

# Распределение Fee на большом временном интервале

6 марта 2018 г.

## Аннотация

Пусть  $fee$  - непрерывная случайная величина  $\geq 0$ . Действительно,  $fee$  в  $\forall$  момент времени может быть представлена числом с мантисой, содержащей произвольное количество цифр. Таким образом, с учетом погрешностей измерения, можно  $\forall$  значению непрерывности с.в. сопоставить некоторое рациональное число (с конечным множеством значащих цифр в мантиссе). Если  $fee$  принимает иррационально значение, то даже в случае алгебраических иррациональных чисел, несмотря на теорему Лиувилля, все ее значения можно аппроксимировать рациональными числами с не более чем двумя значащими цифрами в мантиссе, так как в конечном счете  $fee$  сводится к измерению в денежных единицах, которые представляются с точностью до  $10^{-2}$ . С учетом вышесказанного, плотность вероятности  $f(fee)$  на вещественной прямой непрерывна "почти везде" а значит  $fee$  - непрерывная случайна величина.

## 1 Введение

При функционировании сети блокчей стремление времени  $t$  к  $+\infty$  эквивалентно количеству опытов  $m$  по достижению консенсуса на текущий момент  $t$ . Тогда  $t \rightarrow \infty \curvearrowright m \in \mathbb{N}$ . Если в момент  $t_m$  определяется мастер-узел и эскорт  $m$  раз с начала функционирования сети, то  $m$  и есть условное "время".

### Задача.

Доказать, что при  $t \rightarrow +\infty (m \rightarrow +\infty)$  конечный узел из множества  $B_n$  получит  $fee$  в соответствии с распределением  $f(fee)$  и своим "присутствием" в сети.

### Решение.

Будем считать  $fee$  непрерывной случайной величиной, распределенной во времени, т.е. случайным процессом. Если в общем случае  $fee(t)$  - нестационарный случайный процесс с функцией плотности  $f(fee, t)$ . В момент времени  $t^* f = f(fee, t^*)$  - плотность распределения случайной величины  $fee$  с параметрами, значения которых достигнуты к моменту  $t^*$  (плотности вероятности в "сечении"  $t^*$  случайного процесса  $fee(t)$ ).

Поскольку в силу равномерности распределения номеров узлов в  $B_n$  каждый узел в  $\forall$  момент  $t_m$  может стать мастер-узлом с одинаковой вероятностью  $\frac{1}{n}$ ,  $n$  - фиксированное натурально число, то  $fee$ , получаемая  $m$ -узлом после закрытия блока зависит только от  $f(fee, t^*)$ ,  $t^* = t_m$ . Если предположить, что все узлы из  $B_n$  постоянно находятся в сети, то все они находятся в равном положении и с одинаковой вероятностью получают  $fee$  в одном и том же диапазоне (разумеется  $m$  должно быть "достаточно велико"  $m \gtrsim n$ ) независимо от стационарности или нестационарности случайного процесса  $fee(t)$ .

Рассмотрим случай стационарного нормального случайного процесса  $fee(t)$  с постоянным математическим ожиданием  $M_{fee}$  и среднеквадратическим отклонением  $\sigma_{fee}$ . Тогда  $\forall$  узел в момент закрытия блока, соответствующего моменту  $t_m$  выбора  $m$ -узла и эскорта, получает  $fee$  в диапазоне  $(M_{fee} - 3\sigma_{fee}, M_{fee} + 3\sigma_{fee})$  с вероятностью  $\frac{\Phi(\frac{3}{\sigma_{fee}})}{n} \approx \frac{0,997}{n}$ . Обозначим полученную  $fee$  как  $fee_m$

Если некоторый узел выбирался  $m$ -узлом  $\tilde{m}$  раз к моменту  $t_m$ , но принял задачу по закрытию блока  $\tilde{m}$  раз ( $\tilde{m} \leq \bar{m}$ ) то за закрытие текущего блока он получает  $\gamma = \frac{\bar{m} - \tilde{m}}{\bar{m}} fee_m$ . Остаток  $\frac{\tilde{m}}{\bar{m}} fee_m$  суммируется со значением  $fee_{m+1}$ . Это можно назвать - правило мотивации постоянного включения узла.

В случае нестационарного случайного процесса  $fee(t)$  ситуация с постоянно подключенными узлами в смысле равновероятности получения  $fee$  (по сравнению с остальными узлами) не изменится. Если же некоторый узел на каких-то интервалах времени не принимал задание, т.е. был вне сети ( $\tilde{m} < \bar{m}$ ), то, например, в случае роста  $M_{fee}(t)$  и/или сокращения  $\sigma_{fee}(t)$  узел отключавшийся при больших временах чаще, чем при малых, то он потеряет в вознаграждении гораздо больше, чем постоянно подключенные узлы по сравнению со случаем стационарного случайного процесса  $fee(t)$ . Но это произойдет только по "вине" самого узла.

## Список литературы

- [1] Satoshi Nakamoto (2009). “Bitcoin: A Peer-to-Peer Electronic Cash System”. [www.bitcoin.org](http://www.bitcoin.org) .
- [2] (2018.01.10). “Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?”. <https://howmuch.net/articles/crypto-transaction-speeds-compared> .
- [3] BitFury Group (2015.09.13). “Proof of Stake versus Proof of Work”. <http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf> .
- [4] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, Dawn Song (2016). “The Honey Badger of BFT Protocols”. <https://eprint.iacr.org/2016/199.pdf> .
- [5] Leslie Lamport, Robert Shostak, Marshall Pease (1982). “The Byzantine Generals Problem”. ACM Transactions on Programming Languages and Systems. T.4, 3: 382–401 .
- [6] National Institute of Standards and Technology. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf> .
- [7] S.Josefsson, I.Liusvaara. “Edwards-Curve Digital Signature Algorithm (EdDSA)”. IETF RFC. <https://tools.ietf.org/html/rfc8032> .