Formal Methods for System Verification

Suggestions for projects

Each group will have a dedicated analysis. Below you can find details for each project:

1. **"Crisis of Trust: Analyzing the Verifier's Dilemma in Ethereum's Proof-of-Stake Blockchain"**

Group 5 Modify the number of slots to 25 & modify rewards and delays in Table 1 to the following values:
1 slot - 0.844;
$1 < delay \leq 3$ slots - 0.625;
$3 < delay \leq 25$ slots - 0.188;
$delay > 25$ - 0.625
On the last slide discuss the possible mitigation approaches.

Group 11 Modify the number of slots to 27 & modify rewards and delays in Table 1 to the following values:
$1, 2$ slots - 0.844;
$2 < delay \leq 6$ slots - 0.625;
$6 < delay \leq 27$ slots - 0.188;
$delay > 27$ - 0.625
On the last slide discuss the possible mitigation approaches.

Group 14 Modify the number of slots to 28 & modify rewards and delays in Table 1 to the following values:
$1, 2, 3$ slots - 0.844;
$3 < delay \leq 9$ slots - 0.625;
$9 < delay \leq 28$ slots - 0.188;
$delay > 28$ - 0.625
On the last slide discuss the possible mitigation approaches.

2. **"Verifier's Dilemma in Ethereum Blockchain: A Quantitative Analysis"**

Group 1 Table 4: Consider component E_F. How could we improve it and its verification step V_{EF}? (When the environment produces a block, all of the miners in the environment go to V_{EF}. Can one miner still produce a block? How could we show it in the model?). Modify the value N to $400,000$ and the other parameters that are affected by this change.

Group 4 Table 4: Synchronise the fair components on verification. Modify the value N to $300,000$ and the other parameters that are affected by this change.

Group 8 Table 1: Consider component E_F. How could we improve it and its verification step V_{EF}? (When the environment produces a block, all of the miners in the environment go to V_{EF}. Can one miner still produce a block? How could we show it in the model?). Modify the value N to $200,000$ and the other parameters that are affected by this change. Synchronise the fair components on verification.

Group 10 Tables 1 and 4: Consider component E_F. How could we improve it and its verification step V_{EF}? (When the environment produces a block, all of the miners in the environment go to V_{EF}. Can one miner still produce a block? How could we show it in the model?). Synchronise the fair components on verification.

3. **"Selfish Mining in Public Blockchains"**

Group 2 Extend the model by introducing another mining pool M_S. What kind of analysis can be done with the modified model?

Group 6 Modify the value K to $10,000$ and study the network with various values of w such that $100/1,000/10,000$

Group 13 Modify the value K to $20,000$ and study the network with various values of w such that $150/1,500/15,000$

4. **"Under the space threat: Quantitative Analysis of Cosmos blockchain"**

Assume that Propose and Prevote rates, i.e., γ and β, always correspond to their timeouts.

Group 7 Study the model by examining the Propose timeout such that it can take values of $[1, 2, 3, 4, 5, 6]$s. Which kind of dynamics does it reveal about the network? Reason about this.

Group 12 Study the model by examining the Precommit timeout. Introduce a way to compute its corresponding probability w_3. How does it affect the network?

5. **"Cosmos discovery: Quantitative assessment of Cosmos blockchain"**

Assume that Propose and Prevote rates, i.e., γ and β, always correspond to their processing times.

Group 3 Examine Celestia, a blockchain within the Cosmos ecosystem. Apply adjusted parameters to evaluate the system's throughput and determine the optimal processing times for both homogeneous and non-homogeneous scenarios. Assume that all parameters are doubled relative to those of the Cosmos blockchain.

Group 9 Examine Injective, a blockchain within the Cosmos ecosystem. Apply adjusted parameters to evaluate the system's throughput and determine the optimal processing times for both homogeneous and non-homogeneous scenarios. Assume that all parameters are reduced to $\frac{1}{10}$ of timeouts used in the Cosmos blockchain.