Sphere: A Decentralized Economy-Based Electronic Currency

Egger Mielberg

egger.mielberg@gmail.com

Abstract. A decentralization of electronic currency would allow business activity and development of a single network to be independent of other different business networks. Cost of a decentralized currency of the network can become stable as long as participants of that network are still active.
We propose a solution for such a big problem of traditional economy as a "direct dependency of local prices on global ones".
We also propose an innovative mechanism that allows participants of NCN to get any service of one business network for money (hours) earned in other network ('s).
The currency is implemented by usage of two innovative technologies, "Proof of Participation protocol" (PoP) [3] and "Smart Transactions" [2].

1. Introduction

Traditional finance system is not enough transparent and opened for their daily customers. The principles which it is based on are self-centered. In essence, it does not produce a product of any kind but has a great influence on almost all business fields of global economy. Why is that? The answer is obvious, "Global Control".

Centralization of the system leads to such a problem as inflation. Meantime, the inflation is a result of reduction of gold reserves in a "Gold Standard" monetary system. In other words, a price of bread will likely go up if a value of the gold reserve goes down. Then, the question that appears is "Why would Alice from Arizona have to pay the same price for the bread as well as Bob from New-York does who is unemployed?".

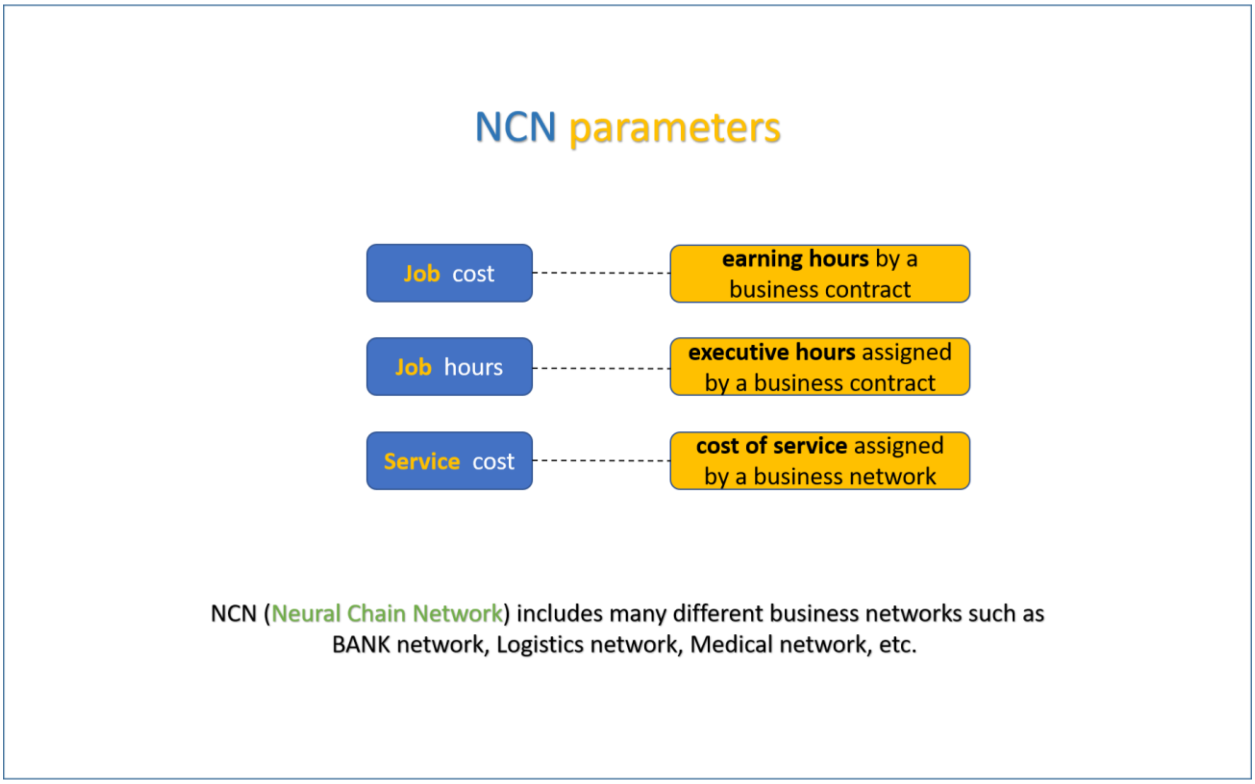
In our vision, a decentralization of business activity of any kind will totally vanish such a notion as inflation. We are confident of possibility to be locally and economically independent for each business unit. A decentralized electronic currency will let the business units form its own economy-based prices on local business network.

2. Decentralization of Currency

In compared with traditional currencies such as US dollars, Euros or other ones, a decentralized currency has a series of advantages. Among the advantages are “an independence of job cost of one business activity from other one”. For example, if a participant of Logistics network has ten years of logistic experience and many of his or her business contracts are executed in that network, any negative economic changes in other business network cannot greatly change the participant’s job cost.

The Advantages:

a. **No Inflation**. The cost of the currency is being formed exclusively inside the network and depends directly on business activity in such network.
b. **Minimum Level of Unemployment**. As the currency is equivalent to hours earned by a business contract and that hours can be exchanged for any service of any business network of NCN, the participant will extremely motivated to earn as many hours as possible. In compared with traditional market, in order to get some service or job the only one the participant will need is hours.
c. **Flexible convertibility**. The currency can be converted as in fiat currency as in other electronic currency by corresponding calculation of a job cost.



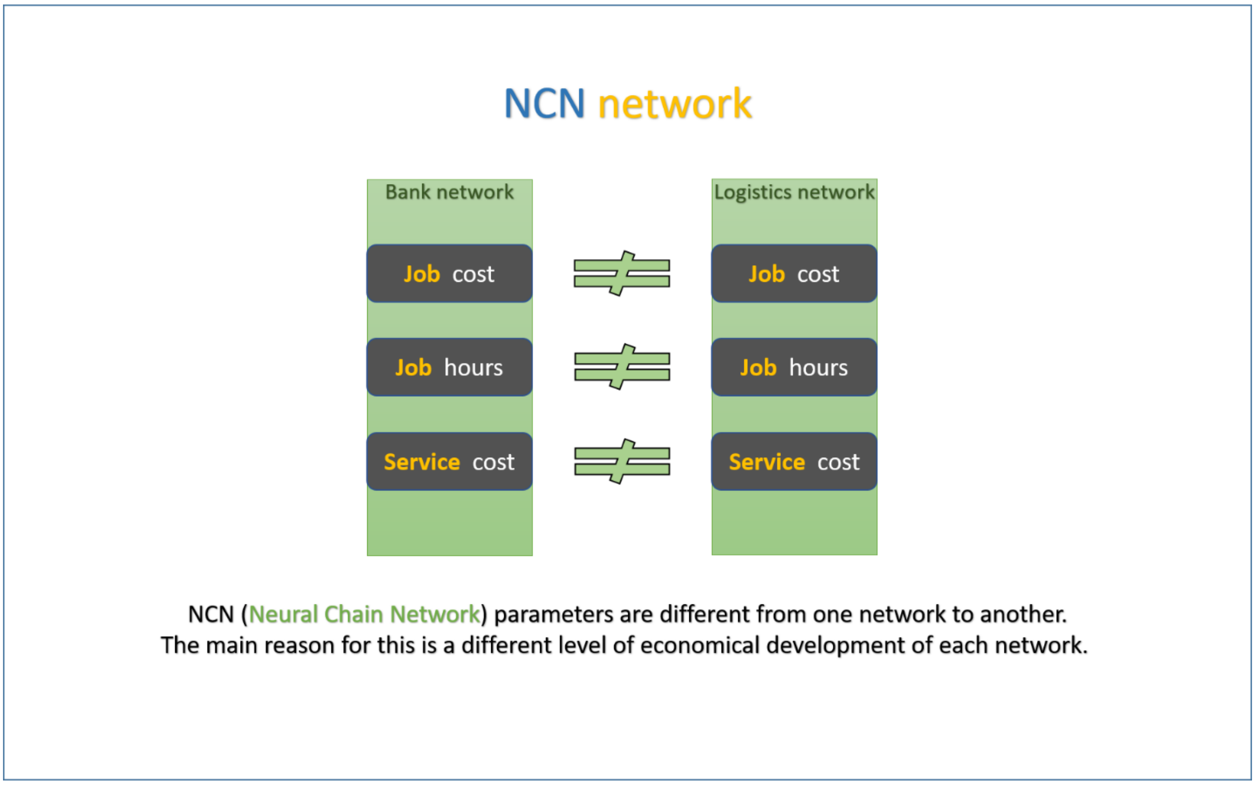
NCN parameters

Job cost — **earning hours** by a business contract

Job hours — **executive hours** assigned by a business contract

Service cost — **cost of service** assigned by a business network

NCN (Neural Chain Network) includes many different business networks such as BANK network, Logistics network, Medical network, etc.



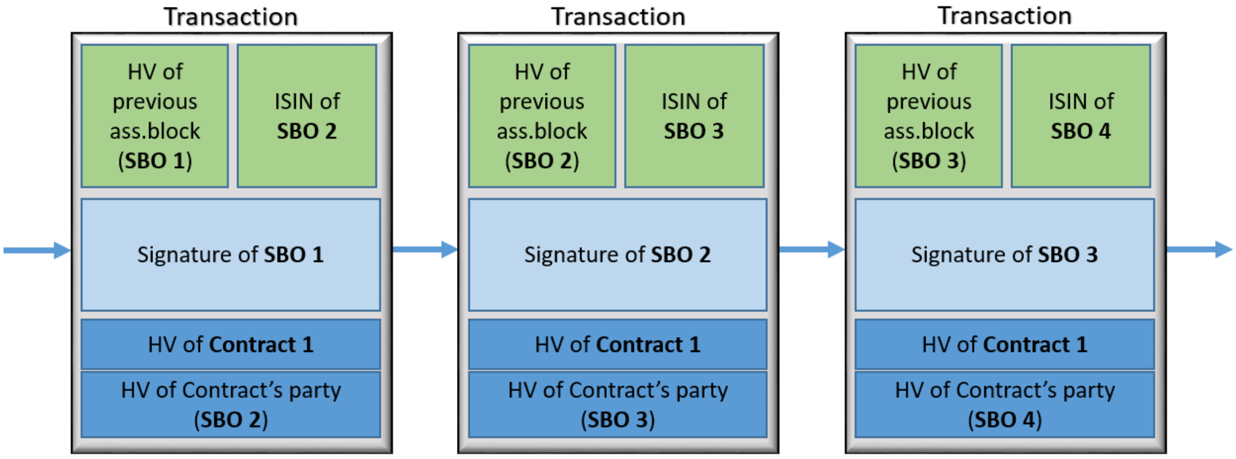
NCN network

Bank network		Logistics network
Job cost	≠	Job cost
Job hours	≠	Job hours
Service cost	≠	Service cost

NCN (Neural Chain Network) parameters are different from one network to another.
The main reason for this is a different level of economical development of each network.

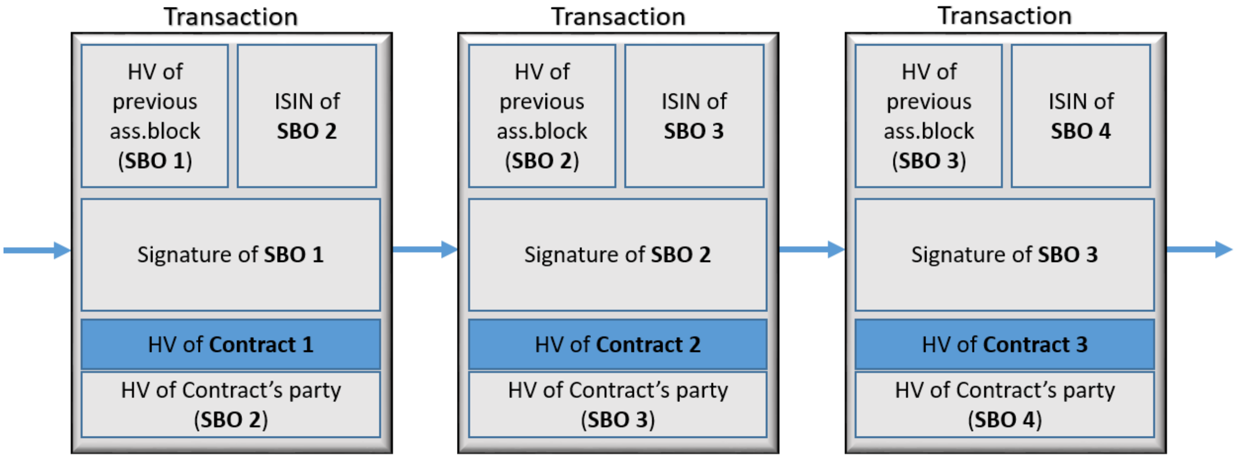
3. Transaction of Currency

SphereCoin is an electronic currency that is defined as a chain of electronic contracts. Standard unit of the currency is “minute” (hours). Minutes and hours are strictly associated with a signed contract. An owner of SphereCoin can transfer it to other one by digitally signing a hash of the previous block of associative chain and ISIN [3] of the next owner with two hashes, “hash of the contract” and “hash of the contract’s party (recipient)” attached to the signature.


Transaction
HV of previous ass.block (SBO 1)
ISIN of SBO 2
Signature of SBO 1
HV of Contract 1
HV of Contract’s party (SBO 2)
Transaction
HV of previous ass.block (SBO 2)
ISIN of SBO 3
Signature of SBO 2
HV of Contract 1
HV of Contract’s party (SBO 3)
Transaction
HV of previous ass.block (SBO 3)
ISIN of SBO 4
Signature of SBO 3
HV of Contract 1
HV of Contract’s party (SBO 4)

“**SBO**” – Smart Box Owner

In compared with Bitcoin transactions, SphereCoin transactions have a series of security-focused advantages. Among them are a usage of previous associative block’s hash value and a strict connection of each transaction to a signed business contract.

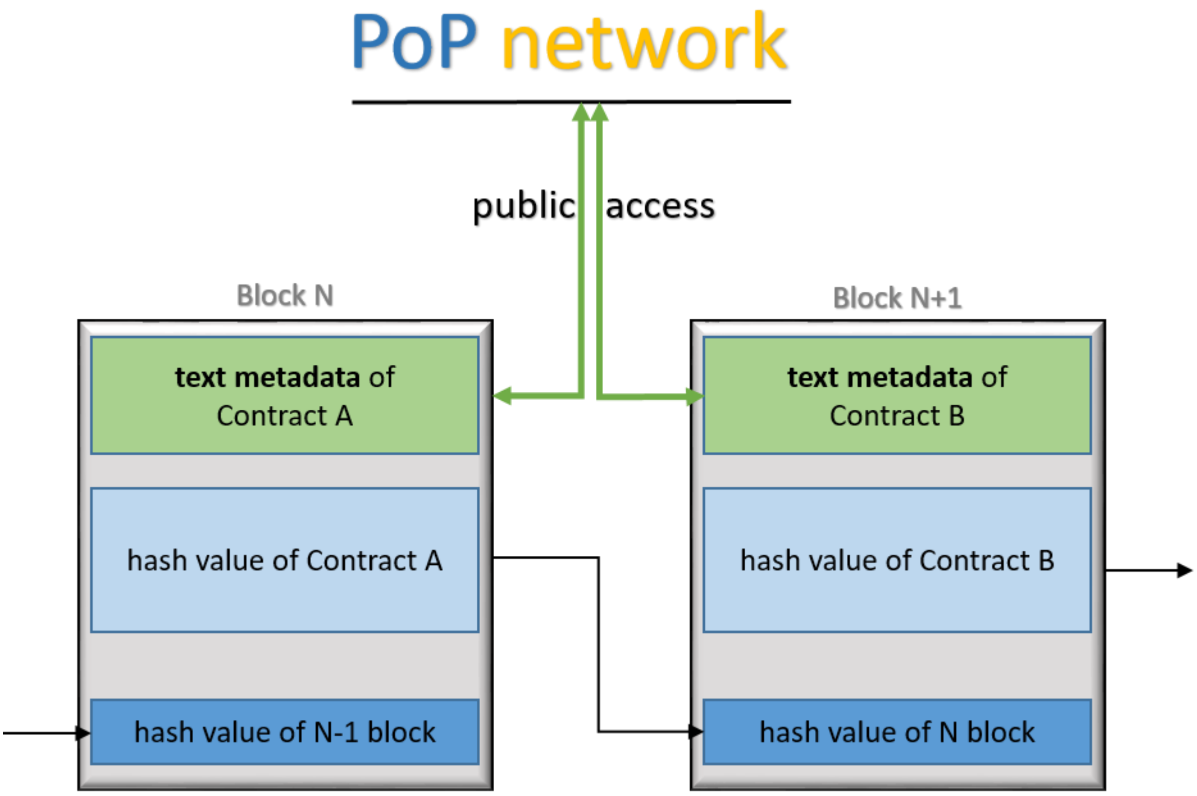

Transaction
HV of previous ass.block (SBO 1)
ISIN of SBO 2
Signature of SBO 1
HV of Contract 1
HV of Contract’s party (SBO 2)
Transaction
HV of previous ass.block (SBO 2)
ISIN of SBO 3
Signature of SBO 2
HV of Contract 2
HV of Contract’s party (SBO 3)
Transaction
HV of previous ass.block (SBO 3)
ISIN of SBO 4
Signature of SBO 3
HV of Contract 3
HV of Contract’s party (SBO 4)

As seen on Figures above, a chain of transactions can be realized as inside a single contract as in a collection of many different contracts.

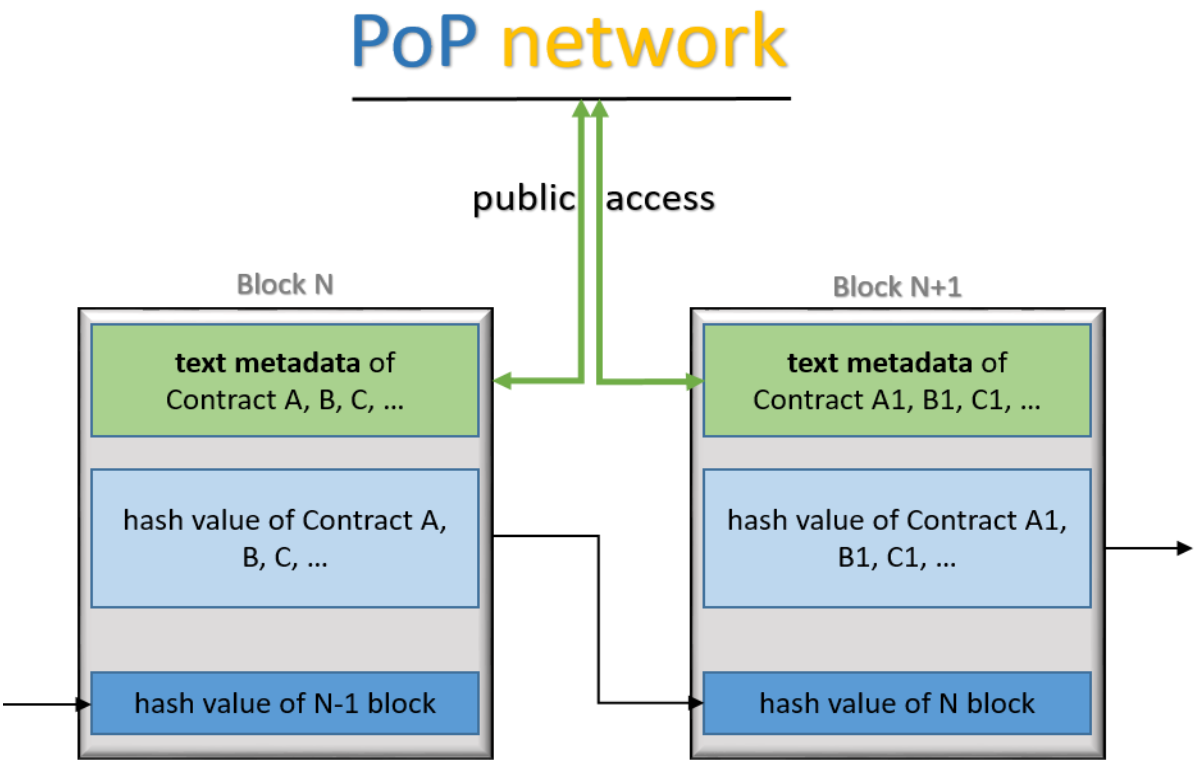
Implementation of SphereCoin transactions is totally realized by a usage of Smart Transactions technology [2].

4. Verification of Currency Transactions

As SphereCoin is directly tied to a business contract, the history of any transactions can easily be found and extracted from the metadata of a block [3]. The metadata can include information about as one contract as many different ones. Text type and publicity of the metadata allow users of NCN (PoP-based network) to fetch a contract-related information at any time without any cryptographic routines.



A block can also have more than one contract. In such a situation the metadata includes information about all contracts of the block.


PoP network
public access
Block N
Block N+1
text metadata of Contract A, B, C, …
hash value of Contract A, B, C, …
hash value of N-1 block
text metadata of Contract A1, B1, C1, …
hash value of Contract A1, B1, C1, …
hash value of N block

For security reason, the metadata can be separated from the block (as a different chain, for example) and stored in a different place (cache memory, different storage, etc.). In such a case, an attacker of the block (‘s) is most likely to be a party (‘s) of a contract. Thus, the attacker will be strictly limited to only his or her contract’s data.

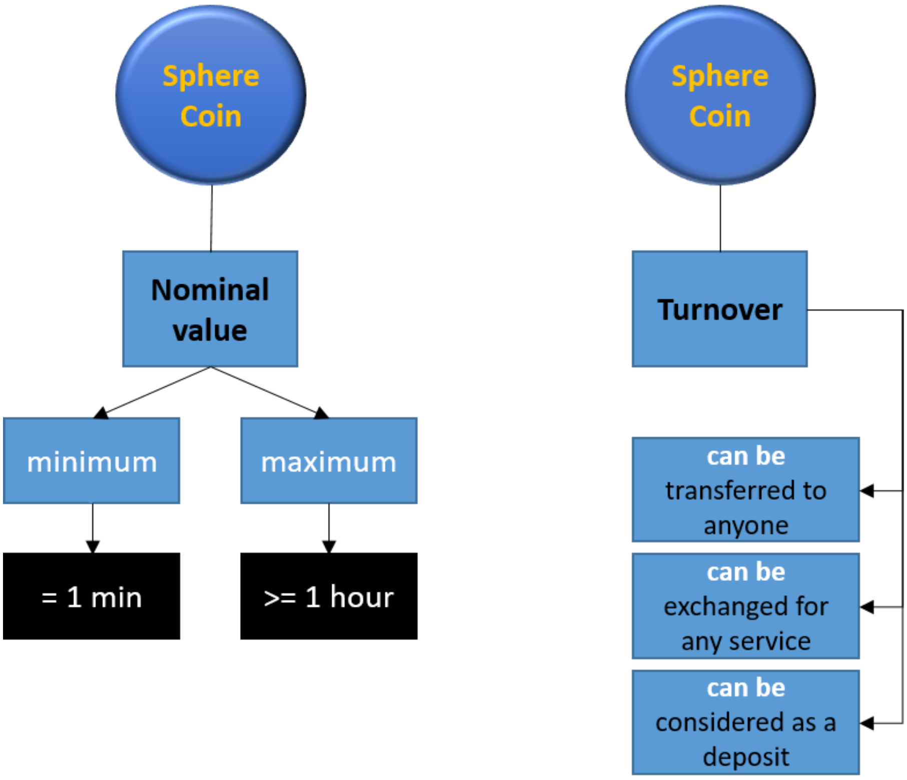
5. Measure Unit of Currency

SphereCoin is an economical value. This value is equivalent to a contract’s hours (job cost value) that a party of the contract earned by an execution of his or her responsibility.

“Minimum value” of SphereCoin is 1 minute (1 min.).

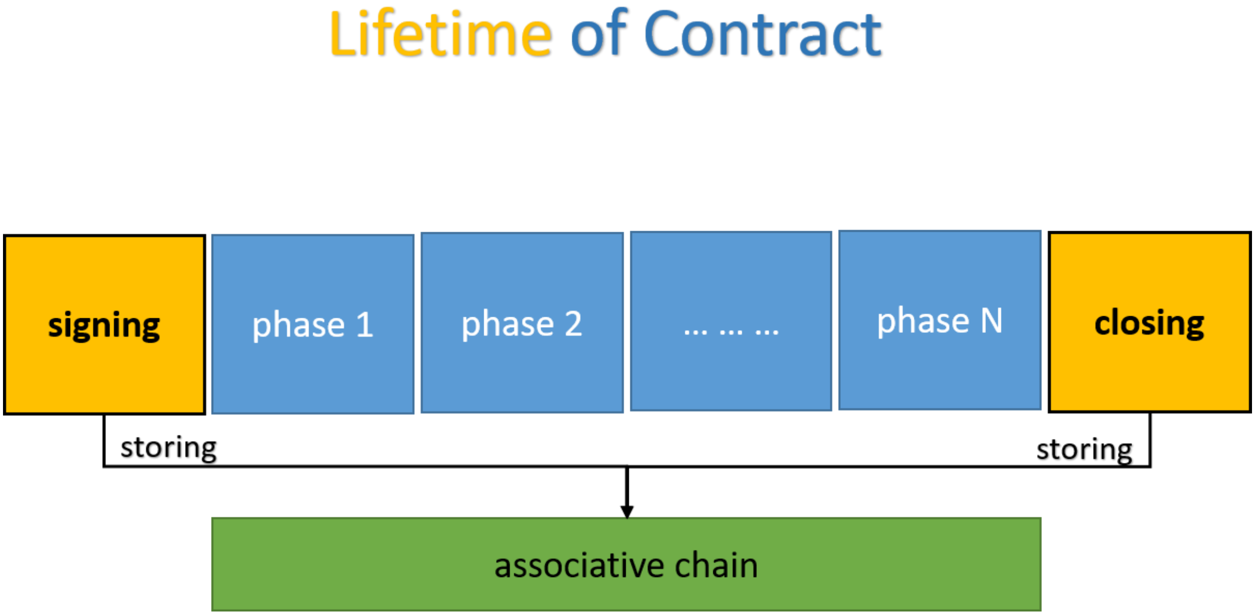
“Maximum value” of SphereCoin is finite number of hours (N hours).

Besides a possibility of transferring or exchanging, SphereCoin can be used for any contract in any associative chain as a means of deposit. This kind of SphereCoin usage is a powerful tool for a business guarantee of execution of a contract.


Sphere Coin
Nominal value
minimum
maximum
= 1 min
>= 1 hour
Sphere Coin
Turnover
can be transferred to anyone
can be exchanged for any service
can be considered as a deposit

6. Timestamp Chain

As shown in [3], the set of contract-related Smart Boxes forms a block for a specific associative chain. In NCN, a contract-related box ('s) is added to the chain twice in a process of execution of the contract.



During the process of contract execution (in any phase), each party stores all transaction information in its local storage (node storage). At time of closing the contract, all the information from each party is collected and hashed and then, added to a chosen chain.

A contract is considered as an opened (signed) one if and only if it was added to the chain. Likewise for a closed contract.

7. Distribution of Currency

As shown in [1], the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. It is intended to provide a way to initially distribute coins into circulation, since there is no central authority to issue them. In such approach, there is a huge gap between Bitcoin and real economy. In an attempt to replace a centralized system with a decentralized one, Bitcoin network enters a participant, a miner, that is not directly associated with an economic activity of the network. Thus, the miner can be considered as a third-party for the network.

In NCN, a distribution of SphereCoins is initialized by only participants of economic activity (contract's parties).

By convention, any transaction of NCN can only be executed through a signed contract. Thus, economy of NCN is being strictly formed by a business activity of its participants [3].

8. Currency Network

SphereCoin network is based and realized on "Proof of Participation" (PoP) protocol [4].

In compared with Bitcoin network [1], for example, SphereCoin network doesn't require its participants, *first*, to broadcast each transaction to all nodes, *second*, to work on finding a difficult "proof-of-work", *third*, to broadcast block of the transactions to all network's nodes, *fourth*, to check if all the transactions are valid.

The steps to run SphereCoin network as simple as follows:

1. "Job request" is multicast to all (several or one) nodes of a specific business network.
2. Node that accepted the "job request" unicasts back a "condition request" in form of a business contract.

3. Node that received the “condition request” can accept or drop it.
4. In case of accepting the “condition request”, all associated nodes choose party (‘s) of the contract that will be responsible for storing the contract-related transactions in an associative chain twice, right after signing and closing the contract. The nodes simultaneously also determine a fee for this job.
5. Nodes are responsible for creating a contract for any business activity as none of the transactions will be processed in NCN without contract’s hash value.

Nodes always need to form a contract to do anything in SphereCoin network.

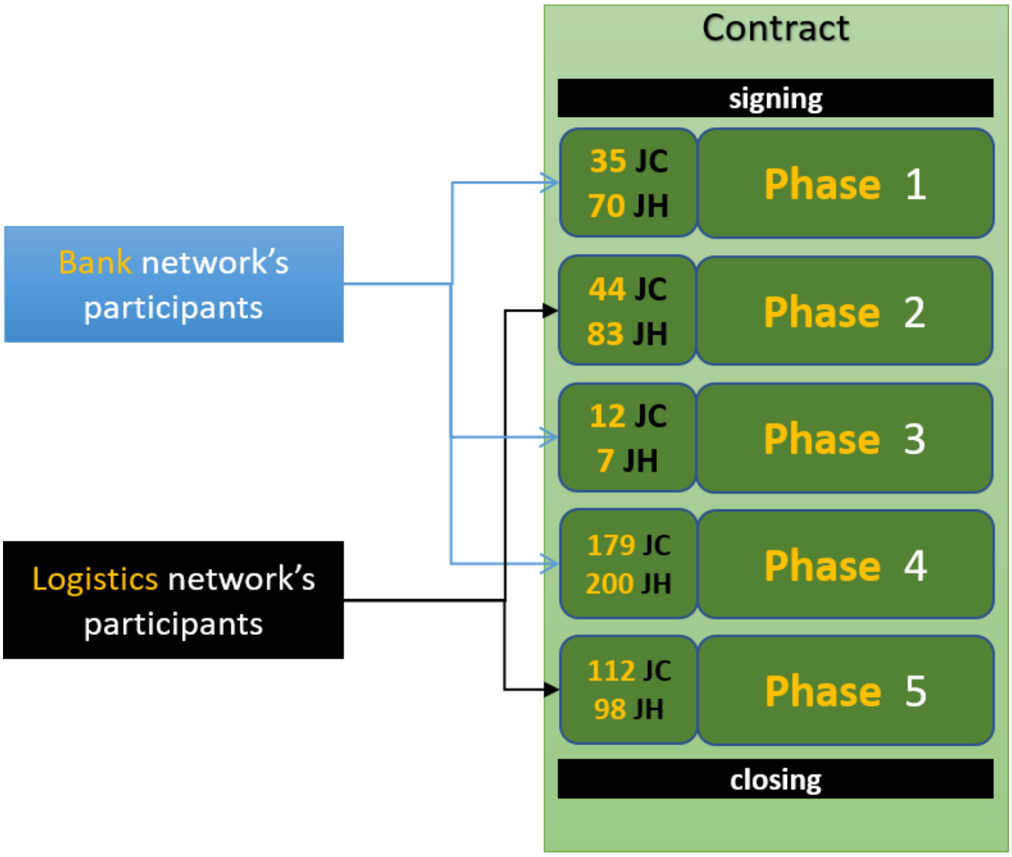
A set of business-related associative networks forms an intellectual network of the networks of services, IntellSphere (NoNoS or NNS).

Last block of an associative chain of IntellSphere the nodes are going to work with can be retrieved at any time by a “block request”.

9. Economy of Currency

In traditional market, any fiat currency is influenced by many different factors that lie in different business sectors. For example, US dollar can go up or down depending on current rate of oil price. The main problem of economy of the traditional market is an existence of direct dependency of local (micro) parameters on global (macro) parameters. For instance, a sugar price in a small town can greatly be influenced by an export price of country oil.

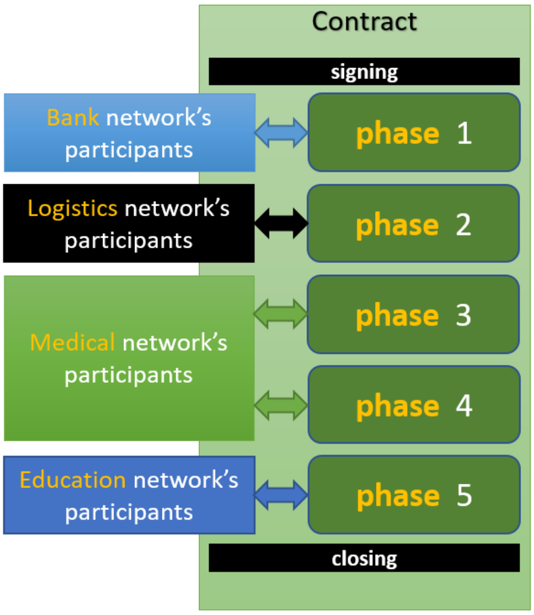
We propose an electronic currency that will totally remove that dependency. Decentralization of the currency allows it to stay stable inside a specific associative network and depend only on business activity of participants of that network. The measure unit of the currency is “hours” (minutes). Depending on level of network development, “job cost” as well as “job hours” can change from one business contract to another.



"JC" – Job Cost
"JH" – Job Hours

A business contract can be implemented in a single network as well as in many different ones. In other words, the contract can have parties from different networks worldwide.

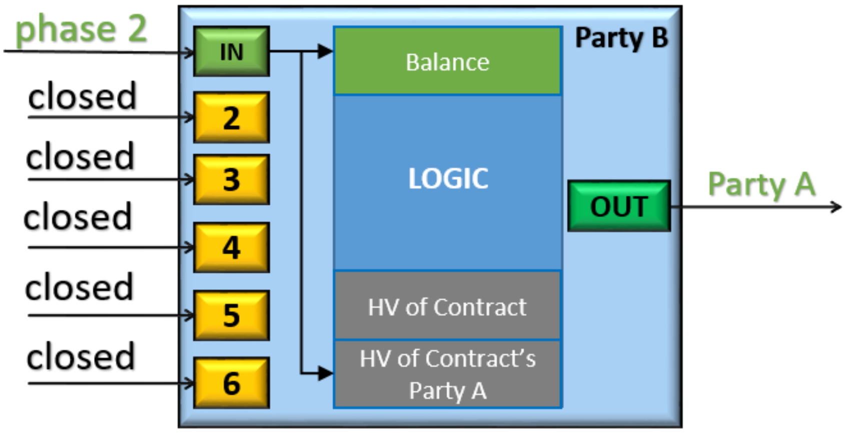
Necessity of participants (specialists) from many different networks for execution of a contract is due to the contract's complexity and economical constituents. As in traditional market, for example, for building a medical center many specialists from various business fields will be required.


Contract
signing
Bank network's participants
phase 1
Logistics network's participants
phase 2
Medical network's participants
phase 3
phase 4
Education network's participants
phase 5
closing

The contract can be implemented by participants from **different** associative networks

10. Smart Box Balance (SBB)

The balance of Smart Box [2] is a **private** and **invisible** component for external participants of NCN. There is only one condition upon which the balance is being revealed is a contract agreement.



“HV” – hash value

As shown in the picture above, a “balance request” can be executed if and only if it is arranged in the contract that Party A must check the balance of

Party B in the phase 2. No other conditions can validate the “balance request”.

On other side, any participant of NCN is eligible at any time to see:

a. other participant’s current status.
b. other participant’s contract information (type, phases, etc.).

Hash value of a contract’s party is revealed only between the contract’s parties. It is invisible for the external participants of NCN for security reason.

11. Sphere Currency Standard (SCS)

Solidity implementation:

```
contract SphereInterface {
        address internal HVCP;          // hash value of contract’s party
        address public constant HVC; // hash value of contract
        string public constant STC;     // start time of contract
        string public ETC;              // end time of contract
        string public constant SC;      // subject of contract
        mapping (address => uint) private balance;
        // balance of contract’s party
        mapping (address => uint) public costOfContract;
        // cost of contract
        mapping (address => uint) private jobCost;
        // cost of contract job for party
        mapping (address => uint) public jobHours;
        // contract hours needed for execution of party’s responsibility

        function getStatus(address participant)
                public
                returns (string state);   // status of participant of NCN
        function getChannelStatus(address HVCP, address HVC)
}
        internal returns (string[] HVCP)
    // status of contract’s party’s channel
    function transfer(address HVCP_from, address HVCP_to,
        address HVC)
        internal returns
        (bool success)
    // transfer between contract’s parties
    function getContractPhase(address HVC)
        public returns
        (string phase)            // current contract phase
    function getParticipantPhases(address participant,
        address HVC)
        public returns
        (string[] phases)
    // get current contract’s party’s phase
    function setETCValue(string _date) internal {
        ETC = _date;
        }                         // set end time of contract
    function getContractParticipants(address HVC)
        public returns
        (address[] participants)
    // get a list of contract parties

    event Transfer (address _from, address _to, address HVC,
        uint value);
    // put information about transaction into associative chain
}
```

SCS can also be realized by other programming languages along with a strong compliance to main concept.

SCS keeps two contract's value out of the public, "participant's wallet balance" (SBB) and "participant salary" (job cost). There are two reasons for that. *First*, security of a participant. *Second*, compliance with a business activity.

SCS allows to also realize additional security for participants by generating HVCP. Hash Value of Contract's Party is assigned to each party of a contract and allows to get the contract's chat strongly ciphered and secured.

12. Conclusion

We hope that our decent work will initiate a first step in building a new client-focused, decentralized and robust financial system with many possibilities to earn for anyone worldwide.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008

[2] E. Mielberg, "Smart Transactions: An In-To-Out Manageable

Transaction System", 2018

[3] E. Mielberg, "Proof of Participation (PoP): Asynchronous Byzantine

Activity-Oriented Protocol", 2018

[4] E. Mielberg, "PoP Protocol. Specification", to be published, 2018-19

[5] E. Mielberg, "Neural Chain: Decentralized chain of transactions", to be published, 2018

[6] "Digital currencies", Bank for International Settlements, https://www.bis.org/cpmi/publ/d137.pdf, 2015

[7] D. He, K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, T. Saadi Sedik, N. Stetsenko, C. Verdugo-

Yepe, “Virtual Currencies and Beyond: Initial Considerations”, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 2016

[8] K. Bartrem, J. Curtis, J. Dorosz, H. Hein, S. Landes, G. Mandile, K. Rahbari, C. Wondra, “Risks and Vulnerabilities of Virtual Currency. Cryptocurrency as a Payment Method”, https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf, 2017

[9] A. D’Alfonso, P. Langer, Z. Vandelis, “The Future of Cryptocurrency”, https://www.economist.com/sites/default/files/the_future_of_cryptocurrency.pdf, 2016

[10] K. Stewart, S. Gunashekar, C. Manville, “Digital Currency and The Future of Transacting”, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE254/RAND_PE254.pdf, 2017

[11] G. Peters, E. Panayi, A. Chapelle, “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective”, https://arxiv.org/pdf/1508.04364.pdf, 2015

[12] M. Bordo, A. Levin, “Central Bank Digital Currency and the Future of Monetary Policy”, https://www.hoover.org/sites/default/files/bordo-levin_bullets_for_hoover_may2017.pdf, 2017

[13] Y. Fanusie, T. Robinson, “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services”, https://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf, 2018

[14] R. Ali, J. Barrdear, R. Clews, J. Southgate, “The economics of digital currencies”, https://www.bankofengland.co.uk/-/media/boe/files/digital-currencies/the-economics-of-digital-currencies, 2014