Under the space threat: Verifier's Dilemma in Cosmos blockchain

Ivan Malakhov, Andrea Marin, Sabina Rossi
Università Ca' Foscari Venezia
{ivan.malakhov,marin,sabina.rossi}@unive.it,

Carla Piazza, Daria Smuseva
Università degli Studi di Udine
carla.piazza@uniud.it, daria.smuseva@unive.it

Abstract

Blockchain technology has witnessed remarkable advancements, with Proof-of-Stake (PoS) emerging as a compelling alternative to traditional Proof-of-Work (PoW) systems. However, PoS-based blockchains are not immune to challenges, notably the Verifier's Dilemma, where validators may compromise network security by neglecting validation processes. This talk delves into the Verifier's Dilemma within the Cosmos blockchain, a prominent PoS platform. We introduce an analytical model using Performance Evaluation Process Algebra (PEPA) to simulate the consensus process, particularly focusing on the CometBFT protocol utilized in Cosmos. Through comprehensive assessment, we unveil insights into network throughput dynamics and the probability of extra rounds required for block finalization. Our findings shed light on potential vulnerabilities and offer valuable perspectives for enhancing the security and efficiency of PoS-based blockchain networks.

1. Introduction

Blockchains are distributed networks of users with intentional lack of central authority that store their data across a network in a form of linked blocks introduced in 2008 [1].

In today's landscape of blockchain technology, two primary categories of networks reign supreme: Proof of Work (PoW) and Proof of Stake (PoS) blockchains. The competition between them also influences the challenges faced within these networks. One such challenge is the Verifier's Dilemma, which initially emerged in PoW-driven permissionless blockchain. Generally speaking, some miners may choose to skip the verification and blindly accept blocks from others for the sake of extra profit, which can compromise the security and reliability of the blockchain [2, 3].

Proof-of-Stake (PoS) systems were aimed to overcome the limitations of PoW and introduced new approach of finding consensus among users, namely Byzantine agreement by voting. While the PoS validators are not involved into heavy mining[1], there still exist mechanisms contributing to unfair behavior. To the best of our knowledge little was made to study the PoS variant of Verifier's Dilemma.

In this talk, (i) we describe Verifier's Dilemma applied to PoS-driven Cosmos blockchain platform, (ii) we provide an analytical model that reflects the validation process seen in a Cosmos-based protocol, namely CometBFT[2] using Performance Evaluation Process Algebra (PEPA) tool first introduced in [4]. Finally, (iii) we perform a comprehensive assessment of outcomes of the model.

2. Background and motivation

In this section we provide a brief description of Cosmos network delving into the protocol underlying it. Further, we describe the problem.

Proof of Stake (PoS) is a consensus algorithm that selects block creators based on their stake in the network. Validators hold or lock funds as stake, influencing their likelihood of block validation and voting power. This is aimed to incentivize honesty and security of the network.

2.1. Cosmos blockchain

Cosmos implements the Tendermint protocol, involving validators with significant stakes in securing the network. Validators stake large amounts of tokens to participate, with top validators controlling substantial stakes. Other users can delegate tokens to validators in exchange for rewards.

Consensus Algorithm. The CometBFT consensus, derived from Tendermint, comprises several steps visualized as follows:

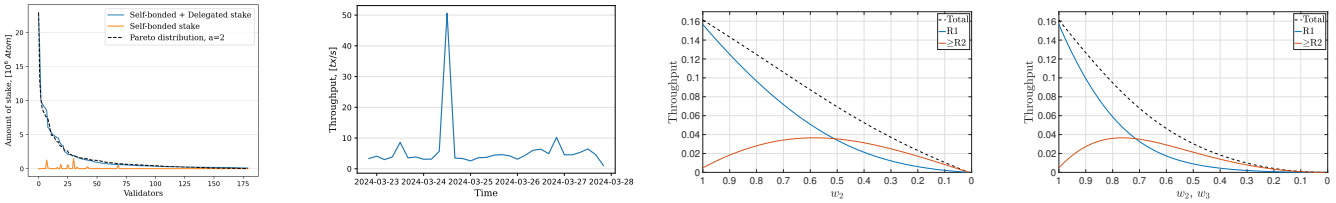
$$\texttt{NewHeight} \longrightarrow (\texttt{Propose} \longrightarrow \texttt{Prevote} \longrightarrow \texttt{Precommit})^{\geq 1} \longrightarrow \texttt{Commit} \longrightarrow \ldots$$

Three special steps, `Propose`, `Prevote`, and `Precommit`, form a round:

1. *Propose*: A validator is selected to propose a block, which includes verified transactions, a previous block hash, a timestamp, and a signature.

[1] For comparison, see https://ccaf.io/cbnsi/cbeci and https://ccaf.io/cbnsi/ethereum.

[2] https://cometbft.com



(a) Distribution of validators' total and self-bonded stakes in Cosmos.

(b) Transaction throughput with 4 hours granularity.

(c) Network throughput as a function of decreasing probability of success in Prevote phase.

(d) Network throughput as a function of decreasing probabilities of success in Prevote and Precommit phases.

Figure 1: Cosmos blockchain data visualization.

2. *Prevote*: Validators vote for or against the proposed block, or vote *nil* if no valid proposal is received.
3. *Precommit*: Validators precommit to the proposed block if a supermajority prevotes for it.

Note that rounds continue until a supermajority precommits to a block, which is then added to the blockchain. If consensus is not reached, the process continues with a new proposer. The algorithm ensures consensus even with up to one-third malicious validators.

Fairness. Fairness in blockchain networks ensures equitable distribution of rewards among participants, crucial for network stability. In systems like Cosmos, fairness is tied to validators' voting power (VP), determined by their token holdings. However, fairness from a system perspective entails balanced VP distribution among validators, preventing dominance by a few. Figure 1a illustrates VP distribution in Cosmos blockchains, revealing concentration among top validators. It poses risks, as a minority could disrupt consensus. The ideal scenario ensures equal weighting of validators.

Block creation time and transaction throughput. Figure 1b illustrates transaction throughput over the 5-day period[3]. Typically around 5 tx/s, there are clear spikes, notably during 2024-03-24, where throughput rapidly escalates up to 50 tx/s. *This indicates occasional bursts of transaction activity, potentially impacting validator consensus despite overall network stability.*

2.2. Verifier's Dilemma

The Verifier's Dilemma, common in blockchain networks, arises when participants seek to conserve resources and gain an unfair advantage by neglecting or deviating from the validation process, jeopardizing network security [5].

In the Cosmos ecosystem, the Verifier's Dilemma manifests when remaining validators mimic the "power votes" of the subset with the highest VP, foregoing rigorous validation to expedite block finalisation. This compromises network throughput and increases computational overhead.

[3]The data can be found on https://flipsidecrypto.xyz

3. Model assessment

In this section we introduce and examine our analytical model. The model reflects the real process schematically depicted in 2.1.

We assess network throughput across probabilities of successful agreement during the Prevote and Precommit phases (corresponding to w_2 and w_3 parameters where $0 \leq w_i \leq 1$). In Figure 1c, we observe how network throughput changes based on the success probability of Prevote phase. Notably, the point where throughput for single-round ($R1$) and multi-round ($\geq R2$) completion intersects is at $w_2 = 0.51$. Additionally, the symmetric increase in Precommit phase failures shifts this intersection to $w_2 = w_3 = 0.71$ (refer to Figure 1d), indicating nearly a 40% rise in the likelihood of needing an extra round, leading to prolonged block creation time.

4. Conclusion

In this talk, we initially delve into the Verifier's Dilemma within the Cosmos blockchain, which is propelled by the Proof-of-Stake consensus mechanism. Following this, we unveil an analytical model that underpins the actual process. Conclusively, we scrutinize the model to glean insightful results that illuminate the network's performance regarding block completion across rounds of consensus.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008). URL `http://www.bitcoin.org/bitcoin.pdf`

[2] M. Alharby, R. C. Lunardi, A. Aldweesh, A. Van Moorsel, Data-driven model-based analysis of the ethereum verifier's dilemma, in: 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2020, pp. 209–220.

[3] D. Smuseva, I. Malakhov, A. Marin, A. van Moorsel, S. Rossi, Verifier's dilemma in ethereum blockchain: A quantitative analysis, in: International Conference on Quantitative Evaluation of Systems, Springer, 2022, pp. 317–336.

[4] J. Hillston, A Compositional Approach to Performance Modelling, Cambridge University Press, 1996.

[5] D. Smuseva, I. Malakhov, A. Marin, S. Rossi, Crisis of trust: Analyzing the verifier's dilemma in ethereum's proof-of-stake blockchain, in: 2023 IEEE International Conference on Blockchain (Blockchain), IEEE, 2023, pp. 332–339.