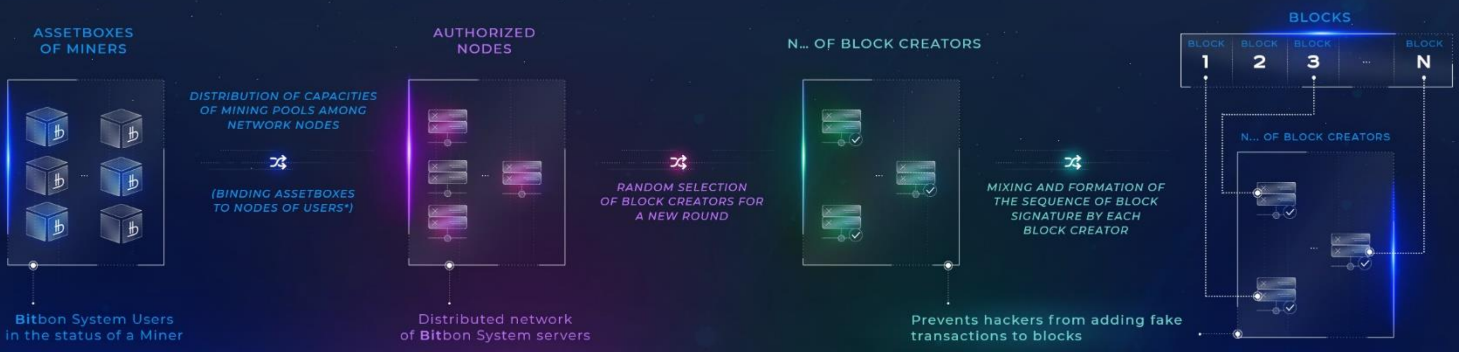
Bitbon System

COMMUNITY PROOF OF STAKE ALGORITHM

CONSENSUS BUILDING USING THE COMMUNITY POS ALGORITHM IN THE BLOCKCHAIN NETWORK OF THE BITBON SYSTEM

(Version dated July 15, 2020)


ASSETBOXES OF MINERS
DISTRIBUTION OF CAPACITIES OF MINING POOLS AMONG NETWORK NODES
(BINDING ASSETBOXES TO NODES OF USERS*)
Bitbon System Users in the status of a Miner
AUTHORIZED NODES
RANDOM SELECTION OF BLOCK CREATORS FOR A NEW ROUND
Distributed network of Bitbon System servers
N... OF BLOCK CREATORS
MIXING AND FORMATION OF THE SEQUENCE OF BLOCK SIGNATURE BY EACH BLOCK CREATOR
Prevents hackers from adding fake transactions to blocks
BLOCKS
BLOCK 1
BLOCK 2
BLOCK 3
...
BLOCK N
N... OF BLOCK CREATORS

*This document is a special version of the Appendix to the **Bit**bon System Public Contract "Mining in the **Bit**bon System" created to make it easier to understand the principles of consensus building using the Community PoS algorithm in the blockchain network of the **Bit**bon System.*

CONTENTS

Introduction

Blockchain is one of the types of a distributed ledger. The key feature of the distributed ledger is its decentralization, which means the absence of an integral center for storing and registering data. At the same time, the information in all the nodes of the distributed ledger must be valid and relevant, which is possible only through achieving consensus among all the nodes of such a ledger. The first consensus building algorithm that was applied to the blockchain network was a general instance of solving the Byzantine fault tolerance, where the number of network nodes is unlimited and can dynamically change.

To solve this problem, an approach to organizing communities that use blockchain can be applied, where ways of joint activity should be proposed instead of sudden sequences, where participants of communities would create decentralized community organizations representing their interests and participating in the development of the Decentralized Autonomous Community. The implementation of such a solution leads to the need for creating not only tools, which will allow the community to manage the blockchain network, but also a social and legal model of relationships between users and state authorities.

Such an approach opens the possibility to increase the performance of blockchain networks by using synchronized protocols while maintaining the security and decentralization of blockchain. A good example of that is the proposed in 2014 by D. Larimer Delegated Proof-of-Stake (DPoS) protocol, its implementation into blockchain allowed for a significant increase in the performance of the network (the number of transactions per second). But this protocol has a number of distinctive system features that substantially limit the possibilities of its application.

Taking into account the relevant matters concerning the development of the distributed ledger technology (DLT), as well as the distinctive features and downsides that were found in modern consensus protocols, Simcord Company developed its own solution, a Community PoS (Proof-of-Stake) consensus building algorithm.

Community PoS consensus building algorithm is an improved DPoS protocol due to the following solutions:

- Introduction of the system of automatic distribution of stakes of miners (designated in the form of Assetbox powers) among the nodes of the blockchain network, which leads to the elimination of the voting centralization problem of DPoS participants, which is caused by the Pareto principle (the 80/20 rule);

- Introduction of the node rating system to prevent incorrect behavior of the blockchain network nodes;

- Development of the system of peer-to-peer (P2P) protocols and communications;

- Decentralized verification of a block by all nodes of the blockchain network and formation of node ratings based on verification results;

- Introduction of a network state “service denied” to register the value of the uncertainty period when business offer cannot qualify the state of the operation carried out by the nodes of the blockchain network;

- Organization of the remuneration distribution system for participating in Community PoS consensus building taking into account the motivation for the development of the **Bit**bon System Decentralized Autonomous Community.

1. The Main Idea of Community PoS

The main idea of Community PoS lies in organization of a community of Users in the status of a miner by uniting their Assetboxes into mining pools. Miners provide their **Bit**bons in their Assetboxes for automatic distribution of powers of these Assetboxes among the nodes of the blockchain network of the **Bit**bon System in order to carry out the voting procedure to form the sequence of block producers, which will sign and announce blocks.

Each community participant aims to attract new Users in order to develop the community. In turn, each new User provides their **Bit**bons in their Assetboxes to form a mining pool, therefore increasing the power of that pool. Mining pools with higher power have a higher chance of participating in block formation because they are supported by a higher number of participants with a bigger amount of **Bit**bons. Each new miner automatically receives an opportunity to participate in the validation of blocks generated by other community members, as well as in formation of new blocks, which significantly complicates the organization of hacker attacks on the network. Each new network participant lowers the chance of malicious nodes entering the group of block producers, while at the same time increasing the requirements for hardware resources and the number of **Bit**bons that the hacker must have in order to carry out an attack on the network. According to the conducted calculations, the likelihood of a hacker being able to predict the moment when they can carry out an attack, i.e. having control over Assetboxes and nodes, which will allow such nodes to enter the list of block producers, is 10^{-40} (which means that the chance is incredibly low, and just as a comparison, imagine if a cat wrote a scientific novel by randomly stepping on a keyboard). Therefore, the increase in the number of network participants leads to a further increase in the ability to withstand attacks on the blockchain network of the **Bit**bon System making any type of attack impossible.

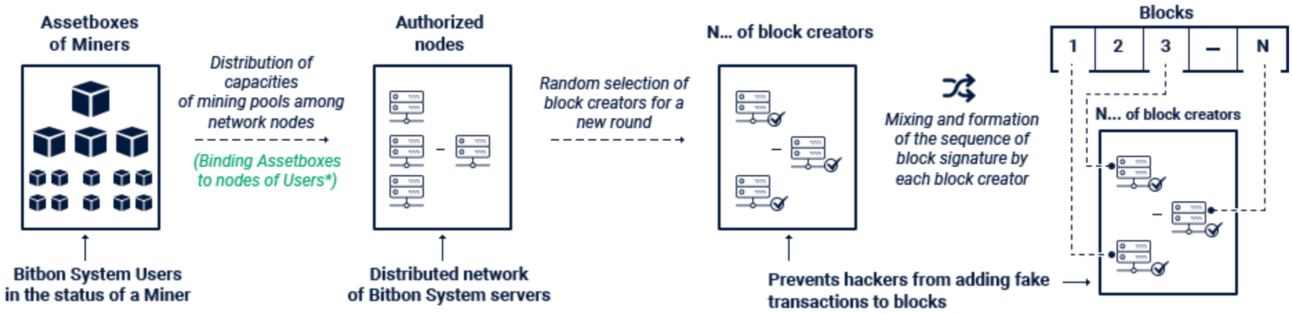

Assetboxes of Miners
Distribution of capacities of mining pools among network nodes
(Binding Assetboxes to nodes of Users*)
Authorized nodes
Random selection of block creators for a new round
N... of block creators
Mixing and formation of the sequence of block signature by each block creator
Blocks
1
2
3
–
N
N... of block creators
Bitbon System Users in the status of a Miner
Distributed network of Bitbon System servers
Prevents hackers from adding fake transactions to blocks

Figure 1. Flowchart of operation of the Community PoS algorithm

Simcord Company plans to implement the consensus building algorithm in two stages. This article describes the algorithm implemented at the first stage (Figure 1), which is a preparation for the transfer to a fully decentralized model of the **Bit**bon System. When moving onto the second stage, the algorithm will be expanded and provide the binding of Assetboxes to nodes of Users (Figure 1*). This will give miners additional motivation to launch their own network nodes and guarantee their reliable operation, which, in turn, will increase the diversity, reliability and security of the **Bit**bon System as a whole.

Another important aspect is the matter of the Community PoS consensus building algorithm's ability to withstand hacker attacks carried out by exploiting the weaknesses of the blockchain technology. Analysis of the Community PoS concept allows us to confidently state that the use of this consensus building method in the blockchain network of the **Bit**bon System will allow it to successfully pass the tests for the attacks listed below:

- **51% attack** means a capture of blockchain network resources, which will allow making decisions on the creation of blocks to discredit the system and/or obtain illegal profit through unsanctioned spending (double spending) and generation of a chain of blocks with data that is beneficial for the hacker.
- **Sibill** means a substitution of valid nodes, blockchain network resources, code or sources of network data for resources controlled by the hacker in order to influence the creation of blocks and add transactions to them to receive illegal profit through unsanctioned spending (double spending).

- **Timejacking** means a transfer of incorrect time to the nodes of the blockchain network that work with a time-sensitive consensus algorithm by passing the hacker's infrastructure element as a valid exact time server for short-term control over block creation and/or substitution of transactions in order to receive illegal profit through unsanctioned spending (double spending).
- **Pool cannibalizing** means an increase of the hacker's resource that influences the size of mining remuneration compared to other network and pool participants through phishing of actions of other participants, as well as exploiting weaknesses of the protocol by using a super resource in order to receive bigger remuneration for mining by pushing out other miners, for example, by showing them the economic inefficiency of mining in this network segment.
- **Block withholding** means not issuing the block and delaying the completion of transactions in order to receive illegal profit through unsanctioned spending (double spending), as well as to get an opportunity to block the operation of the network.
- **Deorganizing attack** means a selective choice not to reveal a block and/or delay the addition of transactions to the block with their further substitution (selective) or breaking of their sequence in order to receive illegal profit through unsanctioned spending (double spending). Destructive activity of the hacker's node is random and hard to predict.
- **Eclipse attack** means a restart of a blockchain P2P network (used to find the nodes and control their state) by sending out spam messages via gossip-like protocols to disrupt the integrity of the network and to further use other attack methods in order to get temporary control over block formation and, therefore, discredit the network.
- **P + epsilon attack** means a manipulation of a consensus building procedure by a hacker through sending out both valid and invalid signals within the network systematically influencing the other network nodes in a way that the majority of participants would vote in favor of the hacker in order to receive illegal profit through unsanctioned spending (double spending).
- **Blacklisting** means the process of sending out protocol messages aiming to add valid nodes to the blacklist of the blockchain network, which, at worst, will allow the hacker to carry out a 51% attack.
- **Transaction malleability** means the process of the hacker exploiting the weaknesses of the consensus protocol to substitute a valid transaction for their own with the same hash code (during a block withholding attack) or any other in order to receive illegal profit through unsanctioned spending (double spending).

- **Selfish mining** means a variation of pool cannibalizing where a big group of miners creates a separate, hidden from other miners valid chain of blocks longer than the primary one revealing it afterwards and receiving remuneration that is out of proportion with the resources spent through manipulations aimed at making this chain primary.
- **Cancellation of all transactions** can occur in case of a 51% attack where a hacker can obtain the majority of blocks and, as a result, get an opportunity to cancel all the following transactions, which can lead to the destruction of the network.
- **Double spending** means the exploitation of the weaknesses of the network (protocol, infrastructure, client) by the hacker in order to receive illegal profit through unsanctioned spending.
- **Random hard forks** mean a divergence of a chain of blocks that later becomes primary because of a global system failure or a random exploitation of the weaknesses of the network.

Organization of the Bitbon System blockchain infrastructure based on the Community PoS consensus gives an opportunity to build a decentralized autonomous community, social, legal, architectural and technical solutions of which will allow for a reasonable and quick reaction to challenges of the modern world and changes of conditions without decreasing the quality of services of this system for end users.

2. Concept of the Community PoS Consensus

2.1. The goal of Community PoS and ways of achieving it

The main goal of the Community PoS consensus is to provide true decentralization of the processes of announcing, verifying and storing data of the distributed ledger with a high level of performance of storage network and guaranteed short wait time of transaction confirmation.

The achievement of this goal is ensured by:

- Using ways of preliminary block production sequence approval by block producers to prevent forks and block collision;
- Centralizing the network at the moment of block formation by the network node in accordance with the block formation sequence;
- Introducing a strict synchronized sequence diagram of network node operation to ensure the exact determination of the state of the blockchain network;
- Introducing the network state “service denied” to register the value of the uncertainty period when business offer cannot qualify the state of the operation carried out by the nodes of the blockchain network;
- Mutual synchronization of network nodes to ensure adherence to the voting and block formation sequence diagram;
- Using a fixed maximum amount of time for processing the transaction (with its cancellation in case of failure to complete it within the given timespan);
- Introducing three types of network node operation protocols:

– Protocol for quorum control and ensuring time synchronization of nodes that is essentially a background process based on the poll of a blockchain P2P network and keeps the information on the availability of the nodes, which can participate in the voting and block formation procedures, up to date;

– Sortition protocol, within which the network node sequence is formed, according to which network nodes will act as block producers;

– Block formation protocol, which includes the creation of the block by the block producer, its verification by other network nodes and a node rating system, which provides the accuracy of carrying out the block producer functions by the network nodes;

- Using the algorithm of the random miner stake (Assetbox powers) distribution among the network nodes prior to sortition of the nodes, the rating of which allows them to be candidates for block producers. Such a decision allows increasing the difficulty of predicting the block producer sequence. The algorithm is based on the value of the "nonce" parameter (the last block or genesis block), which, in turn, is based on a random number from a hardware random number generator and a time stamp by generating a hash code from this information using the Keccak-256 based on elliptic curves. The resulting numeric sequence is used as a key to distribute the Assetbox powers of miners in favor of network nodes (block producer candidates);

- The mechanism of decentralized sortition when determining the sequence of taking on the role of block producers by the nodes, which is conducted by sorting the list of nodes according to the powers allocated in favor of these nodes, defining the sequence limits and observing the nodes' compliance with the rules of participating in the formed sequence of block producers;

- A decentralized verification of the block by all the nodes of the blockchain network and sending out the message on the increase or decrease of the rating of the block producer that generated the block depending on the verification results.

2.2. The roles of nodes in the Community PoS consensus

Each node of the blockchain network of the **Bit**bon System can have the following roles:

- **Synchronization node.** In this role, the blockchain network node, when connecting to the network, synchronizes with the other nodes by receiving blocks, transactions and objects related to them from the other network nodes, verifying them and storing in the local blockchain storage. Synchronization of the node time is conducted in accordance with the timestamp of the last valid block and the latency metric to the block producer that formed this block, as well as the timestamps from the other network nodes. After synchronization, the node conducts the verification and storage of transactions and blocks it receives. If the metric of distributing the block for this node is less than 1 second, then this blockchain network node must accept transactions from client applications for processing and, after verifying them, rebroadcast them to all the other network nodes. Otherwise, or if the quorum of the blockchain network nodes has not been reached, the node does not accept transactions for processing, displaying the "service denied" error.

- **Node participating in the quorum.** This role can be taken on by any synchronization node, whose latency for nodes that are part of the quorum does not exceed 400ms. To implement the protocol of operation of the Community PoS consensus in the blockchain network, the number of nodes has to be higher than the size of the quorum determined by the **Bit**bon System Operators (no less than 2/3 of the number of blockchain network nodes). The node participating in the quorum takes part in the rating formation procedure in accordance with the node rating system. If, while processing transactions and blocks, the quorum participant notices a violation of the processing rules, they send all the network nodes the relevant message on the decrease of the rating of sources of invalid data. If the data is valid, then the message contains the information on the increase of the rating of the relevant block producers.

- **Block producer candidate.** This role can be taken on by any node participating in the quorum with the rating above 10 if it has the mining mode turned on. In this case, such a node will be included in the procedure of distributing powers (stakes) of the pool of Assetboxes of the miner community.

- **Block producer.** This role is taken on by the blockchain network node that is a block producer candidate, which was included in the block producer sequence as a result of conducting the sortition to sign and announce only one block in the specified time period (timeslot) (Figure 2).

2.3. Supporting the sortition system

To eliminate the threats of the **Bit**bon System centralization and to automate the voting procedure of miners within the limits of participating in Consensus building mining of the **Bit**bon System, there is a procedure of automatic redistribution of stakes (Assetbox powers) among block producer candidates.

All that is required in order for an Assetbox to participate in voting is to carry out a one-time transfer of the miner's Assetbox power to the pool by transferring 0.0001 **Bit**bons with a comment "/pool" to any Assetbox of the mining pool.

Assetbox powers that participate in automatic distribution randomly associate among all the nodes of the blockchain network of the **Bit**bon System with the corresponding rating, which meet the relevant requirements for the performance and quality of the connection channel (node in the role of a block producer candidate) at the time of voting.

2.4. Sortition procedure

The goal of the sortition procedure is to form the sequence of block producers based on the Assetbox powers distributed among the block producer candidates, according to which said block producers will sign and announce blocks in the next round.

The sortition procedure is conducted in accordance with the voting and block formation sequence diagram (Figure 2) and contains the rounds, the duration of which is equal to the number of block producers multiplied by the 1-second time interval. The number of block producers is determined by **Bit**bon System Operators.

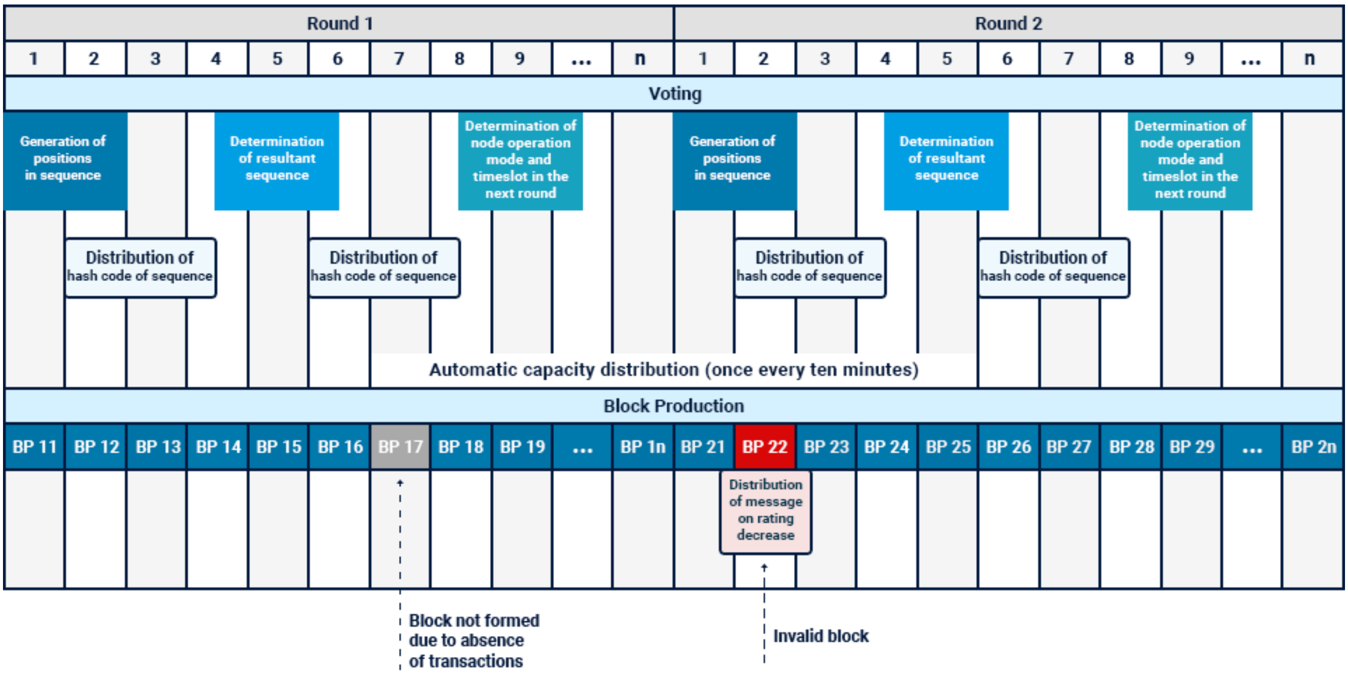

Round 1
Round 2
1 2 3 4 5 6 7 8 9 … n
1 2 3 4 5 6 7 8 9 … n
Voting
Generation of positions in sequence
Determination of resultant sequence
Determination of node operation mode and timeslot in the next round
Distribution of hash code of sequence
Automatic capacity distribution (once every ten minutes)
Block Production
BP 11 BP 12 BP 13 BP 14 BP 15 BP 16 BP 17 BP 18 BP 19 … BP 1n
BP 21 BP 22 BP 23 BP 24 BP 25 BP 26 BP 27 BP 28 BP 29 … BP 2n
Distribution of message on rating decrease
Block not formed due to absence of transactions
Invalid block

Figure 2. Sequence diagram of the Community PoS consensus

The sortition procedure starts after the end of each round and is conducted over the entire duration of the round. The final block of the round or the message of the timestamp instead of it, if this timeslot had no transactions, can serve as an indicator of the end of the round. Voting is carried out in the following order:

- Within the first 2 seconds, every node, based on the Assetbox powers distributed among block producer candidates, must randomly form a list of possible positions (sequence) from 1 to n for each block producer candidate node with power higher than the lower limit and a corresponding rating and then send the hash of this list (sequence) to all the nodes participating in the quorum;

- Out of the nodes that can be included in the sequence, the block producer, which is the last to form a block in this round, is excluded;

- Sequence elements with identical positions are not allowed;

- It is forbidden to include 2 elements with the same identifier in the sequence;

- On the 5th second, each node participating in the quorum, based on the number of votes for each unique sequence hash, must determine whether or not the sequence it formed collected the maximum amount of votes. If not, the node goes into the standby mode awaiting the block producer sequence. Otherwise, the node checks if the number of votes exceeds or equals 2/3 of the quorum. If the number of votes exceeds or equals 2/3 of the quorum, the node announces the sequence. If not, the node announces the message about the sequence forming error and goes into the standby mode until the start of the next round;

- Each node receives either the block production sequence or the error from the other nodes by the 9th second.

Each node, regardless of its role, verifies the received blocks in accordance with the calculated/received sequence of block producers. The block producer candidate specified in the resultant sequence takes on the role of a block producer during its timeslot.

2.5. Block formation

Blocks are formed by block producers in the rounds with the duration of n blocks (for example, the round duration of 21 blocks). The block producer forms the block out of transactions that are in its transaction pool with the timestamp of the latest transaction in the last valid formed block and the moment of block formation in the next timeslot, which it serves according to the rules:

- If no transactions were received in the processed timeslot, the block will not be formed, but all the nodes will be sent the timestamp of the ending of the timeslot;
- The node in the role of a block producer forms a block based on the hash code of the previous valid block out of transactions in its transaction pool;
- During the round, the block producer can form a block only once;
- The block producer cannot under any circumstances form 2 blocks in a row;
- All the nodes (including block producers in this round) take on the role of the synchronization node receiving transactions, carrying them out and checking the received blocks:

o If the block is valid, then both it and the transactions it includes are registered in the storage;

o If the block is invalid, the node ignores it and awaits a valid block with the same number;

- If a block producer was unable to verify the previous block at the time of serving its timeslot, it forms a new one with the same number, which includes all transactions in the transaction pool, with the ones that arrived in the previous timeslots, filtered by the time of creation (excluding the ones that ran out of processing time). Same as with the synchronization nodes, the block producer sends out a message on the decrease of the rating of the previous block producer.

Such measures allow us to avoid creating forks of the chain of blocks, as well as attacks related to the processing delay or ignoring transactions, while at the same time they ensure a guaranteed time of processing a transaction.

2.6. Node rating

The rating of each node is formed through messages that are sent out via a P2P network by all the blockchain nodes of the **Bit**bon System as a result of verifying another block formation. The changes in the rating are accepted by all the network nodes in favor of all the network nodes, in particular in favor of the block producer, and are applied after a time period equal to the duration of three timeslots after block formation, on condition that the number of messages exceeds or equals the quorum (at the same time, the number of messages from each node is being monitored). Only one message from a node for each block is included. Below are the main factors that influence the rating of the nodes:

- Rating is increased:

◦ For the correctly formed block;

◦ For fulfilling the terms of participating in the quorum (issued by a **Bit**bon System Operator);

◦ If a block producer formed at least one block during the day and did not receive the rating decrease;

- Rating is decreased:

◦ If a block producer included more than 10 transactions related to the previous timeslot;

◦ If a block producer formed a block in a timeslot that is not its own;

◦ If a block producer did not form and send the package with a timestamp in its timeslot;

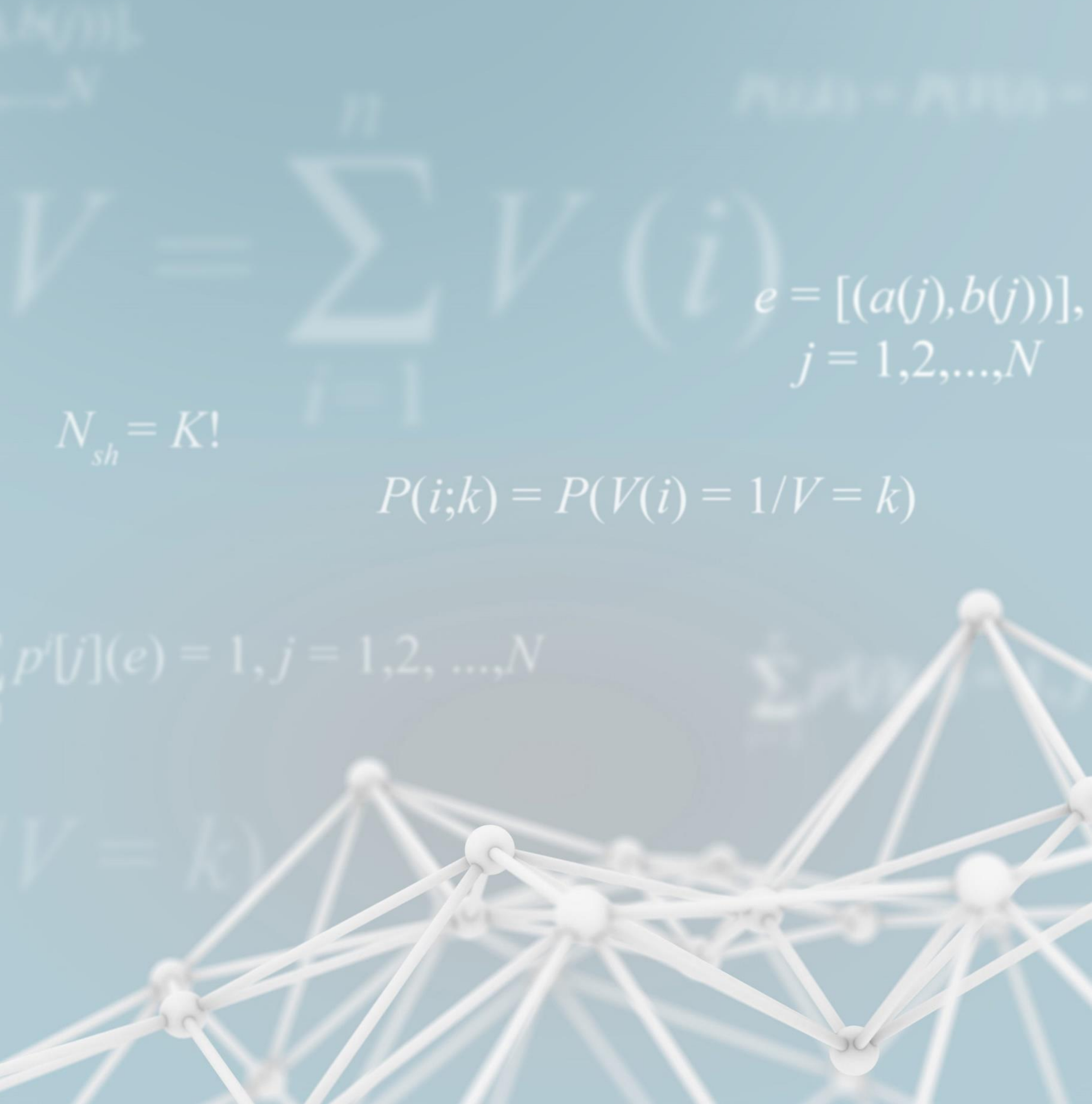
◦ If the node sent more than 2 messages on the increase/decrease of the rating for one block (pause);

◦ If the node broadcasted an invalid transaction or the same transaction once again (for each repetition);

◦ Rating reduction to zero if a block producer formed an invalid block (included an invalid transaction).

The described feedback system allows us to effectively prevent attacks and incorrect behavior of potential hackers, as well as exclude unstable nodes of the blockchain network from the quorum.

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


$V = \sum_{i=1}^{n} V(i)$
$e = [(a(j),b(j))],$
$j = 1,2,\ldots,N$
$N_{sh} = K!$
$P(i;k) = P(V(i) = 1/V = k)$
$p^i[j](e) = 1, j = 1,2, \ldots,N$

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 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 $J^{[l(i)]}(i)$, 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

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

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 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.

Now let us calculate 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,

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

Generally, the states of subsets will change. The result of implementing the **power distribution** stage is shown 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} of privileged unordered subsets out of block producer groups equals

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

Generally, the probability of the element $e(i)$ entering a specific subset A^j (event X), for example for the first $j=1$, 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 $e(i^1)$, event Y) equals $P(Y/X) = \frac{1}{K}$. The probability of the repeated entering by the element of the sequence, which will then enter the privileged group into the same spot equals

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

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

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

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.

Terms and Definitions

Bitbon is a digital asset of the **Bit**bon System, which is a utility token (access token) and, based on the **Bit**bon Protocol, provides a **Bit**bon System Participant with the scope of rights to access the **Bit**bon System services determined in accordance with the number of **Bit**bon accounting units this Participant has. **Bit**bon accounting units are used to implement the method of measuring the exchange value of all digital assets of the **Bit**bon System and ensure their circulation. The **Bit**bon digital asset has been created by SIMCORD LLC, EDRPOU 37657823, and assigned unique attributes and properties based on the **Bit**bon System Public Contract and **Bit**bon Protocol. Using **Bit**bon as a key component of the **Bit**bon System allows **Bit**bon System Users to implement the method for accounting and management of their assets through digital assets for the purpose of secure and equivalent decentralized exchange of digital assets in the **Bit**bon System without intermediaries and money.

Bitbon System is an integral decentralized blockchain-based system, which allows **Bit**bon System Users to implement the method for accounting and management of their assets using digital assets for the purpose of safe and equivalent decentralized exchange of digital assets in the **Bit**bon System without intermediaries and money. The key component of the **Bit**bon System is **Bit**bon.

Digital asset of the Bitbon System is a tokenized information resource derivative of the right to a value and circulating in the form of access token accounting units.

Assetbox is a record (cell) in the blockchain in the form of an identifier created in the **Bit**bon System account for storing and transferring digital assets.

Mining pool is a cluster of Assetboxes of miners, which is formed as a result of the registration of new Assetboxes in the mining pool through an Assetbox that is already participating in mining. Such a connection is called a graph edge of social connections of a specific miner. The graph node has no limitations for the number of graph edges for the lower nodes.

Assetbox power is a value that depends on the number of **Bit**bon accounting units in the Assetbox, as well as on the contribution of a miner to the development and maintenance of the miner community. The miner's Assetbox power is calculated as a total of the base and social powers of the miner’s Assetbox. Base Assetbox power is determined by the individual power of the miner’s Assetbox and the power of the miner’s first line of social connections in the miner community. Social Assetbox power is formed by miner’s social connections starting from the second line and lower. Assetbox power directly influences the miner’s remuneration.