CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Elective Course on Mastering Blockchain: Foundations to Consensus, session-09

Blockchain Trust and Consensus - II

Raghava Mukkamala

Associate Professor & Director, Centre for Business Data Analytics

Copenhagen Business School, Denmark

Email: rrm.digi@cbs.dk, Centre: https://cbsbda.github.io/

Course Coordinator at SRMIST:

Prof. K. Shantha Kumari

Associate Professor

Data Science and Business Systems Department,

SRM Institute of Science and Technology, India

Shanthak@srmist.edu.in

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION AMBA ACCREDITED CEMS PIM

Outline

- Improvements to the Nakamoto Consensus Protocol
- Proof-of-Stake Based Consensus Protocols
  - Chain-Based PoS Consensus
  - Committee-Based Proof-of-Stake
  - BFT-Based Proof-of-Stake
  - Delegated Proof-of-Stake (DPoS)
- Vulnerabilities of Proof-of-Stake Based Consensus Protocols

Quick Recap:
Proof-of-Work/Nakamoto Consensus Protocol

https://alexey-shepelev.medium.com/hierarchical-key-generation-fc27560f786

CBS

Components of Blockchain Consensus Protocol

The following are the five key components of a blockchain consensus protocol

- Block Proposal: Generating blocks and attaching generation proofs.
- Information Propagation: Disseminating blocks and transactions across the network.
- Block Validation: Checking blocks for generation proofs and transaction validity.
- Block Finalization: Reaching agreement on the acceptance of validated blocks.
- Incentive Mechanism: Promoting honest participation and creating network tokens.

Baliga, A. (2017). Understanding blockchain consensus models. Persistent, 4(1), 14. (White paper)
Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In Concurrency: the works of leslie lamport (pp. 203-226).
George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair. Distributed Systems: Concepts and Design Fifth Edition

Nakamoto Consensus Protocol

- The Nakamoto consensus protocol is the key innovation behind Bitcoin and inspired many other cryptocurrency systems, such as Ethereum and Litecoin
- The Nakamoto consensus protocol is summarized by the following rules:
- Block Proposal: Proof of Work (PoW)
    - Block generation requires finding a preimage to a hash result that satisfies a difficulty target, which is dynamically adjusted to maintain an average block generation interval.
- Information Propagation: Gossiping Rule
    - Any newly received or locally generated transaction or block should be immediately advertised and broadcast to peers.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Baliga, A. (2017). Understanding blockchain consensus models. Persistent, 4(1), 14. (White paper)

Nakamoto Consensus Protocol

- Block Validation: Validation Rule
  - A block or transaction must be validated before being broadcast to peers or appended to the blockchain. The validation includes a double-spending check on transactions and proof-of-work validity check on the block header.
- Block Finalization: Longest-Chain Rule
  - The longest chain represents network consensus, which should be accepted by any node that sees it. Mining should always extend the longest chain.
- Incentive Mechanism: Block Rewards and Transaction Fees
  - Generator of a block can claim a certain amount of new tokens plus fees collected from all enclosed transactions in the form of a coinbase transaction to itself.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Baliga, A. (2017). Understanding blockchain consensus models. Persistent, 4(1), 14. (White paper)

Security Analysis of Nakamoto Consensus Protocol

- The fault tolerance of Nakamoto consensus is characterized by the percentage of adversarial hashing power the system can tolerate.

- As long as less than 50% of total hashing power is maliciously controlled, the blocks produced by honest miners are timely propagated, and the main chain by the honest majority can eventually outgrow any malicious branch.

- From the perspective of classical distributed consensus, Nakamoto consensus cleverly circumvents the fundamental 1/3 BFT bound by adopting probabilistic finality.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Baliga, A. (2017). Understanding blockchain consensus models. Persistent, 4(1), 14. (White paper)

Improvements to the Nakamoto Consensus Protocol

Image by rawpixel.com on Freepik

Slides based on Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

CBS

GHOST Protocol

- A variation of GHOST (greedy heaviest-observed subtree) implemented in the previous **Ethereum blockchain** results in a much shorter block interval (10-15 seconds).
- It achieved up to 25 TPS throughput (against Bitcoin's 10-minute block interval and 7 TPS throughput)
- According to the longest-chain rule in Nakomoto protocol/Bitcoin, all unconfirmed blocks in a fork shall be orphaned, wasting honest mining power.
- The longest-chain rule also limits the transaction capacity since there is a tight tradeoff between performance and security.
- The GHOST rule is an alternative to the longest-chain rule in that the orphaned blocks also contribute to the main chain security, effectively reducing the impacts of forks,.

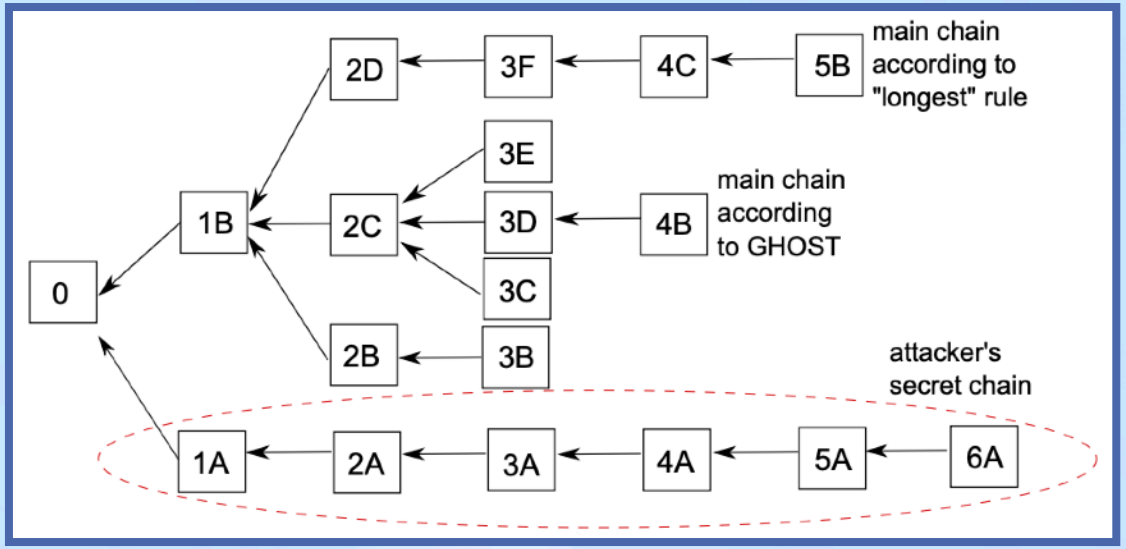


Fig. 3. A block tree in which the longest chain and the chain selected by GHOST differ. An attacker's chain is able to switch the longest chain, but not the one selected by GHOST.

- Like the Nakamoto consensus, the probabilistic finality of the heaviest subtree up to the current block height will hold as long as more than 50% of the mining power is honest.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

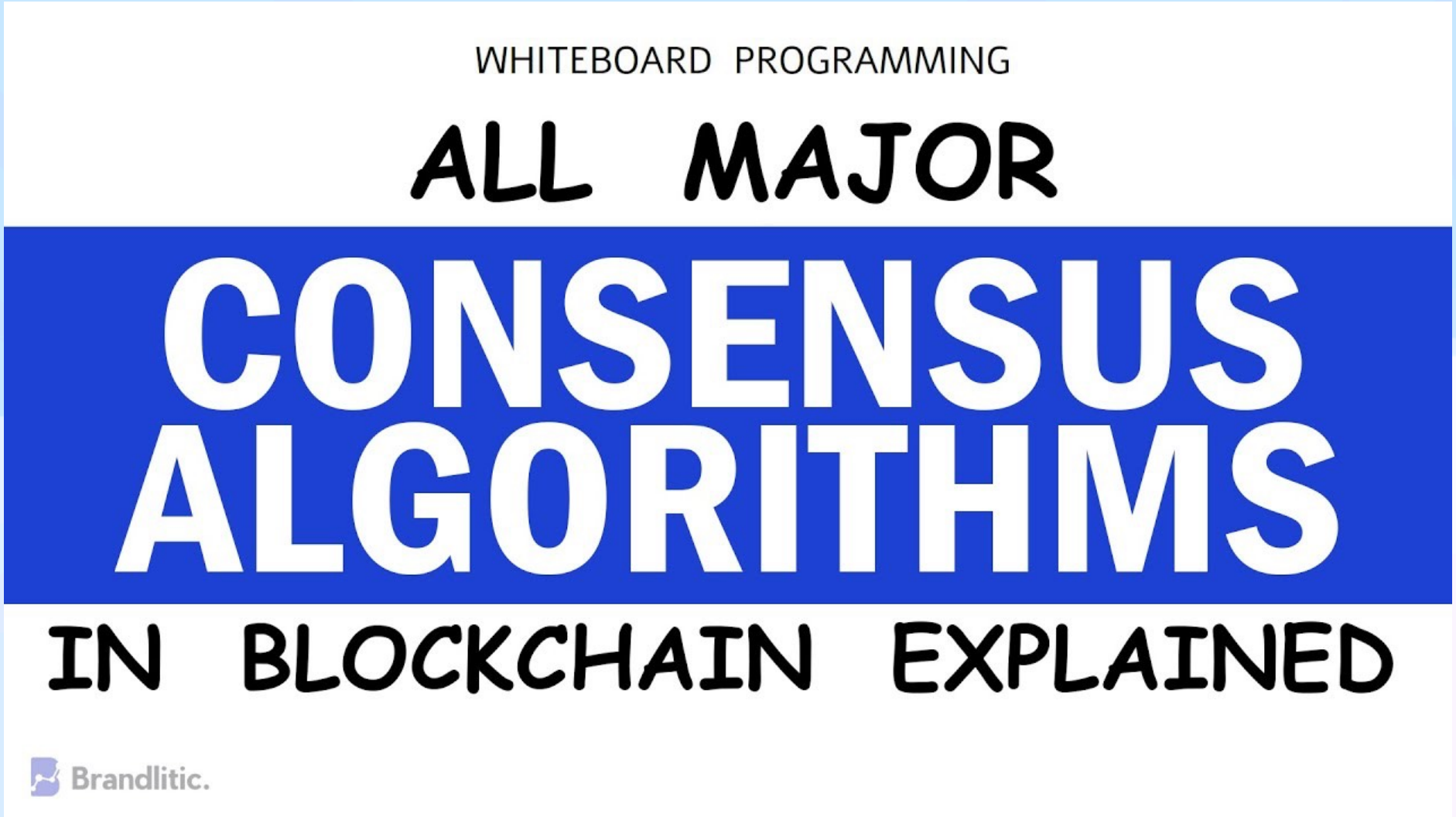
Sompolinsky, Y., & Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. In Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19 (pp. 507-527). Springer Berlin Heidelberg.

List of Major Consensus Protocols and Their Applications

https://alexey-shepelev.medium.com/hierarchical-key-generation-fc27560f786

CBS

All Major Blockchain Consensus Algorithms Explained | Consensus Mechanism in Blockchain



https://www.youtube.com/watch?v=sXP-8pD7PG4&t=1s

Proof of Work (PoW)

1. Proof of Work (PoW)

- **Description**: PoW requires miners to solve complex mathematical puzzles to validate transactions and create new blocks. The first miner to solve the puzzle gets to append the block and is rewarded with cryptocurrency.
- **Practical Blockchain Applications**:
  - **Bitcoin (BTC)**: The original blockchain that introduced PoW. It remains one of the most secure and decentralized networks.
  - **Ethereum (ETH)**: Initially used PoW before transitioning to Proof of Stake (PoS) with Ethereum 2.0.
  - **Litecoin (LTC)**: A faster and lighter version of Bitcoin, also using PoW.
  - **Monero (XMR)**: Privacy-focused cryptocurrency that also uses PoW.
  - **Zcash (ZEC)**: A privacy coin that employs PoW.

litecoin

Proof of Stake (PoS)

2. Proof of Stake (PoS)

- **Description**: PoS selects validators based on the number of coins they hold and are willing to "stake" as collateral. Validators confirm transactions and create blocks, and they are rewarded with new coins or transaction fees.
- **Practical Blockchain Applications**:
  - **Ethereum 2.0**: Transitioned from PoW to PoS in 2022 to enhance scalability and energy efficiency.
  - **Cardano (ADA)**: Uses a PoS algorithm called Ouroboros to offer scalability and sustainability.
  - **Polkadot (DOT)**: Uses PoS to secure a heterogeneous multichain.
  - **Tezos (XTZ)**: Implements a liquid PoS mechanism, where participants can delegate staking rights without transferring ownership.
  - **Cosmos (ATOM)**: Uses a PoS consensus algorithm to allow multiple blockchain interactions.

Delegated Proof of Stake (DPoS)

3. Delegated Proof of Stake (DPoS)

- **Description**: In DPoS, users vote for a small number of delegates to validate transactions and create new blocks. This improves efficiency and speeds up block creation.
- **Practical Blockchain Applications**:
  - **EOS (EOS)**: Uses DPoS to offer a highly scalable platform for decentralized applications (dApps).
  - **Tron (TRX)**: Also uses DPoS to offer fast and scalable transactions, primarily for content distribution platforms.
  - **Steem (STEEM)**: A social media platform with a DPoS mechanism.
  - **BitShares (BTS)**: A decentralized exchange platform using DPoS for faster consensus.

Practical Byzantine Fault Tolerance (PBFT)

4. Practical Byzantine Fault Tolerance (PBFT)

- **Description**: PBFT ensures consensus even when some nodes in the network are faulty or malicious. Nodes must communicate to agree on the next block, requiring a two-thirds majority.
- **Practical Blockchain Applications**:
  - **Hyperledger Fabric**: A permissioned blockchain platform for enterprises that uses PBFT for finality.
  - **Zilliqa (ZIL)**: Uses PBFT for consensus within shards of its network, ensuring high throughput.
  - **Stellar (XLM)**: Uses a variant of PBFT called the Stellar Consensus Protocol (SCP) for fast and scalable payment settlements.

HYPERLEDGER

Proof of Authority (PoA)

5. Proof of Authority (PoA)

- **Description**: PoA relies on a small group of trusted validators who are authorized to validate blocks. It is typically used in private or consortium blockchains.
- **Practical Blockchain Applications**:
  - **VeChain (VET)**: Uses PoA for supply chain management and enterprise-level applications.
  - **Ethereum (Testnet)**: PoA is used in Ethereum's Rinkeby and Kovan testnets.
  - **Microsoft Azure**: Uses PoA for blockchain applications in enterprise environments.

Proof of Burn (PoB)

6. Proof of Burn (PoB)

- **Description**: In PoB, miners "burn" coins by sending them to an address where they are permanently destroyed. This gives them the right to create new blocks, and the amount burned represents their stake in the network.
- **Practical Blockchain Applications**:
  - **Slimcoin**: Uses PoB to incentivize long-term investment.
  - **Counterparty (XCP)**: Originally used PoB to distribute tokens by burning Bitcoin.

7. Proof of Elapsed Time (PoET)

- **Description**: PoET is an energy-efficient consensus mechanism that uses trusted execution environments (like Intel SGX) to ensure that nodes "wait" for a randomly assigned period before creating new blocks.
- **Practical Blockchain Applications**:
  - **Hyperledger Sawtooth**: A modular blockchain platform that uses PoET for efficient consensus in permissioned environments.

8. Directed Acyclic Graph (DAG)

- **Description**: DAGs represent a different structure where transactions are confirmed by referring to previous transactions. There are no blocks, and validation is done simultaneously, increasing speed and scalability.
- **Practical Blockchain Applications**:
  - **IOTA (MIOTA)**: Uses the Tangle, a DAG-based system, for machine-to-machine transactions and IoT applications.
  - **Hedera Hashgraph (HBAR)**: Uses a DAG-based consensus algorithm for high-throughput decentralized applications.
  - **Nano (NANO)**: Uses a block-lattice structure (a form of DAG) for feeless, scalable transactions.

11. Proof of Importance (PoI)

- **Description**: PoI measures the "importance" of a participant based on their coin holdings, transaction activity, and network interaction to validate transactions and create new blocks.
- **Practical Blockchain Applications**:
  - **NEM (XEM)**: Uses PoI to determine who can add blocks to the chain, factoring in reputation and activity, not just stake.

12. Proof of History (PoH)

- **Description**: PoH is used to timestamp transactions and prove the passage of time between events. This is typically used alongside other consensus mechanisms to ensure scalability and performance.
- **Practical Blockchain Applications**:
  - **Solana (SOL)**: Combines PoH with PoS to achieve high throughput and scalability, making it ideal for decentralized finance (DeFi) and dApp platforms.

Proof-of-Stake Based Consensus Protocols

https://alexey-shepelev.medium.com/hierarchical-key-generation-fc27560f786

CBS

Proof of Stake

- Proof-of-Stake (PoS) originates from the Bitcoin community as an energy efficient alternative to PoW mining.
- Simply put, a stake refers to the coins or network tokens owned by a participant that can be invested in the blockchain consensus process.
- From the security point of view, PoS leverages token ownership for Sybil attack mitigation. Compared to a PoW miner whose chance to propose a block is proportional to its brute-force computation power, the chance to propose a block for a PoS miner is proportional to its stake.
- From the economic point of view, PoS moves a miner's opportunity cost from **outside the system** (waste of computation power and electricity) to **inside the system** (loss of capital and investment gain).
- Because of the lack of real mining, we often refer to a PoS miner as a **validator**, **minter**, or **stakeholder** for PoS's close resemblance to investing in capital markets.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
[7] : I Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. NSDI*, 2016, pp. 45–59.
[85] : https://docs.waves.tech/en/blockchain/waves-protocol/waves-ng-protocol#_1-1-problem-statement-and-motivation

Proof of Stake (PoS)

Four classes of PoS protocols:

- chain-based PoS,
- committee-based PoS,
- BFT-based PoS, and
- delegated PoS (DPoS).
- Chain-based PoS inherits many of the components of the Nakamoto consensus protocol such as information propagation, block validation, and block finalization (i.e., longest-chain rule), except that the block generation mechanism is replaced with PoS.

Chain-based PoS

A1	Peercoin	2012
A2	Nxt	2013
A3	Bentov's PoA	2014

Committee-based PoS

B1	Bentov's CoA	2017
B2	Ourosboros	2017
B3	Snow White	2017
B4	Ourosboros Praos	2017

BFT-based PoS

C1	Tendermint	2014
C2	Algorand	2017
C3	Casper FFG	2017

Delegated PoS (DPoS)

D1	BitShares 2.0	2015
D2	Lisk	2016
D3	EOS.IO	2017
D4	Cosmos	2019

Performance Highlights

Consensus Group Size
Uncontrolled: A, C2, C3, B3, B4
Controlled: B1, B2, C1, D

Consensus Finality
Probabilistic: A, B
Deterministic: C, D

Est. Throughput (TPS)
<100: A
100-1K: B, C2
>1K: C1, C3 (if sharding used), D

Consensus Fault Tolerance
50% Stake: A, B
33% Stake: C
33% Consensus Participants: C1, D

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
[7] : I Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. NSDI*, 2016, pp. 45–59.
[85] : https://docs.waves.tech/en/blockchain/waves-protocol/waves-ng-protocol#_1-1-problem-statement-and-motivation

Chain-Based PoS

- Committee-based PoS leverages a multiparty computation (MPC) scheme to determine a committee to orderly generate blocks.
- BFT-based PoS combines staking with BFT consensus, which guarantees the deterministic finality of blocks.
- DPoS employs a social voting mechanism that elects a fixed-size group of delegates for transaction validation and blockchain consensus on behalf of the voters.

Chain-based PoS

A1	Peercoin	2012
A2	Nxt	2013
A3	Bentov's PoA	2014

Committee-based PoS

B1	Bentov's CoA	2017
B2	Ourosboros	2017
B3	Snow White	2017
B4	Ourosboros Praos	2017

BFT-based PoS

C1	Tendermint	2014
C2	Algorand	2017
C3	Casper FFG	2017

Delegated PoS (DPoS)

D1	BitShares 2.0	2015
D2	Lisk	2016
D3	EOS.IO	2017
D4	Cosmos	2019

Performance Highlights

Consensus Group Size
Uncontrolled: A, C2, C3, B3, B4
Controlled: B1, B2, C1, D

Consensus Finality
Probabilistic: A, B
Deterministic: C, D

Est. Throughput (TPS)
<100: A
100-1K: B, C2
>1K: C1, C3 (if sharding used), D

Consensus Fault Tolerance
50% Stake: A, B
33% Stake: C
33% Consensus Participants: C1, D

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
[7] : I Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. NSDI*, 2016, pp. 45–59.
[85] : https://docs.waves.tech/en/blockchain/waves-protocol/waves-ng-protocol#_1-1-problem-statement-and-motivation

Vulnerabilities of Proof-of-Stake Based Consensus Protocols

https://alexey-shepelev.medium.com/hierarchical-key-generation-fc27560f786

CBS

Costless Simulation

- Although heralded as the most promising mechanism to replace PoW, PoS still faces several vulnerabilities.
- Costless simulation is a major vulnerability of non-BFT-based PoS schemes, especially chain-based PoS in which PoS is used to simulate the would-be PoW process.
- Costless simulation literally means any player can simulate any segment of blockchain history at the cost of no real work but speculation, as PoS does not incur intensive computation while the blockchain records all staking history.
- This may give attackers shortcuts to fabricate an alternative blockchain.
- The four subsequent vulnerabilities, namely nothing-at-stake, posterior corruption attack, long-range attack, and stake-grinding attack, are all based on costless simulation.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

Centralization Risk

- PoS faces a similar wealth centralization risk as PoW. In PoS the minters can lawfully reinvest their profits into staking perpetually, which allows the one with a large sum of unused tokens to become wealthier and eventually reach a monopoly status.
- When a player owns more than 50% of tokens in circulation, the consensus process will be dominated by this player and the system integrity will not be guaranteed.
- Take Ethereum's Casper FFG for example, the proposed PoS scheme is built upon the current PoW system, of which the cryptocurrency ethers can be directly used for staking.

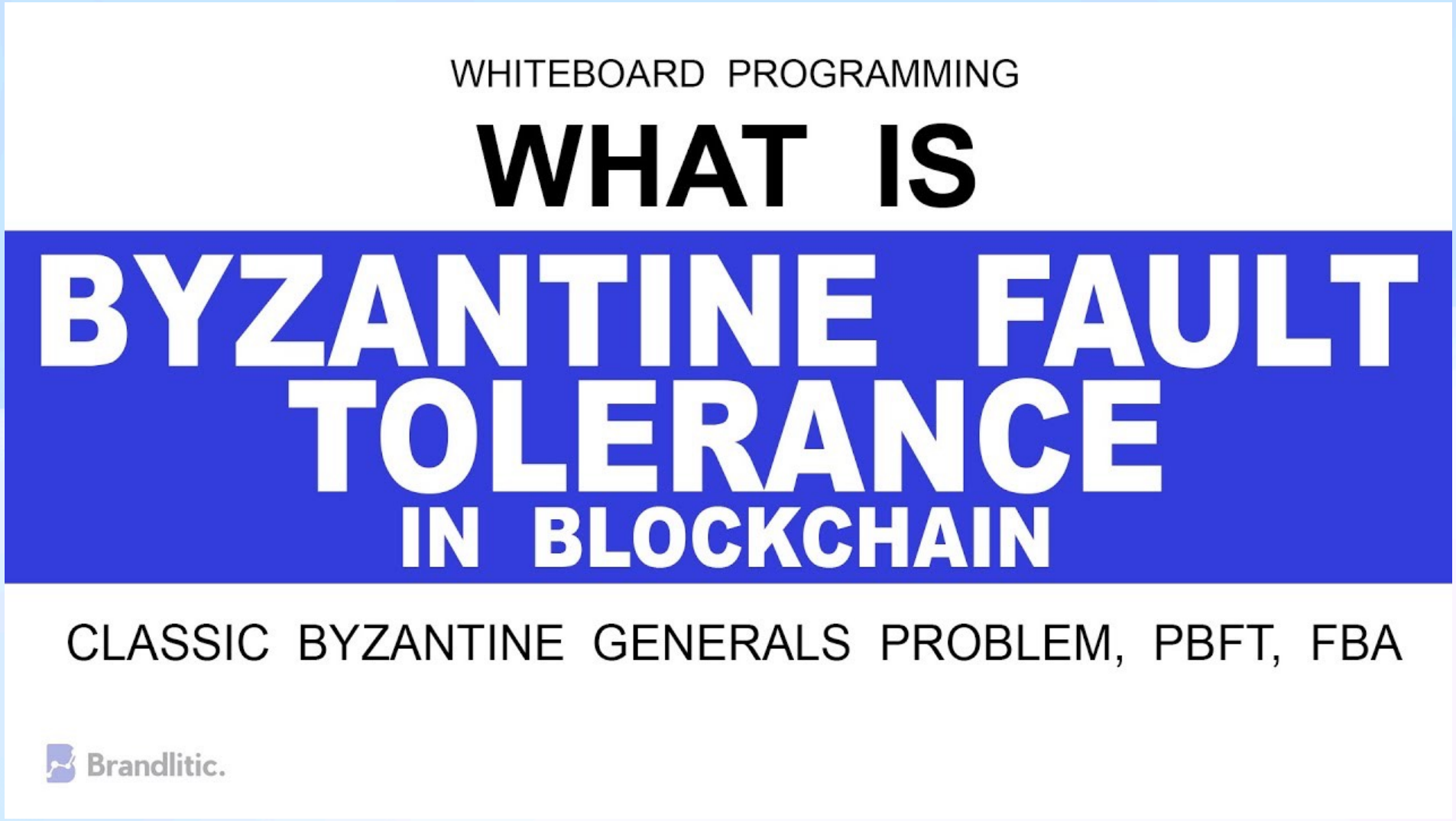
Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Deirmentzoglou, E., Papakyriakopoulos, G., & Patsakis, C. (2019). A survey on long-range attacks for proof of stake protocols. IEEE Access, 7, 28712-28725.

Centralization Risk

- This gives initial advantages to those who have already accumulated huge wealth during Ethereum's PoW operation.
- Potential countermeasures against monopolization in PoS mainly come from the incentive mechanism and economic perspective.
- In addition to the stake valuation scheme that improves the winning chances of small stakeholders (Chain-Based PoS),
- We can use off-chain factors to complicate the staking process (EOSIO for example) and impose taxation on the blocks generated by large stakeholders, to name a few.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Deirmentzoglou, E., Papakyriakopoulos, G., & Patsakis, C. (2019). A survey on long-range attacks for proof of stake protocols. IEEE Access, 7, 28712-28725.

Byzantine Fault Tolerance in Blockchain | Classic Generals Problem & its Solutions: PBFT & FBA



https://www.youtube.com/watch?v=sF7p-RUQXNI&t=1s

Extra Slides (Optional)

Image by rawpixel.com on Freepik

CBS

Chain-Based PoS Consensus

Image by Maicon Fonseca Zanco from Pixabay

CBS

Chain-Based PoS

- Chain-based PoS is within the framework of Nakamoto consensus in that the gossiping-style message passing, block validation rule, longest-chain rule, and probabilistic finality are preserved. Early full-fledged chain-based PoS blockchain systems include Peercoin and Nxt.
- Unlike PoW, PoS does not hinge on wasteful hashing to generate blocks. A minter can solve the hashing puzzle only once for a clock tick.
- Since the hashing puzzle, difficulty decreases with the minter's stake value, the expected number of hashing attempts for a minter to solve the puzzle can be significantly reduced if her stake value is high.
- PoS avoids the brute-force hashing competition that would occur had PoW been used, thus achieving a significant reduction in energy usage.

Algorithm 4: Chain-Based PoS General Procedure (Peercoin, Nxt)

1 Join the network by connecting to known peers;
2 Deposit in the stake pool;
3 Start *BlockGen()*;
/* Main loop */
4 **while** *running* **do**
5 (Same with Nakamoto's protocol except that block validation should include PoS check.)
6 **end**
/* PoS-based block generation */
7 **Function** *BlockGen()*:
8 Pack up transactions and prepare a block header context $\mathscr{C}$ containing the transaction Merkle tree root and other essential blockchain information;
/* PoS hashing puzzle */
9 Set up a clock (whose tick interval is a constant) and check for the following condition per clock tick:

$$Hash(\mathscr{C}|clock\_time) < target \times stake\_value$$

wherein more preceding zero bits in *target* indicate a higher mining difficulty per unit of stake value;
10 **return** new block;
11 **end**

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

Chain-Based PoS - Peercoin

- Both Peercoin [6] and Nxt [96] generally follow Algorithm 4. Their major difference lies in how the stake is valued. Stake value is initially proportional to stake quantity.
- To ensure the profitability of small stakeholders, a stake valuation scheme can be used to adjust the value of an unused stake as time passes.
- Peercoin uses the coin age metric for stake valuation, which lets the value of a stake appreciate linearly with time since the deposit.
- At the end of a block cycle, the value of the winner's stake returns to its base value. To avoid stakeholders from locking in a future block by deliberately waiting long, stake appreciation only continues for 90 days and stays flat since then.
- As a result, the chances of small stakeholders to generate a block are supplemented with time value that encourages them to stay participated even if they have not generated a block for a long time.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

Committee-Based Proof-of-Stake

Image by Maicon Fonseca Zanco from Pixabay

CBS

Committee-Based PoS

- Chain-based PoS still relies on hashing puzzles to generate blocks, whereas Committee-based PoS adopts a more orderly regime: determining a committee of stakeholders based on their stakes and allowing it to generate blocks in turns.
- A secure multiparty computation (MPC) scheme is often used to derive such a committee in the distributed network. MPC is a genre of distributed computing in which multiple parties beginning with individual inputs, shall output the same result [98].
- The MPC process in the committee-based PoS essentially realizes the functionality that takes in the current blockchain state, which includes the stake values from all stakeholders, and outputs a **pseudo-random sequence of stakeholders** (we call it the leader sequence) which will subsequently populate the block-proposing committee.
- This leader sequence should be the same for **all stakeholders** and those with higher stake values may take up more spots in the sequence.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

Committee-Based PoS

Algorithm 5: Committee-Based PoS General Procedure

```
   /* Joining network and staking                    */
1  Join the network by connecting to known peers;
2  Deposit in the stake pool;
   /* Main loop                                      */
3  while running do
       /* Committee election                         */
4      if new block cycle then
5          Participate in CommitteeElect();
6          Check BlockGenSeq for my turns;
7      end
       /* Block proposing & broadcast                */
8      if my turn to generate block then
9          Collect transactions and generate block;
10         Write block to blockchain;
11         Broadcast block to the network;
12     end
       /* Longest-chain&validation rule              */
13     if block is received & is valid & extends the longest
        chain then
14         Write block into blockchain;
15         Relay blocks to other committee members;
16     end
17 end
```

```
17 end
   /* PoS-based committee election                   */
18 Function CommitteeElect():
19     Fetch the current blockchain state and the stake
        information of all participants; use them as the
        MPC input;
20     Participate in the MPC that produces BlockGenSeq, a
        pseudo-random sequence of block generation
        opportunities;
21     return BlockGenSeq;
22 end
```

- In this algorithm, the CommitteeElect() functionality can also be implemented in a privacy-preserving way with **verifiable random function (VRF)** [99] in that only the stakeholder itself knows if it gets elected into the committee.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

Committee-Based PoS - Security Analysis

- Despite having an orderly block-proposing scheme, committee-based PoS still adheres to the longest-chain rule for probabilistic finality.
- So long as fewer than 50% of stakes are held by the malicious party, the honest parties can safely maintain the longest chain.
- To mitigate such risks, the duration of a communication round can be extended sufficiently to ensure that all broadcast messages are delivered before the participants proceed to the next round.
- This, however, leads to longer transaction confirmation latency and lower throughput. A more straightforward approach is limiting the committee size by imposing a minimum stake requirement for the committee members.
- For example, **Cardano**, the cryptocurrency platform that deploys Ouroboros, mandates that every committee member should own no less than 2% of total tokens in circulation. This effectively limits the committee size to 50, safeguarding an efficient consensus process.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

BFT-Based Proof-of-Stake

Image by Maicon Fonseca Zanco from Pixabay

CBS

BFT-based PoS

- Chain-based PoS and committee-based PoS largely follow the Nakamoto consensus framework in that the longest-chain rule is still used to provide probabilistic finality of blocks.
- In comparison, BFT-based PoS incorporates an extra layer of BFT consensus that provides fast and deterministic block finalization.
- Algorithm 6 shows the general procedure of BFT-based PoS at every participant. Block proposing can be done by any PoS mechanism (round-robin, committee-based, etc.) as long as it injects a stable flow of new blocks into the BFT consensus layer.
- Aside from the general procedure, a checkpointing mechanism can seal the blockchain's finality (not shown in Algorithm 6). As a result, the longest-chain rule can be safely replaced by the most recent-stable checkpoint rule for determining the stable main chain.
- Popular BFT-based PoS blockchain protocols include Tendermint, Algorand, and **Casper FFG**.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

BFT-based PoS

Algorithm 6: BFT-Based PoS General Procedure

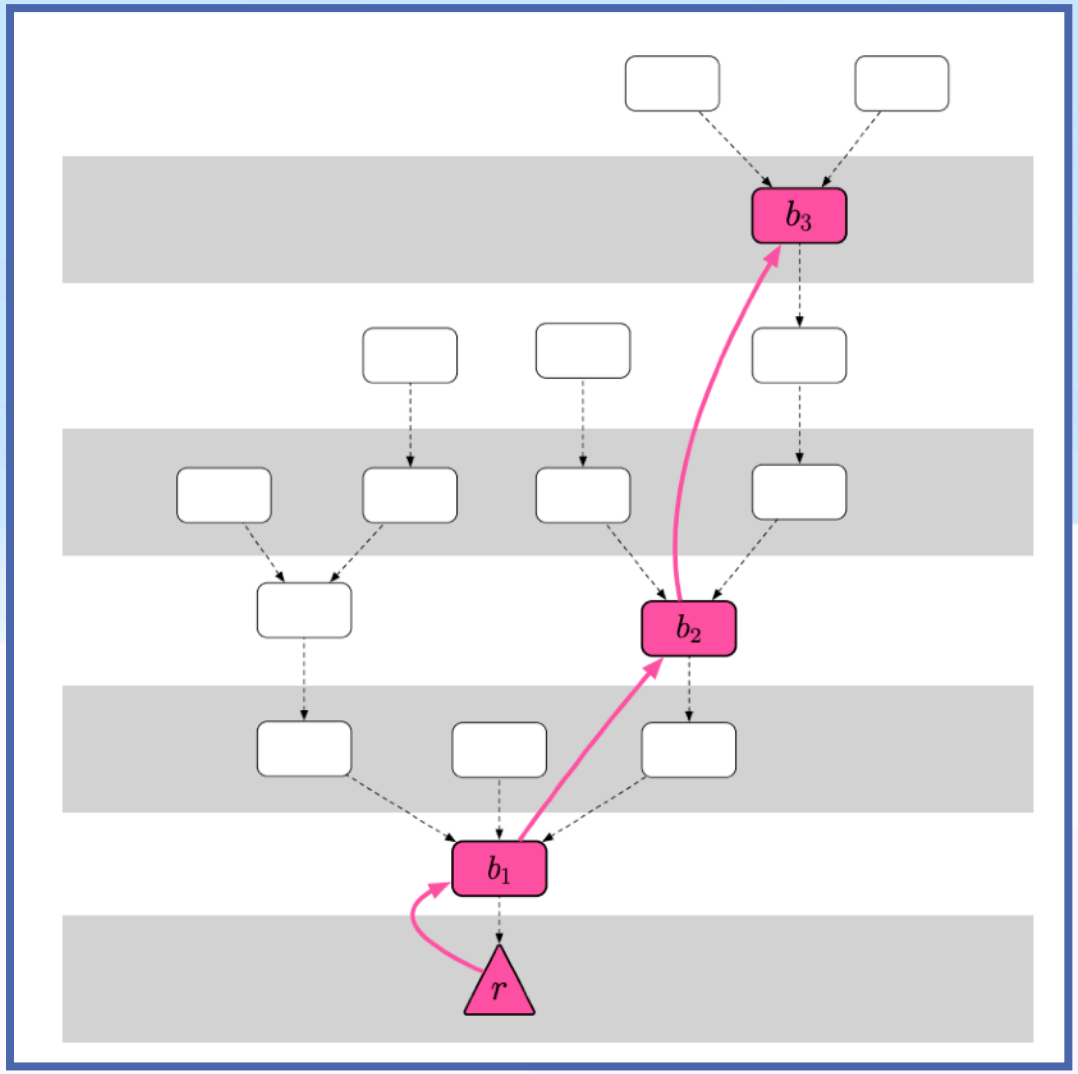
```
1  Join the network by connecting to known peers;
2  Start BlockGen();
   /* Main loop                                   */
3  while running do
       /* Block proposing & broadcast             */
4      if BlockGen() returns block then
5          Add block to its tempBlockSet;
6          Broadcast block to the network;
7      end
       /* Block validation                        */
8      if block is received & is valid then
9          Add block to its tempBlockSet;
10         Relay block to the network;
11     end
       /* BFT consensus layer                     */
12     if new consensus epoch then
13         Perform BlockFinBFT() on tempBlockSet;
14         Write the winning block to blockchain;
15         Clear tempBlockSet;
16     end
17 end
```

```
17 end
   /* PoS-based block generation                  */
18 Function BlockGen():
19     Elect a block proposer, whose success rate is
        proportional to stake value;
20     Propose block;
21     return block;
22 end
   /* BFT-based block finalization                */
23 Function BlockFinBFT():
24     Participate in a BFT consensus that finalizes one
        winning block out of tempBlockSet;
25     return the winning block;
26 end
```

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

BFT-Based PoS - Casper FFG

- It is a light-weight PoS consensus layer built on top of Ethereum's current PoW-based block proposing mechanism (Ethash).
- Newly generated and received blocks are attached to the BlockTree, which is similar to the tree data structure used by the GHOST rule.
- However, the actual consensus subject is the CheckPointTree, a subtree of BlockTree.
- Specifically, for every consensus epoch (100 in BlockTree's height or 1 in CheckPoint Tree's height),



Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Casper FFG: How Does Casper FFG work? How Does Ethereum 2.0 Integrate Casper FFG? (https://medium.com/unitychain/intro-to-casper-ffg-9ed944d98b2d)

Casper FFG

Algorithm 7: Casper FFG

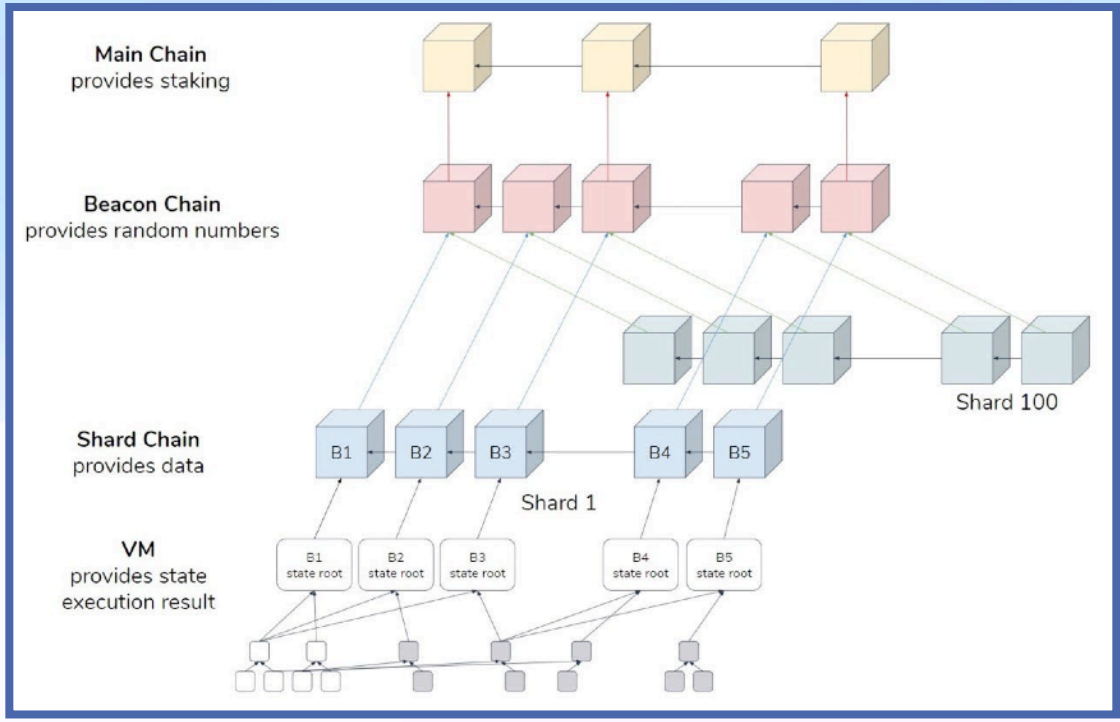
```
1  Deposit in the stake pool;
   /* Main loop                                          */
2  while running do
3      (Block proposing and block validation are the same
        as in Algorithm 6, except that blocks are attached to
        BlockTree rather than stored in a temporary set.)
       /* BFT consensus layer                            */
4      if new consensus epoch then
5          Identify valid checkpoint blocks and attach them
            to CheckPointTree;
6          Participate in CheckPointVote() w.r.t.
            CheckPointTree, which returns CP_s, CP_t;
7          Mark CP_s finalized and CP_t justified;
8      end
9  end
   /* Staked checkpoint voting                           */
```

```
   /* Staked checkpoint voting                           */
10 Function CheckpointVote():
11     Broadcast a vote for a source-target checkpoint pair
        in CheckPointTree;
12     Check received votes against the slashing rules and
        then evaluate them by signer's deposited stake;
13     if pair ⟨CP_s, CP_t⟩'s votes cover more than 2/3 of
        total deposited stakes then
14         return CP_s, CP_t;
15     end
16 end
```

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

Casper FFG and Ethereum 2.0

- Notably, Casper FFG is the preamble project of Casper Correct-by-Construction (Casper CBC), the PoS protocol family that will be used by Ethereum 2.0 to complete the transition to pure PoS [108].
- To further improve performance and scalability, Ethereum 2.0 also plans to combine PoS with sharding [109]. All Ethereum 2.0 participants are divided into shards. Each shard runs a blockchain instance via a consensus scheme not limited to PoS.
- On the top level, the main chain, known as the "beacon chain", will be maintained by a group of known validators via a Casper CBC protocol.
- Each validator is randomly assigned to a shard as the shard manager and periodically commits a digest of the shard chain to the main chain.
- The parallelism of sharding and the energy efficiency of PoS can theoretically scale up both transaction throughput and network size.



Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Casper FFG: How Does Casper FFG work? How Does Ethereum 2.0 Integrate Casper FFG? (https://medium.com/unitychain/intro-to-casper-ffg-9ed944d98b2d)

BFT-Based PoS

Security Analysis: BFT-based PoS's consensus fault tolerance varies among the three above-mentioned implementations. In Tendermint, although block proposers are determined based on PoS, all validators have the equal weight in the consensus process. Therefore Tendermint tolerates up to 1/3 of Byzantine validators. In comparison, Algorand and Casper FFG tolerate up to 1/3 of maliciously-possessed stakes. In Algorand, if an attacker owns more than 1/3 of total tokens, then chance is high that more than 1/3 of the elected committee members are compromised by the attacker, leading to consensus failure of $BA\star$. In Casper FFG, if an attacker owns more than 1/3 of total deposited stakes and dominates the communication within the network, the compromised validators can vote on conflicting checkpoints without getting punished. Since a typical BFT consensus protocol can incorporate a checkpointing mechanism to ensure deterministic finality of blocks, costless simulation attacks can be naturally avoided (to introduce in Section VI-E).

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Casper FFG: How Does Casper FFG work? How Does Ethereum 2.0 Integrate Casper FFG? (https://medium.com/unitychain/intro-to-casper-ffg-9ed944d98b2d)

Delegated Proof-of-Stake (DPoS)

Image by Maicon Fonseca Zanco from Pixabay

CBS

Delegated PoS (DPoS)

- DPoS can be seen as a democratic form of committee-based PoS in that the committee (consensus group) is chosen via public stake delegation.
- DPoS was designed to control the consensus group's size so that the consensus protocol's messaging overhead remains manageable.
- Members of the consensus group are also called delegates. The election of delegates is called the delegation process; an example is shown in Fig. 9.
- In the actual case, the delegation process and the soliciting of votes may involve outside incentives. And the delegation process may turn out to be an interesting socioeconomic phenomenon.

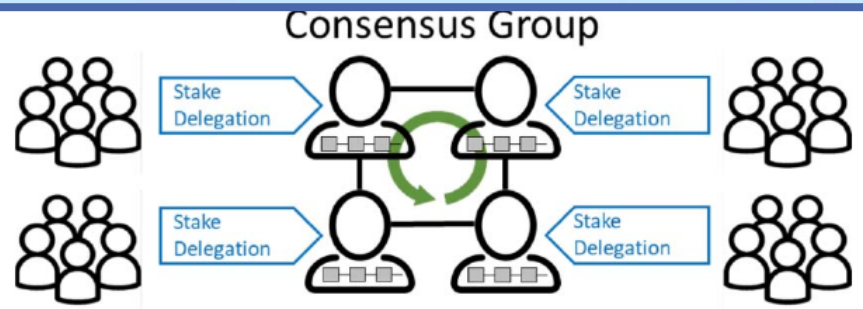


Fig. 9. Illustration of the delegation process in DPoS. Small stakeholders vote for delegates with their stakes and the most voted delegates form the consensus group.

Security Analysis: Assuming BFT is used by the consensus group for block finalization, which is recommended since the group size is limited, DPoS can tolerate 1/3 of delegates being malicious. For example, EOSIO can tolerate at most 6 out of 21 delegates being malicious. In the real world they may not wish to misbehave or collude at all, since all delegates have revealed their identities to voters and would be scrutinized for any misconduct.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.
Casper FFG: How Does Casper FFG work? How Does Ethereum 2.0 Integrate Casper FFG? (https://medium.com/unitychain/intro-to-casper-ffg-9ed944d98b2d)

Thank you!

Raghava Mukkamala

rrm.digi@cbs.dk

https://www.cbs.dk/staff/rrmdigi

https://raghavamukkamala.github.io/

https://cbsbda.github.io/