ToR: A Highly Scalable, General and Secure Cross-Chain Protocol

1 PROOF OF WORKLOAD OPTIMIZATION RATE

Model. We denote the relay chain's throughput as α, meaning it can process α transactions per second. Given $n \geq 2$ parachains in the cross-chain system, fully-connected, denoted as $\{P_i \mid i \in [1, n]\}$. For the parachain P_i, it can generate $\{b_i \mid i \in [1, n]\}$ blocks per second, and the number of cross-chain messages created per block is denoted as $\{x_j \mid j \in [1, b_i]\}$. We consider the average workload during the time interval D which is divided it into a discrete time series $TS = \{t_1, t_2, ..., t_d\}$ with a 1-second interval. For convenience, we define $h(x) = \frac{|x|+x}{2}$, meaning that if $x > 0$ then $h(x) = x$, and if $x <= 0$ then $h(x) = 0$.

Lemma 1. *Based on the above model, in ToR, the average workload of the relay chain is*

$$W^{\circ}_{ToR} = \begin{cases} y_{ToR}, & \alpha \geq y_{ToR} \\ y_{ToR} + \dfrac{(d-1)}{2} * (y_{ToR} - \alpha), & \alpha < y_{ToR} \end{cases}$$

, where $y_{ToR} = \sum\limits_{i=1}^{n} b_i$.

Proof. The relay chain can receive up to $y_{ToR} = \sum\limits_{i=1}^{n} b_i$ transactions (i.e., block header synchronization) per second. Given that the relay chain's throughput is α, we can know W_{ToR} as follows:

$$\begin{aligned} W_{ToR} = \{W_{t_1} &= y_{ToR}, \\ W_{t_2} &= h(W_{t_1} - \alpha) + y_{ToR}, ..., \\ W_{t_d} &= h(W_{t_{d-1}} - \alpha) + y_{ToR}\}. \end{aligned}$$

In terms of varying values of α,

i. if $\alpha \geq y_{ToR}$ then

$$W^{\circ}_{ToR} = W_{t_k} = W_{t_1} = y_{ToR},\ where\ k \in [1, d]$$

ii. if $\alpha < y_{ToR}$ then

$$W_{t_{k+1}} = W_{t_k} - \alpha + y_{ToR},\ where\ k \in [1, d-1]$$

Thus, W_{ToR} forms an arithmetic sequence with a common difference of $\Delta = y_{ToR} - \alpha$. Therefore, it can be derived that:

$$W^{\circ}_{ToR} = y_{ToR} + \frac{(d-1)}{2} * (y_{ToR} - \alpha)$$

□

Lemma 2. *Based on the above model, in AoR, the average workload of the relay chain is*

$$W^{\circ}_{AoR} = \begin{cases} y_{AoR}, & \alpha \geq y_{AoR} \\ y_{AoR} + \dfrac{(d-1)}{2} * (y_{AoR} - \alpha), & \alpha < y_{AoR} \end{cases}$$

, where $y_{AoR} = \sum\limits_{i=1}^{n} b_i + \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{b_i} x_{i,j}$

Proof. the relay chain can receive up to $y_{AoR} = \sum\limits_{i=1}^{n} b_i + \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{b_i} x_{i,j}$ transactions (i.e., block header synchronization and cross-chain messages) per second. We can know W_{AoR} as follows:

$$\begin{aligned} W_{AoR} = \{W'_{t_1} &= y_{AoR}, \\ W'_{t_2} &= h(W'_{t_1} - \alpha) + y_{AoR}, ..., \\ W'_{t_d} &= h(W'_{t_{d-1}} - \alpha) + y_{AoR}\}. \end{aligned}$$

In terms of varying values of α,

i. if $\alpha < y_{AoR}$ then

$$W'_{t_{k+1}} = W'_{t_k} - \alpha + y_{AoR},\ where\ k \in [1, d-1].$$

Thus, W_{AoR} forms an arithmetic sequence with a common difference of $\Delta = y_{AoR} - \alpha$. Consequently, it follows that:

$$W^{\circ}_{AoR} = y_{AoR} + \frac{(d-1)}{2} * (y_{AoR} - \alpha).$$

ii. if $\alpha \geq y_{AoR}$ then

$$W^{\circ}_{AoR} = W'_{t_k} = W'_{t_1} = y_{AoR},\ where\ k \in [1, d-1]$$

Hence,

$$W^{\circ}_{AoR} = \begin{cases} y_{AoR}, & \alpha \geq y_{AoR} \\ y_{AoR} + \dfrac{(d-1)}{2} * (y_{AoR} - \alpha), & \alpha < y_{AoR} \end{cases}$$

□

Thereom 1. *Based on the above model, we have the average workload optimization ratio*

$$\tau \geq 1 - \frac{1}{\varsigma}$$

, where $\varsigma = \overline{x} = \dfrac{\sum_{i=1}^{n} \sum_{j=1}^{b_i} x_{i,j}}{\sum_{i=1}^{n} b_i}$*, which refers to the average number of cross-chain messages in a parachain block.*

Proof. From Lemma 1 and Lemma 2, we can know τ as follows:

$$\begin{aligned} \tau &= 1 - \frac{W^{\circ}_{ToR}}{W^{\circ}_{AoR}} \\ &= 1 - \begin{cases} \dfrac{y_{ToR} + \frac{(d-1)}{2} * (y_{ToR} - \alpha)}{y_{AoR} + \frac{(d-1)}{2} * (y_{AoR} - \alpha)}, & \alpha < y_{ToR} \\ \dfrac{y_{ToR}}{y_{AoR} + \frac{(d-1)}{2} * (y_{AoR} - \alpha)}, & y_{ToR} \leq \alpha < y_{AoR} \\ \dfrac{y_{ToR}}{y_{AoR}}, & y_{AoR} \leq \alpha \end{cases} \end{aligned}$$

Discuss by different conditions.

i. if $\alpha < y_{ToR}$ then

$$\tau = 1 - \frac{W^{\circ}_{ToR}}{W^{\circ}_{AoR}}$$
$$= 1 - \frac{y_{ToR} - \frac{d-1}{d+1} * \alpha}{y_{AoR} - \frac{d-1}{d+1} * \alpha}$$

As the time series length d approaches sufficiently large, given $\lim_{d \to +\infty} \frac{d-1}{d+1} = 1$, we can consequently deduce that

$$\tau = 1 - \frac{y_{ToR} - \alpha}{y_{AoR} - \alpha}$$

Let $g = \frac{y_{ToR} - \alpha}{y_{AoR} - \alpha}$, then

$$g = \frac{1 - \frac{\alpha}{n\overline{b}}}{1 + \frac{\sum_{i=1}^{n} \sum_{j=1}^{b_i} x_{i,j}}{n\overline{b}} - \frac{\alpha}{n\overline{b}}}$$
$$= \frac{1 - \frac{\alpha}{n\overline{b}}}{1 + \overline{x} - \frac{\alpha}{n\overline{b}}}$$

Let $v = 1 - \frac{\alpha}{n\overline{b}}$, then $g = \frac{1}{1 + \frac{\overline{x}}{v}}$.

It can be easily deduced that for $v \in (0, 1)$, $g(v)$ is monotonically increasing, and τ is monotonically decreasing.

Given $\alpha \longrightarrow 0$, τ approaches its minimum value $\frac{1}{1 + \overline{x}}$.

Therefore, if $\alpha < y_{ToR}$, then $\tau > 1 - \frac{1}{\overline{x}}$.

ii. if $y_{ToR} \leq \alpha < y_{AoR}$, then

$$\tau = 1 - \frac{W^{\circ}_{ToR}}{W^{\circ}_{AoR}}$$
$$= 1 - \frac{2 * y_{ToR}}{(d+1) * y_{AoR} - (d-1) * \alpha}$$

Let

$$g(a) = \frac{2 * y_{ToR}}{(d+1) * y_{AoR} - (d-1) * \alpha}$$

, we can know $g(a)$ is monotonically increasing, andτ is monotonically decreasing. Given $\alpha \longrightarrow y_{AoR}$, τ approaches its minimum value $\frac{y_{ToR}}{y_{AoR}}$.

Let $\gamma = \frac{y_{ToR}}{y_{AoR}}$, then

$$\gamma = \frac{\sum_{i=1}^{n} b_i}{\sum_{i=1}^{n} b_i + \sum_{i=1}^{n} \sum_{j=1}^{b_i} x_{i,j}}$$
$$= \frac{1}{1 + \overline{x}}$$

Therefore, if $y_{ToR} \leq \alpha < y_{AoR}$, then $\tau > 1 - \frac{1}{\overline{x}}$.

iii. if $y_{AoR} \leq \alpha$ then $\tau = 1 - \frac{1}{\overline{x}}$.

In summary, from (i.,ii.,iii.), we have $\tau \geq 1 - \frac{1}{\overline{x}}$. □