Model

In this model, we analyze the strategic interactions between two types of players in the Optimistic Rollup system: *proposers* and *validators*. The game is defined as follows:

- **Players**: The model involves two types of players:
  - **Proposer** (P): One player submits batches of transactions to the rollup.
  - **Validators** (V): There are n players are responsible for verifying the transactions in the submitted batches.
- **Game Setup**:
  - We assume there are n rational validators in the system.
  - Each **Validator** can choose between:
    - **Honest Verification** ($\mathcal{V}$): The validator verifies the transactions as required.
    - **Free Riding** ($\mathcal{F}$): The validator does not verify the transactions and just approve the proposed result.
  - The **Proposer** can choose between
    - **Honest Proposing** ($\mathcal{H}$): The proposer submits transactions that are valid and adhere to the rules of the rollup.
    - **Attacking** ($\mathcal{A}$): The proposer submits transactions that are invalid or attempt to exploit the system.
- **Strategies**:
  - Each validator i can adopt a mixed strategy where they choose to verify transactions with probability and free ride with probability α and $1-\alpha$, respectively.
  - The proposer can adopt a mixed strategy where it chooses to be honest and to attack with probability β and $1-\beta$, respectively.
- **Payoff**
  - **Staking Rule**:
    - **Validators** must stake an amount denoted by V to participate in the validation process. This stake acts as collateral to ensure that validators act honestly.
    - **The Proposer** is required to stake an amount denoted by S to submit transactions. This stake serves as a guarantee of their commitment to proposing valid transactions and disincentivizes malicious behavior.
  - **Reward Rule**:
    - **Validators** who correctly verify transactions receive a reward denoted by T, which represents a portion of transaction fees or other incentives provided by the system. Notably, if there are multiply validators correctly verify, each validator receives a portion of the reward T proportional to their deposit amount.
    - **The Proposer** who submits valid transactions receives a reward denoted by B, which is based on transaction fees or a fixed

incentive per batch of transactions proposed.

- **Slash Rule**:
  - **Validators** are subject to slashing if they are found to be malicious or fail to perform their verification duties. This involves forfeiting a portion of their staked amount, f_pV, as a penalty.
  - **The Proposer** is also subject to slashing if they submit invalid or malicious transactions. If the proposer is found to be dishonest, they forfeit all of their staked amount, a portion of which, δS, is given to the honest validator and the rest of which is burned.
- **Verification Cost**:
  - **Honest Verification** incurs a cost denoted by C, which includes the computational resources and time required for validators to verify transactions. This cost is borne by validators who choose to act honestly.
- **Malicious Block Value**:
  - The value of a Malicious Block is denoted by Z which represents the potential gains an attacker could achieve by submitting fraudulent transactions.
- **Payoff Matrix**:
  We assume that (m) out of (n) validators choose to verify. The first number indicates the utility for the proposer, while the second number represents the utility for the validators.

	Honest Proposing	Attacking
Free Riding but Slashed	$(B, \frac{T}{n})$	$(-S, -f_pV)$
Free Riding and not Slashed	$(B, \frac{T}{n})$	$(Z, \frac{T}{n})$
Honest Verification	$(B, \frac{T}{n} - C)$	$(-S, \frac{\delta S}{m} - C)$

Results

Lemma:

- In equilibrium, the proposer does not play a pure strategy.
- In equilibrium with n validators, there is no strategy where all validators are free-riders or one validator purely verifies.
- In equilibrium with n validators, the validators who choose a mixed strategy will exhibit at most two types of behavior.

Conclusion on n Validators

Definition of $m - NE$:

- In the m-NE, m validators play mixed strategies, while the remaining $n-m$ validators adopt a Free Riding ($\mathcal{F}$) strategy.

Denote

- $A = \frac{B+S}{Z+S}$
- $R = \frac{\frac{T}{n}+f_pV}{\delta S}$
- When there are m mixed strategy players:
  - $P_m = \frac{1-A}{m\alpha_m}$, $Q_m = \frac{A}{1-\alpha_m}$
  - $\Delta_m = \frac{P_m - P_{m+1}}{Q_m - Q_{m+1}}$
  - $T_m = \left[\frac{1}{m(m+1)}\left(\frac{1}{A}-1\right) - \frac{\alpha_m}{m+1}\right]\frac{1-\alpha_m}{\alpha_m^2}(m>0)$

Proposition

- $\beta = \frac{\epsilon}{P_m\delta S - Q_m(f_pV+\frac{T}{n})+f_pV}$
- $\alpha_m = 1 - \sqrt[m]{\frac{B+S}{Z+S}}$

Main Theorem

- n-NE always exists.
- When $\Gamma_{m-1} < R \leq \Gamma_m$, additional $n-m$ equilibriums are m-NE, $(m+1)$-NE, $\ldots$, $(n-1)$-NE.
- The probabilities in the equilibrium are shown by the above proposition.

Future

In future work, we will provide a comprehensive computation process and formal proof of the theorem to rigorously validate our findings. We will also analyze the impact of different equilibria on the security of the Optimistic Rollup system, including the effects on system resilience and incentive compatibility. Additionally, we plan to explore potential enhancements to the incentive mechanisms, conduct simulations to test our theoretical results, and investigate generalizations and extensions of the model to other blockchain systems and scenarios. These efforts aim to refine our understanding of the system's dynamics and improve its overall security and effectiveness.

Related

[1] Li, Jiasun. "On the security of optimistic blockchain mechanisms." Available at SSRN 4499357 (2023).

[2] Mamageishvili, Akaki, and Edward W. Felten. "Incentive Schemes for Rollup Validators." The International Conference on Mathematical Research for Blockchain Economy. Cham: Springer Nature Switzerland, 2023.

[3] Landis, Daji. "Incentive Non-Compatibility of Optimistic Rollups." arXiv preprint arXiv: 2312.01549 (2023).