Games in Public Announcement: How to Reduce System Losses in Optimistic Blockchain Mechanisms

Siyuan Liu
School of Software and Microelectronics, Peking University
Beijing, China
2201210311@stu.pku.edu.cn

Yulong Zeng
Beijing YeeZTech Ltd
Beijing, China
freeof123@qq.com

ABSTRACT

Announcement games, where information is disseminated by announcers and challenged by validators, are prevalent in real-world scenarios. Validators take effort to verify the validity of the announcements, gaining rewards for successfully challenging invalid ones, while receiving nothing for valid ones. Optimistic Rollup, a Layer 2 blockchain scaling solution, exemplifies such games, offering significant improvements in transaction throughput and cost efficiency. We present a game-theoretic model of announcement games to analyze the potential behaviors of announcers and validators. We identify all Nash equilibria and study the corresponding system losses for different Nash equilibria. Additionally, we propose a refinement of the original mechanism that can reduce system loss. Finally, we analyze the impact of various system parameters on system loss under the Nash equilibrium and provide recommendations for parameter settings.

KEYWORDS

Optimistic Rollup; Announcement Game; Equilibrium

ACM Reference Format:
Siyuan Liu and Yulong Zeng. 2025. Games in Public Announcement: How to Reduce System Losses in Optimistic Blockchain Mechanisms. In *Proc. of the 24th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2025), Detroit, Michigan, USA, May 19 – 23, 2025*, IFAAMAS, 9 pages.

1 INTRODUCTION

Announcement games are prevalent in various real-world scenarios. In these games, announcers disseminate essential information on public platforms for specific purposes, such as PhD defenses or tender bidding. The announcement remains effective for a predetermined period, during which any party can challenge its validity. Upon raising an objection, the announcer and the objector engage in a contest stage, where the validity of both the objection and the announcement is scrutinized under supervision. The outcome determines the invalidity of either the announcement or the objection, with the loser incurring penalties and the winner gaining rewards. Importantly, if no valid objection is made during the announcement period, the announcement is deemed approved, even if it is invalid, thereby allowing the announcer to secure a significant advantage and causing potential system losses.

A concrete example of an announcement game is the optimistic mechanism in the blockchain Layer-2 (L2) ecosystem. Layer-1 (L1) refers to the base layer of the blockchain architecture, such as Bitcoin or Ethereum's mainnet. L2 solutions, on the other hand, are secondary frameworks or protocols built on top of the L1 blockchain. They aim to enhance the scalability and efficiency of the blockchain without compromising its underlying security.

L2 solutions achieve this by processing transactions[1] off the main blockchain and only recording final state on the L1 blockchain. A prominent L2 scaling solution is Optimistic Rollups. This approach allows certain users (known as aggregator) package a certain number of L2 transactions into a block and publish it on the L1, including a final state indicating the processing result of packaged transactions. The validity of the state cannot be directly verified on L1 due to scalability limitations. However, any user is allowed to challenge a fraud state and provide necessary evidence, before the block is finalized. L1 blockchain is able to determine whether the evidence is correct. If so, the block is discarded and the L1 state reverts. If there is no valid evidence within the announcement period, the block is deemed finalized. Therefore, the optimistic mechanism, with its challenge-based verification process, provides a scalable and efficient solution for ensuring transaction validity, while still remaining a security issue that fraud blocks may be finalized.

Generally speaking, an optimistic rollup game includes the following roles:

- **Aggregator**: The party proposing an L2 block, which can be either valid or invalid, corresponding to honest or attack actions, respectively. If an attack is chosen, the aggregator can specify an unlawfully but public earned income within the L2 block. In this case it is referred to as the attacker.
- **Validator**: The party responsible for verifying the validity of the L2 block proposed by the aggregator. The action space of the validator includes:
  - **Honest-verifier** (verify): The validator actively verifies the validity of the L2 block and issues a challenge if the result of the verification is negative. In either case, the validator needs to bear the verification cost.
  - **Free-rider** (no verify and no challenge): The validator neither verifies nor challenges, assuming the L2 block is correct, and has no cost.

Proc. of the 24th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2025), Y. Vorobeychik, S. Das, A. Nowé (eds.), May 19 – 23, 2025, Detroit, Michigan, USA. © 2025 International Foundation for Autonomous Agents and Multiagent Systems (www.ifaamas.org).

[1] A transaction is an instruction to change the state of a blockchain, which can be initiated by anyone.

– **Chance-taker** (no verify but challenge): The validator does not verify but issues a challenge, assuming the L2 block is incorrect, and has no cost.

If the validator chooses to verify, it is referred to as the verifier; if the validator chooses to challenge, it is referred to as the challenger. In L2 scenario, both the validator and the aggregator are required to stake a deposit, for penalizing dishonst actions.

Announcement games have broad applications, encompassing various domains such as public bidding, tender processes, academic announcements, and blockchain systems like Optimistic Rollup. A common issue in these scenarios is that when an incorrect announcement is finalized, the system incurs substantial losses. For instance, in Optimistic Rollup, if a malicious block is finalized, the attacker gains benefits that are undeserved, undermining the system's stability and credibility. Therefore, achieving lower system losses of announcement games is a crucial research focus, enhancing efficiency and reliability across these diverse fields. The announcement game addresses the complex behaviors and decision-making processes of participants. The probability of validator verification and the probability of aggregator attacking affect each other, leading to the formation of a Nash equilibrium. The situation becomes more intricate with multiple validators, as each validator's behavior is also affected by others. Based on the above findings, it is of interest to study the system losses in equilibrium and how to reduce these losses by adjusting system parameters and fine-tuning mechanisms.

Contribution. In summary, the contributions of this paper include:

(1) We study the equilbrium for n-validator case and find that the number of equilibria depends on a specific parameter, which is the ratio of the average earnings of validators plus the false positive loss to the reward of the success challenger, i.e. $\frac{\frac{T}{2}+f_p V}{\delta S}$ from Tabel 1.
(2) We find all equilibria contain purely free-rider and mixed strategy of free-rider and verifier, and corresponding system losses exhibit monotonicity with respect to the number of mixed-strategy players in the equilibrium.
(3) We purpose a refinement of the original mechanism which subsidizes malicious aggregators get caught. This mechanism, implementable by blockchain smart contract, enables the aggregator to be inclined to choose smaller amounts (Z in Tabel 1) when attacking, in the equilibrium state.
(4) Analyzing the impact of different parameters on system losses and providing suggestions to optimize the design and efficiency of the system.

2 RELATED WORKS

Blockchain technology's rapid growth has highlighted significant scalability issues in L1 blockchains, such as Bitcoin [12] and Ethereum [16], which limit transaction throughput and speed due to their consensus mechanisms [3]. L2 scaling solutions, such as State Channels, Plasma, Sidechains, and Rollups, address these limitations by operating on L2 chains to enhance scalability and efficiency [14]. Over the past year, the volume of atomic arbitrage MEV (Maximal Extractable Value) transactions on major L2 networks has exceeded $3.6 billion, accounting for 1% to 6% of all DEX (decentralized exchange) trading volumes [13]. Among these, Optimistic Rollups have gained substantial traction, with Rollups currently handling a significant portion of Ethereum's transaction volume [15]. Optimistic Rollups, such as Arbitrum [4] and Optimism [2], offer advantages like greater decentralization and compatibility with existing smart contracts by assuming transaction validity unless challenged. However, most current L2 solutions still face centralization issues. To address this, our article provides an in-depth analysis of the Optimistic Rollup system, offering essential theoretical insights for achieving full decentralization in the future.

Related studies in game theory have extensively explored announcement games in various contexts, highlighting the strategic behavior of participants in scenarios involving public announcements [6]. Ågotnes et al. [1] analyze the rational strategies in public announcement games, combining logic and game theory in the study of rational information exchange. Loi Luu et al. [10] analyse the incentivization of validators in blockchain settings. Their study shows that practical attacks exist which either waste miners' computational resources or lead miners to accept incorrect script results, known as the verifier's dilemma. These studies also highlight that announcement games are a practical scenario in blockchain. Hans et al. [7] study blockchain security through the lens of game theory, focusing on the design of reward-sharing mechanisms for validation. Another related paper is [5], where costs of validation differ, and the authors look at the problem of delegating validation.

A concurrent study by Li [9] engages with equilibrium in optimistic rollup. The author presents a model of a potential attack on the well functioning of optimistic rollups and concludes that their current design is not secure. However, the analysis does not take the deposit of validators into consideration and erroneously assumes uniform behavior among validators, resulting in flawed conclusions. Similarly, another concurrent study [11] also investigates equilibrium in optimistic rollup, providing both lower and upper bounds on the optimal number of validators, and advise on optimal design of rewards for optimal design of rewards. However, their model is criticized for its simplicity and lack of consideration for system benefits. Daji et al. [8] first focus on the behavior of chance-taker validators. Their study analysis the equilibrium of a single aggregator and validator, although it does not extend to multi-player scenarios. Our model is optimized based on the aforementioned works. We include the chance-taker as an optional behavior for validators and assume that each validator's behavior is independent. Additionally, we define the benefits of various behaviors for different roles and introduce system rewards. Finally, our model also considers scenarios involving multiple validators.

3 MODEL

Our model mainly consists of two types of roles: the aggregators $\mathcal{A}$ and the validators $\mathcal{V}$. Aggregators $\mathcal{A}$ propose L2 blocks, which can be either valid or invalid. To deter fraudulent proposals, aggregators must stake a deposit, which they forfeit if their block is invalidated. Validators $\mathcal{V}$ verify the validity of the L2 blocks. They have three strategic choices: verifier, free-rider or chance-taker. Validators also act to maximize their utilities. We state some explanations and assumption in this section.

Table 1: The Notation of Parameters

Notations	The Definition of Notations
Z	Malicious Block Value
S	Aggregator's deposit
B	Aggregator's reward
T	Validator's reward
n	The number of validators
V	the validators's deposit.
C	Cost of validation
δ	The proportion of the attacker's deposit that the challenger receives.
f_p	The proportion of penalty deposit when the validator pledges the wrong block.
f_n	The proportion of penalty deposit when the validator challenges the right block.

3.1 Parameters

Table 1 presents the various parameters of the game.

- *Malicious block value Z*: The attacker can arbitrarily assign a value to the malicious block, which he gains as well as the system losses if that block is finalized. This value includes the aggregator's reward.
- *Deposit S and V*: When dishonest players are caught, their deposits are forfeited. The system requires each aggregator to stake a fixed deposit S to penalize malicious behavior. The same applies to validators, who are required to pledge a fixed deposit V on the block.
- *System reward B and T*: If a block is finalized, the system allocates two constant amounts for rewarding the aggregator and the validator set, denoted by the *aggregator's reward B* and the *validator's reward T*. Each validator then receives a portion of the validator reward proportional to their deposit amount. This ensures that system payouts do not exceed a certain amount.
- *Cost C*: We assume that the cost for each honest validator is constant, referring to the computational cost of validation. There is no cost for dishonest (free-rider and chance-taker) validators. Additionally, the cost for aggregators is normalized to zero.
- *Reward proportion of challenger δ*: When an aggregator behaves maliciously and is challenged by a validator, the aggregator forfeits their deposit S, with a portion δS awarded to the validator. This ensures that payouts come solely from malicious actors, deterring collusion between aggregators and validators to exploit the system.
- *Penalty proportion of false positive f_p and false negative f_n*: If a validator incorrectly pledges a malicious block, a penalty of $f_p V$ is imposed. Similarly, if a validator wrongly challenges a correct block, resulting in a failed challenge, a penalty of $f_n V$ is imposed and awarded to the aggregator.
  By definition, δ, f_p, and f_n are all within the range of $[0, 1]$.

We make some assumptions on these parameters to assure that there is no dominate behavior for each party.

Assumption 1. *The validator does not play a dominated strategy, that is $\delta S > T$.*

We hope validators to challenge incorrect blocks instead of colluding with aggregators, so the reward for finding incorrect blocks should be greater than the reward for confirming blocks, that is $\delta S > T$. Additionally, we do not require $T > C$, for the reason that even the validator has a negative benefit of verifying, he may still choose to verify because once the wrong block is discovered, there will be a positive benefit.

Assumption 2. *The aggregator does not play a dominated strategy, that is $Z > B$.*

For the aggregator, choosing a larger value Z does not incur additional cost, as the difference in block values is only a numerical difference throughout the entire block. Moreover, the block value is a public information because it is on chain. So the validators can choose their behavior according to the block value.

3.2 Payoff Matrix

Based on the above analysis, when there is only one aggregator and one validator, the validator will not incur any penalties when choosing the free-rider strategy.

In most scenarios, the chance-taker strategy is dominated because validators must incur a cost to verify for a successful challenge. In L2 scenarios, precise verification of state transitions is required. Without it, validators are disable to win the battle even if the block is incorrect, known as the burden of proof. However, in cases where official authorities handle validation, such as reporting cheating in a game, the chance-taker strategy is viable. This paper focuses on the chance-taker case in a single validator game.

Table 2 presents a game involving one aggregator and one validator in a bimatrix format.

- If the aggregator attacks and the validator challenges, the aggregator loses his deposit and the validator earns a portion of the aggregator's deposit. Additionally, the validator incurs costs if he verifies.
- If the aggregator attacks and there is no challenger, the aggregator earns the malicious block value, and the validator receives the validator reward.
- A honest aggregator always earns the aggregator reward. The validator receives the validator reward if he does not challenge. Honest validators incur costs, while free-riders pay nothing. However, if the validator challenges the correct block, he loses a portion of his deposit, which goes to the aggregator.

3.3 Multiple Players

We assume that when there are multiple challengers, they equally share the challengers' benefit δS, as only the first challenger will gain and each challenger has equal probability to be the first one.

Considering multiple aggregators is pointless because there is no strategic interaction between aggregators. Validators join the game based on the first proposed block. If the first proposed block is invalid, the game proceeds with the second proposed block, and so forth.

Table 2: Payoff matrix of one aggregator and one validator. The first number indicates the utility for the aggregator, while the second number represents the utility for the validator.

	Not Attack	Attack
Free-rider	(B, T)	(Z, T)
Chance-taker	$(B + f_n V, -f_n V)$	$(-S, \delta S)$
Verifier	(B, T-C)	$(-S, \delta S - C)$

Table 3: Payoff matrix of one aggregator and n validators, where m of the n validators choose to verify. The first number indicates the utility for the aggregator, while the second number represents the utility for the validator.

	Not Attack	Attack	
2*Free-rider	$2^*(B, \frac{T}{n})$	Detected	$(-S, -f_p V)$
		Not Detected	$(Z, \frac{T}{n})$
Verifier	$(B, \frac{T}{n} - C)$	$(-S, \frac{\delta S}{m} - C)$	

Table 3 presents a game involving one aggregator and n validators in a bimatrix format. The first number represents the utility (payoff) for the aggregator, and the second number represents the utility for the validator. We assume that m out of n validators choose to verify. We also do not consider the chance-taker case with multiple players.

- If the aggregator attacks and is detected by any validator, the aggregator loses his deposit, and each challenger's earning is part of the aggregator's deposit, distributed evenly among the challengers in expectation. Moreover, if both free-riders and challengers exist simultaneously, all free-riders lose a portion of their deposits.
- If the aggregator attacks and there is no challenger, the aggregator earns the malicious block value, and validators share the validator reward averagely.
- If the aggregator is honest, he always earns the aggregator reward, and validators share the validator reward averagely. Honest validators incur costs, while free-riders pay nothing.

4 EQUILIBRIUM ANALYSIS

In this section, we progressively analyze the equilibrium for the cases of a single validator, two validators, and multiple validators.

4.1 One validator

We use β to denote the probability of $\mathcal{A}$ attacking and α as the probability of $\mathcal{V}$ verifying. Upon not verifying, $\mathcal{V}$ challenge with probability γ to be a change-taker (so w.p. $1-\alpha-\gamma$, $\mathcal{V}$ is a free-rider). Recall the payoff matrix of Table 2 from Section 3.

Lemma 4.1. *There is no pure strategy equilibrium between $\mathcal{A}$ and $\mathcal{V}$.*

Due to space limitations, the proofs of the lemmas and theorems in this paper are included in the supplementary meterial.

We then analyze mixed-strategy equilibria, where the action space for $\mathcal{V}$ is {verifier, free-rider, chance-taker}, and that for $\mathcal{A}$ is {attack, not attack}. This conclusion indicates that in the case of a single validator, except for special circumstances, there is exactly one equilibrium. Depending on the value of C, the validator chooses between a mix of being a free-rider and a verifier, or a mix of being a free-rider and a chance-taker.

Theorem 4.2. *There is a Nash Equilibrium that:*

- *If $C > \frac{(\delta S - T)(T + f_n V)}{\delta S + f_n V}$, $\mathcal{A}$ attacks with probability $\beta = \frac{T + f_n V}{\delta S + f_n V}$, while $\mathcal{V}$ challenges with probability $\gamma = \frac{Z - B}{Z + S + \lambda f_n V}$ and otherwise is free-rider;*
- *If $C < \frac{(\delta S - T)(T + f_n V)}{\delta S + f_n V}$, $\mathcal{A}$ attacks with probability $\beta = \frac{C}{\delta S - T}$, while $\mathcal{V}$ verifies with probability $\alpha = \frac{Z - B}{Z + S}$ and otherwise is free-rider;*
- *Especially, when $C = \frac{(\delta S - T)(T + f_n V)}{\delta S + f_n V}$, there are tree equilibria in total with the following strategy for $\mathcal{V}$:*

verifier	*chance-taker*	*free-rider*
α	0	$1 - \alpha$
0	γ	$1 - \gamma$
α	γ	$1 - \alpha - \gamma$

The definitions of all parameters, as well as the strategy of the aggregator, remain the same as in the previous two cases.

Sketch. In equilibrium, the aggregator and the validator are indifferent between their each behaviors. We obtain the result of Theorem 4.2 by calculating the utilities corresponding to all possible behaviors of the aggregator and the validator. See the Appendix for the specific proof. □

We can learn from the equilibrium above that system loss mainly comes from when a malicious aggregator proposes an incorrect block that has not been verified by the verifier. The system loss of one aggregator and one validator is,

$$\mathcal{L} = \beta(1 - \alpha)Z = \frac{C}{\delta S - T} \frac{(S + B)Z}{S + Z} \tag{1}$$

4.2 Extension to two validators

Starting from this section, we no longer consider the action of a chance-taker due to the fact that the burden of proof is the more common scenario.

When there are two validators, we denote the two validators as $\mathcal{V}_1$ and $\mathcal{V}_2$, with the probabilities of verifying being α_1 and α_2, respectively. In the following we will show that things are different compared to the single validator case:

- The equilibrium may not necessarily be symmetric for the validators.
- There are cases where one validator may choose a pure strategy of being a free-rider.
- The number of equilibria depends on the value of a specific constant, $R = \frac{\frac{T}{2} + f_p V}{\delta S}$

Theorem 4.3. *Denote* $R = \frac{\frac{T}{2} + f_p V}{\delta S}$. *There is an equilibrium that both* $\mathcal{V}_1$ *and* $\mathcal{V}_2$ *play the mixed strategy that they verify with probability* $\alpha = 1 - \sqrt{\frac{B+S}{Z+S}}$, *while* $\mathcal{A}$ *attacks with probability* $\beta_1 = \frac{C}{\delta S(1-\frac{1}{2}\alpha) + \alpha(\frac{1}{2}T + f_p V) - \frac{1}{2}T}$.

If $R \leq \frac{1}{2}$, *in addition to the above equilibrium, there is another equilibrium that* $\mathcal{V}_1$ *plays the mixed strategy verifying with probability* $\alpha = \frac{Z-B}{Z+S}$, *and* $\mathcal{V}_2$ *plays as a free-rider, while* $\mathcal{A}$ *attacks with probability* $\beta_2 = \frac{C}{\delta S - \frac{T}{2}}$.

Sketch. We can derive that a symmetric equilibrium always exists using the indifference condition, while the necessary and sufficient condition for the existence of an asymmetric equilibrium can be obtained through the following conditions:

Indifference condition for the mixed-strategy validator:

$$\beta\delta S + (1-\beta)(\frac{1}{2}T) - C = \frac{1}{2}T. \tag{2}$$

Difference condition for the free-rider vaildator:

$$(1-\alpha\beta)\frac{T}{2} - \beta\alpha f_p V \geq \beta(\alpha\frac{1}{2}\delta S + (1-\alpha)\delta S) + (1-\beta)(\frac{1}{2}T) - C \tag{3}$$

Combining them together yields $R \leq \frac{1}{2}$ □

Interestingly, the system loss of the symmetric equilibrium, denoted by $\mathcal{L}_1$, is:

$$\mathcal{L}_1 = \beta_1 \prod_{i=1}^{2}(1-\alpha_i)Z = \frac{C}{\delta S\left(1-\frac{1}{2}\alpha\right) + \alpha\left(\frac{1}{2}T + f_p V\right) - \frac{1}{2}T}\frac{(S+B)Z}{S+Z}.$$

Similarly, the system loss of the asymmetric equilibrium, denoted by $\mathcal{L}_2$, is:

$$\mathcal{L}_2 = \beta_2 \prod_{i=1}^{2}(1-\alpha_i)Z = \frac{C}{\delta S - \frac{1}{2}T}\frac{(S+B)Z}{S+Z}.$$

It is not hard to see that $\beta_1 > \beta_2$ is equivalent to $R < \frac{1}{2}$, which always holds when the later equilibrium exist. Therefore, the system tends to set $R < \frac{1}{2}$ to introduce an equilibrium with lower losses.

4.3 Extension to n validators

Based on the above analysis, we extend this model to multiplayer games. Unlike Li [9], the n validators are not considered as a unified entity; instead, each validator operates as an independent agent.

We first derive two propositions that no naive pure equilibrium exists in this case either.

Proposition 4.4. *In equilibrium, the aggregator does not play a pure strategy.*

If the aggregator always attacks, validators will challenge the malicious blocks, causing the aggregator to lose their deposit and switch to honest behavior. Conversely, if the aggregator never attacks, validators will free-ride, prompting the aggregator to start attacking for higher revenue.

Proposition 4.5. *In equilibrium, there is no strategy where all n validators are free-riders or where any individual purely verifies.*

Assuming that all validators are free-riders, the aggregator has a strong incentive to attack. In this scenario, if any validator switches their behavior from a free-rider to a verifier, they will achieve greater utility. Consequently, this situation cannot constitute an equilibrium.

From the two properties above, we can conclude that all validators are either purely free riders or play a mixed strategy (with respect to free riding and verifying). **We use "m-NE" to denote the equilibrium where $n-m$ validators are purely free riders, and m validators play a mixed strategy.**

Symmetry of Equilibrium. We prove that all α_i can take at most two distinct values. This implies that under equilibrium, the validators take at most three distinct actions.

Theorem 4.6. *In equilibrium with one aggregator and n validators, the behavior of the validator group adheres to the following rules:*

1. *k validators adopt a mixed strategy with probability α_1;*
2. *$m-k$ validators adopt a mixed strategy with probability α_2;*
3. *$n-m$ validators play a pure strategy as free-riders.*

A special case arises when $\alpha_1 = \alpha_2$, indicating that all validators employing a mixed strategy are symmetric.

Sketch. We prove the conclusion by contradiction. Assume there is an additional probability α_3 besides α_1 and α_2. Then denote F_i as the probability that there are i validators verifying among the remaining $m-2$ validators. The validator with probability α_1 is indifferent between being an honest verifier and a free-rider:

$$\begin{aligned}&\beta[\alpha_2\alpha_3\sum_{k=0}^{m-3}F_k\frac{\delta S}{k+3} + (1-\alpha_2)\alpha_3\sum_{k=0}^{m-3}F_k\frac{\delta S}{k+2}\\ &+ (1-\alpha_3)\alpha_2\sum_{k=0}^{m-3}F_k\frac{\delta S}{k+2} + (1-\alpha_2)(1-\alpha_3)\sum_{k=0}^{m-3}F_k\frac{\delta S}{k+1}] + (1-\beta)\frac{T}{n} - C\\ =&\beta(1-F_0(1-\alpha_2)(1-\alpha_3)(-f_p V) + (1-\beta(1-F_0(1-\alpha_2)(1-\alpha_3))\frac{T}{n}\end{aligned} \tag{4}$$

The same equation holds symmetrically for the probabilities α_2 and α_3. However, by combining these equations, we reach a contradiction when $\alpha_1 \neq \alpha_2 \neq \alpha_3$. This completes the proof. □

According to Theorem 4.6, validators choosing a mixed strategy exhibit at most two distinct verification probabilities. We first analyze the symmetric case where all probabilites are identical, and then observe the asymmetric case where there are two different probabilities.

4.3.1 The Symmetric Case. We define the constant R, which plays a crucial role in determining the properties of the equilibrium.

Definition 4.7.

$$R = \frac{\frac{T}{n} + f_p V}{\delta S}$$

Compared to the constant in the two-validator case, it just replace the number 2 with n.

Number of Equilibra. In this paragraph we analyze the number of (symmetric) equilibria. It is sufficient to consider the condition where m-NE exist. **We use α_m to denote the (identical) probability of being verifier that m mixed strategy validators take. Let A be the probability where no valitador verifies.** It is not hard to see that

Lemma 4.8.

$$A = \frac{B+S}{Z+S} = (1-\alpha_m)^m;$$

The first equation comes from the indifferent condition of the aggregator. The second equation simply comes from the multiplication rule for independent events.

By defining the following constant sequence, we find that whether m-NE exists depends on the relationship between R and this sequence.

Definition 4.9.

$$\Gamma_m = \left[\frac{1}{m(m+1)}\left(\frac{1}{A}-1\right) - \frac{\alpha_m}{m+1}\right]\frac{1-\alpha_m}{\alpha_m^2}(m>0).$$
$$\Gamma_0 = 0$$

We have the following property of Γ_m:

Lemma 4.10. *Γ_m is increasing with m.*

It can be computed that $\Gamma_1 = 1/2$, which implies the result for the two-validator case.

The theorem about the number of equilibria is stated as follows:

Theorem 4.11. *n-NE always exists. For $0 < m < n$, m-NE exist if and only if $R \le \Gamma_m$.*

In other word, if $\Gamma_{m-1} < R \le \Gamma_m$ $(0 < m < n)$, all equilibria are: m-NE, $(m+1)$-NE, ..., $(n-1)$-NE, n-NE.

Sketch. Similar to the two-validator case, we derive the main result from the indifference condition for the mixed-strategy validator

$$\beta(\frac{1-A}{m\alpha_m}\delta S - \frac{A}{1-\alpha_m}(f_p V + \frac{T}{n}) + f_p V) = C, \tag{8}$$

and the difference condition for the free-rider validator

$$\beta(\frac{1-A(1-\alpha_m)}{(m+1)\alpha_m}\delta S - A(f_p V + \frac{T}{n}) + f_p V) \le C. \tag{9}$$

Some mathematical transformations are performed. Combine the above two formulas together it yields $R \le \Gamma_m$. Due to Lemma 4.10 we also have $R \le \Gamma_k, \forall k > m$, which proves the second part of the theorem. □

System Loss. In this paragraph we analyze the system loss of all equilibria and show proof that they exhibit monotonicity. **We use β_m to denote the probability that the aggregator attack in m-NE, and the corresponding system loss is $\mathcal{L}_m$.**

Theorem 4.12. *If $\Gamma_{m-1} < R \le \Gamma_m$, then $\beta_m < \beta_{m+1} < \cdots < \beta_n$, which means that $\mathcal{L}_m < \mathcal{L}_{m+1} < \cdots < \mathcal{L}_n$.*

Sketch. We first deduce from the indifference condition to yield:

$$\beta_m = \frac{C}{P_m\delta S - Q_m(f_p V + \frac{T}{n}) + f_p V},$$

where

$$P_m = \frac{1-A}{m\alpha_m}, Q_m = \frac{A}{1-\alpha_m},$$

and both P_m and Q_m are within the range of $(0,1)$ and increasing with m.

Let $\Delta_m = \frac{P_m - P_{m+1}}{Q_m - Q_{m+1}}$, we have the following properties:

Lemma 4.13. *Δ_m is increasing with m.*

Lemma 4.14. *$\Gamma_m < \Delta_m$.*

Accoording to (8), we have $\beta_m \le \beta_{m+1} \iff R \le \Delta_m$. Combining the above lemmas and the precondition, we have $R \le \Gamma_m < \Delta_m < \Delta_{m+1} < ... < \Delta_n$, thus $\beta_m < \beta_{m+1} < .. < \beta_n$, which prove the theorem. □

In summary, we show the number of equilibria is determined by the relationship between Γ_m and R, and their corresponding system loss is monotonic with respect to m. The optimal equilibrium when $\Gamma_{m-1} < R \le \Gamma_m$ is when there are m mixed strategy validators, which is the minimum possible number.

The maximum system loss for the symmetric case is when there are n mixed strategy validators, which is given by:

$$\mathcal{L}_{sym_n} = \beta_n \prod_{i=1}^{n}(1-\alpha_i)Z = \frac{C}{P_n\delta S - Q_n(f_p V + \frac{T}{n}) + f_p V}\cdot\frac{(S+B)Z}{S+Z}.$$

4.3.2 The Asymmetric Case. Next, we consider the asymmetric case.

Suppose there are k validators who play the mixed strategy with probability α_1, and $m-k$ validators who play the mixed strategy with probability α_2. This scenario introduces variability in validator strategies, making the analysis more complex than the symmetric case. To facilitate the following analysis, we assume $\alpha_1 < \alpha_2$.

Let

$$p_3 = \sum_{i=0}^{k-1} C_{k-1}^i \alpha_1^i (1-\alpha_1)^{k-1-i} \sum_{j=0}^{m-k-1} C_{m-k-1}^j \alpha_2^j (1-\alpha_2)^{m-k-1-j}\frac{1}{i+j+2},$$

$$p_4 = \sum_{i=0}^{k-1} C_{k-1}^i \alpha_1^i (1-\alpha_1)^{k-1-i} \sum_{j=0}^{m-k-1} C_{m-k-1}^j \alpha_2^j (1-\alpha_2)^{m-k-1-j}\frac{1}{i+j+1},$$

$p_5 = (1-\alpha_1)^{k-1}(1-\alpha_2)^{m-k-1}$, we state the lemma as follows.

Lemma 4.15. *The necessary conditions for the equilibrium of asymmetric case are:*

$$(p_3 - p_4)\delta S + p_5(f_p V + \frac{T}{n}) = 0 \tag{11a}$$

$$\frac{C}{\beta} - p_4\delta S - f_p V + p_5(f_p V + \frac{T}{n}) = 0 \tag{11b}$$

$$(1-\alpha_1)^k(1-\alpha_2)^{m-k}Z - \left[1-(1-\alpha_1)^k(1-\alpha_2)^{m-k}\right]S = B \tag{11c}$$

Combining Eq. (11a), Eq. (11b), and Eq. (11c), we can determine the trend of α_1, α_2, and β as R changes. We set $n = 15$, $m = 10$, and other necessary constants. We calculated the probabilities α_1 and α_2 as shown in Fig. 1.

Observation 1. *In equilibrium of the asymmetric case, the probability of verification will be greater for the group with more mixed strategy validators, i.e. $k \le m/2$.*

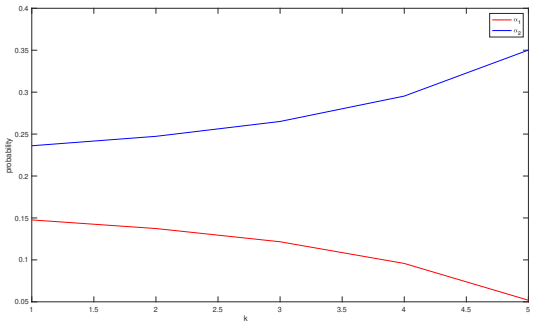

Figure 1: The relationship between the probabilities α_1 and α_2 as the number of verifier k changes.

From Eq. (11b), we can derive that:

$$\beta = \frac{C}{p_4\delta S - p_5(f_p V + \frac{T}{n}) + f_p V}.$$

Fig. 2 shows the variation of β values corresponding to different k values as R changes when $m = 10$. As k increases, the value of β decreases, resulting in a reduction in system losses. As k gradually approaches $\frac{m}{2}$, an additional β value (equilibrium) appears, and this β will gradually converge with the other β. Similarly, we set m to 11 while keeping other variables unchanged, resulting in Fig. 3.

The system loss for the asymmetric case is given by:

$$\mathcal{L}_{asym} = \beta_k \prod_{i=1}^{n}(1-\alpha_i)Z = \frac{C}{p_4\delta S - p_5(f_p V + \frac{T}{n}) + f_p V} \cdot \frac{(S+B)Z}{S+Z}. \tag{12}$$

From Figs. 2 and 3, we observe that

Observation 2. *As k increases, the conditions for the existence of equilibrium become increasingly stringent (the range of R that allows for the existence of equilibrium becomes narrower).*

Observation 3. *As k increases, the attacking probability in the equilibrium (if exist) decreases.*

$k = 0$ represents the symmetric case where all mixed strategy validators play with the same probability, and β is maximized when $k = 0$. Thus the system loss in the symmetric case is always greater than the system loss in the asymmetric case.

5 BREAKING TIE

Revisiting Table 1, all parameters can be adjusted by the system admin expect the malicious block value Z, by which the system loss is primarily effected. Suppose there are n validators, and the i-th validator has a probability α_i of verifying. We have

$$\mathcal{L} = \beta \prod_{i=1}^{n}(1-\alpha_i)Z = \beta\frac{(S+B)Z}{S+Z}. \tag{13}$$

From Eq.(13), we can see that $\mathcal{L}$ increases as the value of Z increases. However, Z is uncontrollable by the system because Z is the malicious block value chosen by the aggregator. In all beforementioned cases, the aggregator's expected utility is indifferent

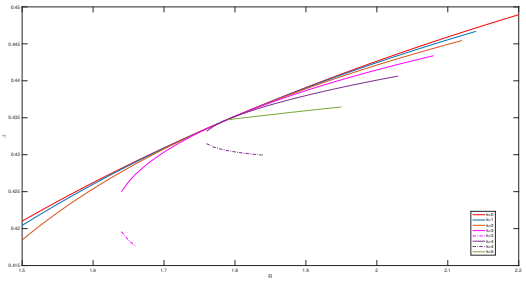

Figure 2: The image of the β as validators k and R changes. The solid line represents the general β that exists for all k, while the dashed line represents the additional β (equilibrium) that appears as k changes.

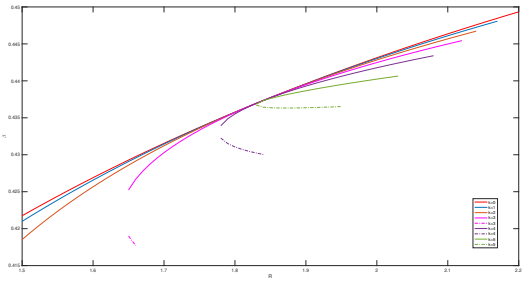

Figure 3: The image of the β as validators k and R changes. The solid line represents the general β that exists for all k, while the dashed line represents the additional β (equilibrium) that appears as k changes.

with Z, which means that he does not have a preference to Z. In this section we analyze how to fine-tune the mechanism so that the aggregator develops a bias toward Z.

To achieve the purpose of breaking tie, we introduce a system interference term D so that the penalty of attacking is related to the probability of the aggregator attacking β and the validator verifying α.

The new payoff matrix is shown in Table 4. The reason why we only add interference term D to the bottom right corner of the payoff matrix is that, only in this scenario the validator and aggregator have engaged in a battle on L1, which can be detected by the blockchain system. This mechanism can be implemented as follows: dynamically record the probability p of the aggregator's attack being challenged. Each time this occurs, in addition to penalizing the aggregator, provide a return amount based on p multiplied by a constant.

Theorem 5.1. *By adding a interference term D, the aggregator tends to choose a smaller Z, while the attacking probability β remains the same.*

Table 4: Payoff matrix with a system interference term D

	$\overline{A}$ $(1-\beta)$	A (β)
$\overline{VC}(1-\alpha)$	(B, T)	(Z, T)
V (α)	(B, $T-C$)	$(-S-\alpha\beta D, \delta S-C)$

Proof. The indifference condition for $\mathcal{V}$ remains unchanged, as the introduction of D does not change the payoff matrix of the validator. Therefore, when reaching equilibrium, $\beta = \frac{C}{\delta S - T}$.

The expected utility of the aggregator is consist of the expected utility of attacking and not attacking, that is $E_A = \beta((1-\alpha)Z + \alpha(-S-\alpha\beta D)) + (1-\beta)B$.

Fix α and other constants, the aggregator chooses β that maximizes E_A, so $E'_A(\beta) = (-\alpha S - 2\alpha^2\beta D) + (1-\alpha)Z - B = 0$. That is

$$(1-\alpha)Z - \alpha S = 2\alpha^2\beta D + B. \tag{14}$$

By replacing $(1-\alpha)Z - \alpha S$,the expected utility E_A can be simplified to

$$E_A(\beta) = \alpha^2\beta^2 D + B \tag{15}$$

Based on conditions above, we then study the optimal Z that the aggregator chooses. Now α is a function of Z (while β is still irrelevant with Z).

Take the derivative of E_A with respect to Z in Eq.(15), we have $E'_A(Z) = 2\alpha\beta^2 D\alpha'$

Take the derivative with respect to Z in Eq.(14), we have $4\alpha\beta D\alpha' + \alpha' S = 1 - \alpha - \alpha' Z$, which implies $\alpha' = \frac{1-\alpha}{4\alpha\beta D + S + Z} > 0$.

Combining with the above conclusions, we can determine the positive or negative value of $E'_A(Z)$ by the positive or negative value of D. When we set D to a negative value, $E'_A(Z) < 0$ holds. Therefore, the aggregator tends to choose a smaller Z, resulting in decreasing the system loss. □

It is worth noting that the system interference term D can be set to a very small value, so the introduction of D does not affect the behavior of other parties.

6 SUGGESTION

Based on the discussion above, we propose several suggestions for the system to maximize its benefits. These recommendations aim to optimize system parameters and mitigate potential losses from malicious behavior by aggregators.

Subsidizing caught aggregators. For the system, we suggest that the system add an interference term D providing subsidy to the caught aggregators. Because the benefits of the aggregator are independent of Z, while system loss $\mathcal{L}$ are positively correlated with Z. By introducing D, the aggregators prefer to choose a smaller Z explained in Section 6.

Decrease R. In the previous section, we discussed the equilibria of games with multiple validators. We observe the rise of more better equilibria characterized by smaller system loss as R decreases. Therefore, we consider reducing the value of R from multiple aspects.

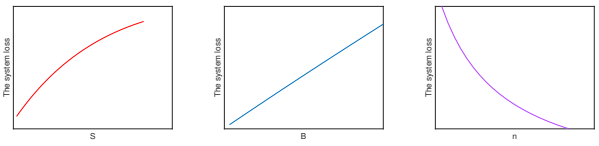

Figure 4: The system loss $\mathcal{L}$ changes by S

Figure 5: The system loss $\mathcal{L}$ changes by B

Figure 6: The system loss $\mathcal{L}$ changes by n

Decerase S. Considering the scenario of multiple validators, the worst system loss $\mathcal{L}$ of multiple validators is,

$$\mathcal{L} = \frac{C}{P_n\delta S - Q_n(f_p V + \frac{T}{n}) + f_p V} \cdot \frac{(S+B)Z}{S+Z}. \tag{16}$$

Treating the system loss $\mathcal{L}$ as a function of deposit S, we make a graph of the system loss $\mathcal{L}$ as S changes, shown in Figure. 4. We can learn that as S increases, the system loss $\mathcal{L}$ increases. Therefore, we can decrease S in order to decrease the system loss of the worst equilibrium.

It is worth noting that though decreasing S will increase R, their optimization directions are different: decreasing R raises more better equilibrium, while decreasing S reduces the system loss of the worst case equilibrium.

Decrease B. Since P_n and Q_n are related to B, we can treat the system loss $\mathcal{L}$ as a function of the reward B. Figure 5 illustrates how the system loss changes as B varies. By decreasing B, we can reduce the system loss in the worst equilibrium.

Increase n. Increasing the number of validators n will also affect the values of P_n and Q_n, thereby increasing Γ_n. This adjustment is more conducive to achieving more better equilibrium. Figure 6 shows the change in system loss with varying n. Increasing n can also reduce the system loss in the worst equilibrium. Additionally, this also helps decrease R, resulting in better equilibria.

Decrease C. From Eq. (16), it is evident that decreasing the verification cost C for the verifier also helps to decrease the system loss, which demonstrates that technological progress can improve productivity.

Increase V and f_p. Since $Q_n < 1$, $\mathcal{L}$ in Eq.16 is decreasing with $f_p V$. Similar to decrease S, increasing $f_p V$ also raises R, resulted in different optimization directions.

Increase δ. Increasing δ helps to decrease the worst system loss. At the same time, increasing δ can decrease R, raising more better equilibria.

Decrease T. $\mathcal{L}$ in Eq.16 is decreasing with T. Therefore, decreasing T can reduce the system loss $\mathcal{L}$. Additionally, this also helps decrease R, raising more better equilibria.

REFERENCES

[1] Thomas Ågotnes and Hans van Ditmarsch. 2011. What will they say?—public announcement games. *Synthese* 179 (2011), 57–85.
[2] Matthew Armstrong. 2021. Ethereum, Smart Contracts and the Optimistic Roll-up. (2021).

[3] Mirko Bez, Giacomo Fornari, and Tullio Vardanega. 2019. The scalability challenge of ethereum: An initial quantitative analysis. In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE, 167–176.
[4] Lee Bousfield, Rachel Bousfield, Chris Buckland, Ben Burgess, Joshua Colvin, E Felten, Steven Goldfeder, Daniel Goldman, Braden Huddleston, H Kalonder, et al. 2022. Arbitrum nitro: A second-generation optimistic rollup.
[5] Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias, and Aikaterini-Panagiota Stouka. 2020. Reward sharing schemes for stake pools. In *2020 IEEE european symposium on security and privacy (EuroS&p)*. IEEE, 256–275.
[6] Jianying Cui and XiaoJia Tang. 2010. A method for solving Nash equilibria of games based on public announcement logic. *Science China Information Sciences* 53 (2010), 1358–1368.
[7] Hans Gersbach, Akaki Mamageishvili, and Manvir Schneider. 2022. Staking pools on blockchains. *arXiv preprint arXiv:2203.05838* (2022).
[8] Daji Landis. 2023. Incentive Non-Compatibility of Optimistic Rollups. *arXiv preprint arXiv:2312.01549* (2023).
[9] Jiasun Li. 2023. On the security of optimistic blockchain mechanisms. *Available at SSRN 4499357* (2023).
[10] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. 2015. Demystifying incentives in the consensus computer. In *Proceedings of the 22Nd acm sigsac conference on computer and communications security*. 706–719.
[11] Akaki Mamageishvili and Edward W Felten. 2023. Incentive Schemes for Rollup Validators. In *The International Conference on Mathematical Research for Blockchain Economy*. Springer, 48–61.
[12] Satoshi Nakamoto. 2008. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* 9 (2008), 15.
[13] Danning Sui. [n.d.]. It's time to talk about L2 MEV. [Online]. https://collective.flashbots.net/t/it-s-time-to-talk-about-l2-mev/3593.
[14] Louis Tremblay Thibault, Tom Sarry, and Abdelhakim Senhaji Hafid. 2022. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access* 10 (2022), 93039–93054.
[15] Louis Tremblay Thibault, Tom Sarry, and Abdelhakim Senhaji Hafid. 2022. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access* 10 (2022), 93039–93054.
[16] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.