Распределение fee между узлами сети блокчейн

noise@sumus.team, engi@sumus.team

20 марта 2018 г.

Аннотация

Правило мотивации постоянного подключения узла к сети ...

1 Введение

Разобьём вопрос о распределении fee между узлами на две части

Часть 1.

Если все узлы из B_n постоянно присутствуют в сети, то они равноправны в том смысле, что вероятность получения $\forall$ узлом в произвольным момент t закрытия блока вознаграждения в интервале величина, которого зафиксирована (достигнута) на данный момент, зависит только от величины интервала и количества узлов n .

Будем считать fee функцией времени t, где в некоторый момент t_k соответствующей проведению отдельной транзакции $fee(t_k)$ принимает значение, равное fee, "начисленному" за эту транзакцию. Пусть T - счётное множество значений всех t_k, в которые осуществляются транзакции, $k = 1, 2, ...$ Для общности будем считать, что множество всех $\mathbb{N}$ есть множество значений этой функции обозначим как Ψ. Таким образом, $fee(t_k)$ есть решетчатая неотрицательная функция, заданная на счётном множестве T. Поскольку fee меняется по закону, который можно установить только статистическими методами, то положим, что $fee(t_k)$ есть решетчатая случайна функция, или, другими словами, дискретный случайны процесс. Вообще говоря, этот процесс может быть нестационарным, но при этом следует допустить его эргодичность. Пусть плотность распределения этого процесса есть $f(fee, t)$, где $t \in T$, $fee \in \Psi$. Φ от f не менее чем, непрерывна по fee, т.е. $fee(t_k)$ при фиксированном t_k является непрерывной случайно величиной.

Пусть также имеет место независимости от процесса закрытия блоков, который в данном случае можно представить как дискретный случайный процесс $g(t_m)$ значениями которого являются номера мастер-узлов $j_{\hat{k}}$ определяемые в моменты $t_{m^*} \in [t'_{m-1}, t'_m)$, $m = 1, 2, 3 \dots$, где t'_m - момент закрытия блока номер m, t'_0 - начальный момент работы сети. Процесс $g(t^*_m)$ - стационарный с равномерным распределением дискретной случайно величины j_k, $k = 1, \dots, n$, $1 \le j_k \le N$ с плотностью вероятности

$$f_g(k) = \sum_{k=1}^{n} \frac{1}{n} \sigma(k - k_\nu) \tag{1}$$

независимый от $fee(t_k)$. Счётное множество всех значений t^*_m обозначим T^*.

В момент времени t_m закрытия блока номер m мастер-узел с номером $j_{\hat{k}}$ получает всю накопленную к этому моменту Δfee_{Σ}, которую будем считать равной

$$\Delta fee_{\Sigma}(t_m^{'}) = \sum_{k=k_{m-1}}^{k_m} fee(t_k) \tag{2}$$

где k_{m-1} - номер момента $t_{k_{m-1}}$, ближайшего к $t_{m-1}^{'}$ справа, а k_m - номер момента t_{k_m}, ближайшего к $t_m^{'}$ слева.

Поскольку для $\forall_k, m : t_k - t_{k-1} \ll t_m^{'} - t_{m-1}{'}$, то дискретная случайная функция $\Delta fee_{\Sigma}(t_m^{'})$ имеет, согласно закону больших чисел, распределение близкое к нормальному, т.е.:

$$F(\Delta fee_{\Sigma} < a, t)) \approx \Phi(\Delta fee_{\Sigma} < a, t)) \tag{3}$$

при произвольных $f(fee, t)$ и является дискретным процессом с неотрицательными значениями.

Таким образом, каждый из n узлов может в момент t_m^* стать мастер узлом с вероятностью $\frac{1}{n}$ и в соответствующий ему момент $t_m^{'}$ получить $\Delta fee_{\Sigma}(t_m^{'})$ например в интервале $(M_{\Delta fee_{\Sigma}} - 3\sigma_{\Delta fee_{\Sigma}}, M_{\Delta fee_{\Sigma}} + 3\sigma_{\Delta fee_{\Sigma}})$ с вероятностью $\approx 0,997$, где $M_{\Delta fee_{\Sigma}}$ и $\sigma_{\Delta fee_{\Sigma}}$ - математическое ожидание и среднеквадратическое отклонение случайного процесса в момент времени $t_m^{'}$.

В результате, в момент $t_m^{'}$ каждый из n узлов получает указанное вознаграждение с вероятностью $\frac{0,997}{n}$.

Приведённые выше результаты справедливы при достаточно длительных реализациях случайных процессов, т.е. при $m \gg n$ и их эргодичности.

Часть 2. Если не все узлы из B_n постоянно присутствуют в сети, то это означает, что есть некоторое подмножество узлов $B_{\widetilde{n}} \subseteq B_n$, $\widetilde{n} \leqslant n$ такое, что для $\forall$ узла из $B_{\widetilde{n}}$ справедливо следующее: пусть этот узел выбирался мастер-узлом $\bar{m}$ раз на отрезке $t \in [t_0', t_m^*)$, но принял задачу по закрытию блока только $\widetilde{m}$ раз ($\bar{m} < \widetilde{m}$), то за закрытие текущего блока, выбор эскорта которого осуществлён в момент t_m^*,этот мастер узел получит вознаграждение

$$\gamma = \frac{\widetilde{m}}{\bar{m}} \Delta fee_{\Sigma}(t_m^{'}) \tag{4}$$

остаток

$$\frac{\bar{m} - \widetilde{m}}{\bar{m}} \Delta fee_{\Sigma}(t_m^{'}) \tag{4a}$$

суммируется в дальнейшем с $\Delta fee_{\Sigma}(t_{m+1}^{'})$.

В силу независимости процесса включения/отключения узла в сети от других случайных процессов, упомянутых выше и естественном предположении о стационарности распределения номеров отключенных узлов, можно утверждать, что введение “мотивирующих” коэффициентов (4), (4a) и перенос остатков не приведёт к изменению классификации случайных процессов, используемых в этой задаче. Можно сказать, что в данном разделе предложено правило мотивации постоянного подключения узла к сети.

Список литературы

[1] Satoshi Nakamoto (2009). “Bitcoin: A Peer-to-Peer Electronic Cash System”. www.bitcoin.org .

.