NeuronChain Technical White Paper

A Financial Smart Contract Blockchain for Decentralized Financial Markets

Maksim Beskorovainy, Timur Akhmedzhanov, Sergei Sukhanov

September, 2018 | v.1.0

The current paper is on github.com/NeuronChain/wiki/technical-whitepaper

Abstract. *Bitcoin and Ethereum have inspired the world with possible use-cases of a "Peer-to-Peer Electronic Cash System"[1] and "Smart Contract"[2] running on decentralized blockchains. However, Bitcoin's structure is eNRONgy-consuming, and its thirst makes it incompatible with humanity's mutual goal to fight climate change, while Ethereum's scaling attempts are vague at best. NeuronChain aims to address these challenges. We propose an eco-friendly solution to meet the transaction throughput needs of global markets. We have parallelized the BitShares Core[3] to maximize blockchain throughput and suggest a distributed model with a hybrid consensus mechanism (DPoI (Delegated Proof of Importance) + TaPoS (Transactions as Proof of Stake)) that requires no mining. This whitepaper explains the functional and technical design concept, and the blockchain governance principles of NeuronChain.*

Content Table

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online] http://bitcoin.org/bitcoin.pd
[2] Ethereum: A Next-GeNRONation Smart Contract and Decentralized Application Platform. [Online] https://github.com/ethereum/wiki/wiki/White-Paper
[3] BitShare Core. [Online] https://github.com/bitshares/bitshares-core

1. Introduction

A blockchain system is a system for decentralized storage of heterogeneous data, fixed in an interconnected chain of blocks. Built-in crypto algorithms guarantee effective and reliable data logging and storage, while a pool of miNRONs ensures trouble-free operation of the entire system. Blockchain's architecture relies solely on the universal trust of all system participants, their privacy, and the absence of a single central control.

As noted above, blocks are used to store system data. As time has shown, the classic approach to block configuration leads to undesirable centralization of data processing operations. Using the example of Bitcoin, one can see that the largest share of miNRON capacity is consolidated in a relatively small geographical area, which, theoretically can create a situation, where a small group of individuals or organisations will dictate their terms to other participants jeopardizing the stable operation of the entire system.

The development of blockchain systems is an ongoing process and their latest versions use new approaches toward data exchange and storage, thereby increasing confidentiality of system participants while getting rid of unwanted centralization.

2. Neuron coin

The NeuronChain blockchain uses the base coin called Neuron (NRON). 1 NRON is split into 10^5 subunits.

Just like in some other blockchain systems, the base unit inherited from BitShares Core, has the property of volume (value), can be transferred via a log to the blockchain, and is protected with a public key algorithm to create a digital signature defined in secp256k1 elliptic curve group.

The Neuron Coin is the internal currency of the NeuronChain blockchain, and it can be freely traded on exchanges, so the coin rate is determined by its cross-exchange rates and has a certain volatility.

3. System elements

3.1. Delegates[4]

We use the term 'Delegate' because it represents our vision of a democratic and decentralized nature of the blockchain. Coin holders delegate their rights to elected members (Delegates) to represent their interests in a constant and transparent functioning of the network. In traditional contracts, a public notary[5] is sometimes used. Delegates are not the "third" party to the contract, but they serve the very important role of certifying that the contract was signed by specified individuals at the specified time. The Delegates in the NeuronChain network work towards validating signatures, collecting transactions, logging them in system blocks, signing the block and sending it into the network.[6]

Under DPOI, the holders can elect any number of Delegates to generate blocks (initially 25). A block is a group of transactions, which update the state of the ledger. Each account is allowed one vote- per share- per

[4] NeuronChain Github: How to become an active delegate

[5] http://en.wikipedia.org/wiki/Notary_public

[6] NeuronChain Github: How to run a block producing Delegate refer to the link

Delegate, a process known as approval voting[7].The top-of-the-list 21 candidates are elected Delegates, and 4 are elected at random.

Any network participant can be a candidate for delegate if he or she meets the following requirements:

Requirements for Delegates

- Register an account and deposit a NRON 20 000
- Create, configure and run a Delegate local full node.

  Minimum Hardware Requirements

  - Core i7 7700 4.2 GHz
  - RAM 64 GB RAM
  - Internet speed 200 MBit/s

  Active Delegate duties

  - Be a reliable[8] block producer
  - Maintain a public seed node
  - Publish accurately, frequently update (check 1-2 times per hour).

A delegate creates a special proposal transaction for nomination, as a candidate for Delegate.

Network participants may, within a specified time limit, cast their vote for one of the Delegate candidates. Each network participant is allowed to vote for one candidate only. Vote counting takes into account the Importance Score (IS)[9] of each holder. All Importance Scores of the holders voting for a delegate candidate are summed up. However, for the purpose of consensus, when agreement or disagreement is voiced by each separate Delegate, each vote is taken into account solely on the basis of the Delegate's own Importance Score, irrespective of the Importance Scores of the network participants, who have voted for him.

A candidate for Delegate is considered elected if he enters the top 21 in terms of IS. If any two candidates vying for the top 21 have equal IS's, priority is given to the candidate, who put forward his candidature earlier, i.e., whose proposals transaction is located in an earlier block. If both candidates put forward their candidatures at the same time (concurrently), i.e., their proposals transactions are located in the same block, priority is given to the candidate, whose proposals transaction was first in the block.

The four additional Delegates are selected from the candidate list at random.

Each time a delegate produces a block, they are rewarded for their work. The reward amount is determined using the "function of linear dependence". However, in order to subordinate delegates' income to the network's income, we apply a factor equal to 1/3 of the network's commission when calculating a delegate's reward, thus making the rewarding process fully decentralized.

$y=kx+b$, where:

$x \neq 0$

$b=0$

[7] https://en.wikipedia.org/wiki/Approval_voting

[8] A block producer is considered reliable if it does not skip blocks when it comes to his turn to produce these blocks. Measurements that could be put into place are e.g. stable internet connection with duplicate channels or node-server duplication for hot swap.

[9] For more details on IS see Calculation of IS

k=⅓*0.02 (Network trx commission)

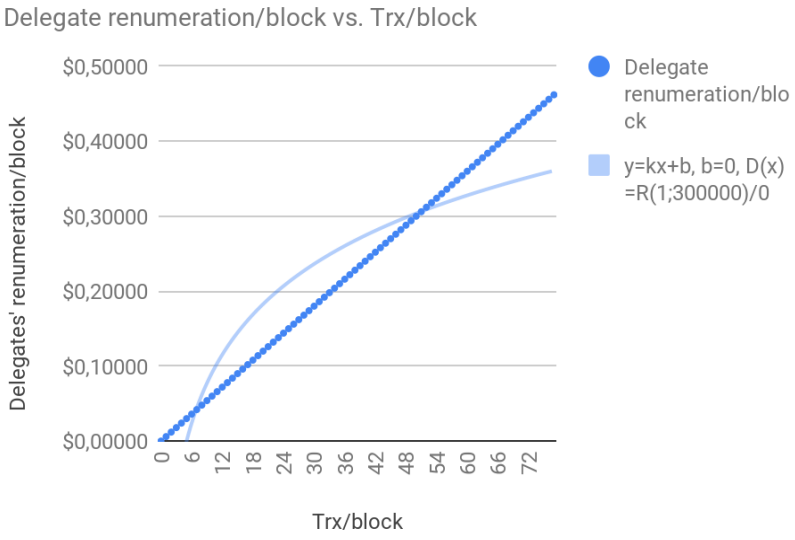
D(x) = R(1;300000)/0

y - Delegate's reward;

x - argument - the number of transactions within a block.

Linear dependence is a condition where greater the number of transactions conducted within a block, the greater is the income a delegate receives.

The formula is described by a graph of linear function y=kx+b:



The amount is paid out of the Reserve Pool (NRON 250 million) which is defined in the Genesis block. A commission transaction fee of 1 NRON is added to the Reserve pool every time a transaction takes place on the NeuronChain blockchain. If a Delegate fails to produce a block, then they are not paid, and may be voted out in the future.

The slate of active Delegates is updated once every maintenance interval (1 day), when the votes are tallied. The Delegates are then shuffled, and each Delegate is given a turn to produce a block- at a fixed schedule of one block every 3 seconds. After all the Delegates have had their turns, they are shuffled again. If a Delegate does not produce a block in their time slot, then that slot is skipped, and the next Delegate produces the next block.

3.2. Deposit

A deposit is placed by a Delegate on his or her account with the deposit amount put on hold.

Funds must be deposited until the nearest maintenance time, whereupon the candidate creates a proposals transaction as nomination for Delegate.

1. NRON 20 000;
2. Only 50% of the daily income will be added to the vesting balance and can be withdrawn;
3. The other 50% of the daily income goes to top-up the deposit;
4. Taking out the whole deposit deprives a Delegate of his status;

5. If a Delegate has waived his status and later re-nominates himself as a Delegate, the deposit must at least be equivalent to the amount withdrawn before.

3.3. Deppen

The NeuronChain blockchain has a built-in incentive mechanism for Delegates called Deppen. It provides network participants with additional guarantees of genuine performances of their obligations by Delegates. Deppen monitors availability of a deposit on the Delegate's account, distributes the Delegate's remuneration between the vesting balance and the deposit account in the ratio of 50/50, with 50% of the Delegate's remuneration placed on the Delegate's deposit account, thus increasing his balance, and launches a write-off (penalty) mechanism for the Delegate's deposit if the Delegate commits action in bad faith.

Possible scenarios for loss of a deposit:

- **Penalty**

a) Deppen writes off the Deposit to the reserve pool;

b) The Delegate is struck off the active delegate list and replaced by a reserve delegate;

c) The Delegate at fault may take back his vesting balance;

d) If he makes a new deposit, he may take part in the voting.

- **Withdrawal from the active delegate list**

e) Deppen transfers the Deposit to the Delegate's account;

f) The Delegate is replaced by another one from the reserve list;

g) The Delegate may take back his vesting balance;

h) If he makes a new deposit in the amount of the withdrawn one, he can become an active delegate.

A Delegate is penalized if he skips/misses five or more blocks in 24 hours.

Action	Penalty	Note
Skipping/ missing out on five or more blocks/ 24h	Minus deposit + accumulated sum	Deprived of delegacy and not allowed to vote

3.4. Committee

The committee is NeuronChain network's administrative authority. They put forward proposals on changing certain parameters of the network, for example, on block generation speed, rewarding delegates, etc. Unlike Delegates, a Committee Member (CM) is not a paid position.

NeuronChain's committee consists of 11 CMs. Any network participant can nominate their candidacy for the Committee membership. To become a member of the committee in the NeuronChain network, one has to have a minimum balance of NRON 10 000.

A candidate creates a "special proposals transaction" for nomination as a Committee Member.

Network participants may, within a specified time limit, cast their votes for one of the candidates for Committee membership. Each network participant is allowed to vote for one candidate only.

Upon expiry of the specified time period (maintenance time) votes and IS of each candidate are counted, with IS of a candidate determined as the ∑IS of all network participants voting for this particular candidate. The candidates, who have entered the TOP-11 based on the voting results, are deemed to be elected as CMs and become eligible to decide on changing the network parameters. More details on the decision making mechanism with regard to changing the network parameters are given in governance chapter.

If any two candidates vying for the TOP-11 have equal IS's, priority is given to the candidate, who put forward his candidature earliest, i.e. whose proposals transaction was located in an earlier block. If both candidates put forward their candidatures at the same time (concurrently), i.e. their proposals transactions are located in the same block, priority is given to the candidate, whose proposals transaction was first in the block.

During each maintenance, votes and IS's of all candidates running for CM are counted, whereupon, if necessary, the Committee membership is adjusted. It is noteworthy that in the current maintenance time the CMs previously elected also take part in the voting as candidates on geNRONal grounds, however, a CM retains the votes received at the previous voting, only if any of the network participants fail to cast their vote for another CM candidate.

CMs have no direct power and all changes to the network parameters are ultimately approved by the coin holders. Within the NeuronChain, the network administrative authority lies with the users, rather than the delegates or CMs. This is in line with our aim to provide a truly decentralized system - offering control to those who are most important, the users.

The Genesis account can technically perform any action that any other account can:

- The accounts that exist at Genesis, their names and public keys;
- Assets and their initial distribution (including the core asset);
- The initial values of chain parameters;
- The account / signing keys of the initial delegates (or in fact, any account at all).[10]

This means it is possible to send funds to the Genesis account or specify the Genesis account as an escrow agent. The Genesis account can also be used to issue new assets. There are many cases, where elected delegates can aid the stakeholders in performing tasks that demand a high degree of trust and accountability.

The concept of a committee was borrowed from the BitShare Core, and therefore the current version of the NeuronChain blockchain committee uses the same algorithm:

for i : active committee members do :

member weight: w[i] ← Vpro − Vcon

end for

members ← SORT(w)

active ← members[0 → C]

for parameter : parameters do

p ← GETPARAMETERS(active, parameter)

x = sort(p[i])

[10] http://docs.bitshares.org/testnet/2-genesis.html?highlight=genesis

$\overline{p} = x\left[\frac{C+1}{2}\right]$ C even

$\overline{p} = \frac{1}{2}\left(x\left[\frac{C}{2}\right] + x\left[\frac{C}{2}+1\right]\right)$ C odd

parameter $\leftarrow \overline{p}$

end for

The NeuronChain blockchain has a set of parameters available that are subject to the holders' approval. Holders can define their preferred set of parameters and thereby vote for a CM who was not elected before, or re-elect an existing CM.

Initially, the NeuronChain blockchain has the following blockchain parameters:

1. Fee structure: fees that have to be paid by users for individual transactions[11];
2. Block interval: i.e., max size of block/transaction;
3. Expiration parameters: i.e. maximum expiration interval;
4. Delegate parameters: i.e. maximum number of delegates (block producers);
5. Committee parameters: i.e. maximum number of CMs;
6. Delegate fee: fee for each witness per signed block;
7. Worker budget: available budget for miscellaneous items (e.g. development).

3.5. Oracles[12]

The concept of Oracles is a proprietary development by NeuronChain.

In order for the blockchain system to interact/interface with external environments, the system needs trusted sources of information that will enter data from the external environments into the system. These are called Oracles in the NeuronChain system.

Any network user can become an Oracle.

The number of Oracles in the system is unlimited.

Each Oracle bets on the answer. The correct answer is selected according to the consensus mechanism.

To achieve a consensus, a simple majority of the Oracles should bet on one answer.

The consensus mechanism also includes the indicator of Oracle's importance[13].

The Oracles who betted on the right answer are rewarded. The Oracles who betted on the wrong answer, lose their bet.

Oracles can answer several types of questions:

- Binary (yes/no)
- Numerical, like "What's the weather like now?"

Oracles can also be used to interact with external blockchain systems.

[11] https://neuronchain.io/explorer/explorer/fees

[12] Under development

[13] Currently, the definition of Oracle's importance is taken per the rules for calculating the Importance Score.

3.6. Voting

All parameters of the system are selected and determined by vote.

Holders of Neuron coins can participate in a vote on a delegate or CM or on a proposal submitted by a committee member.

A holder of Neuron coins has the right to proxy their vote to another coin holder. Casting your vote or setting your proxy is very simple using the interface of the block explorer. If you have not set a proxy, you can vote for a Delegate, CMs and publish your vote.[14]

Unlike BitShares, the NeuronChain blockchain supports the DPoI mechanism, whereby not only the status of the voter balance, but also its network activity is taken into account when determining the "Importance" value. NeuronChain believes that both factors are important to determine the level of participation a user has in the network. Being solely concerned about the bank balances of individuals can lead to a cognitive anchoring on finance.

4. Governance

NeuronChain is governed in a democratic way. The right to take decisions on changing the network state is delegated to a specialized body called the Committee. CMs are elected by network participants by direct vote. More details on the mechanism of electing CMs are given in 3.4.

Newly elected CMs become eligible to take decisions on changing network parameters. Since, as noted earlier, the NeuronChain network is governed in a democratic way, the right to propose changes in the network parameters is granted to any network participant. For this reason, a network participant wishing to make such a proposal must create a corresponding “proposal transaction”.

To create a “proposal transaction”, we use the transaction builder API. Create a transaction builder request with begin_builder_transaction command:

>>> begin_builder_transaction

>>> add_operation_to_builder_transaction $HANDLE [12,{"fee": {"amount": 100000000, "asset_id": "1.3.0"}, "issuer": "1.2.0", "asset_to_update": "1.3.113", "new_options": { "feed_lifetime_sec": 86400, "minimum_feeds": 7, "force_settlement_delay_sec": 86400, "force_settlement_offset_percent": 0, "maximum_force_settlement_volume": 200, "short_backing_asset": "1.3.0", "extensions": []}, "extensions": []}]
>>> propose_builder_transaction2 $HANDLE init0 "2015-12-04T14:55:00" 3600 false

>>> set_fees_on_builder_transaction $HANDLE BTS >>> sign_builder_transaction $HANDLE true[15]

These network parameters include everything from transaction fees to block sizes, Delegate’s reward and block intervals.

Proposals on changing the network parameters are put for voting by CMs , this is a governance function included in NeuronChain itself. Votes are counted with the IS of each candidate being equal to ∑ IS of all network participants, who have voted for this candidate. It means that in fact each CM acts on behalf of those network participants, who have cast their votes in his or her favor.

[14] http://docs.bitshares.org/tutorials/voting.html?highlight=proxi
[15] http://docs.bitshares.org/bitshares/tutorials/committee-propose-action.html

A decision on changing the network parameters is deemed to be taken by the Committee if it is approved by CMs with a total of 50%+1 IS of the aggregate IS of all CMs.

Following the approval of changes of the network parameters by a majority vote of the Committee, corresponding information on the essence of the changes is distributed in the network (forwarded to all network participants). In this situation, no change in the network parameters shall become effective instantaneously and thus taking network participants by surprise. Accordingly, any Committee decision on changing the network parameters comes into force upon expiry of a certain term. The date when the changes in the network parameters become effective is also a network parameter that can be changed.

Decisions taken by the Committee may not be changed; however, if network participants believe that any CMs or a group of CMs they have voted for take decisions against the interest of the network, the network participants may cast their votes for any other candidate in the next maintenance timeslot. This is how the network can control actions of CMs.

5. NeuronChain architecture

5.1. Data storage

Just like in any other cryptocurrency system, NeuronChain looks like a chain of blocks that go one after another. Each complete node in the NeuronChain blockchain stores a full copy of the chain of blocks, and can verify the correctness of the records, as well as release new blocks.

A block is composed of:

- pointer to the previous block
- date and time
- secret hash
- secret of the previous block
- set of transactions
- block producer's signature

5.2. Irreversibility of transactions

How to determine at what point the block transaction is considered to be irreversible:

Let us take the number of Delegates (N) and the last blocks that they signed. The irreversible validation of a block is determined by the number of blocks that follow it and the amount greater than or equal to 66% of number of Delegates (N).

If, as an example, we only have 17 Delegates and a 3-second block confirmation interval, then it takes an average of 34 seconds.

If we have 101 Delegates and a 3-second block confirmation interval, then it takes an average of 3.3 minutes to make the block irreversible.

Understanding this metric helps to avoid misunderstanding in the event of a network failure or de-synchronization of Delegates.

Acceptance of a transaction, before full validation is obtained, poses additional risks for the user who is engaged in it.

5.3. P2P network

A peer-to-peer network is used to distribute the blockchain's ledger throughout the world.

The network consists of open, private and seed nodes, which are used to connect to the p2p network. Anyone can connect to any node and synchronize blockchain data.

Once a node has synchronized the data via the p2p network, it starts accepting newly created blocks and helps other nodes to get them, in order to synchronize the network around the world.

To ensure a minimum network latency, it is recommended that 2 nodes located at different geographic locations ping each other in less than 250ms.

Furthermore, in order to minimize network latency, each node,(once it has received and verified the data) sends the data out to all other nodes that it is linked with.

5.4. Consensus mechanism

NeuronChain uses an updated DPoI + TaPOS + Deppen hybrid consensus mechanism, which provides a high level of security. Evaluation of significance in NeuronChain gives each vote a weight that is calculated by means of a special algorithm and takes into account a user balance and the qualitative characteristics of the voter's transactions.

TaPOS is a mechanism that prevents recurrence of transactions. The transaction contains the header hash of the last known block. This prevents recurrence of transactions, as well as informing the network about what blocks are being produced.

Deppen is a mechanism wherein deposits and penalties can be applied. In order to become a block producer (a Delegate), one needs to make a deposit. If such a producer attempts any harmful action, they are fined a penalty related to their deposit. This mechanism is designed to solve the 'nothing at stake' issue (a producer bears zero risk).

If a Delegate starts to produce blocks for several branches simultaneously, the system automatically writes off the funds from the Delegate's account (deposit) in the amount of the penalty. Therefore, it is not economically feasible for a producer to compete with other producers by creating branching.

5.5. Transactions

Capitalizing on BitShare's structure, NeuronChain also uses the concept of "Operation"[16].

An Operation is defined as:

- A transfer of funds or NRON
- Voting for a Delegate
- Voting for a CM, etc.

After Operations are defined, they are used to make up a "Transaction list" and all "Transactions" are carried out based on that list.

A Transaction consists of:

- Expiration date
- Block number indicator

[16] http://docs.bitshares.org/bitshares/user/transactions.html?highlight=operations#a

- Block prefix indicator
- Set of extensions
- Set of signatures for each operation

5.6. Proposed / multi-signature transactions[17]

The so-called “multi-signature” mechanism requires the consent of 2 or more NRON coin holders for all transactions. Such transactions are only partially valid and not performed until they are fully confirmed (fully validated).

The user submits a transaction and other “signatories” (coin owners) add or remove their confirmation of the transaction. When the required number of confirmations is reached, the proposed operation is used to create a transaction that is subsequently executed. If the transaction fails, it is stored until its expiration date. If, before the expiration date, the confirmation terms are met, the transaction will still be executed.

The transactions that were not executed within the allotted time window can still be conducted using the proposal mechanism. Once the transaction is successfully completed, the proposal is marked as “authorized”.

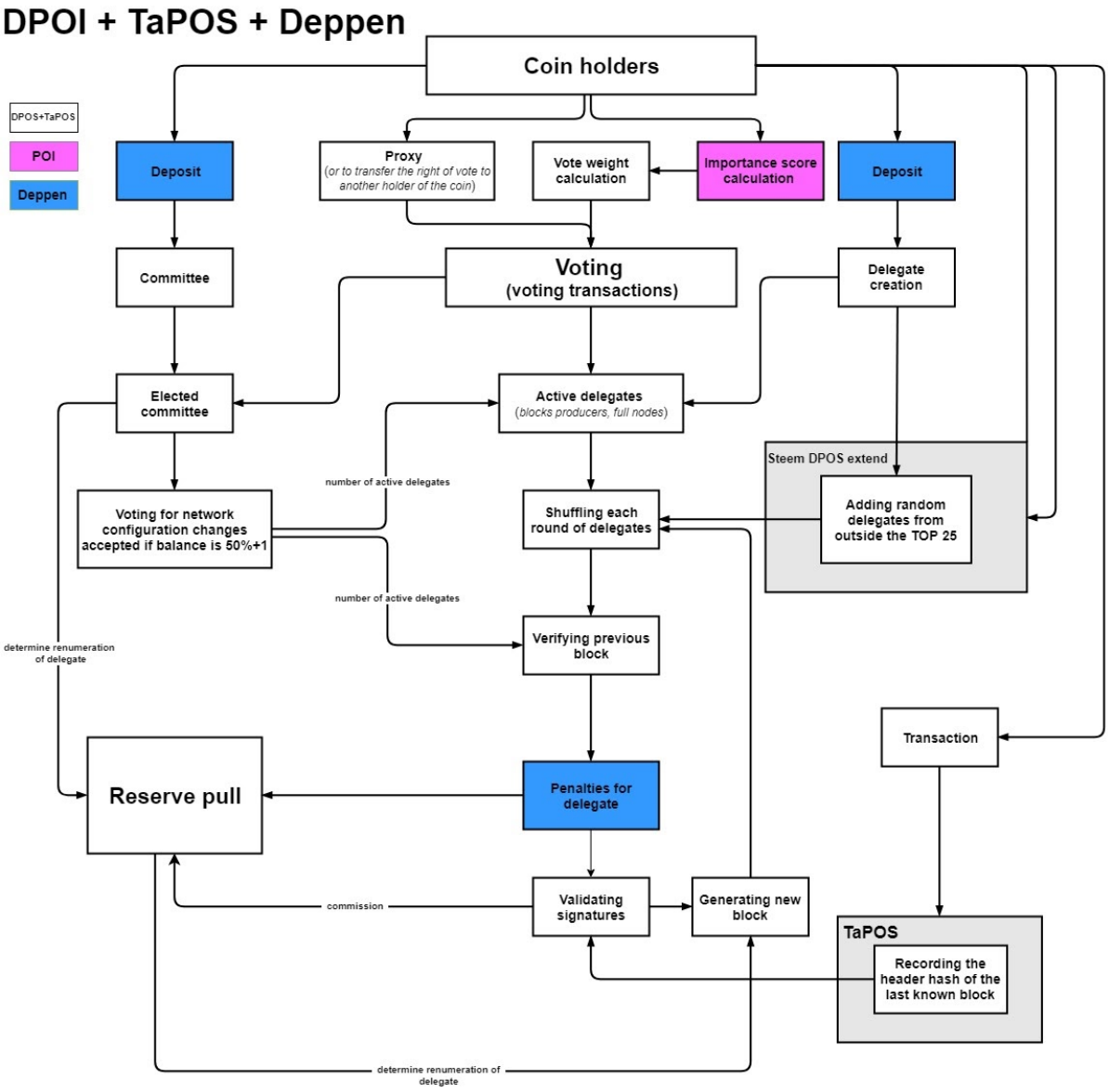
6. DPoI implementation

The NeuronChain DPoI consists of the following elements:

1. BitShares core[18];
2. BitShares delegates system[19];
3. Definition of "significance" (partially NEM’s[20]/ partially NeuronChain’s proprietary development);
4. System of deposits and penalty - Deppen; implementation - NeuronChain;
5. Block producer stimulation (Steem)[21].

[17] https://bitshares.org/doxygen/group__proposed__transactions.html
[18] http://docs.bitshares.org/installation/Build.html
[19] http://docs.bitshares.org/bitshares/tutorials/witness-howto.html
[20] https://github.com/NemProject/nem.core
[21] https://github.com/steemit/steem-js

6.1. Process flow chart



7. Calculation of importance score

Importance score is calculated based on two parameters:

1. Current account balance
2. The number of outbound transactions

In the course of the network maintenance process[22], a transaction graph is generated.

All transactions that have occurred since the previous maintenance are considered.

It also includes transactions with the scope of transfer greater than the set value, which is a dynamic network parameter (in the current version, the default value is 1,000 NRON).

[22] The system status with all service processes ongoing at once: vote calculation, importance score calculation, etc.

For the accounts, this graph contains the calculated number of outgoing (spend) transactions.

Next, the system searches and counts the looped transaction for this account. The number of loops is subtracted from the number of transactions.

The obtained value is written into the account statistics.

The next step is to take the account statistics and take the calculated number of transactions for a certain period.

Period considers from the N block (which is also a network parameter, with the default value of 43,200).

As a result:

- **Transaction rate** = calculated number of outbound transactions (greater than 1,000) less the cyclic transactions for a given period.
- **Current balance** = current account balance
- **Balance multiplier** = dynamic network parameter (0.5 by default)

=> **Importance Score** = transaction rate + balance multiplier * current balance

7.1. Importance Score value calculation

A network user's vote weight is based on importance score as suggested in NEM[23][24].

Find below the Importance Score algorithm calculation procedure.

7.2. Requirements for User Vote Importance Scoring

To be eligible for Importance Scoring, more than 10,000 NRON has to be on a user's account (as defined as network parameter set by the CM's).

The principal Importance Score (ψ)equation:

$$\psi = (normalize_1(max(0, \nu + \sigma\omega_o)) + \hat{\pi}\omega_i)\,\chi$$

including:

$$normalize_1(\upsilon) = \upsilon \,/\, ||\upsilon||$$

ν — account balance in NRON

σ — weighted net loss in NRON

$\hat{\pi}$ —NCRawareRank value (see 6.5)

χ — weight vector, considering transaction graph topology (0.9 for isolated vertices and hubs and 1 for cluster elements)

ω_o, ω_i — appropriate constants (initially, 1.25 and 0.1337, respectively)

The important calculation stages are:

- the transaction matrix creation
- the transaction graph clustering
- the NCDawareRank (see 7.5)

[23] https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf
[24] https://github.com/NemProject/nem.core

7.3. Transaction Matrix

Assuming, that Importance Scoring occurs in block N, multiple outgoing transactions are selected for all the accounts being scored to meet the following criteria:

- Transfer amount is greater than or equal to 1,000 NRON
- Transaction has been effected in one of the 864,000 latest blocks (≈ 30 *days*)
- Beneficiary participates in the Importance Scoring procedure

Then, each transaction is weighted:

$$\omega_{ijk} = amount * exp(ln(0.9) \left[(h - h_{ijk}) / 28800 \right]$$

where i – payer ID, j - payee ID, k - transaction ID. h_{ijk} - block ID, where the transaction is recorded.

Then, the transaction weights are aggregated as $\hat{\omega} = \sum_k \omega_{ijk}$ and netted for loss $\hat{o_{ij}} = \hat{\omega_{ij}} - \hat{\omega_{ji}}$. In case $\hat{o_{ij}} < 0$, then the value is zeroed as $\hat{o_{ij}} = 0$. The end matrix values are normalized as $o_{ij} = \hat{o_{ij}} / \sum_i o_{ij}$. In case $\sum_i o_{ij} \leq 0$, then the matrix value is zeroed as $o_{ij} = 0$.

Thus, the transaction matrix represents the weighted value of the NRON net outgoing flow, between the respective accounts for the last 30 days. Given this, the earlier the transaction, the lower is its relevance for Importance Scoring.

7.4. Graph Clustering

The transactions' graph is clustered using the SCAN[25] algorithm, which draws on the search for the basic cluster vertices, with the follow-on cluster expansion based on those.

The clustering algorithm divides the graph into clusters, hubs and isolated vertices based on the structural similarity measure:

$$\sigma(u, v) = |\Gamma(u) \cap \Gamma(v)| / \sqrt{|\Gamma(u) \cap \Gamma(v)|}$$

where $|.|$ is the power of the set and Γ is the set of adjacent vertices:

$$\Gamma(u) = \{v \in V \mid \{u, v\} \in E\} \cup \{u\}$$

The vertices relate to one cluster provided their structural similarity measure is higher than the preset threshold.

$$N_\epsilon(u) = \{v \in \Gamma(u) \mid \sigma(u, v) \geq \epsilon\}$$

If a vertex has many similar neighbors (over μ), then such vertex becomes the base one for cluster creation (cluster nucleus).

$$CORE_{\epsilon,\mu}(v) \Leftrightarrow N_\epsilon(v) \geq \mu$$

Clusters propagate from the nucleuses. The vertices, that are similar to the base one, are added to the cluster.

[25] Xiaowei Xu, Nurcan Yuruk, Zhidan Feng, and Thomas AJ Schweiger. Scan: a structural clustering algorithm for networks. In Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, pages 824–833. ACM, 2007.

$$DirREACH_{\epsilon,\mu}(u,v) \Leftrightarrow CORE_{\epsilon,\mu}(u) \wedge v \in N_{\epsilon}(u)$$

The clustering algorithm looks as follows:

ALGORITHM SCAN($G =< V, E >, \epsilon, \mu$)

// all vertices in V are labeled as unclassified;

for each unclassified vertex $v \in V$ do

// STEP 1. check whether v is a core;

if $CORE_{\epsilon,\mu}(v)$ then

// STEP 2.1. if v is a core, a new cluster is expanded;

geNRONate new cluster ID;

insert all $x \in N_{\epsilon}(u)$ into queue Q;

while $Q \neq 0$ do

y = first vertex in Q;

R = $\{x \in V \mid DirReach_{\epsilon,\mu}(y,x)\}$;

for each x ∈ R do

if x is unclassified or non-member then

assign current cluster ID to x;

if x is unclassified then

insert x into queue Q;

remove y from Q;

else

// STEP 2.2. if v is not a core, it is labeled as non-member

label v as non-member;

end for.

// STEP 3. further classifies non-members

for each non-member vertex v do

if ($\exists x, y \in \Gamma(v)$: $x.clusterID \neq y.clusterID$) then

label v as hub

else

label v as outlier;

end for.

end SCAN.

7.5. NCDawareRank Algorithm

NCDawareRank is another significant component of the Importance Scoring in DPoS. The NCDawareRank is calculated as follows:

$\hat{\pi} = O\eta\pi + M\mu\pi + E(1-\eta-\mu)\pi$

O — transaction matrix;

M — transactions graph clusters' matrix;

E — transition probability matrix (between clusters);

π — NCDawareRank (recursion formula);

η — constant share of transactions' matrix importance (initially: 0.7);

μ — constant share of clusters' matrix importance (initially, 0.1).

The NCDawareRank algorithm A_k blocks are determined by the SCAN graph clustering algorithm.

Let χ_u , i.e. set of adjacent accounts, be designated as follows:

$$\chi_u = \bigcap_{\omega \in (u \cup G_u)} A_{(\omega)}$$

$A_{(\omega)}$ - NCD block, with ω vertex;

G_u – n of adjacent accounts in the transactions' matrix (non-zero elements in μ line).

The M matrix can be found as $M_{v,u} = 1 / N_u \, |A_{(v)}|$ (if $v \in \chi_u$, or 0 otherwise).

The E matrix has a simple formula: $E = ev^T$, where e is the single vector and v^T is the transition probability matrix.

NCDawareRank per se is calculated iteratively:

$$NCDawareRank^r(i) = (1-\eta-\mu) / |G| + \sum_{k=1}^{s} (\eta o_{ik} + \mu m_{ik}) * NCDawareRank^{r-1}(k)$$

o_{ik} and m_{ik} - elements of O and M matrices, respectively.

The algorithm runs until the difference of NCDawareRank values between the iterations is higher than the preset ϵ constant.

7.6. Resistance to Manipulations with Importance Score

There are multiple scenarios of possible manipulations, all designed to seize the majority of the network votes. However, the complex Importance Scoring mechanism secures sustainability to such manipulations.

8. Loop Attack

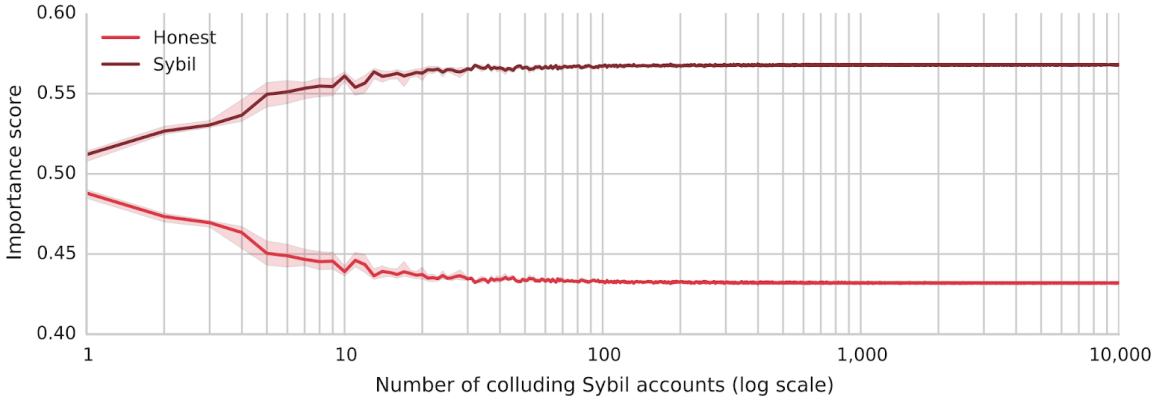
The simplest scenario to overstate the Importance Score consists of performing multiple transactions that create a loop in the graph. Indeed, the outgoing NRON flow (spend transaction) is essential for the Importance Score. However, in the DPoI, the incoming flows are subtracted from all the outgoing ones, which results in net outgoing flow. Therefore, it does not make a difference whether an account sends 10,000 NRON a million times or once.

9. Sybil Attack

The Sybil attack is another potential scenario of excess Importance Score inflation, which boosts multiple account creation by malicious users for multiple transactions between them, e.g. to increase NCDawareRank.

To counter such an attack, the following factors apply in the Importance Scoring:

- The NCDawareRank algorithm is by design more sustainable to such attacks than, for example, PageRank.
- Similar to crossing a loop attack, high values cannot be secured in the transactions' matrix.
- Transaction input into the Importance Score declines over time.
- The Importance Score determines the share of importance versus all network users, so the number of transactions passing the network impacts on individual Importance Scores.
- The minimum surplus account balance requirement will not allow creation of an indefinite number of fake accounts.
- The current account balance is a significant plus for one's Importance Score.



This graph shows a simulated Sybil attack where multiple extra accounts are generated and random transfers are made. In the meantime, a regular "honest" account makes no transaction at all. We see that although such steps beef up the Importance Score (reasonably though, because the attacker is network-active and makes transactions for a fee), yet the Importance Score increment is limited and does not speed up by the amount of accounts created. Additionally, in a real-life network scenario, other users will also be generating transactions, and therefore, the attacker's share will be much less.

Appendix: Terminology

Block Explorer: The block explorer is NeuronChain's native web application accessible through a compatible browser that allows anyone to search and navigate the blocks of the NeuronChain blockchain, their contents, and their relevant details.

Committee Member: An elected network user, who may vote on the blockchain changeable parameters and who meets the requirements set forth in clause 3.4. hereof.

Delegate: A block certifier, a user, who collects, verifies and logs in system blocks transactions that meet the requirements set forth in clause 3.1. hereof.

Genesis Bock: The genesis block is the first block of the NeuronChain blockchain.

Holder: A participant of the NeuronChain Network that owns NRON.

Incoming/Inbound transactions: A transaction a participant of the network receives through conducting a transaction with another party of the network.

Maintenance Time: A service state of the system, in which information on the network state change is processed.

Open Node: A node open for connection.

Outgoing/Outbound transactions: A transaction of debiting NRON from the holder's wallet and crediting the same to the wallets of other NeuronChain participant.

PageRank: A link ranking algorithm. PageRank applies to accounts linked with each other and assigns each of these accounts a digital index, which in turn denotes the "importance", or in other words, "authority" of this account as compared to all other accounts known in the system.

Private Node: A node "elevated" without external links.

Reserve Pool: A pool used for collection of transaction fees and for remuneration of delegates and employees.

Stakeholders: NRON coin holders.

Seed Node: Nodes that provide, upon connection thereto, reliable information about availability of other nodes in the network.

Witness: Witnesses are transaction signatures of the NeuronChain blockchain.