УДК 004.75 DOI: 10.18698/0236-3933-2022-2-4-17

РАСПРЕДЕЛЕНИЕ ВОЗНАГРАЖДЕНИЯ МЕЖДУ УЗЛАМИ СЕТИ БЛОКЧЕЙН И ПРАВИЛО ИХ МОТИВАЦИИ

А.П. Бардин[1] lovvi@mail.ru
А.В. Новицкий[1] a@sumus.team
Ю.Ю. Шумилов[2, 3] shm@bmstu.ru

[1] **Sumus Company Limited, Гонконг, КНР**
[2] **МГТУ им. Н.Э. Баумана, Москва, Российская Федерация**
[3] **Финансовый университет, Москва, Российская Федерация**

Аннотация

Предложен подход к оценке возможности равноправного получения узлами блокчейна вознаграждения за закрытие блоков. Для описания потоков транзакций и закрытия блоков применена теория случайных процессов. Проанализировано распределение получаемых узлами вознаграждений за закрытие блока, незначительно различающихся по величине и являющихся значениями нормально распределенной случайной величины. Уточнены понятия мастер-узла и пустого блока. Предложена оценка вероятности получения узлами блокчейна вознаграждения за закрытие блока, близкого к среднему значению на основе закона больших чисел. Рассмотрен вариант работы блокчейна, в котором часть узлов отключена от сети. В этом случае распределение вознаграждения между узлами меняется, но равноправие узлов может сохраниться при соблюдении предлагаемых дополнительных условий. Сформулировано правило мотивации узлов для поддержания их постоянного подключения к сети за счет переноса вознаграждения, предназначавшегося узлам, не ответившим на запрос стать мастер-узлом, и суммирования их с вознаграждением для первого узла, ответившего на запрос. Применены специальные функции штрафа, регулирующие размер вознаграждения, что позволяет сохранить равноправие узлов. Рассмотрен более общий случай, допускающий временное отключение части узлов сети блокчейн. Выполнен анализ ситуации, когда узлы отключаются вынужденно по техническим причинам

Ключевые слова

Транзакция, узел, блок, вознаграждение, мотивация, функция штрафа

Поступила 16.07.2021
Принята 13.09.2021

Введение. Вопрос о распределении вознаграждения между узлами сети блокчейн важен для соблюдения равноправия узлов, что является одним из основополагающих принципов блокчейна [1, 2]. Узлы, постоянно подключенные к сети, могут считаться равноправными в том смысле, что вероятность получения любым узлом вознаграждения в момент времени t закрытия блока, значения которого лежат в заданном промежутке времени, зависит только от длительности промежутка времени и числа узлов в сети, имеющих потенциальную возможность закрыть блок [3–5]. Часто возникает ситуация, когда узел, зарегистрированный в сети, не отвечает на обращение к нему. Это приводит к нарушению работы сети блокчейн, например, к задержкам при закрытии блоков и накоплению рассогласования в работе узлов, что отрицательно сказывается на быстродействии сети в целом. Поэтому актуальна разработка правила мотивации узлов для их постоянного подключения к сети.

Постановка задачи. Пусть A_N, $|A_N| = N$ — множество узлов во всей сети блокчейн. Вне зависимости от типа блокчейна будем называть мастер-узлом тот узел, который уполномочен алгоритмом формирования и закрытия блока осуществлять окончательную подпись результатов принятия решения о закрытии блока. Этот узел получает все вознаграждение за закрытие блока. Пусть $B_n \subseteq A_N$, $|B_n| = n$ — множество узлов, которые могут стать мастер-узлами.

Предположим, что размер вознаграждения за проведение транзакции ζ — это функция времени t и в некоторый момент времени t_k $(k = 1, 2, ...)$, соответствующий проведению отдельной транзакции, $\zeta(t_k)$ принимает значение, равное вознаграждению, начисленному за эту транзакцию [2]. Пусть T — множество значений всех t_k, в которые осуществляются транзакции. Множество значений функции $\zeta(t_k)$ обозначим Ψ. Таким образом, $\zeta(t_k)$ — решетчатая неотрицательная функция, заданная на счетном множестве T. Поскольку ζ меняется по закону, который можно установить только статистическими методами, то предположим, что $\zeta(t_k)$ — случайная решетчатая функция или, другими словами, дискретный случайный процесс.

Примем следующие допущения: процесс может быть нестационарным, но при этом эргодическим и слабо коррелированным; для процесса ряды, соответствующие математическому ожиданию и дисперсии, абсолютно сходятся. Пусть плотность распределения процесса $f(\zeta, t_k)$, где $t \in T$, $\zeta \in \Psi$. Функция f не менее непрерывна по ζ, а значит, $\zeta(t_k)$ при фиксированном t_k является непрерывной случайной величиной.

Независимый от ζ процесс закрытия блоков можно представить как дискретный случайный процесс $g(t_m)$, значениями которого являются номера мастер-узлов $j_{\hat{k}}$, определяемые в моменты $t_m \in \left[t'_{m-1},\ t'_m \right)$, $m = 1, 2, \ldots$, где t'_m — момент закрытия блока m; t'_0 — начальный момент работы сети. Множество всех значений t_m обозначим T^*. Здесь принимается предположение о стационарности процесса $g(t_m)$. Это допущение справедливо для достаточно большого числа сетей блокчейн. Например, для сетей семейства pBFT и sdBFT характерно равномерное распределение дискретной случайной величины $j_{\hat{k}}$, $1 \le \hat{k} \le n$, что определяется принятыми в них алгоритмами закрытия блоков [3, 4].

Задача состоит в том, чтобы, исходя из предположения о независимости постоянно присутствующих в сети узлов, определить закон распределения вознаграждения за закрытие блока. Это позволит сделать выводы о соблюдении равноправия узлов в сети блокчейн. Следует также оценить распределение вознаграждения в сети, когда часть узлов подключена к ней непостоянно. Требуется сформулировать правило мотивации узлов для постоянного подключения к сети.

Обоснование нормальности распределения вознаграждения между независимыми постоянно подключенными узлами. В момент времени t_m закрытия блока m мастер-узел $j_{\hat{k}}$, закрывший этот блок, получает всю накопленную к этому моменту сумму вознаграждений за отдельные транзакции $\Delta\zeta_\Sigma$:

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

где k_{m-1} — номер момента времени $t_{k_{m-1}}$,, ближайшего к t'_{m-1} справа, а k_m — номер момента времени 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 $\Delta\zeta_\Sigma\left(t'_m\right)$ является суммой большого числа k случайных величин и, согласно закону больших чисел, при соблюдении допущений, приведенных в постановке задачи, имеет распределение, близкое к нормальному [6–8]:

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

Следовательно, $\Delta\zeta_\Sigma\left(t'_m\right)$ с достаточной точностью является нормальным дискретным случайным процессом при подобных друг другу k функ-

циях плотности вероятности $f\left(\zeta,\ t_k\right)$. Поскольку среднее время закрытия блока второй по популярности сети блокчейн Ethereum [9] равно 30 с, то даже при низкой скорости поступления транзакций в блокчейн, например при ~ 10^2 тран./с, получим $k = 3 \cdot 10^3$. В современных блокчейнах скорость поступления транзакций достигает 10^4 тран./с, поэтому k может достигать значений ~ 10^4.

Следует учитывать, что в сетях блокчейн, например типа Биткойн, возникают так называемые пустые блоки, в составе которых нет пользовательских транзакций, а только транзакции, распределяющие премию за закрытие блока. Эти блоки появлялись в первую эпоху сети Биткойн в связи с недостаточно большим числом пользователей и эмитированных токенов. Со второй по четвертую эпоху пустые блоки появляются из-за ошибки в программном обеспечении участников сети, формирующих блоки. Пустые блоки исключаются из рассмотрения при анализе распределения вознаграждения, поэтому условия применимости закона больших чисел не нарушаются.

Таким образом, каждый узел n может в момент времени t_m стать мастер-узлом с вероятностью p' и в соответствующий момент t'_m получить вознаграждение $\Delta\zeta_{\Sigma(t'_m)}$, значение которого находится, например, в интервале $\left(M_{\Delta\zeta_\Sigma} - 3\sigma_{\Delta\zeta_\Sigma},\ M_{\Delta\zeta_\Sigma} + 3\sigma_{\Delta\zeta_\Sigma}\right)$, с вероятностью $p^* = 0,997p'$, где $M_{\Delta\zeta_\Sigma}$ и $\sigma_{\Delta\zeta_\Sigma}$ — математическое ожидание и среднеквадратическое отклонение случайного процесса (1) в момент времени t'_m.

Например, при равномерном распределении номеров мастер-узлов в момент t'_m каждый узел n получает указанное вознаграждение с вероятностью $0,97/n$. Уменьшение интервала значений $\Delta\zeta_\Sigma\left(t'_m\right)$ в 1,5 раза, приводит к незначительному изменению указанной вероятности.

Приведенные результаты справедливы при достаточно длительных реализациях случайных процессов, т. е. при $m \gg n$ и их эргодичности [10].

Распределение вознаграждения между узлами, не подключенными постоянно. Правило мотивации. Рассмотрим вопрос распределения ζ между узлами в случае, когда не все узлы из множества B_n постоянно присутствуют в сети. Это означает, что есть некоторое подмножество узлов $B_{\tilde{n}} \subseteq B_n$ (полагаем $\tilde{n} < n/3$) такое, что для любого узла из $B_{\tilde{n}}$ справедливо следующее: этот узел выбран мастер-узлом $\overline{m} < m$ раз на отрезке времени $t \in \left[t'_0,\ t^*_m\right)$, но принял задачу по закрытию блока только $\tilde{m}$ раз ($\tilde{m} < \overline{m}$). Для обеспечения правильной работы сети следует стремиться к тому, чтобы все ее узлы были постоянно подключены к сети.

Для уменьшения числа узлов, отключенных от сети на некотором отрезке времени, сформулируем правило мотивации для узлов, стимулирующее их на постоянное подключение к сети: за закрытие текущего блока мастер-узел получает вознаграждение

$$\gamma_m = \frac{\tilde{m}}{\bar{m}} \Delta\zeta_{\Sigma(t'_m)}, \tag{3}$$

остаток вида

$$\frac{\bar{m} - \tilde{m}}{\bar{m}} \Delta\zeta_{\Sigma(t'_m)} \tag{4}$$

суммируется в дальнейшем с $\Delta\zeta_{\Sigma\left(t'_{m+1}\right)}$.

В силу независимости процесса включения/отключения узла в сети от других упомянутых случайных процессов и при предположении о стационарности и равномерности распределения номеров отключаемых узлов можно утверждать, что предложенное правило мотивации, подразумевающее введение мотивирующих коэффициентов $M = \tilde{m}/\bar{m}$, и суммирование остатков с вознаграждением за следующий блок не приведут к изменению классификации случайных процессов, используемых в этой задаче.

Вероятность того, что в произвольный момент времени t_m определения нового мастер-узла им станет непостоянно подключенный узел из $B_{\tilde{n}}$, составит $\tilde{p} = \tilde{n}/n$. Тогда в момент времени t'_m закрытия блока m с данным мастер-узлом этот узел получит вознаграждение $\frac{\tilde{m}}{m}\Delta\zeta_{\Sigma(t'_m)}$. Если следующий мастер-узел не принадлежит множеству $B_{\tilde{n}}$, то в момент времени t'_{m+1} он получит вознаграждение

$$\Delta\zeta_{\Sigma\left(t'_{m+1}\right)} + \frac{\bar{m} - \tilde{m}}{m} \Delta\zeta_{\Sigma}\left(t'_m\right). \tag{5}$$

В момент времени t'_{m+2} новый мастер-узел (если он вновь не принадлежит множеству $B_{\tilde{n}}$) получит за закрытие $m+2$ блоков $\Delta\zeta_{\Sigma\left(t'_{m+2}\right)}$ вознаграждение без надбавок. В этом случае перенос выплаты $\frac{\bar{m}-\tilde{m}}{m}\Delta\zeta_{\Sigma(t'_m)}$ станет надбавкой к вознаграждению соответствующего мастер-узла, тем самым мотивируя все узлы из множества B_n быть постоянно подключенными к сети. Это не приведет к неконтролируемому росту надбавок к $\Delta\zeta$. Если новый мастер-узел принадлежит множеству $B_{\tilde{n}}$, то в момент времени t'_{m+2} повторится ситуация, сложившаяся в момент времени t'_m, а значит,

если появление мастер-узлов из множества $B_{\tilde{n}}$ происходит не подряд, а хотя бы через одного, то накопления надбавок не происходит.

Пусть на отрезке $\left[t'_m,\ t^*_m \right]$ из m мастер-узлов $\hat{m}$ оказались из множества $B_{\tilde{n}}$ (с возможными повторными назначениями одних и тех же узлов мастер-узлами).

Согласно биномиальному распределению, вероятность этого запишем в виде

$$P_{\hat{m},\, m} = C_m^{\hat{m}}\, \tilde{p}^{\hat{m}} \left(1 - \tilde{p}\right)^{m - \hat{m}}. \tag{6}$$

Вероятность события «из m опытов $\hat{m}$ раз появляется номер узла из $B_{\tilde{n}}$» равна

$$\tilde{p}^{\tilde{m}} \left(1 - \tilde{p}\right)^{m - \tilde{m}}, \tag{7}$$

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

Предположим, что $\overline{\Delta\zeta_\Sigma} = \max\limits_{i = 1, \ldots, \hat{m}} \Delta\zeta_\Sigma \left(t'_{k_i} \right)$, тогда оценка суммы вознаграждений в целом за закрытие $\hat{m}$ блоков принимает значение $\hat{m}\, \Delta\zeta$; оценка суммы выплаченных вознаграждений — $\hat{m}\, M_{\min}\, \overline{\Delta\zeta}$ (учитывая невыплату надбавки).

Верхнюю оценку суммы невыплаченных вознаграждений за $\hat{m}$ шагов можно представить так:

$$\hat{m} \left(1 - M_{\min}\right) \overline{\Delta\zeta}. \tag{8}$$

При достаточно большом $\hat{m}$ в момент времени $t_{k_{\hat{m}} + 1}$ первый мастер-узел, не принадлежащий множеству $B_{\tilde{n}}$, помимо $\Delta\zeta_\Sigma \left(t_{k_{\hat{m}} + 1} \right)$ получит

надбавку, оцениваемую по формуле (8), которая может оказаться чрезмерно большой.

Сумма S выплаченных вознаграждений составляет

$$S = \sum_{i=1}^{\hat{m}} \Delta\zeta_{\Sigma}\left(t'_{k_i}\right) M_i, \tag{9}$$

а сумма $S_{\text{н}}$ невыплаченных вознаграждений за закрытие $\hat{m}$ блоков будет равна

$$S_{\text{н}} = \sum_{i=1}^{\hat{m}} \Delta\zeta_{\Sigma}\left(t'_{k_i}\right) - S = \sum_{i=1}^{\hat{m}} \left(1 - M_i\right) \Delta\zeta_{\Sigma}\left(t'_{k_i}\right). \tag{10}$$

Одновременно $S_{\text{н}}$ является надбавкой, получаемой мастер-узлом, не принадлежащим множеству $B_{\tilde{n}}$, следующим сразу за $\hat{m}$ узлами из множества $B_{\tilde{n}}$.

Поскольку приведенная ситуация относится к числу маловероятных, то она не может привести в целом к заметному нарушению правила мотивации.

Например, если $\tilde{p} = 0{,}1,\ m = 10^2,\ \hat{m} = 5,$ то

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

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

Функции штрафа для неподключенных узлов. Для того чтобы даже в этих случаях не было сомнений в получении пропорциональной надбавки узлом, следующим за $\hat{m}$ и не принадлежащим множеству $B_{\tilde{n}}$, следует ввести функцию, позволяющую более избирательно подходить к «штрафованию» узлов из множества $B_{\tilde{n}}$. Например, при достаточно большом M_i (ненамного меньше единицы) снижение выплаты таким узлам не происходит или весьма незначительно.

Обозначим эту функцию как $\varphi(M),\ \ M \in \left[0, 1\right],\ \ \varphi \in \left[0, 1\right]$. Все M_m принадлежат ее множеству определения. Тогда размер вознаграждения мастер-узла за закрытие блока в момент времени t'_m будет составлять

$$\gamma_{\varphi m} = \varphi(M) \Delta\zeta_{\Sigma}\left(t'_m\right). \tag{12}$$

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

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

где $M_1 \in [0, 1]$, $\lambda < 0$, $|\lambda|$ достаточно велик, в этом случае $\varphi(0) \approx 0$, $\varphi(1) \approx 1$.

В качестве примера приведем $M_1 = 1/2$, $\lambda = -10$, тогда $\varphi(M) = \frac{1}{1 + e^{5(1-2M)}}$, где значения $\varphi(0) \approx 0,006$, $\varphi(1) \approx 0,994$. Примеры функции при разных значениях M_1 и λ показаны на рис. 1.

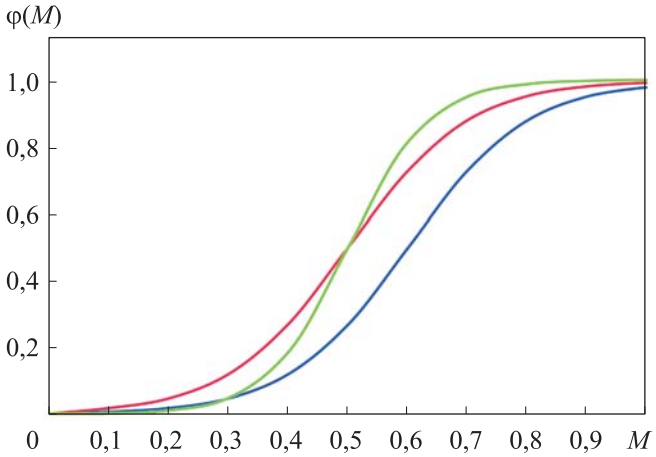

Рис. 1. График гладкой функции штрафа при $M_1 = 0,5$, $\lambda = -10$ (красная кривая); $M_1 = 0,6$, $\lambda = -10$ (синяя); $M_1 = 0,5$, $\lambda = -30$ (зеленая)

Эта функция является гладкой, регулирование уровня выплат осуществляется с помощью параметра 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 функцией (13):

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

Эту функцию штрафа также можно описать как кусочно-линейную [11]:

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

$$+ \frac{C-1}{2(M_2 - M_1)}|M - M_2|. \qquad (15)$$

Функция (14) позволяет легко обнулять надбавки узлам, следующим после текущего мастер-узла, за счет уменьшения M_2 и, если необходимо, усиливать штрафование узлов с малым M за счет уменьшения C и, возможно, увеличения M_1. График этой функции приведен на рис. 2.

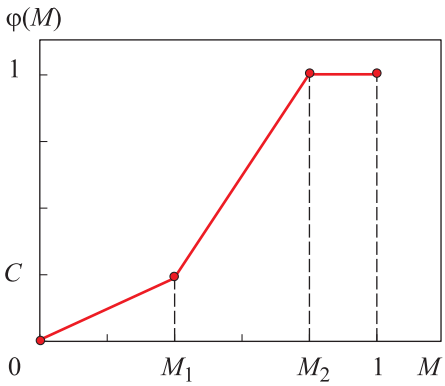

Рис. 2. График непрерывной кусочно-линейной функции штрафа

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

Усилить этот эффект можно, изменяя правило мотивации: накопленную надбавку получает не первый мастер-узел из множества $B_n \setminus B_{\tilde{n}}$, выбранный после мастер-узла из множества $B_{\tilde{n}}$, а первый мастер-узел, для которого $\varphi = 1$. Такой узел может как принадлежать, так и не принадлежать множеству $B_{\tilde{n}}$. В этом случае получение каким-либо мастер-узлом чрезмерной надбавки на любом конечном интервале времени становится маловероятным.

Рассмотрим множество $B_{\hat{n}}$, состоящее из узлов, которые могут отключаться, как и узлы из множества $B_{\tilde{n}}$, но не преднамеренно, а по техническим причинам и которые стремятся эти причины (неполадки) устранить. Узлы, не стремящиеся устранить неполадки, принадлежат множеству $B_{\bar{n}} \subset B_{\tilde{n}}$.

Допустим, что состав непустого множества $B_{\bar{n}}$ полностью обновляется за среднее время ΔT, тогда примерно за время

$$\tau = \left(\left[\frac{n - \bar{n}}{\hat{n}} \right] + 1 \right) \Delta T \qquad (16)$$

все узлы из множества $B_n \setminus B_{\bar{n}}$ пройдут по одному разу устранение неполадок при условии, что время работы любого узла без неполадок не меньше τ. Через время $l\tau$, где l — достаточно большое натуральное число,

все указанные узлы с одинаковой вероятностью один раз подвергнутся воздействию правила мотивации [12–15], которое будет дополнительным стимулом для как можно более оперативного устранения неполадок.

Следовательно, все узлы из множества $B_n \setminus B_{\tilde{n}}$ находятся в равных условиях с точки зрения применения правила мотивации и с учетом полученных результатов можно сделать вывод о том, что распределение вознаграждения между узлами будет соответствовать их вкладу в работу сети.

Заключение. Предложенный подход к оценке вероятности получения узлами блокчейна вознаграждения за закрытие блока, близких к среднему значению, опирающийся на закон больших чисел, показал, что в определенном интервале значений вознаграждения, граница которого зависит от значения среднеквадратического отклонения, можно говорить о равноправии в блокчейне узлов, постоянно подключенных к сети. Это равноправие понимается как возможность каждого узла, ставшего мастер-узлом, с высокой вероятностью получить вознаграждение, значение которого находится в заданном интервале. Чем больше значение среднеквадратического отклонения, тем меньше равноправие узлов, поскольку даже при выполнении правила трех сигм различие в размерах получаемых разными узлами вознаграждений возрастает. Рост среднеквадратического отклонения может быть связан с возникновением разного рода коалиций узлов в сети блокчейн, преследующих свои интересы в ущерб интересам большинства узлов. Разработка методов выявления этих коалиций и их структуры будет предметом дальнейших исследований.

Сформулировано правило мотивации узлов для поддержания их постоянного подключения к сети за счет переноса вознаграждения, предназначавшегося узлам, не ответившим на запрос стать мастер-узлом, и суммирования его с вознаграждением для первого узла, ответившего на запрос. При этом узел, вновь подключившийся к сети после отсутствия в ней некоторое время, став мастер-узлом, получит первое вознаграждение, уменьшенное пропорционально числу обращений к нему, оставленных без ответа.

Рассмотрение более общего случая, допускающего временное отключение некоторого подмножества узлов, показало, что применение специальных функций штрафа, регулирующих размер вознаграждения, позволяет сохранить равноправие узлов и в этом случае. Применение правила мотивации к узлам, временно отключенным от сети для устранения технических неполадок, позволяет стимулировать их владельцев на максимальное ускорение процесса восстановления работоспособности узла.

Показано, что наиболее удобными для практического использования являются кусочно-линейные функции штрафа, поскольку они позволяют достаточно гибко и локально настраивать свойства функций для более точного применения правила мотивации.

ЛИТЕРАТУРА

[1] Satoshi N. Bitcoin: a peer-to-peer electronic cash system. *bitcoin.org*: *веб-сайт.* URL: https://bitcoin.org/en/bitcoin-paper (дата обращения: 20.01.2018).

[2] Chepurnoy A., Larangeira M., Ojiganov A. Rollerchain, a blockchain with safely pruneable full blocks. *arXiv preprint arXiv:1603.07926*, 2016.
DOI: https://doi.org/10.48550/arXiv.1603.07926

[3] Transactions speeds: how do cryptocurrencies stack up to Visa or PayPal? *howmuch.net: веб-сайт*.
URL: https://howmuch.net/articles/crypto-transaction-speeds-compared (дата обращения: 12.08.2019).

[4] Proof of stake versus proof of work. *bitfury.com: веб-сайт*.
URL: http://bitfury.com/content/5-white-apersresearch/pos-vs-pow-1.0.2.pdf (дата обращения: 02.10.2019).

[5] Budish E. The economic limits of bitcoin and the blockchain. *NBER Working Paper Series*, 2018, no. 24717. URL: http://www.nber.org/papers/w24717 (дата обращения: 04.04.2022).

[6] Сенатов В.В. Центральная предельная теорема. Точность аппроксимации и асимптотические разложения. М., Либроком, 2009.

[7] Де Гроот М. Оптимальные статистические решения. М., Мир, 1974.

[8] Lehmann E.L., Romano J.P. Testing statistical hypotheses. Springer Science + + Business Media, 2005.

[9] Ethereum. *bits.media: веб-сайт*. URL: https://bits.media/ethereum (дата обращения: 26.05.2020).

[10] Кудрявцев К.Я. Доказательство нормальности распределения подмножества случайных величин на основе преобразования блочных матриц. *Вестник НИЯУ МИФИ*, 2021, т. 10, № 1, с. 70–76.
DOI: https://doi.org/10.1134/S2304487X21010107

[11] Шумилов Ю.Ю., Шумилов Б.Ф. Аналитическое описание многомерных многозначных функций в системах управления. В кн.: Методы проектирования сложных систем. М., Энергоатомиздат, 1985, с. 42–48.

[12] Деон А.Ф., Меняев Ю.А. Полное факториальное моделирование равномерных последовательностей целых случайных величин. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2017, № 5 (116), с. 132–149.
DOI: https://doi.org/10.18698/0236-3933-2017-5-132-149

[13] Applebaum B. Pseudorandom generators with long stretch and low locality from random local one-way functions. *Proc. 44th Ann. ACM STOC*, 2012, pp. 805–816.
DOI: https://doi.org/10.1145/2213977.2214050

[14] Lewis T.G., Payne W.H. Generalized feedback shift register pseudorandom number algorithm. *J. ACM*, 1973, vol. 20, no. 3, pp. 456–486.
DOI: https://doi.org/10.1145/321765.321777

[15] Sunklodas J. On normal approximations to strongly mixing random fields. *Theory Probab. Appl.*, 2010, vol. 52, no. 1, pp. 125–132.
DOI: https://doi.org/10.1137/S0040585X97982815

Бардин Алексей Павлович — директор по исследованиям и разработкам компании Sumus Company Limited (2103, 21/F, Tower 1, Lippo Centre, 89 Queensway, Admiralty, Hong Kong).

Новицкий Анатолий Викторович — технический директор компании Sumus Company Limited (2103, 21/F, Tower 1, Lippo Centre, 89 Queensway, Admiralty, Hong Kong).

Шумилов Юрий Юрьевич — д-р техн. наук, профессор кафедры «Прикладная математика» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1); профессор департамента информационной безопасности Финансового университета (Российская Федерация, 125993, Москва, Ленинградский пр-т, д. 49).

Просьба ссылаться на эту статью следующим образом:

Бардин А.П., Новицкий А.В., Шумилов Ю.Ю. Распределение вознаграждения между узлами сети блокчейн и правило их мотивации. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2022, № 2 (139), с. 4–17.
DOI: https://doi.org/10.18698/0236-3933-2022-2-4-17

DISTRIBUTION OF FEE BETWEEN BLOCKCHAIN NODES AND THE RULE OF THEIR MOTIVATION

A.P. Bardin[1] lovvi@mail.ru
A.V. Novitskiy[1] a@sumus.team
Yu.Yu. Shumilov[2, 3] shm@bmstu.ru

[1] **Sumus Company Limited, Hong Kong, China**
[2] **Bauman Moscow State Technical University, Moscow, Russian Federation**
[3] **Financial University, Moscow, Russian Federation**

Abstract

The article cconsiders the proposed approach for assessing the possibility of equitable receipt of fees by blockchain nodes for closing blocks. The theory of random processes is applied to describe transaction flows and block closings. The distribution of fees received by the nodes for closing a block is analyzed.

Keywords

Transaction, node, block, fee, motivation, penalty function

The fees are the values of a normally distributed random variable and they differ slightly in value. The concept of a master node and an empty block is specified. An estimate of the probability of fee receiving by blockchain nodes for closing a block which are close to the average value is proposed based on the law of large numbers. The variant of the operation of the blockchain network, in which some of the nodes are disconnected from the network, is considered. In this case, the distribution of fees between the nodes is changed, but the equality of the nodes can still be preserved if the proposed additional conditions are met. A rule is formulated for motivating nodes to maintain their constant connection to the network by transferring fees intended for nodes that did not respond to the request to become a master node and summing them with the fee for the first node that responded to the request. Special penalty functions regulating the amount of the fee are applied, which makes it possible to maintain the equality of nodes in this case as well. The more general case allowing temporary shutdown of a part of the nodes of the blockchain network is considered. The analysis of the situation when the nodes are forced to shut down for technical reasons is performed

Received 16.07.2021
Accepted 13.09.2021

REFERENCES

[1] Satoshi N. Bitcoin: a peer-to-peer electronic cash system. *bitcoin.org: website*. Available at: https://bitcoin.org/en/bitcoin-paper (accessed: 20.01.2018).

[2] Chepurnoy A., Larangeira M., Ojiganov A. Rollerchain, a blockchain with safely pruneable full blocks. *arXiv preprint arXiv:1603.07926*, 2016.
DOI: https://doi.org/10.48550/arXiv.1603.07926

[3] Transactions speeds: how do cryptocurrencies stack up to Visa or PayPal? *howmuch.net: website*.
Available at: https://howmuch.net/articles/crypto-transaction-speeds-compared (accessed: 12.08.2019).

[4] Proof of stake versus proof of work. *bitfury.com: website*.
Available at: http://bitfury.com/content/5-white-apersresearch/pos-vs-pow-1.0.2.pdf (accessed: 02.10.2019).

[5] Budish E. The economic limits of bitcoin and the blockchain. *NBER Working Paper Series*, 2018, no. 24717. Available at: http://www.nber.org/papers/w24717 (accessed: 04.04.2022).

[6] Senatov V.V. Tsentral'naya predel'naya teorema. Tochnost' approksimatsii i asimptoticheskie razlozheniya [Central-limit theorem. Approximation accuracy and asymptotic expansions]. Moscow, Librokom Publ., 2009.

[7] De Groot M. Optimal statistical decisions. John Wiley & Sons, 2004.

[8] Lehmann E.L., Romano J.P. Testing statistical hypotheses. Springer Science + + Business Media, 2005.

[9] Ethereum. *bits.media: website*. Available at: https://bits.media/ethereum (accessed: 26.05.2020).

[10] Kudryavtsev K.Ya. Proof of normality of distribution of a subset of random variables based on the transformation of block matrices. *Vestnik NIYaU MIFI*, 2021, vol. 10, no. 1, pp. 70–76 (in Russ.). DOI: https://doi.org/10.1134/S2304487X21010107

[11] Shumilov Yu.Yu., Shumilov B.F. Analiticheskoe opisanie mnogomernykh mnogoznachnykh funktsiy v sistemakh upravleniya [Analytic description of multidimensional multivalue functions in control systems]. V kn.: Metody proektirovaniya slozhnykh system [In: Design methods for complex systems]. Moscow, Energoatomizdat Publ., 1985, pp. 42–48 (in Russ.).

[12] Deon A.F., Menyaev Yu.A. Complete factorial simulation of integer random number uniform sequences. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2017, no. 5 (116), pp. 132–149 (in Russ.).
DOI: https://doi.org/10.18698/0236-3933-2017-5-132-149

[13] Applebaum B. Pseudorandom generators with long stretch and low locality from random local one-way functions. *Proc. 44th Ann. ACM STOC*, 2012, pp. 805–816. DOI: https://doi.org/10.1145/2213977.2214050

[14] Lewis T.G., Payne W.H. Generalized feedback shift register pseudorandom number algorithm. *J. ACM*, 1973, vol. 20, no. 3, pp. 456–486.
DOI: https://doi.org/10.1145/321765.321777

[15] Sunklodas J. On normal approximations to strongly mixing random fields. *Theory Probab. Appl.*, 2010, vol. 52, no. 1, pp. 125–132.
DOI: https://doi.org/10.1137/S0040585X97982815

Bardin A.P. — Chief Research and Development Officer, Sumus Company Limited (2103, 21/F, Tower 1, Lippo Centre, 89 Queensway, Admiralty, Hong Kong, China).

Novitskiy A.V. — Chief Technology Officer, Sumus Company Limited (2103, 21/F, Tower 1, Lippo Centre, 89 Queensway, Admiralty, Hong Kong, China).

Shumilov Yu.Yu. — Dr. Sc. (Eng.), Professor, Department of Applied Mathematics, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation); Professor, Department of Information Security, Financial University (Leningradskiy prospekt 49, Moscow, 125993 Russian Federation).

Please cite this article in English as:

Bardin A.P., Novitskiy A.V., Shumilov Yu.Yu. Distribution of fee between blockchain nodes and the rule of their motivation. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2022, no. 2 (139), pp. 4–17 (in Russ.). DOI: https://doi.org/10.18698/0236-3933-2022-2-4-17