

Подходы к выбору /проектированию/ функций управляющих эмиссией криптоассетов блокчейна

noise@sumus.team, a@sumus.team

5 мая, 2018

Аннотация

Кажется, что может быть проще чем печатать деньги. Печатай и получай удовольствие ...

1 Введение

Любая система, должна находиться в динамическом равновесии - это аксиома. Для начала опустим выбор диапазона параметров, в котором система находится в состоянии равновесия. Пусть это некие точки a и b с координатами (x_1, y_1) (x_2, y_2) при которых система существует. Если мы выходим из этого диапазона - система деградирует (не важно по каким причинам). Сначала рассмотрим вопрос о распределении fee между узлами для случая, когда все узлы из B_n постоянно присутствуют в сети, то они равноправны в том смысле, что вероятность получения любым узлом в произвольный момент t , соответствует закрытию блока вознаграждения в интервале, величина которого зафиксирована (достигнута) на данный момент, зависит только от величины интервала и количества узлов n .

Система должна управляться, по некому закону в рамках заданных координат. Рассмотрим два способа построения функции управления: первый, это гладкая функция проходящая через две заданные точки, второй - кусочно-постоянная функция.

2 Описание экспоненциальной функции, проходящей через две заданные точки

Пусть заданы две точки: (x_1, y_1) (x_2, y_2) . Нужно найти параметры функции $f(x) = k \cdot e^{\lambda x}$, обеспечивающие ее прохождение через две заданные точки. Запишем для определения k λ два уравнения в начальной и конечной точках:

$$\begin{cases} ke^{\lambda x_1} = y_1 \\ ke^{\lambda x_2} = y_2 \end{cases} \quad (1)$$

Выразим k из первого уравнения (1):

$$k = y_1 e^{-\lambda x_1} \quad (2)$$

Подставив (2) во второе уравнение (1): $y_1 e^{-\lambda(x_2 - x_1)} = y_2$, тогда

$$\lambda = \frac{\ln \frac{y_2}{y_1}}{x_2 - x_1} \quad (3)$$

Подставим (3) в (2) получим

$$k = y_1 \cdot \exp \left[-\frac{\ln \left(\frac{y_2}{y_1} \right)}{(x_2 - x_1)} \cdot x_1 \right] \quad (4)$$

С учетом (3) и (4) запишем

$$f(x) = k \cdot e^{\lambda x} = y_1 \cdot \exp \left[\frac{\ln \left(\frac{y_2}{y_1} \right)}{x_2 - x_1} \cdot (x - x_1) \right] \quad (5)$$

Эта функция имеет выпуклость *help* во всех точках множества представления. Замечание: если решать систему управлений (1) в другом порядке, то снова получится решение (5) Пример. Пусть $x_1 = 1; y_1 = 1; x_2 = 2; y_2 = 2$. Тогда $f(x) = 2^{x-1}$ Вывод. При высоких требованиях к гладкости функции $f(x)$ и низких требованиях к значениям, принимаемым на (x_1, x_2) формула (5) может быть полезной.

График

3 Формула кусочно-постоянной функции

Пусть $f(x)$ Будем считать fee функцией времени t , где в некоторый момент t_k , соответствующий 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, $k = 1, 2, \dots$ Множество значений этой функции обозначим 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 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 $f(fee, t)$, где $t \in T$, $fee \in \Psi$. Функция f не менее чем непрерывна по fee , причём $fee(t_k)$ при фиксированном t_k является непрерывной случайной величиной.

Пусть также имеет место независимый от fee процесс закрытия блоков, который в данном случае можно представить как дискретный случайный процесс $g(t_m)$, значениями которого являются номера мастер-узлов j_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_k , $1 \leq j_k \leq N$. Счётное множество всех значений t_m обозначим T^* .

В момент времени t_m закрытия блока номер m мастер-узел с номером j_k получает всю накопленную к этому моменту Δfee_Σ , которую будем считать равной

$$\Delta fee_\Sigma(t'_m) = \sum_{k=k_{m-1}}^{k_m} fee(t_k) \quad (6)$$

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 решетчатая случайная функция $\Delta fee_\Sigma(t'_m)$ является суммой большого числа случайных величин и согласно закону больших чисел (при соблюдении условий указанных выше), имеет распределение близкое к нормальному, т.е.:

$$F(\Delta fee_\Sigma < a, t)) \approx \Phi(\Delta fee_\Sigma < a, t)) \quad (7)$$

и является при произвольных, но подобных друг-другу при любых k $f(fee, t_k)$ 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 (6) 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.

Рассмотрим теперь вопрос распределения fee между узлами для случая, когда не все узлы из B_n постоянно присутствуют в сети. Это означает, что есть некоторое фиксированное подмножество узлов $B_{\tilde{n}} \subseteq B_n$, $\tilde{n} \leq n$ такое, что для любого узла из $B_{\tilde{n}}$ справедливо следующее: пусть этот узел выбирался мастер-узлом $\tilde{m} < m$ раз на отрезке $t \in [t'_0, t_m)$, но принял задачу по закрытию блока только \tilde{m} раз ($\tilde{m} < \tilde{m}$), то за закрытие текущего блока, выбор эскорта которого осуществлён в момент t_m^* , этот мастер узел получит вознаграждение

$$\gamma_m = \frac{\tilde{m}}{\tilde{m}} \Delta fee_\Sigma(t'_m) \quad (8)$$

остаток

$$\frac{\tilde{m} - \tilde{m}}{\tilde{m}} \Delta fee_\Sigma(t'_m) \quad (9)$$

суммируется в дальнейшем с $\Delta fee_\Sigma(t'_{m+1})$. 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 \tilde{n} отключаемых узлов, можно утверждать, что введение “мотивирующих” коэффициентов $M = \frac{\tilde{m}}{\tilde{m}}$, 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 $B_{\tilde{n}}$, есть $\tilde{p} = \frac{\tilde{n}}{n}$. Тогда в момент t'_m закрытия блока номер m с данным мастер-узлом этот узел получит вознаграждение $\frac{\tilde{m}}{m} \Delta fee_\Sigma(t'_m)$. Если следующий мастер-узел не принадлежит $B_{\tilde{n}}$, то в момент t'_{m+1} он получит вознаграждение

$$\Delta fee_\Sigma(t'_{m+1}) + \frac{\tilde{m} - \tilde{m}}{m} \cdot \Delta fee_\Sigma(t'_m) \quad (10)$$

В момент t'_{m+2} новый мастер-узел, если он вновь не принадлежит $B_{\tilde{n}}$, получит за закрытие $m+2$ блока $\Delta fee_{\Sigma}(t'_{m+2})$ уже без надбавок и в этом случае перенос выплаты $\frac{\tilde{m} - \tilde{m}}{\tilde{m}} \cdot \Delta fee_{\Sigma}(t'_m)$ станет надбавкой соответствующему мастер-узлу, мотивируя все узлы из B_n быть постоянно подключёнными и это не приведёт к неконтролируемому росту надбавок к Δfee . Если новый мастер-узел $\in B_{\tilde{n}}$, то в момент t'_{m+2} повториться ситуация сложившаяся в момент t'_m , и если появление мастер-узлов из $B_{\tilde{n}}$ 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 $B_{\tilde{n}}$ (с возможными повторными назначениями одних и тех же узлов мастер-узлами). Вероятность этого есть, согласно биномиальному распределению

$$P_{\tilde{m}, m} = C_m^{\hat{m}} \cdot \tilde{p}^{\hat{m}} \cdot (1 - \tilde{p})^{m - \hat{m}} \quad (11)$$

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

$$\tilde{p}^{\hat{m}} \cdot (1 - \tilde{p})^{m - \hat{m}} \quad (12)$$

если рассматривать только один набор мастер-узлов, назначаемых в моменты t_{k_i} , $i = 1, \dots, \tilde{m}$, $1 \leq k_j \leq m$, в котором появляются мастер-узлы из $B_{\tilde{n}}$. Наиболее “критичным” с точки зрения накопления надбавки является вариант, когда закрывается \hat{m} блоков подряд, для каждого из которых мастер-узел принадлежал $B_{\tilde{n}}$. Вероятность этого равна (12). Поскольку каждый узел из $B_{\tilde{n}}$ включается и отключается по-своему, то для оценки накопления вознаграждения за счёт надбавки выберем $\max_{i=1, \dots, \hat{m}} \left\{ \frac{\bar{m}_{k_i} - \tilde{m}_{k_i}}{\bar{m}_{k_i}} \right\} = M_{\max} < 1$, соответственно $M_{\min} = \min_{i=1, \dots, \hat{m}} \left\{ \frac{\tilde{m}_{k_i}}{\bar{m}_{k_i}} = M_{k_i} \right\} < 1$. 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 $\overline{\Delta fee_{\Sigma}} = \max_{i=1, \dots, \hat{m}} \Delta fee_{\Sigma}(t'_{k_i})$. Оценка суммы вознаграждения в целом за закрытие \hat{m} блоков в этом случае $\hat{m} \cdot \Delta fee$. Оценка суммы выплаченных вознаграждений есть $\hat{m} \cdot M_{\min} \cdot \overline{\Delta fee}$ (учитывая невыплату надбавки). Верхняя оценка суммы невыплаченного вознаграждения за \hat{m} шагов есть

$$\hat{m} \cdot (1 - M_{\min}) \cdot \overline{\Delta fee} \quad (13)$$

При достаточно большом \hat{m} в момент $t_{k_{\hat{m}+1}}$ первый мастер узел, не принадлежащий $B_{\tilde{n}}$, помимо $\Delta fee_{\Sigma}(t_{k_{\hat{m}+1}})$ получит надбавку, оцениваемую как (13), 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

$$S = \sum_{i=1}^{\hat{m}} \Delta fee_{\Sigma}(t'_{k_i}) \cdot M_i \quad (13a)$$

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

$$S_H = \sum_{i=1}^{\hat{m}} \Delta fee_{\Sigma}(t'_{k_i}) - S = \sum_{i=1}^{\hat{m}} (1 - M_i) \Delta fee_{\Sigma}(t'_{k_i}) \quad (13b)$$

Одновременно S_H 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 $\tilde{p} = 0.1$, $m = 10^2$, $\hat{m} = 5$, то

$$\tilde{p}^{\hat{m}} \cdot (1 - \tilde{p})^{m - \hat{m}} = 10^{-5} \cdot (0.9)^{95} \quad (14)$$

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, при достаточно большом M_i (немного 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

$$\gamma_{\varphi_m} = \varphi(M) \cdot \Delta fee_{\Sigma}(t'_m) \quad (15)$$

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

$$\varphi(M) = \frac{1}{1 + e^{\lambda(M - M_1)}}, M_1 \in [0, 1], \lambda < 0 \quad (16)$$

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

$$\varphi(M) = \frac{1}{1 + e^{5 \cdot (1 - 2M)}}$$

где значения $\varphi(0) \approx 0.006$, $\varphi(1) \approx 0.994$. Примеры функции при разных значениях M_1 и λ показаны на рис. 3

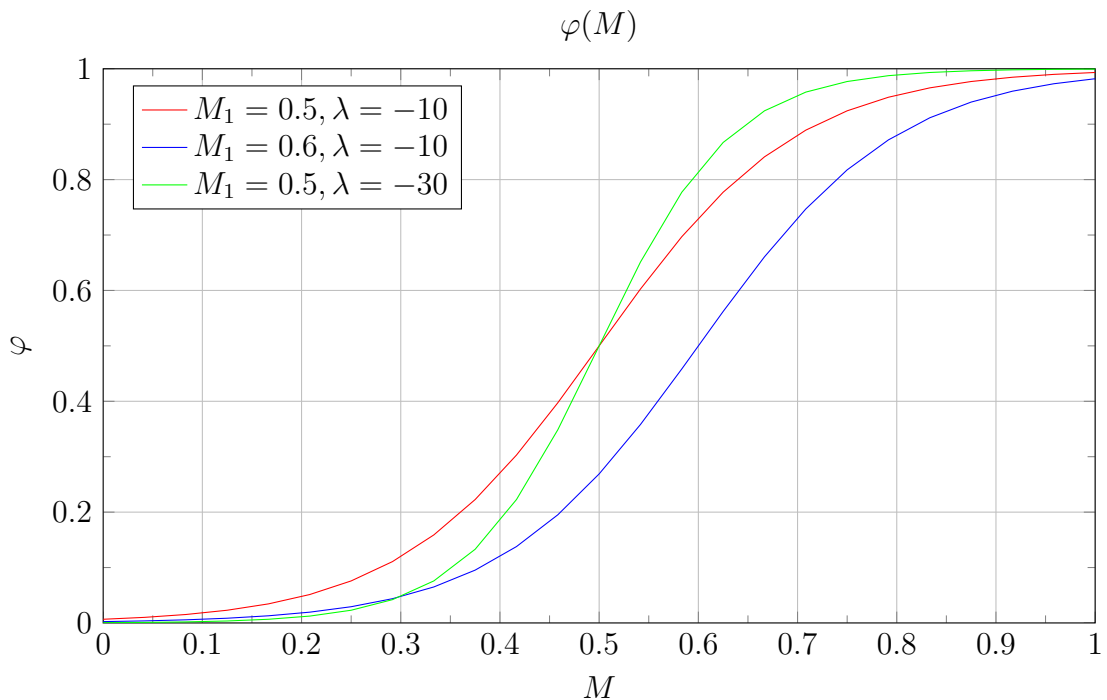


Рис. 1. График гладкой функции φ

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 16, см. рис. 2

$$\varphi(M) = \begin{cases} \frac{C}{M_1} \cdot M, & 0 \leq M \leq M_1; \\ \frac{1-C}{M_2-M_1} \cdot M - \frac{(1-C)M_1}{M_2-M_1}, & M_1 \leq M \leq M_2; \\ 1, & M_2 < M \leq 1. \end{cases} \quad (17)$$

Эту функцию, также можно записать линейно.

$$\varphi(M) = \frac{1}{2} + \frac{C}{2M_1} \cdot |M| + \frac{(M_1 - CM_2)}{(2(M_2 - M_1) \cdot M_1)} \cdot |M - M_1| + \frac{C - 1}{2(M_2 - M_1)} \cdot |M - M_2| \quad (17a)$$

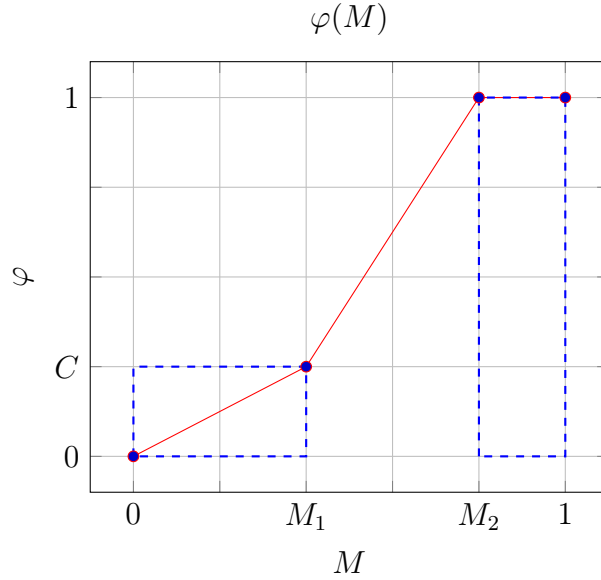


Рис. 2. График дискретной функции φ

Функция (17) 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 (17) рост надбавки в случае закрытия \hat{m} блоков мастер-узлами, из $B_{\hat{n}}$ подряд может быть полностью остановлен.

Усилить этот эффект можно изменениями правила мотивации: накопленную надбавку получает не первый мастер-узел из $B_n \setminus B_{\hat{n}}$, выбранный после мастер-узла из $B_{\hat{n}}$, а первый мастер-узел, для которого $\varphi = 1$. Как можно видеть, такой узел может как $\notin B_{\hat{n}}$ так и $\in B_{\hat{n}}$. 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 $B_{\hat{n}}$, но не преднамеренно, а по техническим причинам, и стремящихся эти неполадки устранить. Узлы, не стремящиеся устранить неполадки, относятся к множеству $B_{\hat{n}} \subset B_{\hat{n}}$.

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

время

$$\tau = \left(\left\lceil \frac{n - \bar{n}}{\hat{n}} \right\rceil + 1 \right) \Delta T \quad (18)$$

Все узлы из $B_n \setminus B_{\bar{n}}$ 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 $B_n \setminus B_{\bar{n}}$ 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 $B_{\bar{n}}$ будет рассмотрена в следующих статьях.

Список литературы

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