Selfish Behavior in the Tezos Proof-of-Stake Protocol

Michael Neuder [1†] Daniel J. Moroz [2]
Rithvik Rao [2] David C. Parkes [2]

[1]Dept. of Computer Science, University of Colorado, Boulder

[2]School of Engineering and Applied Sciences, Harvard University

Cryptoeconomic Systems Conference
March 2020

[†] Work completed while MN was visiting Harvard University.

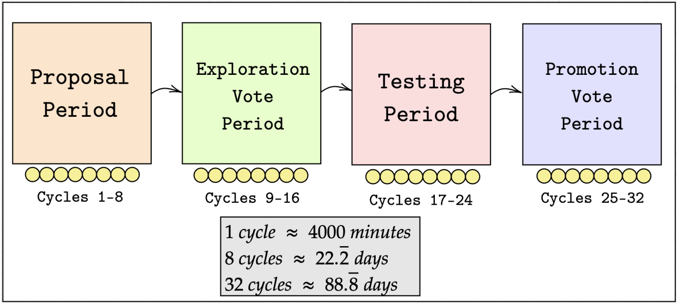
Content

1. Related Work
2. Tezos
   - Overview
   - Proof-of-Stake Mechanism
   - Delay Function
   - Reward Functions
3. Selfish Endorsing Attack
   - Example Length-2 Attack
   - Feasibility & Profitability
   - Probability
4. Results
5. Future Work

Related Work

- Eyal and Sirer (2013) outline how an attacker can earn a larger relative percentage of blocks in a Proof-of-Work mechanism by not immediately publishing blocks.
  - Slows down block production, but is profitable because of difficulty adjustment.
- Brown-Cohen et al. (2019) demonstrate theoretical weaknesses in PoS.
  - Our work is an instance of the *Predictable Selfish Mine* described in their work.

- 2014 White Paper from Arthur Breitman and ICO in 2017.
- Currently 10^{th} largest digital currency by market cap at $2 billion.
- Implements an *Optional Delegated Proof-of-Stake*.
- A built in mechanism for updating the protocol democratically.



Proof-of-Stake Mechanism

- Currency is divided into groups of 8,000 tokens called *rolls*.
- At each block-height random roll selection is used to select:
    1. A list of bakers indexed by priority (discussed further).
    2. A group of 32 endorsers to vote on block quality.
- Both bakers and endorsers are incentivized to participate with rewards.
- To be eligible to stake, deposit and reward tokens are frozen 5 cycles.

Tezos

Delay Function

Delay function under Emmy^{+}

$$\mathcal{D}(p, e) = 60 + 40p + 8\max(24 - e,\ 0) \tag{1}$$

- p is the priority of the baker.
- e is the number of endorsements included.
- Determines when a block is considered valid.
- Minimum of 60 seconds between blocks.

Block Reward under Emmy$^+$

$$\mathcal{R}_b(p, e) = \frac{16}{p+1}\left(\frac{4}{5} + \frac{1}{5} \cdot \frac{e}{32}\right) \tag{2}$$

- p is the priority of the baker.
- e is the number of endorsements included.
- Max value of 16 XTZ if $p = 0$ and $e = 32$.

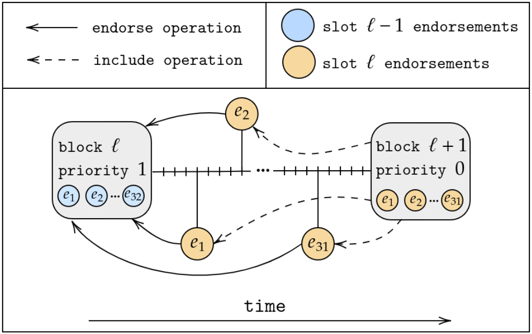
Endorsement Reward under Emmy^{+}

$$\mathcal{R}_e(p_i) = \frac{2}{p_i + 1} \tag{3}$$

- p_i is the priority of the block which includes the endorsement.
- Max value of 2 XTZ if $p_i = 0$.

Tezos

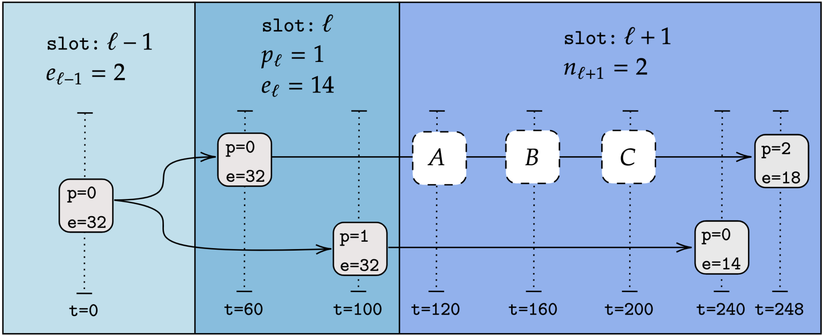
Example Rewards



- Slot $\ell - 1$ rewards
  1. $R_b(1, 32) = 16$ XTZ
  2. $R_e(1) = 1$ XTZ
- Slot $\ell - 1$ rewards
  1. $R_b(0, 31) = 15.9$ XTZ
  2. $R_e(0) = 2$ XTZ

Selfish Endorsing Attack

Example Length-2 Attack



- Attacker creates two blocks before the honest network.
- Only endorses private chain, hence the name *Selfish Endorsing*.

Selfish Endorsing Attack

Feasibility & Profitability

Delay Lemma

$$\mathcal{D}_2(p_\ell, e_\ell, n_{\ell+1}) = 40(p_\ell - n_{\ell+1}) + 8\max(24 - e_\ell, 0) - 8\max(e_\ell - 8, 0) \tag{4}$$

- Allows calculation of difference in time between selfish and honest chain creating two blocks.
- If $\mathcal{D}_2 < 0$, then an attack is *feasible*.

Selfish Endorsing Attack

Feasibility & Profitability

Reward Lemma

$$\mathcal{R}_2(p_\ell, e_{\ell-1}, e_\ell) = 16\left(\frac{1}{p_\ell + 1} + \frac{e_\ell}{160} - \frac{1}{5}\right) + 2e_{\ell-1}\left(\frac{1}{p_\ell + 1} - 1\right) \qquad (5)$$

- Allows calculation of difference in reward for attacker to play honestly versus selfishly.
- If $\mathcal{R}_2 > 0$, then an attack is *profitable*.

Selfish Endorsing Attack

Probability

Joint probability mass function of state variables

$$\begin{aligned}\Pr[\, t \mid \alpha \,] = &\underbrace{(1-\alpha)^{p_\ell}\alpha}_{\Pr[\mathcal{P}=p_\ell]} \times \underbrace{\alpha^{n_{\ell+1}}(1-\alpha)}_{\Pr[\mathcal{N}=n_{\ell+1}]} \\ &\times \underbrace{\binom{32}{e_{\ell-1}}\alpha^{e_{\ell-1}}(1-\alpha)^{32-e_{\ell-1}}}_{\Pr[\mathcal{E}=e_{\ell-1}]} \times \underbrace{\binom{32}{e_\ell}\alpha^{e_\ell}(1-\alpha)^{32-e_\ell}}_{\Pr[\mathcal{E}=e_\ell]} \\ = &\binom{32}{e_{\ell-1}} \cdot \binom{32}{e_\ell} \cdot \alpha^{n_{\ell+1}+e_{\ell-1}+e_\ell+1} \cdot (1-\alpha)^{65+p_\ell-e_{\ell-1}-e_\ell} \end{aligned} \tag{6}$$

- Joint of 2 Geometric R.V.'s and 2 Binomial R.V.'s.
- α is percentage of rolls owned by attacker.

Results

The set of feasible & profitable length-2 attacks

$$\mathcal{A}_2 = \{(e_{\ell-1}, e_\ell, p_\ell, n_{\ell+1}) \mid \mathcal{D}_2 < 0 \ \wedge \ \mathcal{R}_2 > 0\} \tag{7}$$

The value of length-2 attack

$$\mathcal{V}_2 = \sum_{t \in \mathcal{A}_2} \Pr[\, t \mid \alpha \,] \cdot \mathcal{R}_2 \tag{8}$$

Results

α	$\mathcal{C} \cdot \Pr[\mathcal{A}_2]$		%	$\mathcal{C} \cdot \mathcal{V}_2$		%
0.1	0.04	0.17	425%	0.09	0.21	233%
0.15	3.88	2.16	56%	7.07	2.02	29%
0.2	33.91	7.70	23%	52.61	6.10	12%
0.25	136.76	12.91	9.4%	175.91	9.00	5.1%
0.3	309.66	12.66	4.1%	324.55	7.92	2.4%
0.35	407.33	8.07	2.0%	361.14	4.60	1.3%
0.4	318.98	3.53	1.1%	254.94	1.85	0.7%

- $\mathcal{C}$ is the number of minutes in a year.
- Blue column represents results before heuristic fix and green represents after.

Future Work

- Apply framework to other PoS mechanisms
- Longer attacks
  1. Have not been formally analyzed
  2. Computationally difficult
- Double spend attacks.

Thanks!

Questions