

Параллельные блокчейны.

noise@sumus.team

28 октября 2019 г.

Пусть задано m параллельных блокчейнов (сабчейнов) $B_{n_1}, \dots, B_{n_m} : B_n = \bigcup_{j=1}^m B_{n_j} \subseteq A_N$.

Синхронным параллельным блокчейном назовём блокчейн, для которого в любой момент времени закрыто одинаковое количество блоков в каждом $B_{n_j}, j = 1, \dots, m$.

Если блокчейн несинхронный, то для описания рассогласования сабчейнов и блокчайна в целом можно задать функцией $f_j(t), j = 1, \dots, mt \in [0, +\infty)$, где $f_j(t)$ равно количеству закрытых блоков в B_{n_j} на момент t .

$f_j(t)$ — кусочно-постоянная неубывающая функция вида $f_j(t) = K_j, t \in [t_{K,j}, t_{K+1,j})$, где $t_{K,j}$ — момент закрытия блока номер K_j , $t_{K+1,j}$ — момент закрытия блока номер $K_j + 1$ в B_{n_j} ;

Невязкой сабчейнов B_{n_i}, B_{n_j} на интервале $[0, t^*]$ назовём (1) $I_{ij} = \int_0^{t^*} |f_i(t) - f_j(t)| dt$.

Тогда невязкой блокчайна B_n назовём (2) $I = \sum_{j=2, i < j}^n I_{ij}$

Задача минимизации I есть задача синхронизации блокчайна. Очевидно, что $\inf I = 0$ — синхронный блокчейн

$\sup I = \int_0^{t^*} |f_i(t)| dt$ — параллельность не работает.

Рассмотрим синхронный блокчейн. Пусть T — время от начала формирования одного блока до его закрытия, $T \leq T_{fix}$ — ограничение на время закрытия блока; T является *const* для всего блокчайна.

Будем сравнивать непараллельный блокчейн (нп-блокчейн) с параллельным (п-блокчейн). Когда в нп-блокчайне за время T закрывается 1 блок, в параллельном блокчайне закрывается m блоков, а значит среднее время закрытия одного блока в этом блокчайне есть $\frac{T}{m}$. Пусть $\hat{\tau}$ — время, затрачиваемое всеми узлами блокчайна (нп-блокчейн и п-блокчейн) на обработку одного сообщения о закрытии одного блока. В параллельном блокчайне из-за одновременного закрытия m блоков время, затрачиваемое на обработку всеми узлами m одновременно поступивших сообщений равно $m\hat{\tau}$. При этом в нп-блокчайне требуется только $\hat{\tau}$ времени для обработки единственного сообщения.

Время, затрачиваемое на соотнесение одной транзакции и кошелька узлами, участвующими в закрытии одного блока обозначим $\tilde{\tau}$. Поскольку во всех блоках одинаковое количество транзакций, то время, затрачиваемое при закрытии 1 блока в нп-блокчайне и в п-блокчайне будет одинаковым и равным $K_T \cdot \tilde{\tau}$.

Рассмотрим норму блокчайна как метрику, заданную на паре (“идеальный” блокчайн, реальный блокчайн), где “идеальный” блокчайн в данном случае мгновенно выполняет любые операции (за время o). Рассмотрим пространство состояний блокчайна, где координата x_1 — время на обработку сообщений о закрытии блоков всеми узлами, x_2 — среднее время на закрытие одного блока, x_3 — время, затрачиваемое на соотнесение транзакций с кошельком. Для п-блокчайна $x_1 = m \cdot \hat{\tau}; x_2 = \frac{T}{m}; x_3 = K_T \cdot \tilde{\tau}$; для нп-блокчайна $x_1 = \hat{\tau}; x_2 = T; x_3 = K_T \cdot \tilde{\tau}$. П-блокчайн “лучше” нп-блокчайна если его норма меньше нормы нп-блокчайна, то есть для нормы $|x_1| + |x_2| + |x_3|$ получим $m \cdot \hat{\tau} + \frac{T}{m} + K_T \cdot \tilde{\tau} < \hat{\tau} + T + K_T \cdot \tilde{\tau}$ или

$$(3) m \cdot \hat{\tau} + \frac{T}{m} < \hat{\tau} + T;$$

Для решения неравенства (3) решим уравнение

$$(4) m \cdot \hat{\tau} + \frac{T}{m} = \hat{\tau} + T \text{ или}$$

(5) $\hat{\tau} \cdot m^2 - (T + \hat{\tau})m + T = 0$. Решим это уравнение

$$D = (T + \hat{\tau})^2 - 4T\hat{\tau} = (T - \hat{\tau})^2 \geq 0; m = \frac{T + \hat{\tau} \pm |T - \hat{\tau}|}{2\hat{\tau}}.$$

Условия “физически” реального решения:

(1) $D \geq 0$; (2) $m \geq 1$; из первого условия получим (3) $T \geq \hat{\tau}$, откуда получим корни квадратного уравнения

$$m_1 = 1; m_2 = \frac{T}{\hat{\tau}} \geq 1; m \in [m_1, m_2] — интервал допустимых значений m .$$

Найдём m_{opt} , обеспечивающее \min нормы п-блокчейна:

$$(5) m_{opt} = \arg \min \left(m\hat{\tau} + \frac{T}{m} \right), m \in \left[1, \frac{T}{\hat{\tau}} \right]$$

$$\left(m\hat{\tau} + \frac{T}{m} \right)' = \hat{\tau} - \frac{T}{m^2} = 0 \text{ или}$$

$$m_{opt} = \left(\frac{T}{\hat{\tau}} \right)^{\frac{1}{2}}. \text{ Заметим, что в } m_{opt} : m\hat{\tau} = \frac{T}{m}.$$

$$m_{opt} \in [m_1, m_2].$$

Дополнительные условия. Дополнительной причиной рассогласования п-блокчейна может стать “уход в раунды” одного или нескольких сабчейнов (из-за ухода в раунды при попытке принятия транзакции). Это может привести к уменьшению количества работающих сабчейнов на интервале $[0, t^*]$.

Пусть l — число сабчейнов, которые ушли в “раунды” на интервале $[0, t^*]$. Если известно распределение l^* как случайной величины, например, нормальное распределение с МО l^* , то надо учитывать, что количество работающих сабчейнов в среднем на большом t^* будет меньше $m - l^*$.

Пусть множество \mathbf{B} — множество блоков, закрытых на момент времени t^* , B_n (или A_N) — множество узлов, принимавших участие в закрытии блоков. Если между ними может быть установлено взаимно однозначное соответствие (биекция) в котором каждому блоку поставлен в соответствие узел, его закрывший (без консенсуса), то такой блокчейн назовём полностью децентрализованным.

Если все блоки закрыты одним узлом (мастер-узлом), то это полностью централизованный блокчейн.

Будем считать, что полностью централизованному блокчейну соответствует значение коэффициента $K = 1$, где ...

α_1 — мощность множества узлов B_n ...

$$1 - \frac{\alpha_1}{\alpha_2} = \frac{\alpha_2 - \alpha_1}{\alpha_2};$$

$r = \frac{1}{\alpha_2}$ — полностью централизованный блокчейн.

α_2 — мощность \mathbf{B}