Распределение вознаграждения между узлами сети блокчейн

noise@sumus.team, engi@sumus.team

25 апреля, 2018

Аннотация

Предлагается подход к оценке возможности равноправного получения узлами блокчейна вознаграждения за закрытие блоков. Для описания потоков транзакций и закрытия блоков применяется теория случайных процессов. Приводится пример получения узлами вознаграждений, незначительно различающихся по величине и являющихся значениями нормально распределённой случайной величины.

1 Введение

Сначала рассмотрим вопрос о распределении вознаграждения между узлами для случая, когда все узлы из B_n постоянно присутствуют в сети. Тогда они равноправны в том смысле, что вероятность получения любым узлом в произвольный момент t закрытия блока вознаграждения в интервале, величина которого зафиксирована на этот момент, зависит только от величины интервала и количества узлов n [1].

2 Основные положения и допущения

Будем считать величину вознаграждения ζ функцией времени t, где в некоторый момент t_k, соответствующий проведению отдельной транзакции, $\zeta(t_k)$ принимает значение равное ζ, "начисленному" за эту транзакцию [2]. Пусть T — счётное множество значений всех t_k, в которые осуществляются транзакции, $k = 1, 2, \dots$. Множество значений этой функции обозначим Ψ. Таким образом, $\zeta(t_k)$ есть решетчатая неотрицательная функция, заданная на счётном множестве T. Поскольку ζ меняется по закону, который можно установить только статистическими методами, то положим, что $\zeta(t_k)$ есть решетчатая случайная функция, или, другими словами, дискретный случайный процесс. Вообще говоря, этот процесс может быть нестационарным, но при этом следует допустить его эргодичность и слабую коррелированность. Также будем считать, что у этого процесса есть математическое ожидание и дисперсия. Пусть плотность распределения этого процесса есть $f(\zeta, t)$, где $t \in T$, $\zeta \in \Psi$. Функция f не менее чем непрерывна по ζ, а значит $\zeta(t_k)$ при фиксированном t_k является непрерывной случайной величиной. У $\zeta(t_k)$ есть математическое ожидание и дисперсия [3].

Пусть также имеет место независимый от ζ процесс закрытия блоков, который в данном случае можно представить как дискретный случайный процесс $g(t_m)$, значениями которого являются номера мастер-узлов $j_{\widehat{k}}$, определяемые в моменты $t_m \in [t'_{m-1}, t'_m)$, $m = 1, 2 \dots$, где

t'_m – момент закрытия блока номер m, t'_0 – начальный момент работы сети. Процесс $g(t_m)$ – стационарный с равномерным распределением дискретной случайной величины $j_{\widehat{k}}$, $1 \leq j_{\widehat{k}} \leq N$. Счётное множество всех значений t_m обозначим T^*.

3 Обоснование нормального распределения вознаграждения между постоянно подключёнными узлами

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

$$\Delta\zeta_\Sigma(t'_m) = \sum_{k=k_{m-1}}^{k_m} \zeta(t_k) \tag{1}$$

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 каждое значение случайной функции $\Delta\zeta_\Sigma(t'_m)$ является суммой большого числа случайных величин и согласно закону больших чисел (при соблюдении условий, указанных выше), имеет распределение близкое к нормальному [4]

$$P((\Delta\zeta_\Sigma < a), t) \approx \Phi(a, t) \tag{2}$$

а значит, $\Delta\zeta_\Sigma(t'_m)$ при произвольных, но подобных друг-другу при любых k функциях плотности $f(\zeta, t_k)$, с достаточной точностью является нормальным дискретным случайным процессом [5].

Таким образом, каждый из n узлов может в момент t_m стать мастер-узлом с вероятностью $\frac{1}{n}$ и в соответствующий момент t'_m получить $\Delta\zeta_\Sigma(t'_m)$, например, в интервале $(M_{\Delta\zeta_\Sigma} - 3\sigma_{\Delta\zeta_\Sigma}, M_{\Delta\zeta_\Sigma} + 3\sigma_{\Delta\zeta_\Sigma})$, с вероятностью $\approx 0,997$, где $M_{\Delta\zeta_\Sigma}$ и $\sigma_{\Delta\zeta_\Sigma}$ — математическое ожидание и среднеквадратическое отклонение случайного процесса (1) в момент времени t'_m.

В результате, в момент t'_m каждый из n узлов получает указанное вознаграждение с вероятностью $\frac{0,997}{n}$. Уменьшение интервала значений $\Delta\zeta_\Sigma(t'_m)$, например, в полтора раза приводит к незначительному изменению указанной вероятности.

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

4 Пример

Покажем, что при способе вознаграждения узлов, описанном выше, эти вознаграждения будут распределены по нормальному закону. Рассмотрим в качестве $\zeta(t_k)$ дискретный случайный процесс, значениями которого являются вознаграждения за одиночные транзакции в системе БИТКОЙН [6]. На основе этого процесса, вычисляются по формуле (1) значения второго дискретного случайного процесса, значениями которого являются вознаграждения $\Delta\zeta_\Sigma$ каждому мастер-узлу, закрывшему блок. На временном интервале от 18.02.2017 до 13.12.2018 процесс $\Delta\zeta_\Sigma$ принимает 10^5 значений, среди которых наибольшим является 2,0 BTC. Именно этот процесс должен иметь нормальное распределение. Разделим 10^5 значений этого процесса, упорядоченных по времени, на 10 кусков, в каждом из которых будет по 10^4 значений $\Delta\zeta_\Sigma(t'_m)$. Таким образом, получены 10 реализаций исследуемого случайного процесса, в каждом из которых по 10^4 значений

$\Delta\zeta_\Sigma$. Эта операция справедлива, если процесс эргодический [3]. Реализацией № i, $i = 1, \ldots, 10$ будем обозначать $\Delta\zeta(t_j)$, где при фиксированном i индекс j "пробегает" значения от 1 до 10^4. Сечением №j случайного процесса $\Delta\zeta_\Sigma(t_j)$ будет множество значений $\Delta\zeta_{\Sigma_i}$ при фиксированном j и $i = 1, \ldots, 10$.

В произвольно взятом j-том сечении будет 10^4 значений случайной величины $\Delta\zeta_{\Sigma_j}$. Разобьём отрезок $[\min\Delta\zeta_{\Sigma_j}, \max\Delta\zeta_{\Sigma_j}]$ на r одинаковых отрезков (в нашем случае $r = 10$). Откладывая по оси абсцисс значения случайной величины $\Delta\zeta_{\Sigma_j}$, а над каждым из r отрезков откладывая по оси ординат количество значений $\Delta\zeta_{\Sigma_j}$ попавших в этот отрезок, получим график, показанный на рис. 1. После его нормировки делением значений решетчатой функции на 10^4 получим так называемый ряд распределения случайной величины, значения которой равны средним значениям $\Delta\zeta_{\Sigma_j}$ по каждому из r отрезков разбиения отрезка $[\min\Delta\zeta_{\Sigma_j}, \max\Delta\zeta_{\Sigma_j}]$ (мы полагаем, что на каждом из r отрезков случайная величина $\Delta\zeta_{\Sigma_j}$ принимает практически одни и те же значения). Ряд распределения для дискретных случайных величин является аналогом плотности распределения для непрерывных случайных величин. Нетрудно видеть, что огибающая графика решетчатой функции на рис. 1 будет гауссовой кривой. По ряду распределения нетрудно построить функцию распределения, которая будет кусочно-постоянным приближением функции Лапласа.

Таким образом, экспериментально подтверждено, что вознаграждение за закрытие блока есть нормально распределённая случайная величина, являющаяся функцией времени, другими словами нормальным дискретным случайным процессом.

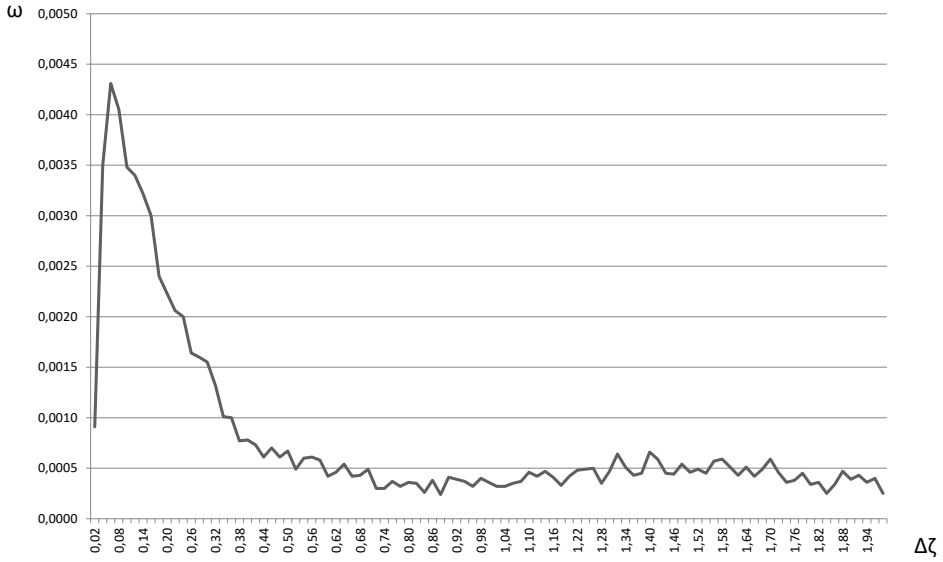

Рис. 1. Экспериментальная кривая плотности распределения вознаграждения между узлами.

5 Распределение вознаграждения между узлами, не подключёнными постоянно

Рассмотрим теперь вопрос распределения ζ между узлами для случая, когда не все узлы из B_n постоянно присутствуют в сети. Это означает, что есть некоторое фиксированное подмножество узлов $B_{\widetilde{n}} \subseteq B_n$, $\widetilde{n} \leq n$ (считаем, что $\widetilde{n} < n/3$) такое, что для любого узла из $B_{\widetilde{n}}$ справедливо следующее: пусть этот узел выбирался мастер-узлом $\overline{m} < m$ раз на отрезке $t \in [t'_0, t^*_m)$, но принял задачу по закрытию блока только $\widetilde{m}$ раз ($\widetilde{m} < \overline{m}$). Тогда за закрытие текущего блока мастер

узел получит вознаграждение

$$\gamma_m = \frac{\widetilde{m}}{\overline{m}}\Delta\zeta_\Sigma(t_m^{'}) \tag{3}$$

остаток

$$\frac{\overline{m}-\widetilde{m}}{\overline{m}}\Delta\zeta_\Sigma(t_m^{'}) \tag{4}$$

суммируется в дальнейшем с $\Delta\zeta_\Sigma(t_{m+1}^{'})$. Можно сказать, что предложено правило мотивации постоянного подключения узла к сети.

В силу независимости процесса включения/отключения узла в сети от других случайных процессов, упомянутых выше, и естественном предположении о стационарности и равномерности распределения номеров $\widetilde{n}$ отключаемых узлов, можно утверждать, что введение "мотивирующих" коэффициентов $M = \dfrac{\widetilde{m}}{\overline{m}}$, и перенос остатков не приведут к изменению классификации случайных процессов, используемых в этой задаче.

Вероятность того, что в произвольный момент t_m определения нового мастер-узла им станет непостоянно подключенный узел из $B_{\widetilde{n}}$, есть $\widetilde{p} = \dfrac{\widetilde{n}}{n}$. Тогда в момент $t_m^{'}$ закрытия блока номер m с данным мастер-узлом этот узел получит вознаграждение $\dfrac{\widetilde{m}}{m}\Delta\zeta_\Sigma(t_m^{'})$. Если следующий мастер-узел не принадлежит $B_{\widetilde{n}}$, то в момент $t_{m+1}^{'}$ он получит вознаграждение

$$\Delta\zeta_\Sigma(t_{m+1}^{'}) + \frac{\overline{m}-\widetilde{m}}{m}\cdot\Delta\zeta_\Sigma(t_m^{'}) \tag{5}$$

В момент $t_{m+2}^{'}$ новый мастер-узел, если он вновь не принадлежит $B_{\widetilde{n}}$, получит за закрытие $m+2$ блока $\Delta\zeta_\Sigma(t_{m+2}^{'})$ уже без надбавок и в этом случае перенос выплаты $\dfrac{\overline{m}-\widetilde{m}}{m}\cdot\Delta\zeta_\Sigma(t_m^{'})$ станет надбавкой соответствующему мастер-узлу, мотивируя все узлы из B_n быть постоянно подключёнными и это не приведёт к неконтролируемому росту надбавок к $\Delta\zeta$. Если новый мастер-узел $\in B_{\widetilde{n}}$, то в момент $t_{m+2}^{'}$ повторится ситуация сложившаяся в момент $t_m^{'}$, а значит если появление мастер-узлов из $B_{\widetilde{n}}$ идёт не подряд, а хотя бы "через один", то накопление надбавок не происходит.

Пусть на отрезке $[t_0^{'}, t_m^{*}]$ из m мастер-узлов $\widehat{m}$ оказались из $B_{\widetilde{n}}$ (с возможными повторными назначениями одних и тех же узлов мастер-узлами). Вероятность этого есть, согласно биноминальному распределению

$$P_{\widehat{m},m} = C_m^{\widehat{m}}\cdot\widetilde{p}^{\,\widehat{m}}\cdot(1-\widetilde{p})^{m-\widehat{m}} \tag{6}$$

Вероятность события "из m опытов $\widehat{m}$ раз появляется номер узла из $B_{\widetilde{n}}$" равна

$$\widetilde{p}^{\,\widehat{m}}\cdot(1-\widetilde{p})^{m-\widetilde{m}} \tag{7}$$

если рассматривать только один набор мастер-узлов, назначаемых в моменты $t_{k_i}^{*}, i = 1,\ldots,\widehat{m}; 1 \le k_j \le m$, в котором появляются мастер-узлы из $B_{\widetilde{n}}$. Наиболее "критичным" с точки зрения накопления надбавки является вариант, когда закрывается $\widehat{m}$ блоков подряд $k_{i+1} = k_i + 1\,, i = 1,\ldots,\widehat{m}-1$, для каждого из которых мастер-узел принадлежал $B_{\widetilde{n}}$. Вероятность этого равна (7). Поскольку каждый узел из $B_{\widetilde{n}}$ включается и отключается по-своему, то для оценки накопления вознаграждения за счёт надбавки выберем $\max\limits_{i=1,\ldots,\widehat{m}}\left\{\dfrac{\overline{m}_{k_i}-\widetilde{m}_{k_i}}{\overline{m}_{k_i}}\right\} = M_{\max} < 1$, соответственно $M_{\min} = \min\limits_{i=1,\ldots,\widehat{m}}\left\{\dfrac{\widetilde{m}_{k_i}}{\overline{m}_{k_i}} = M_{k_i}\right\} < 1$. Очевидно, что $M_{\max}$ и $M_{\min}$ определяются при одном и том

же M_{k_i} , $M_{\max} = 1 - M_{\min}$.

Положим $\overline{\Delta\zeta_\Sigma} = \max\limits_{i=1,\ldots,\widehat{m}} \Delta\zeta_\Sigma(t'_{k_i})$. Оценка суммы вознаграждения в целом за закрытие $\widehat{m}$ блоков в этом случае $\widehat{m} \cdot \Delta\zeta$. Оценка суммы выплаченных вознаграждений есть $\widehat{m} \cdot M_{\min} \cdot \overline{\Delta\zeta}$ (учитывая невыплату надбавки). Верхняя оценка суммы невыплаченного вознаграждения за $\widehat{m}$ шагов есть

$$\widehat{m} \cdot (1 - M_{\min}) \cdot \overline{\Delta\zeta} \; . \tag{8}$$

При достаточно большом $\widehat{m}$ в момент $t_{k_{\widehat{m}}+1}$ первый мастер узел, не принадлежащий $B_{\widetilde{n}}$, помимо $\Delta\zeta_\Sigma(t_{k_{\widehat{m}}+1})$ получит надбавку, оцениваемую как (8), которая может оказаться чрезмерно большой.

Если не использовать оценки надбавок и вознаграждений, которые введены для упрощения расчётов, и сохранить их точные значения, то приведённые выше выводы останутся справедливыми. Действительно, сумма выплаченных вознаграждений S есть

$$S = \sum_{i=1}^{\widehat{m}} \Delta\zeta_\Sigma(t'_{k_i}) \cdot M_i \tag{9}$$

а сумма S_H невыплаченных вознаграждений за закрытие $\widehat{m}$ блоков будет равна:

$$S_H = \sum_{i=1}^{\widehat{m}} \Delta\zeta_\Sigma(t'_{k_i}) - S = \sum_{i=1}^{\widehat{m}} (1 - M_i)\Delta\zeta_\Sigma(t'_{k_i}) \tag{10}$$

Одновременно S_H является надбавкой, получаемой мастер-узлом $\notin B_{\widetilde{n}}$, следующим сразу за $\widehat{m}$ узлами из $B_{\widetilde{n}}$.

Так как описанная выше ситуация относится к числу маловероятных, то она не может привести в целом к заметному нарушению правила мотивации. Действительно, если например $\widetilde{p} = 0.1$, $m = 10^2$, $\widehat{m} = 5$, то

$$\widetilde{p}^{\,\widehat{m}} \cdot (1 - \widetilde{p})^{m - \widetilde{m}} = 10^{-5} \cdot (0,9)^{95} \tag{11}$$

поскольку $0,9^{95} \ll 10^{-2}$, то вероятность такого события $\ll 10^{-7}$.

Для того, чтобы даже в таких случаях не было сомнений в получении пропорциональной надбавки узлом, следующим за $\widehat{m}$ и не принадлежащим $B_{\widetilde{n}}$, следует ввести функцию, позволяющую более избирательно подходить к "штрафованию" узлов из $B_{\widetilde{n}}$. Например, при достаточно большом M_i (ненамного меньше 1) снижение выплаты таким узлам не происходит или весьма незначительно.

Обозначим эту функцию $\varphi(M)$, $M \in [0,1]$, $\varphi \in [0,1]$. Все M_m принадлежат ее множеству определения. Тогда вознаграждение мастер-узла за закрытие m-го блока в момент t'_m будет равно

$$\gamma_{\varphi_m} = \varphi(M) \cdot \Delta\zeta_\Sigma(t'_m) \tag{12}$$

Функция $\varphi(M)$ является неубывающей. Примером такой функции может быть сигмоида.

$$\varphi(M) = \frac{1}{1 + e^{\lambda(M - M_1)}}, M_1 \in [0,1], \lambda < 0 \tag{13}$$

где $M_1 \in [0,1], \lambda < 0, |\lambda|$ - достаточно велико. В этом случае $\varphi(0) \approx 0$, $\varphi(1) \approx 1$. В качестве примера, пусть $M_1 = 1/2, \lambda = -10$, тогда $\varphi(M) = \dfrac{1}{1 + e^{5 \cdot (1 - 2M)}}$ где значения $\varphi(0) \approx 0,006$, $\varphi(1) \approx 0,994$. Примеры функции при разных значениях M_1 и λ показаны на рис. 2 .

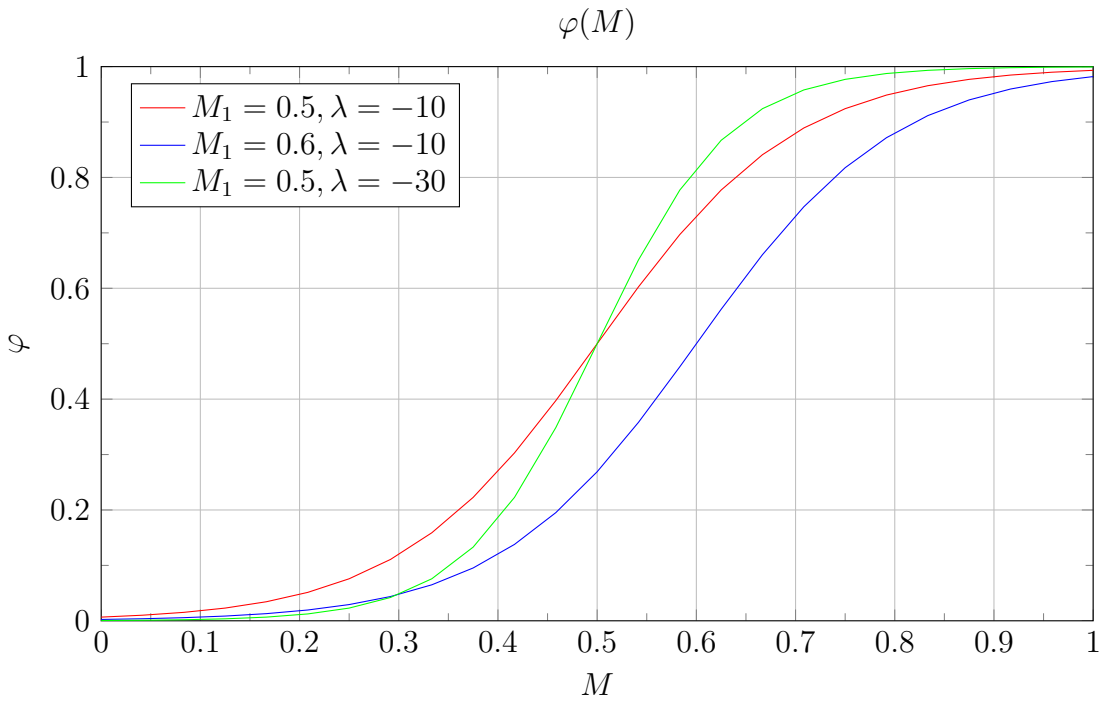

Рис. 2. График гладкой функции φ

Эта функция является гладкой, возможность управления уровнем выплат отражена одним параметром M_1 и при этом невозможно задать интервал значений переменной M, на котором при достаточно больших M не происходит штрафование соответствующего этому значению мастер-узла.

Следующий вариант функции $\varphi(M)$ имеет значительные преимущества перед (13), рис. 3.

$$\varphi(M) = \begin{cases} \dfrac{C}{M_1} \cdot M, & 0 \le M \le M_1\,; \\ \dfrac{1-C}{M_2 - M_1} \cdot M - \dfrac{(1-C)M_1}{M_2 - M_1}, & M_1 \le M \le M_2\,; \\ 1, & M_2 < M \le 1\,. \end{cases} \tag{14}$$

Эту функцию также можно описать как кусочно-линейную функцию

$$\varphi(M) = \frac{1}{2} + \frac{C}{2M_1} \cdot |M| + \frac{(M_1 - CM_2)}{(2(M_2 - M_1) \cdot M_1)} \cdot |M - M1| + \frac{C-1}{2(M_2 - M_1)} \cdot |M - M_2| \tag{15}$$

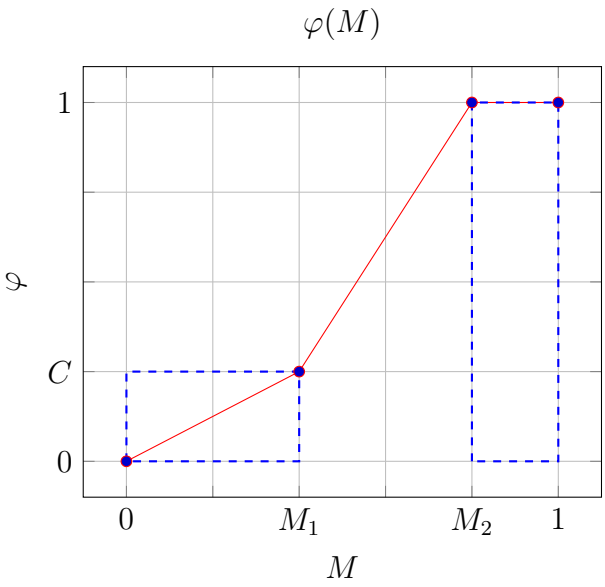

Рис. 3. График непрерывной кусочно-линейной функции φ

Функция (14) позволяет легко “обнулять” надбавки узлам, следующими после текущего мастер-узла за счёт уменьшения M_2 и при необходимости усиливать штрафование узлов с малым M за счёт уменьшения C и, возможно, увеличения M_1.

Благодаря функции (14) рост надбавки в случае закрытия $\widehat{m}$ блоков $\widehat{m}$ мастер-узлами, из $B_{\widetilde{n}}$ подряд может быть полностью остановлен.

Усилить этот эффект можно изменениями правила мотивации: накопленную надбавку получает не первый мастер-узел из $B_n \backslash B_{\widetilde{n}}$, выбранный после мастер-узла из $B_{\widetilde{n}}$, а первый мастер-узел, для которого $\varphi = 1$. Как можно видеть, такой узел может как $\notin B_{\widetilde{n}}$ так и $\in B_{\widetilde{n}}$. В этом случае получение каким-либо мастер-узлом чрезмерной надбавки на $\forall$ конечном интервале времени становится практически невероятным.

Рассмотрим множество $B_{\widehat{n}}$, состоящее из узлов, которые также могут отключаться, как и узлы из $B_{\widetilde{n}}$, но не преднамеренно, а по техническим причинам, и стремящихся эти неполадки устранить. Узлы, не стремящиеся устранить неполадки, относятся к множеству $B_{\overline{n}} \subset B_{\widetilde{n}}$.

Допустим, что состав $B_{\overline{n}} \neq \varnothing$ полностью обновляется за среднее время ΔT. Примерно за время

$$\tau = \left(\left[\frac{n - \overline{n}}{\widehat{n}} \right] + 1 \right) \Delta T \tag{16}$$

Все узлы из $B_n \backslash B_{\overline{n}}$ пройдут по одному разу устранения неполадок, при условии, что время работы $\forall$ узла без неполадок $\geq \tau$. Через время $l \cdot \tau$, где l – достаточно большое натуральное число, все указанные узлы с равной вероятностью l раз подвергнутся воздействию мотивировочного правила, которое будет дополнительным стимулом для как можно более оперативного устранения неполадок.

Следовательно, все узлы из $B_n \backslash B_{\widetilde{n}}$ находятся в равных условиях с точки зрения применения мотивировочного правила, и с учётом результатов, полученных выше, можно сделать вывод о том, что распределение вознаграждения между узлами будет соответствовать их вкладу в работу сети. Более подробно данная модель для узлов из $B_{\overline{n}}$ будет рассмотрена в следующих статьях.

6 Выводы

Предложенный в этой статье подход к оценке вероятности получения узлами блокчейна вознаграждений за закрытие блока, близких к среднему значению, опирающийся на закон больших чисел, показал, что в этом смысле в блокчейне обеспечивается равноправие узлов, постоянно подключённых к сети. Рассмотрение более общего случая, допускающего временное отключение части узлов, показало, что применение специальной функции, управляющей размером вознаграждения, позволяет сохранить равноправие узлов и в подобных случаях.

Список литературы

[1] a@sumus.team, k@sumus.team, rr@sumus.team. “Consensus Algorithm for Bigger Blockchain Networks” (April 27, 2018).

[2] Eric Budish. The Economic Limits of Bitcoin and the Blockchain (June 5, 2018). https://faculty.chicagobooth.edu/

[3] Birkhoff, George D. (December 1931). “Proof of the ergodic theorem” (PDF). Proceedings of the National Academy of Sciences of the United States of America.

[4] Lehmann, Erich L; Romano, Joseph P (2006-03-30). “Weak law converges to constant”. ISBN 9780387276052.

[5] Sunklodas, J. “On normal approximations to stongly mixing random fields”. Theory Probab. Appl., 52(1):125-132, 2010.

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