Supplementary Materials for Modeling and Evaluation of the Block Proposing Mechanism in Ethereum 2.0-based Blockchains

Shuhan Qi, Qinglin Zhao, *Senior Member, IEEE*, Zijie Liu, MengChu Zhou, *Fellow, IEEE*, Meng Shen, *Member, IEEE*, Peiyun Zhang, *Senior Member*, and Yi Sun

Proof of Lemma 1: Consider a Δ-synchronous network where Δ≤ 2δ<2Δ. Note that Proposer i broadcasts a block B_i at the beginning of slot i. We now prove Lemma 1(a)-(c):

a) Since δ<Δ≤ 2δ, a newly generated block will surely be received within 2 slots, but not necessarily received in one slot. Therefore, in slot i, proposer i surely receives B_{i-2} and all blocks preceding it but may not receive B_{i-1}. This confirms Lemma 1(a).

b) When proposer i-1 proposes B_{i-1} in slot i-1. There are two cases:

   i) B_{i-2} is on the canonical chain, indicating that B_{i-2} is the B_{ch} in slot i-1.
   - If proposer i-1 did not receive B_{i-2} in slot i-1, it missed B_{ch}, placing B_{i-1} off the canonical chain.
   - If proposer i-1 received B_{i-2} in slot i-1, it received B_{ch}, placing B_{i-1} on the canonical chain.

   ii) B_{i-2} is off the canonical chain, indicating that B_{ch} is another block among blocks from B_0 to B_{i-3}.
   - According to Lemma 1(a), in slot i-1, proposer i-1 has received all blocks from B_0 to B_{i-3}, it indicates that proposer i-1 has surely received B_{ch} and places B_{i-1} on the canonical chain.

Therefore, B_{i-2} and B_{i-1} cannot both be absent from the canonical chain simultaneously. However, it is possible that either of them or both will be on the global canonical chain. This confirms Lemma 1(b).

c) When proposing a block at slot i, Proposer i follows the fork choice rules and points B_i to the canonical chain in its own view. With Lemma 1(a), it is straightforward for proposer i to determine the canonical chain from B_0 to B_{i-2}. However, how to link B_i depends on whether $B_{i-1}$is the B_H and whether proposer i receives B_{i-1}.

When proposer i receives block B_{i-1}, we know that:
- if B_{i-1} is B_{ch}, then B_i points to B_{i-1} according to Rule 1;
- otherwise, B_{i-2} is B_{ch} according to (b) and hence B_i points to B_{i-2}.

When proposer i does not receive the B_{i-1}, we know that:
- if B_{i-1} is B_H and $B_{i-2}$is on the canonical chain, then B_i points to B_{i-2};
- if B_{i-1} is B_H but B_{i-2} is not on the canonical chain, then B_{i-3} is B_H according to (b) and hence B_i points to B_{i-3};
- otherwise, B_{i-2} is B_H according to (b) and hence B_i points to B_{i-2}.

Thus, B_i points to either block B_{i-1}, B_{i-2} or B_{i-3}, conclusively proving Lemma 1(c).
■

Proof of Theorem 1: Consider a Δ-synchronous network where Δ⩽ 2δ<2Δ. The state space of this Markov Chain is $S \in \{S_1, S_2\}$ where $\{S_1 = (1,1)$ and $S_2 = (2,0)\}$. Let π_i,i=1,2, denote the steady probability of state S_i, respectively. According to the definition of the state, π_0 (π_1) denotes the probability that the newly generated block in current slot is on (off) the canonical chain. Assume $\Delta = 1$ is a unit time.

i) **Steady-state probabilities (π_i):** We obtain π_i by solving the equation:

$$\begin{cases}\pi_0 = p\pi_0 + \pi_1 \\ \pi_1 = (1-p)\pi_0 \\ \pi_0 + \pi_1 = 1\end{cases}$$

Thus, we can derive that:

$$\begin{cases}\pi_0 = \dfrac{1}{2-p} \\ \pi_1 = \dfrac{1-p}{2-p}\end{cases}$$

When δ=1, each proposer can surely see the previously generated block since $\Delta = 1$.

ii) **Throughput (Γ):** Since $\pi_0$denotes the probability that the newly generated block in current slot is on the canonical chain, the expected number of blocks on the canonical chain per slot is $\pi_0 \times 1 = \pi_0$. In one time unit (i.e., $\Delta = 1$), there are $\frac{1}{\delta}$ slots and hence the throughput is given by

$$\Gamma = \frac{\pi_0}{\delta} = \begin{cases}\frac{1}{\delta(2-p)}, & \delta \in [\frac{1}{2}, 1) \\ 1, & \delta = 1\end{cases}$$

iii) **Efficiency (η):** According to the definition of efficiency, we have:

$$\eta = \frac{\frac{\pi_0}{\delta}}{\frac{1}{\delta}} = \begin{cases}\dfrac{1}{2-p}, & \delta \in \left[\dfrac{1}{2}, 1\right) \\ 1, & \delta = 1\end{cases}$$

iv) **Fork probability (P_f):** Since $\pi_0 = \frac{1}{2-p}$, and there are δ blocks per unit time, the probability of $1/\delta$ blocks being all on the canonical chain is ${\pi_0}^{1/\delta}$. Therefore, the fork probability is:

$$P_{\mathrm{F}}=\begin{cases}1-\dfrac{1}{(2-p)^{\frac{1}{\delta}}}, & \delta\in\left[\dfrac{1}{2},1\right)\\ 0 & ,\delta=1\end{cases}$$

■

Proof of Lemma 2: Consider a Δ-synchronous network where Δ < 3δ < 3/2Δ. Proposer i broadcasts a block B_i at the beginning of slot i. We now prove Lemma 2(a)-(c):

a) Since δ<Δ⩽ 3δ, a newly generated block will surely be received within 3 slots, but not necessarily received in one slot. Therefore, in slot i, proposer i surely receives B_{i-3} and all blocks preceding it but may not receive B_{i-2} and B_{i-1}. This confirms Lemma 1(a).

b) When proposer i-1 proposes B_{i-1} in slot i-1. There are four cases:
   i) B_{i-2} and B_{i-3} are on the canonical chain, indicating that B_{i-2} is theB_H in slot i-1.
      - If proposer i-1 did not receive B_{i-2} in slot i-1, it missed B_H, placing B_{i-1} off the canonical chain.
      - If proposer i -1 received B_{i-2} in slot i -1, it received B_H, placing B_{i-1} on the canonical chain.
   ii) B_{i-3} is off the canonical chain, B_{i-2} is on the canonical chain, indicating that B_{i-2} is the B_H in slot i-1. Same as case i), if proposer i-1 received B_{i-2} in slot i-1, B_{i-1} is on the canonical chain, otherwise it will be off the canonical chain.
   iii) B_{i-3} is on the canonical chain, B_{i-2} is off the canonical chain, indicating that B_{i-3} is the B_{ch} in slot i-1. If proposer i-1 received B_{i-3} in slot i-1, B_{i-1} is on the canonical chain, otherwise it will be off the canonical chain.
   iv) B_{i-2} and B_{i-3} are off the canonical chain, B_H is another block among blocks from B_0 to B_{i-4}. According to Lemma 2(a), in slot i-1, proposer i-1 has received all blocks from B_0 to B_{i-3}, it indicates that proposer i-1 has surely received B_H and places B_{i-1} on the canonical chain.

Therefore, B_{i-3}, B_{i-2}, and B_{i-1} cannot be all absent from the canonical chain. However, it is possible that each or multiple of them are on the canonical chain, thus proving Lemma 2(b).

c) When proposing a block at slot i, Proposer i follows the fork choice rules and points B_i to the canonical chain in its own view. The features influence a proposer's choice are 1) The blocks it received. 2.) the blocks are on the canonical chain or not. Lemma 2(a) and (b) show that a proposer i may not receive B_{i-2} or B_{i-1}, and there are at most 2 continuously blocks off the canonical simultaneously. As analyzed in Proof of Lemma 1(c), a proposer i might fail to receive B_{i-2} and B_{i-1}, resulting in B_i 's pointing to anyone of B_{i-1}, B_{i-2}, or B_{i-3}. Because of the 3-synchronous network, the connection options in case 2 has two more possibilities:
   - If proposer i does not receive block B_{i-2} and B_{i-1}, B_{i-4} is on the canonical chain but B_{i-3} is not, B_{i-4} is B_H. Proposer i receives B_{i-4} and point B_i to it.
   - If B_{i-2}, B_{i-1} are not received, B_{i-3}, B_{i-4} are not on the canonical chain, B_{i-5} is the B_H, according to Lemma 2(b). Proposer i receives B_{i-5} and point B_i to it. Also, B_{i-5} the earliest block that B_i may point to.

Thus, B_i can only point to B_{i-5}, B_{i-4}, B_{i-3}, B_{i-2}, or B_{i-1}, proving Lemma 2(c).

■

Proof of Theorem 2: Consider a Δ-synchronous network where Δ<3δ<3/2Δ. The state space of this Markov Chain is $S\in\{S_0,S_1,\ldots\ldots S_7\}$ where $\{S_0=(1,0,1),\ S_1=(1,1,1),\ S_2=(2,2,0),\ S_3=(1,2,1), S_4=(2,1,0), S_5=(3,3,0),\ S_6=(1,1,0), S_7=(2,2,0)*\}$. Let π_i, $i=1,\ldots,7$, denote the steady probability of state S_i, respectively. Let $\pi=(\pi_0,\ldots,\pi_7)$, according to the definition of the state, π_0, π_1 and π_3 ($\pi_{2,4,5,6\ and\ 7}$) denotes the probability that the newly generated block in current slot is on (off) the canonical chain. Assume $\Delta=1$ is a unit time. We have the following one-step transition probability matrix:

$$P=\begin{bmatrix}0 & p_1 & q_1 & 0 & 0 & 0 & 0 & 0\\ p_1 & 0 & q_1p_2 & 0 & q_1q_2 & 0 & 0 & 0\\ p_2 & 0 & 0 & p_1q_2 & 0 & q_1q_2 & 0 & 0\\ 0 & p_1 & 0 & 0 & 0 & 0 & q_1 & 0\\ p_2 & 0 & 0 & 0 & 0 & 0 & 0 & q_2\\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & p_1q_2+p_2 & q_1q_2 & 0 & 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

Steady-state probabilities: π_i is obtained by solving the equation $\begin{cases}\pi=\pi P,\\ \sum_{i=0}^{m}\pi_i=1\end{cases}$.

i) Throughput ($\boldsymbol{\Gamma}$): Since π_0, π_1 and π_3 denote the probability that the newly generated block in current slot is on the canonical chain, the expected number of blocks on the canonical chain per slot is $(\pi_0+\pi_1+\pi_3)\times 1=\pi_0+\pi_1+\pi_3$. In one time unit (i.e., $\Delta=1$), there are $\frac{1}{\delta}$ slots and hence the throughput is:

$$\Gamma=\frac{\pi_0+\pi_1+\pi_3}{\delta},\quad \delta\in[\frac{1}{3}\Delta,\frac{1}{2}\Delta)$$

ii) Efficiency ($\boldsymbol{\eta}$): According to the definition of efficiency, we have:

$$\eta=\frac{\frac{\pi_0+\pi_1+\pi_3}{\delta}}{\frac{1}{\delta}}=\pi_0+\pi_1+\pi_3$$

iii) Fork probability P_F: Since there are $1/\delta$ blocks per unit time, the probability of $1/\delta$ blocks being all on the canonical chain is $(\pi_0+\pi_1+\pi_3)^{1/\delta}$. Therefore, the fork probability is:

$$P_F=1-(\pi_0+\pi_1+\pi_3)^{\frac{1}{\delta}}$$

■