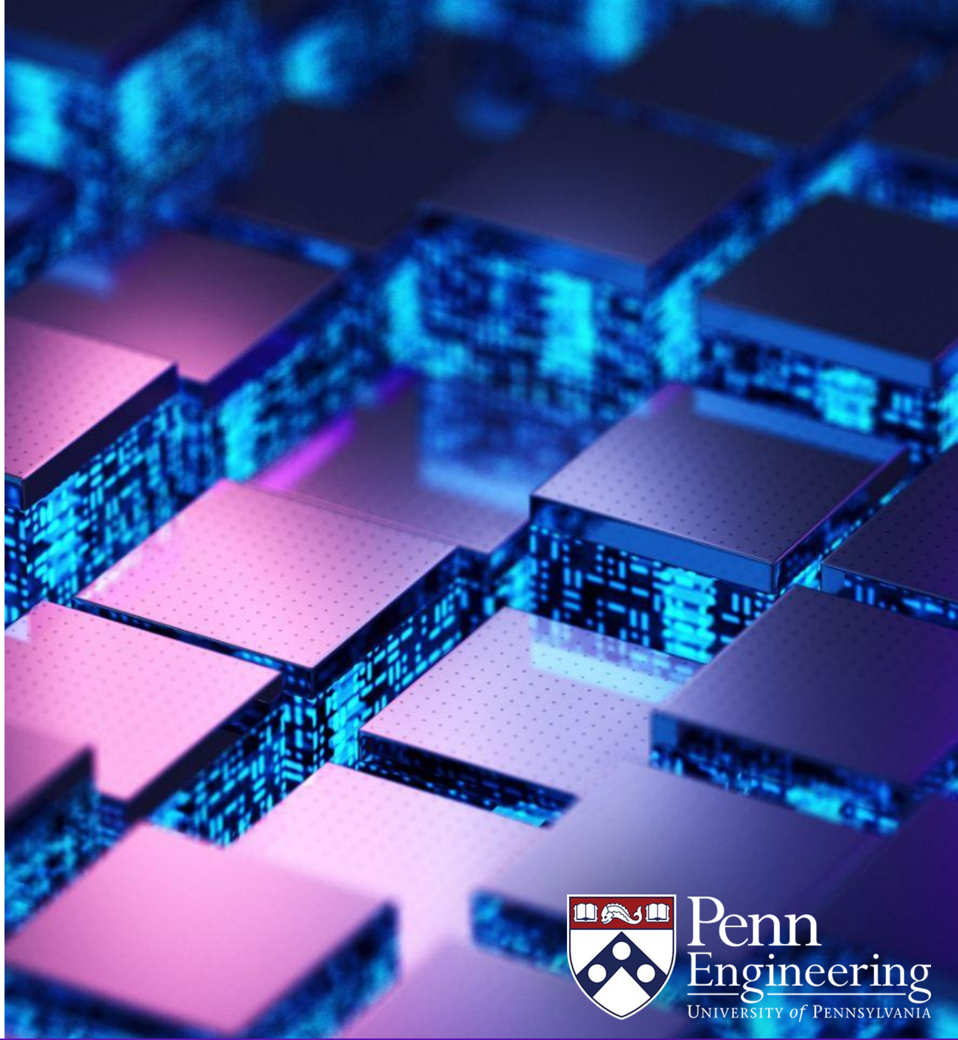
EAS 5830: BLOCKCHAINS

Committee-based consensus



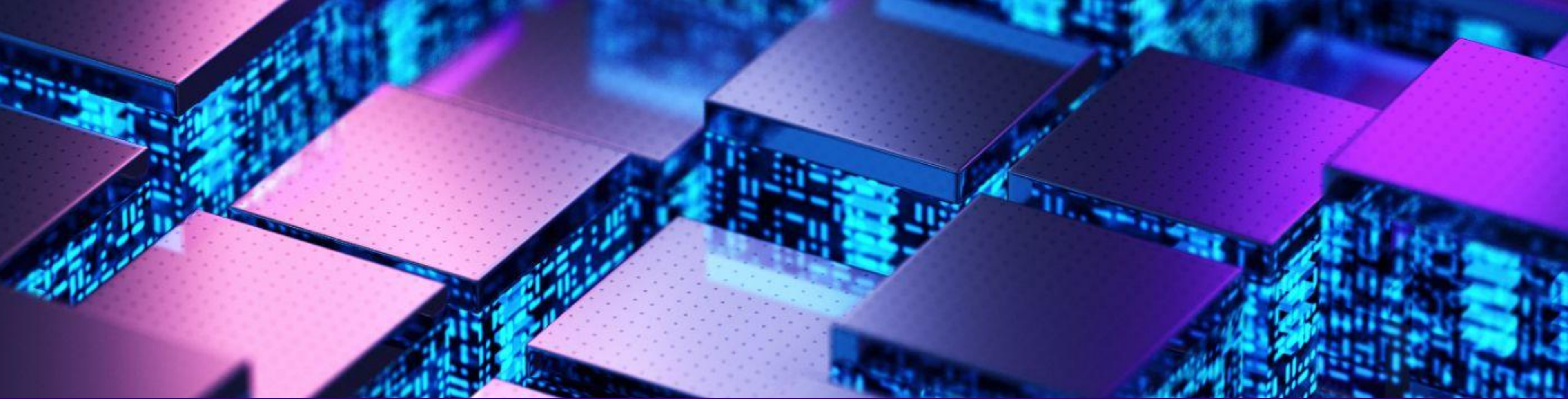
Dr. Brett Hemenway Falk

Committee-based consensus

- Select a “committee”Committee produces blocks
- Committee “certifies” blocks by running a classical consensus mechanism

How does committee reach consensus?

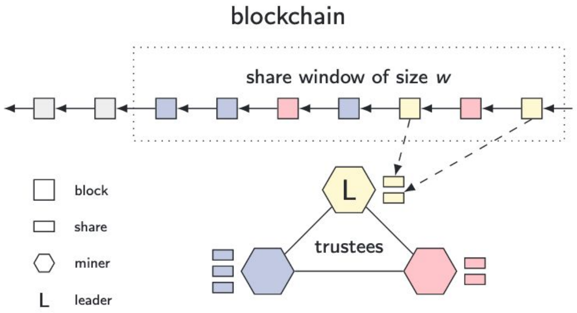
- PBFT
- Tendermint
  - CometBFT
- Clique
- Aura
- Hotstuff



Selecting a committee

Byzcoin

- Committee-based consensus with PoW
  - ByzCoin
- Committee is selected based on hash power
- Committee runs PBFT to “certify” blocks

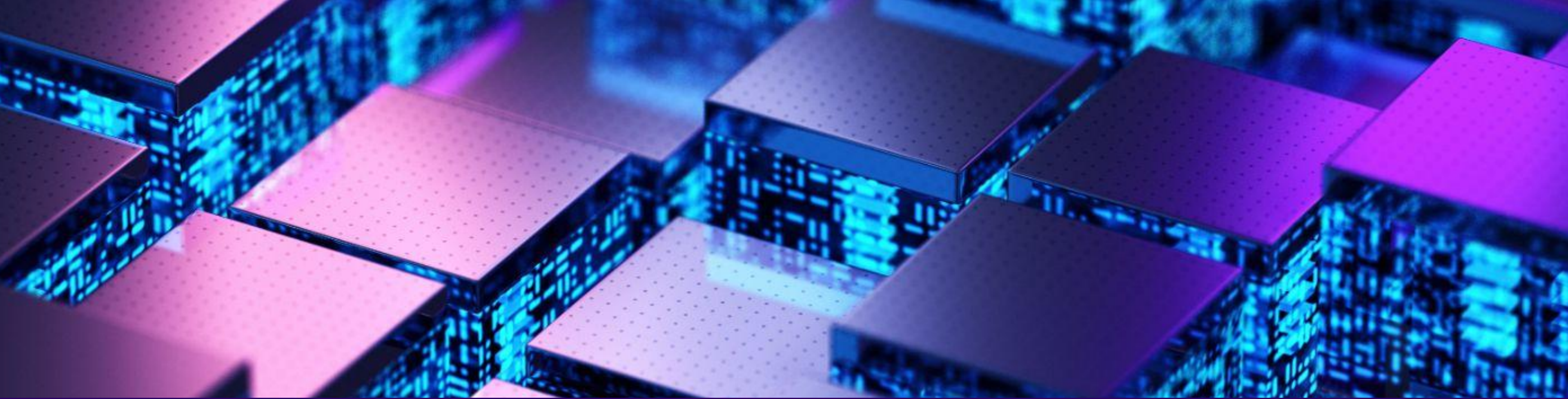


How do you select a committee?

- Sybil Resistance (identifying voters)
  - Proof-of-Stake
  - Proof-of-work
- Voting mechanism
  - Single-vote
    - Most Cosmos Chains
    - BNB
    - Tron
  - Approval voting
    - EOS
    - TELOS
  - Lottery
    - Algorand
    - Espresso

Blockchains using committee-based consensus

- Cosmos
  - Crypto.org
  - Secret
  - Osmosis
  - Terra
  - And More
- BNB
- Polygon PoS
- Algorand
- Tron
- EOS
  - TELOS



Pros of Committee-Based Consensus

Specialization

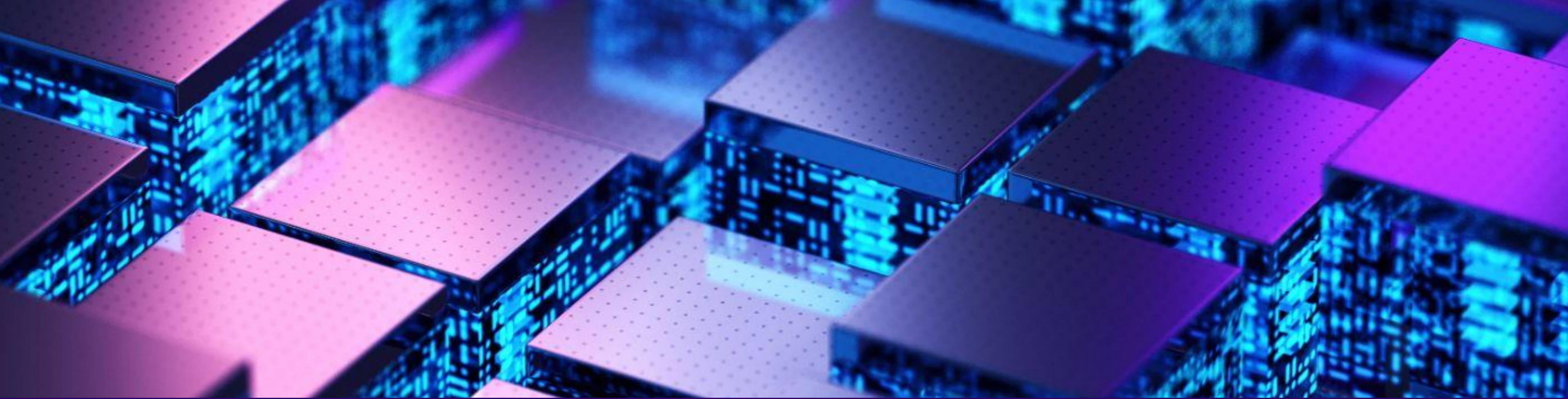
- Professional block producers can have high-capacity hardware
- Leads to
  - Better uptime
  - Higher throughput

Instant Finality

- Nakamoto Consensus has “eventual finality”
  - Consensus based on the “longest-chain rule”
  - This causes forks:
    - Ethereum had about 300 “uncles” per day (pre-merge)
    - Bitcoin has fewer than 1 “uncle” per month
- Committee-based consensus can achieve “instant finality”
  - Instant finality means that once a block is finalized, it is finalized forever
    - All existing blockchains using committee-based consensus achieve instant finality
    - Instant finality means no forks
  - Finality comes from the safety of the permissioned consensus algorithm run by the committee

Committee can perform functions beyond consensus

- Secret mempool
  - Secret Network (SGX)
  - Osmosis (Distributed Key Generation)
- Long-term secrets
  - Can a public-blockchain keep a secret?
- Price oracles
  - Block producers can provide price feeds
- Elections
  - Block producers can control another chain
- Manage cross-chain liquidity
  - Thorchain, Axelar, Zetachain



Cons of Committee-Based Consensus

The committee must be small

- Binance Chain uses 11 Block Producers
- BNB chain uses 21 Block Producers
- EOS uses 21 Block Producers
- Tron uses 27 Block Producers
- Oasis uses 110 Block Producers
- Cosmos uses 180 Block Producers
- Algorand uses 20-6000 Committee Members

The committee may become static

- First 89 million blocks of EOS produced by only 63 producers
- First 9 million blocks on Cosmos Hub produced by 215 producers
  - First 55,000 Bitcoin blocks had payouts to more than 275,000 addresses
  - First 8 million blocks of Ethereum mined by more than 5,000 distinct addresses