
- Alice makes a transaction to Bob: **`A->B: BTC 10`**
- Alice includes the scripts with the transactions
- Alice broadcasts this transaction in the Bitcoin network

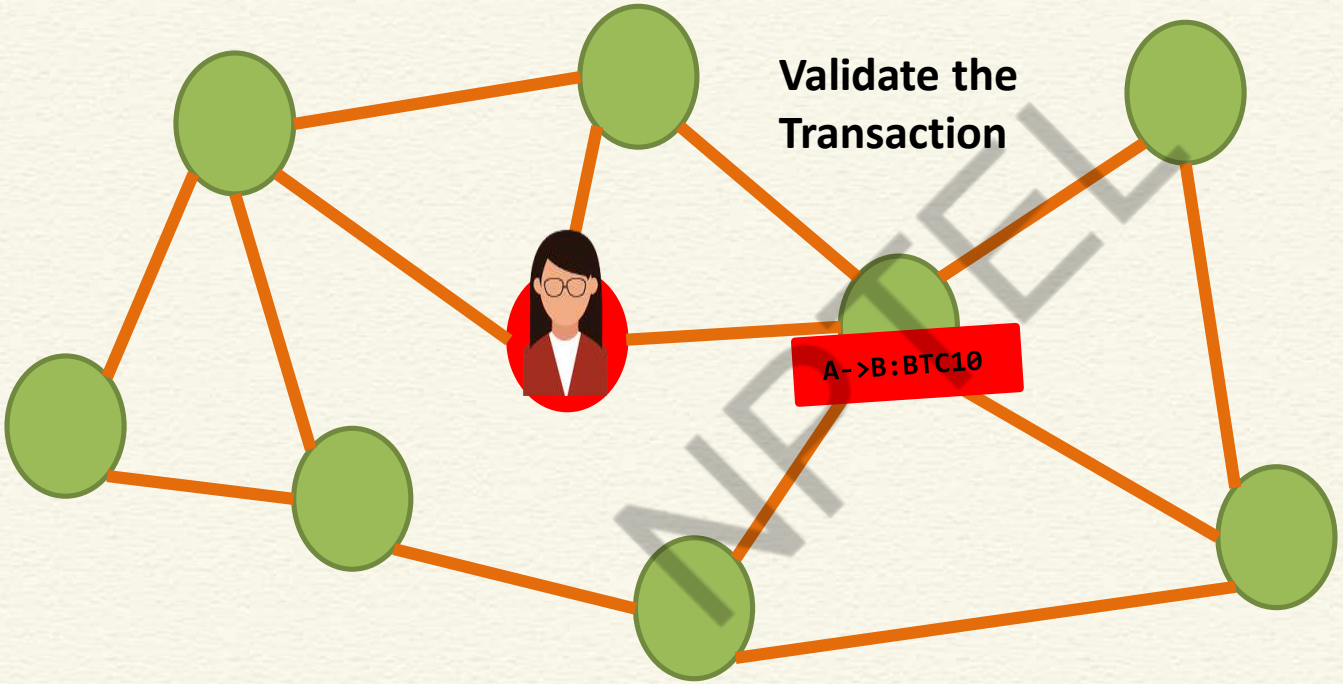
Transaction Flooding in a Bitcoin Network



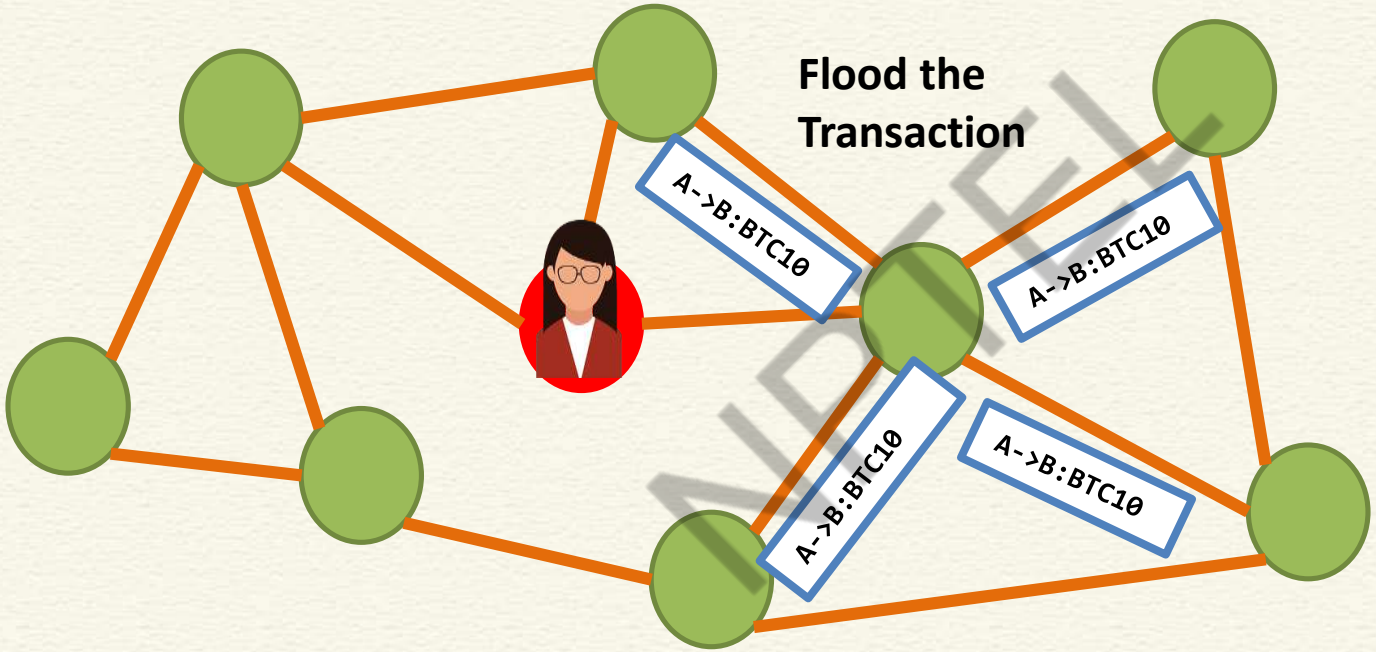
Transaction Flooding in a Bitcoin Network



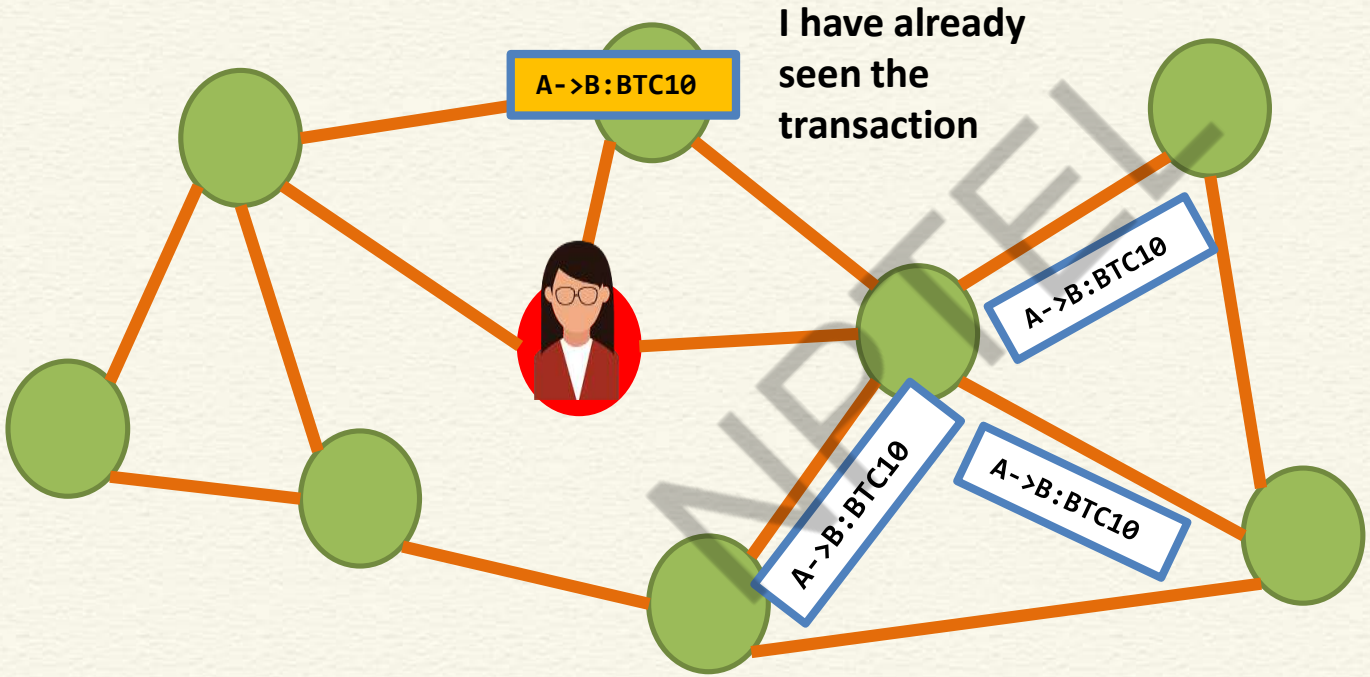
Transaction Flooding in a Bitcoin Network



Transaction Flooding in a Bitcoin Network



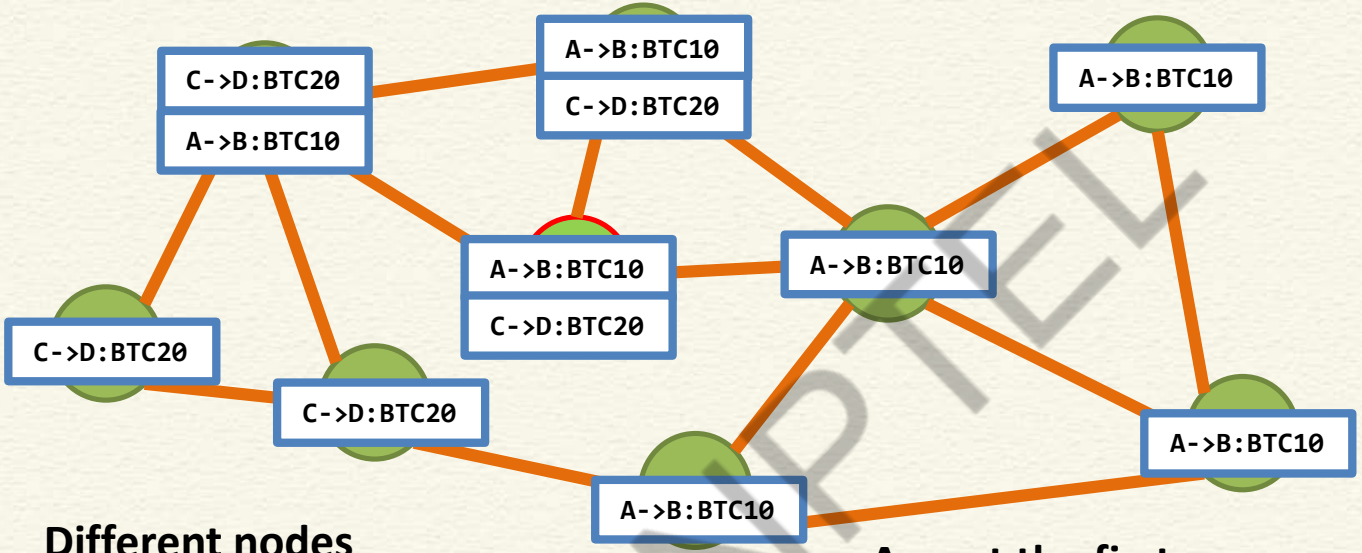
Transaction Flooding in a Bitcoin Network



Which Transactions Should You Relay?

- The transaction is valid with current blockchain
  - No conflict
  - No double spending
- The script matches with a pre-given set of whitelist scripts – Avoid unusual scripts, avoid infinite loops
- Does not conflict with other transactions that I have relayed after getting the blockchain updated – avoid double spending

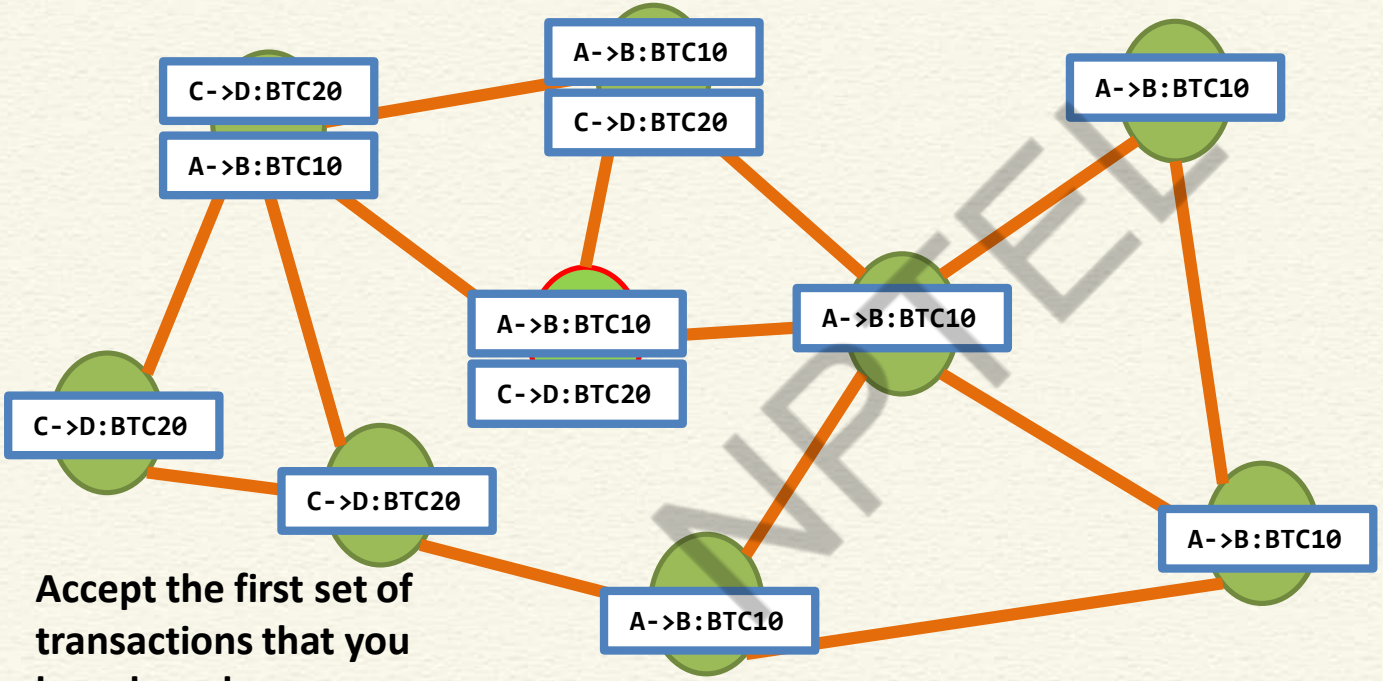
Transaction Flooding in a Bitcoin Network



Different nodes may have different transaction pools

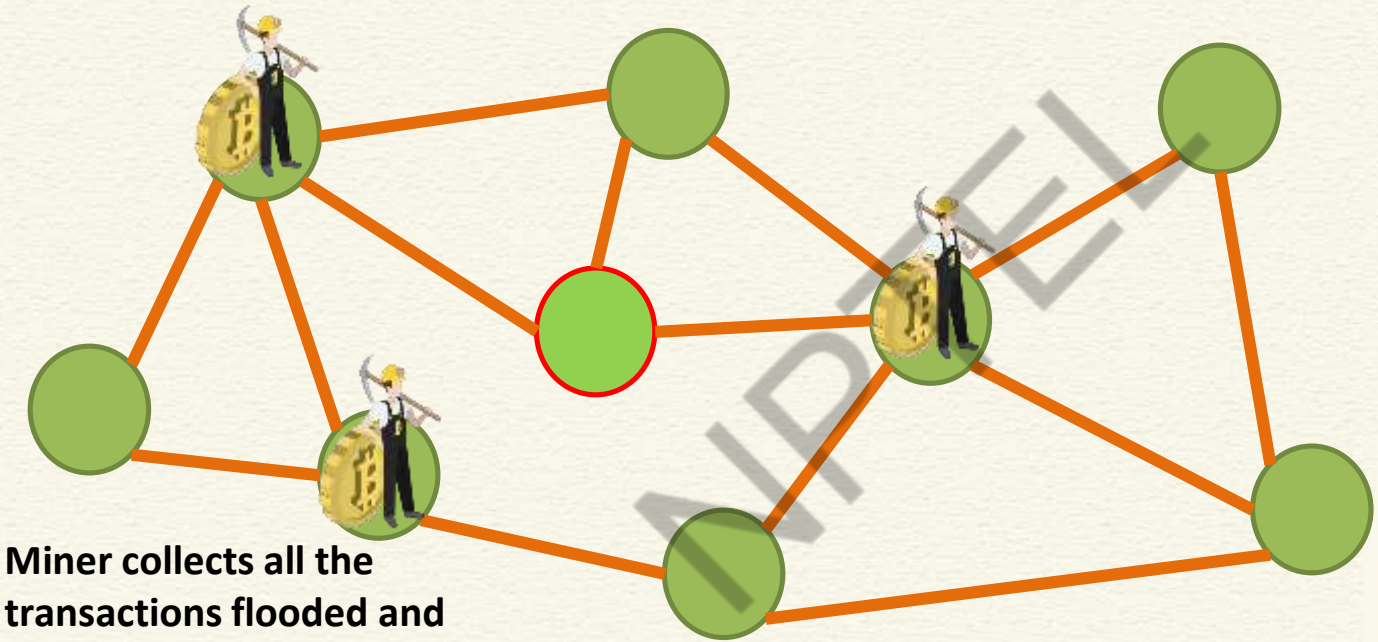
Accept the first transactions that you have heard

Transaction Flooding in a Bitcoin Network



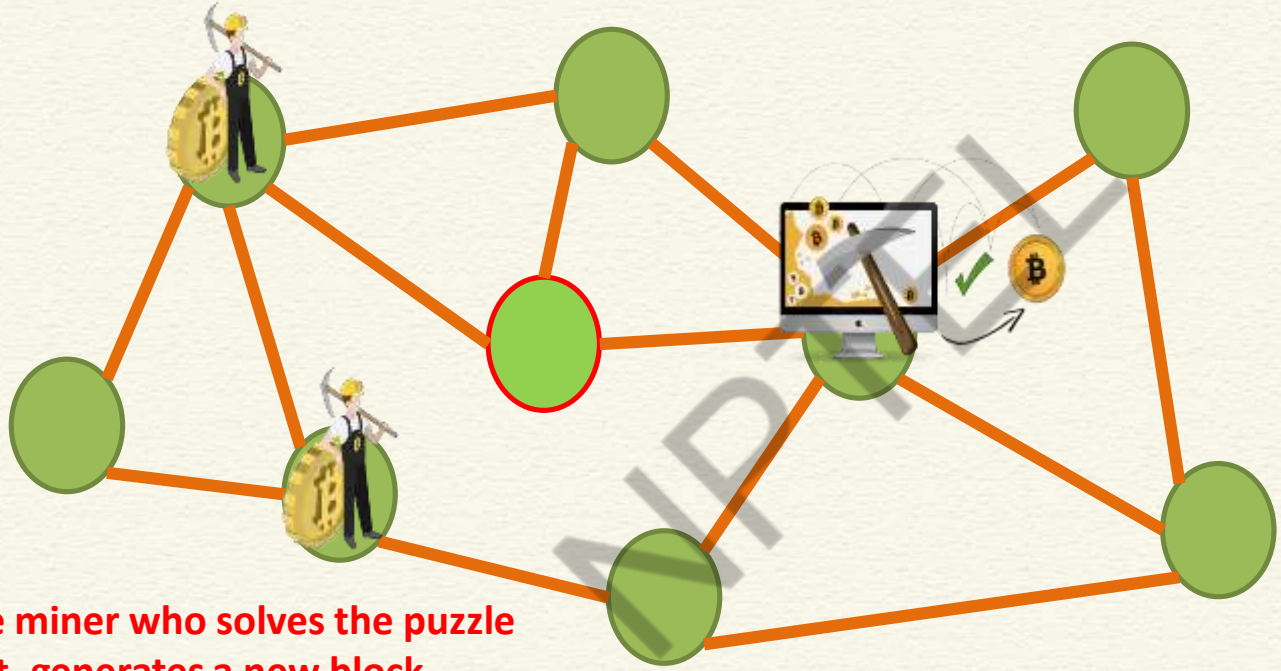
Accept the first set of transactions that you have heard

Mining in a Bitcoin Network



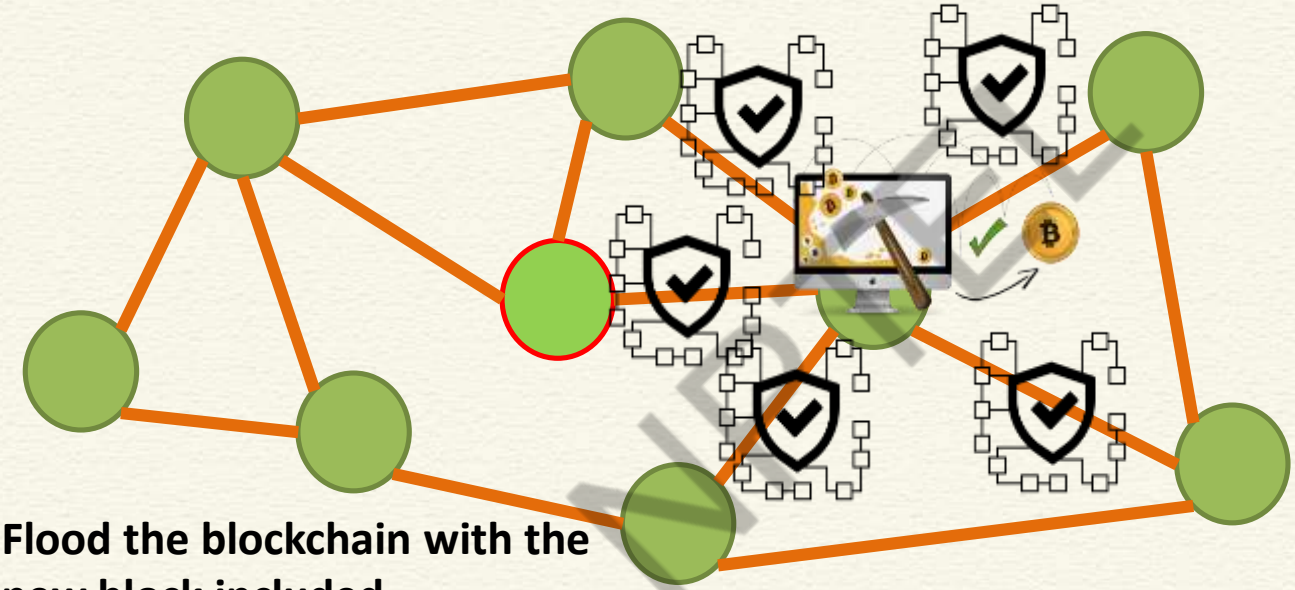
Miner collects all the transactions flooded and starts mining

Block Generation



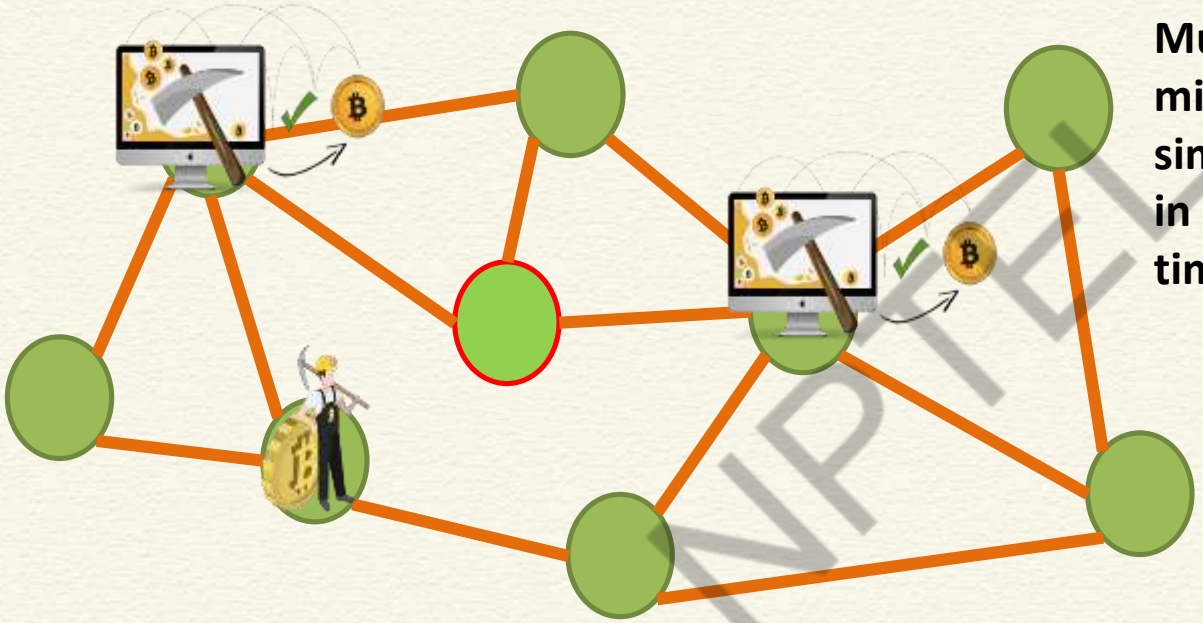
The miner who solves the puzzle first, generates a new block

Block Flooding



Flood the blockchain with the new block included

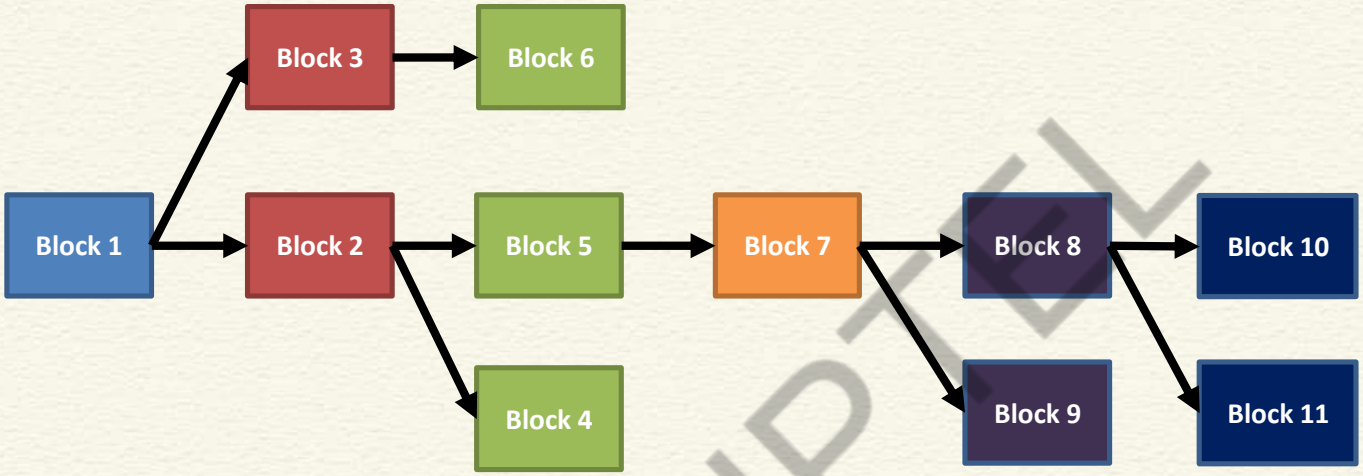
Block Propagation



Multiple miners can mine a new block simultaneously or in a near identical time

"Forks" may get created

Block Propagation – Accept the Longest Chain



- "Accidental" forks occur rarely. Even if they occur, eventually only one becomes part of the longest chain
- There are "intentional" forks of two type: hard forks and soft forks to come up with new versions like Bitcoin Cash, etc., or to upgrade software versions

Which Block to Relay

- Block contains the correct hash based on the existing blockchain
- All the transactions inside the block are valid
  - Check the scripts
  - Validate with the existing blockchain
- The block is included in the current longest chain
  - Do not relay the forks

CONCLUSIONS

- Shown how a new node can join the bitcoin network
- Creation and propagation of transactions
- Accumulating transactions and mining new blocks
- Propagation of new bitcoin blocks
- Discussed how forking is handled in a blockchain

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Blockchain: Hype or Innovation by Tatiana Gayvoronskaya and Christoph Meinel, Springer (2021)
- Any other standard textbook on blockchain/bitcoin

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 17: Blockchain Elements - V

CONCEPTS COVERED

- Start of the Bitcoin Network and Creation of Coins
- Variation of Block Reward with Time
- Handling of Double Spending Problem
- Payment using Bitcoin and Anonymity
- Bitcoin Exchange

KEYWORDS

- Block Reward
- Double Spending
- Anonymity
- Bitcoin Exchange

Bitcoin Basics – Creation of Coins

- **Controlled Supply:** Must be limited for the currency to have value – any maliciously generated currency needs to be rejected by the network
- Bitcoins are generated **during the mining** – each time a user discovers a new block
- The rate of block creation is adjusted every 2016 blocks to aim for **a constant two week adjustment period**
- The last bitcoin will be mined in 2140 (estimated and unless changed)

Bitcoin Basics – Creation of Coins

- Number of bitcoins generated per block is set to decrease **geometrically**, with a 50% reduction for every 210,000 blocks, or approximately 4 years
- This reduces with time the amount of bitcoins generated per block
  - Theoretical limit for total bitcoins: Slightly less than *21 million*
  - Miners will get less reward as time progresses
  - How to pay the mining fee – increase the transaction fee

Projected Number of Bitcoins

Date reached	Block	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
2009-01-03	0	1	50.00	2009	0	2625000	2625000	infinite	12.500%
2010-04-22	52500	1	50.00	2010	2625000	2625000	5250000	100.00%	25.000%
2011-01-28	105000	1	50.00	2011*	5250000	2625000	7875000	50.00%	37.500%
2011-12-14	157500	1	50.00	2012	7875000	2625000	10500000	33.33%	50.000%
2012-11-28	210000	2	25.00	2013	10500000	1312500	11812500	12.50%	56.250%
2013-10-09	262500	2	25.00	2014	11812500	1312500	13125000	11.11%	62.500%
2014-08-11	315000	2	25.00	2015	13125000	1312500	14437500	10.00%	68.750%
2015-07-29	367500	2	25.00	2016	14437500	1312500	15750000	9.09%	75.000%
2016-07-09	420000	3	12.50	2016	15750000	656250	16406250	4.17%	78.125%
2017-06-23	472500	3	12.50	2018	16406250	656250	17062500	4.00%	81.250%
	525000	3	12.50	2019	17062500	656250	17718750	3.85%	84.375%
	577500	3	12.50	2020	17718750	656250	18375000	3.70%	87.500%
	630000	4	6.25	2021	18375000	328125	18703125	1.79%	89.063%
	682500	4	6.25	2022	18703125	328125	19031250	1.75%	90.625%
	735000	4	6.25	2023	19031250	328125	19359375	1.72%	92.188%
	787500	4	6.25	2024	19359375	328125	19687500	1.69%	93.750%

Information Source: https://en.bitcoin.it/wiki/

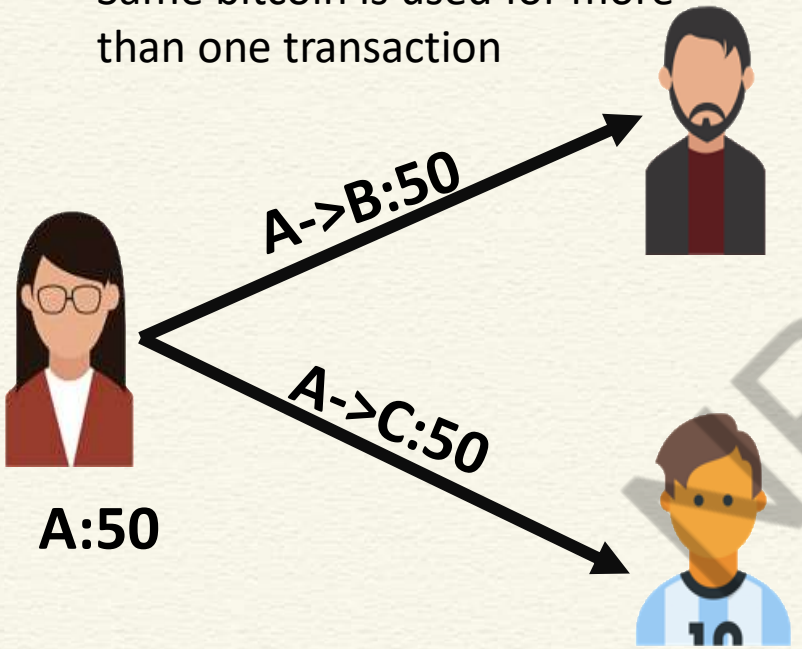
Bitcoin Basics – Sending Payments

- Alice wants to send bitcoin to Bob
  - Bob sends his address to Alice
  - Alice adds Bob's address and the amount of bitcoins to transfer in a "transaction" message
  - Alice signs the transaction with her private key, and announces her public key for signature verification
  - Alice broadcasts the transaction on the Bitcoin network for all to see

Information Source: https://en.bitcoin.it/wiki/

Double Spending

- Same bitcoin is used for more than one transaction



- Double spending Cash??
- In a centralized system for digital currency, the bank prevents double spending
- **How can we prevent double spending in a decentralized network?**

Handle Double Spending using Blockchain

- When multiple valid continuation to this chain appear, only the longest such branch is accepted and it is then extended further **(longest chain)**
- Once a transaction is committed in the blockchain, everyone in the network can validate all the transactions by using Alice's public address
- The validation prevents double spending in bitcoin

Bitcoin Anonymity

- Bitcoin is permission-less, you do not need to setup any “account”, or required any e-mail address, user name or password to login to the wallet
- The public and the private keys do not need to be registered, the wallet can generate them for the users
- The **bitcoin address** is used for transaction, not the user name or identity

Bitcoin Anonymity

- A **bitcoin address** mathematically corresponds to a public key based on ECDSA – the digital signature algorithm used in bitcoin
- A sample bitcoin address: 1PHYrmdJ22MKbJevpb3MBNpVckjZHt89hz
- Each person can have many such addresses, each with its own balance
  - Difficult to know which person owns what amount

To Sum it All Up!!

- Bitcoins do not really “exist” as any tangible or electronic object.
- There is no bit”coin” as you see in its logo
- Owning a bitcoin simply means you have access to a key pair that includes
  - A public key to which somebody else had sent some bitcoin
  - A matching private key that gives you the authority to send the previously received bitcoin to another address
- If you lose your private key, you lose the corresponding bitcoin(s)

Physical Payment using Bitcoin

- All that is needed is a (set of) private key(s) – Public key can be generated from the private key.
- Safely store the private key – in your desktop, on the web, mobile phone, special hardware attachment, printed on a piece of paper as QR
- For online payment, you can use the wallet and an appropriate mode of applying the private key
- For off line payments like in store payments or paying to your friend, you can use your mobile phone to present the private key or use the hardcopy!! As simple as using PayTm, Google Pay and so on.

Bitcoin Exchange

- Trading bitcoin as commodity
- Centralized exchanges – (In India: WazirX, CoinDCX, Zebpay, CoinSwitch Kuber, etc.)
  - Identity verification using KYC documents
  - Maintain your balance in Bitcoin and another currency like INR.
  - You set the buying and selling prices and quantities
  - If necessary, you can take the money out in a referred currency
  - Some exchanges provide the payout option in anonymous prepaid cards
- There can also be decentralized exchanges with appropriate procedures for handling similar requirements

CONCLUSIONS

- Generation (Mining) of new coins
- Variation of block reward with time
- Handling double spending
- Anonymity in bitcoin
- Paying using bitcoin and role of exchange

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Blockchain: Hype or Innovation by Tatiana Gayvoronskaya and Christoph Meinel, Springer (2021)
- Any other standard textbook on blockchain/bitcoin

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 !!

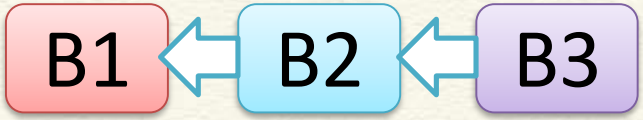
Permissionless Blockchain

ethereum

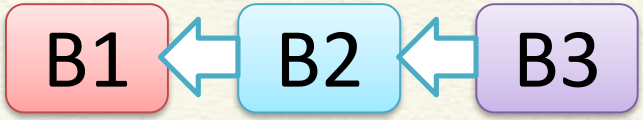
Consensus Challenges

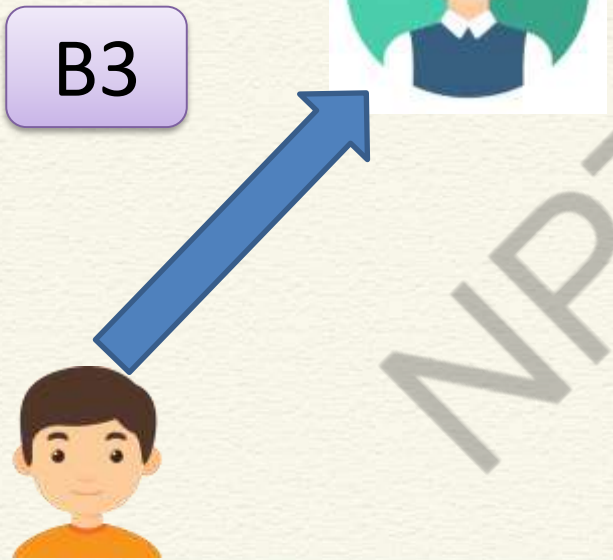
- **Participants do not know others**
  - Cannot use message passing !!
- **Anyone can propose** a new block
  - Who is going to add the next block in the blockchain?
- The network is **asynchronous**
  - We do not have any global clock
  - A node may see the blocks in different orders

Consensus Challenges

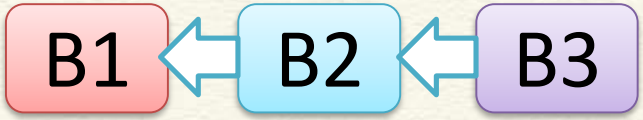


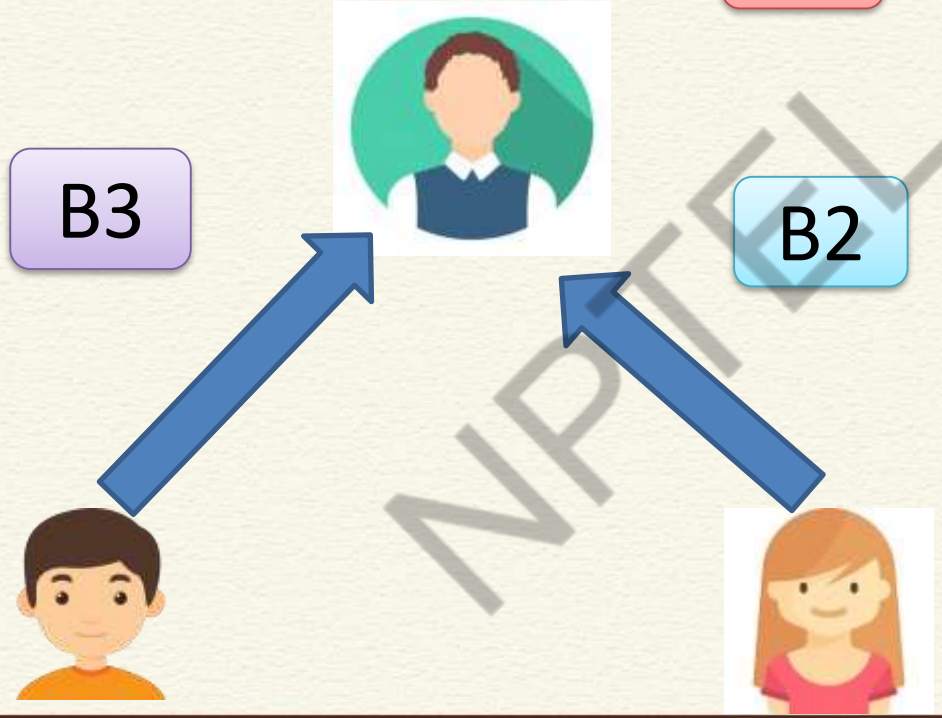
Consensus Challenges





Consensus Challenges





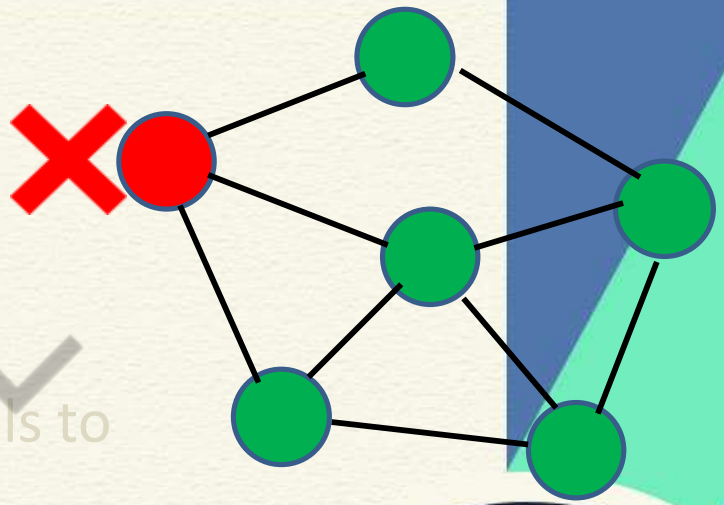
Consensus Challenges

- 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

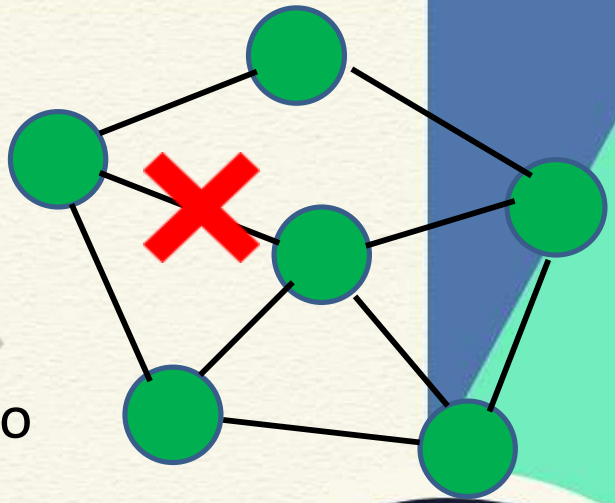
- Synchronous vs Asynchronous Networks
  - **Synchronous**: I am sure that I'll get the message in real time (theoretically no delay or minimum delay)
  - **Asynchronous**: I am not sure whether and when the message will arrive

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

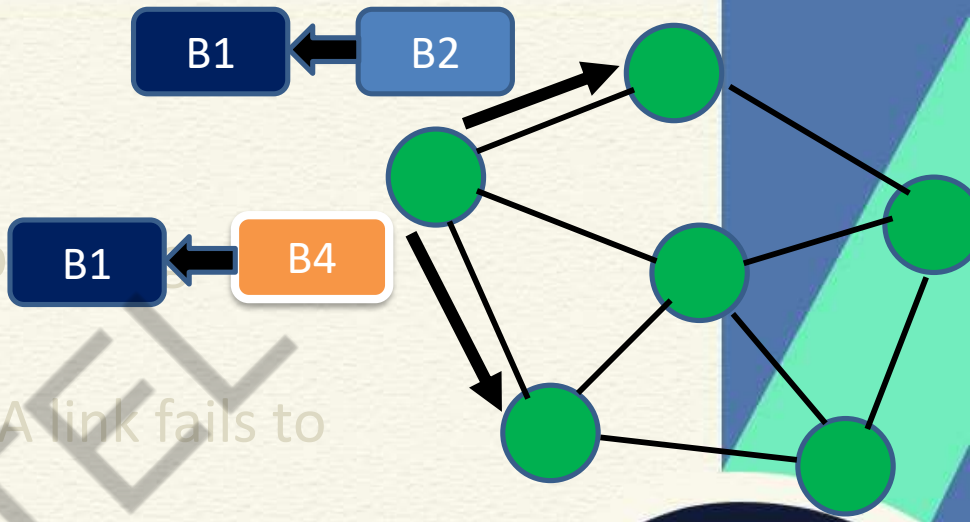
Failure in a Network



- **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

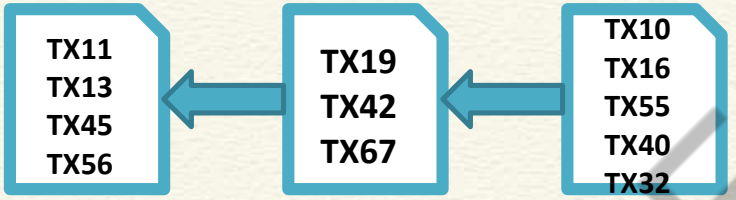
The Consensus Problem

Miner 1

Miner 2

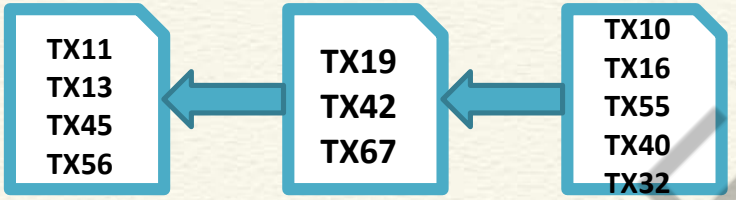
Miner 3

The Consensus Problem

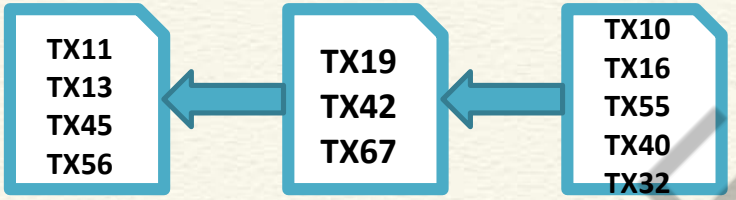


Bitcoin Unconfirmed TX : https://www.blockchain.com/btc/unconfirmed-transactions

The Consensus Problem



The Consensus Problem



Unconfirmed TX

TX16
TX17

Miner 1

Unconfirmed TX

TX17

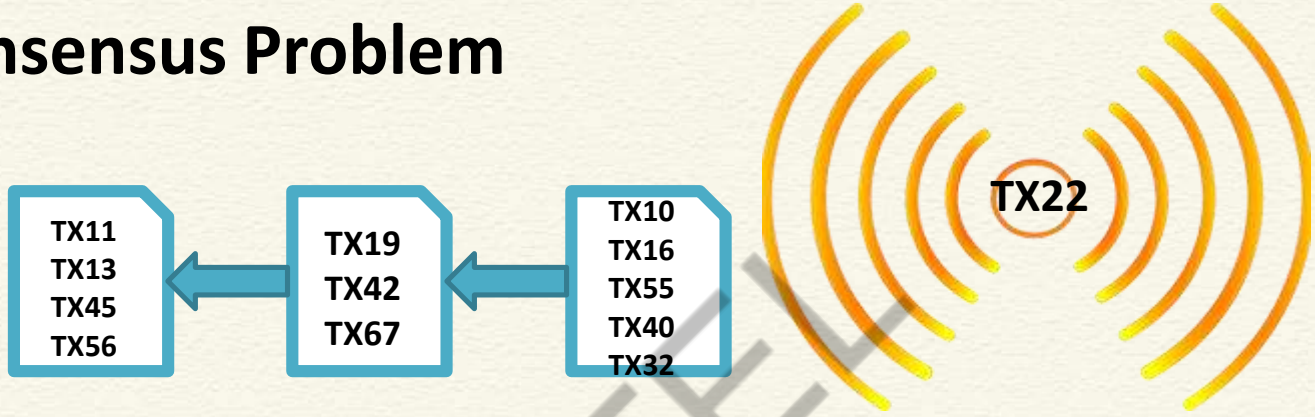
Miner 2

Unconfirmed TX

TX16
TX17

Miner 3

The Consensus Problem



Unconfirmed TX

TX16
TX17

Miner 1

Unconfirmed TX

TX17
TX22

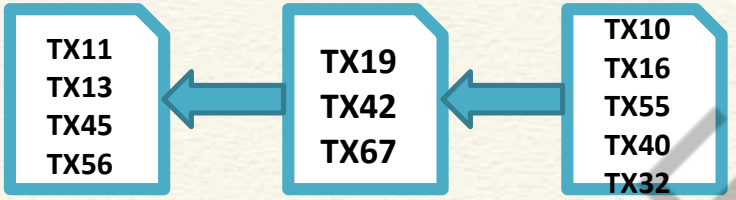
Miner 2

Unconfirmed TX

TX16
TX17
TX22

Miner 3

The Consensus Problem



Unconfirmed TX

TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

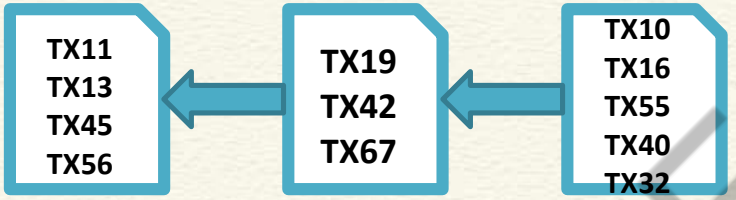
Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

The Consensus Problem



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?

NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 19: Nakamoto Consensus (Proof of Work)

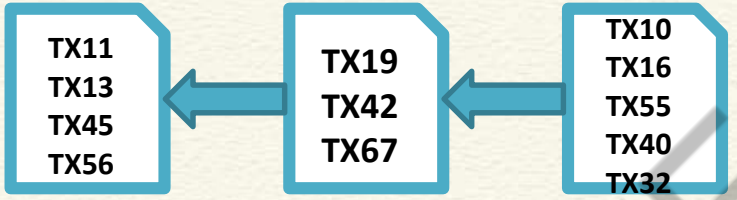
CONCEPTS COVERED

- Nakamoto Consensus
- Block Mining

KEYWORDS

- PoW
- Block Mining
- Safety and Liveness

The Consensus Problem



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

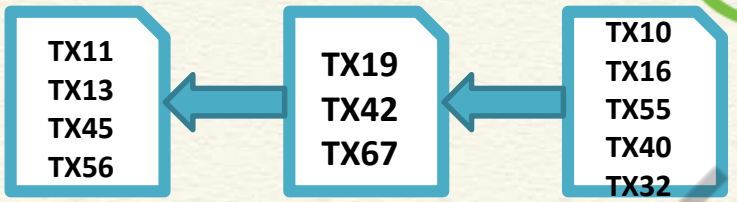
Miner 3

Safety vs Liveness

Safety-1: The next block should be "**correct**" in practice

- Transactions are verified, block contains **correct Hash** and **Nonce**

Safety vs Liveness



This can be ensured – the block mined by a miner is verified by all

Safety-1: The next block should be "**correct**" in practice

- Transactions are verified, block contains **correct Hash** and **Nonce**

Safety vs Liveness

Safety-2: All the miners should agree on a single block

- The next block of the blockchain should be selected unanimously

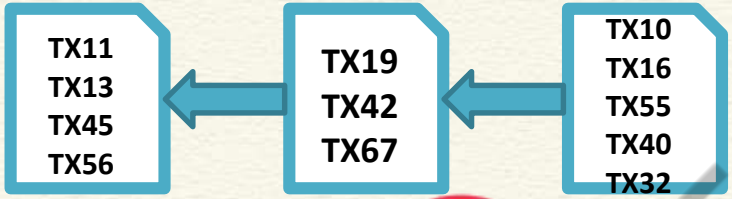
Safety vs Liveness

Miners do not know each other – how can they agree on the same block?

Safety-2: All the miners should agree on a single block

- The next block of the blockchain should be selected unanimously

Safety vs Liveness



PoW compromises here

Safety-2: All the miners should agree on a single block

- The next block of the blockchain should be selected unanimously

Safety vs Liveness

Liveness: Add a block as long as it is correct (contains valid transactions from the unconfirmed TX list) and move further

Safety vs Liveness

Two (or more) different miners may add two (or more) different blocks

Liveness: Add a block as long as it is correct (contains valid transactions from the unconfirmed TX list) and move further

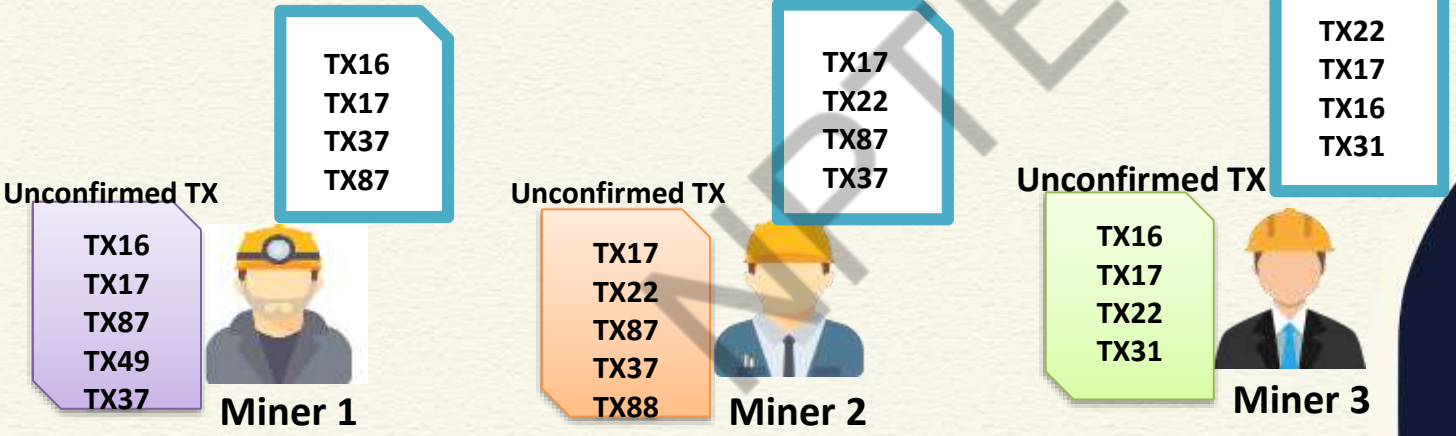
Safety vs Liveness

Two (or more) different miners may add two (or more) different blocks

Will resolve this later!

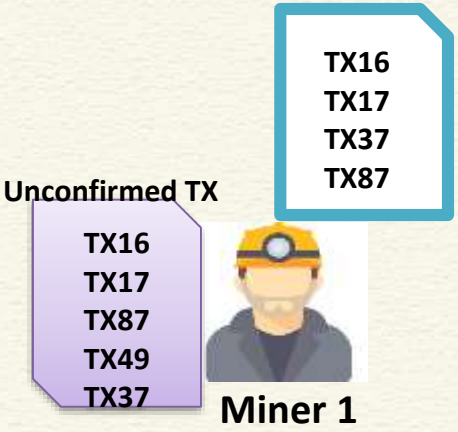
Liveness: Add a block as long as it is correct (contains valid transactions from the unconfirmed TX list) and move further

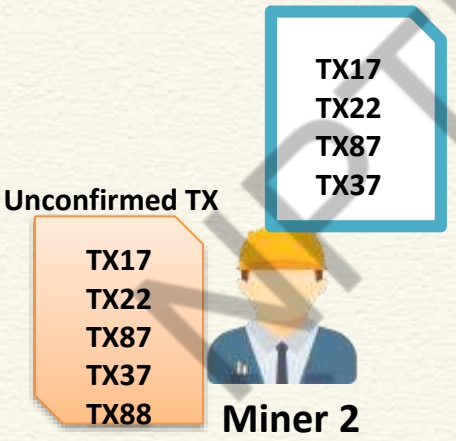
Safety vs Liveness

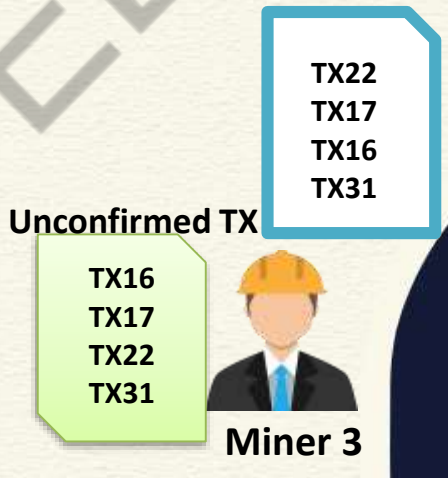


Safety vs Liveness

- No fixed ordering of transactions
- No fixed number of transactions per block
- Limit on the Block size

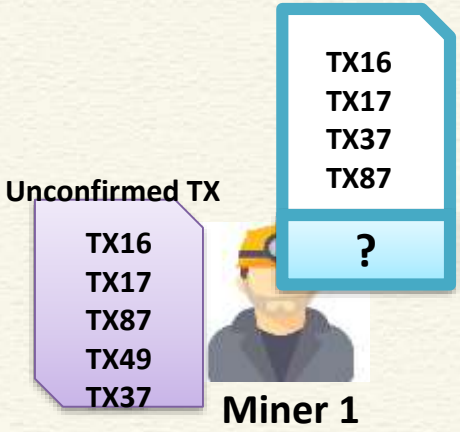


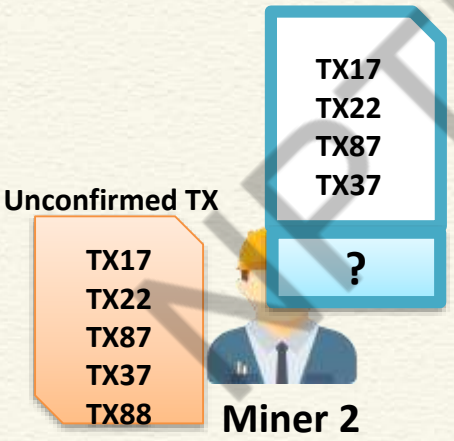


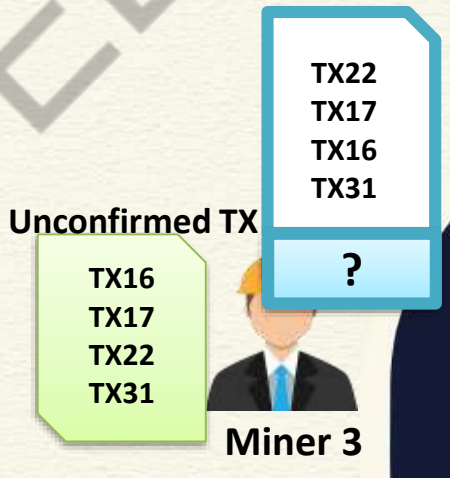


Safety vs Liveness

- Generate the proof (nonce)
  - Generation: Complex
  - Verification: Easy

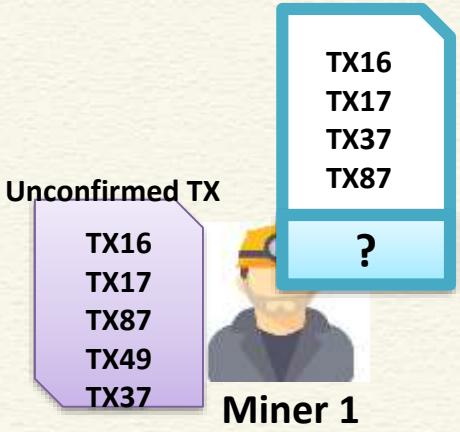


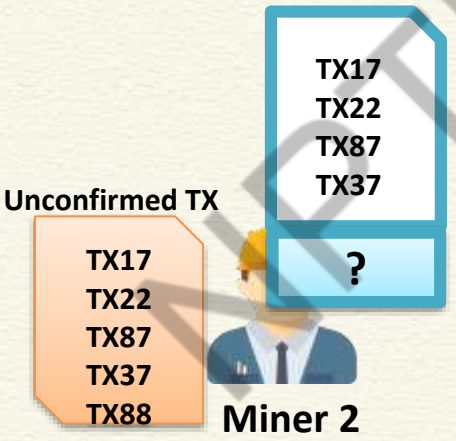


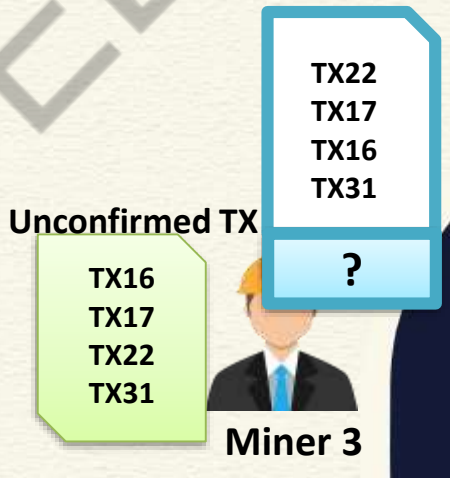


Safety vs Liveness

- **Expectation**: One of the miners will be able to generate the proof

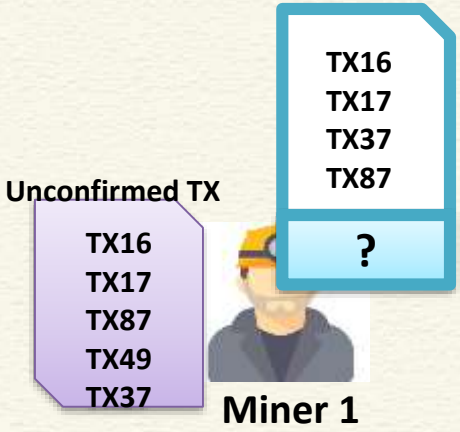


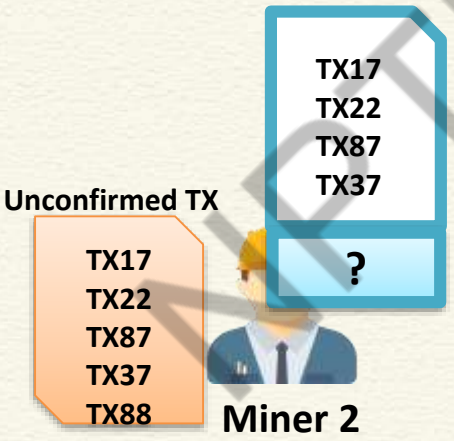


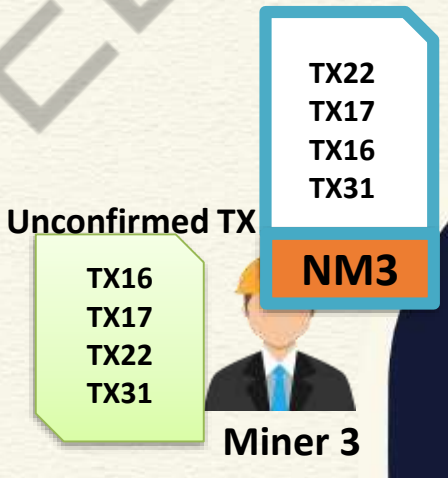


Safety vs Liveness

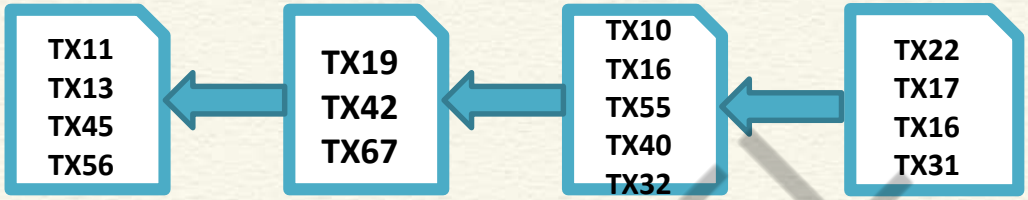
- **Expectation**: One of the miners will be able to generate the proof





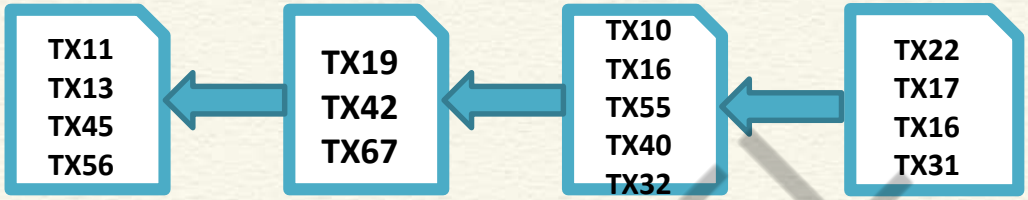


Safety vs Liveness



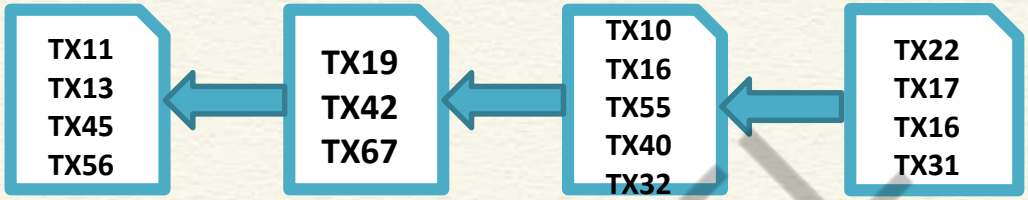
- **Sign the block and broadcast**
  - Gossip over the P2P network

Safety vs Liveness



- **Remove the committed transactions from unconfirmed TX list**

Safety vs Liveness



- Start the next round ...

Conclusion

- Nakamoto Consensus (PoW)
  - Any correct blocks can be added
  - No guarantee that every miner will try to mine the same block
  - No guarantee that you can see your transaction in the latest block
- What if two miners mine block simultaneously?

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

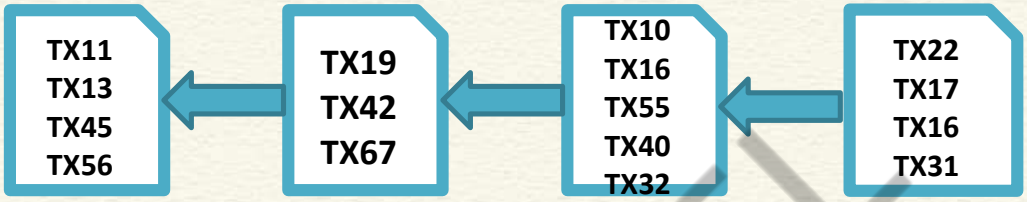
CONCEPTS COVERED

- PoW Forks
- Attacks on PoW
- The Monopoly Problem

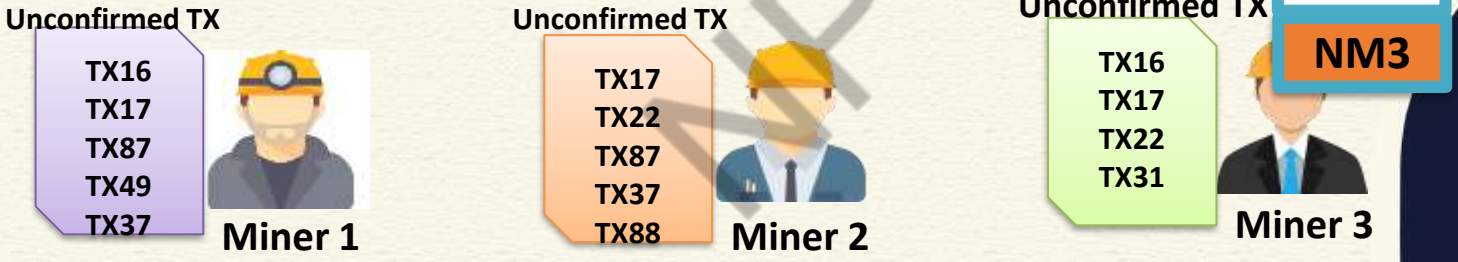
KEYWORDS

- Forks
- Security
- 51% attack

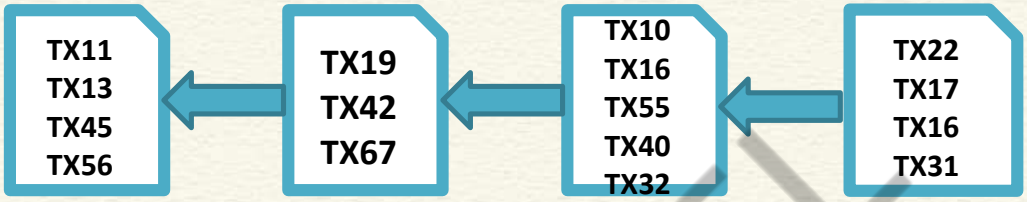
PoW: Mining a New Block



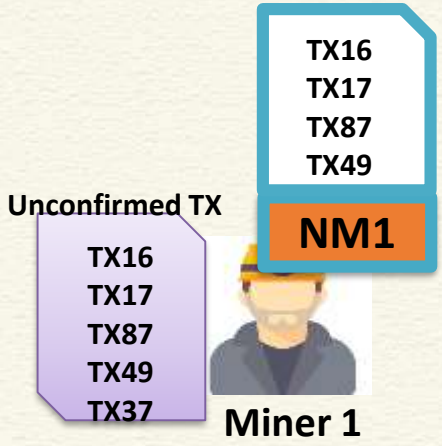
- The miner who is able to solve the puzzle becomes the leader
- The block from the leader is appended in the blockchain

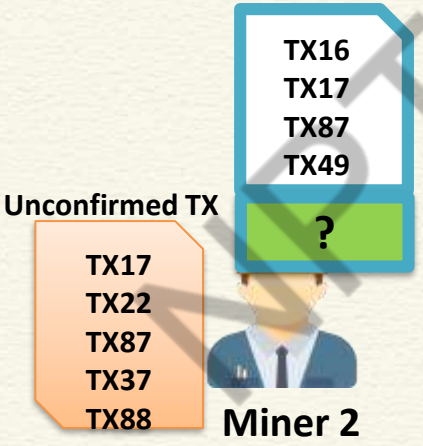


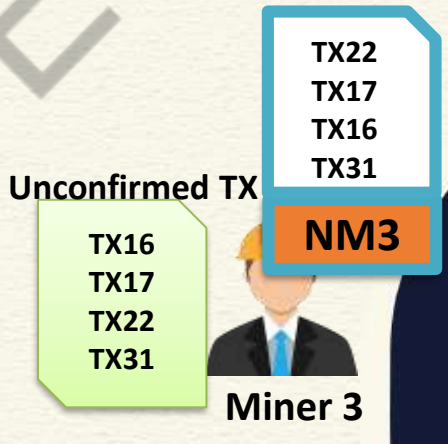
PoW: Mining a New Block



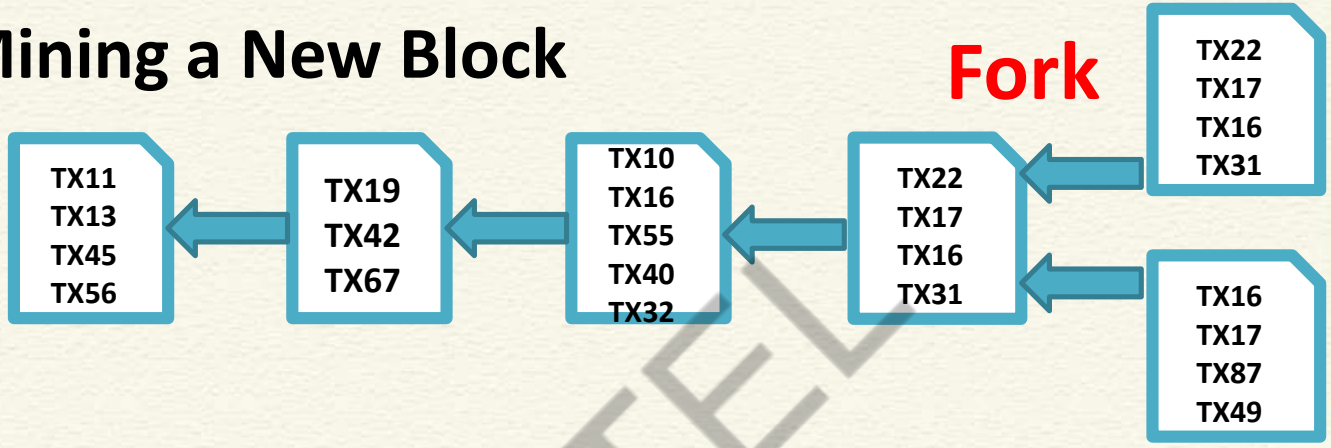
What if two miners solve the puzzle simultaneously?







PoW: Mining a New Block



Unconfirmed TX

TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

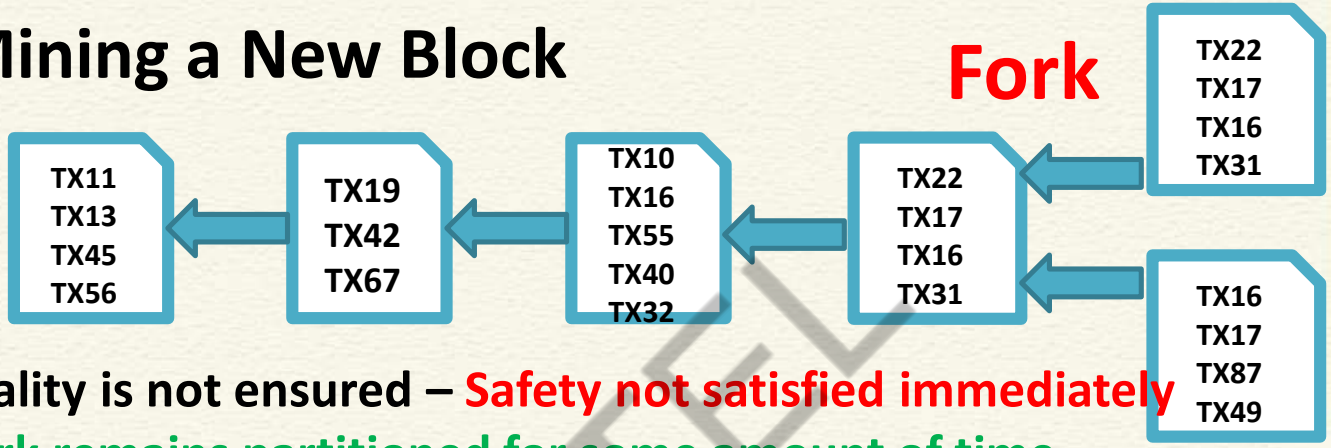
Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

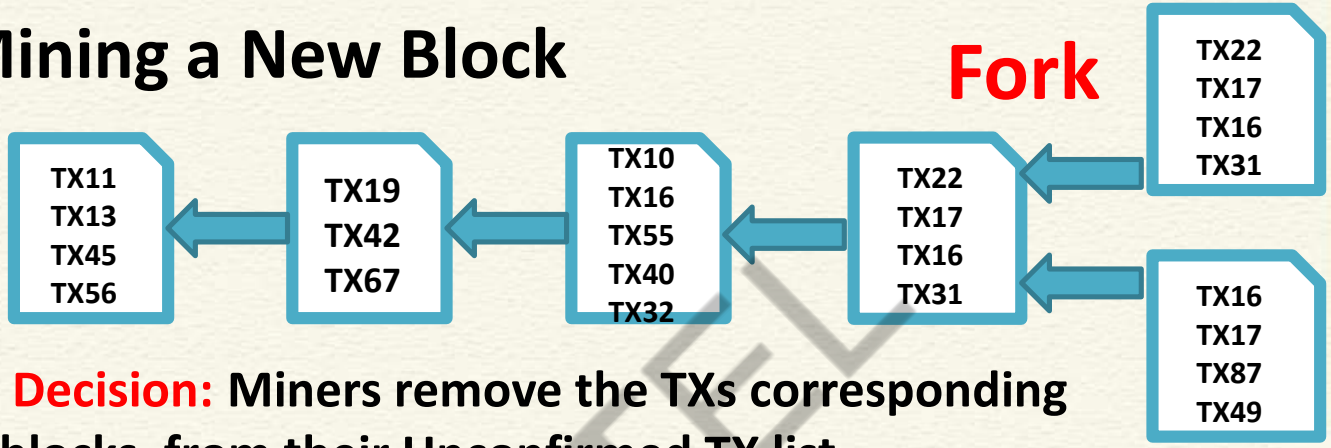
PoW: Mining a New Block



Consensus finality is not ensured – Safety not satisfied immediately

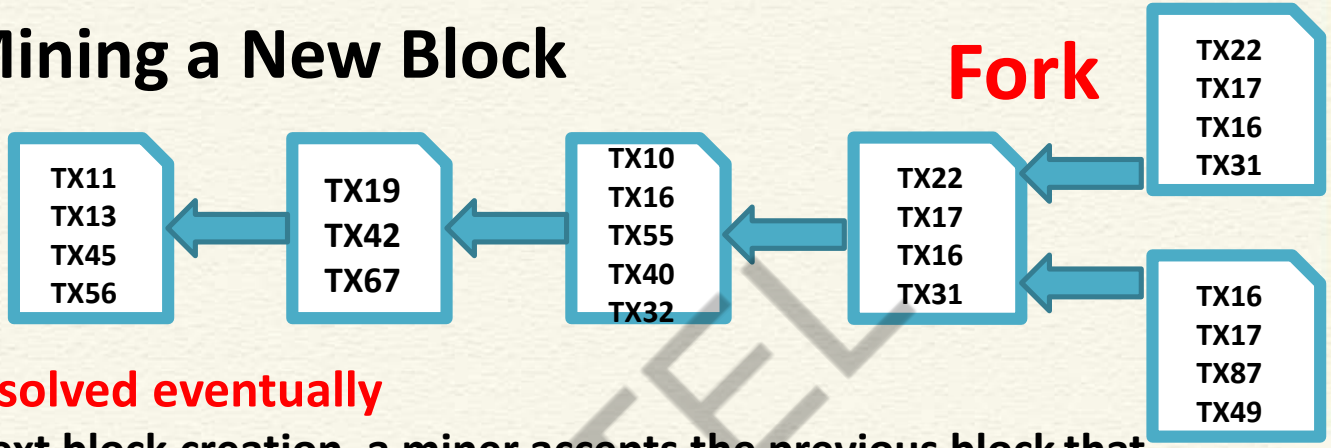
- The network remains partitioned for some amount of time

PoW: Mining a New Block



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

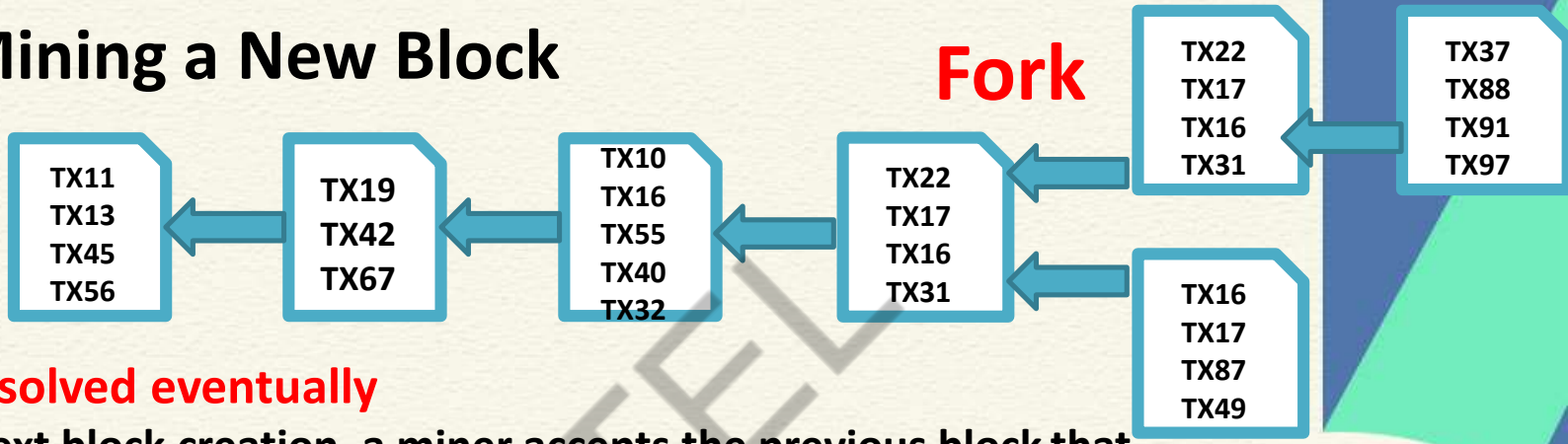
PoW: Mining a New Block



Forks are resolved eventually

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

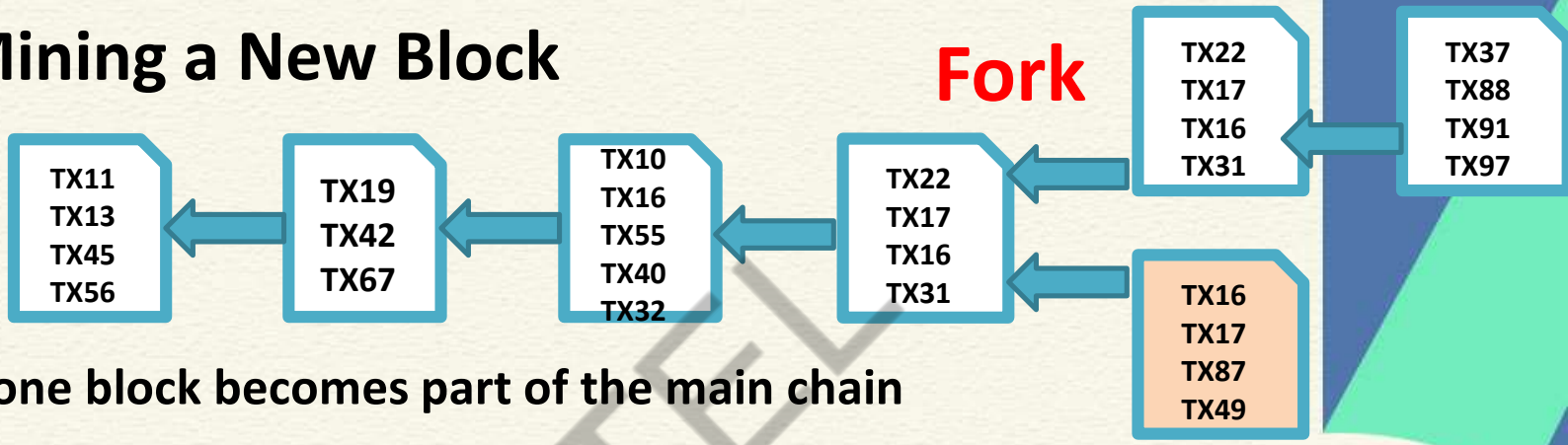
PoW: Mining a New Block



Forks are resolved eventually

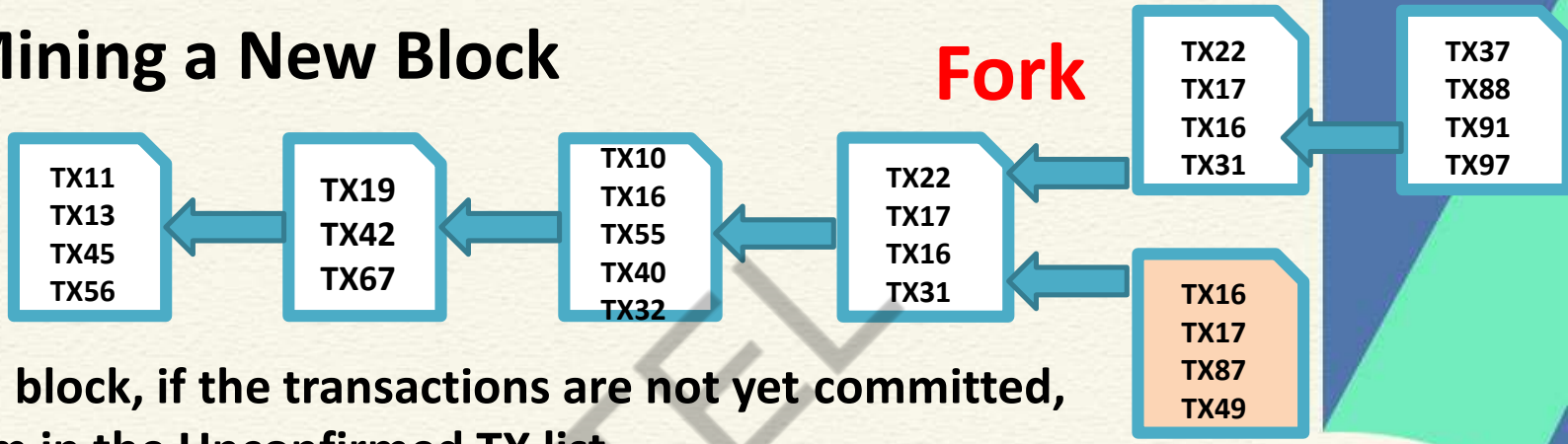
- For the next block creation, a miner accepts the previous block that it hears from the majority of the neighbor

PoW: Mining a New Block



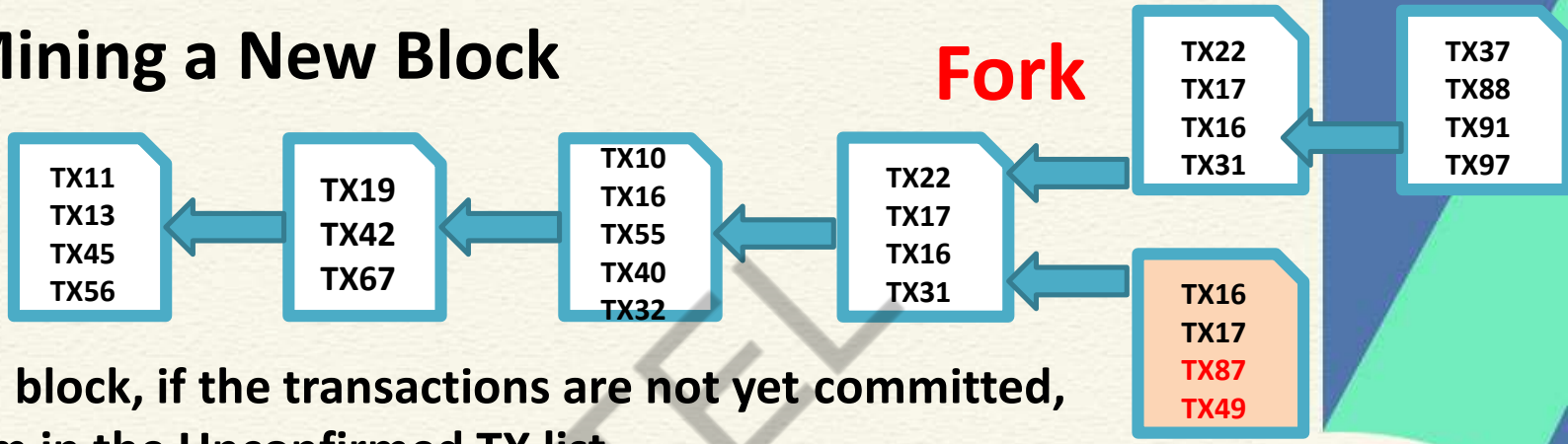
Eventually, one block becomes part of the main chain

PoW: Mining a New Block



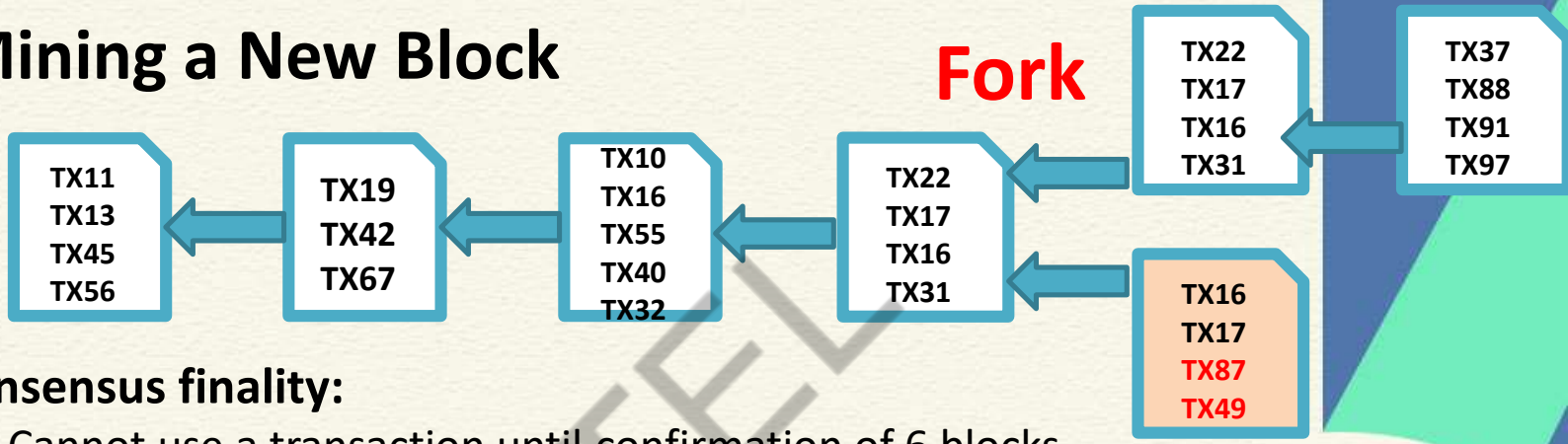
For a forked block, if the transactions are not yet committed, include them in the Unconfirmed TX list

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