EXSCUDO

NEXTGEN
FINANCIAL
ECOSYSTEM

EON

Whitepaper

Version 1a - EON v0.5.0

2017

Abstract

EON is a decentralized blockchain based-platform that provides an infrastructure for the Exscudo Ecosystem services. This platform is not meant to be viewed as an alternative to Bitcoin, Ethereum and other altcoin, as it is designed for the execution of specific tasks of Exscudo. This fact determines the decisions made. For the realization of the platforms, approaches that have been tested in other existing crypto platforms are being used.

Introduction

Bitcoin gave us enthusiasm and an understanding of decentralized solutions. Since then, many developers and teams have tried and succeeded in modernizing the source code in order to advance and enhance the capabilities of the protocol. We are not an exception. We strived to create a fast and flexible decentralized network that would be able to realize business scenarios that require either trust or escrow agents. Besides, in the face of the blockchain's growing volume problem (scalability), our blockchain must not become enormous. This will enhance the possibilities of maintenance of the decentralized network. Moreover, the rush for the right to sign a block must not be hardware-dependent. It should fit the model and logic of the network in a much deeper manner.

EON solves all these tasks. The transaction is flexible and fast (1333 transactions per minute)[1]. We can make the blockchain 'collapse onto itself' an infinite number of times without losing the integrity of the network. This is an unrivalled innovative solution that allows us to keep the size of the operational blockchain limited.

The architecture of the platform is built on a simple core that realizes a mathematical model and services that provide additional functionalities.

The core forms the decentralized part of the system that consists of a variety of peers and executes the functionality of support on user account and financial operations.

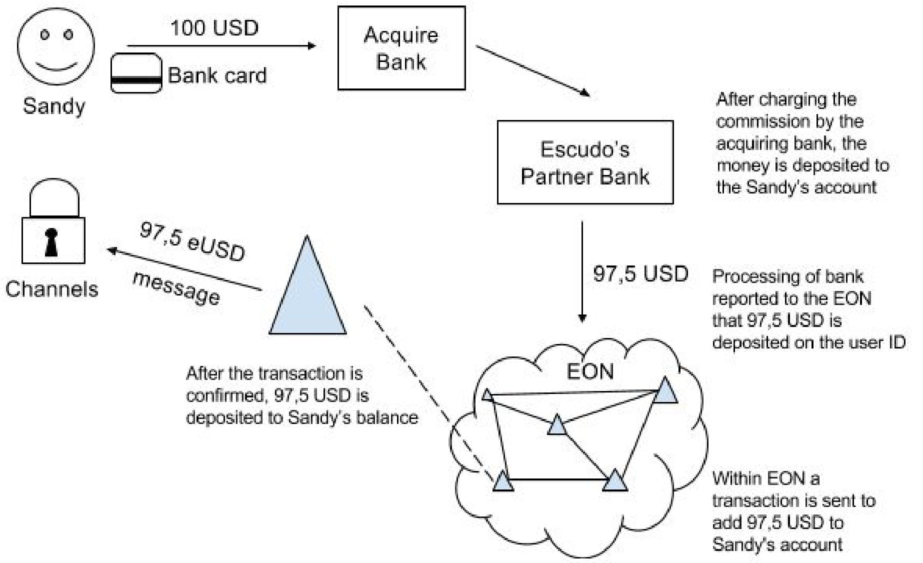
Every peer stores the full information and carries out the validation of transactions task. When the peer completes this task, he receives a reward. Practically, the peer receives a commission when the block is created, and it equals the sum of commissions for all transactions in that block.

[1] Intentionally limited for the launch of the project.

The services, on their side, interact with the distributed part and can receive a margin for offering some functionality. These services can be centralized or decentralized objects. This classification allows us to keep the core as simple as possible. It provides for additional options of development and growth of external services independently from the network core. The question of trust on external services which arises when the functionality doesn't work 'on one core', is solved for every single service in particular.

Tokenization

Due to the nature of EON's architecture (speed, flexibility, the ability to issue tokens and colored coins), we can organize the circulation of obligations, with a high degree of reliability, and the repayments or claims under these obligations within the EON system are executed quickly and with a minimal cost. In the case where the obligation is beyond the scope of the EON system, the speed of execution will depend on the specifics of the third-party systems.



After charging the commission by the acquiring bank, the money is deposited to the Sandy's account

Processing of bank reported to the EON that 97,5 USD is deposited on the user ID

Within EON a transaction is sent to add 97,5 USD to Sandy's account

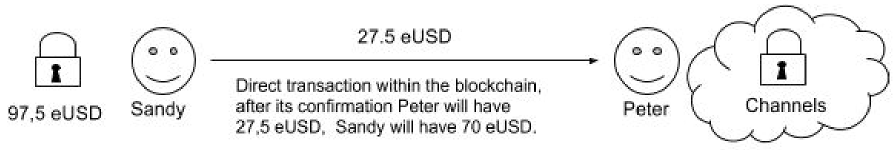
After the transaction is confirmed, 97,5 USD is deposited to Sandy's balance

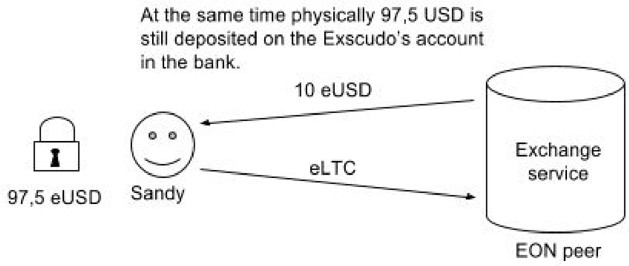
Thanks to the EON platform, we get a trustworthy obligation for 97.5 USD, the weakest point of which can only be the processing of the bank, because it is an initiator of the transaction.

Digital obligations eUSD circulate in the EON system, which inherit all the features of EON:

- blockchain-based;
- fast;
- valid.

Now we have an understanding of the Sandy's funds history and we can observe the following possibilities:


97,5 eUSD
Sandy
27.5 eUSD
Direct transaction within the blockchain, after its confirmation Peter will have 27,5 eUSD, Sandy will have 70 eUSD.
Peter
Channels


At the same time physically 97,5 USD is still deposited on the Exscudo's account in the bank.
10 eUSD
eLTC
97,5 eUSD
Sandy
Exchange service
EON peer

All other cryptocurrencies can be sent to EON but in this case, the transaction initiator will be the blockchain of the corresponding cryptocurrency.

Why do we need this process with a crypto currency?

- The EON network is much faster and efficient than most cryptocurrency networks such as Bitcoin. As long as transactions on the Bitcoin network have difficulties with rapid confirmation, this approach is indeed justified.
- It's much easier for us to store the transaction history, because it doesn't increase the size of the EON blockchain significantly.

Nodes

The nodes' goal is to validate incoming transactions and the formation of blocks in accordance with the rules.

A network node can be set up on any device with a special software. It performs sending of transactions, blocks and auxiliary information in accordance with the established rules. The specified rules for data transmission among the nodes are regulated by the protocol. In the case where an individual network node stops working within the accepted protocol (e.g. because of the modification or absence of critical updates) after some time, it is "isolated" from the network, and stops participating in the creation of new blocks. If several nodes stop working within the protocol, they are isolated and make up a subnet.

Separately, the process of interaction between the node and the "outside world" can be expressed in the following operations[2]:

[2] From the point of view of influence on the work of the node

receiving, checking and saving new transactions received from the The term "active nodes" is used since each particular peer works with a limited list of active connections which is randomly generated based on a pool of known addresses.

In theory, each particular node may not have information about the structure of the entire network.

In the current version, the protocol provides synchronization of data that can be conditionally divided into 3 streams:

- Synchronization of "unconfirmed"[3] transactions, in which the local pool of transactions is expanded with new ones obtained by polling a randomly chosen peer (similar to the "theory" of handshakes);
- Blockchain synchronization based on the complexity criterion;
- Collecting information about the structure of the network and exchanging meta-information.

For the dissemination of data over the network, randomly chosen peers are used. This ensures that transactions are randomly disseminated, to make it impossible to determine or anticipate the data path, and to determine from which node the data has got to the network.

Consensus

Generation of new blocks in the system is done by special "delegate"[4] accounts. Each delegate must confirm the obligation to issue blocks by depositing part of his funds by issuing the relevant transaction. The funds deposited by the delegate are frozen on his account until the release of the reverse transaction. The minimum level of deposited funds for participation in the process of creating blocks should be at least 25.000 coins.

New blocks in the network are created at fixed time intervals of 3 minutes. Each delegate can propose its own version of the block for validation by the network. If various branches are observed in the blockchain, the chain with the greatest "complexity" is accepted. The parameter for account A and i-th block is determined according to the following rule:

[3] All transactions are considered "unconfirmed" until they are included in the current block.

[4] A delegate is any account that wants to participate in the generation of blocks. His account must contain a certain number of coins. It is a kind of property qualification.

Product

$$D_i = D_{i-1} + bal\ A \times M \big/ hash\,(hash\,B_{i-1}, A) \qquad (1)$$

where:

D	Blockchain "complexity";
bal A	Linear function of the volume of deposited funds;
M	Range of hash-function values;
$hash\,(hash\,B_{i-1}, A)$	"Generation signature" field[5].

The probability of generating a block that will be accepted by the network correlates with the deposited funds: the more funds there are, the higher the probability.

Commission for the created block, which is defined as the sum of all transactions fees in the block, is sent to the creator of the block.

To exclude the possibility of creating a fork that begins, in the limit, with the genesis block and having a greater "complexity" than the current chain, the maximum permissible reorganization depth of the chain is set at 480 blocks.

The necessity for the depositin funds leaves room for manipulating the deposit in order to obtain the right to create a new block. To avoid such situations, the rate of withdrawal of funds from the deposit is limited to the maximum depth of the reorganization of the block.

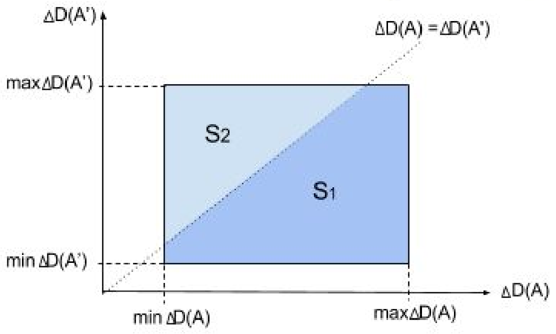
The probability of creating a better block, assuming that the nodes are in a consistent state, have a similar set of transactions and the hash function gives an even distribution of the hash values, with N number of accounts is equal to:

$$P_x = \prod_{j=0}^{N} P\,(A,\ A_j) \quad (2)$$

Provided that the geometric probability for $\Delta D(A) > \Delta D(A')$ equals:

$$P(A,\ A') = S_1(A,\ A')/(\,S_1(A, A') + S_2(A,\ A')\,)$$

$$\Delta D(A) = A \times M \big/ hash\,(hash\,B_{i-1}, A)$$



The problems of short-term forks are discussed in a separate document.

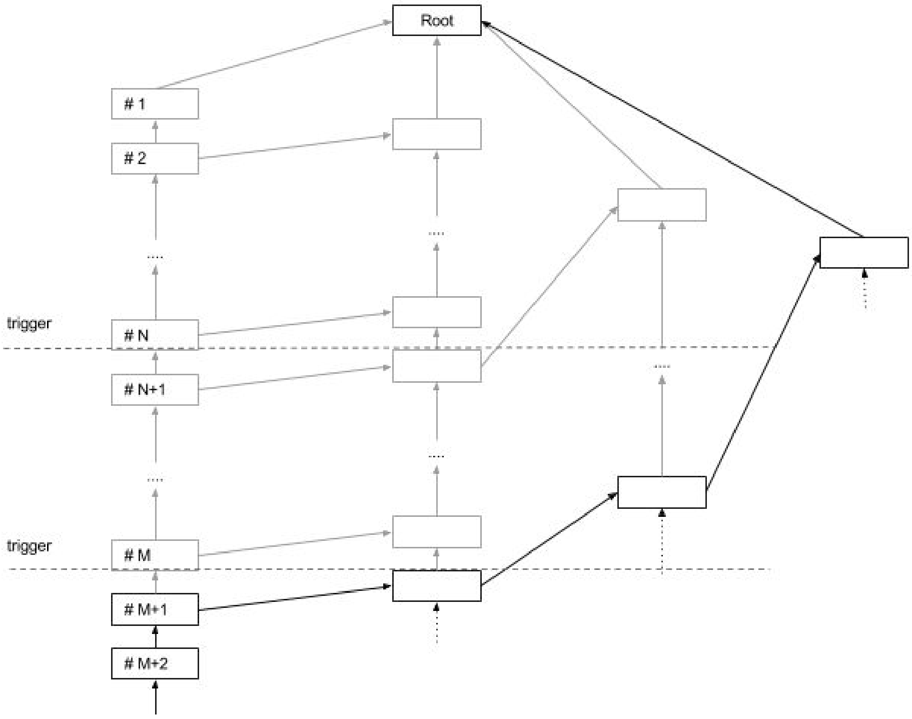
[5] More details are given in the the structure of the block section.

Emission

There is a one-time issuance of coins and it is limited to a size of 240,000,000 EON coins. The initial distribution of coins is made in the genesis block. There is no mining. The percentages of the coin distribution can be found on the ICO page https://exscudo.com/ico/.

Blocks

As with other crypto-currencies, transactions in EON are stored in a sequence of blocks, formed according to certain rules, known as the blockchain. Each node stores a copy of the blockchain. A new block can be created by any account with a certain number of coins reserved on it. Every block can contain up to **4000** transactions, but at the same time its size cannot exceed **1Mb**. Given that some information (e.g. accounts) saved in the blockchain is not subject to distributed storage, and some information is just difficult to distribute because all the network information (financial transactions) needs to be processed, we face a challenge of storing large volumes of data. A user is interested in the amount of funds rather than the origin of funds, so after a certain time the block packaging is used - a snapshot of data is created in order to reduce the size of the block. When creating a snapshot, transaction transfers are replaced with account balances. Such packaging can be performed on several levels according to the scheme below:



In order to store the entire structure of transactions, the “archivists” nodes are implemented.

The block header contains the following information:

- Block ID, version, block height in the chain;
- Block creation timestamp. It is set in seconds relative to the genesis block creation. Blocks in the network are formed over a fixed time interval of 3 minutes;
- The account ID of the block creator;
- Link to the creator account in the form of a public key;
- The ID and hash of the previous block, and the hash of the snapshot of the top-level block;
- The number of transactions included in the block and the block commission, which is the sum of commissions for all the transactions of the block;
- The total length of the data included in the block and their hash sum;
- “Generation signature” field. This field is used to prove the possession of the address. To do this, the accountant who participates in the creation of the block signs the same field of the previous block with his own key;
- Complexity of the block. The consensus rule the criterion used to match blockchains is described by expression 1;
- Block signature.

Transactions

The term “transaction” is used to define a data packet signed by the sender, which contains a description of some action - an atomic change in the state of the system. This action is initiated by the user of the system.

All transactions of the network are considered unconfirmed until they are added to the block. Every newly created block is distributed over the blockchain by the node which created it. When the block is accepted by the network, the transactions included into it are considered confirmed. However, it is quite possible that any newly created block is destroyed during the consensus process and the transactions will again become unconfirmed. Therefore, it makes sense to talk about the degree of trust, which is related to the number of confirmations by means of the subsequent blocks. The “greater” is the depth of the block, the less probable it is that it can change its status. A transaction that has 480 confirmations[6] can not change its status.

[6] It is related to the allowed depth of the reorganization of the blockchain.

The transaction structure is similar to those in NXT [link].

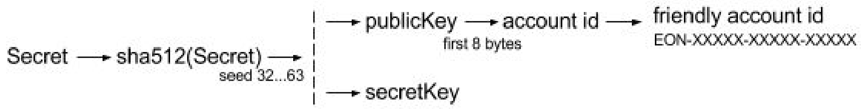
The transaction contains the following fields:

- Transaction type. The type reflects the specifics of a particular action. Each transaction type is processed in accordance with its own hard-coded logic. Transactions of an unknown type to node processing are not accepted.
- Time of creation. Each transaction has a timestamp corresponding to its creation time expressed in seconds after the genesis block creation. This fact determines the impossibility of creating the same transactions faster than once a second[7]. In the future, this field is used to identify and delete old transactions. This field helps determine and delete old transactions.
- Lifetime. It defines the time after which the "unconfirmed" transaction is destroyed. It is set in minutes. By default, the transaction lifetime is 60 minutes. A transaction with expired lifetime is not accepted by peers for processing.
- Reference to the “base” transaction. The transaction which is included in the block earlier than the current one, is considered “base”. This is an optional field used for forming chains of dependencies and fixing the start state.
- Recipient address. EON transactions, unlike Bitcoin transactions, do not have locking scripts, and are similar to NXT transactions. Instead of locking scripts to determine the sender and the recipient, an EON transaction contains ID’s of the users. You cannot send a transaction "to nowhere", because the recipient ID is checked for existence.
- Commission. A commission is charged for adding a transaction to the block. Also, the commission influences the ranking of transactions in the formation of a new block. The commission is set by the sender of the transaction and can not be zero except when registering a new account.
- Data. The content of the field is determined by the specifics of the transaction type. It can also contain encrypted data.
- The sender address. It is a link to the sender's account in the form of the sender's public key.
- Signature.

[7] It defines some features of the services: for example, it restricts sending the same messages to a recipient in the chat.

Accounts

EON uses explicitly specified links to determine senders and recipients. Thus, to send messages and money, any user should be registered in the system. Transactions sent from/to an unknown account, are not accepted by the nodes for processing. To solve the registration of new users problem, transactions of a particular type are used - "registration" transactions. "Registration" transactions do not contain any data which may deanonimize a user and they are designed to store a public key in the network from a key pair generated on the basis of a user's secret phrase. This key is used to verify the validity of the data signature sent to the network by user. The key is generated according to the following scheme:



Taking into account the fact that the registration is made without charging a commission, the corresponding transactions have a minimum priority and are included in the block last.

Multisignature

The use of a multi-signature is determined by the type of transaction. In general, the process looks like this:

- The transaction is initiated and signed;
- Other members see it and add their signature to the transaction. Once the transaction has acquired the required number of signatures, it is included for processing.
- If the transaction did not receive the required number of signatures during its lifetime, it is deleted.

Cryptographic basis

For the exchange of keys, an algorithm on elliptic curves is used - Curve25519 (link) of Bernstein, which in the original is defined as a Diffie-Hellman function.

For the digital signature of messages, a special case is used: Edwards-curve Digital Signature Algorithm (EdDSA) - Ed25519 (link).

Each user of the network has a 32-byte secret key that does not leave his device, and a 32-byte public key that is hosted on the blockchain in the registration transaction. To authenticate and encrypt messages between two users, a common secret key is used, which is generated using the keys of both users.

CONTACTS

General inquiries
info@exscudo.com

Press inquiries
press@exscudo.com

exscudo.com