Proof-of-Stake

Objectives

Objective

Describe several consensus algorithms at a fundamental level

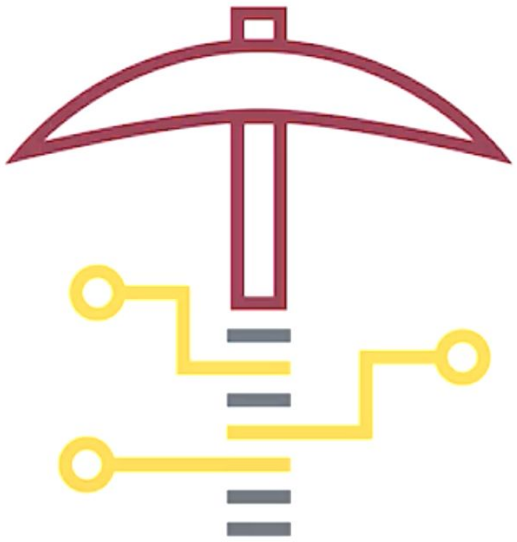
Objective

Identify trade-offs associated with consensus algorithms

Background

Consensus Algorithms (public and decentralized blockchain networks)

- Need source of randomness or pseudo-randomness to select miner
  - Miner adds next block to blockchain
  - Block is generally proportional to limiting economic resource



Proof-of-Work

- Randomness comes from miners guessing different nonces
  - Search for valid block header bash
  - computational power is the limiting economic resource
- Not the only consensus algorithm
- Computational power not always the limiting economic resource

Introduction to Proof-of-Stake PoS

Proof-of-Stake

- Consensus algorithm that chooses block producer based on proportional economic stake
  - Peercoin
- Randomness derived from within protocol

Proof-of-Stake Algorithms

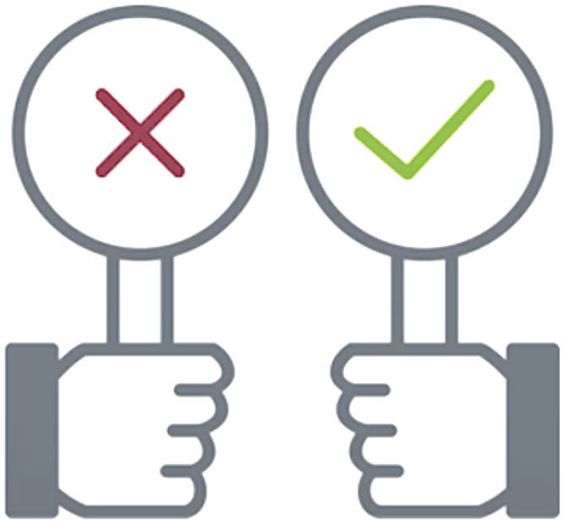
- Chain-Based Proof-of-Stake
- Byzantine Fault Tolerance Proof-of-Stake

Chain-Based PoS - Example

- Protocol chooses block for next block producer to point to
- Protocol randomly chooses **block producer** to produce during specified time period
  - Based on proportional economic stake within protocol
- During this time, block producer must produce a valid block
  - Must point to the previous block chosen by the protocol
- Block producer gets rewarded for producing a valid block

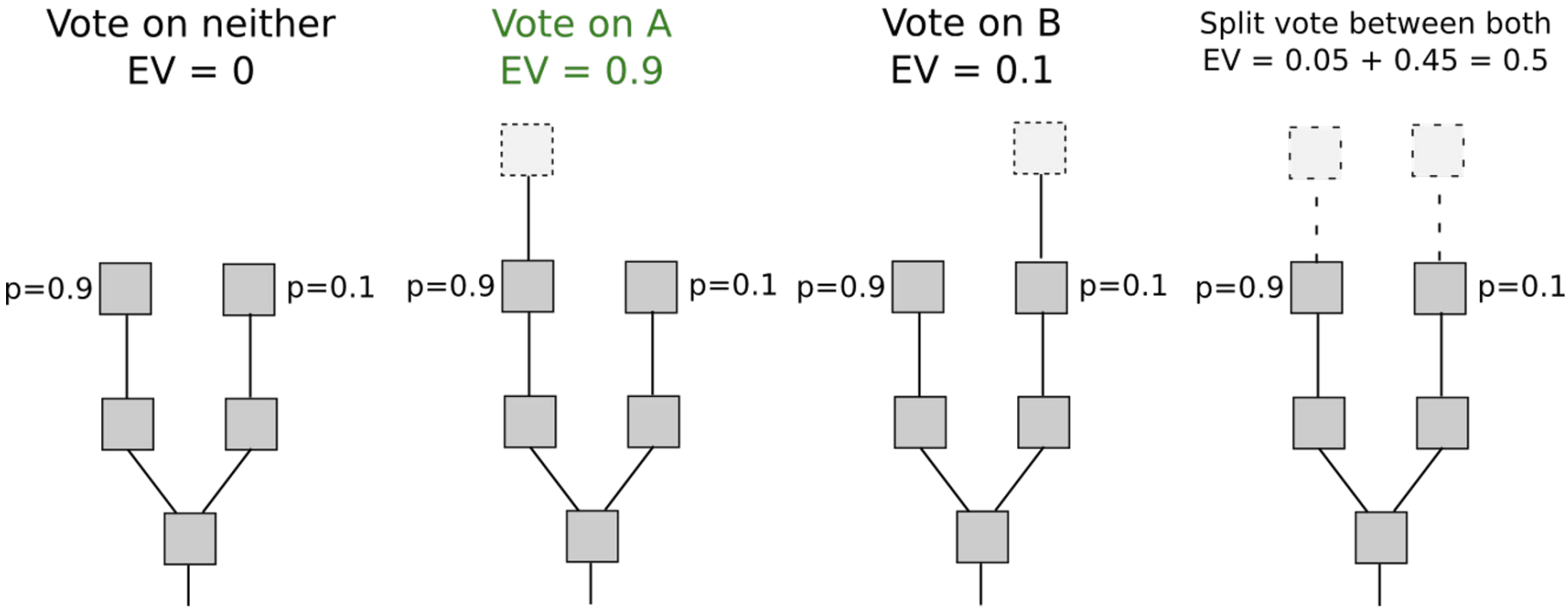
Byzantine Fault Tolerance PoS - Example

- Protocol chooses block for next block producer to point to
- Protocol randomly chooses **block producer** to produce during specified time period
  - Based on proportional economic stake within protocol
- Block proposer must produce a block during that time
- Validity of proposed block voted on
  - Valid if two-thirds or more of votes say the block is valid
- Block proposer rewarded



Nothing-at-Stake Problem (1/2)

- Owning tokens to stake will not disincentivize bad behavior
- Major security concern in PoS



Nothing-at-Stake Problem (2/2)