Defending Against Malicious Reorgs in Tezos Proof-of-Stake

Michael Neuder Daniel J. Moroz
Rithvik Rao David C. Parkes

School of Engineering and Applied Sciences
Harvard University

ACM Advances in Financial Technology
October 2020

Introduction

Contributions

- Describe reorg attacks in Tezos.
  - Selfish mining and double spend attacks.
- Calculate the probability of attacks based on length of reorg and attacker strength.
- Examine how protocol modifications impact the probability of attacks.
- Present a method to detect potentially vulnerable chain states.[†]

[†] Not discussed in presentation. See paper.

Introduction

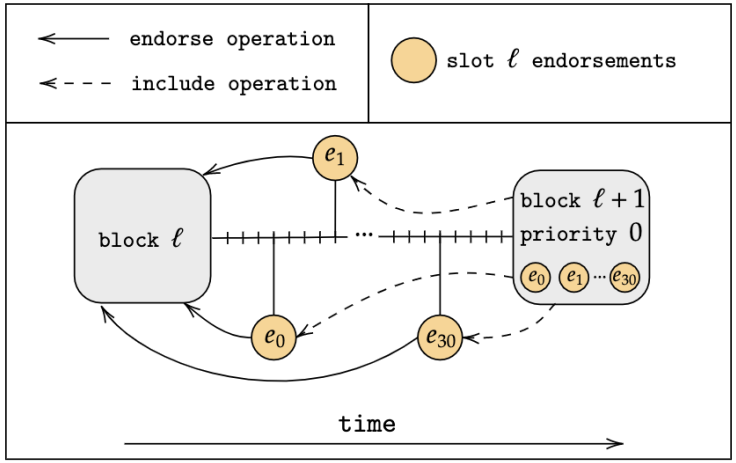
Related Work

- Eyal and Gün Sirer (2013) present "Selfish Mining".
- Brown-Cohen et al. (2019) demonstrate theoretical weaknesses in longest-chain PoS, which we instatiate in Tezos.
  - Predictable selfish mine.
  - Predictable double spend.
- Neuder, Moroz, Rao, Parkes (2020) examines length-2 malicious reorgs to accomplish selfish mining in Tezos.
- Nomadic Labs (2020) blog post explores similar questions, but using different methodology.

Tezos

Proof-of-Stake Basics

- Two roles in block creation: bakers (miners) and endorsers.
  - $[\texttt{baker}_0, \texttt{baker}_1, ...]$ – ordered list of eligible bakers.
  - $[\texttt{endorser}_0, \texttt{endorser}_1, ..., \texttt{endorser}_{31}]$ – unordered group of 32 endorsers.

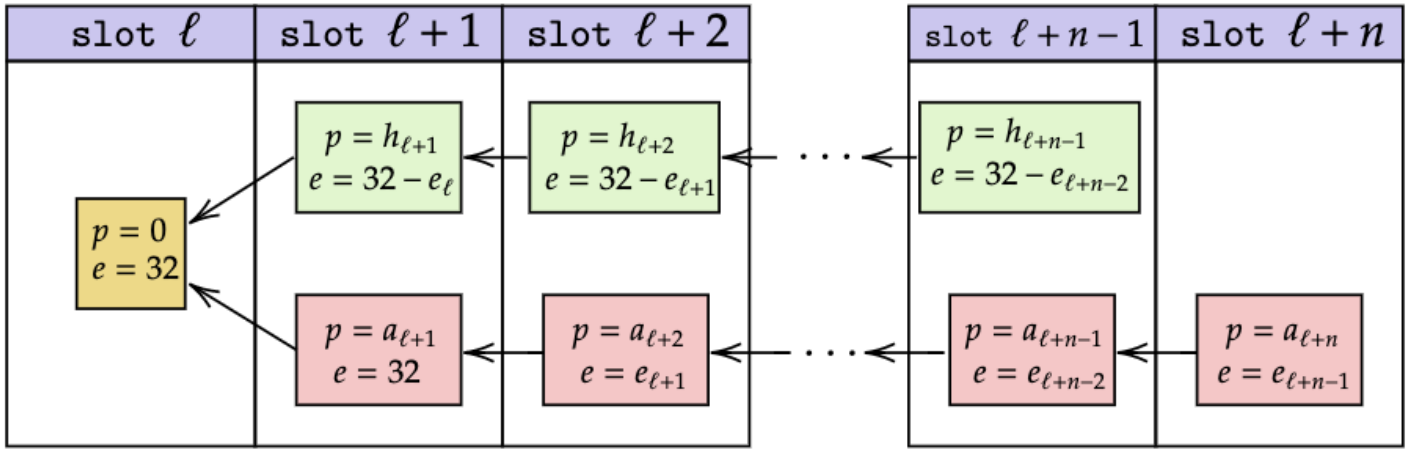


- $\mathcal{D}(p, e) = 60 + 40 \cdot p + 8 \cdot \max(24 - e, 0)$.
- If $p = 0$ and $e \geq 24$, $\mathcal{D} = 60$.
- Baking and endorsing rights are randomly allocated proportionally to the amount of stake owned, but are known far in advance.

Malicious Reorgs

Model

- *Key result*: malicious reorgs caused by a private attacker fork.

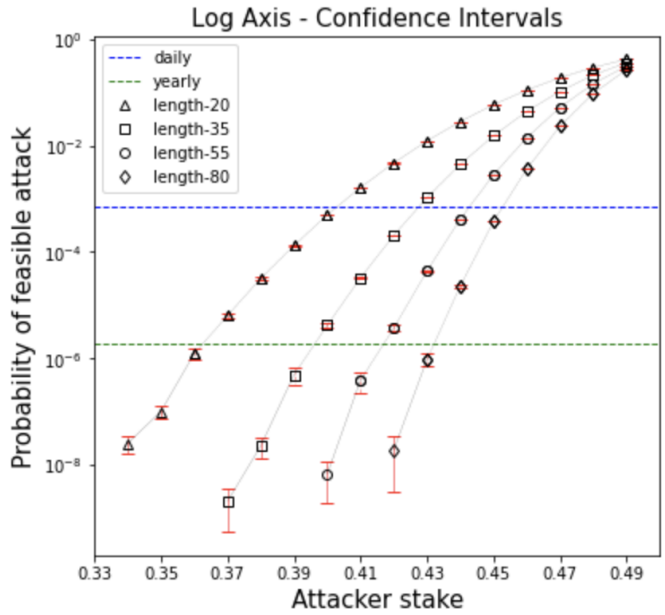


- Rate of block creation on each of the forks is a function of:
  - h_i – the highest priority amongst honest bakers at slot i.
  - a_i – the highest priority owned by the attacker at slot i.
  - e_i – the number of endorsements owned by the attacker at slot i.
- These are random variables that together create the random process that we study.

Malicious Reorgs

Results

- Using Monte Carlo and importance sampling methods, we calculate the probability of reorgs as a function of attacker stake.



- Confidence intervals (red error bars) are 99% Clopper-Pearson and importance sampling.

Protocol Modifications

Parameters

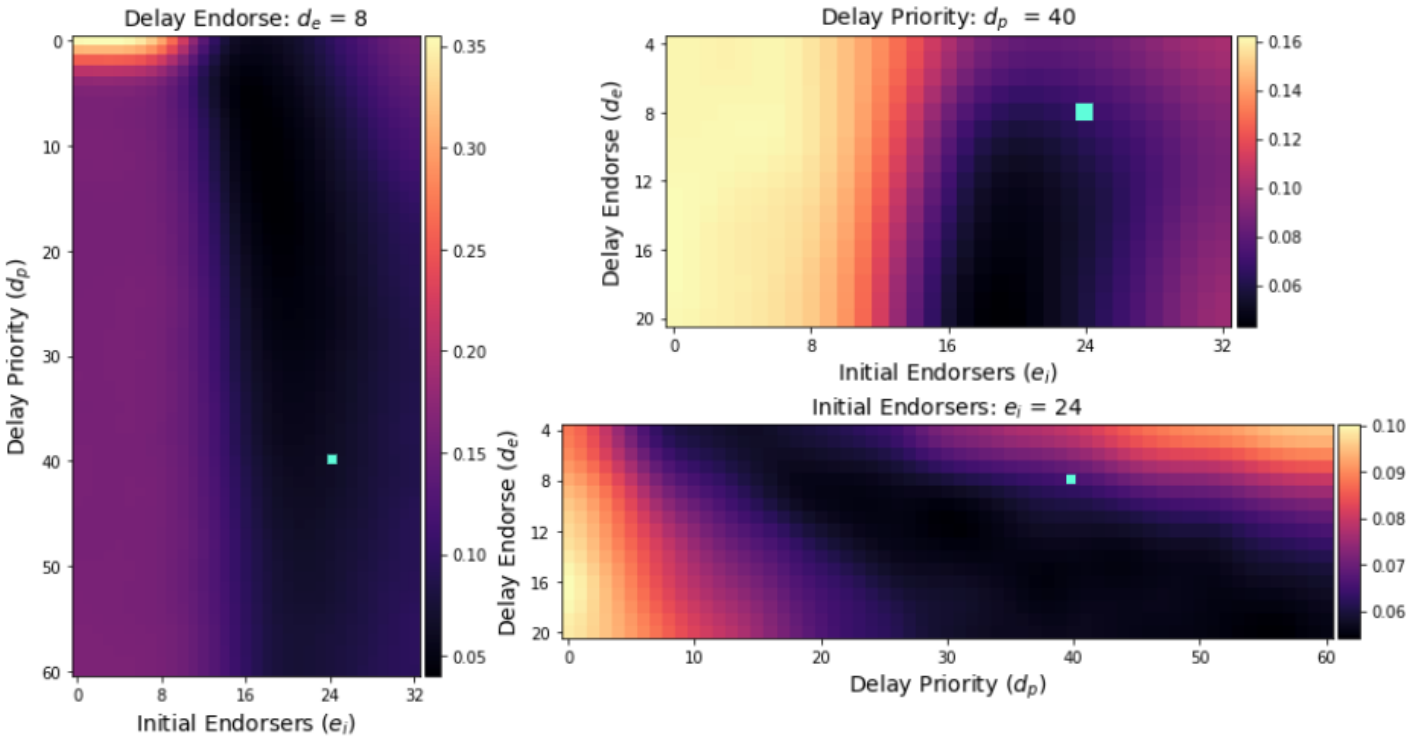
$$\mathcal{D}(p, e) = 60 + d_p \cdot p + d_e \cdot \max(e_i - e, 0). \quad (1)$$

- d_p – The time penalty for each drop in baker priority.
- d_e – The time penalty for missing attestation (past e_i).
- e_i – The number of endorsements needed to avoid any missing endorsement penalties.
- Current implementation is $d_p = 40, d_e = 8, e_i = 24$.

Protocol Modifications

Current Implementation

- Let $\lambda = (d_p, d_e, e_i)$.
- Then define* $g(\beta) = (1 - \beta) \cdot \Pr[\texttt{sm}|\lambda] + \beta \cdot \Pr[\texttt{dr}|\lambda]$
- For $\beta = 0.5$, we obtain the average of the two probabilities.

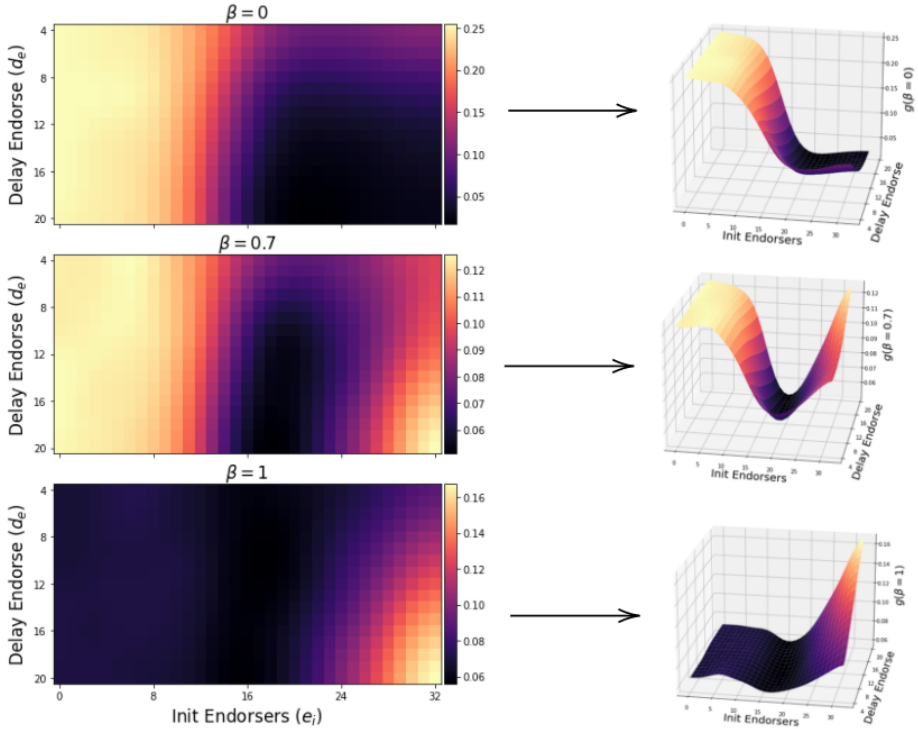


*sm = Selfish mine & dr = deep reorg

Protocol Modifications

Selfish mining vs deep reorgs

- $g(\beta) = (1 - \beta) \cdot \Pr[\mathtt{sm}|\lambda] + \beta \cdot \Pr[\mathtt{dr}|\lambda]$.
- We vary β to modify weighting of selfish mining and deep reorgs.



Conclusion

- Summary
  - Tezos Proof-of-Stake
  - Malicious Reorgs
  - Protocol Modifications
  - Detection Metric (see paper)
- Future work
  - Other PoS protocols.
  - Ensemble attacks.
  - Alternative delay functions.

Thanks!