RAIDO
network
trusted crypto-ledger
(RDO)

ver.0.2

White Paper may change depending on changes made by the community
to the logic of the network and other aspects

Abstract

We present RAIDO - a blockchain based on the ECC cryptographic encryption standard (elliptic curve cryptography).

All of today's blockchain architectures suffer from a number of challenges, not least because of the practical means of expansion, scalability, unpredictable network fees, processing speed and so on, RAIDO Network is committed to addressing these challenges by creating the following seven key benefits:

Scalability. The principle of the RAIDO Delegated Proof-of-stake (DPoS) network allows to avoid wasting resources on processing transactions, while maintaining high system throughput for processing a single transaction, as well as increase the number of transactions that can be processed under peak conditions up to 500 TX/sec and more.

Processing speed. The block is created after at least one signed transaction is received, which creates a high speed transaction confirmation. Thus, the network can be used to implement instant digital payment systems.

Transaction cost. The transaction cost is fixed, which allows forecasting the implementation of business processes based on working with the network, including through the execution of ESCROW-functions in Smart contracts in the following versions of the network.

Participation in management. Coin owners directly participate by voting in decisions on changes to the network parameters and implementation of improvements. Each member of the network may also propose network improvements for voting with a request for an award when accepting such a proposal.

Opportunities for improvement. Thanks to the voting mechanism and improvement opportunities, the network remains flexible for development and adaptation over time. All changes are made with sufficient inclusiveness and transparency to ensure effective management of the decentralized system.

Applicability. The technology meets the urgent need for fast and secure transactions, which creates the basis for operating Smart contracts with the ability to receive and process external data. It is also planned to introduce decentralized applications providing ESCROW functionality.

Final emission. The absence of dynamic emission enables to avoid a decrease in the value of a unit of account as a result of additional emission.

Network consensus

The effectiveness of the network is directly connected with two very important parts of the consensus architecture, particularly: the canonicality and improvement of the network while maintaining consensus. A harmonious combination of these factors creates opportunities for effective network development without compromising on security and hardfork risks.

A significant problem with DPoS networks is the lack of automation of communication between coin holders and validators. In RAIDO Network this problem has been solved by automating stacking work.

Transactional core

The blockchain's transactional core is implemented as a mono-chain architecture in an abstract, purely functional module. By minimizing the functionality of the transactional core, a high degree of security and transaction speed is achieved while maintaining the practical means of expanding the kernel.

The software package, which reconciles thanks to the DPoS network consensus protocol, can achieve high throughput without increasing processing capacity.

Framework for ESCROW functionality

The second stage of the network development is the creation of a framework for ESCROW-smart contracts and interface-oriented decentralized applications with ESCROW algorithms and functions of receiving external data. The implementation of this framework creates the possibility of using the network to implement digital contracts with fast execution.

Cryptography algorithm

Raido network uses the general principles of the (ECC - elliptic curve cryptography) standard, using its own practical method of implementing encryption within the network.

To validate transactions, the Edwards-curve Digital Signature Algorithm (EdDSA) is used - a digital signature scheme using a variant of Shnor's scheme based on an elliptic curve.

The optimal combination of network principles and signature algorithm ensures high efficiency.

Public key

The public key in the EdDSA scheme is the point key of the curve $A \in E(\mathbb{F}_q)$, encoded in b bits.

Signature

EdDSA signature in message M by public key A is a pair (R, S), encoded in 2b bits, point of the curve $R \in E(\mathbb{F}_q)$ and an integer $0 < S < \ell$ satisfying the verification equation

$$2^c SB = 2^c R + 2^c H(R, A, M)A.$$

Private key

A private key in the EdDSA scheme is a b-bit string k that must be selected uniformly and randomly. The corresponding public key in this case is $A = sB$, where $s = H_{0,\ldots,b-1}(k)$ is the least significant b-bit H (k) interpreted as a big endian integer. The signature of the message M is a pair (R,S) where R=rB for $r = H(H_{b,\ldots,2b-1}(k), M)$ and

$$S \equiv r + H(R, A, M)s \pmod{\ell}.$$

Unit of account

To solve the problem of accounting for fractional values, the network uses only integers.

Network unit quark

1 quark (minimum value of RDO coin) = 0,00000001 RDO

Unit of account RDO

1 RDO = 100,000,000 quark

Transactions

Transactions are signed with a private key. Transactions are publicly validated and contain the following components:

id: is a unique identifier of a transaction that is assigned in frames of the algorithm when a transaction is sent to the network

input: transaction inputs containing the following data

transaction: hash of the transaction the output of which is used;

index: the serial number of the output, which is used in the current transaction;

amount: the input amount of the output that is used in the current transaction;

address: the public key of the wallet owner of the funds;

signature: a transaction signature, generated with a private key through an encryption algorithm, is public information required to validate the transaction;

node (optional): the Master node address from which unstaking is performed;

outputs: transaction outputs, contains the following data:

amount: the amount to be sent, the Output amount must be less than the Input amount by the Network fee value;

address: the recipient's addresses;

node (optional): the Master node address to which staking is performed.

hash: a checksum of transaction data;

type: the type of transaction required for automatic separation of ordinary and service transactions, there are the following versions of the transaction types in the network:

regular –a regular network transaction;

reward –reward payment to the stakers;

fee – reward payment to the holder of the Master node

An example of a regular transaction:

```
{
 "id": "de6b234e6c896f95524fef72fead47dd48bd41eb5f986227182cc5d28265f48b",
 "data": {
  "inputs": [
   {
    "index": 1,
    "amount": 9615310000000,
    "address":
"392bbad53749bec66276562d2857ee4ae1e77f5c808b66031834c57636152d93",
    "signature":
"7d04fc3cf93d6d5289ccd81b950766b52544d22f70d1c12f9b835553467fa09e23aa0
3b40d955c144a32be16da9a85e3b2960da3b42dc72d1e75aa3b7939270d",
    "transaction":
"88d95aee74459b794809a8d630a2944a3175687638879188fba047eaf35e9a83"
   }
  ],
  "outputs": [
   {
    "amount": 2300000000,
    "address":
"8479646a2b271a0c846a1093a23bccc2c0ffc557f981d3434315532602c0a5d5"
   },
   {
    "amount": 9613000000000,
    "address":
"392bbad53749bec66276562d2857ee4ae1e77f5c808b66031834c57636152d93"
   }
  ]
 },
 "hash":
"25a4782812d32d46184e175d9f684a1d6bc07b1228e5b722b5cc093c9c9648d2",
 "type": "regular"
}
```


Blocks

The assigned Master node checks for transactions, if a pending transaction is found, creates a block. For a block to be recognized consistent the Master node checks the transaction data in the block, the checksum, signatures.

Every block consists of the following parameters:

Hash: is a control value that includes the inputs and outputs parameters of transactions that are included in the block, is also the block identifier in the network;

index: the serial number of the block in the network;

timestamp: block generation time;

transactions: information about the nested transactions.

Every block contains the hash of the previous successfully validated block.

Master nodes (validators)

Transaction confirmation method of the delegated proof of ownership (DPoS).

Transaction validation nodes are Master nodes with clusters. Master nodes perform two functions:

- block generation from validated transactions by checking matching signatures of the transactions included in the block;

- validation of blocks: double consumption checking, hash matching, signature matching.

When generating a block, the Network fee amount is generated by a Fee-type transaction, the destination of which is the Master node that collected the block.

Master node gets validation right on receipt of delegated RDOs. In the next version of the network, a mechanism to create clusters will be implemented in Master Nodes that become separate validation nodes when populated with a given number of delegated RDOs.

Staking

Delegation of rights is exercised by validation nodes through Stake transactions, where the RDO owner indicates the amount and address of the Master node. Stake transaction realizes RDO hold in favor of the indicated Master node. The ability to revoke Stake by performing an Unstake transaction can only be exercised by the address that previously performed the Stake transaction.

The network commission is distributed in Reward transactions among the stakers' addresses in proportion to the Stake amount every 32 blocks (validation cycle) created by the Master node. The Master node sends the Reward transaction with all stakers' addresses upon completion of the next validation cycle.

To receive a Reward, the holder must keep the steak during the entire validation cycle.

The algorithm is implemented automatically.

Emission

While generating genesis block, the network forms the final emission. Additional emission is not provided.

RAIDO Foundation

A non-profit association the purpose of which is to maintain and develop the RAIDO Network. RAIDO Foundation activities are regulated by separate documents that are not included in the White Paper.

RAIDO Foundation functions

-implementation of conversion operations of the transition period;

- development and support of the main components of the network;

-initiation of holders' internal voting;

-expertise of the proposed changes and improvements to the network;

-holding and targeted use of the RDO coin fund.

Trust Fund

The RAIDO Foundation possesses an RDO fund that can pay for the implementation of its own functions. The undistributed emission constitutes the basis of the trust fund. At the same time RAIDO Foundation is not entitled to exploit the funds of the trust fund for staking/participating in the internal voting.

The annual implementation of the trust fund in frames of the necessity to develop the fund's network should not exceed 20% of its starting value.

Internal voting

The voting in the network is realized by the consensus and decentralized management principle. The implementation of the voting mechanism is foreseen in the next version of the network.

Any RDO holder with a sufficient number of RDO can participate in the voting.

Ownership of 100 RDO gives the right to cast 1 vote. One participant can have an unlimited number of votes. The votes for the given period only are counted.

The voting must be announced at least 5 days before to be held. The period for voting is indicated in the announcement on the Raido Foundation website.

To declare a vote successful, 1/2 of those who voted +1 vote is required:

-adjustment of network variables, including network commission, block generation time, minimum amount for staking, Master node commission, cluster size, etc;

- adding changes to the framework and logic of work of Smart contracts and external applications;

-adding changes to the service infrastructure;

-dealing with organizational issues not related to the technical side of the network work;

-adding changes to the network core.

Questions that cannot be put to a vote:

- changes that can pose a risk to the security and integrity of the network;

- implementation of additional emission RDO.

Transition period

The implementation period of the transition of RF Tokens from the ERC20 standard to its own network, during which an appropriate conversion of old tokens to new coins is implemented.