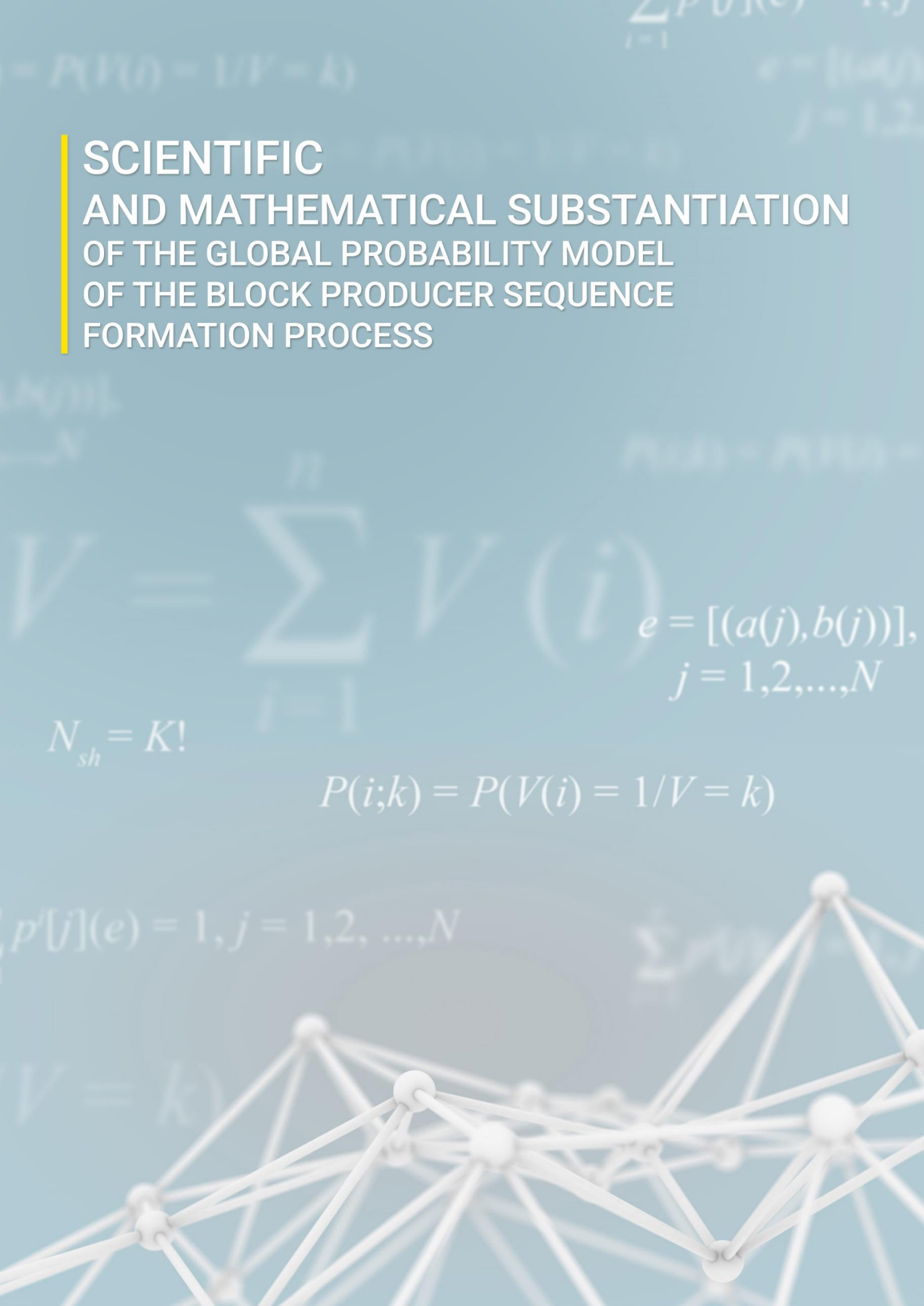
SCIENTIFIC AND MATHEMATICAL SUBSTANTIATION OF THE GLOBAL PROBABILITY MODEL OF THE BLOCK PRODUCER SEQUENCE FORMATION PROCESS



3. Scientific and Mathematical Substantiation of the Global Probability Model of the Block Producer Sequence Formation Process

3.1. Distribution of Assetbox powers among network nodes, block producer candidates

The source data is represented by the group of Assetboxes $e=\left[e(1),e(2),...,e(N)\right]$. Each Assetbox $e(j)$ is characterized by a unique identifier a out of the multitude A and a power (positive numeric characteristic) $b(j)$.

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

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

where N is a number of Assetboxes participating in Consensus building mining.

Assetbox powers are transferred randomly (quasirandomly) in favor of a set of blockchain network nodes (block producer candidates). The power of each Assetbox is transferred to only one node. Depending on the state of the group $e=\left[\left(a(j),b(j)\right), j=1,2,...,N\right]$, there is a number of positive probabilities

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

of transferring the power of a j Assetbox to the i block producer candidate. For each Assetbox, the sum of probabilities of transferring the power of this Assetbox to a specific node, a block producer candidate, for all the nodes, equals one

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

The probability of distributing powers of the Assetbox group with the numbers $J^{[l(i)]}=\left[j(1), j(2),..., j\left(l(i)\right)\right]$ in favor of the i **node** equals

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

Whereas the probability of transferring powers of only these Assetboxes to the i node equals

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

If the i node receives the precise set of Assetbox powers $J^{\left[l(i)\right]}(i)$, and the other nodes, block producer candidates, receive other, unrelated sets of Assetbox powers, while combining such sets with all the nodes amounts to the entire multitude of Assetbox powers, the probability that all the nodes will receive the powers of their own unique sets of Assetboxes is defined as a product of probabilities for all the blockchain nodes

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

which means

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

3.2. Forming a block producer sequence out of block producer candidates

Each node with its own set of Assetbox powers out of the total set of n blockchain network nodes can be selected into the block producer group out of k nodes ($k < n$).

The probability $p(i)[H]$ of choosing the i node into the selected group depends on the state of the nodes $H = (E^1, E^2,..., E^n)$ where the state of the nodes is determined by the Assetbox powers distributed in their favor

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

$V(i)$ is a random value that shows the number of entrances of the i node into the chosen group, which means that $V(i)$ is an indicator of the i node entering the chosen group, $i = 1,2,...,n$, which receives the values of 0 or 1. $V = \sum_{i=1}^{n} V(i)$ denotes the number of nodes in the chosen group. The probability of the i node entering the chosen group of block producers k equals

$$P(i;k) = P(V(i) = 1 / V = k) \qquad (7)$$

the conditional probability of the i node entering the chosen group on condition that the number of nodes in the chosen group equals k.

This conditional probability is determined as a relation of the probability of the product $P(V(i) = 1, V = k)$ of these two events to the probability of the $P(V = k)$ condition.

The probability of the condition equals

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

the total of the probability of the products of events of the specific node's membership in a group (chosen or not chosen) of events when the chosen group consists of k nodes.

Then we calculate the probability of the product $P(V(i) = 1, V = k)$, i.e. distinguish the summands out of this total, in which $V(i) = 1$ and the total of other indicators equals $k - 1$. This probability is determined as follows

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

The probability of the i node entering the chosen group of block producers k equals

$$P(i;k) = P(V(i) = 1 / V = k) \qquad (10)$$

the conditional probability of the i node entering the chosen group on condition that the number of the nodes in the chosen group equals k and

$$P(i;k) = P(V(i) = 1 / V = k) = \frac{P(V(i) = 1, V = k)}{P(V = k)},$$

or

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

where $p\left(i\right)=p(i)[H]$.

3.3. Events of the repeated formation of the block producer sequence

The conditional probability of the i node entering the chosen group of block producers at the r position on condition that the size of the group of block producers is k nodes equals $\frac{1}{k}$.

The conditional probability $P^{(r)}(w,k)$ of repeating the fragment of the sequence out of the determined w nodes in the group of block producers of k nodes on condition that the nodes, which participated in the selection procedure are already included in the sequence equals the probability

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

that this sequence fragment is positioned at the beginning of the sequence of block producers multiplied by the number of positions in the sequence $(k-w+1)$, in which this sequence fragment can be placed, in the group of block producers of k nodes

$$P^{(r)}(w,k)=\left(k-w+1\right)P(w,k)=\frac{1}{k(k-1)...(k-w+2)}.\qquad(13)$$

The probability of the condition of forming the $i(1),i(2),...,i(w)$ sequence fragment equals the produce of the probabilities $p(i(1)),p(i(2)),...,p(i(w))$. The probability $p^{(r)}=p^{(r)}(i(1),i(2),...,i(w))$ of the sequence fragment $i(1),i(2),...,i(w)$ occurring at another step in the group of block producers equals the produce of the conditional probability $P^{(r)}(w,k)$ and the probability of the condition $p(i(1))p(i(2))...p(i(w))$ and equals

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

3.4. Evaluation of the probability of stationarity of the results of the block producer sequence formation process regarding the stages of distribution of Assetbox powers and block producer sequence formation

As the evaluation of the solution options, we can determine the number of possible ways to divide the multitude $A = \left\{a^{(1)}, a^{(2)}, ..., a^{(N)}\right\}$ out of N elements into the unrelated subsets $A^{(i)}$, $A = A^1 + A^2 + ... + A^K$, where $i = 1, 2, ..., K$ and $K < N$, which equals K^N. The first element $a(1)$ of the multitude A can enter any of the subsets K, the second element $a(2)$ of the multitude A can enter any of the subsets K … and so on N times. The division of the source multitude A into the unrelated subsets $A^{(i)}$, where $i = 1, 2, ..., K$ is a result of the stage of distributing Assetbox powers in favor of network nodes, block producer candidates (hereinafter the "**Power distribution"**).

This way, each subset $A^{(i)}$ takes on the condition E^i that is defined by the elements $a(i(s))$, $s = 1, 2, ..., l = l(i)$ within it,

$$E^i = \left[a(i(1)), a(i(2)), \ldots, a(i(l))\right],\ i = 1, 2, ..., K, \text{ and } \sum_{i=1}^{K} l(i) = N. \qquad (15)$$

Generally, the states of subsets will change. The result of implementing the **Power distribution** stage as a number of shifts N_{sh} of subsets of the multitude A (assuming that the shift, in this case, means the arrangement $A^{(i)}$ by the value of the condition E^i), which equals

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

Each shift is the source data for the process of **forming the sequence of block producers**, with the help of which the privileged subsets $A^{(v)}$ are selected out of $A^{(i)}$ subsets, where

$v = 1, 2, ..., \Pi$. The total number of selections N_{select} out of subsets K of unordered groups of block producers Π equals

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

Generally, the probability of the element $a\left(i\left(1\right)\right)$ entering a specific subset $A^{(i)}$ (event X), for example for the first $i = 1$, equals $P(X) = \frac{1}{K}$. The probability of selecting the subset $A^{(1)}$ into the privileged group (group of block producers) on condition that the event X has occurred (in the subset $A^{(1)}$ there is an element $a\left(i\left(1\right)\right)$, event Y) $P(Y/X) = \frac{1}{K}$. The probability of the repeated entering by the element of the sequence, which will then enter the privileged group into the same spot

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

u elements were selected into the subset and this subset entered the privileged group into a specific position in a group of block producers, the event X will be the selection of the same number u of elements into the same subset during the next step, and the event Y is a selection of this subset into the privileged group into the same position. We calculate $P(X) = \frac{1}{K^u}$, $P(Y/X) = \frac{1}{K}$ and

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

Based on the above-mentioned, we determine the value of the probability of distributing Assetbox powers into a specific network node and the probability of distributing a specific network node, a block producer candidate, into a privileged group of nodes that produce blocks.

The probability of the events described above will be low with high values of variables.