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

a@sumus.team, rr@sumus.team

4 мая, 2018

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

1 Введение

Разобьём вопрос о распределении fee между узлами на две части

Выбор кортежа очередных нод для участия в консенсусе, может содержать и белые и чёрные НОДы, что является простой схемой случайных опытов, которая называется - схема Бернулли. В общем случае, вероятность элементарного события содержащего μ успехов составляет

$$P\{\mu = m\} = P_n(m) = C_n^m \cdot n^m \cdot q^{n-m} \tag{1}$$

где $m = \overline{0, n}$; C_n^m – это количество комбинаций (сочетаний) m различных элементов без учёта порядка их появления из n элементов; p – вероятность "успеха" в отдельном испытании; q – вероятность неуспеха в отдельном испытании, т.е. $q = 1 - p$. Числа $P_n(m)$ называются биномиальными вероятностями, а формула (1) называется формулой Бернулли.

Одно из следствий схемы Бернулли, это определение вероятности события A, которое произойдёт в n испытаниях не менее r раз, но не более k раз, равна

$$P(A) = \sum_{m=r}^{k} P_n(m) \tag{2}$$

Чтобы определить вероятность того, что "белые" НОДы не смогут наложить "вето" на блок сформированный "черными" нодами проведём расчёт. Для этого определим для нашей задачи исходные данные.

1. $n = 100$ – размер кортежа НОД участвующих в консенсусе, т.е. количество испытаний;
2. m – количество "белых" НОД;
3. общее количество НОД в системе 10000, количество "белых" НОД 4999, а "чёрных" НОД 5001;

4. соответственно вероятность $p = \frac{4999}{10000} = 0.4999$, а $q = \frac{5001}{10000} = 0.5001$.

Следовательно

$$P_{100}(m \leq [1/3 \cdot 100]) = \sum_{m=0}^{33} C_{100}^{m} \cdot 0.4999^{100-m} \cdot 0.5001^{m} \approx 0.00088893... \quad (3)$$

Т.е. вероятность наступления события при котором белые НОДы не смогут заблокировать создание ложного блока составит $\approx 9 \cdot 10^{-4}$.

Определим теперь вероятность создания "легального"блока белыми нодами

$$P_{100}(m > [2/3 \cdot 100]) = \sum_{m=67}^{100} C_{100}^{m} \cdot 0.4999^{100-m} \cdot 0.5001^{m} \approx 0.00043998... \quad (4)$$

Т.е. вероятность наступления события при котором белые НОДы смогут создать "легальный"блок составит $\approx 4 \cdot 10^{-4}$.

Мы исходим из того, что задача достижения консенсуса в первом приближении сводится к получению участниками распределенной системы согласованного решения в случае, если некоторое их количество не приняло участие в согласовании решения. Это может произойти по следующим причинам:

1. Ошибка при передаче сообщения о принятии решения одним из участников.
2. Слишком медленная передача сообщения о принятии решения одним из участников.
3. Сбой в работе участника в системе.
4. Введение в заблуждение при принятии решения в системе, как умышленное, так и неумышленное.

Если рассматривать причины 1-3 неучастия в выработке консенсуса, то для принятия решения достаточно чтобы выполнялось условие $n > m+1$ [**?**], где m – количество участников, которые не участвовали в консенсусе, а n – количество участников принявших решение. В случае появления в системе участников, не участвующих в консенсусе по четвертой причине задача сводится к задаче византийских генералов, которая имеет решение, когда

$$n > 3 \cdot m \quad (5)$$

Если вместо n генералов рассмотреть n узлов блокчейна, участвующих в выработке консенсуса, то очевидно, что эта задача подобна задаче византийских генералов. Для решения проблемы роста времени достижения консенсуса предлагается из конечного множества узлов B_n ,мощность этого множества $\overline{B}_n = n$, выделять подмножество $\overline{B}_{n'}$ $(B_{n'} = n^{'})$ и исходя из предположения о равномерности распределения свойств узлов во всей сети блокчейн решать задачу не на B_n, а на $B_{n'}$ при $n \gg n^{'}$. Общее количество узлов во всей сети блокчейн положим равным N. Обозначим множество этих узлов A_N.

Список литературы

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

.