FINE 434: FinTech

Lecture 19

Professor Fahad Saleh

McGill University - Desautels

Motivation

"[What] would happen if we removed the step of spending money on power and equipment?... Why not simply allocate... 'power' directly to all currency holders in proportion to how much currency they actually hold?... The primary advantage... is obvious:... it removes the wasteful... mining cycle"
- Narayanan, Bonneau, Felten, Miller and Goldfeder (2016)

Overview

"Proof of Stake (PoS) is a category of [blockchain] consensus algorithms... that depend on a validator's economic stake in the network... There are many kinds of [PoS] algorithms... so there are many 'flavors' of proof of stake. "
- Ethereum GitHub

For now, we will not focus upon the technical details of PoS protocols. Instead, we consider an abstraction in which each leaf block selects the subsequent validator randomly with each node's selection probability equaling the proportion of native coins ('stake') she holds.

Overview

"Proof of Stake (PoS) is a category of [blockchain] consensus algorithms... that depend on a validator's economic stake in the network... There are many kinds of [PoS] algorithms... so there are many 'flavors' of proof of stake. "
- Ethereum GitHub

For now, we will not focus upon the technical details of PoS protocols. Instead, we consider an abstraction in which each leaf block selects the subsequent validator randomly with each node's selection probability equaling the proportion of native coins ('stake') she holds.

Are there any problems with this scheme?

Some Issues

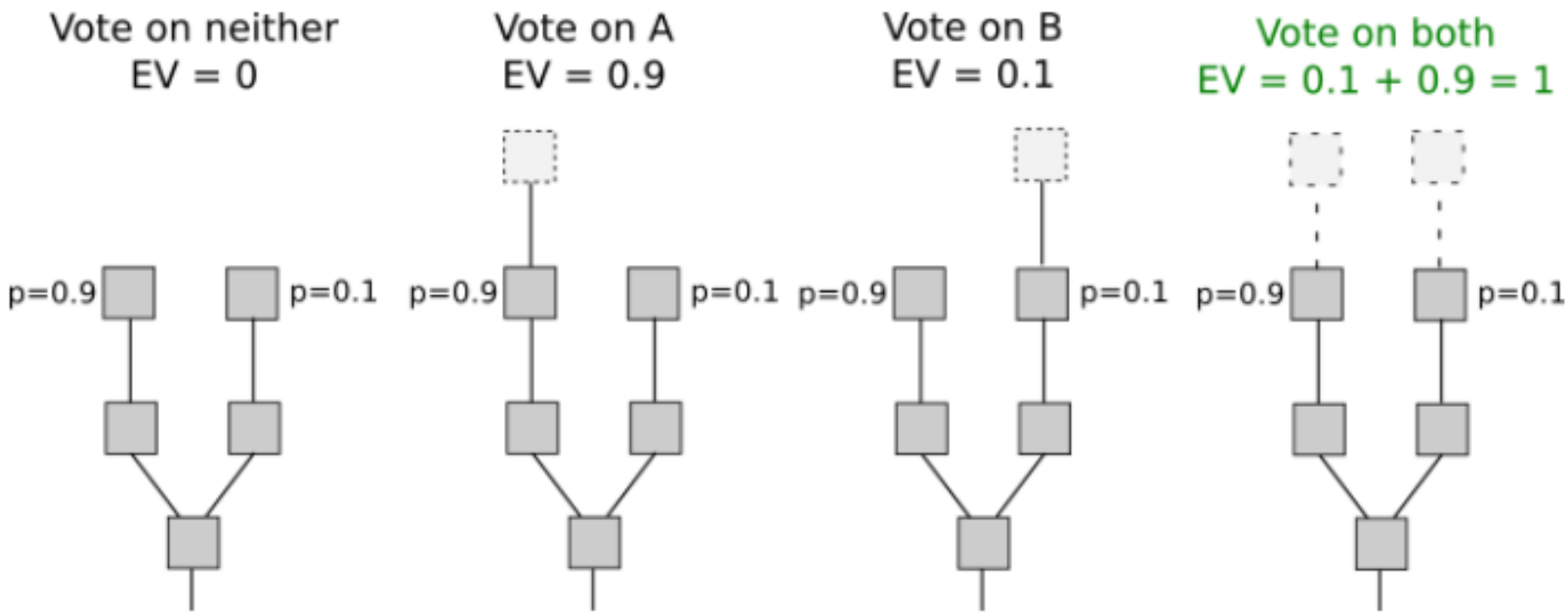
- Nothing-at-Stake Problem
- Wealth Concentration
- Predictability

"The generic vulnerability of virtual mining schemes is what's often called the **nothing–at-stake problem**"
- Narayanan, Bonneau, Felten, Miller and Goldfeder (2016)

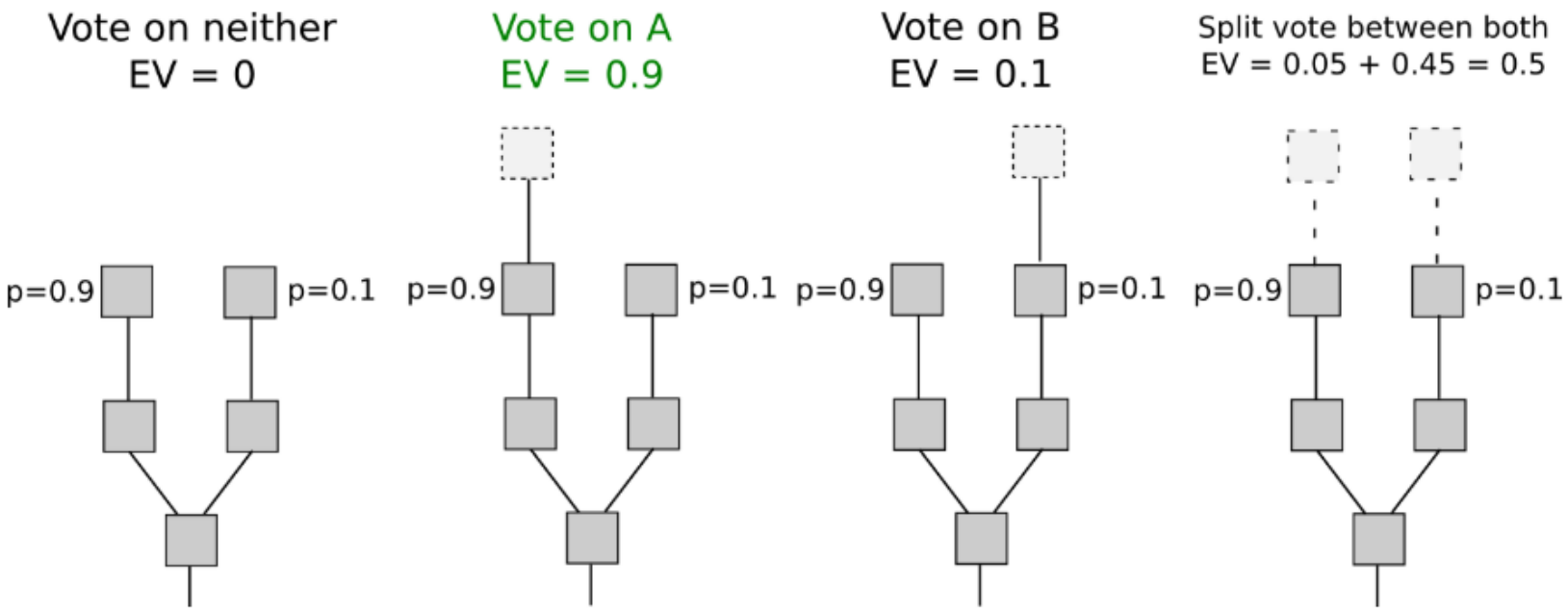
"In many early proof of stake algorithms, ...there are only rewards for producing blocks... [so that if] there are multiple competing chains, it is in a validator's incentive to try to make blocks on top of every chain at once"
- Ethereum GitHub

The Nothing-at-Stake problem alleges that perpetuating disagreement constitutes a weakly dominant strategy within a PoS protocol. Then, a single fork arising amounts to a fatal event. Forks may arise due to latency...

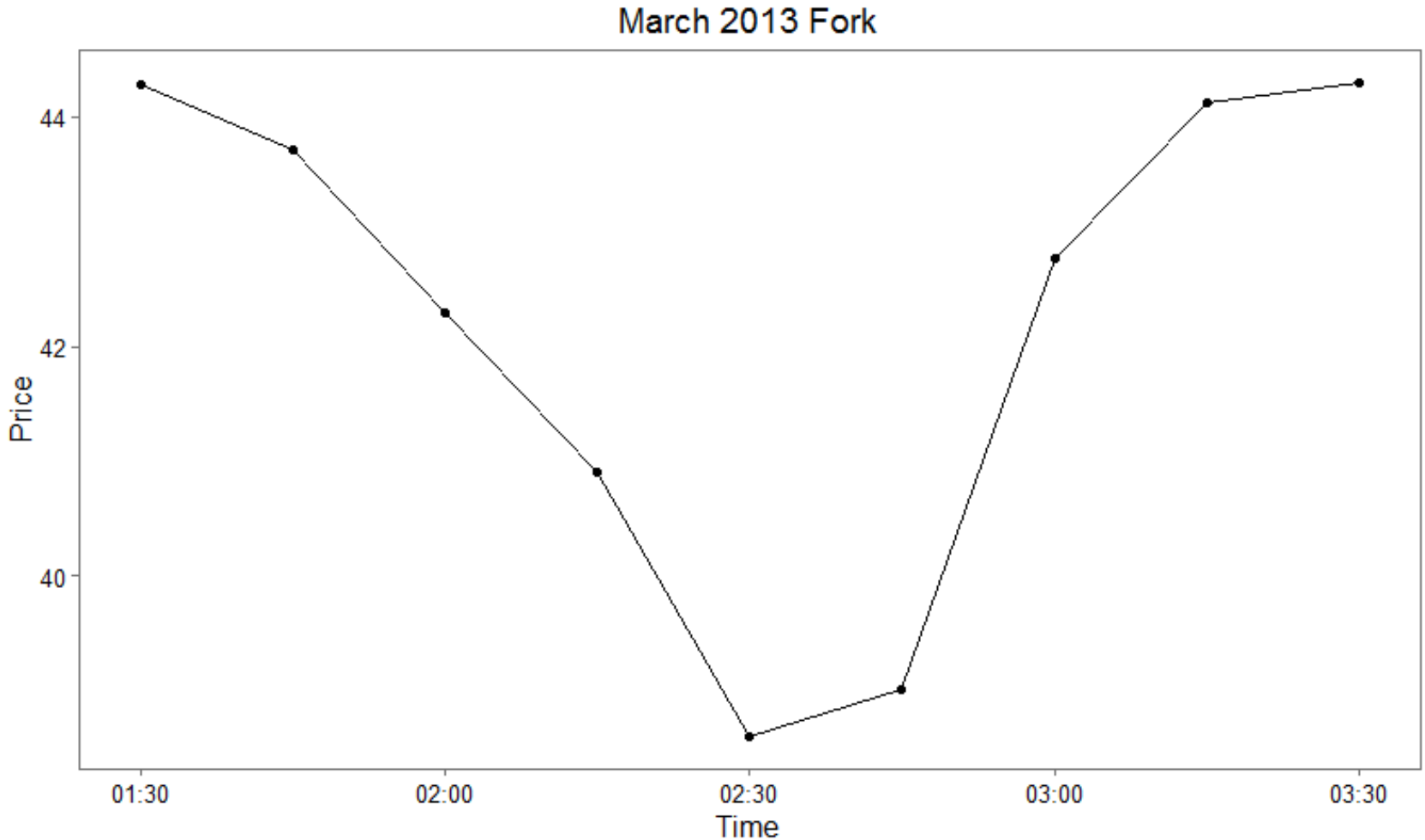
Nothing-at-Stake (PoS)



Something-at-Stake (PoW)



Consensus and Coin Prices



Does PoS need a Block Reward?

The Nothing-at-Stake problem arises due to the block reward

PoW requires a block reward to compensate for computational expense

PoS requires negligible computational expense

A stake-holder possesses an incentive to maintain her own asset value

i.e., If your car needs repair, do YOU need explicit compensation to get it repaired?

Not-Nothing-at-Stake

- Modest Reward Schedules counter Nothing-at-Stake
- Validators face implicit costs via stake devaluation
- Modest Reward is insufficient to overcome the cost
- Explicit punishment schemes help further

... do they??

Evolution of Shares in a Proof-of-Stake Cryptocurrency*

Ioanid Roşu† Fahad Saleh‡

"Do the rich always get richer by investing in a cryptocurrency for which new coins are issued according to a Proof-of-Stake (PoS) protocol? We answer this question in the negative"

Intuition

Without trading, PoS wealth shares do not move on average.

More formally, wealth shares follow a martingale process. Why?

Intuition

Without trading, PoS wealth shares do not move on average.

More formally, wealth shares follow a martingale process. Why?

Suppose there are 10 coins. Alice owns 9. Bob owns 1.

High probability (90%) that Alice wins, but minimal gain

Low probability (10%) that Alice loses, but bigger loss

Magnitude of change offsets probability of outcome

Concrete Examples

Suppose there are 10 coins. Alice owns 9. Bob owns 1.

Assume that the block reward is one coin.

What are Alice and Bob's expected shares after one PoS draw?

Alice: $\frac{9}{10} \times \frac{10}{11} + \frac{1}{10} \times \frac{9}{11} = \frac{99}{10 \times 11} = \frac{9}{10}$

Bob: $\frac{9}{10} \times \frac{1}{11} + \frac{1}{10} \times \frac{2}{11} = \frac{11}{10 \times 11} = \frac{1}{10}$

HW: Demonstrate that this stability holds in general

Two Concerns

- We showed that stability holds on average. That does not rule out wealth concentration with high probability.

- We said no trading. People do trade...

Concern #1

Low reward to supply ratio yields stability with high probability

Intuition
Suppose block reward n equaled 10^n of outstanding supply to that point. That ensures wealth concentration irrespective of selection criteria.

Suppose the block reward were zero. That ensures stability.

Concern #1

Low reward to supply ratio yields stability with high probability

Intuition
Suppose block reward n equaled 10^n of outstanding supply to that point. That ensures wealth concentration irrespective of selection criteria.

Suppose the block reward were zero. That ensures stability.

Take-away: Keep block rewards low to keep shares stable

Concern #2

Trading is irrelevant (... unless you have better information)

Intuition
To purchase a larger share, you need to forgo consumption today

Your (expected) larger share tomorrow will perfectly off-set your forgone consumption today

All trading strategies generate the same pay-off

Formal Barriers to Longest-Chain Proof-of-Stake Protocols

Jonah Brown-Cohen* Arvind Narayanan† Christos-Alexandros Psomas‡
S. Matthew Weinberg§

"At a conceptual level, the barriers stem from the following: all cryptocurrencies require some source of (pseudo)randomness"

An Application of Law of Excluded Middle

Predictability

"Intuitively, it is good for protocols to be unpredictable in the sense that miners do not learn that they are eligible to mine a block until shortly before it is due to be mined."

Recency

"the negation of predictability... The main security concern ...is that intuitively each chain has its own pseudorandomness... certain deviations are easier to detect when chains share the same pseudorandomness"

Predictability Problems

"Many attacks, such as double-spending or selfish-mining can become much more profitable if miners know in advance when they become eligible to mine"

"Preventing predictable selfish mining is challenging... it remains open whether ... [any] reward schemes [preclude predictable selfish mining]"

"A simple defense specifically against predictable doublespend attacks is to accept long confirmation times... Our analysis indicates that... it [is] virtually impossible to have quick confirmation times in a predictable Proof-of-Stake"

Recency Problems

Undetectable Nothing-at-Stake

"we cannot 'punish' suspected deviant miners without the risk of punishing honest but poorly-connected miners."

This point creates a philosophical problem for punishment schemes like Ethereum's Casper...

Two Potential Alternatives

- No Rewards
  "no-rewards is at least as incentive compatible as [other] reward schemes"
- Byzantine Consensus Protocols
  "[Undetectable Nothing-at-Stake] can be readily recognized as malicious, and safely ignored."