



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

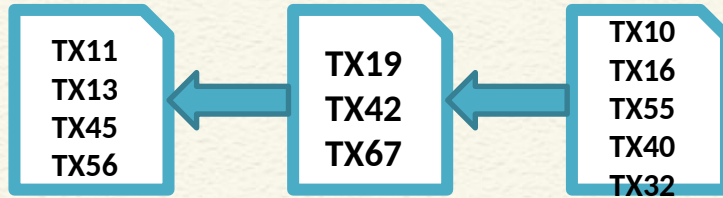


KEYWORDS

- 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

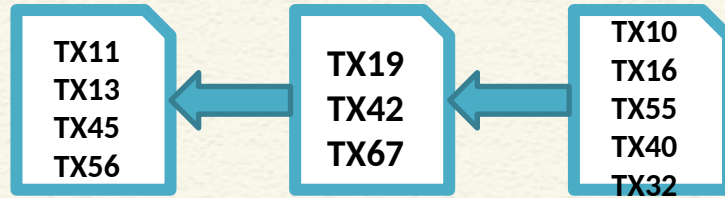
Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

Safety vs Liveness



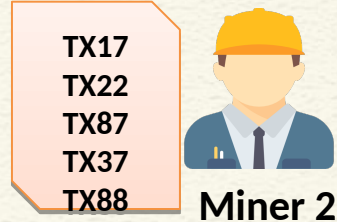
Safety-1: The next block should be "correct" in practice

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

Unconfirmed TX



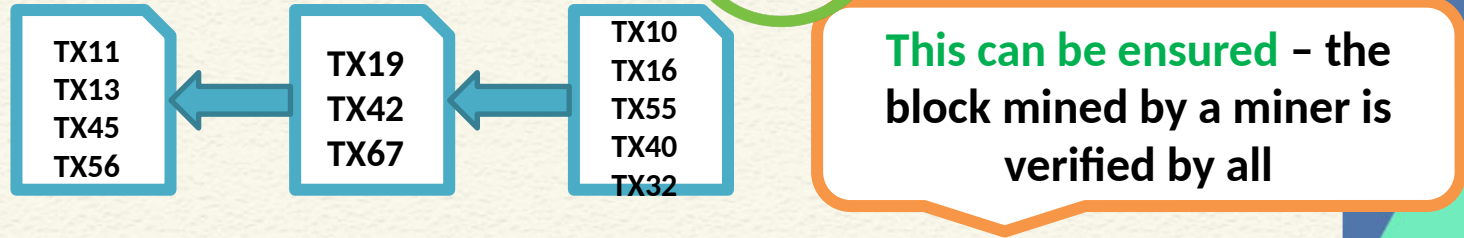
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness



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

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

Unconfirmed TX

TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

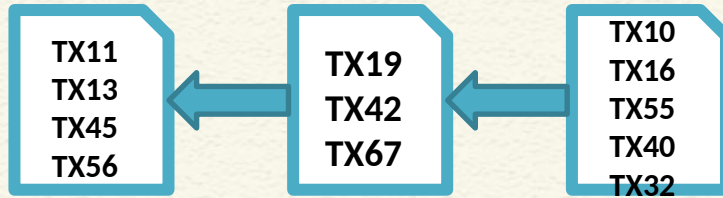
Miner 2

Unconfirmed TX

TX16
TX17
TX22
TX31

Miner 3

Safety vs Liveness



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

- The next block of the blockchain should be selected unanimously


Unconfirmed TX



TX16
TX17
TX87
TX49
TX37

Miner 1

Unconfirmed TX



TX17
TX22
TX87
TX37
TX88

Miner 2

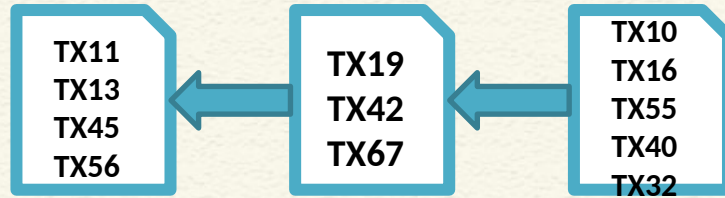
Unconfirmed TX



TX16
TX17
TX22
TX31

Miner 3

Safety vs Liveness



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

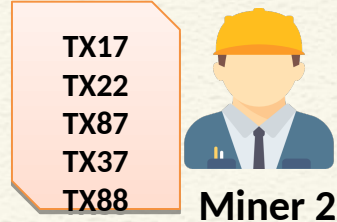
Safety-2: All the miners should agree on a single block

- The next block of the blockchain should be selected unanimously

Unconfirmed TX



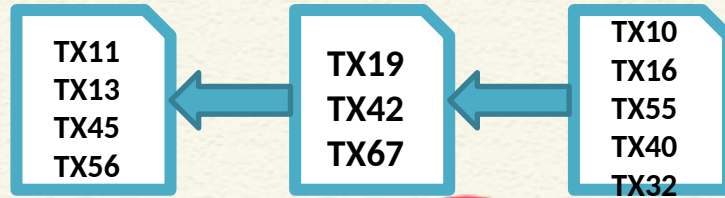
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness



PoW compromises here

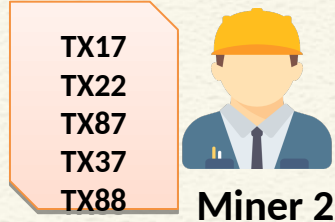
Safety-2: All the miners should agree on a single block

- The next block of the blockchain should be selected unanimously

Unconfirmed TX



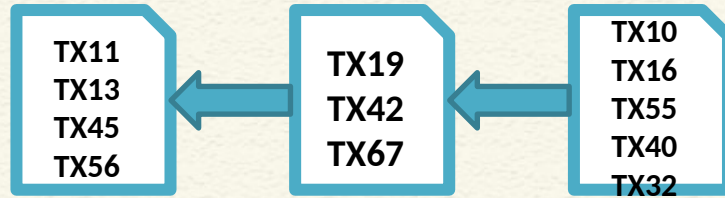
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness

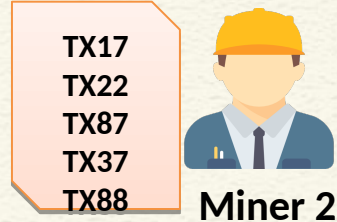


Liveness: Add a block as long as it is correct
(contains valid transactions from the unconfirmed TX list)
and move further

Unconfirmed TX



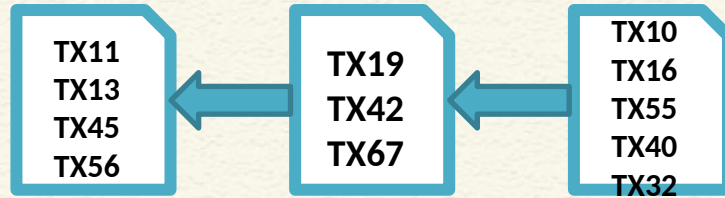
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness



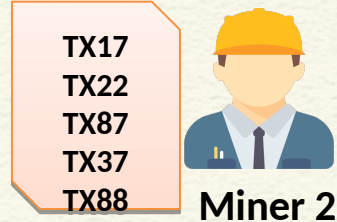
Two (or more) different miners may add two (or more) different blocks

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

Unconfirmed TX



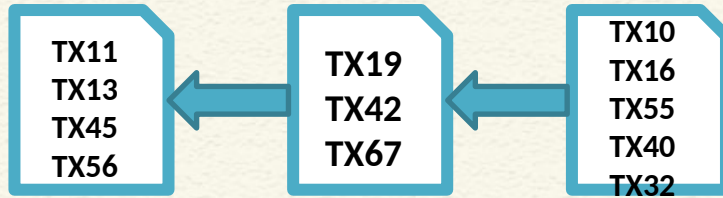
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness



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

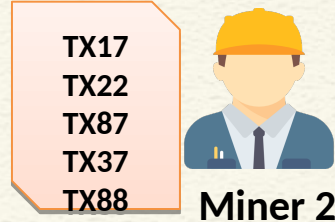
Will resolve this later!

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

Unconfirmed TX



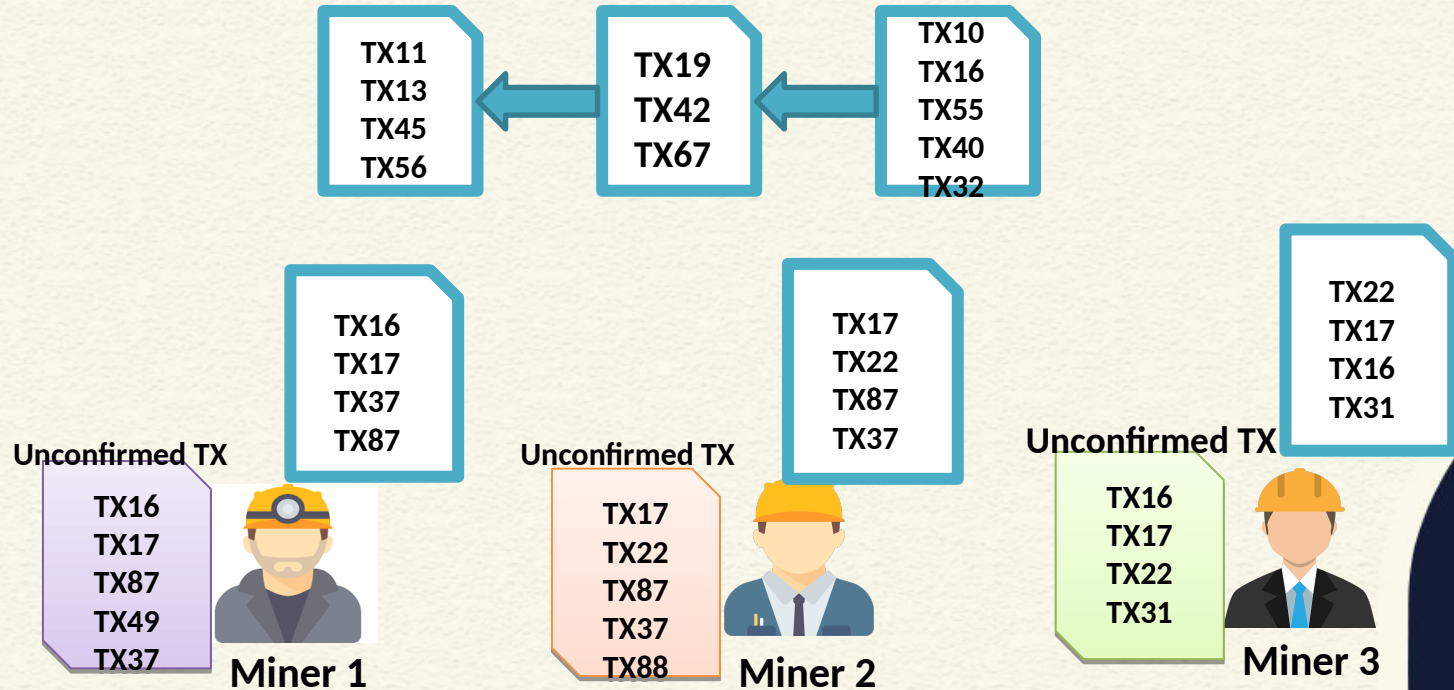
Unconfirmed TX



Unconfirmed TX

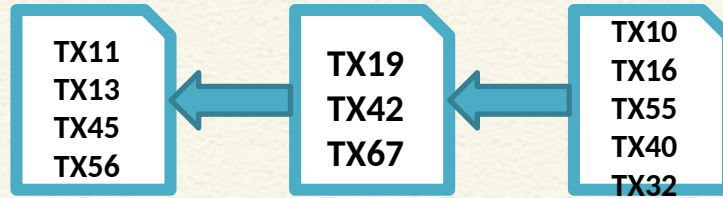


Safety vs Liveness



Safety vs Liveness

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



Unconfirmed TX

TX16
TX17
TX87
TX49
TX37



Miner 1

TX16
TX17
TX37
TX87

Unconfirmed TX

TX17
TX22
TX87
TX37
TX88



Miner 2

TX17
TX22
TX87
TX37

Unconfirmed TX

TX16
TX17
TX22
TX31

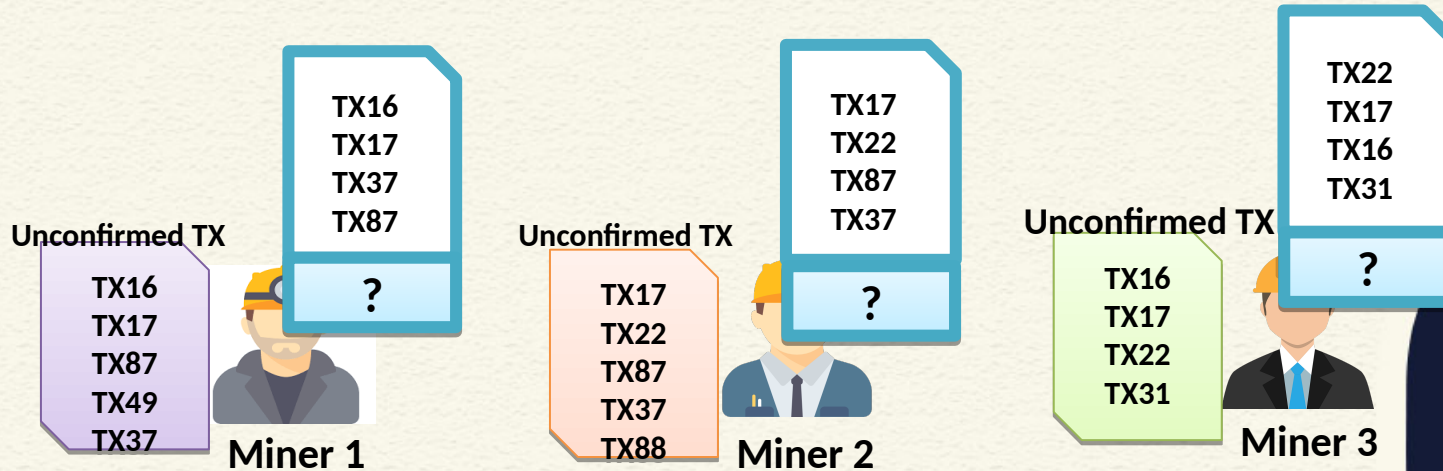
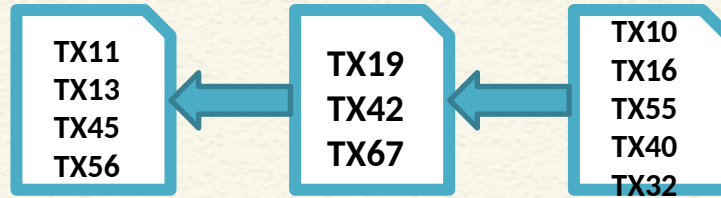


Miner 3

TX22
TX17
TX16
TX31

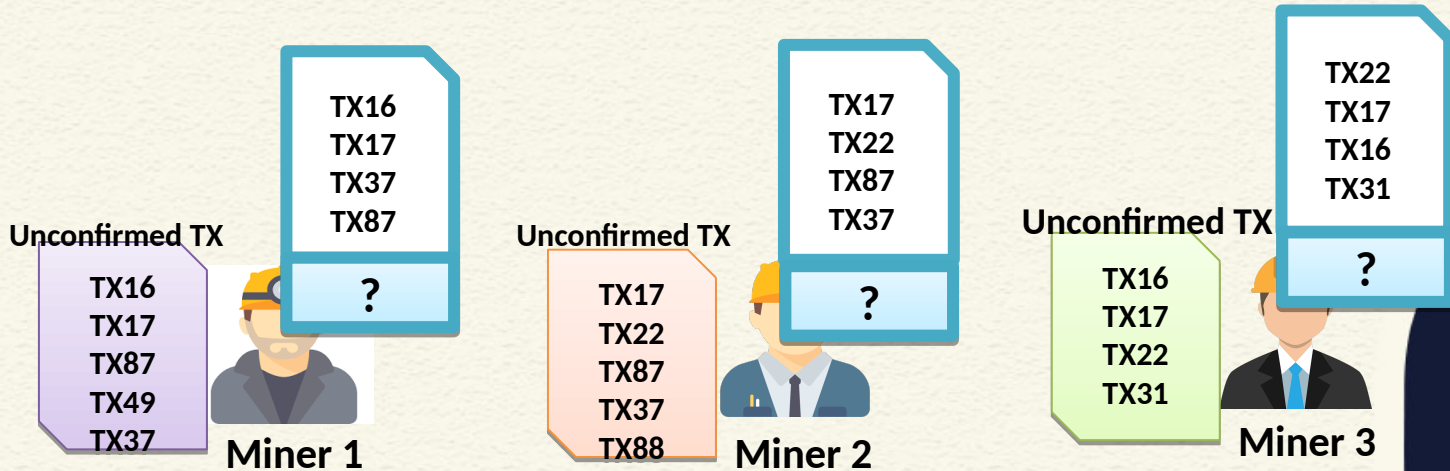
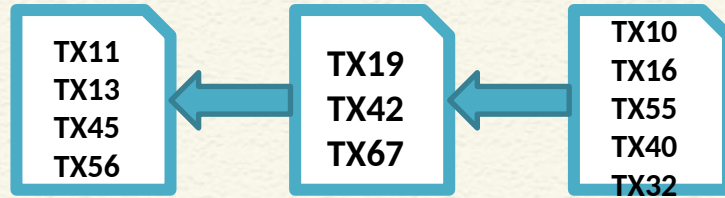
Safety vs Liveness

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



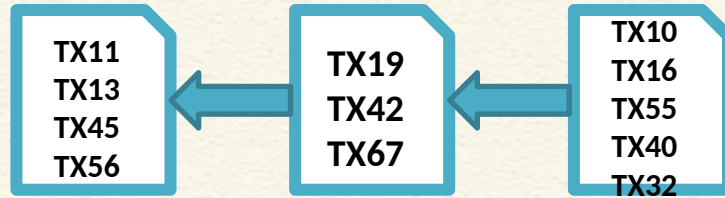
Safety vs Liveness

- 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

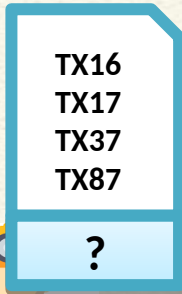


Unconfirmed TX

TX16
TX17
TX87
TX49
TX37



Miner 1

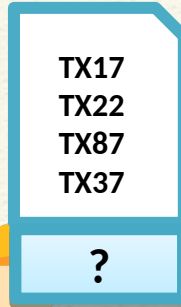


Unconfirmed TX

TX17
TX22
TX87
TX37
TX88

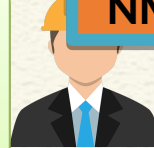


Miner 2

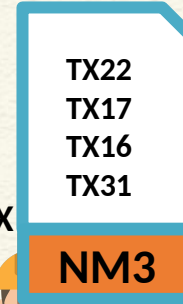


Unconfirmed TX

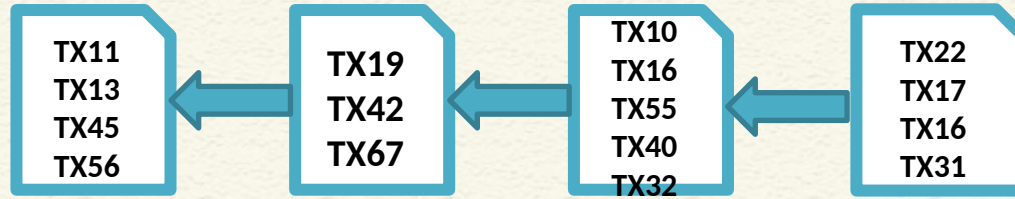
TX16
TX17
TX22
TX31



Miner 3



Safety vs Liveness

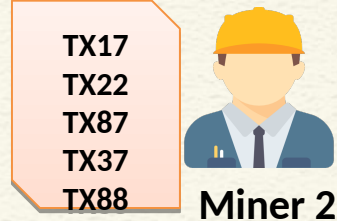


- Sign the block and broadcast
 - Gossip over the P2P network

Unconfirmed TX



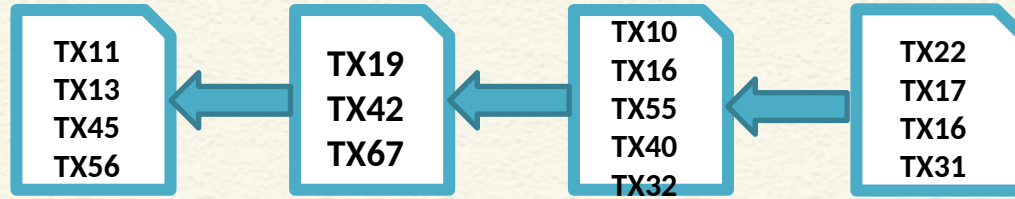
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness

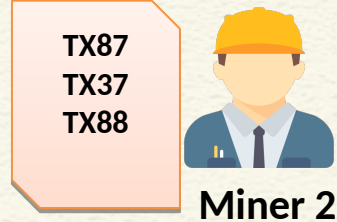


- Remove the committed transactions from unconfirmed TX list

Unconfirmed TX



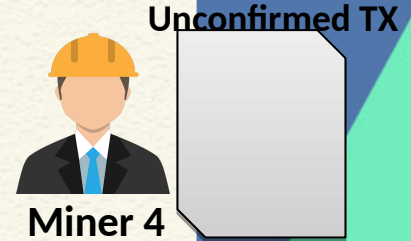
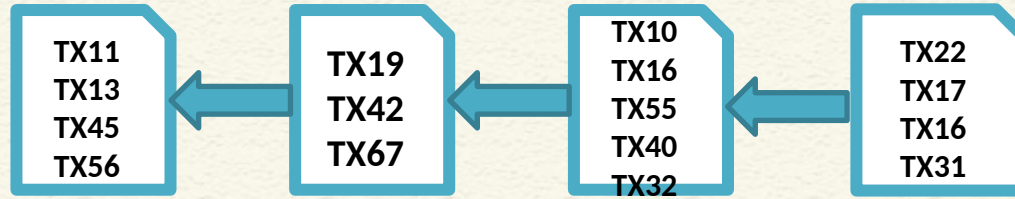
Unconfirmed TX



Unconfirmed TX



Safety vs Liveness

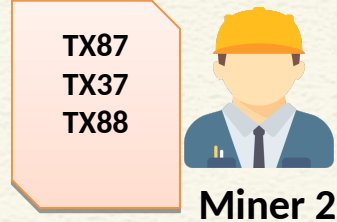


- Start the next round ...

Unconfirmed TX



Unconfirmed TX



Unconfirmed TX



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?



*Thank
you*

