Appendix

A. Proof of Theorem 1

Theorem 1. *The maximum effective transaction throughput of the system grows linearly with the number of shards.*

Proof. We assume that, on average, each transaction in the system involves n accounts. For example, in the Ethereum system, transactions have only one input and one output, so $n = 2$. In a blockchain system where transactions are multiple-input and multiple-output, n can be 2, 3, or more. The probability that a transaction with n accounts involves m shards is represented by α_m.

All involved shards need to process an effective transaction once. If a transaction involves m shards, the number of times the transaction needs to be processed is m. Thus, the expected number of times an effective transaction needs to be processed by different shards is $\sum_{m=1}^{n} m\alpha_m$. If the maximum effective transaction throughput of the system, or the maximum rate at which the system can process effective transactions is τ, then the maximum overall transaction processing rate of the system is $\tau \sum_{m=1}^{n} m\alpha_m$.

When the system reaches an equilibrium of transaction processing supply and demand, the maximum overall transaction processing rate of the system is equal to the sum of the maximum overall transaction processing rates of each shard μ, which is $k\mu$. Thus, we can get the following:

$$k\mu = \tau \sum_{m=1}^{n} m\alpha_m. \tag{9}$$

Let χ_i be the random variable where

$$\chi_i = \begin{cases} 1, & \text{if the transaction involves shard } i \\ 0, & \text{if the transaction does not involve shard } i \end{cases} \tag{10}$$

The probability that any account is assigned to shard i is $\frac{1}{k}$. Correspondingly, the probability that an account is not assigned to i is $1 - \frac{1}{k}$.

Thus, the probability that a transaction does not involve shard i is:

$$P(\chi_i = 0) = \left(1 - \frac{1}{k}\right)^n = \left(\frac{k-1}{k}\right)^n. \tag{11}$$

Correspondingly, the probability that a transaction involves shard i is:

$$P(\chi_i = 1) = 1 - P(\chi_i = 0) = 1 - \left(\frac{k-1}{k}\right)^n. \tag{12}$$

The expectation is

$$\begin{aligned} E(\chi_i) &= 0 \cdot P(\chi_i = 0) + 1 \cdot P(\chi_i = 1) \\ &= 1 - \left(\frac{k-1}{k}\right)^n. \end{aligned} \tag{13}$$

Let ξ denote the number of shards processing a transaction with n accounts.

$$\xi = \chi_1 + \chi_2 + \cdots + \chi_k. \tag{14}$$

According to the linearity of expectation,

$$\begin{aligned} E(\xi) &= E(\chi_1) + E(\chi_2) + \cdots + E(\chi_k) \\ &= k \cdot \left[1 - \left(\frac{k-1}{k}\right)^n\right]. \end{aligned} \tag{15}$$

According to the definition of expectation,

$$E(\xi) = \sum_{m=1}^{n} \alpha_m m. \tag{16}$$

Combining Eq. (15) and Eq. (16), we can get

$$E(\xi) = k \cdot \left[1 - \left(\frac{k-1}{k}\right)^n\right] = \sum_{m=1}^{n} \alpha_m m. \tag{17}$$

Combining Eq. (17) with Eq. (9), we can get

$$\begin{aligned} \tau &= \frac{k\mu}{\sum_{m=1}^{n} \alpha_m m} = \frac{k\mu}{k \cdot \left[1 - \left(\frac{k-1}{k}\right)^n\right]} \\ &= \frac{\mu}{1 - \left(\frac{k-1}{k}\right)^n} \\ &= \frac{\mu k^n}{k^n - (k-1)^n}. \end{aligned} \tag{18}$$

Because

$$\lim_{k\to\infty} \frac{k^n - (k-1)^n}{nk^{n-1}} = \lim_{k\to\infty} \frac{k^n - k^n + nk^{n-1} + o(k^{n-1})}{nk^{n-1}} = 1, \tag{19}$$

combining Eq. (18) and Eq. (19), we can get:

$$\lim_{k\to\infty} \frac{\mu k}{n\tau} = \lim_{k\to\infty} \frac{k^n - (k-1)^n}{nk^{n-1}} = 1. \tag{20}$$

Therefore, when $k \to \infty$, $\tau \sim \frac{\mu}{n} k$.

When the number of shards k is large enough, the blockchain system that randomly assigns transactions to shards can also make the effective throughput of the system τ increase linearly with the number of shards. □

B. Proof of Theorem 2

Theorem 2. *The average transaction processing latency of the system decreases as the number of shards increases.*

Proof. Effective transactions consist of intra-shard transactions and cross-shard transactions. For a system where accounts are randomly assigned to shards, the probability that a transaction involving n accounts is an intra-shard transaction P_{in} is

$$P_{\text{in}} = \frac{1}{k^{n-1}}. \tag{21}$$

Correspondingly, the probability that a transaction involving n accounts is a cross-shard transaction P_{cr} is

$$P_{\text{cr}} = 1 - \frac{1}{k^{n-1}}. \tag{22}$$

Therefore, the arrival rate of intra-shard transactions λ_{in} and cross-shard transactions λ_{cr} in the system are

$$\begin{aligned} \lambda_{\text{in}} &= \lambda P_{\text{in}} = \frac{\lambda}{k^{n-1}}, \\ \lambda_{\text{cr}} &= \lambda P_{\text{cr}} = \lambda \left(1 - \frac{1}{k^{n-1}}\right), \end{aligned} \tag{23}$$

where λ is the arrival rate of effective transactions in the system.

We assume that, on average, each transaction in the system involves n accounts, the number of input shards is s_1, and the number of output shards is s_2. Then, the arrival rate of sub-transactions processed by all input shards is

$$\lambda_{\text{sub}} = s_1 \lambda_{\text{cr}} = s_1 \lambda \left(1 - \frac{1}{k^{n-1}}\right). \tag{24}$$

When the system attains its statistical equilibrium, the departure process of a $M/M/1$ queue is the same Poisson as the arrival process [25]. Thus, the arrival rate of cross-shard transactions processed by all output shards is

$$\lambda_{\text{crout}} = s_2 \lambda_{\text{sub}} = s_1 s_2 \lambda \left(1 - \frac{1}{k^{n-1}}\right). \tag{25}$$

Due to the homogeneity assumption of shards, all shards have the same transaction arrival rate. Each shard is an M/M/1 queue whose transaction arrival rate is $\frac{1}{k}$ of the transaction arrival rate of the total system. An arbitrary shard $i \in \{1, 2, \dots, k\}$ processes three types of transactions: intra-shard transactions, cross-shard transactions with input accounts within the shard, and cross-shard transactions with output accounts within the shard. Thus, the transaction arrival rate $\lambda_0(k)$ of a shard is:

$$\begin{aligned} \lambda_0(k) &= \frac{\lambda_{\text{in}} + \lambda_{\text{sub}} + \lambda_{\text{crout}}}{k} \\ &= \lambda \frac{1}{k^n} + \lambda s_1 (1 + s_2) \left(\frac{1}{k} - \frac{1}{k^n}\right). \end{aligned} \tag{26}$$

The growth of λ_0 as k grows can be expressed as

$$\begin{aligned} &\lambda_0(k+1) - \lambda_0(k) \\ &= \lambda \frac{-b(k+1)^{n-1} k^{n-1} + (b-1)\left[(k+1)^n - k^n\right]}{(k+1)^n k^n}, \end{aligned} \tag{27}$$

where $b = s_1(1 + s_2) > 0$.

As $k \to \infty$,

$$\lambda_0(k+1) - \lambda_0(k) < 0. \tag{28}$$

Thus, when k is sufficiently large, λ_0 will decrease as k increases.

According to the property of M/M/1 [25], the expectation of the transaction processing latency W_p is

$$W_p = \frac{1}{\mu - \lambda_0}. \tag{29}$$

Because

$$\frac{\mathrm{d}W_p}{\mathrm{d}\lambda_0} = \frac{1}{(\mu - \lambda_0)^2} > 0, \tag{30}$$

W_p increases as the transaction arrival rate λ_0 increases, and W_p decreases as λ_0 decreases.

Combining this result with the conclusion from Ineq. (28), we can conclude that when the number of shards k is sufficiently large, the transaction arrival rate λ_0 decreases as k increases, and the transaction processing latency W_p also decreases. □

C. Proof of Theorem 3

Theorem 3. *For each epoch with an unbiased and random committee formation algorithm, as long as $\beta < \frac{1}{3}$ and the number of validators in the committee n is sufficiently large, any committee is honest with an overwhelming probability.*

Proof. The committee formation algorithm can be modeled as random sampling. Let X denote a random variable representing the number of malicious validators selected in the committee. The distribution of X follows the hypergeometric distribution with parameters n, N, M where n is the number of validators in the committee, N is the total number of validators, and $M = \beta N$ is the total number of malicious validators. The probability that a committee of size n contains k malicious validators is:

$$P(X = k) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}}, \tag{31}$$

where $\binom{M}{k}$ is the binomial coefficient. From the hypergeometric distribution, the expectation and variance of X are given by

$$E(X) = n\beta, \tag{32}$$

$$Var(X) = \frac{nM(N-n)(N-M)}{N^2(N-1)} = n\beta(1-\beta)\frac{N-n}{N-1}. \tag{33}$$

The probability p_C^{A} that the number of malicious validators exceeds $\frac{1}{3}$ of the total number of validators in the committee is:

$$p_C^{\text{A}} = P(X \geq \frac{1}{3}n) = P(X - \beta n \geq n(\frac{1}{3} - \beta)). \tag{34}$$

According to Chebyshev's inequality,

$$P(X - \beta n \geq n(\frac{1}{3} - \beta)) \leq \frac{n\beta(1-\beta)\frac{N-n}{N-1}}{n^2(\frac{1}{3} - \beta)^2} \tag{35}$$

$$= \frac{\beta(1-\beta)}{(\frac{1}{3} - \beta)^2(N-1)}(\frac{N}{n} - 1). \tag{36}$$

Given $\eta > 0$, $n_0 = \left\lceil \frac{N}{\frac{(\frac{1}{3-\beta})^2\eta}{\beta(1-\beta)} + 1} \right\rceil$, for any $n \geq n_0$, Ineq. (35) satisfies:

$$P(X - \beta n \geq n(\frac{1}{3} - \beta)) \leq \frac{\beta(1-\beta)}{(\frac{1}{3} - \beta)^2(N-1)}(\frac{N}{n} - 1) \tag{37}$$

$$\leq \frac{\beta(1-\beta)}{(\frac{1}{3} - \beta)^2(N-1)}(\frac{N}{n_0} - 1) \tag{38}$$

$$\leq \eta. \tag{39}$$

Combining Ineq.(34), Ineq.(35) and Ineq. (37), we have $p_C^{\text{A}} \leq \eta$, which means that the probability that the number of malicious validators exceeds $\frac{1}{3}$ of the total number of validators in the committee is less than η. Therefore, the committee is honest as long as $\beta < \frac{1}{3}$ and the number of validators in the committee n is sufficiently large. □