3. НАУЧНОЕ МАТЕМАТИЧЕСКОЕ ОБОСНОВАНИЕ ОБЩЕЙ ВЕРОЯТНОСТНОЙ МОДЕЛИ ПРОЦЕССА ФОРМИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ БЛОК-ПРОДЮСЕРОВ

3.1. Распределение мощностей Assetbox по узлам сети — кандидатам в блок-продюсеры

Исходными данными выступает группа Assetbox $e=\left[e(1),e(2),...,e(N)\right]$. Каждый Assetbox $e(j)$ характеризуется уникальным идентификатором a из множества A и мощностью (положительной числовой характеристикой) $b(j)$

$$e=\left[\left(a(j),b(j)\right)\right],$$

$$j=1,2,...,N,$$

где N — число Assetbox, участвующих в Майнинге обеспечения консенсуса.

Имеется набор узлов сети блокчейн — кандидатов в блок-продюсеры, в пользу которых случайно (квазислучайно) передаются мощности Assetbox. Мощность каждого Assetbox передается только одному из узлов. В зависимости от состояния группы $e=\left[\left(a(j),b(j)\right), j=1,2,...,N\right]$ возникает набор положительных вероятностей

$$\left[p^i[j](e), i=1,...,n; j=1,2,...,N\right]$$

передачи мощности j-го Assetbox i-му кандидату в блок-продюсеры. Для каждого Assetbox сумма вероятностей передачи мощности этого Assetbox определенному узлу-кандидату в блок-продюсеры для всех узлов равна единице

$$\sum_{i=1}^{n} p^i[j](e)=1, j=1,2,...,N. \quad (1)$$

Вероятность распределения мощностей группы Assetbox с номерами $J^{[l(i)]} = \left[j(1), j(2), ..., j\left(l(i)\right) \right]$ в пользу i **-го узла** равна

$$P^i(J^{[l(i)]}) = p^i(j^i(1), j^i(2), ..., j^i(l(i))) = p^i[j^i(1)](e)p^i[j^i(2)](e)...p^i[j^i(l(i))](e). \quad (2)$$

Вероятность же передачи i **-му узлу только мощностей этих Assetbox** равна

$$P^i[J^{[l(i)]}.] = P^i(J^{[l(i)]})\exp[\sum_{j \in J^{[i]}} \ln[1 - p^i[j](e)]], i = 1, 2, ..., n. \quad (3)$$

Если узлу i в точности передан набор мощностей Assetbox $J^{[l(i)]}(i)$, а остальным узлам-кандидатам в блок-продюсеры передаются другие непересекающиеся наборы мощностей Assetbox, при этом объединение таких наборов по всем узлам дает все множество мощностей Assetbox, тогда вероятность того, что всем узлам будут переданы мощности своих уникальных наборов Assetbox определяется как произведение по всем узлам сети блокчейн вероятностей

$$P^i(J^{[L(i)]}) = p^i(j^i(1), j^i(2), ..., j^i(l(i))) = p^i[j^i(1)](e)p^i[j^i(2)](e)...p^i[j^i(l(i))](e), \quad (4)$$

то есть

$$P[J^{[L(1)]}(1), ..., J^{[L(n)]}(n)] = P^1(J^{[L(1)]})P^2(J^{[L(2)]})...P^n(J^{[L(n)]}). \quad (5)$$

3.2. Формирование последовательности блок-продюсеров из кандидатов в блок-продюсеры

Каждый узел со своим набором мощностей Assetbox из общего набора в n узлов сети блокчейн может быть выбран в группу блок-продюсеров из k узлов ($k < n$).

Вероятность $p(i)[H]$ выбора i-го узла в избранную группу зависит от состояния узлов $H=(E^1,E^2,...,E^n)$, где состояние узлов определяется мощностями Assetbox, распределенными в их пользу

$$E^i=\left[e\left(j^i(1)\right),e\left(j^i(2)\right),...,e\left(j^i\left(l(i)\right)\right)\right],i=1,2,...,n. \qquad (6)$$

Пусть $V(i)$ — случайная величина, показывающая число попаданий i-го узла в избранную группу, то есть $V(i)$ — индикатор попадания i-го узла в избранную группу, $i=1,2,...,n$, принимающая значения 0 или 1. Обозначим через $V=\sum_{i=1}^{n}V(i)$ число узлов в избранной группе. Тогда вероятность попадания i-го узла в избранную группу из k блок-продюсеров равна

$$P(i;k)=P\left(V(i)=\frac{1}{V=k}\right) \qquad (7)$$

условной вероятности попадания i-го узла в избранную группу при условии, что число узлов в избранной группе равно k.

Эту условную вероятность находим как отношение вероятности произведения $P(V(i)=1,V=k)$ этих двух событий к вероятности $P(V=k)$ условия.

Для этого запишем вероятность условия

$$P(V=k)=\sum_{\frac{V(i)}{V=k}}\exp\left[\sum_{i=1}^{n}\ln\left[p(i)^{(V(i))}\left(1-p(i)\right)^{(1-V(i))}\right]\right] \qquad (8)$$

как сумму вероятностей произведения событий принадлежности определенного узла группе (избранной или неизбранной) событий, когда избранная группа состоит из k узлов.

Затем найдем вероятность произведения $P(V(i)=1, V=k)$, то есть из этой суммы выделим те слагаемые, в которых $V(i)=1$, а сумма остальных индикаторов равна $k-1$, а именно, найдем вероятность

$$P(V(i)=1, V=k)=p(i)\sum_{[V-V(i)=k-1]}\exp\left[\sum_{r\neq i}^{n}\ln\left[p(r)^{(V(r))}\left(1-p(r)\right)^{(1-V(r))}\right]\right]. \qquad (9)$$

Искомая вероятность попадания i-го узла в избранную группу из k блок-продюсеров равна

$$P(i;j)=P\left(\frac{V(i)=1}{V=k}\right) \qquad (10)$$

условной вероятности попадания i-го узла в избранную группу при условии, что число узлов в избранной группе равно k и

$$P(i;j)=P\left(\frac{V(i)=1}{V=k}\right)=\frac{P(V(i)=1, V=k)}{P(V=k)}$$

или

$$P(i;k)=\frac{p(i)\sum_{[V-V(i)=k-1]}\exp\left[\sum_{r\neq i}^{n}\ln\left[p(r)^{(V(r))}\left(1-p(r)\right)^{(1-V(r))}\right]\right]}{\sum_{\frac{V(i)}{V=k}}\exp\left[\sum_{i=1}^{n}\ln\left[p(i)^{(V(i))}\left(1-p(i)\right)^{(1-V(i))}\right]\right]}, \qquad (11)$$

где $p(i)=p(i)[H]$.

3.3. События повторного формирования последовательности блок-продюсеров

Предположим, что условная вероятность попадания i-го узла в избранную группу блок-продюсеров на r-ю позицию при условии, что размер группы блок-продюсеров составляет k узлов, равна $\frac{1}{k}$.

Тогда условная вероятность повторения фрагмента последовательности из определенных w узлов в группе блок-продюсеров из k узлов, при условии, что узлы, участвовавшие в процедуре выбора, уже включены в последовательность, равна вероятности

$$P(w,k)=\frac{1}{k(k-1)(k-2)...(k-w+1)} \quad (12)$$

того, что данный фрагмент последовательности размещен в начале последовательности блок-продюсеров, помноженной на число позиций последовательности $(k-w+1)$, в которых данный фрагмент последовательности может быть размещен, в группе блок-продюсеров из k узлов

$$P(w,k)=\frac{k-w+1}{k(k-1)(k-2)...(k-w+1)}=\frac{1}{k(k-1)...(k-w+2)}. \quad (13)$$

Вероятность же условия формирования фрагмента последовательности $i(1),i(2),...,i(w)$ равна произведению вероятностей $p(i(1)),p(i(2)),...,p(i(w))$. Таким образом, вероятность $p^r(i(1),i(2),...,i(w))$ появления фрагмента последовательности ($i(1),i(2),...,i(w)$) на очередном шаге в группе блок-продюсеров равна произведению условной вероятности $P(w,k)$ на вероятность условия $p(i(1))p(i(2))...p(i(w))$ и равна

$$p^r=p^r(i(1),i(2),...,i(w))=\frac{p(i(1))p(i(2))...p(i(w))}{k(k-1)...(k-w+1)}. \quad (14)$$

3.4. Оценка вероятности стационарности результатов процесса формирования последовательности блок-продюсеров относительно этапов распределения мощностей Assetbox и формирования последовательности блок-продюсеров

В качестве оценки вариантов решения можно определить количество возможных способов разбить множество A на непересекающиеся подмножества A^j, где $j=1,2,...,K$ и $K<N$, равное K^N. То есть первый

элемент A^1 множества A может попасть в любое из K подмножеств, второй элемент A^2 множества A может попасть в любое из K подмножеств... и так N раз. Разбиение исходного множества A на непересекающиеся подмножества A^j, где $j = 1, 2, ..., K$, являются результатом этапа распределения мощностей Assetbox в пользу узлов сети — кандидатов в блок-продюсеры (далее «**Распределение мощности»**).

Каждое подмножество A^j таким образом принимает состояние E^j, определяемое попавшими в него элементами $e(i)$.

$$E^j = \left[e\left(i^j(1)\right), e\left(i^j(2)\right), \ldots, e\left(i^j\left(l(j)\right)\right) \right],\ i = 1, 2, ..., K \text{, а } j = 1, 2, ..., N. \quad (15)$$

Поскольку в общем случае состояния подмножеств будут изменяться, мы можем представить результат реализации этапа **Распределения мощности** как число перестановок N_{sh} подмножеств множества A (предполагая, что под перестановкой в данном случае имеется в виду упорядочивание A^j по величине состояния E^j), которое равно

$$N_{sh} = K! \quad (16)$$

Каждая перестановка является исходными данными для операции **формирования последовательности блок-продюсеров**, с помощью которой из подмножеств A^j выбираются привилегированные подмножества A^k, где $k = 1, 2, ..., D$. Общее количество выборов N_{select} из K подмножеств D неупорядоченных групп блок-продюсеров равно

$$N_{select} = \frac{K!}{D!(K-D)!}. \quad (17)$$

В общем случае вероятность попадания элемента $e(i)$ в конкретное подмножество A^j (событие X), например, первое $j = 1$, равна $P(X) = \frac{1}{K}$.

При этом вероятность выбора подмножества A^1 в привилегированную группу (группу блок-продюсеров) при условии, что событие X состоялось (в подмножестве A^1 размещен элемент $e(i^1)$, событие Y) $P(Y / X) = \frac{1}{K}$. Тогда

вероятность повторного попадания элемента в подмножество, которое впоследствии попадет в привилегированную группу на то же место

$$P(XY) = P(Y / X)P(X) = \frac{1}{K^2}. \quad (18)$$

Если учесть, что в подмножество было выбрано u элементов и это подмножество попало в привилегированную группу на определенную позицию в группе блок-продюсеров, событием X будет выбор на следующем шаге такого же количества u элементов в то же подмножество, а событием Y — выбор этого подмножества в привилегированную группу в ту же позицию. Тогда $P(X) = \frac{1}{K^u}$, $P(Y / X) = \frac{1}{K}$ и

$$P(XY) = P(Y / X)P(X) = \frac{1}{K^{(u+1)}}. \qquad (19)$$

На основании вышеизложенного можно определить значение вероятности распределения мощностей Assetbox в конкретный узел сети и вероятность распределения конкретного узла сети — кандидата в блок-продюсеры в привилегированную группу узлов, которые осуществляют производство блоков.

Таким образом, вероятность произведения описанных выше событий будет мала при больших значениях аргументов.