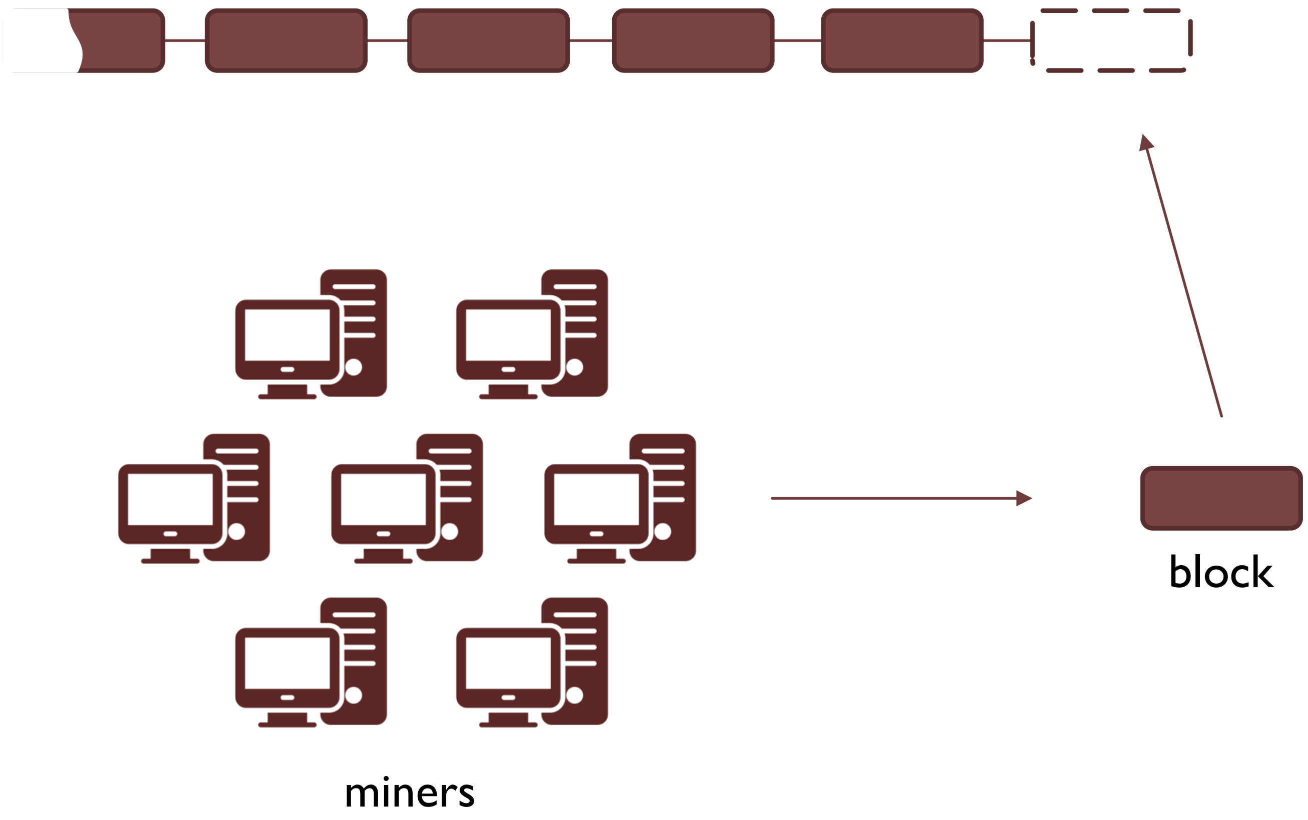
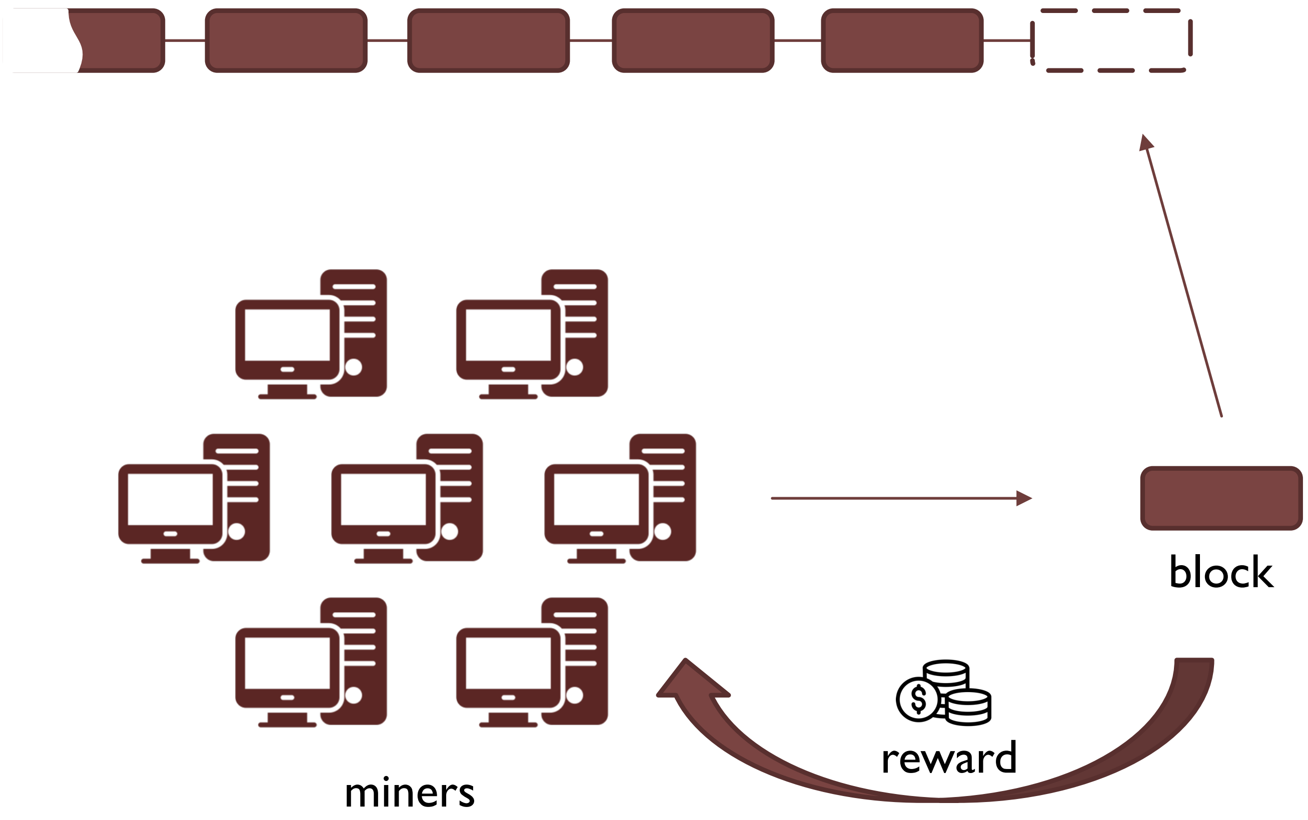
Selfish Mining in Public Blockchains: a Quantitative Analysis

Daria Smuseva

BACKGROUND: PoW Blockchain

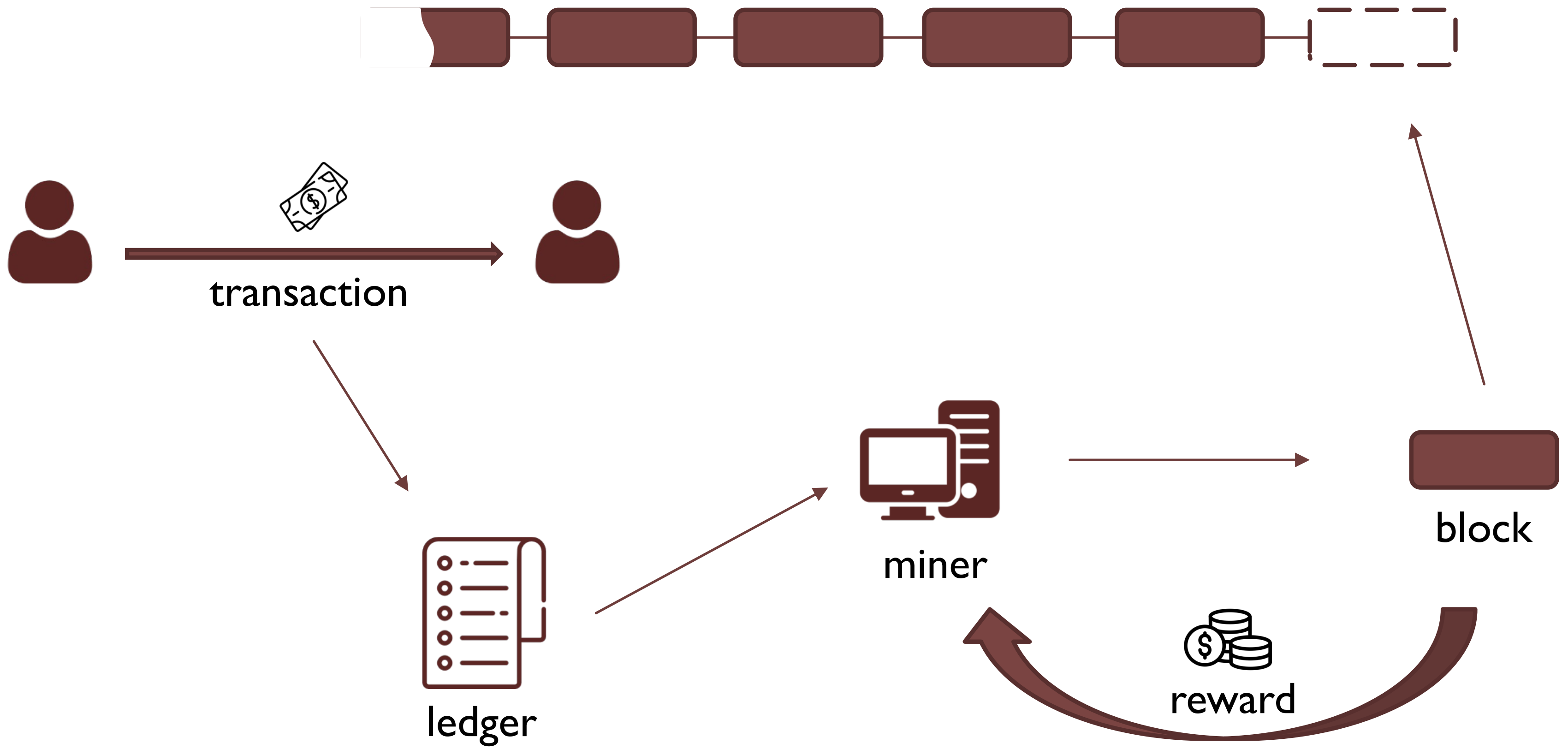


BACKGROUND: PoW Blockchain

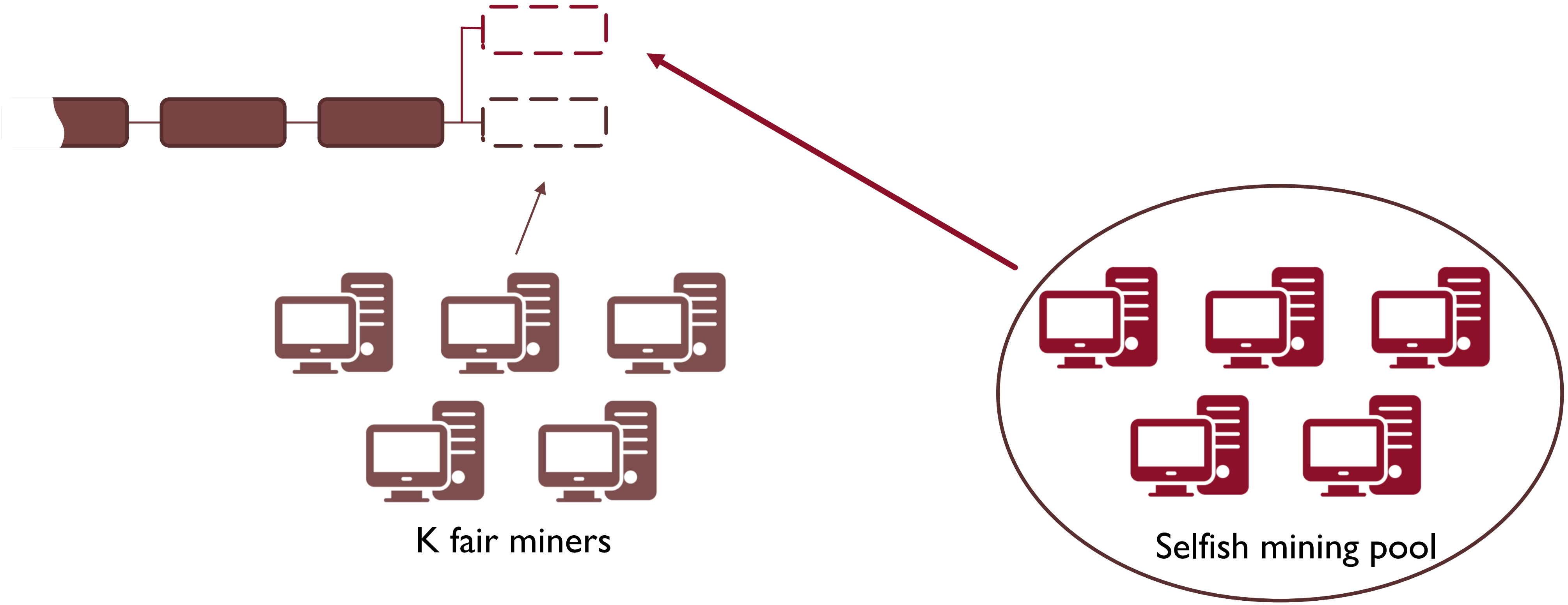


Two types of reward:
- Block reward
- Transactions fees

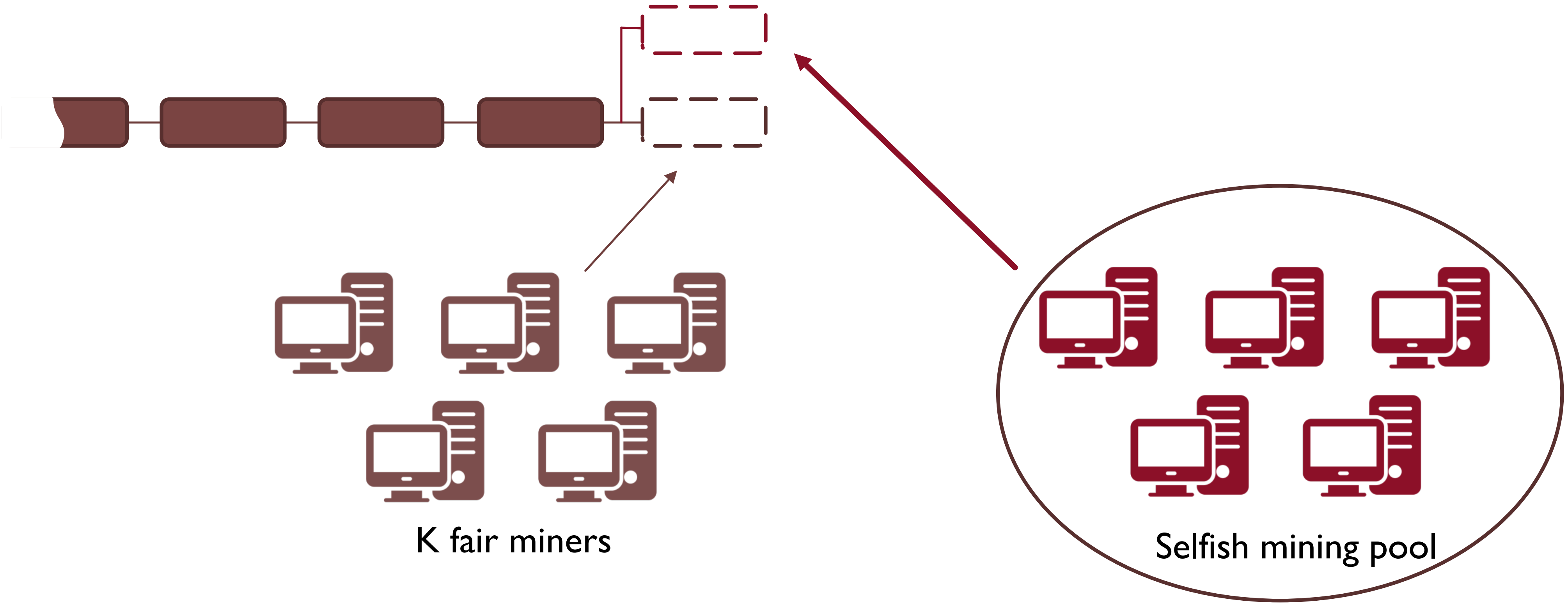
BACKGROUND: PoW Blockchain



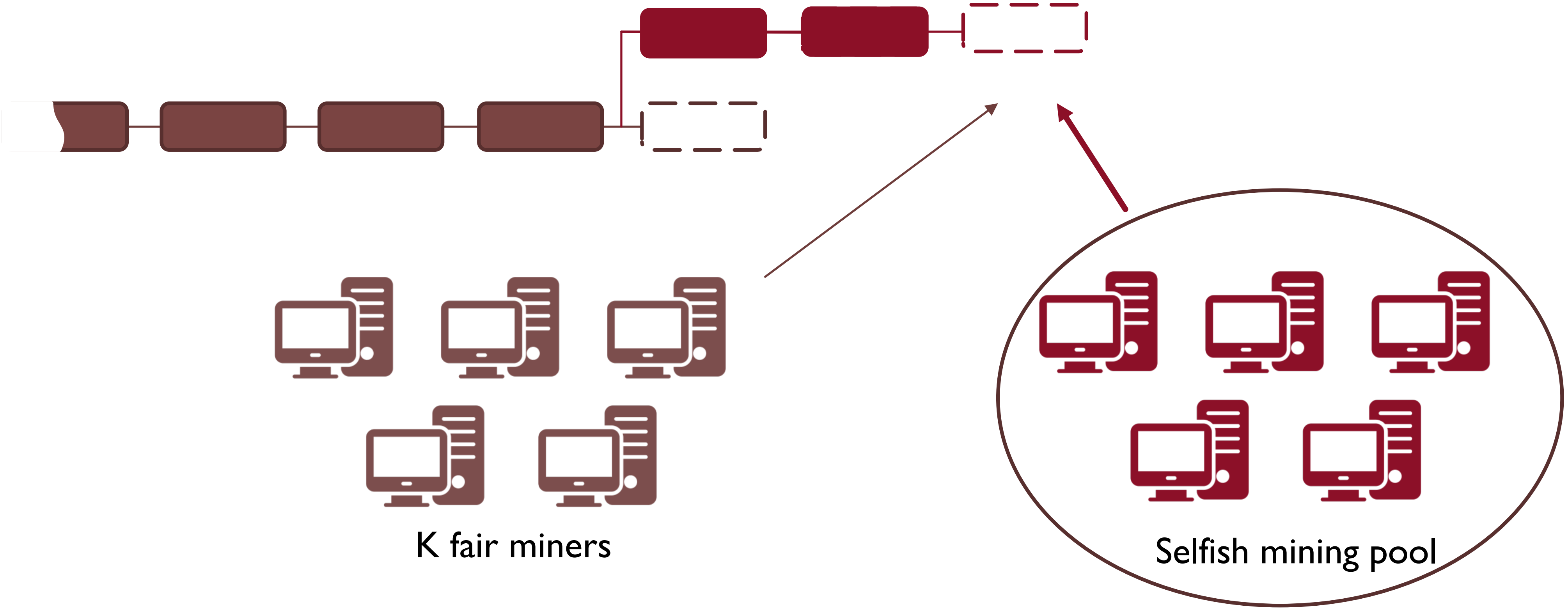
Selfish mining: three scenarios



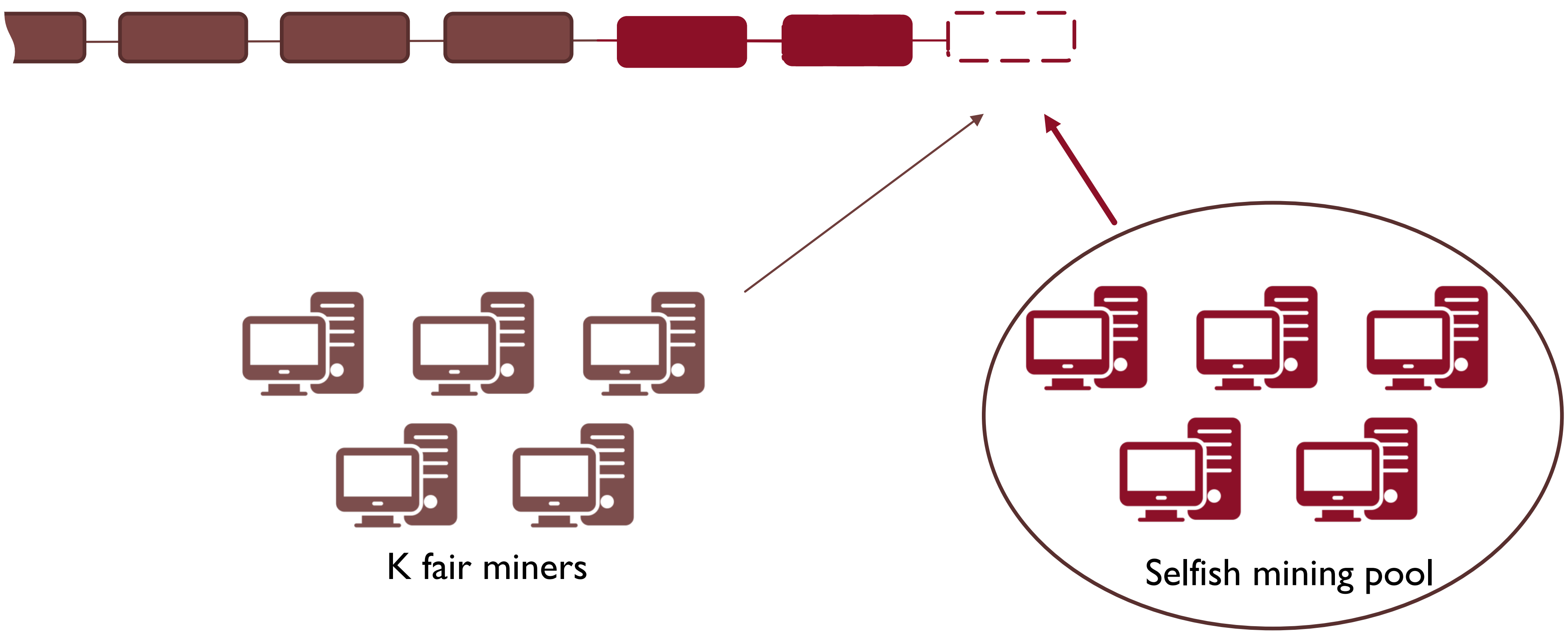
1. One of the fair miners creates a block



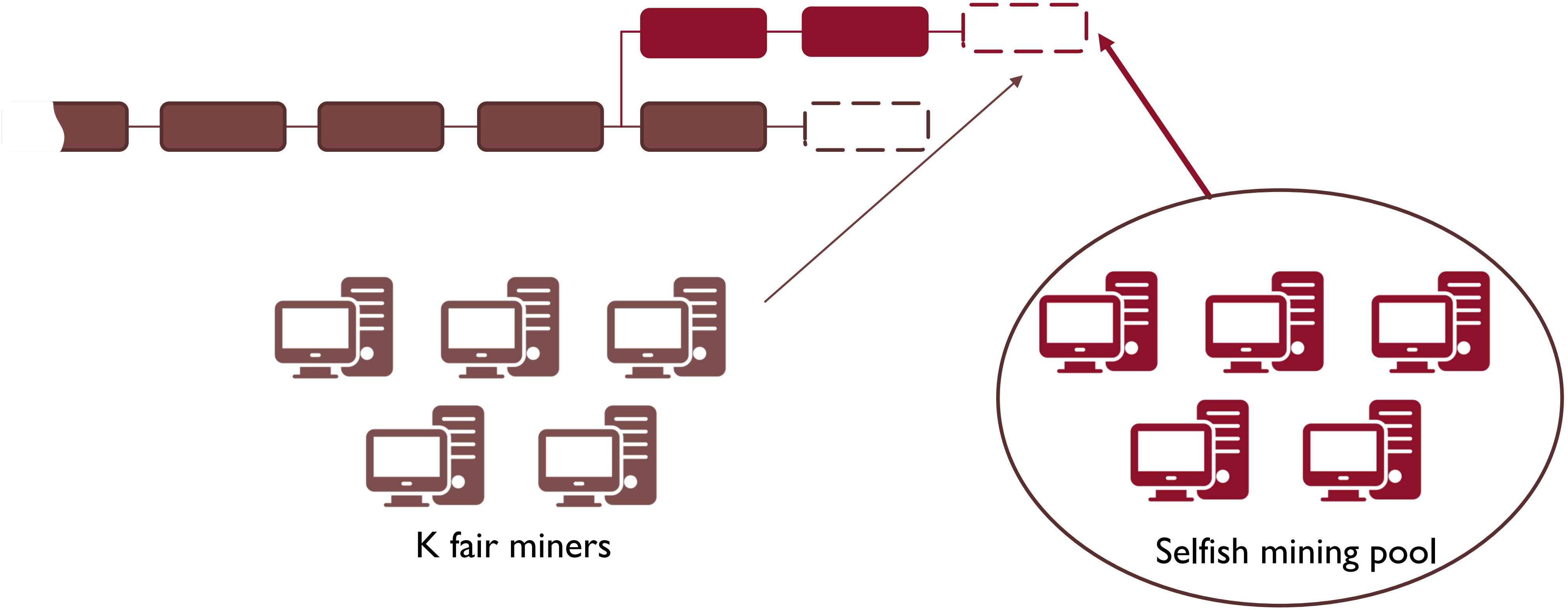
2. The selfish pool creates two blocks



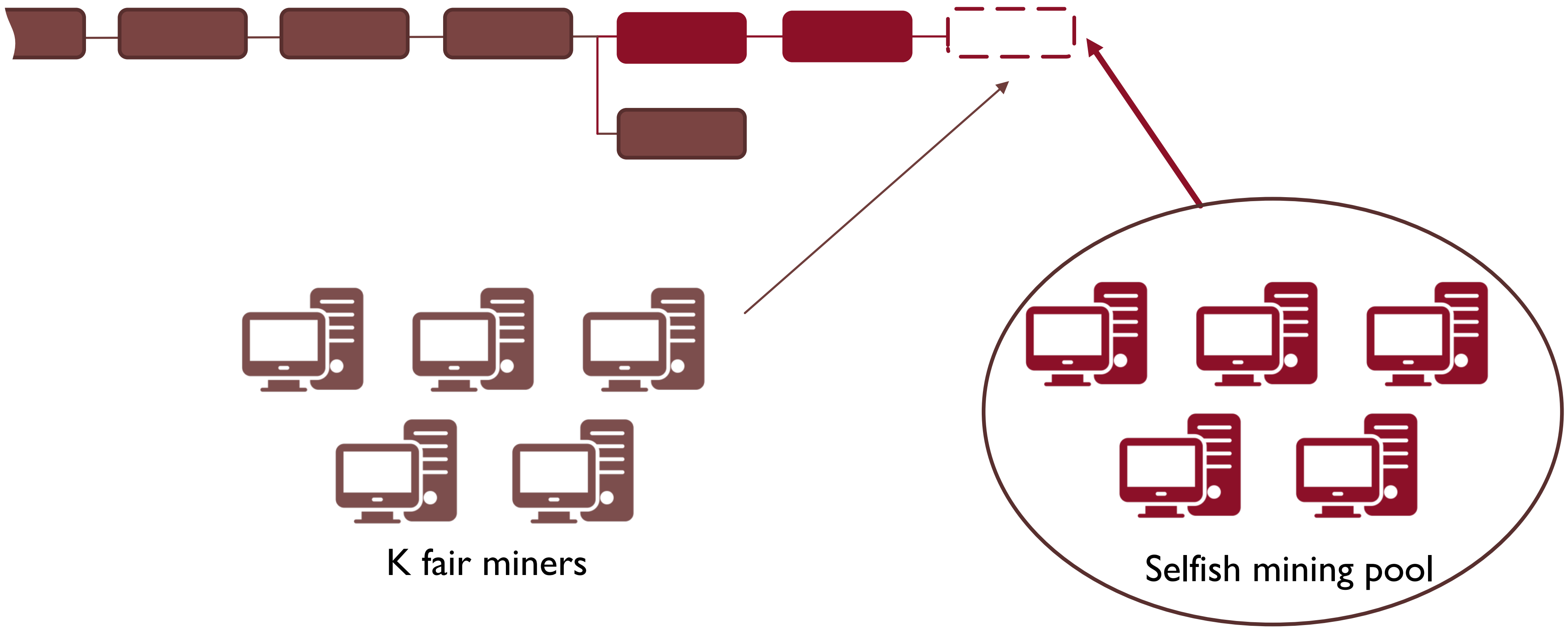
2. The selfish pool creates two blocks



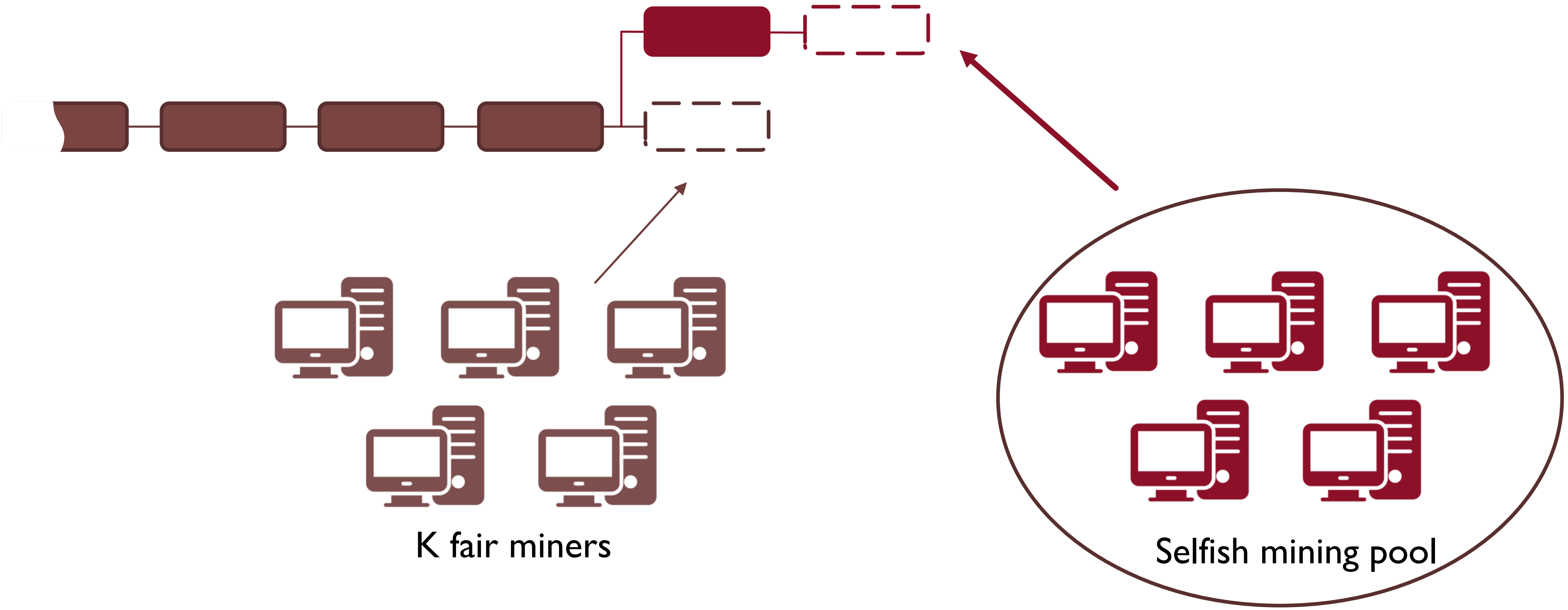
2. The selfish pool creates two blocks



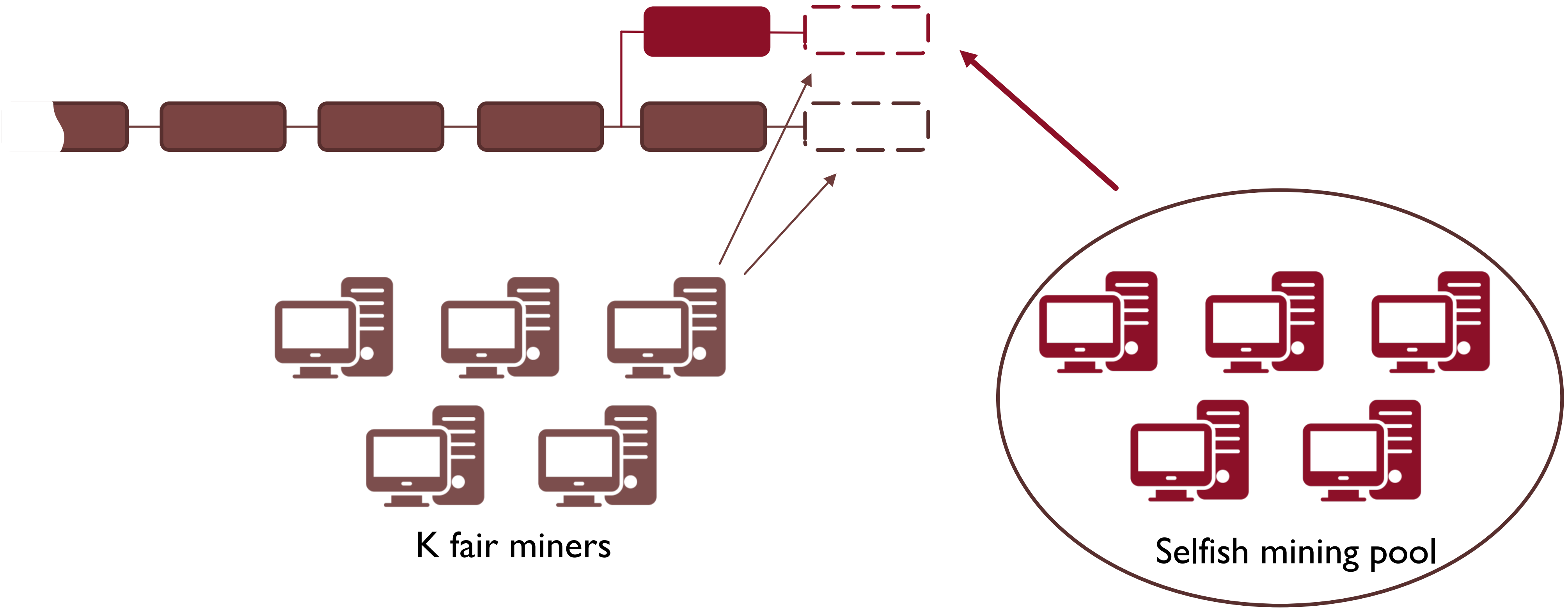
2. The selfish pool creates two blocks



3. A fair miner created a block while the pool has already mined one



3. A fair miner created a block while the pool has already mined one



Performance Evaluation Process Algebra (PEPA)

$$P ::= P \underset{L}{\bowtie} P \;\mid\; P/L \;\mid\; S \qquad\qquad S ::= (\alpha, r).S \;\mid\; S + S \;\mid\; A$$

α - action type

r - rate

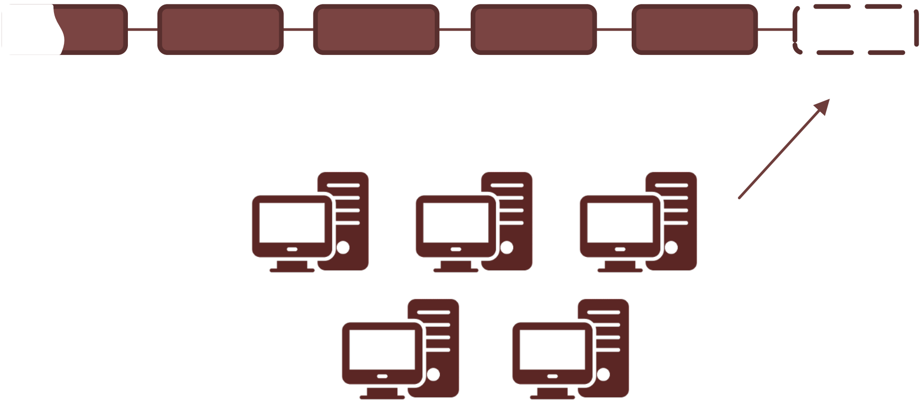
τ - unknown action type

L - cooperation set

Assumptions

- All fair miners have equal computational power;
- All transactions are valid;
- Verification is synchronised;
- We ignore the time it takes to check the hash outcome of the PoW;
- We do not consider block propagation delay between nodes.

PEPA model of a network with K fair miners



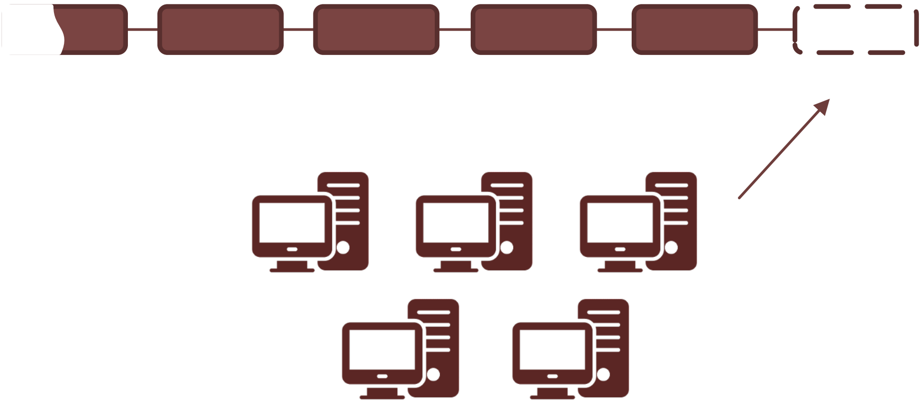
K fair miners

$$
\begin{aligned}
M_i &\overset{def}{=} (m_i, \gamma).M_i + \sum_{j \neq i} (m_j, \top).V_i \\
V_i &\overset{def}{=} \sum_{j \neq i} (v_j, \beta).M_i + \sum_{j \neq i} (m_j, \top).V_i
\end{aligned}
$$

$$
Network \overset{def}{=} (..((M_1 \underset{L \cup L_{12}}{\bowtie} M_2) \underset{L \cup L_3}{\bowtie}) \underset{L \cup L_4}{\bowtie} \dots) \underset{L \cup L_K}{\bowtie} M_K
$$

where $i, j \in \{1, \dots, K\}$ and $L = \{m_1, \dots, m_K\}, L_{12} = \{v_3, \dots, v_K\}$,
$L_j = \{v_1, \dots, v_K\} \setminus \{v_j\}$ for $j \geq 3$

PEPA model of a network with K fair miners



K fair miners

$$
\begin{aligned}
M_i &\overset{def}{=} (m_i, \gamma).M_i + \sum_{j \neq i} (m_j, \top).V_i \\
V_i &\overset{def}{=} \sum_{j \neq i} (v_j, \beta).M_i + \sum_{j \neq i} (m_j, \top).V_i
\end{aligned}
$$

$$
\mathit{Network} \overset{def}{=} (..((M_1 \underset{L \cup L_{12}}{\bowtie} M_2) \underset{L \cup L_3}{\bowtie}) \underset{L \cup L_4}{\bowtie} \dots) \underset{L \cup L_K}{\bowtie} M_K
$$

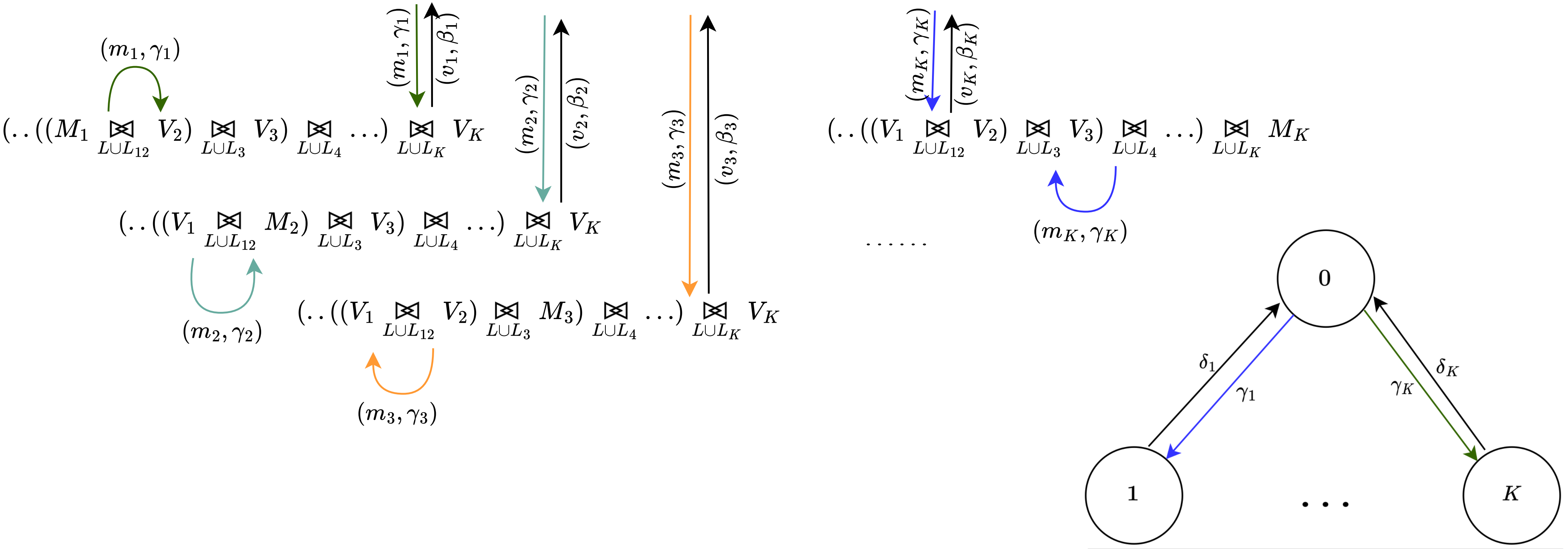
where $i, j \in \{1, \dots, K\}$ and $L = \{m_1, \dots, m_K\}, L_{12} = \{v_3, \dots, v_K\}$,
$L_j = \{v_1, \dots, v_K\} \setminus \{v_j\}$ for $j \geq 3$

Example:

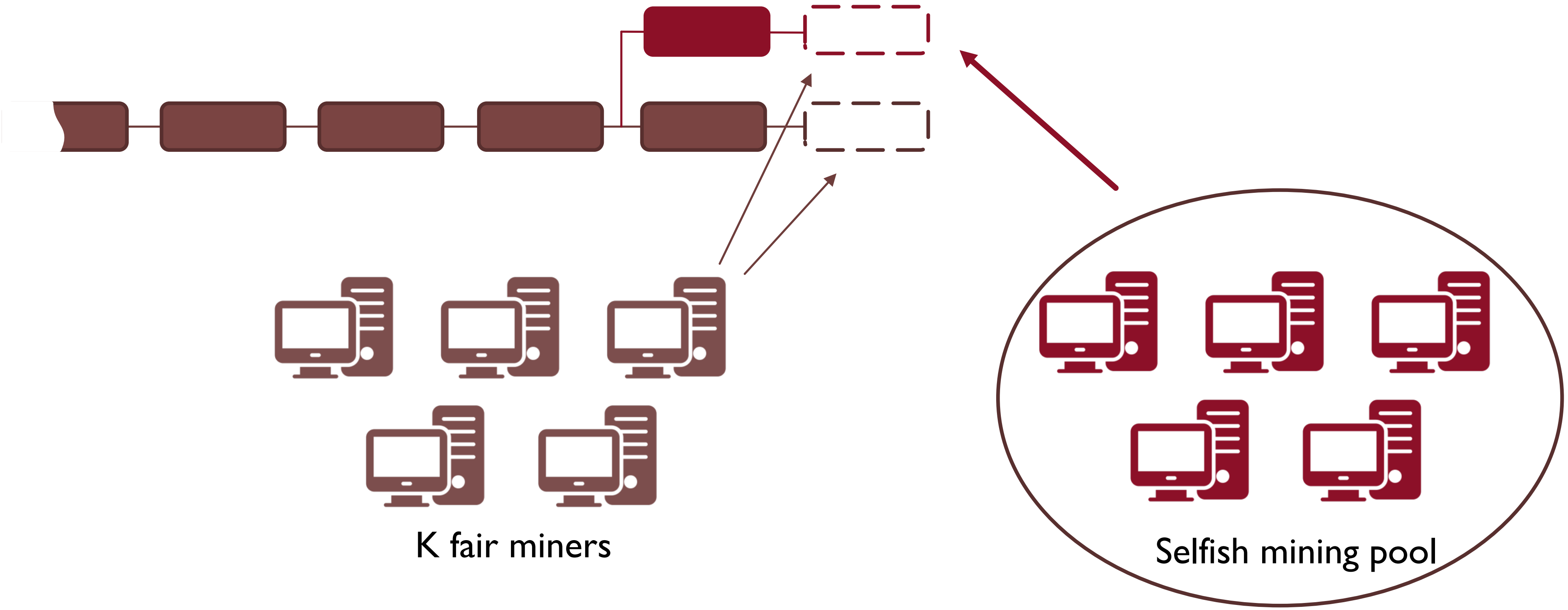
$$
\begin{aligned}
M_1 &\overset{def}{=} (m_1, \gamma).M_1 + (m_2, \top).V_1 + \dots + (m_K, \top).V_1 \\
V_1 &\overset{def}{=} (v_2, \beta).M_1 + \dots + (v_K, \beta).M_1 + (m_2, \top).V_1 + \dots + (m_K, \top).V_1
\end{aligned}
$$

Derivation graph and Markov chain

$$Network \stackrel{def}{=} (\ldots((M_1 \underset{L\cup L_{12}}{\bowtie} M_2) \underset{L\cup L_3}{\bowtie} M_3) \underset{L\cup L_4}{\bowtie} \ldots) \underset{L\cup L_K}{\bowtie} M_K$$



K fair miners and a selfish mining pool



PEPA model of a network with K fair miners and a selfish mining pool M_S

$$
\begin{aligned}
M_{F_i} &\stackrel{def}{=} (m_{F_i}, \gamma).M_{F_i} + \sum_{j \neq i} (m_{F_j}, \top).V_i + \boxed{(m_{S_2}, \top).V_{i_S}} \\
V_i &\stackrel{def}{=} \sum_{j \neq i} (v_j, \beta).M_{F_i} + \sum_{j \neq i} (m_{F_j}, \top).V_i \\
&\boxed{V_{i_S} \stackrel{def}{=} (v_S, \beta).M_{F_i} + (m_{S_2}, \top).V_{i_S}}
\end{aligned}
$$

$$
\boxed{
\begin{aligned}
M_S &\stackrel{def}{=} (m_{S_1}, w\gamma).C + \sum_{i} (m_{F_i}, \top).V_S \\
C &\stackrel{def}{=} (m_{S_2}, w\gamma).M_S + \sum_{i} (m_{F_i}, \top).V_S \\
V_S &\stackrel{def}{=} \sum_{i} (v_i, \beta).M_S + \sum_{j \neq i} (m_{F_j}, \top).V_S
\end{aligned}
}
$$

$$
\mathit{Network} \stackrel{def}{=} \boxed{M_S} \underset{L \cup V}{\bowtie} (..((M_{F_1} \underset{L \cup V_{12}}{\bowtie} M_{F_2}) \underset{L \cup V_3}{\bowtie} M_{F_3}) \ldots) \underset{L \cup V_K}{\bowtie} M_{F_K})
$$

where $i, j \in \{1, \ldots, K\}$ and $L = \{\boxed{m_{S_2}}, m_1, \ldots, m_K\}, V = \{v_1, \ldots, v_K\},$

$V_{12} = \{\boxed{v_S}, v_3, \ldots, v_K\}, V_j = \{\boxed{v_S}, v_1, \ldots, v_K\} \setminus \{v_j\}$ for $j \geq 3$

PEPA model of a network with K fair miners and a selfish mining pool M_S

$$M_{F_i} \stackrel{def}{=} (m_{F_i}, \gamma).M_{F_i} + \sum_{j \neq i} (m_{F_j}, \top).V_i + (m_{S_2}, \top).V_{i_S}$$

$$V_i \stackrel{def}{=} \sum_{j \neq i} (v_j, \beta).M_{F_i} + \sum_{j \neq i} (m_{F_j}, \top).V_i$$

$$V_{i_S} \stackrel{def}{=} (v_S, \beta).M_{F_i} + (m_{S_2}, \top).V_{i_S}$$

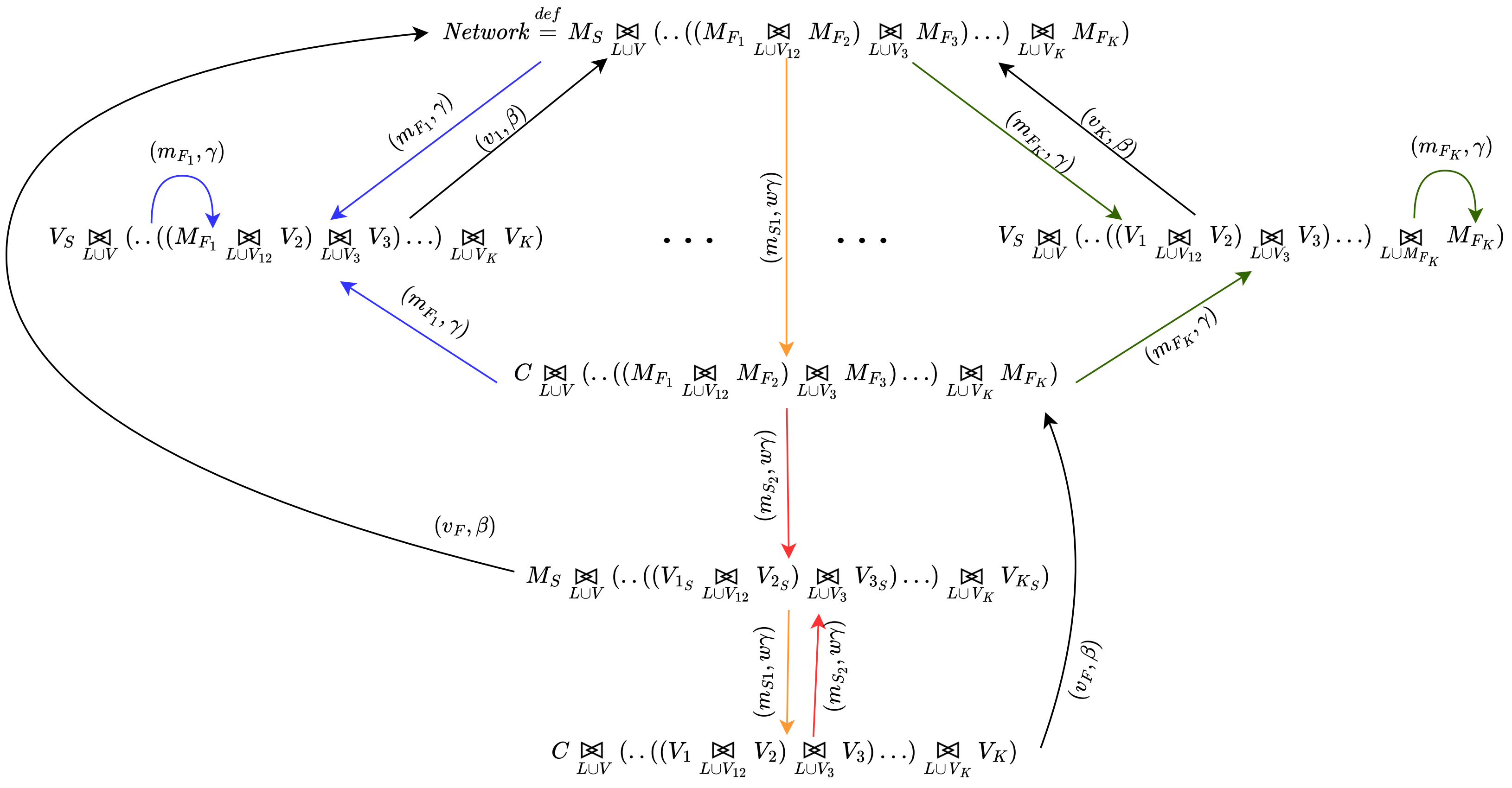
$$M_S \stackrel{def}{=} (m_{S_1}, w\gamma).C + \sum_{i} (m_{F_i}, \top).V_S$$

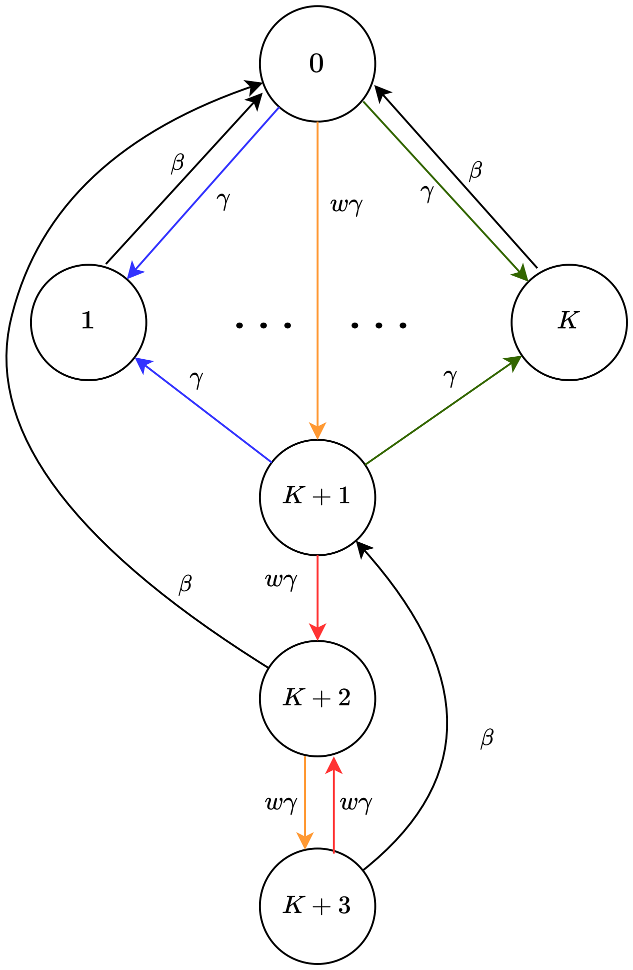
$$C \stackrel{def}{=} (m_{S_2}, w\gamma).M_S + \sum_{i} (m_{F_i}, \top).V_S$$

$$V_S \stackrel{def}{=} \sum_{i} (v_i, \beta).M_S + \sum_{j \neq i} (m_{F_j}, \top).V_S$$

$$Network \stackrel{def}{=} M_S \underset{L \cup V}{\bowtie} (..((M_{F_1} \underset{L \cup V_{12}}{\bowtie} M_{F_2}) \underset{L \cup V_3}{\bowtie} M_{F_3}) \ldots) \underset{L \cup V_K}{\bowtie} M_{F_K})$$

where $i, j \in \{1, \ldots, K\}$ and $L = \{m_{S_2}, m_1, \ldots, m_K\}, V = \{v_1, \ldots, v_K\}$,
$V_{12} = \{v_S, v_3, \ldots, v_K\}, V_j = \{v_S, v_1, \ldots, v_K\} \setminus \{v_j\}$ for $j \geq 3$


$Network \stackrel{def}{=} M_S \underset{L\cup V}{\bowtie} (..((M_{F_1} \underset{L\cup V_{12}}{\bowtie} M_{F_2}) \underset{L\cup V_3}{\bowtie} M_{F_3})\dots) \underset{L\cup V_K}{\bowtie} M_{F_K})$
$V_S \underset{L\cup V}{\bowtie} (..((M_{F_1} \underset{L\cup V_{12}}{\bowtie} V_2) \underset{L\cup V_3}{\bowtie} V_3)\dots) \underset{L\cup V_K}{\bowtie} V_K)$
$\dots$ $\dots$
$V_S \underset{L\cup V}{\bowtie} (..((V_1 \underset{L\cup V_{12}}{\bowtie} V_2) \underset{L\cup V_3}{\bowtie} V_3)\dots) \underset{L\cup M_{F_K}}{\bowtie} M_{F_K})$
$C \underset{L\cup V}{\bowtie} (..((M_{F_1} \underset{L\cup V_{12}}{\bowtie} M_{F_2}) \underset{L\cup V_3}{\bowtie} M_{F_3})\dots) \underset{L\cup V_K}{\bowtie} M_{F_K})$
$M_S \underset{L\cup V}{\bowtie} (..((V_{1_S} \underset{L\cup V_{12}}{\bowtie} V_{2_S}) \underset{L\cup V_3}{\bowtie} V_{3_S})\dots) \underset{L\cup V_K}{\bowtie} V_{K_S})$
$C \underset{L\cup V}{\bowtie} (..((V_1 \underset{L\cup V_{12}}{\bowtie} V_2) \underset{L\cup V_3}{\bowtie} V_3)\dots) \underset{L\cup V_K}{\bowtie} V_K)$
(m_{F_1}, γ)
(v_1, β)
(m_{F_K}, γ)
(v_K, β)
$(m_{S1}, w\gamma)$
$(m_{S_2}, w\gamma)$
(v_F, β)


0
1
K
$K+1$
$K+2$
$K+3$
β
γ
$w\gamma$

Aggregation through lumping all fair miners into an environment

$$
\begin{array}{rcl}
E_F & \stackrel{def}{=} & (m_{E_F}, K\gamma).V_{E_F} + (m_{S2}, \top).V_{E_S} \\
V_{E_F} & \stackrel{def}{=} & (v_{E_F}, \beta).E_F + (m_{E_F}, \gamma).V_{E_F} \\
V_{E_S} & \stackrel{def}{=} & (v_S, \beta).E_F + (m_{S2}, \top).V_{E_S} \\
\hline
M_S & \stackrel{def}{=} & (m_{S1}, w\gamma).C + (m_{E_F}, \top).V_S \\
C & \stackrel{def}{=} & (m_{S2}, w\gamma).M_S + (m_{E_F}, \top).V_S \\
V_S & \stackrel{def}{=} & (v_{E_F}, \beta).M_S + (m_{E_F}, \top).V_S \\
\hline
Lumped\_Network & \stackrel{def}{=} & E_F \underset{L}{\bowtie} M_S \\
\text{where} & & L = \{m_{E_F}, m_{S2}, v_{E_F}\}
\end{array}
$$

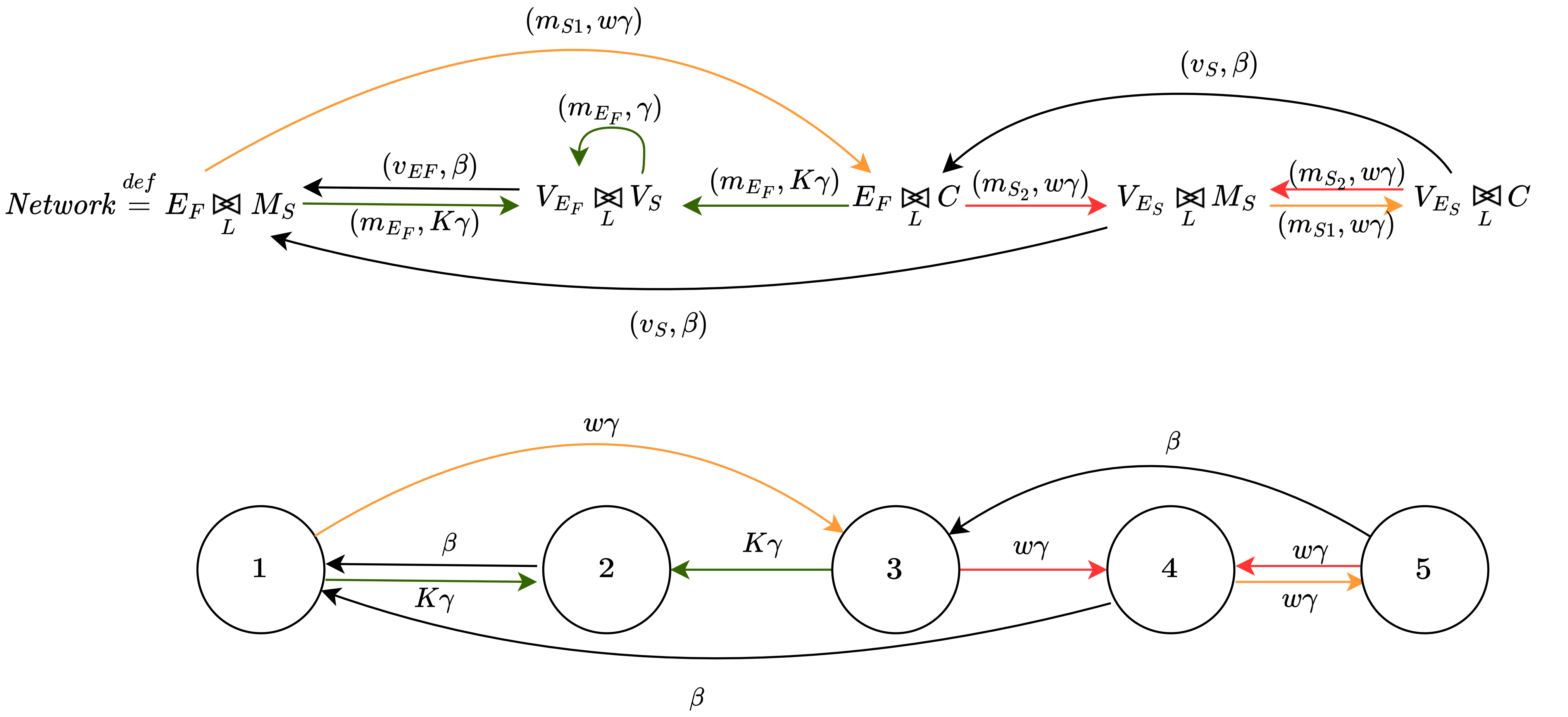
Example

- 100 fair miners
- One selfish pool of 100 miners
- HP of each fair miner is 0.00083 blocks/s
- Block verification time T_v is 3.18 sec

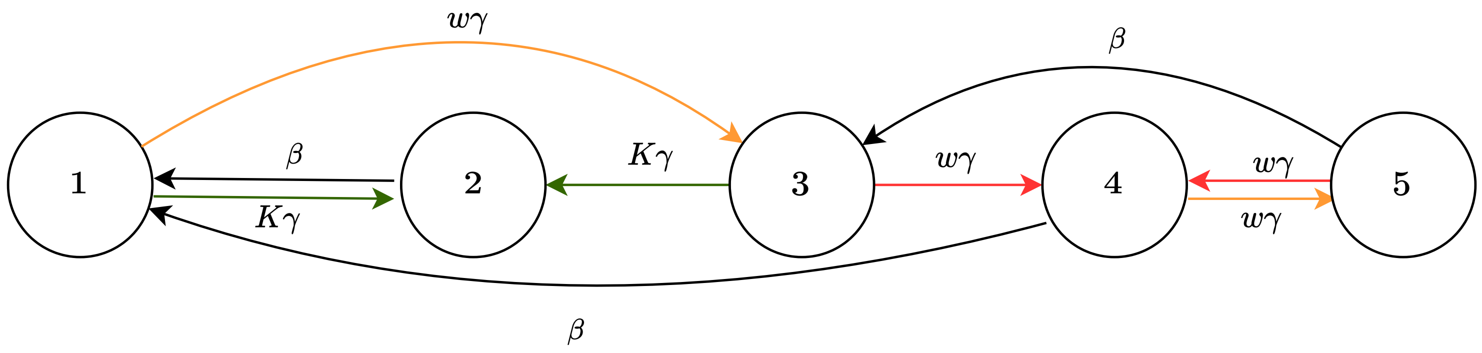
Parameter	Value
K	100 fair miners
γ	8.3×10^{-4} blocks/s
β	$0.314\ \mathrm{s}^{-1}$
w	100

$$
\begin{array}{rcl}
E_F & \stackrel{\mathit{def}}{=} & (m_{E_F}, K\gamma).V_{E_F} + (m_{S2}, \top).V_{E_S} \\
V_{E_F} & \stackrel{\mathit{def}}{=} & (v_{E_F}, \beta).E_F + (m_{E_F}, \gamma).V_{E_F} \\
V_{E_S} & \stackrel{\mathit{def}}{=} & (v_S, \beta).E_F + (m_{S2}, \top).V_{E_S} \\
\hline
M_S & \stackrel{\mathit{def}}{=} & (m_{S1}, w\gamma).C + (m_{E_F}, \top).V_S \\
C & \stackrel{\mathit{def}}{=} & (m_{S2}, w\gamma).M_S + (m_{E_F}, \top).V_S \\
V_S & \stackrel{\mathit{def}}{=} & (v_{E_F}, \beta).M_S + (m_{E_F}, \top).V_S \\
\hline
\mathit{Lumped\_Network} & \stackrel{\mathit{def}}{=} & E_F \underset{L}{\bowtie} M_S \\
\text{where} & & L = \{m_{E_F}, m_{S2}, v_{E_F}\}
\end{array}
$$

Derivation graph and Markov chain of the Lumped Model



Steady state distribution

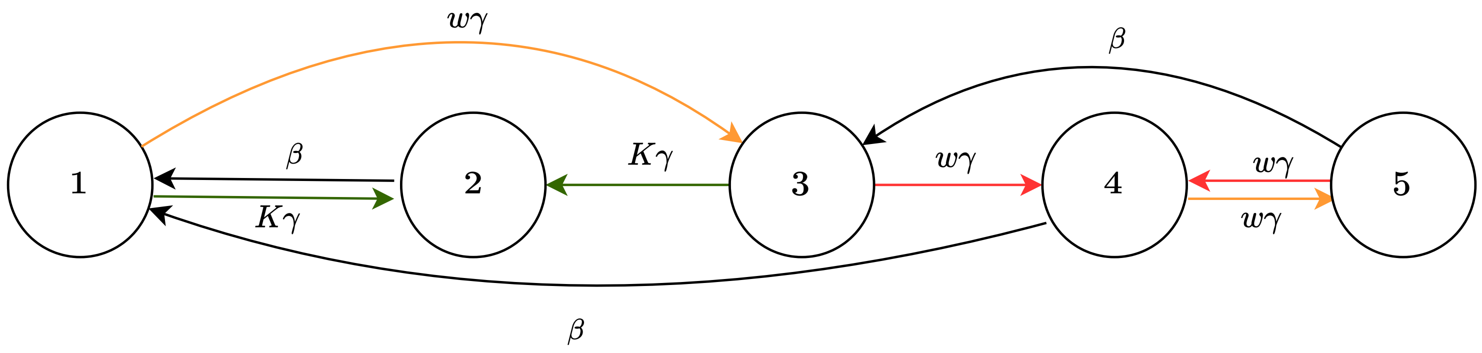


$$\pi_1 = \frac{\beta(\beta(K+w)+\gamma w(2K+w))}{G} \qquad \pi_2 = \frac{\gamma K(\beta(K+2w)+\gamma w(2K+3w))}{G}$$

$$\pi_3 = \frac{\beta w(\beta+2\gamma w)}{G} \qquad \pi_4 = \frac{\gamma w^2(\beta+\gamma w)}{G} \qquad \pi_5 = \frac{\gamma^2 w^3}{G}$$

$$G = \gamma K^2(\beta+2\gamma w) + K(\beta+\gamma w)(\beta+3\gamma w) + 2w(\beta+\gamma w)^2$$

Steady state distribution



$$\pi_1 = \frac{\beta(\beta(K+w)+\gamma w(2K+w))}{G} \qquad \pi_2 = \frac{\gamma K(\beta(K+2w)+\gamma w(2K+3w))}{G}$$

$$\pi_3 = \frac{\beta w(\beta+2\gamma w)}{G} \qquad \pi_4 = \frac{\gamma w^2(\beta+\gamma w)}{G} \qquad \pi_5 = \frac{\gamma^2 w^3}{G}$$

$$G = \gamma K^2(\beta+2\gamma w) + K(\beta+\gamma w)(\beta+3\gamma w) + 2w(\beta+\gamma w)^2$$

$$\pi_1 \approx 0.475964,\ \pi_2 \approx 0.1946725,\ \pi_3 \approx 0.260505,\ \pi_4 \approx 0.0569526,\ \pi_5 \approx 0.011907$$

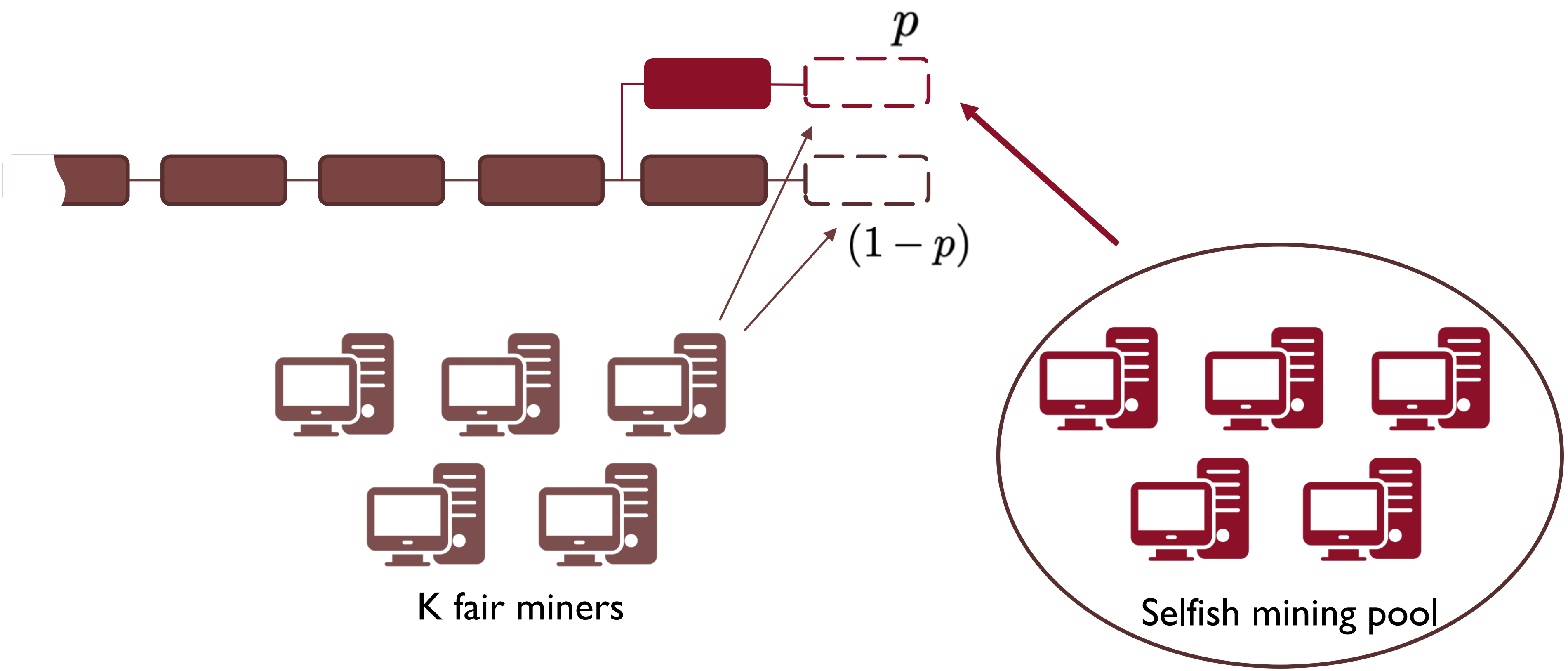
Performance indices

Reward is proportional to **effective throughput***

*effective throughput $\ll$ invested HP

Performance indices

$X_p = p(X_{m_{S1}} - X_{m_{S2}})$ - the throughput of the pool being able to impose the first block without producing the second



Performance indices

$X_p = p(X_{m_{S1}} - X_{m_{S2}})$ - the throughput of the pool being able to impose the first block without producing the second

$$X_S = 2X_{m_{S2}} + X_p = (2-p)X_{m_{S2}} + pX_{m_{S1}}$$

$$X_S^N = \frac{X_S}{w} = \frac{(2-p)X_{m_{S2}} + pX_{m_{S1}}}{w}$$

$$X_{EF} = X_{m_{EF}} - X_{m_{S2}} - X_p = X_{m_{EF}} - (1-p)X_{m_{S2}} - pX_{m_{S1}}$$

$$X_F = \frac{X_{EF}}{K} = \frac{X_{m_{EF}} - (1-p)X_{m_{S2}} - pX_{m_{S1}}}{K}$$

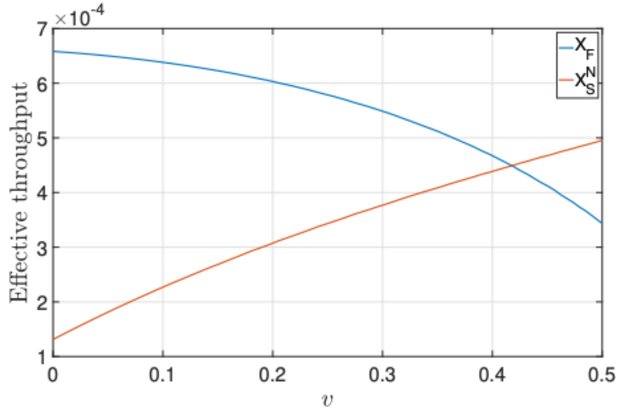
$$R = \frac{X_S}{X_S + X_{EF}}$$

The convenience of selfish behaviour

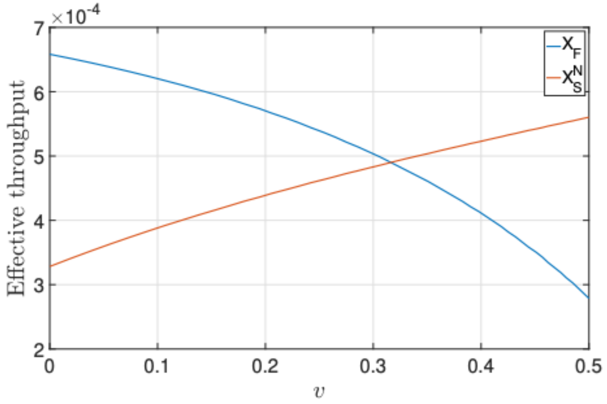
$$v = w/(w + K) \qquad\qquad v < 0.5$$

v - fraction of hash power controlled by the selfish pool

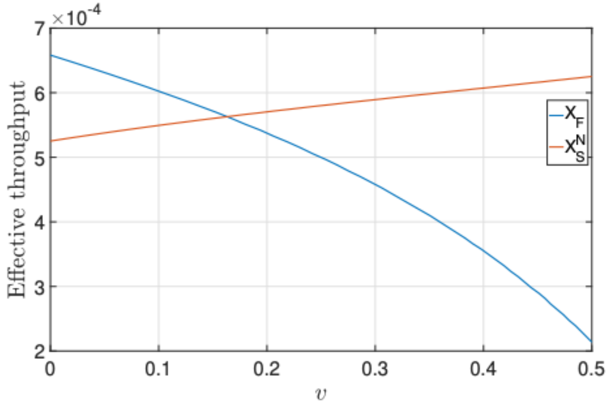
$p = 0.2$



$p = 0.5$



$p = 0.8$

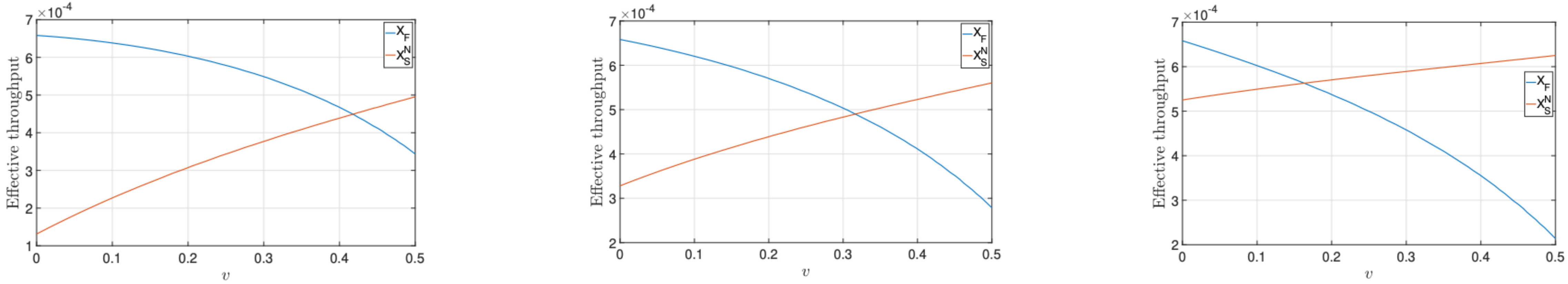


Normalized profit of honest and selfish miners

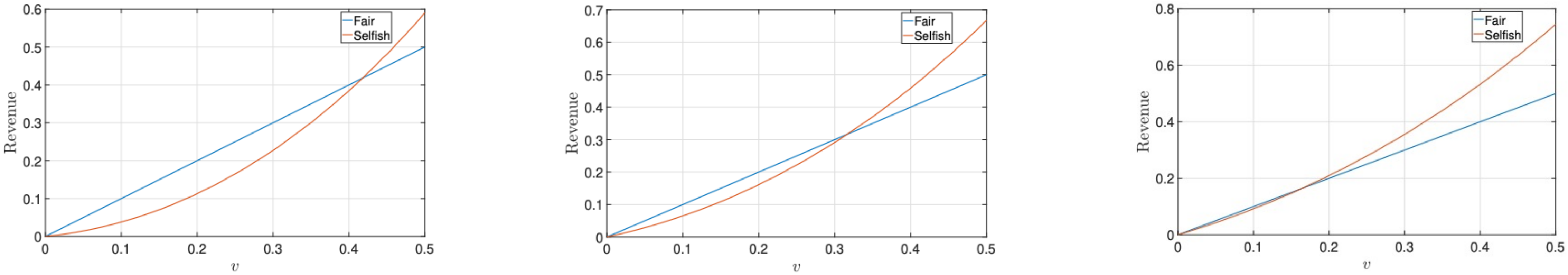
$$X_F = \frac{X_{EF}}{K} = \frac{X_{m_{EF}} - (1-p)X_{m_{S2}} - pX_{m_{S1}}}{K}$$

$$X_S^N = \frac{X_S}{w} = \frac{(2-p)X_{m_{S2}} + pX_{m_{S1}}}{w}$$

$p = 0.2$ $p = 0.5$ $p = 0.8$



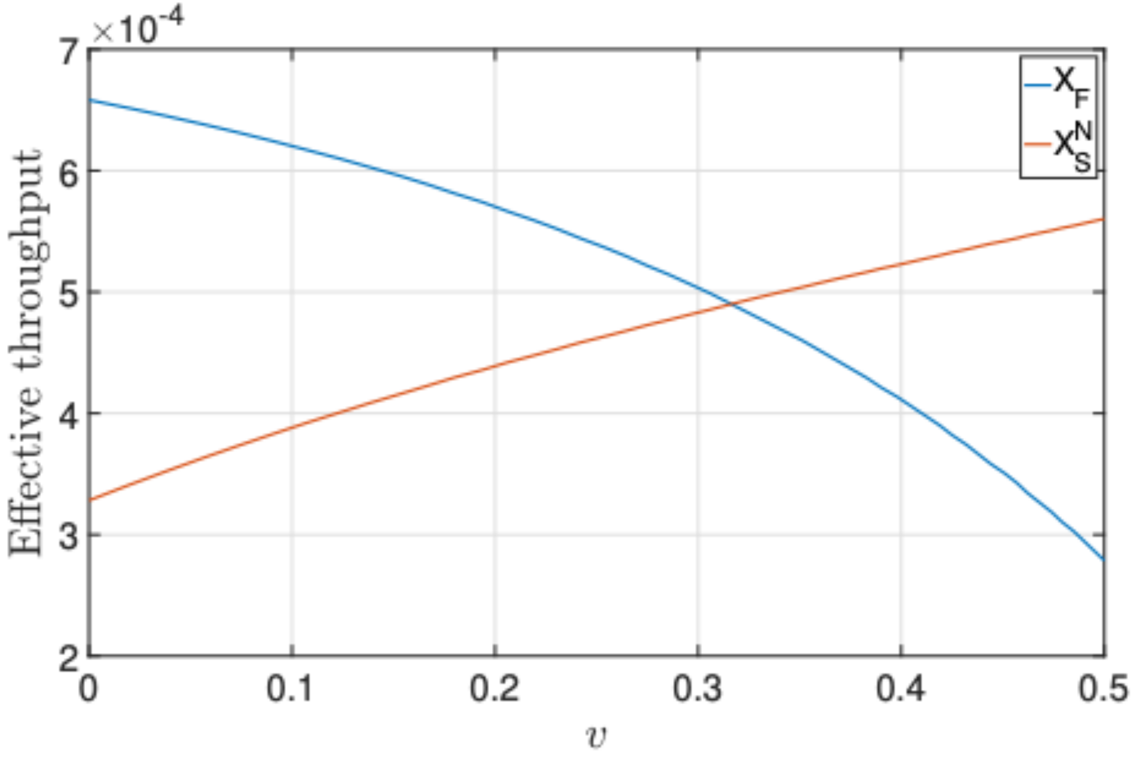
Normalized profit of honest and selfish miners



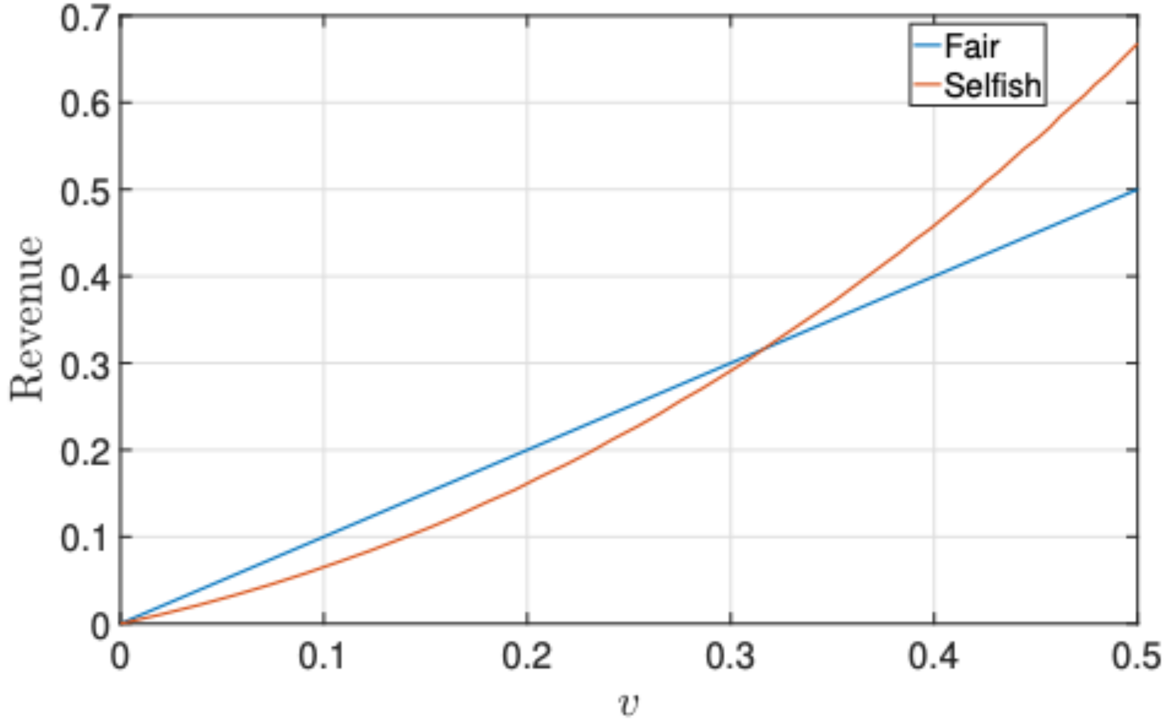
Revenue of selfish miners with respect to a totally fair network $R = \dfrac{X_S}{X_S + X_{EF}}$

$p = 0.5$

Normalized profit of honest and selfish miners



Revenue of selfish miners with respect to a totally fair network



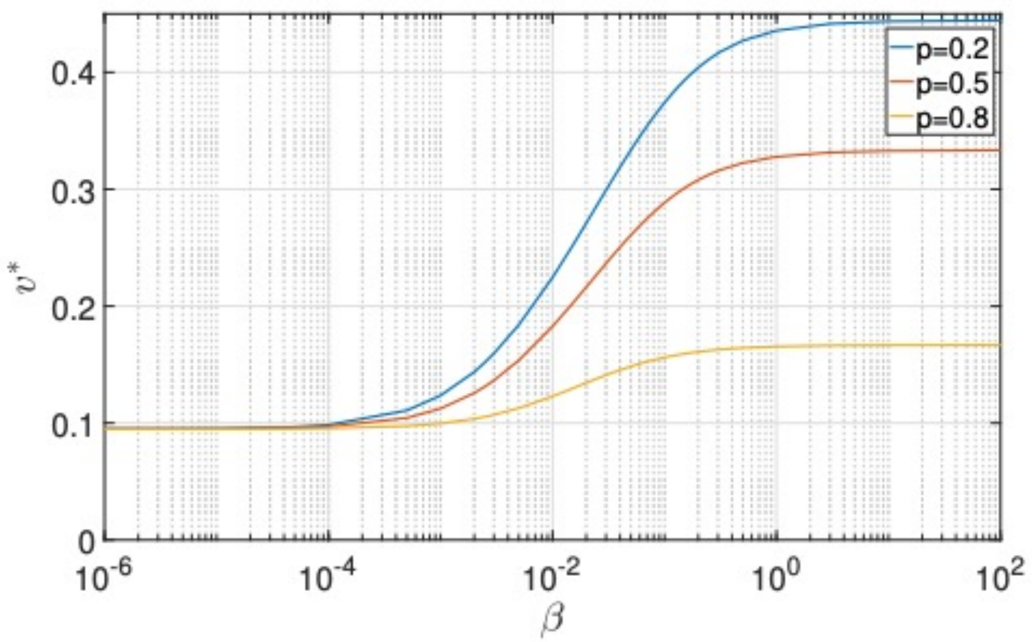
The impact of the verification time on the minimum fraction of selfish miners at which they have an advantage over the fair miners

$$v^* = w^*/(w^* + K)$$

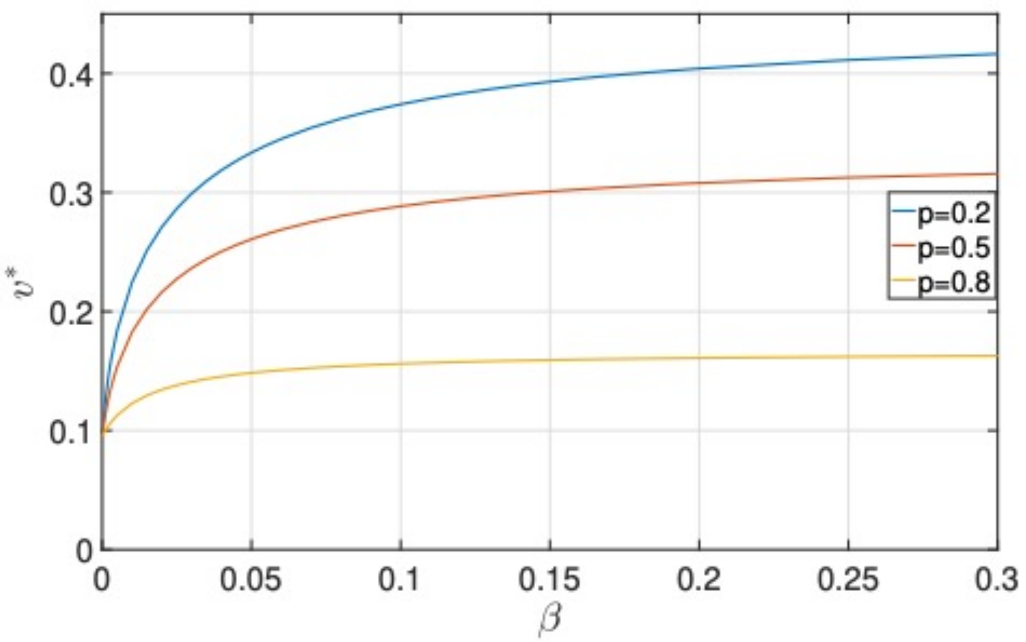
v^* - the **minimum** fraction of hash power that must be controlled by the selfish pool to take advantage by the attack

w^* - the **minimum** positive solution w of the equatior $X_F = X_S^N$

The impact of the verification time on the minimum fraction of selfish miners at which they have an advantage over the fair miners

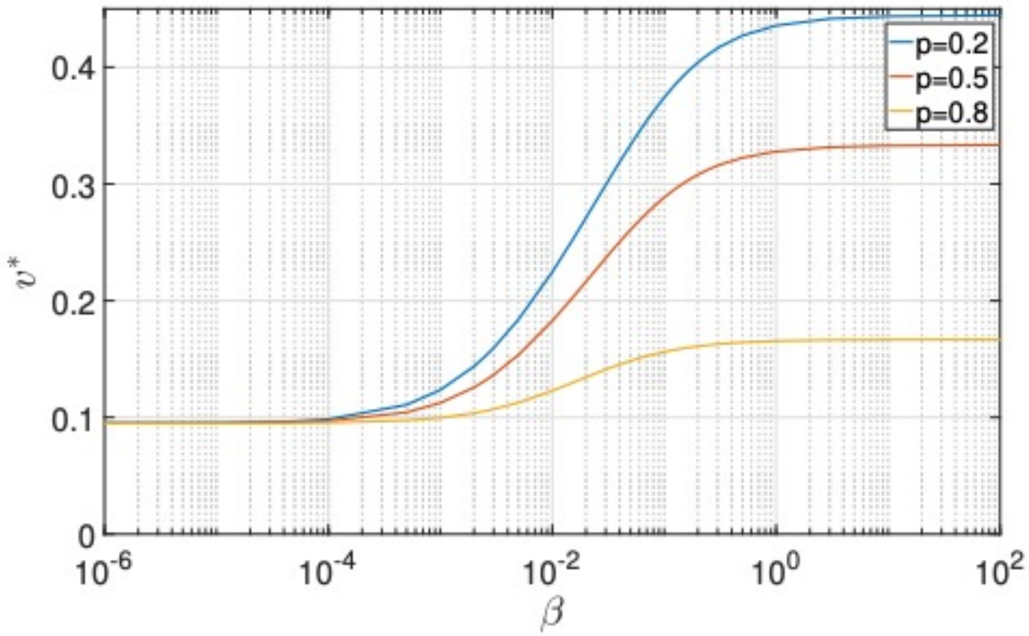


Semi-logarithmic scale



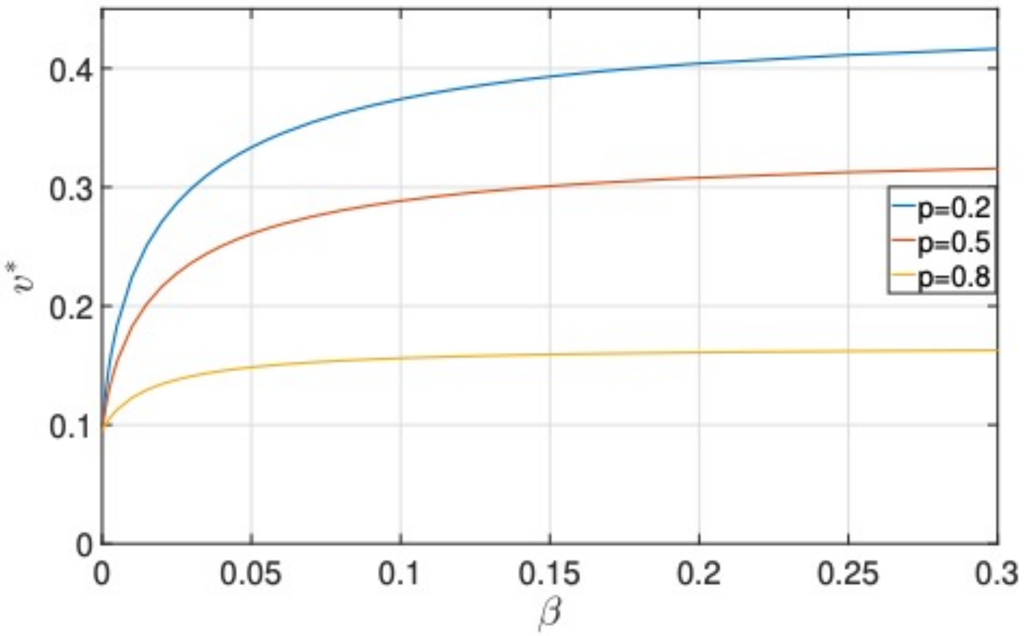
Linear scale with β ∈ [0, 0.3]

The impact of the verification time on the minimum fraction of selfish miners at which they have an advantage over the fair miners



10^6 sec 10^{-2} sec

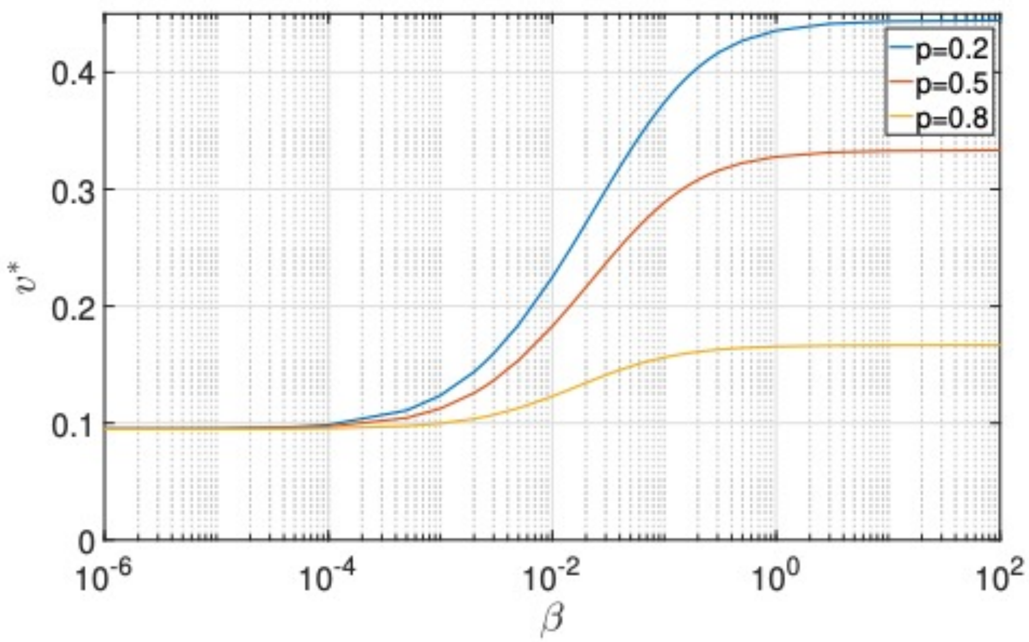
Semi-logarithmic scale



3.33 sec

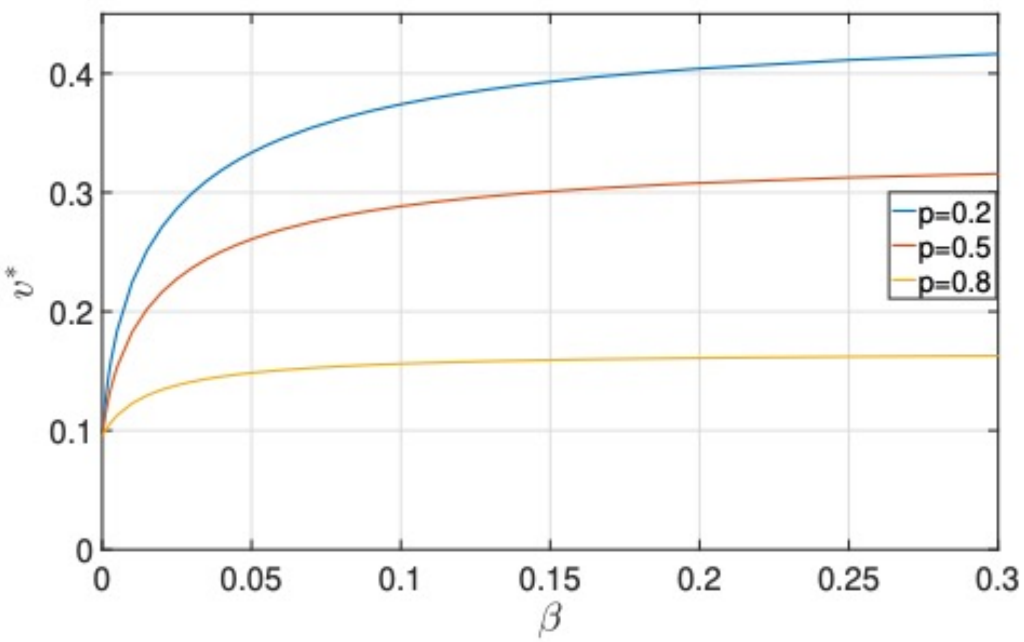
Linear scale with β ∈ [0, 0.3]

The impact of the verification time on the minimum fraction of selfish miners at which they have an advantage over the fair miners



10^6 sec 10^{-2} sec

Semi-logarithmic scale



3.33 sec

Linear scale with $\beta \in [0, 0.3]$

Slower verification times drastically reduce the demand of hash power for the greedy miners

Conclusion

- Our study provides a quantitative analysis of the selfish miner attack in blockchain systems based on a stochastic model expressed with PEPA
- We have derived the conditions under which the attack becomes convenient for selfish miners
- We have shown that the verification time of the transactions affects the rationality of the attacker
- This work contributes to the understanding of the selfish miner attack and can help in the development of more robust and efficient blockchain systems
- Further research can explore the extension of our model to consider more complex scenarios and the application of our findings in real-world blockchain systems.

Thank you!