Подходы к построению функций, управляющих эмиссией crypto assets, при заданных исходных параметрах

noise@sumus.team, k@sumus.team, a@sumus.team

22 ноября 2018 г.

Аннотация

Постоянно возникает вопрос, как для систем в которых обращаются crypto assets проводить их эмиссию. Существуют различные подходы, кто-то наделяет один центр полномочиями по эмиссии crypto assets, а кто-то реализует функцию как алгоритм.

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 и слабую коррелированность. Также будем считать, что у этого процесса есть математическое ожидание и дисперсия. 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, $k = 1, \dots, n$,

$1 \leq j_k \leq N$ 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 $\Delta fee_\Sigma(t_m^{'})$ является суммой большого числа случайных величин и согласно закону больших чисел (здесь считаются выполненными условия теоремы Маркова и Чебышева для дисперсии), имеет распределение близкое к нормальному, т.е.:

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

и является при произвольных, но подобных $f(fee,)$ дискретным случайным 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 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 фиксированное 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 $\bar{m} < m$ 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 $\Delta fee_\Sigma(t_{m+1}^{'})$. Ленивых НОД не может быть больше $\frac{n}{3}$. Можно сказать, что в данном разделе 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 $M = \dfrac{\widetilde{m}}{\bar{m}}$, $1 - M = 1 - \dfrac{\widetilde{m}}{\bar{m}}$ /не понял эту формулу/и перенос остатков не приведёт 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 $\dfrac{\widetilde{m}}{m}\Delta fee_\Sigma(t^{'}_m)$. Если следующий мастер-узел не принадлежит $B_{\widetilde{n}}$, то в момент $t^{'}_{m+1}$ он получит вознаграждение

$$\Delta fee_\Sigma(t^{'}_{m+1}) + \frac{\bar{m} - \widetilde{m}}{m} \cdot \Delta fee_\Sigma(t^{'}_m) \tag{5}$$

В момент $t^{'}_{m+2}$ новый мастер-узел, если он вновь не принадлежит $B_{\widetilde{n}}$, то получит за закрытие $m+2$ блока $\Delta fee_\Sigma(t^{'}_{m+2})$ уже без "надбавок" и в этом случае перенос выплаты $\dfrac{\bar{m} - \widetilde{m}}{m} \cdot \Delta fee_\Sigma(t^{'}_m)$ станет надбавкой соответствующему мастер-узлу, стимулируя стремления всех узлов из B_n быть постоянно подключёнными и это не приведёт к неконтролируемому росту "надбавок" к Δfee. Если новый мастер-узел $\in B_{\widetilde{n}}$, то в момент $t^{'}_{m+2}$ повториться ситуация сложившаяся в момент $t^{'}_m$ и это значит, что если появление мастер-узлов из $B_{\widetilde{n}}$ идёт не подряд, а хотя бы "через один", то накопленные премии не происходит.

Пусть на отрезке $[t^{'}_0, t^*_m]$ из m мастер-узлов $\hat{m}$ оказались из $B_{\widetilde{n}}$ (с возможными повторными назначениями одних и тех же узлов мастер-узлами). Вероятность этого есть биноминальное распределение

$$P_{\widetilde{m},m} = C^{\hat{m}}_m \cdot \widetilde{p}^{\,\hat{m}} \cdot (1 - \widetilde{p})^{m - \widetilde{m}} \tag{6}$$

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

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

если выбирать только один набор $t^*_{k_i}$, $i = 1, \ldots, \widetilde{m}$, $1 \le k_j \le m$, в котором появляются мастер-узлы из $B_{\widetilde{n}}$. Наиболее "критичным" с точки зрения накопления надбавки является вариант, когда закрывается $\hat{m}$ блоков подряд, 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 премии $\max\limits_{i=1,\ldots,\hat{m}} \left\{ \dfrac{\bar{m}_{k_i} - \widetilde{m}_{k_i}}{\bar{m}_{k_i}} \right\} = M_{\max} < 1$, соответственно $M_{\min} = \min\limits_{i=1,\ldots,\hat{m}} \left\{ \dfrac{\widetilde{m}_{k_i}}{\bar{m}_{k_i}} = M_{k_i} \right\} < 1$. Очевидно, что для $M_{\max}$ и $M_{\min}$ получаются при одном и том же M_{k_i}. Т.е. $M_{\max} = 1 - M_{\min}$.

Положим $\overline{\Delta fee_\Sigma} = \max\limits_{i=1,\ldots,\hat{m}} \Delta fee_\Sigma(t^{'}_{k_i})$ Оценка суммы вознаграждения в целом за закрытие $\hat{m}$ блоков в этом случае $\hat{m} \cdot \Delta fee$. Оценка суммы выплаченных вознаграждений есть $\hat{m} \cdot M_{\min} \cdot \Delta fee$ (учитывая невыплату надбавки). Верхняя оценка суммы невыплаченного вознаграждения за $\hat{m}$ шагов есть $\hat{m} \cdot (1 - M_{\min}) \cdot \overline{\Delta fee}$ При достаточно большом $\hat{m}$ в момент $t_{k\hat{m}+1}$ первый мастер узел, не принадлежащий $B_{\widetilde{n}}$ помимо $\Delta fee_\Sigma(t_{k\hat{m}+1})$ получит надбавку $\hat{m} \cdot (1 - M_{\min}) \cdot \overline{\Delta fee}$ которая может оказаться чрезмерно большой.

Если не использовать оценки надбавок и вознаграждений, которые введены для сокращения выкладок, и сохранить точные значения, то приведённые выше выводы останутся справедливыми.

Действительно, сумма выплаченных вознаграждений S есть

$$S = \sum_{i=1}^{\hat{m}} \Delta fee_{\Sigma}(t'_{k_i}) \cdot M_i \tag{8}$$

а сумма S_M невыплаченных вознаграждений за закрытие $\hat{m}$ блоков будет равна:

$$S_M = \sum_{i=1}^{\hat{m}} \Delta fee_{\Sigma}(t'_{k_i}) - S = \sum_{i=1}^{\hat{m}} (1 - M_i) \Delta fee_{\Sigma}(t'_{k_i}) \tag{8a}$$

Одновременно S_M является надбавкой, получаемой мастер узлом $\notin B_{\tilde{n}}$, следующим сразу за $\hat{m}$ узлами из $B_{\tilde{n}}$.

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

$$\widetilde{p}^{\,\hat{m}} \cdot (1 - \widetilde{p})^{m - \widetilde{m}} = 10^{-5} \cdot (0.9)^{95} \tag{9}$$

поскольку $0.9^{95} \ll 10^{-2}$, то вероятность такого события $\ll 10^{-7}$.

Однако для того, чтобы даже в таких случаях не было сомнений в получении пропорциональной надбавки узлом, следующим за $\hat{m}$ и не принадлежащим $B_{\tilde{n}}$, следует ввести функцию, позволяющую более дифференцированно подходить к “штрафованию” узлов из $B_{\tilde{n}}$. Например, ппр идостаточно большом M_i (ненамного меньше 1) снижение выплаты таким узлам не происходит.

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

$$\gamma_{\varphi} = \varphi(M) \cdot \Delta fee_{\Sigma}(t'_m) \tag{10}$$

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

$$\varphi(M) = \frac{\arctan(M - M_1) + \arctan(M_1)}{\arctan(1 - M_1) + \arctan(M_1)}, M_1 \in [0, 1] \tag{11}$$

графики функции при разных значениях M_1 показаны на рисунке 1

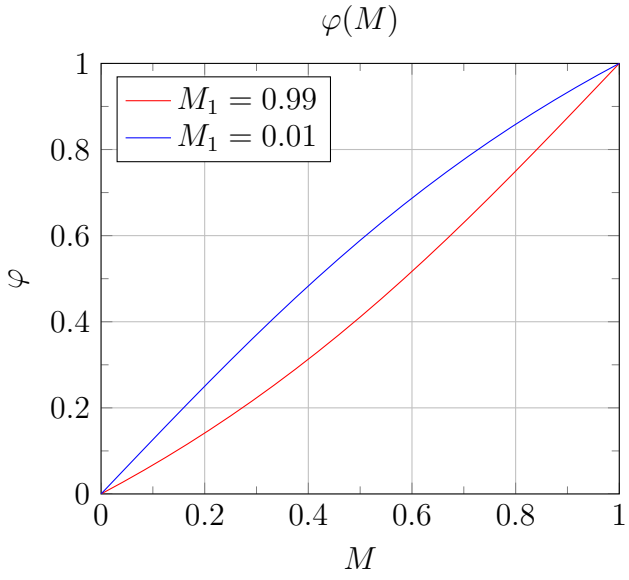

Рис. 1. График гладкой функции φ

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

Следующий вариант функции $\varphi(M)$ имеет значительные преимущества перед 11, см. рис. 2

$$\varphi(M) = \begin{cases} \dfrac{C}{M_1} \cdot M, & 0 \le M \le M_1; \\ \dfrac{1-C}{M_2 - M_1} \cdot M - \dfrac{(1-C)M_1}{M_2 - M_1}, & M_1 \le M \le M_2; \\ 1, & M_2 < M \le 1. \end{cases} \tag{12}$$

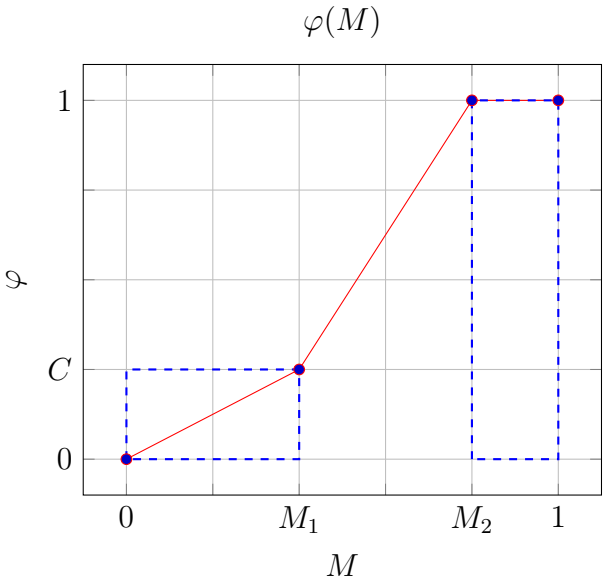

Рис. 2. График дискретной функции φ

Функция (12) позволяет легко “обнулять” надбавки следующими после текущего мастер-узлам за счёт уменьшения M_2, и при необходимости усиливать штрафование узлов с малым M за счёт уменьшения C и, возможно, увеличения M.

Благодаря функции (12) рост надбавки в случае закрытия $\hat{m}$, блоков $\hat{m}$ мастер-узлами узлами из $B_{\tilde{n}}$ подряд может быть полностью остановлен.

Усилить этот эффект можно изменениями привали мотивации: накопленную надбавку получает на первый мастер мастер-узел из $B_n \backslash B_{\tilde{n}}$, выбранный после мастер-узла из $B_{\tilde{n}}$, а первый мастер-узел, для которого $\varphi = 1$. В этом случае получение каким-либо мастер-узлом чрезмерной надбавки на $\forall$ конечном интервале времени становится практически невероятным.

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

Допустим, что состав $B_{\hat{n}}$ полностью обновляется за среднее время ΔT. К обновляемым относится также множество $B_{\hat{n}} = \varnothing$. Примерно за время

$$\tau = \left(\left[\frac{n - \bar{n}}{\hat{n}} \right] + 1 \right) \Delta T \tag{13}$$

Все узлы из $B_n \backslash B_{\tilde{n}}$ пройдут по одному разу устранение неполадок, при условии, что время работы $\forall$ узла без неполадок $\ge \tau$. Через время $l \cdot \tau$, где l - достаточно большое натуральное число, все указанные узлы с равной вероятностьюl раз подвергнутся воздействию мотивировочного

правила, которое будет дополнительным стимулом для как можно более оперативного устранения неполадок.

Следовательно, все узлы из $B_n \backslash B_{\tilde{n}}$ 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.

Список литературы

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

.