Smart Transactions: An In-To-Out Manageable Transaction System

Egger Mielberg

egger.mielberg@gmail.com

21.04.2018

Abstract. Fully realized ACCP-based (Atomicity, Consistency, Concurrency, Permanency) online transactions would allow, *first*, to connect and manage all associative input transactions to a single output transaction, *second*, to eliminate any third party that is not a participant of transaction contract, *third*, to fully automate an execution of multi-steps contracts with a possibility to track them on every step, *fourth*, to promptly identify and extract any transaction data, and *fifth*, to dynamically scale a transaction network proportionally to the amount of its active participants.

We propose a mechanism that allow every single participant of the transaction network to dynamically manage any transaction on his or her own economic way.

1. Introduction

Billions of transactions of any kind are executed per minute on a daily basis. Some of this transactions include only two parties. Other transactions have much more than two ones. A single contract can have many parties with a set of specific functionalities and obligations per party. The main problem in a correct execution of the contract that include either many predetermined steps or many parties is to dynamically track and change contract conditions in case of all parties' agreement.

In our elaborated point of view, a solution of the problem is a smart transaction box that is customizable and manageable in real time by all parties of a single contract. Need for changes of contract's conditions is

triggered off by exclusively economical changes of the contract. The smart transaction box has an approximate internal structure of multipolar neuron. Like the multipolar neuron the box has many input channels and only one main output channel. Manageability of the box is realized through embedded voting system. The voting system allows parties of the contract to dynamically adjust any disputes between each other. By the flexible associative internal structure the box is capable of classifying all transactional inputs and composing a specific contract-related output in real time. The input and output can be any transaction-oriented data of any kind.

The smart transaction box can be implemented as a single server (node) or a single programmable module. A set of the boxes forms *a decentralized associative network*. The boxes of the network are bound to each other by exclusively one or many signed contracts. The process of identification in the network is based on two components, "*contract's hash value*" and "*hash value of contract's party*".

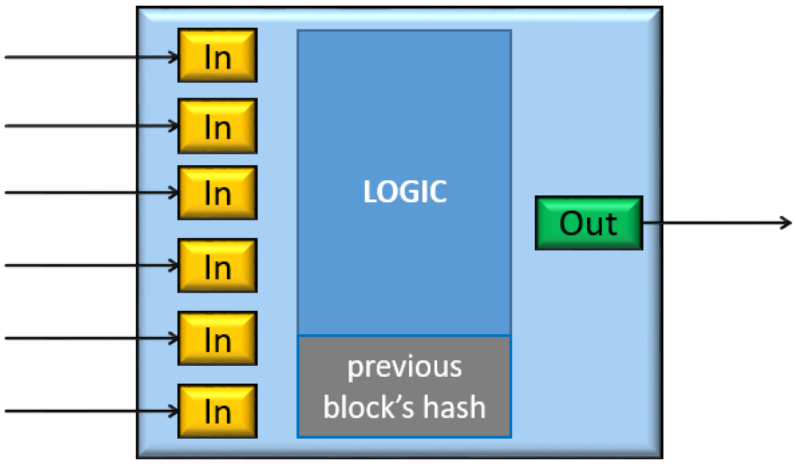
The network is secure as long as all parties of a contract are honestly interested in execution of a prescribed contract ('s). To hack a single contract or multi-contract network is practically impossible because of time that an attacker would need to decipher two hash values.

2. Smart Transaction (MISO)

2.1. Definition

We define a smart transaction as a smart box that has its own predetermined work logic. The work logic determines two components: input type and association policy between all possible inputs.

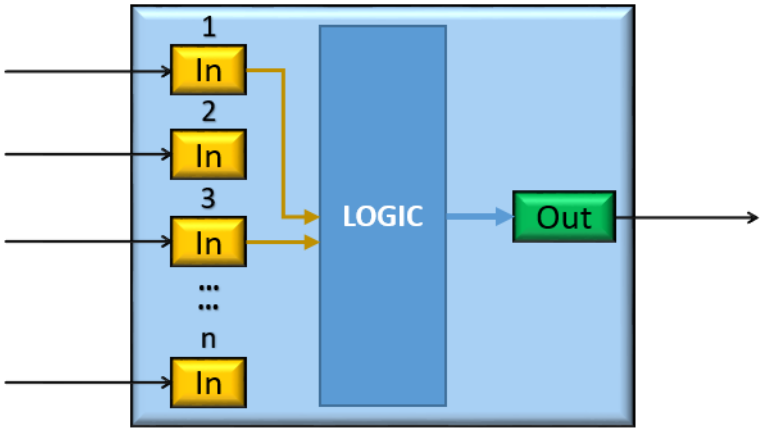
Smart Transaction



Structure of the smart box is designed by the principle of **MISO** (Multiple Inputs Single Output). The logic of the smart box is directly bound to and composed by a contract. The predetermined logic triggers outputs automatically. The logic has also a hash of previous block of an associative chain.

2.2. Functional schema

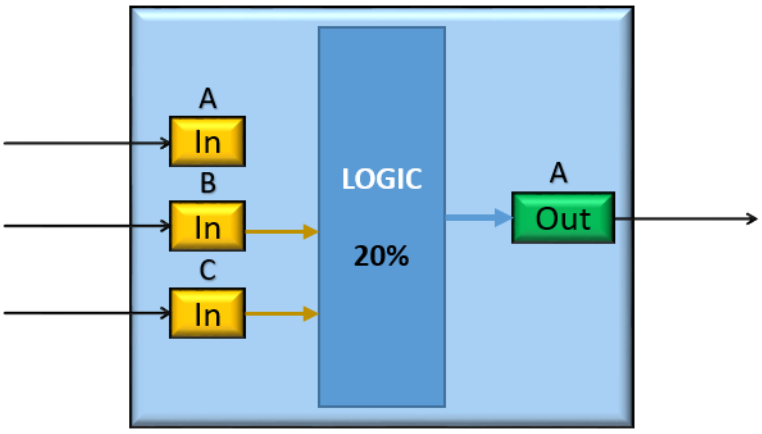
Smart Transaction



The logic can exclusively work according to a signed contract. Some inputs can immediately be output, other ones can be held or recalculated before any output.

For example, there is a contract between three parties. Each party has its own contract's obligations. There is also a written rule according to which the first party (A) should get 20% of all transfers made by other two parties (B & C).

Smart Transaction



The rules of the contract can dynamically be changed by usage of the voting system.

2.3. Manageability

For manageability purpose the voting system is existed. The main goal of voting system is to update the signed contract during its execution. Need for changes in the contract can be caused by as a party's proposal as an inability or failure of execution of the contract's obligations.

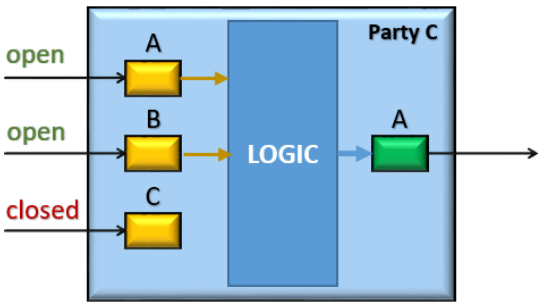
2.4. Implementation.

Variants of usage of the smart transactions are exclusively dependent on collaboration conditions of contract's parties. Two or more parties of a contract can themselves determine an order and conditions of its execution.

Let's take above-mentioned example**.**

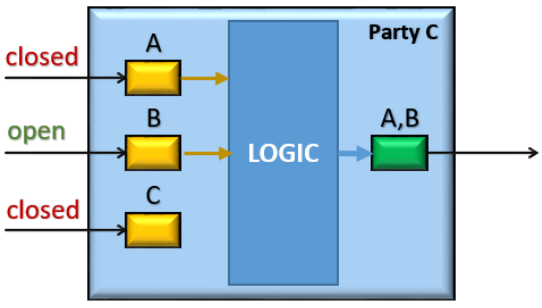
Stage 1

Smart Transaction



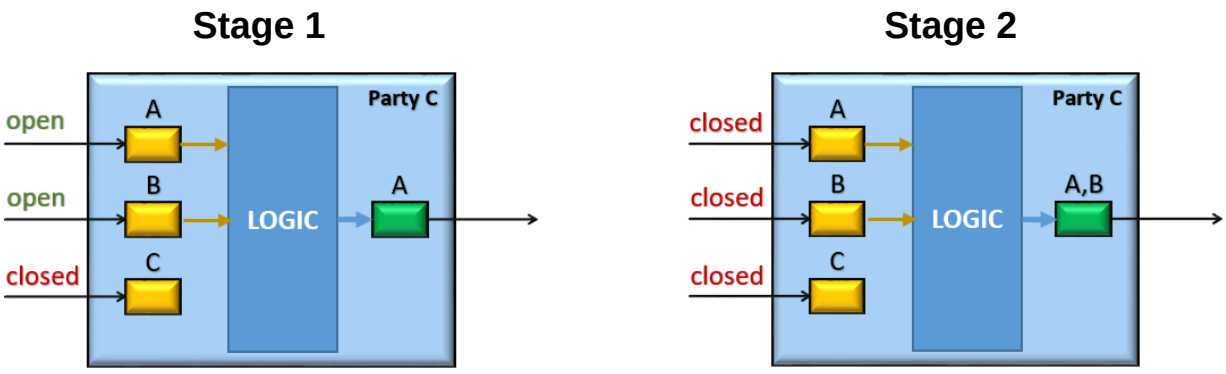
Stage 2

Smart Transaction



Party C has, say, 7 stages of execution of the signed contract. Any two of the stages is shown above. After stage 1 the party C can only receive

a transfer (money or data) from party B and send the transfer to both, the party A and party B. In this case, a single stage can be interpreted as an execution of one of the contract's obligation.



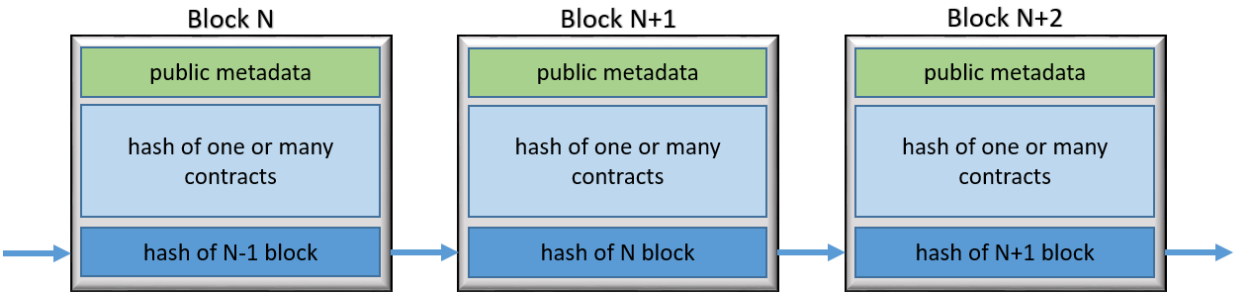
By other conditions, after execution of the contract's obligation in Stage 1 the party C will only be able to send. All input transactions are prohibited.

3. Timestamp chain

Generally, the amount of smart transaction boxes is equal to the amount of parties of a signed contract. A set of contract-related boxes forms a block or several blocks if the size of the block is pretty big. Then, the block ('s) is hashed and added to an *associative chain*, **Neural Chain**. Each associative chain is specified for a single type of business service. For instance, *Money Transfer Associative Chain* is intended to store all the activities of a contract's parties related to a transfer of money if the main goal of the contract is a money transmission. *Lending Associative Chain* is intended to store all the lend contracts, etc.

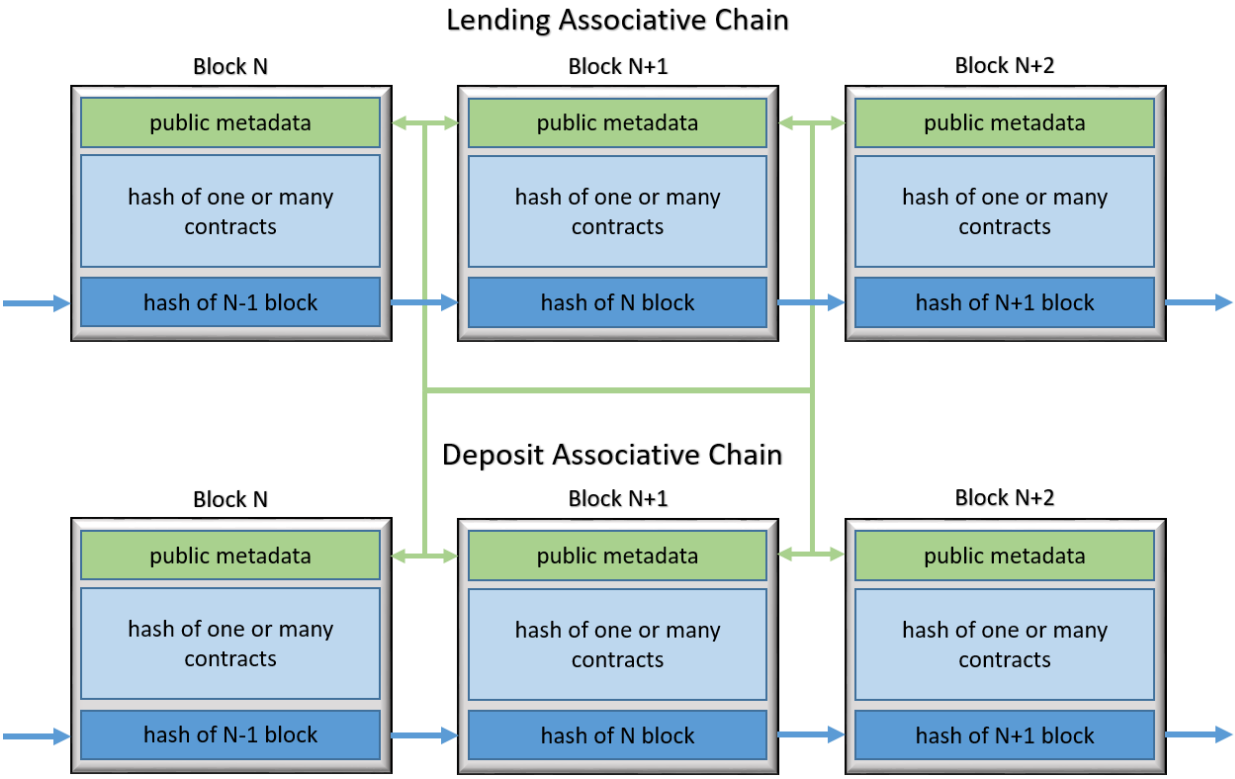
We propose a timestamp associative chain which is related to a specific activity of network participants. In our conception, a network (crypto or any other kind) is a network that consists of many associative chains connected to each other.

Lending Associative Chain



One associative chain can connect to other associative chain through a public metadata module of the block.

Neural Chain



4. Proof of Participation

Proof of Work (PoW) is the currently main mechanism that deters a denial of service attacks and primarily used for mining blocks in a Blockchain-based network. But every single cryptocurrency such as Bitcoin that is based on PoW are pretty vulnerable to an attack that can come from one of well-hardware-equipped miner (‘s). Thus, a focus of

the mining is on the power of calculating cluster. That is why a PoW-based cryptocurrency cannot be economically stable on their nature.

We propose a new innovative mechanism, **“Proof of Participation”** (PoP), main focus of which is on an economic activity of participant of a network. The network that is based on two technologies, “Smart Transactions” and “PoP” is called as a **Neural Chain Network** (NCN). In NCN, “PoP” is the main mechanism that deters a denial of service attacks and used for mining neural associative blocks. In compared with PoW, the obvious advantage is a focus on a participant’s economic activity not for their money or equipment-based status.

That is why a PoP-based cryptocurrency is considered as an economy-dependable one on their nature.

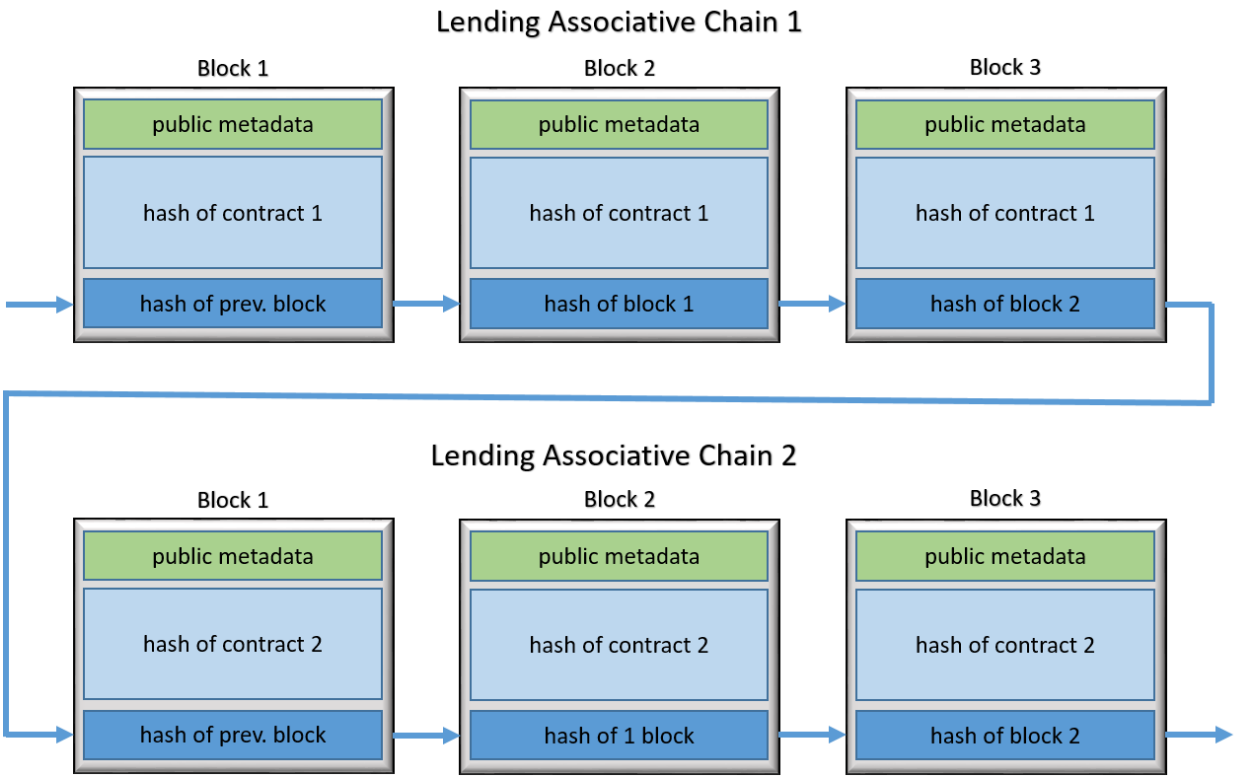
In NCN, mining process is that every its participant is eligible and capable of earning coins or tokens by participation in a role of borrower, lender, employee, employer or other business position.

A miner is a participant or group of participants that provides a service of any business kind to other participant or group of participants of NCN.

Economic basis of “PoP” makes any PoP-based cryptocurrency independent of other cryptocurrencies such as Bitcoin, Ether, Litecoin, Ripple, etc.

5. Associative Network

In our notion, an associative network is a network that consists of one or many associative chains related to each other by a single business service.



NCN is consisted of many associative networks of business services of any kind.

6. Incentive to a contract execution

In NCN, there is no a single separate position such as a miner whose

exclusive responsibility would be a block generation and addition it to an associative chain. The task of the generation and addition of blocks is an exclusive right of participants of NCN.

By convention, parties of the contract vote and decide who of them will be responsible for execution of three-steps-procedure:

1. Generate a hash of contract's activity and text metadata of the contract.
2. Choose an associative chain and get a hash of its last block.
3. Form and add the contract's block ('s) to the chosen associative chain.

The three-steps-procedure should be executed right after completion of the contract.

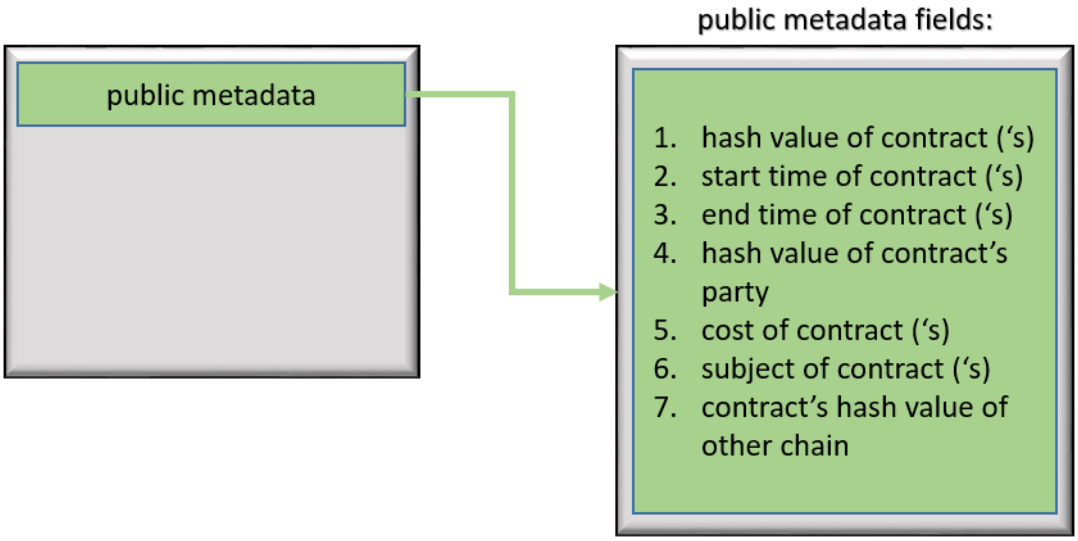
A reward for the execution of the three-steps-procedure is assigned by the parties of the contract through a quorum.

Thus, in NCN, the incentive is directly connected to a complete execution of the contract.

7. “Smart Transaction” search

In NCN, search algorithm is realized through a usage of metadata of the blocks. The metadata has the following features:

a) It is public and visible for any participant of NCN.
b) It is in a text format.
c) It has an anthology structure.



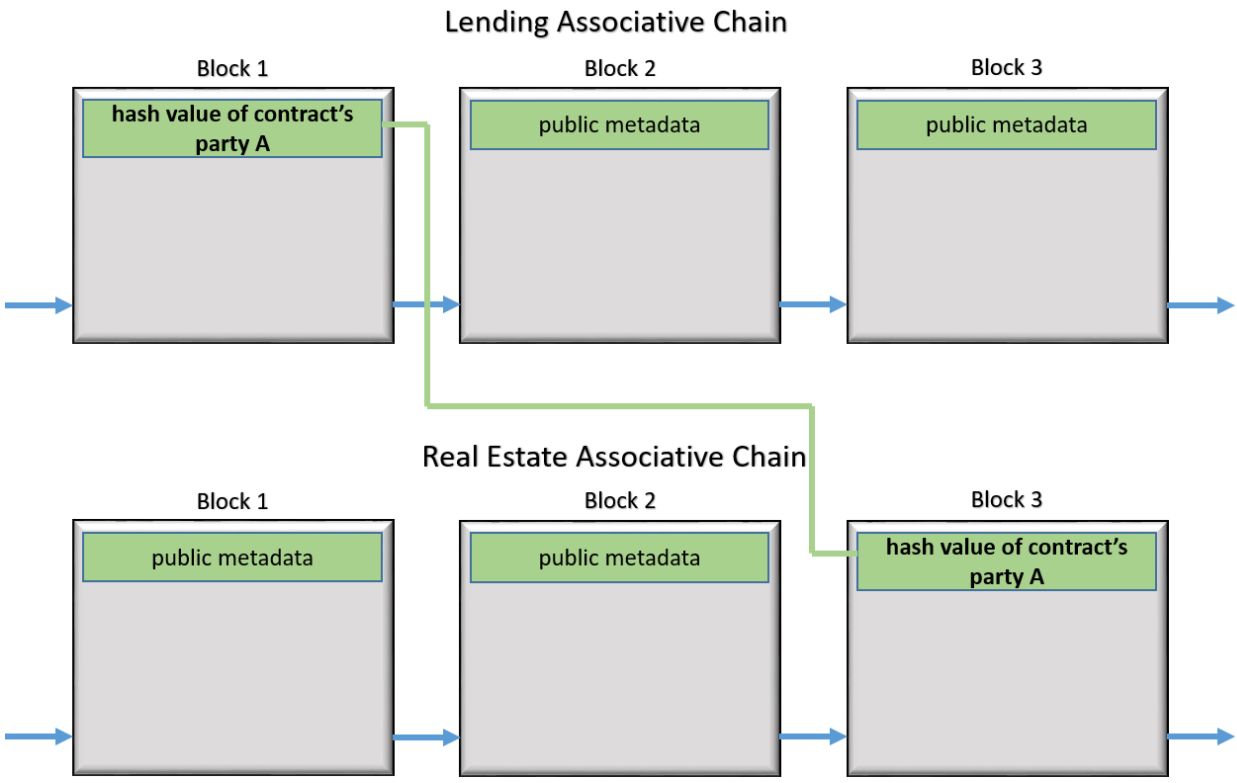
List of the metadata fields can be changed if needed.

As the metadata is a small size and related to a specific business activity, the search algorithm is pretty fast and semantics-oriented.

The anthology structure of the metadata let participants of NCN classify contracts inside a single associative chain.

8. “Smart Transaction” analysis

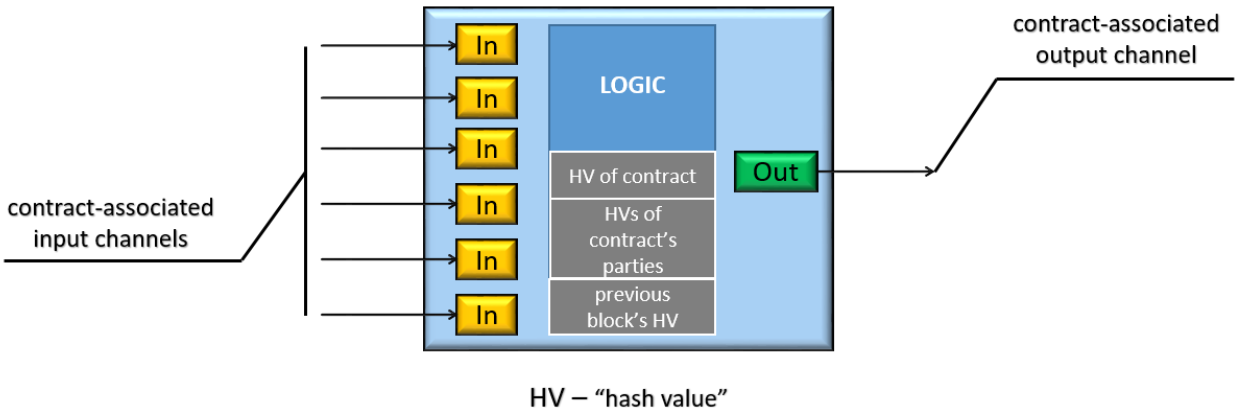
In NCN, algorithm of intellectual analysis is realized through a usage of the fields of the metadata. For example, a participant can form own associative chain by choosing one or more metadata fields.



So, if a chosen field is “hash value of contract’s party” the intellectual analysis can be implemented across many associative chains. Possibility of a cross-chain analysis let participants track any other participant’s activity.

9. Transaction privacy

In our case, the privacy of a smart transaction (smart box) is totally determined by a condition of the contract (‘s). A smart box is governed through a predetermined contract-focused logic. Two main features the logic determines are “*a group of contract’s parties*” and “*a level of privacy between contract’s parties*”. If a quorum is met the logic of the smart box can also include any additional conditions of its implementation.



The main task of hash value of the previous block is to minimize a fraud between parties of a contract ('s).

The hash value of the contract let avoid an intervention of any untrusted third party.

The hash value of the contract's party is primarily used for an identification of party's responsibility according to the signed contract.

10. **Atomicity** (**A**CCP)

In our context, "Atomicity" is a property of Smart Transaction Box intended to guarantee that all the contract-associated transactions will be executed "**in all or nothing**". The execution is strongly conformed to a signed contract. The "Atomicity" is realized even in the event of power failures or crashes.

11. **Consistency** (A**C**CP)

In our context, "Consistency" is a property of Smart Transaction Box intended to guarantee that all transactions in NCN will strictly be conformed to a signed contract ('s). The property guarantees that every transaction will be valid according to a predetermined contract rules. Correctness of the transaction is controlled by the logic of Smart Transaction Box.

12. **Concurrency** (AC**C**P)

In our context, "Concurrency" is a property of Smart Transaction Box intended to guarantee that any input transaction of NCN will be

executed on a “**First-Come-First-Served**” (FCFS) basis. As for an output transaction it is totally up to the logic of Smart Transaction Box.

13. **Permanency** (ACC**P**)

In our context, “Permanency” is a property of Smart Transaction Box intended to guarantee that immediately after execution of any transaction in NCN all the related data will be stored without possibility of future change. The property along with other features of NCN realizes a principle of inevitability.

14. Conclusion

We have proposed a fast, manageable and intellectual mechanism for a practical implementation of business agreements of any kind. The mechanism presents a set of tools needed for tracking a step-by-step execution of a signed business contract. PoP makes participants of NCN economically self-motivated. Functional structure of Smart Transaction Box let the participants realize an intellectual search and analysis of transaction data. Identification mechanism of NCN let any group of participants form their own contract-associated chain and stand apart from a fraudulent third party. ACCP-based transaction guarantees a high level security and inevitability of transaction execution.

References

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

[2] A. Back, "Hashcash - A Denial of Service Counter-Measure", http://www.hashcash.org/papers/hashcash.pdf, 2002

[3] J. Poon, T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", https://lightning.network/lightning-network-paper.pdf, 2016

[4] J. Poon, V. Buterin, "Plasma: Scalable Autonomous Smart Contracts", https://plasma.io/plasma.pdf, 2017

[5] E. Lombrozo, J. Lau, P. Wuille, "Segregated Witness (Consensus layer) ", https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki, 2015

[6] C. Decker, R. Wattenhofer, "Bitcoin Transaction Malleability and MtGox", https://arxiv.org/pdf/1403.6676.pdf, 2014

[7] H. Lodish, A. Berk, S. Zipursky, P. Matsudaira, D. Baltimore, J. Darnell, "Molecular Cell Biology", 4th edition, 2000

[8] R. Merkle, "Protocols for public key cryptosystems", http://www.merkle.com/papers/Protocols.pdf, 1980

[9] I. Tetko, "Associative Neural Network", https://link.springer.com/article/10.1023%2FA%3A1019903710291, 2002

[10] V. Sigillito, "Associative memories and feedforward networks: a synopsis of neural-network research at the Milton S. Eisenhower Research Center", http://www.jhuapl.edu/techdigest/views/pdfs/V10_N3_1989/V10_N3_1989_Sigillito.pdf, 1989

[11] N. Prasad, K. Prasad, S. Yeruva, P. Murty, "A Study on Associative Neural Memories", https://pdfs.semanticscholar.org/da30/381af30678e7eebd0a1d5dd251ea45330035.pdf, 2010