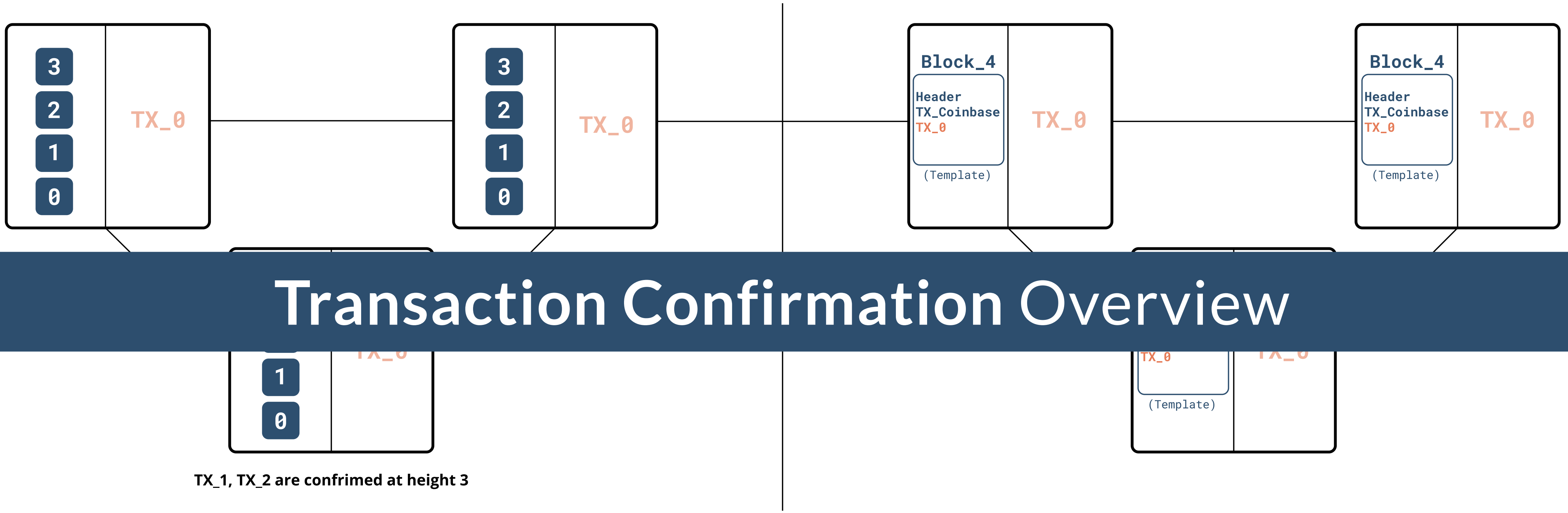
Transaction Confirmation Overview



TX_1, TX_2 are confirmed at height 3

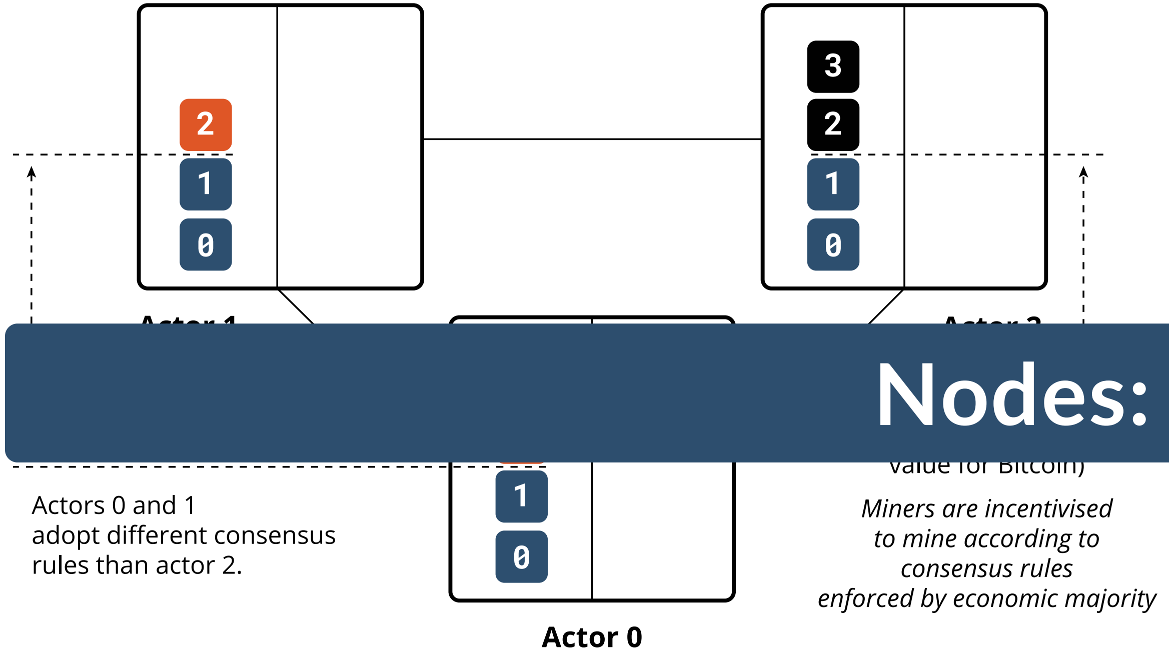
1. New transaction is signed and broadcast
Coin ownership secured by public key cryptography.

2. Transaction propagates through p2p mempool
Transactions are buffered, not yet confirmed.

3. Miners build block with mempool transactions
Incentivised to include TX with highest fees.

4. Nodes accept first block with valid block hash
Chain is extended by new block.

Nodes: Validation



value for Bitcoin)

Miners are incentivised to mine according to consensus rules enforced by economic majority

Actors 0 and 1 adopt different consensus rules than actor 2.

Actors validate confirmation of received coin.

- Resist double spend / Inflation.
- Anonymity for covert validation.
- Trade in Bitcoin (for goods/service) gives it value.

Block size / Block interval / TX formats / Scripting.

- Incompatible rules imply different coin

The economic majority decides valuable coin

- Economic majority != Node majority.
- Economic majority exchanges most value for coin.

Miner incentivised to grind for valuable coin

Miners: Transaction Ordering

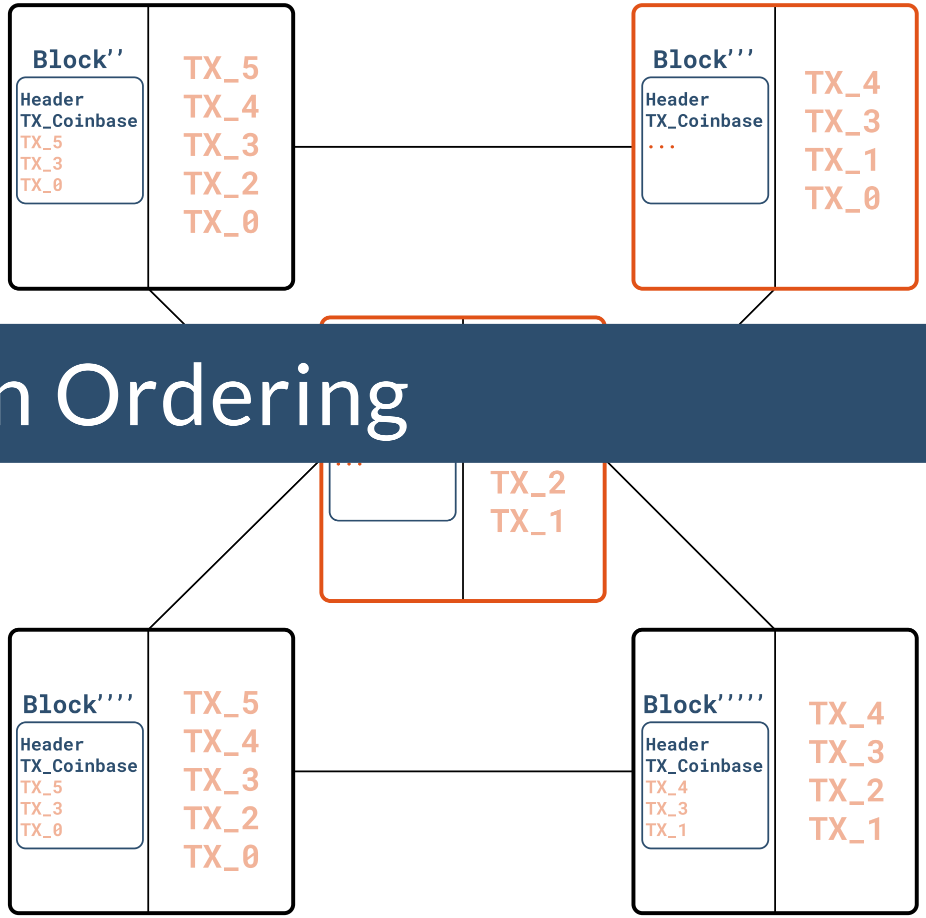
Provide transaction ordering service

- Solution to Byzantine's General's Problem
- Proof-of-work is anonymous and verifiable
- Miner chooses which/any transaction to include

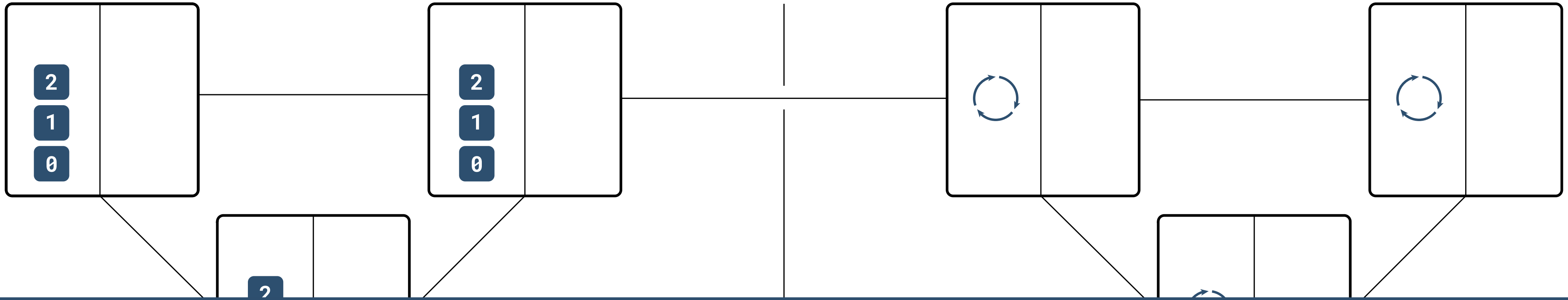
- Majority can sustainably mine longest chain
- Majority can omit selected/all transactions,

Miner majority can be diluted anytime

- Anonymous hashing power can be added
- Incentivised by higher fees
- Censorship can be resisted with higher fees



**As fees increase,
non-censoring mining power
dilutes censoring miner-share.**



Security Model Summary

Actors use Bitcoin to collectively resist money tax

- Inflation, Forex, Censorship, Regulation, Direct tax.
- Utility of Bitcoin = alternative money tax.
- Full node enables anonymous transaction validation.

Economic majority decides on coin to exchange for value

- Validation rule set adoption implies best utility.

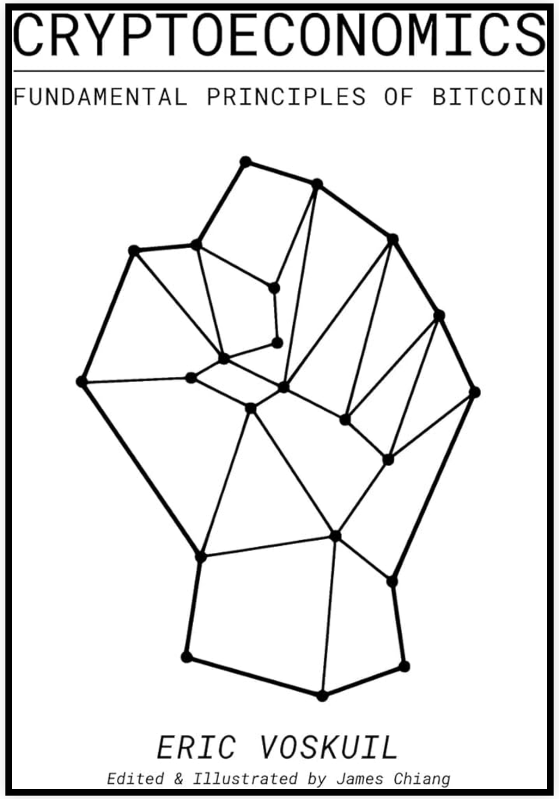
Public key cryptography secures coin ownership

- Only private key can spend.

Miners provide a transaction ordering service

- Network consensus on TX ordering (Byzantine).
- Transaction confirmation incentivised by fees.
- Miner hash power share can be diluted anytime, which counteracts censorship power of miner majority.

Reading recommendation



CRYPTOECONOMICS

FUNDAMENTAL PRINCIPLES OF BITCOIN

ERIC VOSKUIL

Edited & Illustrated by James Chiang

Or online: Libbitcoin wiki