Safeguarding PoS Consensus

A Comparative Analysis of Proposer Protection Mechanisms Against Various Attack Vectors

Author: Bc. Tereza Burianová **Supervisor:** Ing. Martin Perešíni

Proof-of-Stake Consensus

- validators update the chain by **proposing blocks**
- proposers are **randomly selected**
- incentive: rewards, slashable stake

Ethereum

- proposer selected every 12 seconds (one slot)
- selection made **in advance** to let validators prepare
- results are **publicly known**, even to attackers
- possibly nation-state actors

Simulation

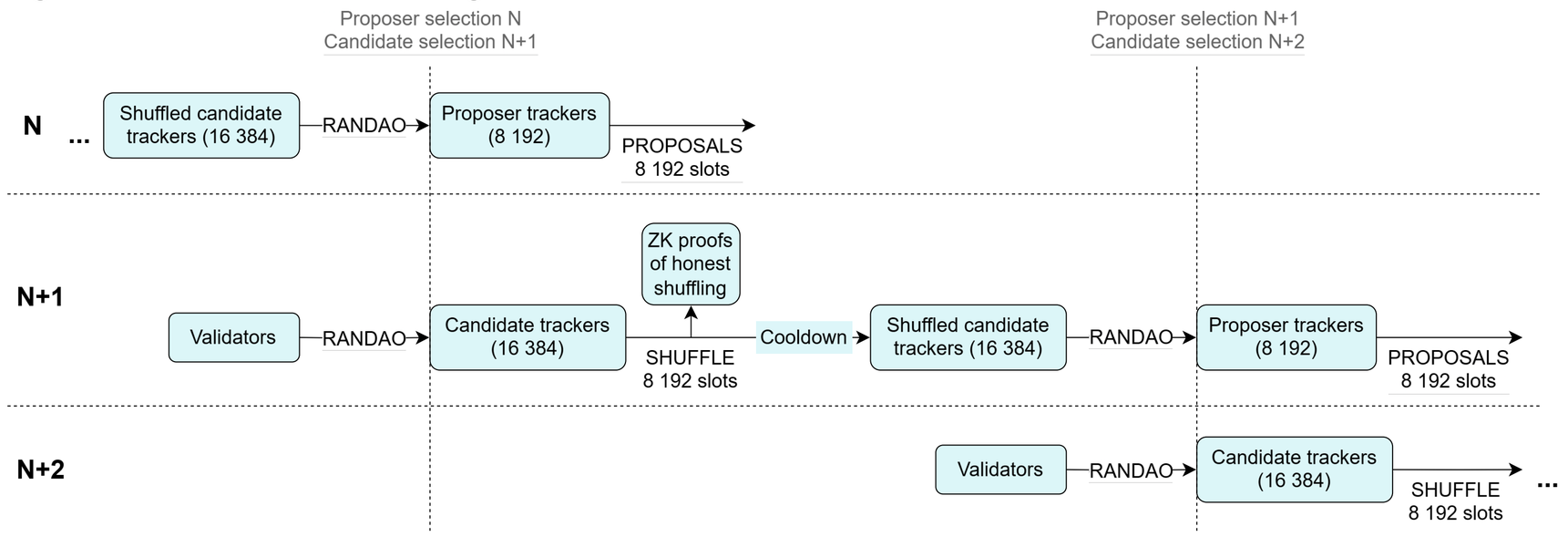
- **goal:** measure effectiveness and overhead of protection mechanisms
- **protection mechanisms:** Secret Single Leader Election

Secret Single Leader Election (SSLE)

- Only proposer knows they have been selected

- **Whisk:**
  - shuffling
  - hidden identity: BLS G1 point, random secret
  - Zero-Knowledge Proofs
- **Homomorphic sortition:**
  - Threshold Fully Homomorphic Encryption
  - hidden identity: encrypted random numbers
  - independent FHE circuits

Fig. 1: The pipeline in the SSLE algorithm Whisk.



Attack: Malicious DoS

Legend: - proposed block, - missed slot

Attacker aims to negatively impact the network by attempting to DoS every proposer.

Fig. 2: Malicious DoS with no protection.

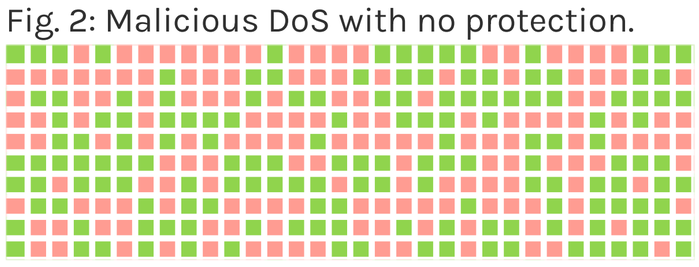
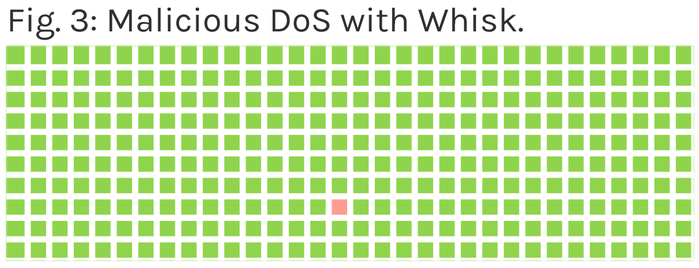
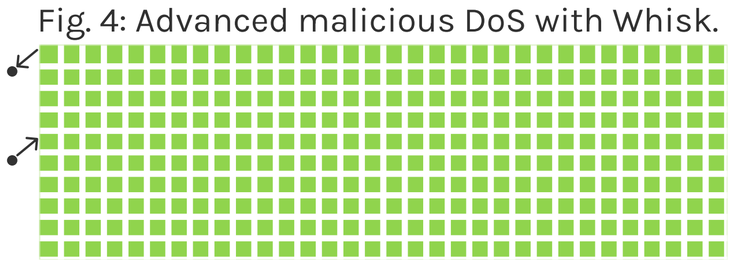


Fig. 3: Malicious DoS with Whisk.



only if proposer gets selected twice in a row (very rare - over 1 mil. validators)

Fig. 4: Advanced malicious DoS with Whisk.



attacker randomly attacks many candidates at once after the shuffling phase (arrows)

Attack: Censorship

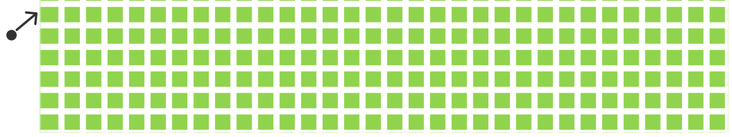
Attacker targets a validator group, preventing them from participating in the consensus.

Fig. 5: Censorship with no protection.

Fig. 6: Censorship with Whisk.

the rarity of DoS success combined with a smaller group of victims

Fig. 7: Advanced censorship with Whisk.



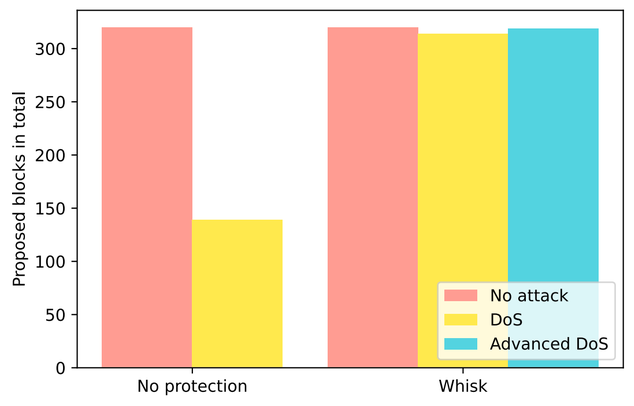
continuous DoS of victims that also were candidates before shuffling, low probability of success

Protection Results

DoS:

- slots missed: **55.43 % / 1.36 %**
- proposers affected: **56.63 % / 1.36 %**

Fig. 8: Comparison of proposed blocks during DoS.



Censorship:

- slots missed: **6.00 % / 0.21 %**
- victims affected: **61.82 % / 2.19 %**

Fig. 9: Comparison of proposed blocks during censorship.

Time measurements in one run:

- no protection: **5 160 ms**
- Whisk: **74 961 ms (14x longer)**

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025

ethereum

Source of brand assets: https://ethereum.org/en/assets/