CS 168: Blockchain and Cryptocurrencies

Beyond Proof of Work

Prof. Tom Austin
San José State University

Why do we have proof-of-work?

- A form of leader election
  - Block producer
- Provides "eventual consensus"
- No trust needed
- "One CPU one vote"
  - Or maybe "one ASIC one vote"

Problems with Proof-of-Work (PoW)

- Increasing centralization
  - Application Specific Integrated Circuits (ASICs)
  - Mining pools
- Waste of resources
- Slow
- No true finality

Alternatives to Bitcoin's PoW

- ASIC-resistant PoW
- "Useful" PoW
- Proof-of-stake (PoS)
- Others?

Sometimes called "Proof-of-Concepts" (PoX)

Alternatives to Bitcoin's PoW

- **ASIC-resistant PoW**
- "Useful" PoW
- Proof-of-stake (PoS)
- Others?

Ethash

- Used by Ethereum
- Memory hard
- Miner needs 1 GB DAG
- ASICs delayed by plans of PoS
- But they exist now
  - Suspicion that ETH won't switch to PoS
  - Ethereum Classic

Alternatives to Bitcoin's PoW

- ASIC-resistant PoW
- **"Useful" PoW**
- Proof-of-stake (PoS)
- Others?

"Useful" Proof-of-Work

- **Goal**: Provide the same properties as Bitcoin's proof-of-work
  - Hard to find proof
  - Efficient verification
  - Adjustable difficulty
  - Non-reusable work
- *Also* provide a public good
  - Use computational work to benefit society

Useful PoW Challenges

- Must tie problem instances to transactions
  - Otherwise, computational work does not verify transactions
- Prevent solution reuse/precomputation.
- What if there is no solution to a problem instance?
- Other issues?

Primecoin

- Proof-of-work searches for prime numbers
  - Cunningham chains
- Created by Sunny King
  - Pseudonym
- https://primecoin.io/bin/primecoin-paper.pdf

Alternatives to Bitcoin's PoW

- ASIC-resistant PoW
- "Useful" PoW
- **Proof-of-stake (PoS)**
- Others?

Proof-of-Stake (PoS)

- **Core idea**: people invested in currency won't destroy it.
- "Virtual miners" (sometimes called *validators*)
- Scarce resource: coins
  - Many different forms
- (Yes, the acronym is unfortunate)
- Nguyen et al., *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities.* IEEE Access 2019.

Nothing at Stake Problem

- With PoW, miners spend resources to “vote” for a winning chain
- With PoS, a miner might “vote” for all chains
  - Good strategy for validator – shares in spoils whichever chain wins
  - Bad for network
- *PoS protocols must address the nothing at stake problem*

Rough Breakdown of Proof-of-Stake Approaches

- Proto-PoS
  - Hybrid PoW/PoS
  - PoW protocols that leverage PoS concepts
- Follow-the-satoshi (FTS) protocols
- Byzantine Fault Tolerant approaches

Proto-PoS Protocols

Important Proto-PoS Protocols

- Bitcoin-NG
  - Introduced concepts used by PoS protocols
- Proof-of-Activity (PoA) protocol
  - Follow-the-satoshi (FTS) algorithm
- Peercoin
  - Proof-of-coin-age
  - First available PoS cryptocurrency

Important Proto-PoS Protocols

- **Bitcoin-NG**
  - **Introduced concepts used by PoS protocols**
- Proof-of-Activity (PoA) protocol
  - Follow-the-satoshi (FTS) algorithm
- Peercoin
  - Proof-of-coin-age
  - First available PoS cryptocurrency

Bitcoin-NG (Next Generation)

- *Not* proof-of-stake
- Goal: Increase transaction throughput
- Like Bitcoin, proof-of-work allows miner to make a block, BUT:
  - Miner becomes *leader* until next PoW block (key block)
  - Leader makes additional blocks (microblocks) *without* PoW
  - Other miners build off of microblocks
- <Example in class>

Bitcoin-NG Reward and Punishment

- Current “leader” makes micro blocks
  - Leader receives 40% of transaction fees
  - *Next* leader receives 60%
- Mining rewards not released immediately
- If leader posts conflicting blocks:
  - *poison transaction* includes *proof of fraud*
  - leader loses mining rewards
  - similar concept used in some PoS protocols

Important Proto-PoS Protocols

- Bitcoin-NG
  - Introduced concepts used by PoS protocols
- **Proof-of-Activity (PoA) protocol**
  - **Follow-the-satoshi (FTS) algorithm**
- Peercoin
  - Proof-of-coin-age
  - First available PoS cryptocurrency

Proof-of-Activity

- Hybrid PoW/PoS
- Goal: Better security against future attacks
  - ???
- PoW miners generate empty block headers
- Follow-the-satoshi
  - A satoshi is picked at random from *all* minted satoshi.
  - The owner participates in block formation.
  - Simple idea… but “random” is hard.

Important Proto-PoS Protocols

- Bitcoin-NG
  - Introduced concepts used by PoS protocols
- Proof-of-Activity (PoA) protocol
  - Follow-the-satoshi (FTS) algorithm
- **Peercoin**
  - **Proof-of-coin-age**
  - **First available PoS cryptocurrency**

Peercoin (AKA PPCoin)

- Created by Sunny King and Scott Nadal
  - Same Sunny King as Primecoin paper
- Goal: Avoid cost of energy consumption
- Fork of Bitcoin
- Proof-of-coin-age
  - PoS/PoW hybrid
- Also involves a checkpoint mechanism
- https://whitepaper.io/document/139/peercoin-whitepaper

Coin age

- 10 coins held 90 days = 900 coin days
- When spent, coin age consumed
- Time becomes security critical
  - Not clear why time was used instead of block height

Peercoin Specification

- Many details are not clearly spelled out.
  - In essence, reference implementation is the spec
  - https://github.com/peercoin/peercoin
- *Minters* make PoS blocks
- *Coinstake* transactions replace coinbase transactions
  - *Kernel* input involves limited proof-of-work target
  - Minter pays itself
  - Coin age consumed

Lab: Hybrid PoW/PoS target

Modify SpartanGold so that:

- Proof-of-work target varies based on *coin-age* of miner
  - 500 coin-age doubles PoW target.
    (e.g. 20 leading zeroes reduced to 19)
- Coin-age unit: 1 coin, unspent for 1 block
- Coin-age consumed when:
  - Miner finds proof
  - Miner writes a transaction

Lab: Things to note

- Your changes will be in `coin-age-block.js`.
- Miners: Minnie, Mickey, Donald, Scrooge.
  - Minnie, Mickey, and Donald start w/ 300 gold
  - Scrooge starts w/ 3000 gold
  - Same computational power
- Run `driver-pow.js`
  - All miners should earn rewards at roughly an even rate
- Run `driver-coin-age.js`
  - *After your changes*, Scrooge should earn more rewards

Next time

- Pure Proof-of-Stake Protocols
- Homework 3