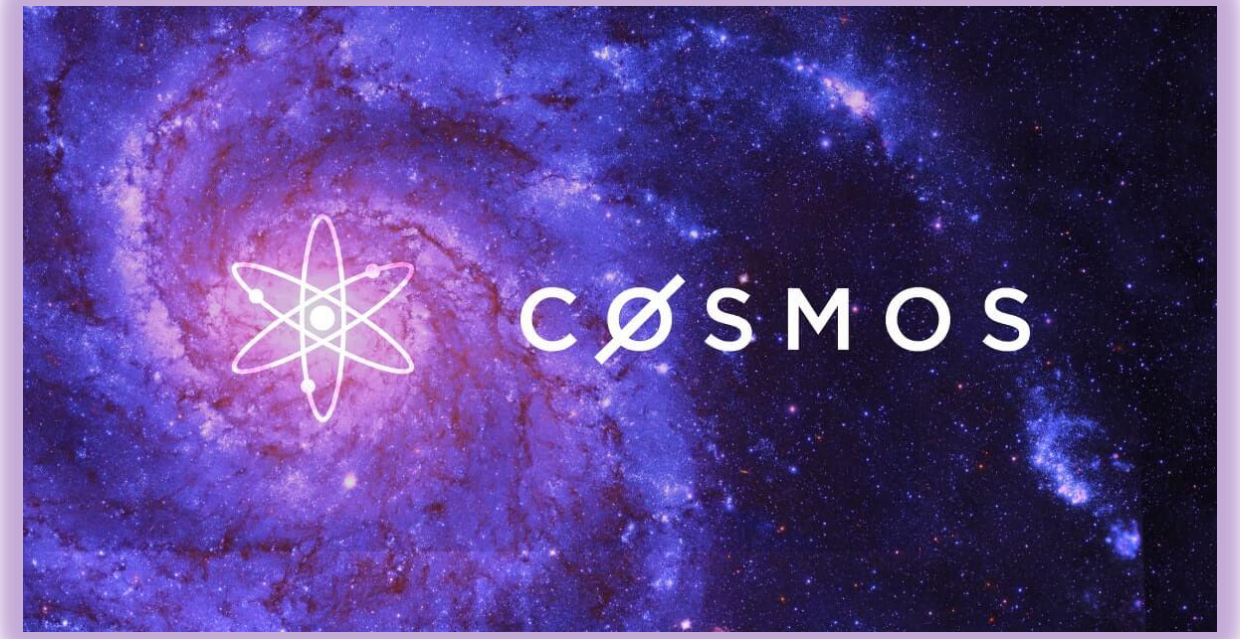
Towards a Resilient Cosmos: Evaluating Consensus Process in PoS Networks

Daria Smuseva Ivan Malakhov Andrea Marin Carla Piazza and Sabina Rossi

MASCOTS 2024

About Cosmos Ecosystem

- Network of blockchain networks
- Inter-Blockchain Communication
- PoS consensus
- Multi-round consensus
- CosmosBFT (ex Tendermint)



PoS Blockchains

Characteristics:

- Validators
- Agreement by voting
- Stake
  - Voting power
  - Propose probability
  - Reward

Examples:

- Ethereum
- Algorand
- Cosmos
- …

Challenges:

- Verifiers Dilemma
- Frontrunning Economic Attack
- Reorg Attack
- Balancing-type Attacks
- Voting Delay Attack
- …

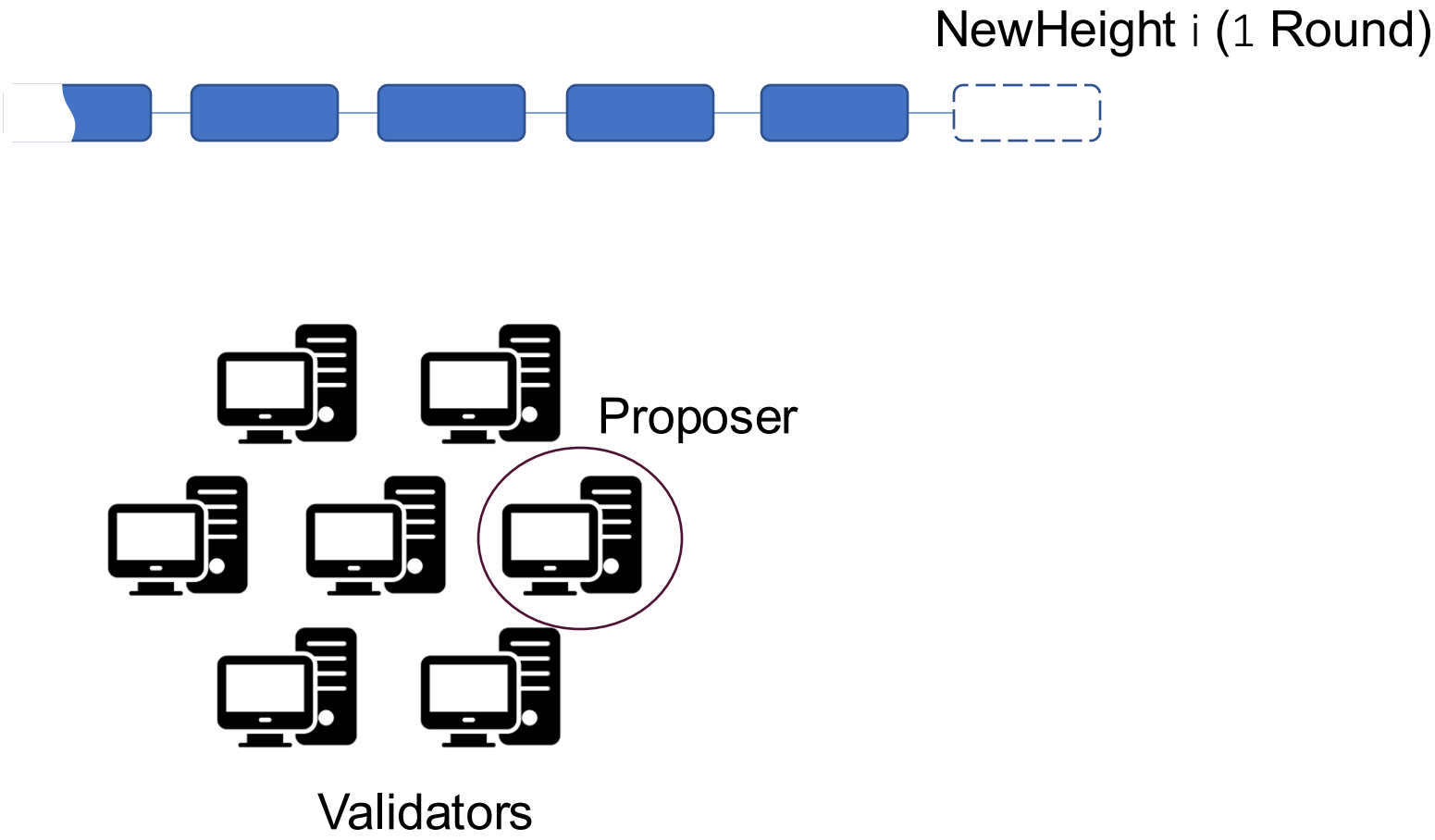
Cosmos consensus

$$\text{NewHeight} \rightarrow \underbrace{(\text{Propose} \rightarrow \text{Prevote} \rightarrow \text{Precommit})}_{\text{Round}}^{\geq 1} \rightarrow \text{Commit} \rightarrow$$

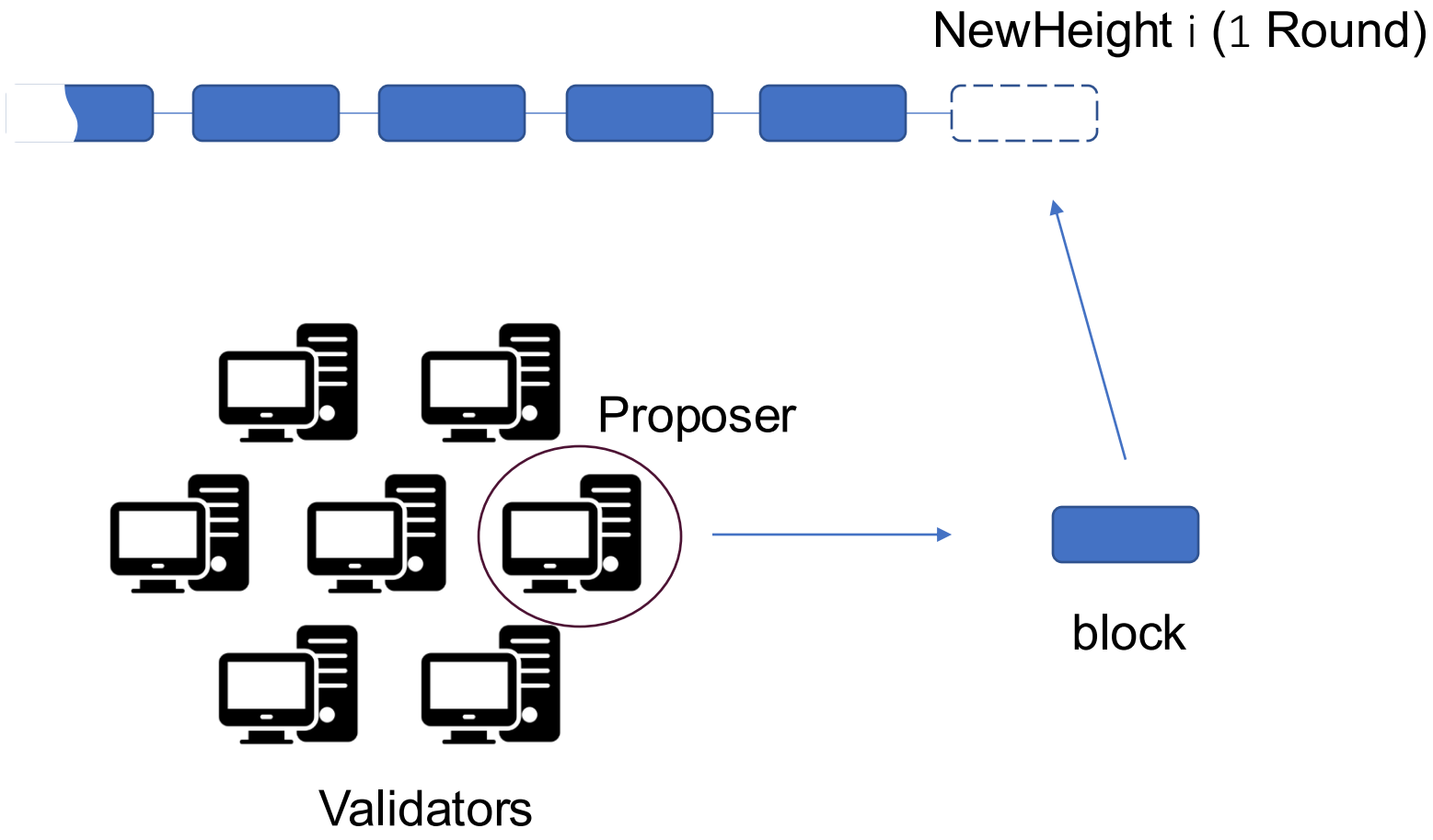
Notes:

- One or more rounds needed
- New round increases step timeouts

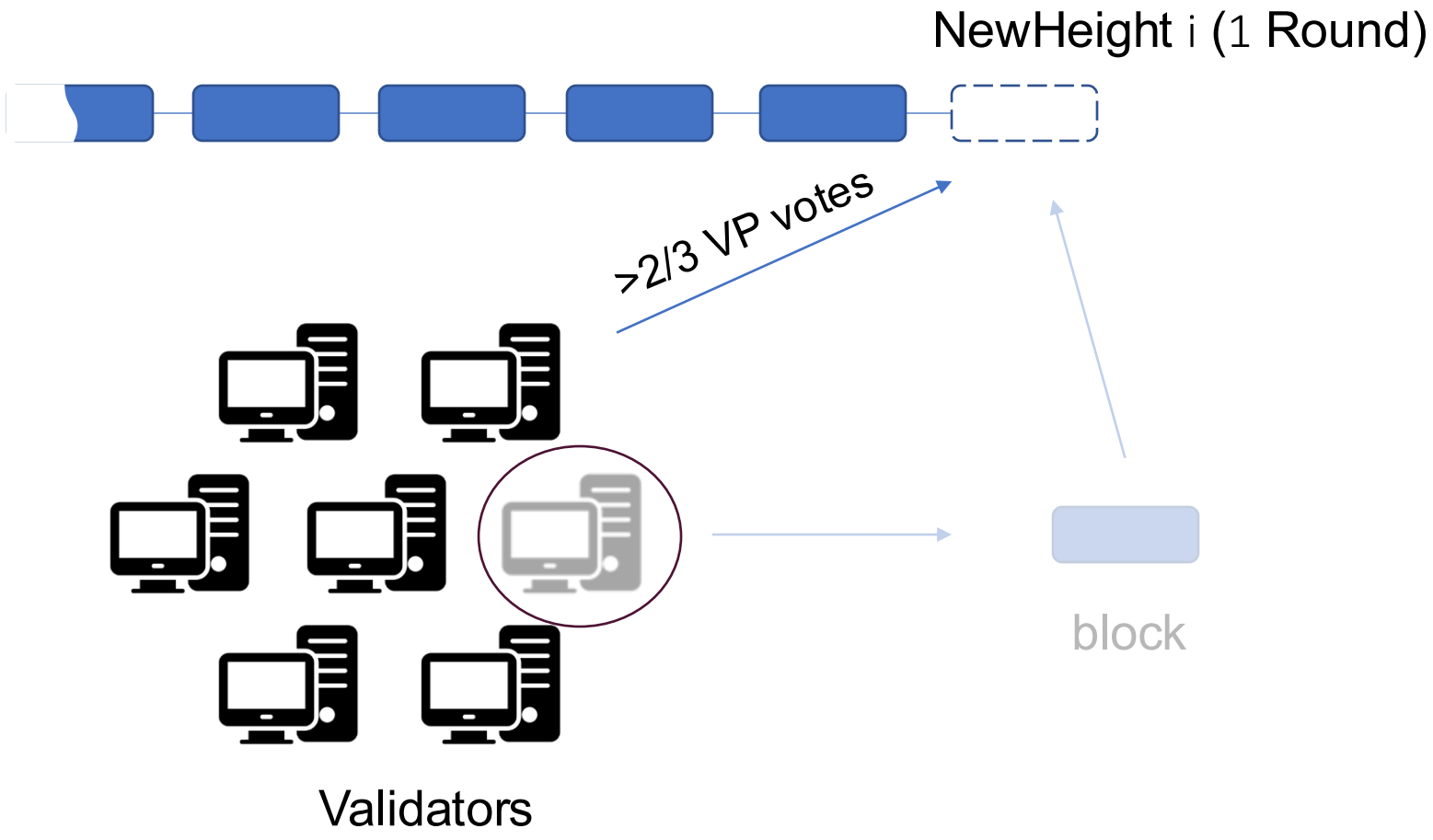
Consensus: Example



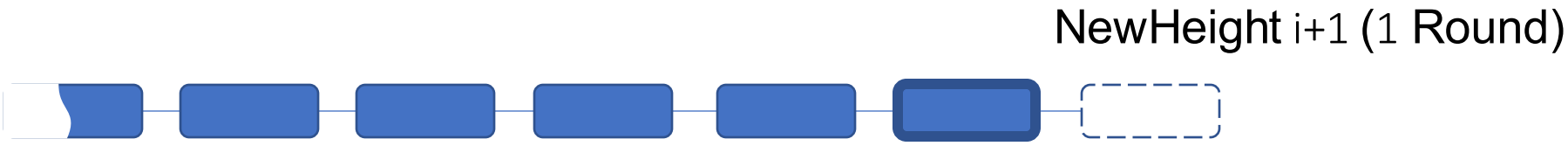
Consensus: Example

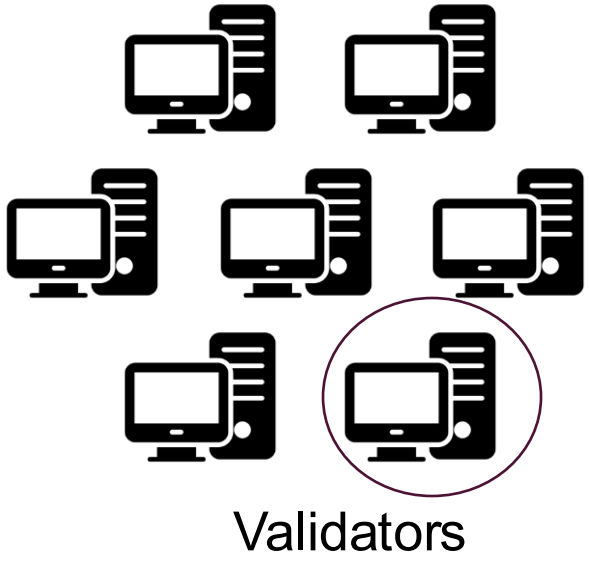


Consensus: Example

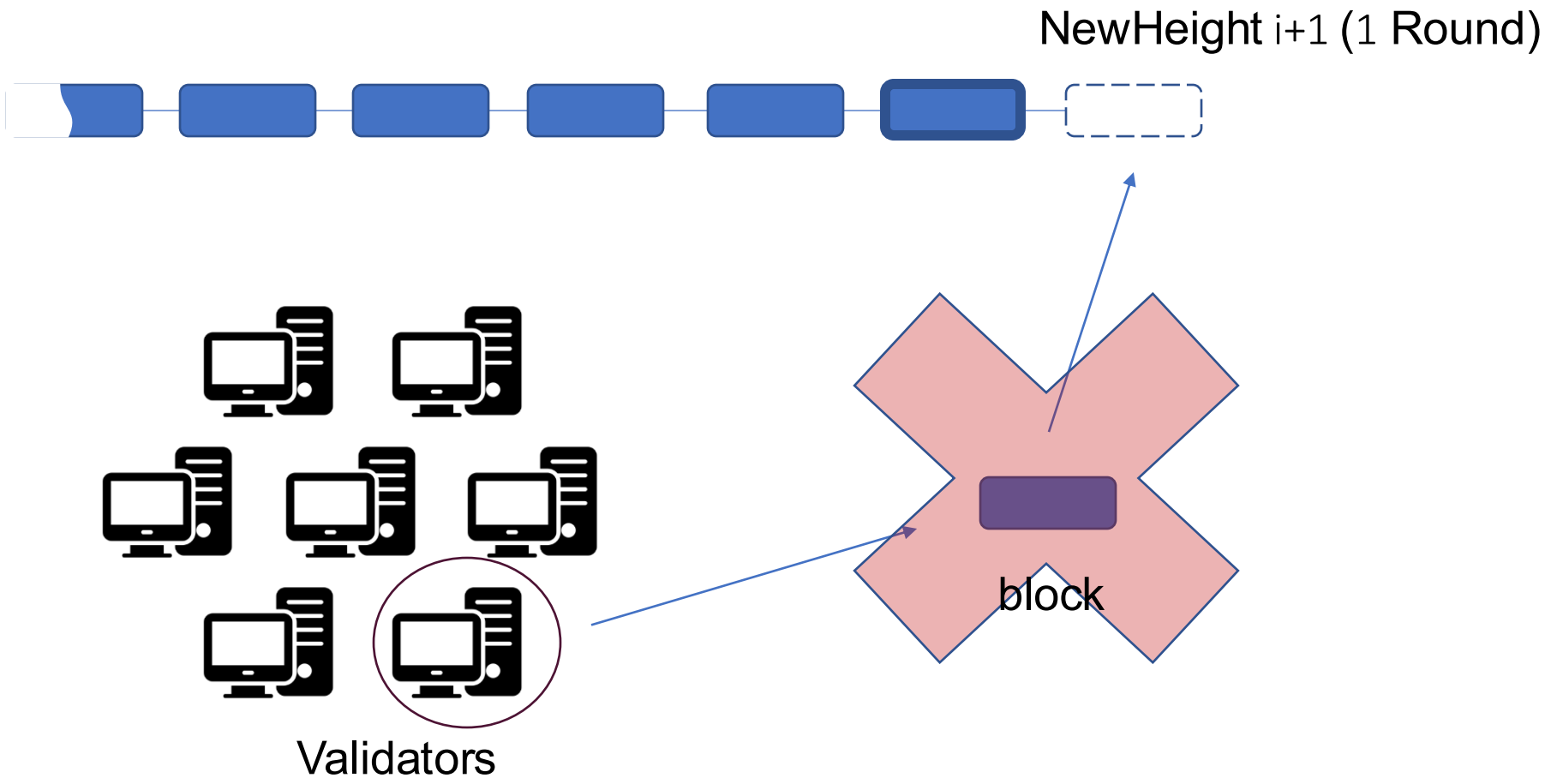


Consensus: Example

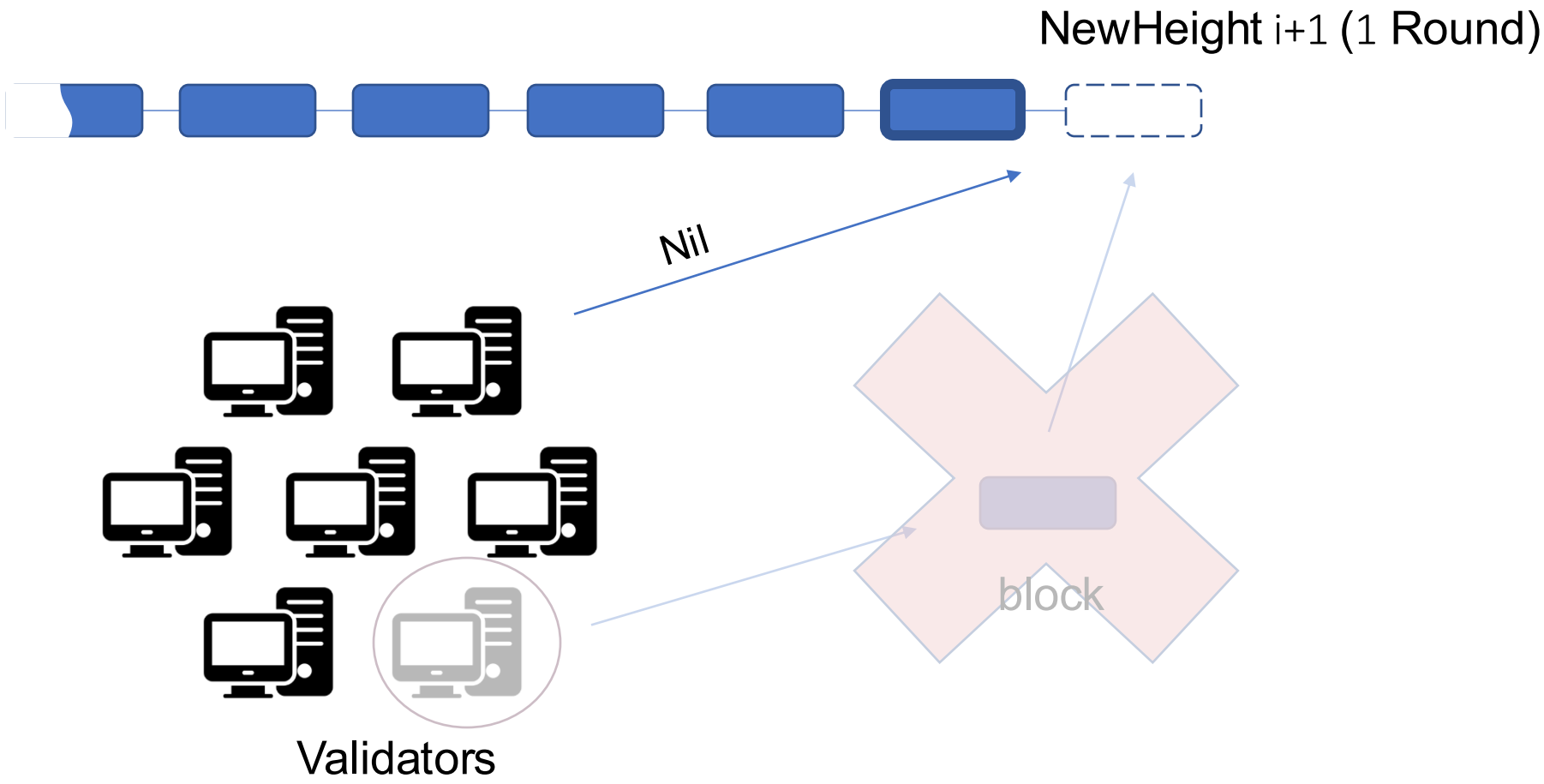




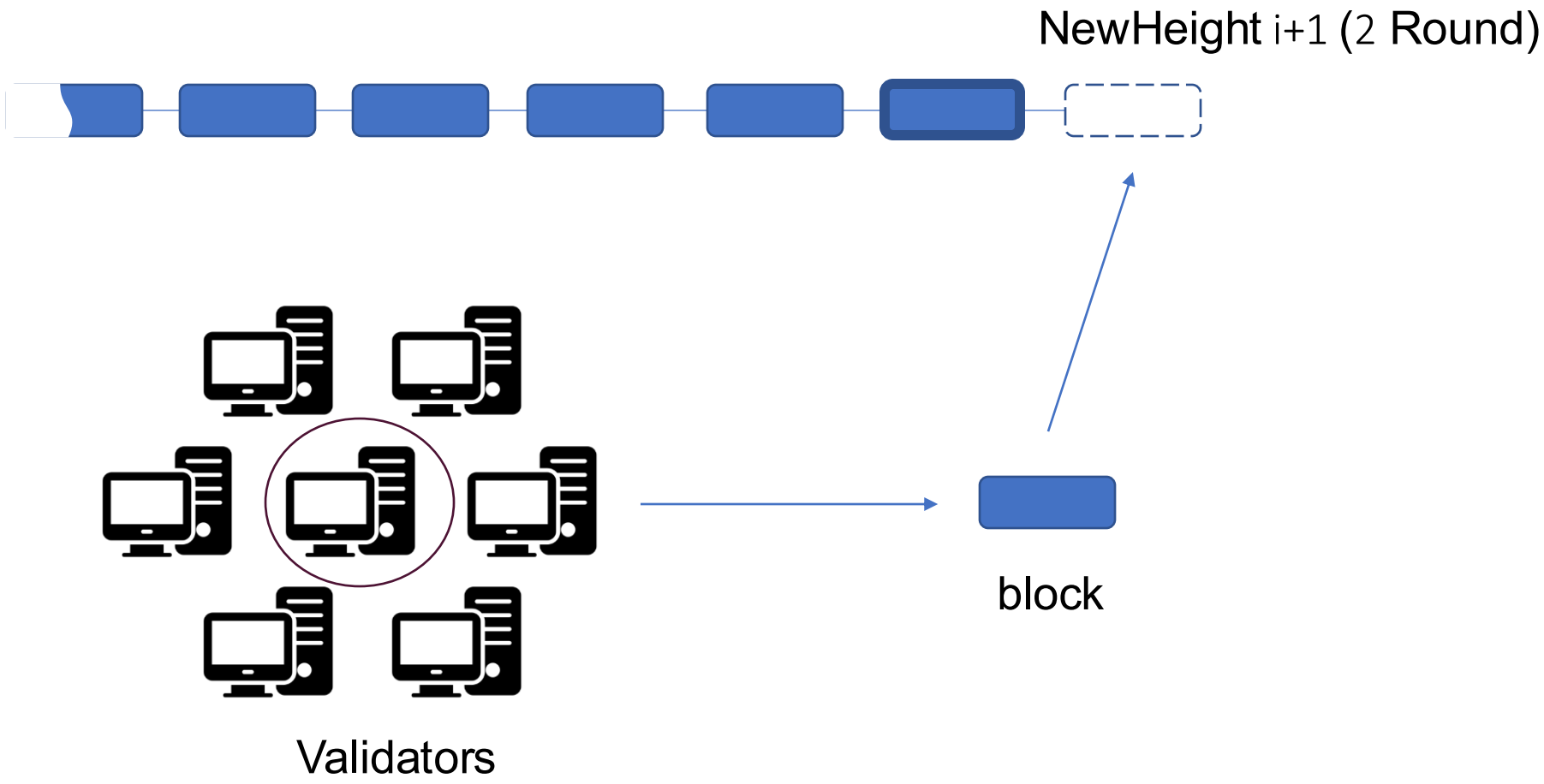
Consensus: Example



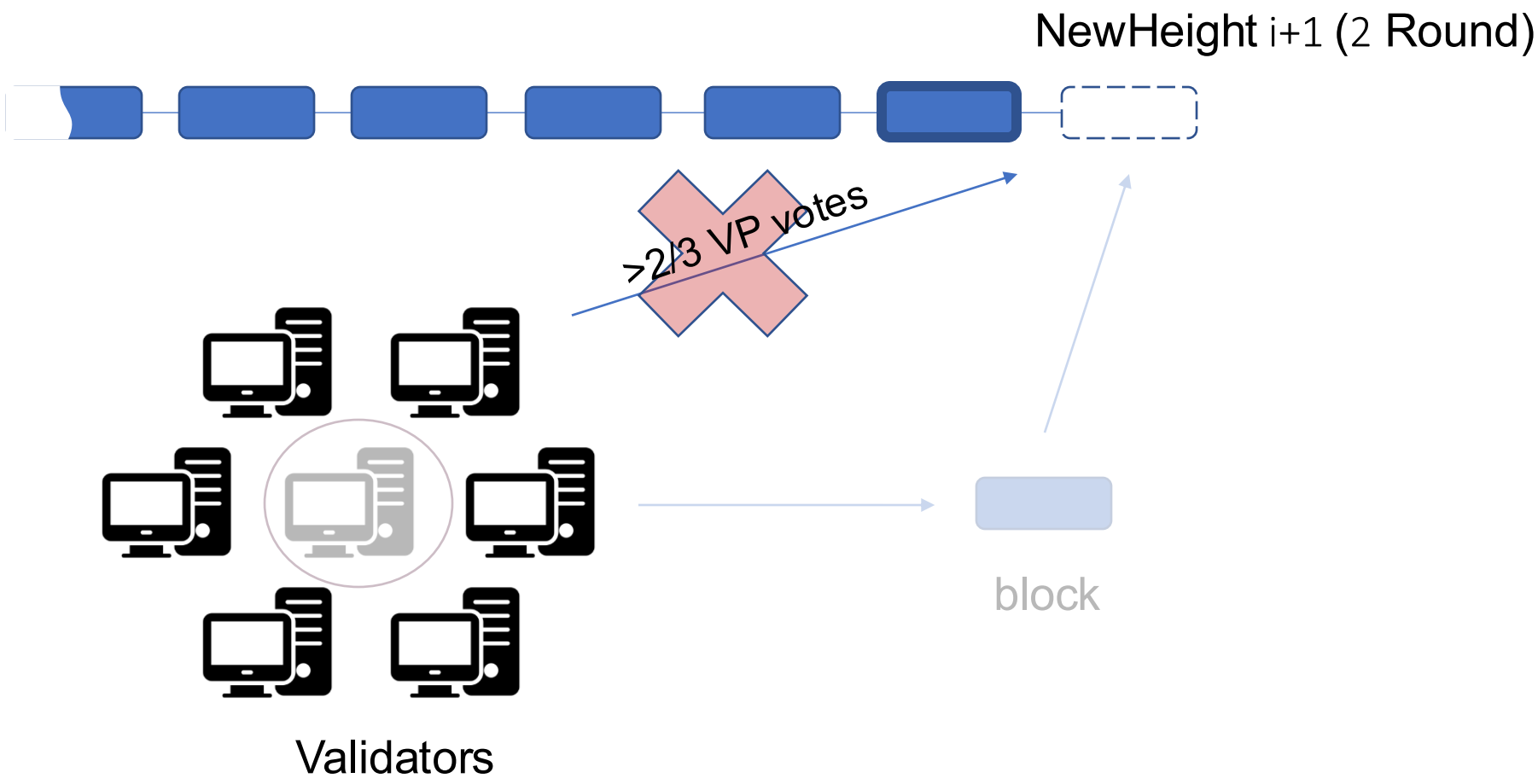
Consensus: Example



Consensus: Example



Consensus: Example



Problem statement

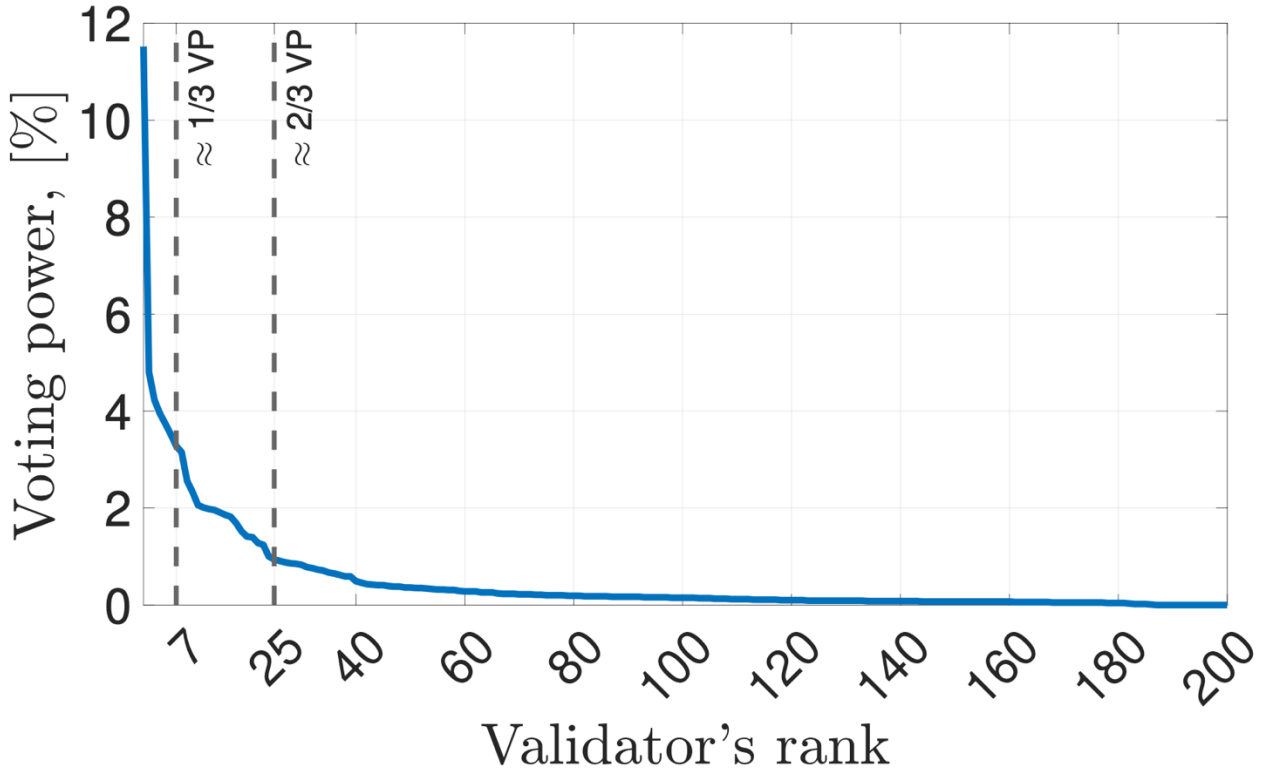
Lack of performance assessment of Cosmos blockchain protocol

Contribution

- Analytical models of Cosmos consensus mechanism
  - Impact of multi-round consensus
  - Optimal processing time for network configuration
  - Effect of increased timeout durations
  - Impact of colluding validators
  - Effects of partial validator unavailability

NOTE: We use Cosmos blockchain as a viable example of Cosmos network

Cosmos blockchain: data visualization



Voting Power distribution of Cosmos blockchain

Performance Evaluation Process Algebra (PEPA)

Operators:

$$P ::= P \underset{L}{\bowtie} P \mid P/L \mid S$$

Cooperation Hiding

$$S ::= (\alpha, r).S \mid S + S \mid A$$

Prefix Choice

- α - action type
- r - activity rate
- τ - unknown action type
- $\top$ - unspecified rate
- L - cooperation set

- P - model component
- S - sequential component
- A - countable set of constants

Base Model introduction

$$
\begin{array}{lcl}
NewHeight & \stackrel{def}{=} & (nh, n).Round_1 \\
\hline
Round_i & \stackrel{def}{=} & (r, n).Propose_i \\
Propose_i & \stackrel{def}{=} & (p, w_{1_i}\gamma_i).Prevote_i + (p, (1 - w_{1_i})\gamma_i).NilPrevote_i \\
Prevote_i & \stackrel{def}{=} & (pv, w_{2_i}\beta_i).Precommit_i + (pv, (1 - w_{2_i})\beta_i).Unsuccess_i \\
NilPrevote_i & \stackrel{def}{=} & (npv, \beta_i).Unsuccess_i \\
Unsuccess_i & \stackrel{def}{=} & (pc, \delta_i).Round_i \\
Precommit_i & \stackrel{def}{=} & (pc, w_3\delta_i).Commit_i + (pc, (1 - w_{3_i})\delta).Round_j \\
Commit_i & \stackrel{def}{=} & (c_i, \eta).NewHeight
\end{array}
$$

where $\gamma_i = max\left(\frac{1}{t_1}, \frac{1}{T_1 + (i-1)g}\right)$, $\beta_i = max\left(\frac{1}{t_2}, \frac{1}{T_2 + (i-1)g}\right)$,

$\delta_i = \frac{1}{T_3 + (i-1)g}$, $\eta = \frac{1}{T_4}$, $i \in \{1, \ldots, R\}$ and $j = min(i+1, R)$

Model with different proposers introduction

$$
\begin{array}{rcl}
NewHeight & \stackrel{def}{=} & (nh, n).Round_1 \\
\hline
Round_i & \stackrel{def}{=} & (r, p_{FF}\, n).Propose_{i_{FF}} + (r, p_F\, n).Propose_{i_F} + (r, p_S\, n).Propose_{i_S} \\
Propose_{i_{FF}} & \stackrel{def}{=} & (p, w_{1_{i_{FF}}} \gamma_{i_{FF}}).Prevote_i + (p, (1 - w_{1_{i_{FF}}})\gamma_{i_{FF}}).NilPrevote_i \\
Propose_{i_F} & \stackrel{def}{=} & (p, w_{1_{i_F}} \gamma_{i_F}).Prevote_i + (p, (1 - w_{1_{i_F}})\gamma_{i_F}).NilPrevote_i \\
Propose_{i_S} & \stackrel{def}{=} & (p, w_{1_{i_S}} \gamma_{i_S}).Prevote_i + (p, (1 - w_{1_{i_S}})\gamma_{i_S}).NilPrevote_i \\
Prevote_i & \stackrel{def}{=} & (pv, w_{2_i} \beta_i).Precommit_i + (pv, (1 - w_{2_i})\beta_i).Unsuccess_i \\
NilPrevote_i & \stackrel{def}{=} & (pv, \beta_i).Unsuccess_i \\
Unsuccess_i & \stackrel{def}{=} & (pc, \delta_i).Round_j \\
Precommit_i & \stackrel{def}{=} & (pc, w_3 \delta_i).Commit_i + (pc, (1 - w_3)\delta_i).Round_j \\
Commit_i & \stackrel{def}{=} & (c_i, \eta).NewHeight
\end{array}
$$

where $\gamma_{i_{FF/F/S}} = max\left(\frac{1}{t_{1_{FF/F/S}}}, \frac{1}{T_1 + (i-1)g}\right)$, $\beta_i = max\left(\frac{1}{t_2}, \frac{1}{T_2 + (i-1)g}\right)$,

$\delta_i = \frac{1}{T_3 + (i-1)g}$, $i \in \{1, \ldots, R\}$ and $j = min(i+1, R)$, and $\eta = \frac{1}{T_4}$ while $p_{FF} + p_F + p_S = 1$

Model parameterization

Propose rate

$$\gamma_i = max\left(\frac{1}{t_1}, \frac{1}{T_1 + (i-1)g}\right)$$

Prevote rate

$$\beta_i = max\left(\frac{1}{t_2}, \frac{1}{T_2 + (i-1)g}\right)$$

Name	Duration
Propose timeout, (T_1)	3s
Prevote timeout, (T_2)	1s
Precommit timeout, (T_3)	1s
Timeout increase, (g)	0.5s
Commit timeout, (T_4)	1s

Model parameterization

Success probabilities (for the first Round)

$$w_{1_{FF/F/S}} = Pr[X_{1_{FF/F/S}} \leq T_1] = 1 - e^{-\frac{1}{t_{1_{FF/F/S}}} T_1}$$

$$w_2 = Pr[X_2 \leq T_2] = 1 - e^{-\frac{1}{t_2} T_2}$$

$$w_3 \to 1$$

Model parameterization

Success probabilities (for the first Round)

$$w_{1_{FF/F/S}} = Pr[X_{1_{FF/F/S}} \leq T_1] = 1 - e^{-\frac{1}{t_{1_{FF/F/S}}}T_1}$$

$$w_2 = Pr[X_2 \leq T_2] = 1 - e^{-\frac{1}{t_2}T_2}$$

$$w_3 \to 1$$

Model parameterization

Success probabilities (for the first Round)

$$w_{1_{FF/F/S}} = Pr[X_{1_{FF/F/S}} \leq T_1] = 1 - e^{-\frac{1}{t_{1_{FF/F/S}}} T_1}$$

$$w_2 = Pr[X_2 \leq T_2] = 1 - e^{-\frac{1}{t_2} T_2}$$

$$w_3 \to 1$$

Model parameterization

Success probabilities (for the first Round)

$$w_{1_{FF/F/S}} = Pr[X_{1_{FF/F/S}} \leq T_1] = 1 - e^{-\frac{1}{t_{1_{FF/F/S}}} T_1}$$

$$w_2 = Pr[X_2 \leq T_2] = 1 - e^{-\frac{1}{t_2} T_2}$$

$$w_3 \to 1$$

Prevote rates for FF , F , S

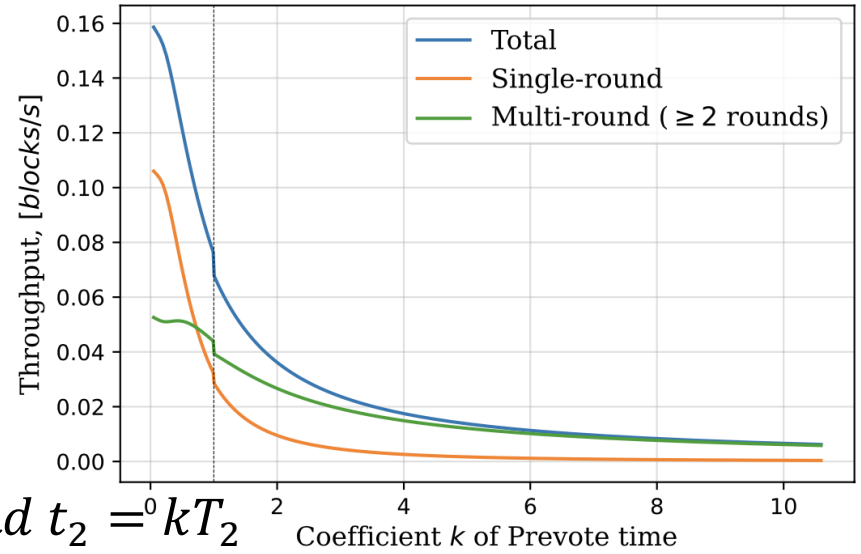
$$\overline{VP}_{FF} = 0.0483, \quad \overline{VP}_F = 0.0184, \quad \overline{VP}_S = 0.0021$$

$$t_{1_{FF}}^{-1} = \frac{\overline{VP}_{FF}}{\overline{VP}_F} \frac{1}{3}, \quad t_{1_F}^{-1} = \frac{\overline{VP}_F}{\overline{VP}_F} \frac{1}{3}, \quad t_{1_S}^{-1} = \frac{\overline{VP}_S}{\overline{VP}_F} \frac{1}{3}$$

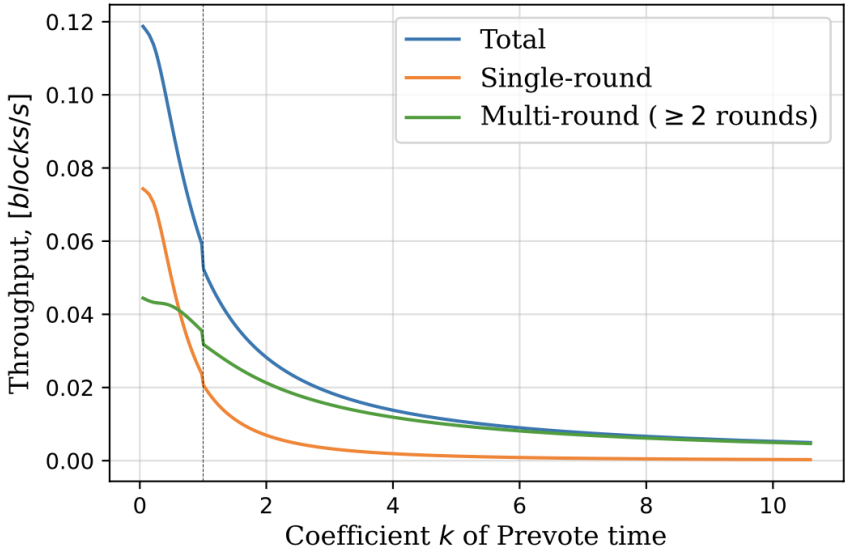
Numerical results: multi-round throughput

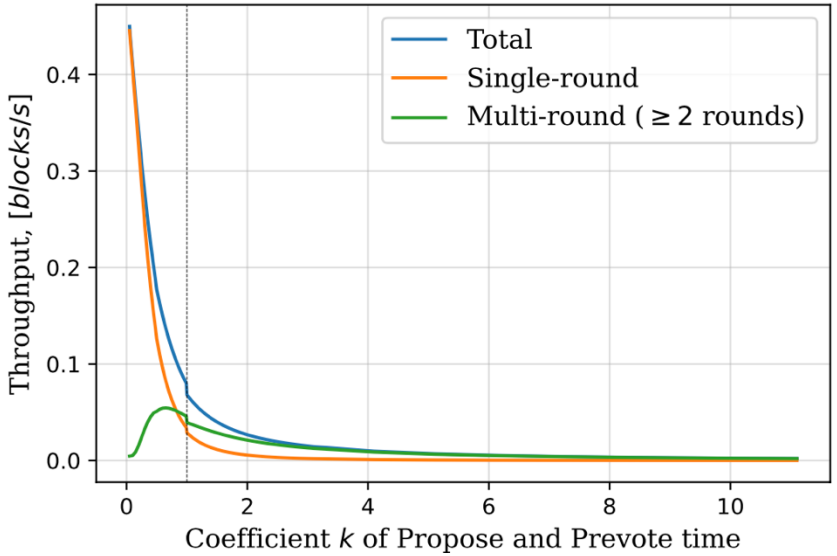
$t_1 = kT_1$ *and* $t_2 = kT_2$

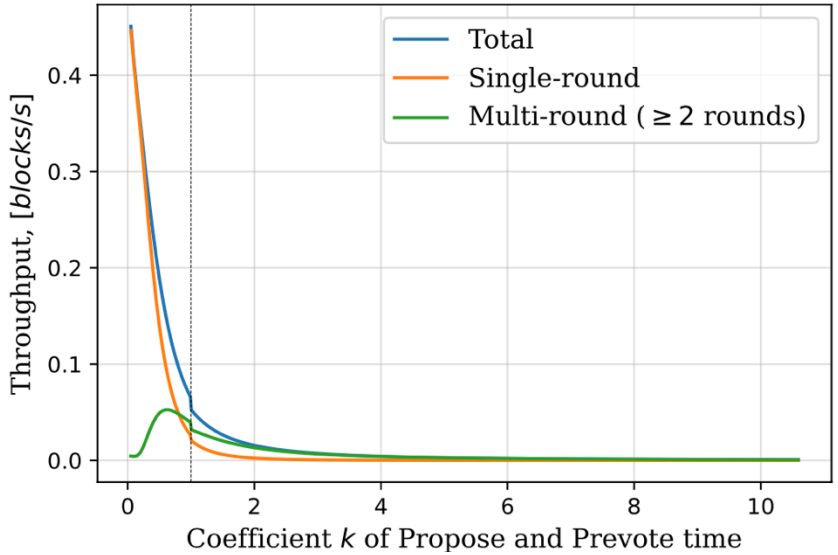
Non-homogeneous



Homogeneous

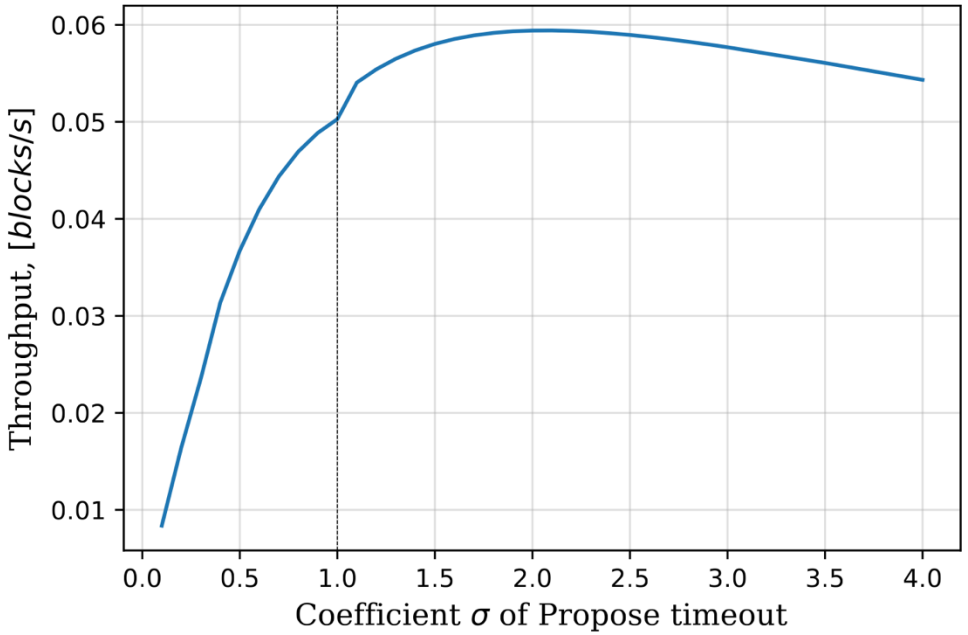




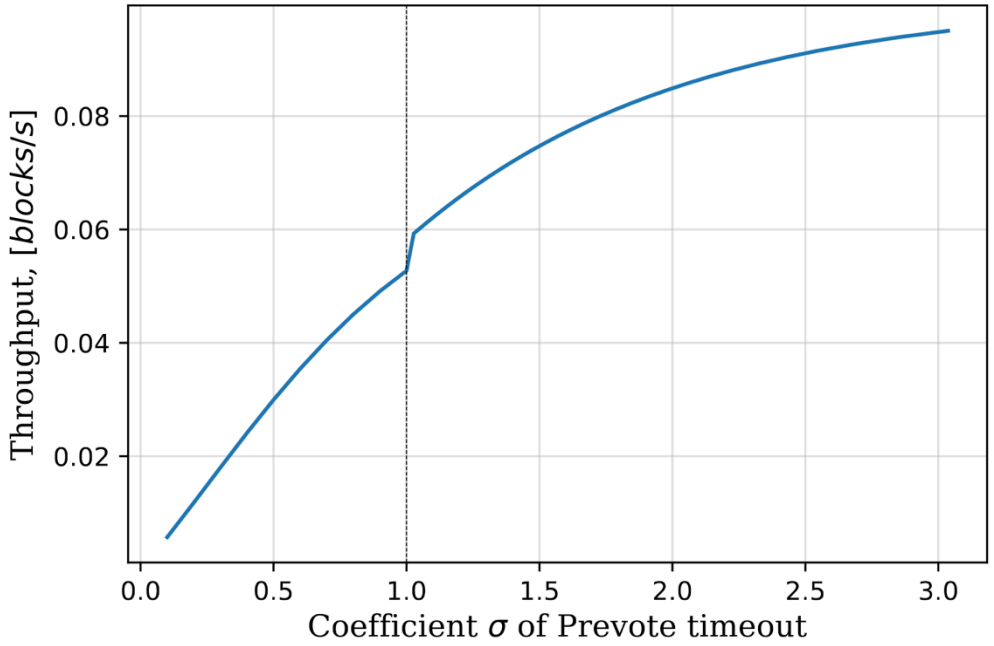


Numerical results: optimal timeout

$$T_1^* = \sigma t_1^* \text{ and } T_2^* = \sigma t_2^* \implies \text{For } Round_1 \quad w_1^* = w_2^* = 1 - e^{-\sigma}$$



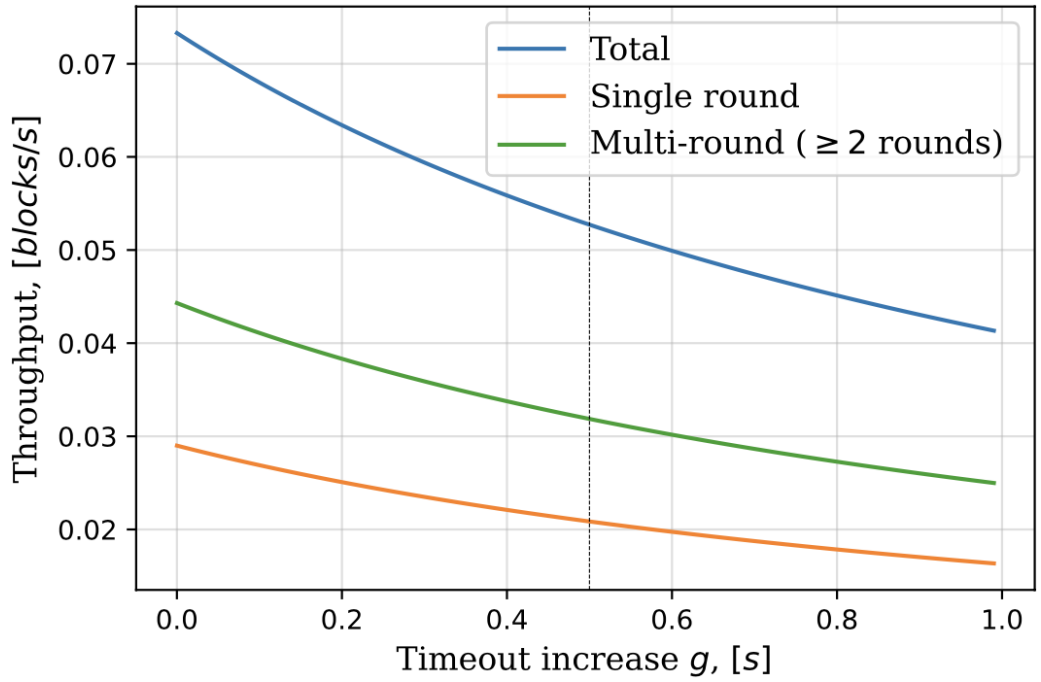
Homogeneous validators



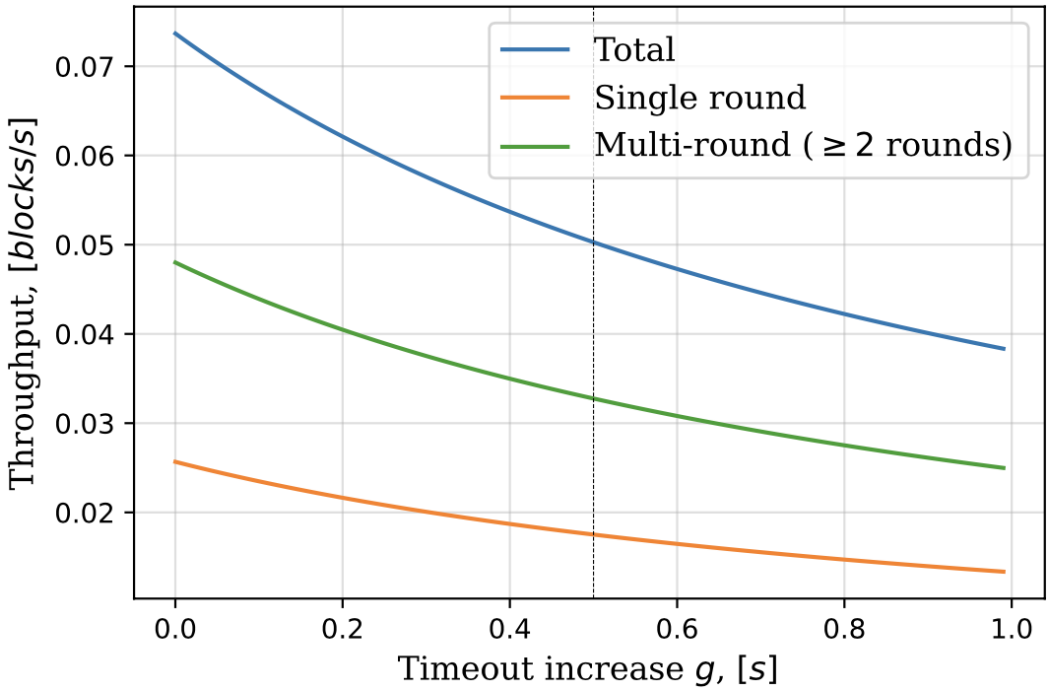
Non-homogeneous validators

Numerical results: timeout increase

$$\gamma_i = max\left(\frac{1}{t_1}, \frac{1}{T_1 + (i-1)g}\right) \quad \text{and} \quad \beta_i = max\left(\frac{1}{t_2}, \frac{1}{T_2 + (i-1)g}\right)$$



Homogeneous validators



Non-homogeneous validators

Model with colluded validators

$$
\begin{array}{rcl}
NewHeight & \stackrel{def}{=} & (nh, n).Round_1 \\
Round_i & \stackrel{def}{=} & (r, d_C n).Propose_{i_C} + (r, d_T n).Propose_{i_T} + (r, d_R n).Propose_{i_R} \\
\hline
Propose_{i_C} & \stackrel{def}{=} & (p, w_{1_i}\gamma_i).Prevote_{i_C} + (p, (1 - w_{1_i})\gamma_i).NilPrevote_i \\
Prevote_{i_C} & \stackrel{def}{=} & (pv, w_{2_i}\beta_i).Precommit_{i_C} + (pv, (1 - w_{2_i})\beta_i).Unsuccess_i \\
Precommit_{i_C} & \stackrel{def}{=} & (pc, w_3\delta_i).Commit_{i_C} + (pc, (1 - w_3)\delta_i).Round_j \\
Commit_{i_C} & \stackrel{def}{=} & (c_C, \eta).NewHeight \\
\hline
Propose_{i_T} & \stackrel{def}{=} & (p, w_{1_i}\gamma_i).Prevote_{i_T} + (p, (1 - w_{1_i})\gamma_i).NilPrevote_i \\
Prevote_{i_T} & \stackrel{def}{=} & (pv, \beta_i).Unsuccess_i \\
\hline
Propose_{i_R} & \stackrel{def}{=} & (p, w_{1_i}\gamma_i).Prevote_{i_R} + (p, (1 - w_{1_i})\gamma_i).NilPrevote_i \\
Prevote_{i_R} & \stackrel{def}{=} & (pv, w_{2_i}\beta_i).Precommit_{i_R} + (pv, (1 - w_{2_i})\beta_i).Unsuccess_i \\
Precommit_{i_R} & \stackrel{def}{=} & (pc, w_3\delta_i).Commit_{i_R} + (pc, (1 - w_3)\delta_i).Round_j \\
Commit_{i_R} & \stackrel{def}{=} & (c, \eta).NewHeight \\
\hline
NilPrevote_i & \stackrel{def}{=} & (npv, \beta_i).Unsuccess_i \\
Unsuccess_i & \stackrel{def}{=} & (pc, \delta_i).Round_j
\end{array}
$$

Colluded

Target

Rest

where $\gamma_i = max\left(\frac{1}{t_1}, \frac{1}{T_1 + (i-1)g}\right)$, $\beta_i = max\left(\frac{1}{t_2}, \frac{1}{T_2 + (i-1)g}\right)$, $\delta_i = \frac{1}{T_3 + (i-1)g}$,

$\eta = \frac{1}{T_4}$, $i \in \{1, \ldots, R\}$, $j = min(i+1, R)$, and $d_C = \frac{1}{3}$, $d_T \in [0, \frac{2}{3}]$, $d_R = 1 - (d_C + d_T)$, with $d_R \geq 0$

Model with absent validators

$$NewHeight \stackrel{def}{=} (nh, n).Round_1$$

$$Round_i \stackrel{def}{=} (r, d_A n).Propose_{i_A} + (r, (1 - d_A)n).Propose_{i_R}$$

Absent

$$Propose_{i_A} \stackrel{def}{=} (p, \boxed{a}w_{1_i}\gamma_i).Prevote_{i_A} + (p, (1 - \boxed{a}w_{1_i})\gamma_i).NilPrevote_i$$

$$Prevote_{i_A} \stackrel{def}{=} (pv, w_{2_i}\beta_i).Precommit_{i_A} + (pv, (1 - w_{2_i})\beta_i).Unsuccess_i$$

$$Precommit_{i_A} \stackrel{def}{=} (pc, w_3\delta_i).Commit_{i_A} + (pc, (1 - w_3)\delta_i).Round_j$$

$$Commit_{i_A} \stackrel{def}{=} (c_A, \eta).NewHeight$$

Rest

$$Propose_{i_R} \stackrel{def}{=} (p, w_{1_i}\gamma_i).Prevote_{i_R} + (p, (1 - w_{1_i})\gamma_i).NilPrevote_i$$

$$Prevote_{i_R} \stackrel{def}{=} (pv, \boxed{a}w_{2_i}\beta_i).Precommit_{i_R} + (pv, (1 - \boxed{a}w_{2_i})\beta_i).Unsuccess_i$$

$$Precommit_{i_R} \stackrel{def}{=} (pc, w_3\delta_i).Commit_{i_R} + (pc, (1 - w_3)\delta_i).Round_j$$

$$Commit_{i_R} \stackrel{def}{=} (c, \eta).NewHeight$$

$$NilPrevote_i \stackrel{def}{=} (npv, \beta_i).Unsuccess_i$$

$$Unsuccess_i \stackrel{def}{=} (pc, \delta_i).Round_j$$

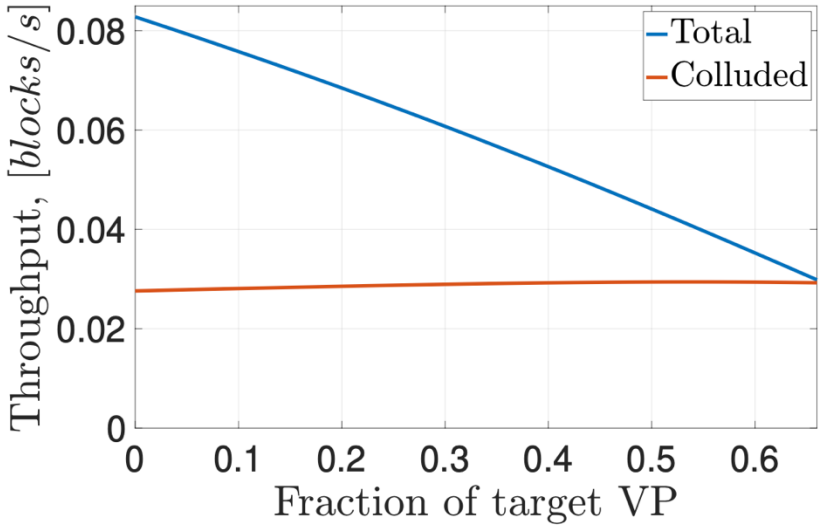
a - presence probability

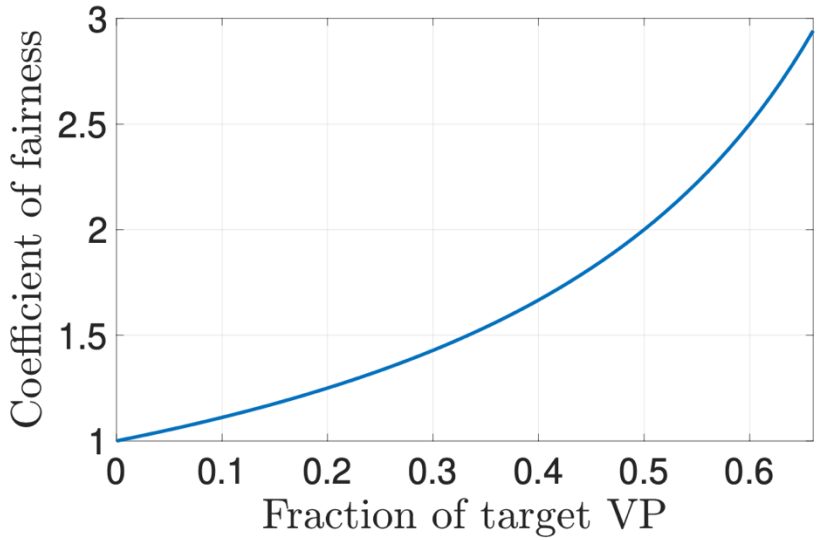
where $\gamma_i = max\left(\frac{1}{t_1}, \frac{1}{T_1 + (i-1)g}\right)$, $\beta_i = max\left(\frac{1}{t_2}, \frac{1}{T_2 + (i-1)g}\right)$, $\delta_i = \frac{1}{T_3 + (i-1)g}$,

$\eta = \frac{1}{T_4}$, and $d_A = \frac{1}{3}$, $a \in [0, 1]$

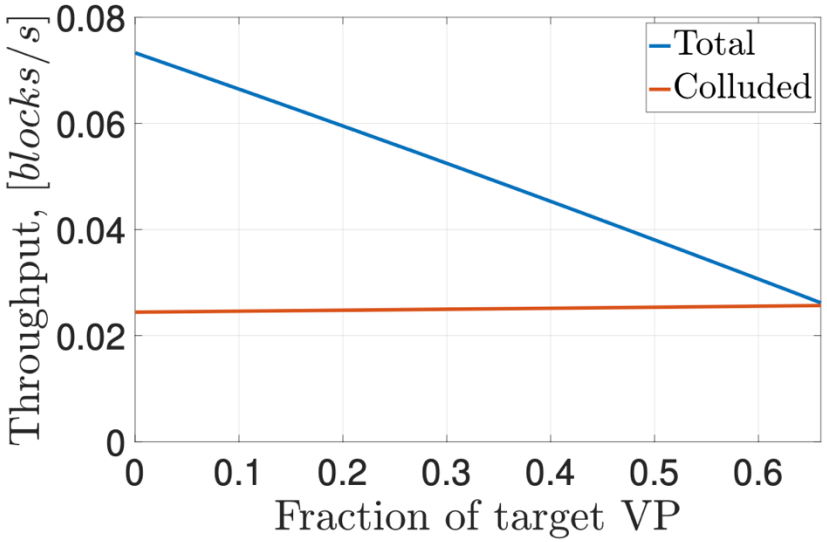
Numerical results: colluded attack

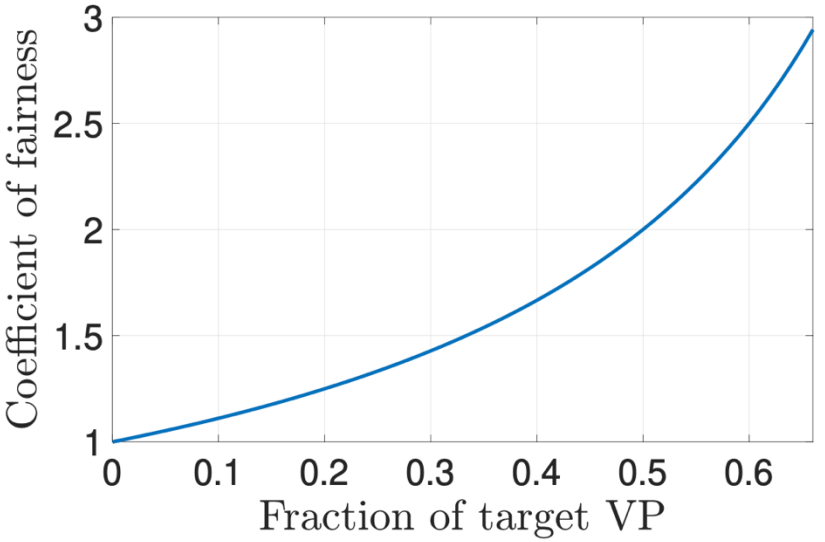
Base





Aggregated





Numerical results: colluded attack

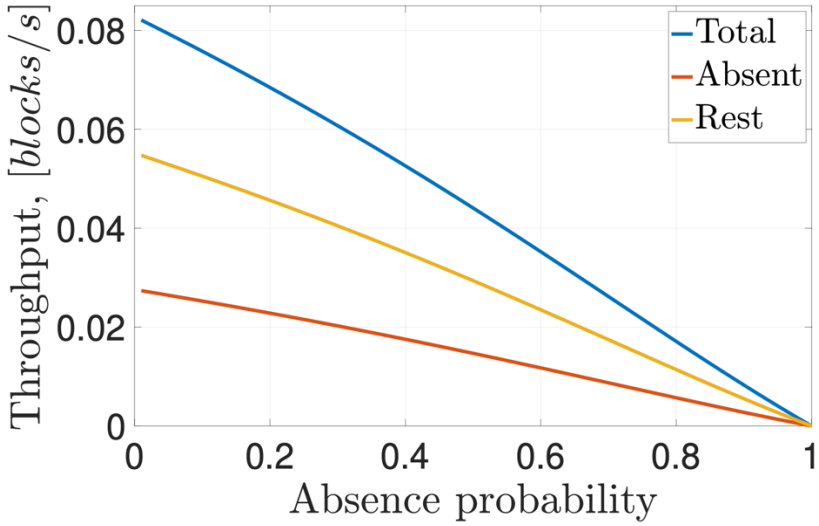
$$\phi_v = \frac{\frac{X_v}{X}}{\frac{VP_v}{VP}}$$

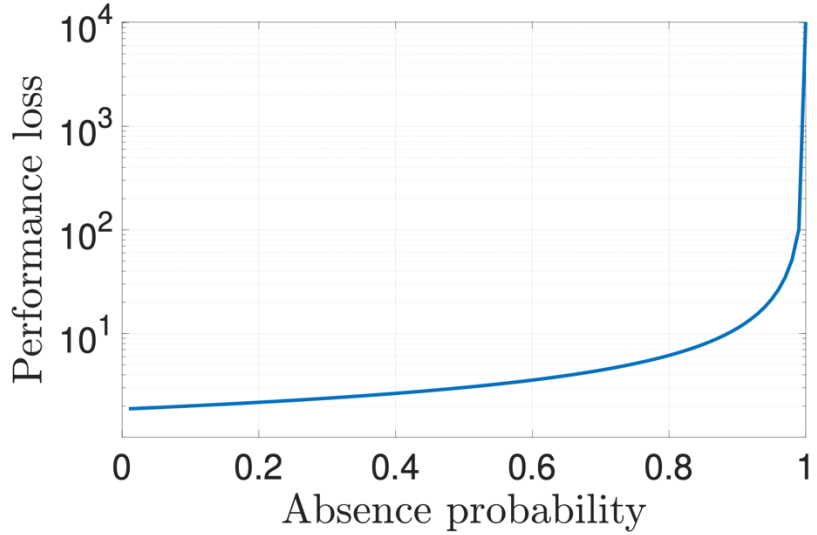
$\frac{X_v}{X}$ - fraction of throughput *produced* by validator(s) v

$\frac{VP_v}{VP}$ - fraction of voting power *possessed* by validator(s) v

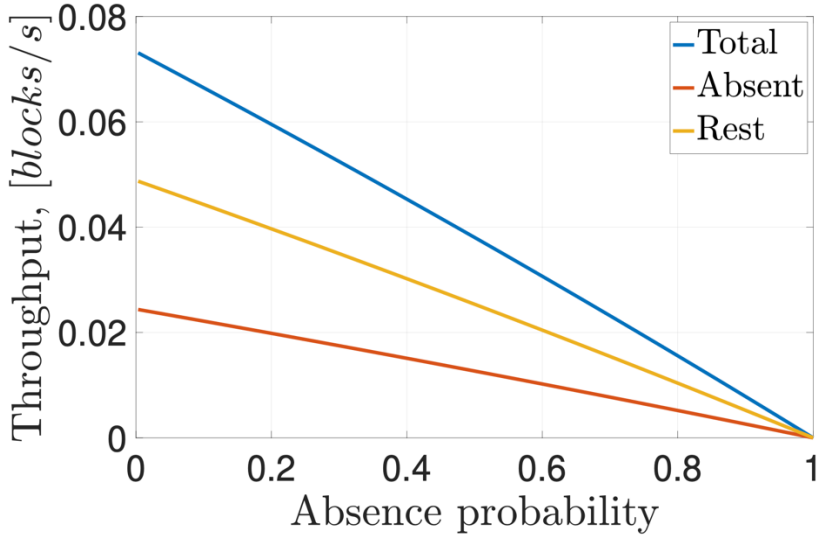
Numerical results: absent superminority

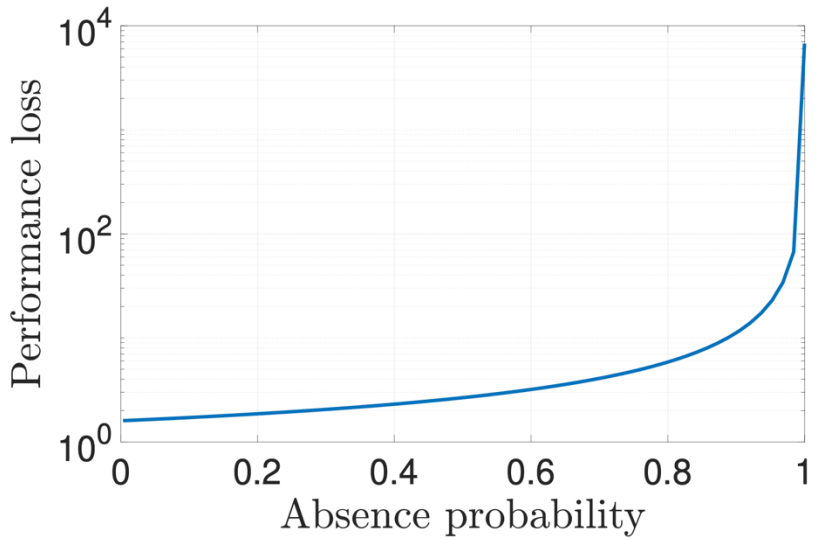
Base





Aggregated





Conclusion

- We assessed the performance of Cosmos blockchain studying:
  - Different verification time of round steps
  - Optimal timeout for better throughput
  - Timeout increase dynamics
  - Performance outcomes on colluded validators
  - Performance outcomes of absent validators
- We disccussed unfairness mitigation approaches


Thank you!