



Technical description of the Waves Enterprise platform

Release master

<https://wavesenterprise.com>

Apr 09, 2020

BLOCKCHAIN-PLATFORM WAVES ENTERPRISE

FEATURES OVERVIEW

The Waves Enterprise Blockchain Platform is a scalable digital infrastructure solution that combines the features of public and private blockchains for corporate and government use. The platform uses operation protocol, rather than business logic, to solve the problem of trust between parties. The *Proof-of-Stake* (PoS) and *Proof-of-Authority* (PoA) consensus mechanisms guarantee the correctness of data added to the blockchain, while decentralization provides counterparty independence for data access.

1.1 Waves Enterprise Blockchain Highlights

- Built on Scala programming language.
- Includes technologies and best use practices of use proven on the Waves public blockchain platform.
- Adapted for corporate and government use.
- Supports *PoS* and *PoA* consensus algorithms, and allows administrators to choose the most fitting one during deployment.
- Ensures high throughput rate.
- Supports two types of *smart contracts*: Turing-incomplete RIDE contracts and Turing-complete Docker contracts.
- Delivered as a set of microservices.
- Uses cryptographic algorithms certified by state regulators.
- Supports confidential and direct data exchange via private groups without loading data onto external networks.
- Implements the permission management system at the consensus level.
- Waves Enterprise web client features *transactions* explorer, wallet, creation of transactions, smart contract development, blockchain status monitoring, and permission management.

1.1.1 Waves Enterprise network deployment options

1. Operating in the main public network.
2. Operating in a private network anchored to the main network.
3. Operating in an independent private network.

1.2 Main network

The main network is supported by a consortium of companies from various economic sectors including banking, industrial, real estate, logistics, etc. Companies which use the main network may use public blockchain for their projects or for supplying blockchain processes, e.g. banking enterprises delivering fiat *gateways*, and state registrars granting access to cloud-based GOST cryptography.

1.3 Independent private network

Independent private networks may be used by companies that do not want to share their processes publicly. Waves Enterprise allows such companies to deploy a stand-alone private network out of the box and configure it in accordance with their business needs.

Following features are configurable:

- Consensus type.
- Cryptography provider.
- Number of nodes.
- Blockchain operating parameters.

1.4 Private network with block hashes broadcast to main network

This solution combines the advantages of public and private networks. Private networking allows companies to conceal private information from the public blockchain, while the broadcast of private block hashes to the main network ensures reliability of information, thanks to the scalability of the main network.

OFFICIAL RESOURCES

- Official site of the blockchain-platform [Waves Enterprise](#)
- [Github](#) project
- Official site of the blockchain-platform [Waves](#)

ARCHITECTURE

The Waves Enterprise platform is based on distributed ledger technology and represents a fractal network consisting of:

- A master blockchain, Waves Enterprise Mainnet, which secures the operation of the network, serving as a global arbiter and a reference chain, and
- A number of custom, separated sidechains that can be tuned easily according to specific business needs.

This construction principle optimizes the platform for higher speeds, large volumes of calculations, consistency and availability of data, and resistance to malicious changes in information.

The *Anchoring mechanism* uses the strengths of both consensus algorithms to create a net configuration. The main Waves Enterprise blockchain is based on the *Proof-of-Stake* consensus algorithm, which is supported by independent participants. At the same time, enterprise sidechains do not need to interact with miners and can use the *Proof-of-Authority* algorithm. Sidechains are embedded in the main blockchain using the anchoring mechanism, placing cryptographic proof of transactions in the main blockchain network.

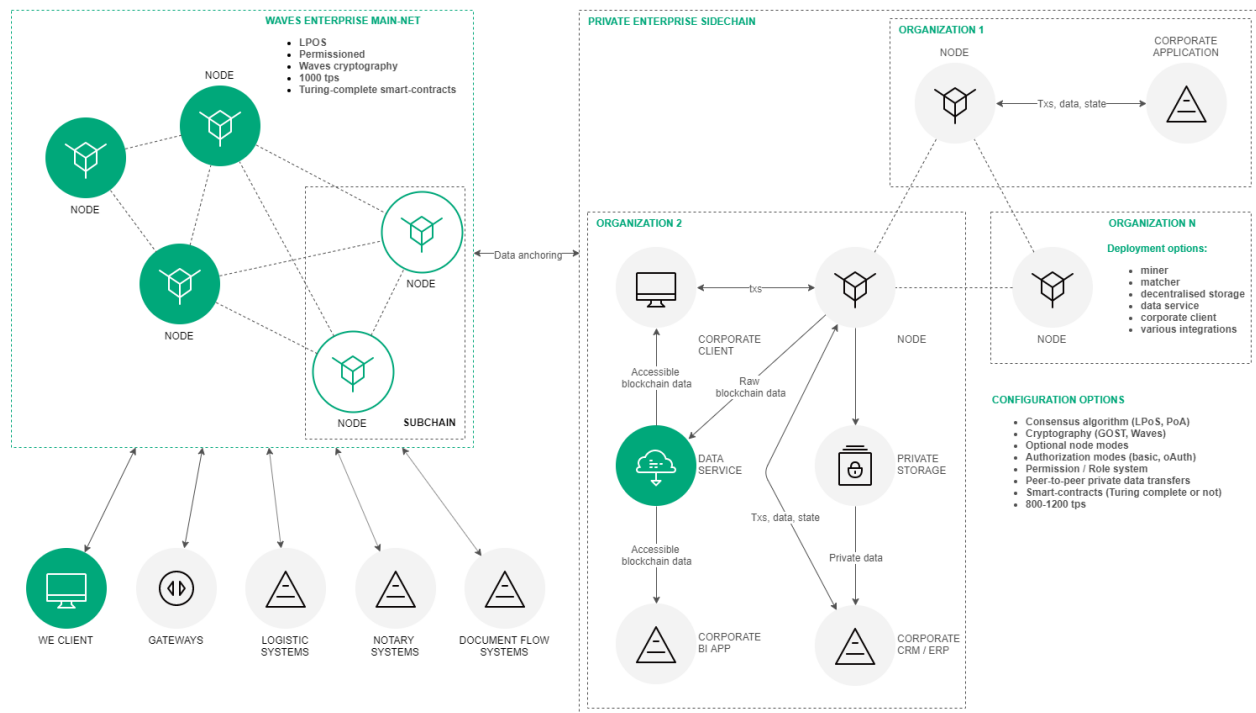


Fig. 1: Network topology including Waves Enterprise and sidechains

3.1 Node architecture and additional services

The node component is mandatory, since it ensures the functioning of and interaction within the blockchain network. Other components serve auxiliary purposes that significantly simplify user interaction with the blockchain platform. The Waves Enterprise Blockchain Platform instance consists of five basic modules and several additional microservices. The main modules include:

- Node - The main software, which is installed on the computer and works directly with the blockchain.
- Waves Enterprise corporate client – A *web-application* that provides contemporary and multifunctional user interface for the blockchain platform.
- Smart-contracts module – An environment for deploying and executing of Turing-complete *Docker smart-contracts*. Docker containers with smart-contracts are deployed on remote virtual machine for additional security.
- Data service – A *service* that aggregates data from the blockchain in RDBMS (PostgreSQL) storage and provides full-text search on any information within the blockchain via the RESTfull web service.
- Private store - A PostgreSQL database provides private information processing and storing mechanisms, along with an encrypted peer-to-peer communication service.

Additional services include:

- Authorization service – A single authorization service for system components.
- Data crawler - A service that extracts data from blockchain node and loads it into data-service component.
- Generator - A service that generates key pairs for new accounts and creates `api-key-hash`.
- Custom microservice plugins - A set of plugins for processing and customizing data transferred to and from external systems.
- Monitoring Service – An external monitoring service that uses an open-source database (InfluxDB) to store time rows with application data and metrics. The database is installed by the client separately.

Node components

The node includes the following internal components:

- Node API – A REST API node interface which can receive data from the blockchain, sign and send transactions, send private data, and create and call smart contracts.
- Node storage – A system component that provides key-value storage (based on LevelDB) for a full set of validated and confirmed transactions and blocks, same as the current state of objects.
- Unconfirmed transaction pool – A component that provides a temporary storage and queue service for validated transactions until they are included into a block.
- Consensus and cryptolibraries – Configurable and customizable logical components responsible for achieving agreement between nodes and cryptographic algorithms.
- Key store - A component used to store key pairs for the node itself and node users (optional). All keys are secured by passwords.
- Miner – A component responsible for creating transaction blocks that are recorded in the blockchain. The miner component is in charge of interaction with Docker-smart contracts.
- Network layer – A logic layer that provides interaction between nodes on the application level via network protocol over the TCP.

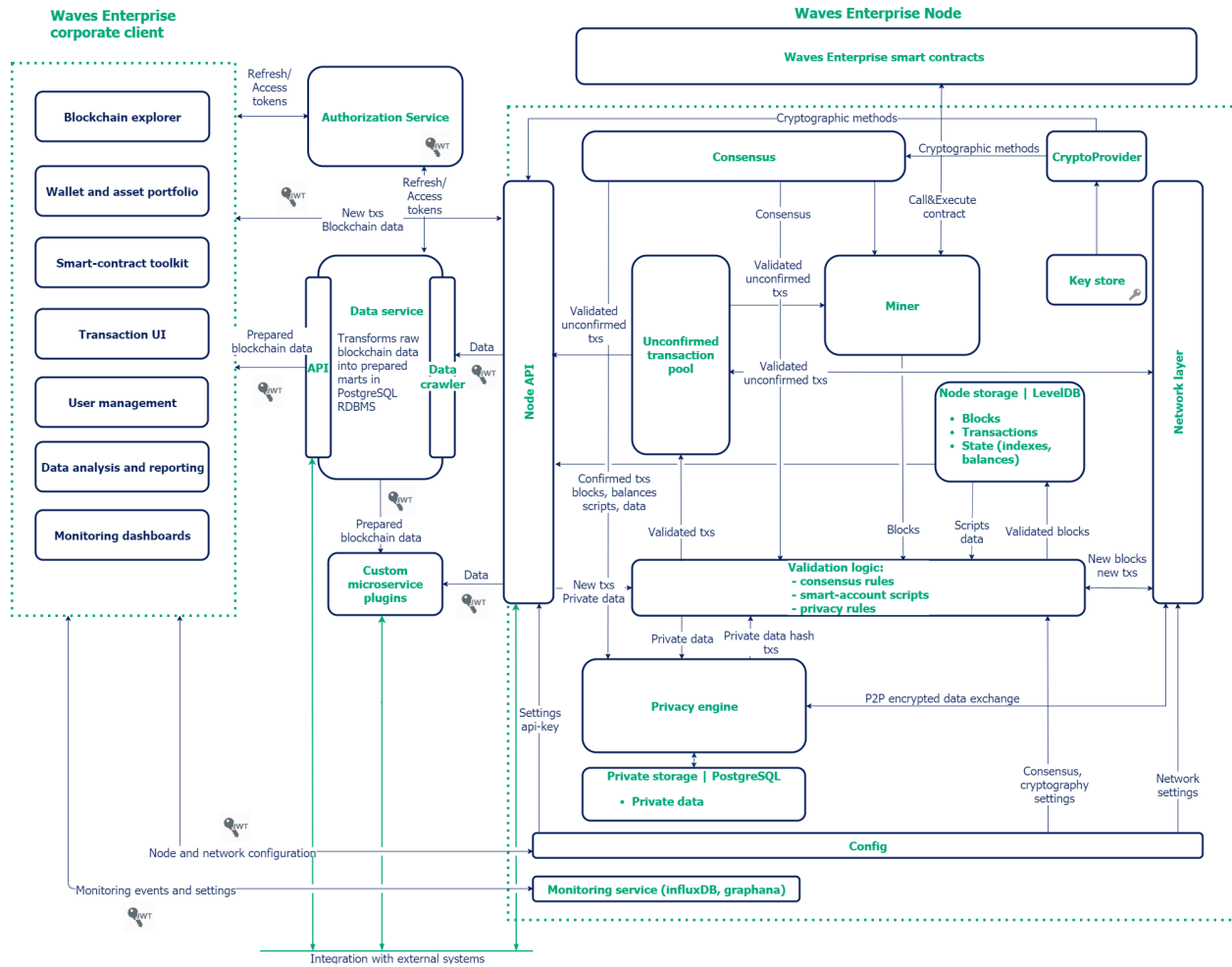


Fig. 2: A detailed diagram of the node architecture and additional microservices

- Validation logic – A logic layer containing such transaction verification rules as basic sign verification and advanced scripted verification.
- Config – A set of node configuration parameters specified in the `node-name.conf` file.
- Monitoring Service – An external monitoring service that uses an open-source database (InfluxDB) to store time rows with application data and metrics. The InfluxDB database is installed by the client separately.

WAVES-NG PROTOCOL

The Waves Enterprise Operation Protocol provides performance advantages relative to other blockchains.

4.1 Terms

- Block — A set of transactions registered in the blockchain, signed by the miner, and containing a link to the proof of the previous block. Limited to 1 MB or 6000 transactions.
- Round — A period of time between the issuance of key blocks. This floating value is controlled by the consensus algorithm depending on the load on the network, averaging 40 seconds.
- Proof of ownership — The acquisition of mining rights in the PoS consensus.
- Node — A network host that runs the Waves Enterprise blockchain application.
- Miner — A node whose address has sufficient balance and a “mining” permission.
- Key block — A block that contains no transactions, only service information such as:
 - Miner public key — to verify proof of microblocks.
 - Amount of miner’s fee for the previous block.
 - Miner’s proof.
 - Link to previous key block.
- Liquid Block — A service term to describe the state of a block before issuing the next key block, i.e. completing its mining.
- Microblock — A service term for a set of transactions applied to the state of blockchain every 5 seconds. Limited to 500 transactions. Each microblock is signed by the miner’s private key.

4.2 Protocol description

The Waves-NG protocol was developed by Waves Platform based on [Bitcoin-NG](#) to increase the throughput of the Waves blockchain based on the architecture on which Waves Enterprise is implemented. The idea of the protocol is to create microblocks continuously, rather than create one large block in each round of mining. Small blocks can be forwarded and checked more quickly.

Mining rounds begin with generation of the key block. Each key block, along with the address of the miner identified in it, are determined by consensus. (For more details, see *Consensus*.) A key block containing only a proof with no transactions is generated quickly. Before the next block is generated, microblocks with transactions are generated every five seconds without proof of stake, which increases the speed of processing.

Each microblock is linked to the previous one, and the key block is added to the blockchain as soon as the next miner generates its key block.

This approach reduces the time to confirm a transaction compared to other blockchains.

4.2.1 1. Process for Creating a Liquid Block

1. The mining address is determined by consensus.
2. A miner creates and distributes a key block on the network.
3. Every 5 seconds, the miner creates a microblock containing transactions and sends it out to the network. Each microblock must be linked to the previous microblock or key block.
4. The process continues until a new valid key block appears on the network.

4.2.2 2. Miner reward mechanism in Waves-NG

The Waves Enterprise protocol offers financial incentive for participants to comply with the rules of the blockchain. 40 % of the block transaction fee is distributed to the miner who created the block, and 60 % of the fee is given to the miner of the following block. The fee credit transaction is performed after 100 blocks to ensure a trust interval of checks.

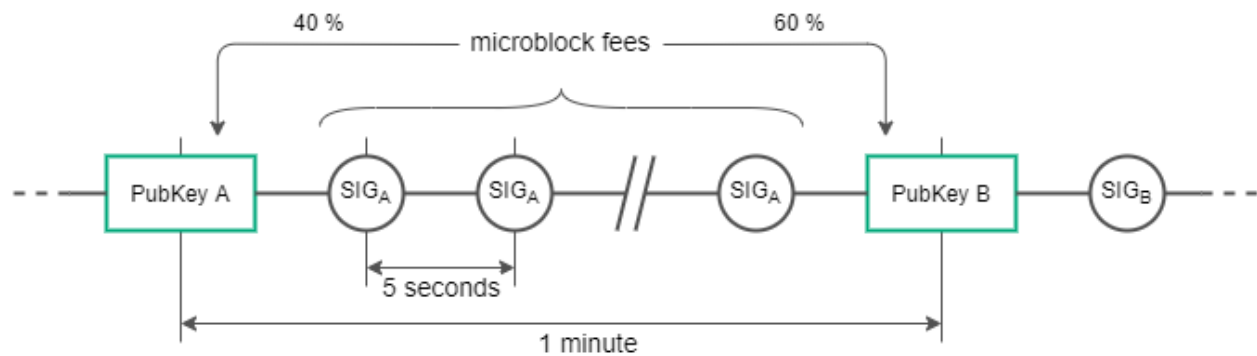


Fig. 1: Fee distribution diagram

4.2.3 3. Conflict resolution

A miner that continues the chain by creating two microblocks with the same parent is punished and loses income from fees; the discoverer of the fraud receives the miner's award for the block. The distributed nature of blockchain means each node stores a copy of the blockchain. When the next microblock appears, the node applies changes to its copy of the blockchain and checks it against other nodes of the network. At this point, inconsistencies in transactions can be detected.

CONSENSUS ALGORITHMS

Blockchain is a decentralized system with no central authority. This makes the system non-corrupt, but it also creates difficulties with final decision-making and organization of work. These problems are solved by a consensus mechanism, which allows the blockchain's participants to reach agreement. Voting takes into account the majority opinion without the interests of the minority, but it also guarantees an agreement that benefits the entire network.

You can choose the consensus mechanism during the initial configuration of the network. The description of available mechanisms, as well as their pros and cons, are described below.

5.1 LPoS consensus algorithm

Proof of ownership with the right to lease. In PoS systems, the creation of a block does not require energy-intensive calculations, the miner's task is to create a digital block proof.

5.1.1 Proof of Stake

The mechanism for allocating block creation rights is based on the number of tokens in the user's account. The more tokens a user has, the more likely he or she can create a block.

In Proof of Stake consensus the right to generate a block is determined by pseudo-random way, because by knowing the previous miner and balances of all users in the system the following miner can be identified. This is possible due to a deterministic computation of a block's generating signature, which can be obtained by SHA256 hashing of current block's generating signature and the account's public key. The first 8 bytes of the resulting hash is converted to a number, referred to as the account hit - X_n and will be a pointer to the following miner. The time of block generation for account i is calculated as:

$$T_i = T_{min} + C_1 \log\left(1 - C_2 \frac{\log \frac{X_n}{X_{max}}}{b_i A_n}\right)$$

where:

- b_i - a stake (stake of participant's balance of overall balance of the system)
- A_n - baseTarget, the adaptive ratio, regulating the average time of issue of the block;
- X_n - an account hit;
- T_{min} - 5 seconds, a constant defining the minimum time interval between blocks;
- C_1 - a constant, which equals 70 and adjusts the form of allocation of the interval between blocks;
- C_2 - a constant which equals 5E17 and adjusts the baseTarget value (complexity).

Based on this formula, the probability of selecting the participant to be rewarded depends on the participant's stake of assets in the system. The bigger the stake, the higher the chance of reward. The minimum number of tokens needed for mining is **50000 WEST**. BaseTarget is a parameter that maintains the block generation time within a given range. BaseTarget in its turn is calculated as:

$$(S > R_{max} \rightarrow T_b = T_p + \max(1, \frac{T_p}{100})) \wedge (S < R_{min} \wedge \wedge T_b > 1 \rightarrow T_b = T_p - \max(1, \frac{T_p}{100}))$$

where

- $R_{max} = 90$ - a maximum reduction of complexity when the block generation time in the network exceeds 40 seconds;
- $R_{min} = 30$ - a minimal increase of complexity when the block generation time in the network is less than 40 seconds;
- S - the average generation time, at least for the last three blocks;
- T_p - the previous baseTarget value;
- T_b - the computed baseTarget value.

For an advanced description of technical features and enhancements of the classic PoS algorithm, see [this article](#).

Advantages Over Proof of Work

The absence of complex calculations allows PoS networks to lower the hardware requirements for system participants, which reduces the cost of deploying private networks. No additional emission is required, which in PoW systems is used for rewarding miners for finding a new block. In PoS systems, a miner receives a reward in the form of fees for transactions which appeared in its block.

5.1.2 Leased Proof of Stake

A user who has an insufficient stake for effective mining may transfer his balance for lease to another participant and receive a portion of the income from mining. Leasing is a completely safe operation, as tokens do not leave the user's wallet, but are delegated to another miner, which gives the miner a greater opportunity to earn mining rewards.

5.2 Proof of Authority

In a private blockchain, tokens are not always needed. For example, a blockchain can be used to store hashes of documents exchanged by organizations. In this case, in the absence of tokens and fees from transactions, a solution based on the PoS consensus algorithm is redundant. The Waves Enterprise Blockchain Platform offers the option of a Proof of Authority (PoA) consensus algorithm. Mining permission is issued centrally in the PoA algorithm, which simplifies the decision-making compared to the PoS algorithm. The PoA model is based on a limited number of block validators, which makes it scalable. Blocks and transactions are verified by pre-approved participants who act as moderators of the system.

5.2.1 Algorithm description

An algorithm determining the miner of the current block is formed based on the parameters below. The parameters of the consensus are specified in the `consensus` block of the node configuration file.

- t - the duration of a round in seconds (the parameter of the node configuration file: `round-duration`).
- t_s - the duration of a synchronization period, calculated as $t \cdot 0.1$, but not more than 30 seconds (the parameter of the node configuration file: `sync-duration`).
- N_{ban} - a number of missed consecutive rounds for issuing the ban for the miner (the parameter of the node configuration file: `warnings-for-ban`);
- P_{ban} - a share of the maximum number of banned miners, in percentage from 0 to 100 (the parameter of the node configuration file: `max-bans-percentage`);
- t_{ban} - the duration of the miner ban in blocks (the parameter of the node configuration file: `ban-duration-blocks`).
- T_0 - the unix time for generation the Genesis block.
- T_H - the unix time for generation of H Block, a key block for NG.
- r - the round number, calculated as $(T_{\text{Current}} - T_0) \text{ div } (t + t_s)$.
- A_r - the leader of round r , which has the right to create key blocks and microblocks for NG in the round r .
- H - the height of the chain in which the key block and microblocks for NG are created. The leader of round A_r has the right to generate a block at height H .
- M_H - the miner issuing block at height H .
- Q_H - the queue of miners active at height H .

The Q_H queue is generated using addresses which are given mining permissions by a permission transaction, which was not revoked until height H and did not expire until the time T_H .

The queue is sorted by the time stamp of the mining rights transaction. The node which was granted the rights earlier will be higher in the queue. To keep the network consistent, this queue will be the same on each node.

A new block is created at each round r . A round lasts t seconds. After each round, t_s seconds count down to complete data synchronization in the network. During the synchronization period, microblocks and key blocks are not generated. For each round, a single leader, A_r , has the right to create a block in this round. A leader can be defined on each node of the network with the same result. The leader of the round is defined as follows:

1. Miner M_{H-1} is defined, which created the previous key block at height $H-1$.
2. The Q_H queue of active miners is calculated.
3. Inactive miners are excluded from the queue (see more in *Exclusion of inactive miners*).
4. If the $H-1$ block miner (M_{H-1}) is in the Q_H queue, the following miner becomes the leader A_r .
5. If the $H-1$ block miner (M_{H-1}) is not in the Q_H queue the miner following the $H-2$ block miner (M_{H-2}) becomes the leader A_r and so on.
6. If no miners of blocks ($H-1.1$) are in the queue, the first miner in the queue becomes the leader.

This algorithm identifies and checks the miner, which creates each block of the chain by calculating the list of authorized miners for each moment of time. If the block was not created by the designated leader within the allotted time, no blocks are generated within that round, and the round is skipped. Leaders who skip block

generation are temporarily excluded from the queue by the algorithm described in the paragraph *Exclusion of inactive miners*.

The block generated by the leader A_r with the time of the block T_H from the half-interval $(T_0 + (r-1) \cdot (t + t_s))$; $T_0 + (r-1) \cdot (t + t_s) + t$ is determined to be valid. The block created by the miner out of its turn or not in time is considered invalid. After a round of t duration, the network synchronizes the data for t_s . The leader A_r has t_s seconds to propagate the validation block over the network. If any node of the network during t_s has not received a block from the leader A_r , this node recognizes the round as “skipped” and expects a new H block in the next round $r+1$, from the following leader A_{r+1} .

Several consensus parameters — type (PoS or PoA), t , t_s — are specified in the configuration file of the host network. *The parameter T should be the same for all network participants*, otherwise the network will fork.

5.2.2 Synchronization of time between network hosts

Each host should synchronize the application time with a trusted NTP server at the beginning of each round. The server address and port are specified in the node configuration file. The server must be available to each network node.

5.2.3 Exclusion of inactive miners

If any miner has missed the block creation N_{ban} times in a row, this miner is excluded from the queue at t_{ban} subsequent blocks, which is determined by (`ban-duration-blocks` parameter in the configuration file). The exception is made by each node on its own based on the calculated queue Q_H and information about block H and miner M_H . The P_{ban} parameter specifies the maximum allowable share of excluded miners in the network relative to all active miners at any given time. If at achievement of N_{ban} round passes, the maximum share of the excluded miners P_{ban} is reached, the exception of the next miner is not made.

5.2.4 Monitoring

The PoA consensus monitoring helps to identify how non-valid blocks are created and distributed, as well as how miners skip the queue. Network administrators perform additional troubleshooting and blocking of malicious nodes.

To monitor the process of generating blocks using the PoA algorithm, the following details are entered in InfluxDB:

- Active list of miners sorted by granting of mining rights.
- Scheduled round timestamp.
- Actual round timestamp.
- Current miner.

5.2.5 Changing consensus settings

Changing consensus parameters (time of round and synchronization period) is performed based on the node configuration file (see the insert) at the height from-height. If a node fails to specify new parameters, the transaction will fork.

Sample configuration:

```
// specifying inside of the blockchain parameter
consensus {
  type = poa
  sync-duration = 10s
  round-duration = 60s
  ban-duration-blocks = 100
  changes = [
    {
      from-height = 18345
      sync-duration = 5s
      round-duration = 60s
    },
    {
      from-height = 25000
      sync-duration = 10s
      round-duration = 30s
    }
  ]
}
```


CRYPTOGRAPHY

The Waves Enterprise platform provides the possibility to choose the cryptography used depending on the specifics of the project under implementation and the jurisdiction of the customer.

6.1 Hashing

Hashing operations in the platform are performed by Blake2b256 and Keccak256 functions sequentially, or by “Stribog” function in accordance with GOST R 34.11-2012 “Information Technology. Cryptographic protection of information. Hash function”. The output data block size is 256 bits.

6.2 Electronic signature

Algorithms for key generation, formation and verification of electronic signature are implemented on the basis of Curve25519 elliptic curve (ED25519 with X25519 keys), or in accordance with GOST R 34.10-2012 “Information technology. Cryptographic protection of information. The processes of formation and verification of electronic digital signature”.

6.3 Data encryption

The platform implements the ability to encrypt data using session keys based on the Diffie-Helman protocol. This operation is used to encrypt any type of text information, such as smart contract data, which should not be available to other blockchain participants. Encryption can be performed individually for each recipient, with the formation of a unique instance of ciphertext, or with the formation of a single ciphertext for a group of recipients.

The algorithms used for symmetric encryption comply with the AES standard or GOST R 34.12-2015 “Information technology. Cryptographic protection of information. Block cipher”.

Symmetric CEK and KEK keys are used to encrypt/decrypt data. CEK (Content Encryption Key) is the key for the encrypting text data, KEK (Key Encryption Key) is the key for encrypting the CEK. The CEK key is generated by a node randomly using the appropriate hashing algorithms. The KEK key is generated by a node based on Diffie-Hellman algorithm, using public and private keys of sender and recipients, and is used to encrypt the CEK key.

For a description of encryption methods and their use, see *Data encryption operations*.

ROLE MODEL

The blockchain platform implements a mechanism limiting actions of participants based on the role model which allows the platform owner to protect participants from threats, such as:

- attacks of unscrupulous miners on blockchain network;
- unauthorized issue of tokens;
- unauthorized access to confidential information;
- other illegal actions of intruders.

The procedure for issuing and revoking permissions is given in module *Role management*.

7.1 Roles list

The following table provides a list of possible platform roles:

| Role name | Authority |
|--------------------|--|
| permissioner | Add transactions to modify the permission list |
| blacklister | Add transactions to modify the black list |
| miner | Create new blocks |
| issuer | Add transactions for issuing, reissuing, and burning tokens |
| dex | Add the exchange transaction (deprecated) |
| contract_developer | Add the transaction to create a docker contract |
| connection-manager | Add the transaction for registering/deleting node in the blockchain network |
| banned | It is forbidden to send any transactions to the blockchain. A group of all participants with this role forms a blacklist |

7.2 Permission model

Permission model describes a mechanism for applying different types of permissions when validating operations in a blockchain.

Hint: The node with the **permissioner** role can assign to itself any existing role in the system.

| Action | Action permission condition |
|--|-----------------------------------|
| Assign or remove a role | Available permissioner role |
| Add or Remove from blacklist | Available blacklister role |
| Registration of the new node to the net | Available contract_developer role |
| Generation and issue of blocks | Available miner role |
| Token operations (issue, reissue, burn) | Available issuer role |
| Token transfer (transfer, mass transfer) | User not in the blacklist |
| Token leasing (lease, lease cancel) | User not in the blacklist |
| Creating an alias (alias) | User not in the blacklist |
| Create a docker contract | Available contract_developer role |
| Execution of docker contract | User not in the blacklist |

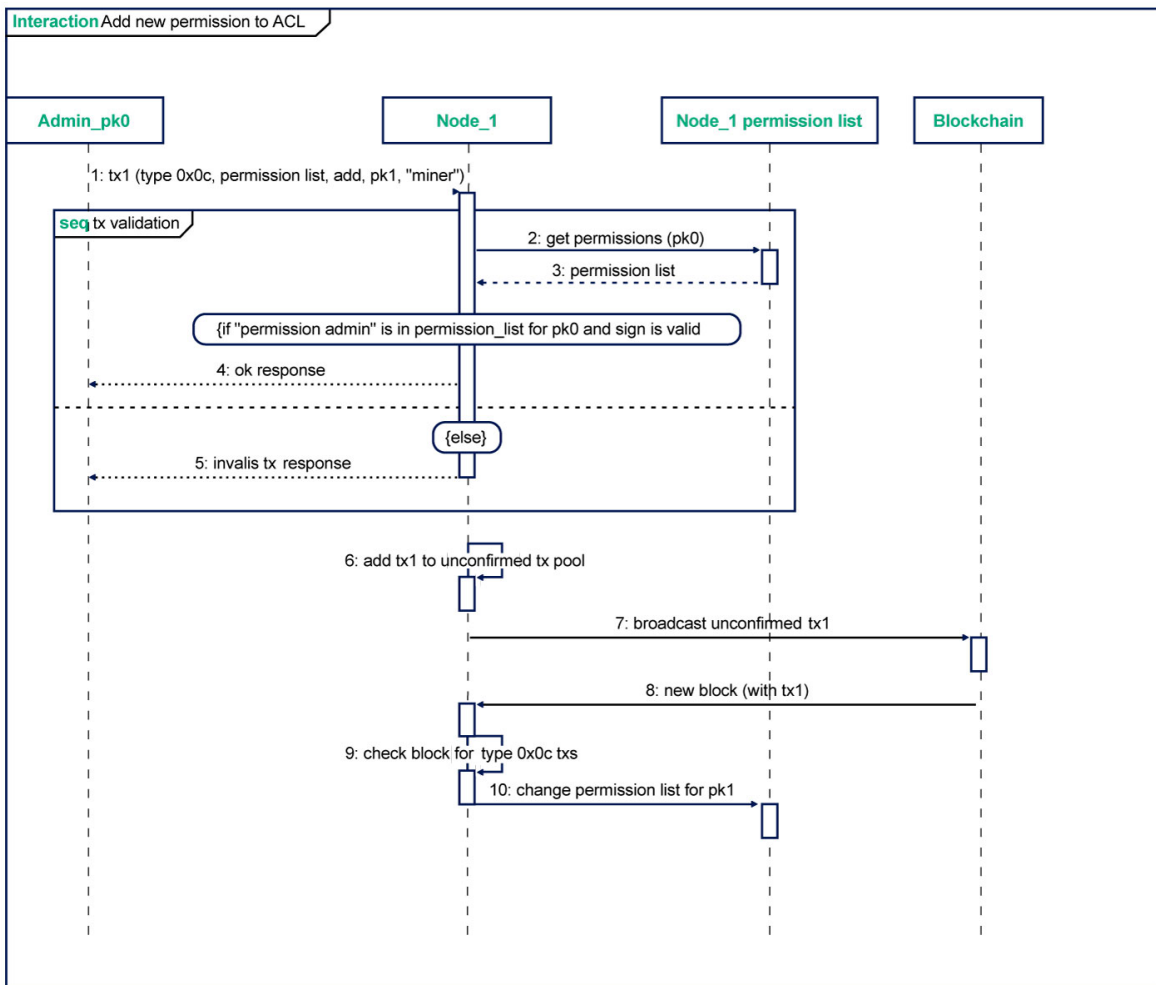
7.3 Update the permission list

A permission transaction is used to modify the permission list.

JSON description:

- Transaction Type
- Version
- Sender PublicKey
- Target Address or Alias
- Timestamp
- Operation Byte
- Role Byte
- Timestamp
- Due Timestamp Defined Byte (0 - None, 1 - Defined)
- Due Timestamp Bytes

The following diagram shows the sequence of actions when updating a permission list.



When modifying the permission list, the platform performs the following checks:

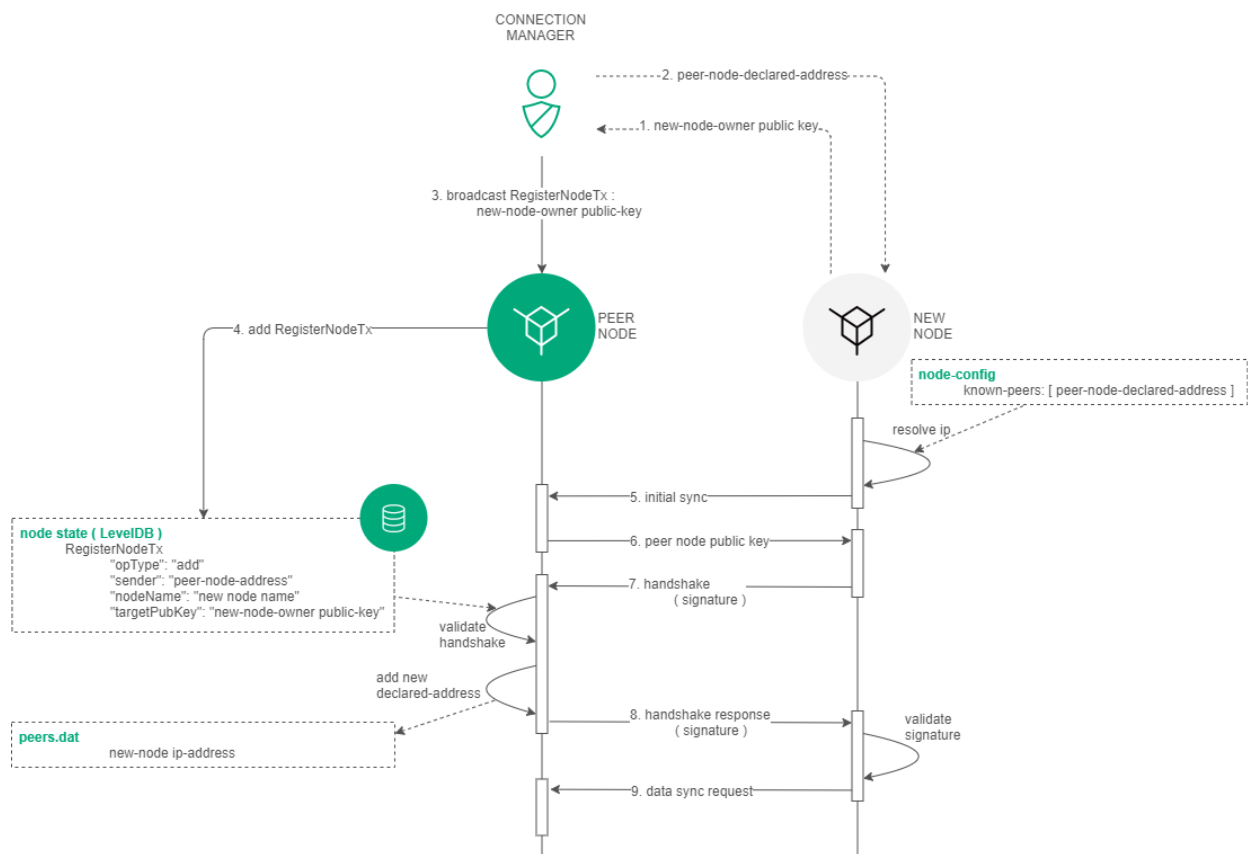
1. Sender is not in the blacklist.
2. Sender has the role of permissioner.
3. DueTimestamp (role duration) > Timestamp (current time).
4. This role is not active (if added) or active (if removed).

ACCESS MANAGING

The Waves Enterprise Blockchain Platform implements a closed blockchain model where the addition of new participants is controlled by an individual user with authority. The closed model also supports the restriction for the data access for all participants. This model offers increased security compared to open blockchains and added flexibility in configuring access levels and distribution of rights.

Only a user with the “Connection Manager” role can add new participants to the Waves Enterprise blockchain. The *111 RegisterNode* transaction is used to connect a new node to the network. This transaction contains the credentials of the connected node. Each node creates and updates the table, which includes all approved network participants.

A handshake-message.

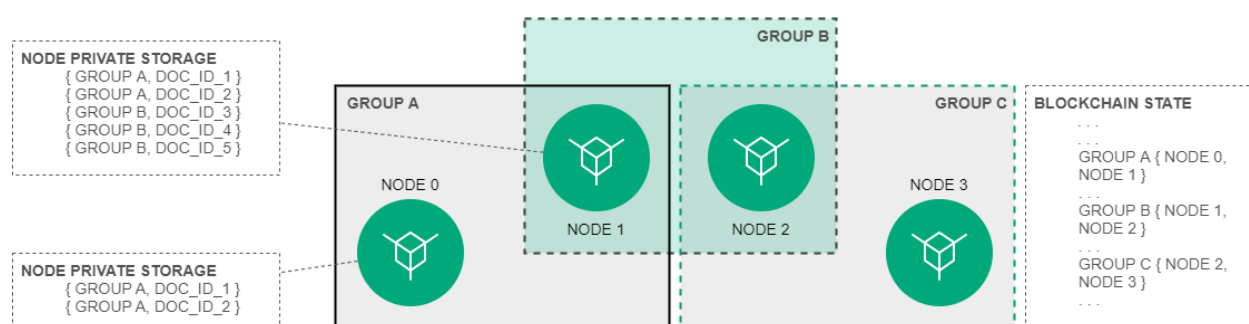


The process of disconnecting a participant from the network is similar to the process of connection, except that the “Connection Manager” user sends the *111 RegisterNode* transaction with the `opType: "remove"`

parameter. Since the handshake request is executed once every 30 seconds, the next request after the participant is removed from the network will be denied, as the connected participant would now lack credentials in the blockchain node table.

DATA PRIVACY

The Waves Enterprise Blockchain Platform provides confidential data transfer and storage between participants interacting on the network. The protection of confidential data during its transfer and storage is provided by a set of groups, which contain a list of participants that can interact with private data.



9.1 Access groups

Access groups are created by network participants who need to arrange a private data exchange. Any participant can create an access group and add into it any number of other participants. Only nodes can exchange information within a group.

The group contains the following parameters:

- name (policyName);
- description (policyDescription);
- duration (policyDueDate);
- the list of confidential data recipients (policyRecipients);
- the list of the policy owners with editing rights (policyOwners).

The access group is created by sending a *CreatePolicy* transaction (type = 112, group creation) to the blockchain.

Owners can change the access group by sending the *UpdatePolicy* transaction (type = 113, group editing) to the blockchain.

For external access and getting the information about groups there are using specified *API Node* requests: GET /privacy/{policy}/recipients, GET /privacy/{policy}/getHashes, GET /privacy/getInfo/{hash}.

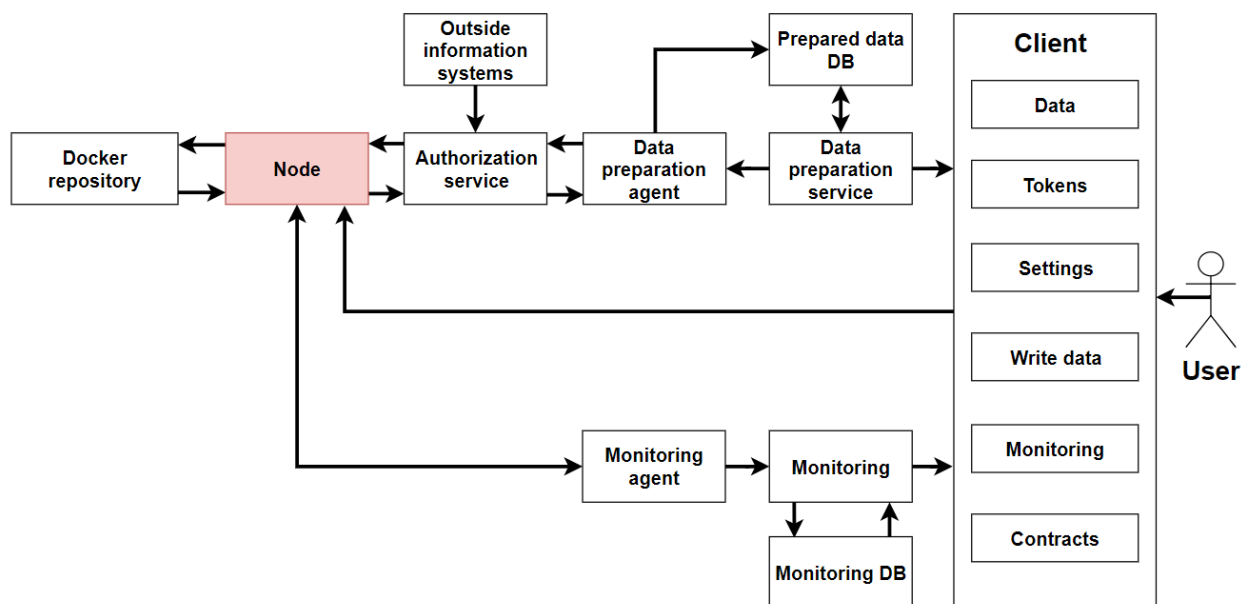
9.2 Sending and receiving the data

The data is sent via `POST /privacy/sendData` request through its own node of the organization, which checks whether the sender is a member of the specified group. If that check is successful, the data is written to the node store, and the *PolicyDataHash* transaction (type = 114, sending the data hash) is initiated with the calculated hash sum of the data. The size limit for transferring data to the network is 20 MB.

When a receiving party receives a transaction with the hash sum from the transmitted data, it checks whether the blockchain node is involved in the group specified in the transaction. If the participant belongs to the group, the `getPrivateData` request for confidential data is executed at the network address of the group participant via P2P connection. To ensure the security of data transmission over an unprotected communication channel, a set of encryption algorithms and the Diffey-Hellman protocol are used.

CLIENT

Waves Enterprise client is a convenient way to manage your blockchain. Client is intended for operations in the Waves Enterprise *public network*.



The client includes sections for use of all blockchain features:

- “Data” — allows to find information about transactions or users through flexible search and advanced filter system.
- “Tokens” — allows to transfer, issue, lease tokens.
- “Contracts” — provides tools for publishing and calling docker contracts. Contracts are available for publishing from the repository, the address of which was specified when the client was built.
- “Enter Data” — allows sending data transactions and files from the interface.
- “Settings” — allows managing permissions for user actions in the blockchain.

The client supports the following browsers:

- Google Chrome.
- Mozilla Firefox.
- Opera.
- Apple Safari.

- Microsoft Edge.

If the client web interface does not work properly, or if you see any errors during loading pages, please, update your browser to the latest version.

Data

This section contains information about blockchain transactions. For information, use the filter and the search string to specify the transaction fields to search for.

Available transaction filters:

- All transactions - displays of all transactions.
- Data transactions - displays of the data transactions.
- Tokens - a selection of transactions with tokens. When this value is selected, an additional option of contextual filtering by types of token operations (for example, transfer, lease or issue of tokens) appears.
- Permissions - a transactions selection by operations with aliases and by user permissions. When selected, context filters are available by permission type (for example, mining, contract publishing, or access control).
- Groups - a selection of privacy data access groups transactions. When this value is selected, an additional option of contextual filtering by operation types (for example, a creation or an update of the access group) appears.
- Contracts - a selection of the contracts transactions. When this value is selected, an additional option of contextual filtering by contracts types (for example, Docker or RIDE) appears.
- Unconfirmed transactions - a selection of the unconfirmed transactions.
- Users - users info. When this value is selected, an additional option of contextual filtering by permissions types (for example, mining, publish smart-contract or access control) appears.

Tokens

This section shows the balance of authorized account. Allows transferring tokens to other network participants, transfer tokens for lease and manage tokens. Token management requires the “Token Management” permission.

Contracts

The section displays information on existing contracts in the network and allows you to run the selected contracts. You can use the search string with transaction parameters for the filtration. Contract publishing requires the “contract-developer” role.

Data transactions

The section allows to create data transactions and view information about existing data transactions.

Settings

The section contains basic information about the user’s account (public and private keys, secret phrase), also the current version of the client and allows you to change the language of the interface. Also you can add permissions to another users. This option requires the “permissioner” role.

BLOCKS, TRANSACTIONS, MESSAGES

11.1 Blocks

This module contains the structure of block storage in the Waves Enterprise blockchain.

| Field order number | Field | Type | Field size in bytes |
|--------------------|---|-------|---------------------|
| 1 | Version (0x02 for Genesis block, 0x03 for common block) | Byte | 1 |
| 2 | Timestamp | Long | 8 |
| 3 | Parent block signature | Bytes | 64 |
| 4 | Consensus block length (always 40 bytes) | Int | 4 |
| 5 | Base target | Long | 8 |
| 6 | Generation signature* | Bytes | 32 |
| 7 | Transactions block length (N) | Int | 4 |
| 8 | Transaction #1 bytes | Bytes | M1 |
| ... | ... | ... | ... |
| 8 + (K - 1) | Transaction #K bytes | Bytes | MK |
| 9 + (K - 1) | Generator's public key | Bytes | 32 |
| 10 + (K - 1) | Block's signature | Bytes | 64 |

Generation signature is calculated based on the hash (Blake2b256) of the following fields:

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------------------|-------|---------------------|
| 1 | Previous block's generation signature | Bytes | 32 |
| 2 | Generator's public key | Bytes | 32 |

The block signature is calculated based on the following data:

| Field order number | Field | Type | Field size in bytes |
|--------------------|--|-------|---------------------|
| 1 | Version (0x02 for Genesis block,, 0x03 for common block) | Byte | 1 |
| 2 | Timestamp | Long | 8 |
| 3 | Parent block signature | Bytes | 64 |
| 4 | Consensus block length (always 40 bytes) | Int | 4 |
| 5 | Base target | Long | 8 |
| 6 | Generation signature* | Bytes | 32 |
| 7 | Transactions block length (N) | Int | 4 |
| 8 | Transaction #1 bytes | Bytes | M1 |
| ... | ... | ... | ... |
| 8 + (K - 1) | Transaction #K bytes | Bytes | MK |
| 9 + (K - 1) | Generator's public key | Bytes | 32 |

11.2 Transactions

In this section we can see the structure of transaction storage in the blockchain platform of Waves Enterprise. For some types of transactions, versioning is introduced.

Important: All transactions use the `timestamp` field containing a time stamp in the **Unix Timestamp** format in milliseconds.

Table 1: Transaction types

| № | Transaction type | Description |
|-----|--|---|
| 1 | <i>Genesis transaction</i> | Initial binding of the balance to the addresses of nodes created at the start of the blockchain |
| 3 | <i>Issue Transaction</i> | Tokens issue |
| 4 | <i>Transfer Transaction</i> | Tokens transfer |
| 5 | <i>Reissue Transaction</i> | Tokens reissue |
| 6 | <i>Burn Transaction</i> | Tokens burn |
| 8 | <i>Lease Transaction</i> | Tokens lease |
| 9 | <i>Lease Cancel Transaction</i> | Cancel of the tokens lease |
| 10 | <i>Create Alias Transaction</i> | Alias creation |
| 11 | <i>MassTransfer Transaction</i> | Mass tokens transfer. Minimum commission is specified |
| 12 | <i>Data Transaction</i> | Transaction with the data in the key-value pairs format. Minimum commission is specified |
| 13 | <i>SetScript Transaction</i> | Transaction which is binding a script with a RIDE contract to an account |
| 14 | <i>Sponsorship Transaction</i> | Transaction which is signing a sponsorship asset |
| 15 | <i>SetAssetScript</i> | Transaction which is binding a script with a RIDE contract to an asset |
| 101 | <i>Genesis Permission Transaction</i> | Assignment of the first network administrator for further distribution of rights |
| 102 | <i>Permission Transaction</i> | Issuance/withdrawal of rights from the account |
| 103 | <i>CreateContract Transaction</i> | Docker-contract creation |
| 104 | <i>CallContract Transaction</i> | Docker-contract call |
| 105 | <i>ExecutedContract Transaction</i> | Docker-contract execution |
| 106 | <i>DisableContract Transaction</i> | Docker-contract disable |
| 107 | <i>UpdateContract Transaction</i> | Docker-contract update |
| 110 | <i>GenesisRegisterNode Transaction</i> | Node registration in the genesis block with the blockchain start |
| 111 | <i>RegisterNode Transaction</i> | A new node registration |
| 112 | <i>CreatePolicy Transaction</i> | Access group creation |
| 113 | <i>UpdatePolicy Transaction</i> | Update the access group |
| 114 | <i>PolicyDataHash Transaction</i> | A data hash sending to the net |

For more information, see *Commissions on the network “Waves Enterprise Mainnet”*

11.2.1 1. Genesis transaction

| Field | Broadcasted JSON | Blockchain state | Type |
|-----------|------------------|------------------|---------|
| type | + | + | Byte |
| id | + | | Byte |
| fee | + | | Long |
| timestamp | + | + | Long |
| signature | + | | ByteStr |
| recipient | + | + | ByteStr |
| amount | + | + | Long |
| height | + | | |

11.2.2 3. Issue Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| assetId | | + | | ByteStr |
| name | + | + | + | Array[Byte] |
| quantity | + | + | + | Long |
| reissuable | + | + | + | Boolean |
| decimals | + | + | + | Byte |
| description | + | + | + | Array[Byte] |
| chainId | | + | + | Byte |
| script | + (opt) | + | + | Bytes |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 3,
  "version": 2,
  "name": "Test Asset 1",
  "quantity": 10000000000,
  "description": "Some description",
  "sender": "3FSCKyfFo3566zwiJjSFLBwKvd826KXUaqR",
  "password": "",
  "decimals": 8,
  "reissuable": true,
  "fee": 100000000
}
```

Broadcasted JSON

```
{
  "type": 3,
  "id": "DnK5Xfi2wXUJx9BjK9X6ZpFdTLdq2GtWH9pWrcxcmrhB",
  "sender": "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ",
  "senderPublicKey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "fee": 100000000,
  "timestamp": 1549378509516,
  "proofs": [
    ↪ "NqZGcbcQ82FZrPh6aCEjuo9nNnkPTvyhrNq329YWydaYcZTywXUwDxFaknTMEGuFrEndCjXBtrueLWaqbJhpeiG" ],
  "version": 2,
  "assetId": "DnK5Xfi2wXUJx9BjK9X6ZpFdTLdq2GtWH9pWrcxcmrhB",
  "name": "Token Name",
  "quantity": 10000,
  "reissuable": true,
  "decimals": 2,
  "description": "SmarToken",
  "chainId": 84,
  "script": "base64:AQa3b8tH",
  "height": 60719
},
```

11.2.3 4. Transfer Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| recipient | + | + | + | ByteStr |
| assetId | + (opt) | + | + | ByteStr |
| fee assetId | + (opt) | + | + | Bytes |
| amount | + | + | + | Long |
| attachment | + (opt) | + | + | Bytes |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 4,
  "version": 2,
  "sender": "3M6dRZXaJY9oMA3fJKhMALyYKt13D1aimZX",
  "password": "",
  "recipient": "3M6dRZXaJY9oMA3fJKhMALyYKt13D1aimZX",
  "amount": 40000000000,
  "fee": 100000
}
```

Broadcasted JSON

```
{
  "senderPublicKey": "4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
  "amount": 200000000,
  "fee": 100000,
  "type": 4,
  "version": 2,
  "attachment": "3uaRTtZ3taQtRSmquqeC1DniK3Dv",
  "sender": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
  "feeAssetId": null,
  "proofs": [
    "2hRxJ2876CdJ498UCpErNfDSYdt2mTK4XUnmZNgZiq63RupJs5WTrAqR46c4rLQdq4toBzk2tSYCeAQWEQyi72U6"
  ],
  "assetId": null,
  "recipient": "3GPtj5osoYqHpyfmsFv7BMiyKsVzbG1ykfL",
  "id": "757aQzJiQZRfVRuJNnP3L1d369H2oTjUEazwtYxGngCd",
  "timestamp": 1558952680800
}
```

11.2.4 5. Reissue Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| chainId | | + | + | Byte |
| assetId | + | + | + | ByteStr |
| quantity | + | + | + | Long |
| reissuable | + | + | + | Boolean |
| password | + (opt) | | | String |
| height | | | | |

JSON to sign

```
{
  "type": 5,
  "version": 2,
  "quantity": 10000,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "assetId": "7bE3JPwZC3QcN9edctFrLAKYysjfMEk1SDjZx5gitSGg",
  "reissuable": true,
  "fee": 100000001
}
```

Broadcasted JSON

```
{
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "quantity": 10000,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "chainId": 84,
  "proofs": [
    ↪ "3gmgGM6rYpxuuR5QvJkugPsERG7yWYF7JN6QzpUGJwT8Lw6SUHkzzk8R22A7cGQz7TQQ5NifKxvAQzwpYDQbwmBg" ],
  "assetId": "7bE3JPwZC3QcN9edctFrLAKYysjfMEk1SDjZx5gitSGg",
  "fee": 100000001,
  "id": "GsNvk15Vu4kqtRmMSPyW21WzgJpZrLBwjCREHWuwnvh5",
  "type": 5,
  "version": 2,
  "reissuable": true,
  "timestamp": 1551447859299,
  "height": 1190
}
```

11.2.5 6. Burn Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| chainId | | + | + | Byte |
| assetId | + | + | + | ByteStr |
| quantity | + | | + | Long |
| amount | | + | | Long |
| password | + (opt) | | | String |
| height | | | | |

JSON to sign

```
{
  "type": 6,
  "version": 2,
  "sender": "3MtrNP7AkTRuBhX4CBti6iT21pQpEnmHtyw",
  "password": "",
  "assetId": "7bE3JPwZC3QcN9edctFrLAKYysjfMEk1SDjZx5gitSGg",
  "quantity": 1000,
  "fee": 100000,
  "attachment": "string"
}
```

Broadcasted JSON

```
{
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
```

(continues on next page)

(continued from previous page)

```

"amount": 1000,
"sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
"chainId": 84,
"proofs": [
↪ "kzTwsNXjJkzk6dpFFZZXyeimYo6iLTVbCnCXBD4xBtyrNjysPqZfGKk9NdJUTP3xeAPhtEgU9hsdwzRVo1hKMgS" ],
"assetId": "7bE3JPwZC3QcN9edctFrLAKYysjfMEk1SDjZx5gitSGg",
"fee": 100000,
"id": "3yd2HZq7sgun7GakisLH88UeKcpYMUEL4sy57aprAN5E",
"type": 6,
"version": 2,
"timestamp": 1551448489758,
"height": 1190
}

```

11.2.6 8. Lease Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| amount | + | + | + | Long |
| recipient | + | + | + | ByteStr |
| status | | + | | |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```

{
  "type": 8,
  "version": 2,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "recipient": "3N1ksBqc6uSksdiYjCzMtvEpiHhS1JjkbPh",
  "amount": 1000,
  "fee": 100000
}

```

Broadcasted JSON

```

{
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "amount": 1000,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "proofs": [
↪ "5jvmWkmU89HnxXFXNAd9X41zmiB5fSGoXMirsaJ9tNeyiCAJmjm7MR48g789VucckQw2UEXaVXfhdsEBuUrchvrq" ],
  "fee": 100000,
}

```

(continues on next page)

(continued from previous page)

```

"recipient": "3N1ksBqc6uSksdiYjCzMtvEpiHhS1JjkbPh",
"id": "6Tn7ir9MycHW6Gq2F2dGok2stokSwXJadPh4hW8eZ8Sp",
"type": 8,
"version": 2,
"timestamp": 1551449299545,
"height": 1190
}

```

11.2.7 9. Lease Cancel Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| chainId | | + | + | Byte |
| leaseId | + (txId) | + | + | Byte |
| leaseId | | + | | |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```

{
  "type": 9,
  "version": 2,
  "fee": 100000,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "txId": "6Tn7ir9MycHW6Gq2F2dGok2stokSwXJadPh4hW8eZ8Sp"
}

```

Broadcasted JSON

```

{
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "leaseId": "6Tn7ir9MycHW6Gq2F2dGok2stokSwXJadPh4hW8eZ8Sp",
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "chainId": 84,
  "proofs": [
    ↪ "2Gns72hraH5yay3eiWeyHQEA1wTqiiAztaLjHinEYX91FEv62HFV38Hq89GnsEJFHUvo9KHYtBBrb8hgTA9wN7DM" ],
  "fee": 100000,
  "id": "9vhxB2ZDQcqiumhQbCPnAoPBLuir727qgJhFeBNmPwmu",
  "type": 9,
  "version": 2,
  "timestamp": 1551449835205,
  "height": 1190
}

```


11.2.8 10. Create Alias Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| alias | + | + | + | Bytes |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 10,
  "version": 2,
  "fee": 100000,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "alias": "hodler"
}
```

Broadcasted JSON

```
{
  "type": 10,
  "id": "DJTtaiMpb7eLuPW5GcE4ndeE8jWswPjx8gPYmbZPJjpag",
  "sender": "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ",
  "senderPublicKey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "fee": 0,
  "timestamp": 1549290335781,
  "signature":
  ↪ "2qYepod9DhpxVad1yQDbv1QzU4KLKcbjjdtGY7De2272K76nbQfaXsRnyd31hUE8bhvLjjpHRdtoLVzbBDzRZYEY",
  "proofs": [
  ↪ "2qYepod9DhpxVad1yQDbv1QzU4KLKcbjjdtGY7De2272K76nbQfaXsRnyd31hUE8bhvLjjpHRdtoLVzbBDzRZYEY" ],
  "version": 1,
  "alias": "testperson4",
  "height": 59245
}
```

11.2.9 11. MassTransfer Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| assetId | + (opt) | + | + | ByteStr |
| attachment | + (opt) | + | + | |
| number of transfers | + | + | + | List[Transfer] |
| transferCount | | + | + | |
| totalAmount | | + | | |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 11,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "fee": 2000000,
  "version": 1,
  "transfers":
  [
    { "recipient": "3MtHszoTn399NfsH3v5foeEXRRrchEVtTRB", "amount": 100000 },
    { "recipient": "3N7BA6J9VUBfBRutuMyjF4yKTUetrRfFHMc", "amount": 100000 }
  ],
  "height": 1190
}
```

Broadcasted JSON

```
{
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "fee": 2000000,
  "type": 11,
  "transferCount": 2,
  "version": 1,
  "totalAmount": 200000,
  "attachment": "",
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "proofs": [
    ↪ "2gWpMWdgZCjbygCX5US3aAfftKtGPRSK3aWGJ6RDnWJf9hend5sBFAgY6u3Mp4jN8cqwaJ5o8qrKNedGN5CPN1GZ" ],
  "assetId": null,
  "transfers":
  [
    {
      "recipient": "3MtHszoTn399NfsH3v5foeEXRRrchEVtTRB",
      "amount": 100000
    }
  ],
}
```

(continues on next page)

(continued from previous page)

```

    {
      "recipient": "3N7BA6J9VUBfBRutuMyjF4yKTUEtrRFfHMc",
      "amount": 100000
    }
  ],
  "id": "D9jUSHHcJqVAvkFMiRfDBhQbUzoSfQqd9cjaunMmtjdu",
  "timestamp": 1551450279637
}

```

11.2.10 12. Data Transaction

Warning: The transaction has limits:

1. "key": "value" pairs count no more than 100,

```

"data": [
  {
    "key": "objectId",
    "type": "string",
    "value": "obj:123:1234"
  }, {...}
]

```

2. The byte composition of the signed transaction should not exceed more than 150 KB.

Hint: You do not need to specify the `senderPublicKey` parameter if you are signing a transaction where the author and the sender are the same.

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type | Size (Bytes) |
|---------------------|--------------|------------------|------------------|------------------|--------------|
| type | + | + | + | Byte | 1 |
| id | | + | | Byte | 1 |
| sender | + | + | | PublicKeyAccount | 3264 |
| sender's public key | + (opt) | + | + | PublicKeyAccount | 3264 |
| fee | + | + | + | Long | 8 |
| timestamp | + (opt) | + | + | Long | 8 |
| proofs | | + | + | List[ByteStr] | 32767 |
| version | + | + | | Byte | 1 |
| authorPublicKey | | + | + | PublicKeyAccount | 3264 |
| author | + | + | | | 3264 |
| data | + | + | + | | 3264 |
| password | + (opt) | | | String | 32767 |
| height | | + | | | 8 |

JSON to sign

```
{
  "type": 12,
  "version": 1,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "author": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "data": [
    {
      "key": "objectId",
      "type": "string",
      "value": "obj:123:1234"
    }
  ],
  "fee": 100000
}
```

Broadcasted JSON

```
{
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "authorPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "data":
  [
    {
      "type": "string",
      "value": "obj:123:1234",
      "key": "objectId"
    }
  ],
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "proofs": [
    ↪ "2T7WQm5XW8cFHfiFkdDEic9oNiT7aFiH3TyKkAREopr1VJvzRkqHAVnQ3eiYZ3uYN8uQnPopQEH4XV8z5SgSwsf" ],
  "author": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "fee": 100000,
  "id": "7dMMCQNTusahZ7DWtNGjCwAhRYpjaH1hseprMbpn2BkD",
  "type": 12,
  "version": 1,
  "timestamp": 1551680510183
}
```

11.2.11 13. SetScript Transaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| chainId | | + | + | Byte |
| version | + | + | + | Byte |
| script | + (opt) | + | + | Bytes |
| name | + | + | + | Array[Byte] |
| description | + (opt) | + | + | Array[Byte] |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 13,
  "version": 1,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "fee": 1000000,
  "name": "faucet",
  "script": "base64:AQQAAAAHJG1hdGNoMAUAAAAACdHgG+RXSszQ=="
}
```

Broadcasted JSON

```
{
  "type": 13,
  "id": "HPDyqnQJHJskN8kwszF8rck3E5tQiuim1fEN42w6PLmt",
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "fee": 1000000,
  "timestamp": 1545986757233,
  "proofs": [
    ↪ "2QiGYS2dqh8QyN7Vu2tAYaioX5WM6rTSDPGbt4zrWS7QKTzobjmR2kjjpvGNj4tDPsYPbcDunqBaqhaudLyMeGFgG" ],
  "chainId": 84,
  "version": 1,
  "script": "base64:AQQAAAAHJG1hdGNoMAUAAAAACdHgG+RXSszQ==",
  "name": "faucet",
  "description": "",
  "height": 3805
}
```

11.2.12 14. SponsorshipTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| assetId | + (opt) | + | + | ByteStr |
| fee | + | + | + | Long |
| isEnabled | + | + | + | Boolean |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| chainId | | + | + | Byte |
| version | + | + | + | Byte |
| script | + (opt) | + | + | Bytes |
| name | + | + | + | Array[Byte] |
| description | + (opt) | + | + | Array[Byte] |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "sender": "3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t",
  "assetId": "G16FvJk9vabwxjQswh9CQAhbZzn3QrwqWjwnZB3qNVox",
  "fee": 100000000,
  "isEnabled": false,
  "type": 14,
  "password": "1234",
  "version": 1
}
```

Broadcasted JSON

```
{
  "type": 14,
  "id": "Ht6kpnQJHJskN8kwszF8rck3E5tQiuM1fEN42wGfdk7",
  "sender": "3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t",
  "senderPublicKey": "Gt55fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUoPhy89",
  "fee": 100000000,
  "assetId": "G16FvJk9vabwxjQswh9CQAhbZzn3QrwqWjwnZB3qNVox",
  "timestamp": 1545986757233,
  "proofs": [
    ↪ "5TfgYS2dqh8QyN7Vu2tAYaioX5WM6rTSDPGbt4zrWS7QKTzobjmR2kjppvGNj4tDPsYPbcDunqBaqhaudLyMeGFh7" ],
  "chainId": 84,
  "version": 1,
  "isEnabled": false,
  "height": 3865
}
```

11.2.13 15. SetAssetScriptTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | + | + | + | Byte |
| chainId | | + | + | Byte |
| assetId | + | + | + | ByteStr |
| script | + (opt) | + | + | Bytes |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 15,
  "version": 1,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "password": "",
  "fee": 100000000,
  "script": "base64:AQQAAAAHJG1hdGNoMAUAAAAcDhgG+RXSzQ==",
  "assetId": "7bE3JPwZC3QcN9edctFrLAKYysjfMEk1SDjZx5gitSGg"
}
```

Broadcasted JSON

```
{
  "type": 15,
  "id": "CQpEM9AEDvgxKfgWLH2HxE82iAzpXrtqsDDcgZGPAF9J",
  "sender": "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ",
  "senderPublicKey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "fee": 100000000,
  "timestamp": 1549448710502,
  "proofs": [
    ↪ "64eodpuXQjaKQQ4GJBaBrqiBtmkjSxseKC97gn6EwB5kZtMr18mAUHPRkZaHJeJxaDyLzGEZKqhYoUknWfNhXnkf" ],
  "version": 1,
  "chainId": 84,
  "assetId": "DnK5Xfi2wXUJx9BjK9X6ZpFdTLdq2GtWH9pWrcxcmrhB",
  "script": "base64:AQQAAAAHJG1hdGNoMAUAAAAcDhgG+RXSzQ==",
  "height": 61895
}
```

11.2.14 101. GenesisPermitTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|-----------|--------------|------------------|------------------|------|
| type | + | + | Byte | |
| id | + | | Byte | |
| fee | + | | Long | |
| timestamp | + | + | Long | |
| signature | + | | ByteStr | |
| target | + | + | ByteStr | |
| role | + | + | String | |
| height | | | | |

11.2.15 102. PermissionTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | | + | | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | | | + | Byte |
| target | + | + | + | ByteStr |
| PermissionOp | | | + | PermissionOp |
| opType | + | + | | String |
| role | + | + | | String |
| dueTimestamp | + (opt) | + | | Option[Long] |
| password | + (opt) | | | String |
| height | | + | | |

JSON to sign

```
{
  "type": 102,
  "sender": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
  "password": "",
  "senderPublicKey": "4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
  "fee": 0,
  "proofs": [],
  "target": "3GPtj5osoYqHpyfmsFv7BMiyKsVzbG1ykfL",
  "opType": "add",
  "role": "contract_developer",
  "dueTimestamp": null
}
```

Broadcasted JSON

```
{
  "senderPublicKey": "4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
  "role": "contract_developer",
```

(continues on next page)

(continued from previous page)

```

"sender": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
"proofs": [
  "5ABJCRKGo6jmDZCRWcLQc257CCeczmcjmtfJmbBE7TP3KsVkwvisH9kEkfYPckVCzEMKZTCd3LKAPcN8o4Git3j"
],
"fee": 0,
"opType": "add",
"id": "8zVUH7nsDCcpwyfxiq8DCTgqL7Q23FW1KWepB9EZcFG6",
"type": 102,
"dueTimestamp": null,
"timestamp": 1559048837487,
"target": "3GPtj5osoYqHpyfmsFv7BMiyKsVzbG1ykfL"
}
    
```

11.2.16 103. CreateContractTransaction

Warning: The byte composition of the signed transaction should not exceed more than 150 KB.

The `contractVersion` field specifies the contract version, the 1 value is for the new contract, and the 2 value is for the updated contract. The contract is updated by using the 107 transaction. When you create a contract, the 104 transaction is automatically created, this transaction is calling the contract to validate it. If the contract fails or runs with error, transactions 103 and 104 will be discarded and will not fall into the block.

The `feeAssetId` field is optional and used only for *gRPC contracts* (the field value `version = 2`).

| Field | JSON sign | to | Broadcasted JSON | Blockchain state | Type | Size(Bytes) |
|---------------------|-----------|----|------------------|------------------|--------------------|-------------|
| type | + | | + | + | Byte | 1 |
| id | | | + | | Byte | 1 |
| sender | + | | + | | PublicKeyAccount | 3264 |
| sender's public key | | | + | + | PublicKeyAccount | 3264 |
| password | + (opt) | | | | String | 32767 |
| fee | + | | + | + | Long | 8 |
| timestamp | + (opt) | | + | + | Long | 8 |
| proofs | | | + | + | List[ByteStr] | 32767 |
| version | | | + | + | Byte | 1 |
| fee assetId | + (opt) | | | | Byte | 1 |
| image | + | | + | + | Array[Byte] | 32767 |
| imageHash | + | | + | + | Array[Byte] | 32767 |
| contractName | + | | + | + | Array[Byte] | 32767 |
| params | + | | + | + | List[DataEntry[_]] | 32767 |
| height | | | + | | | 8 |

JSON to sign

```

{
  "fee": 100000000,
    
```

(continues on next page)

(continued from previous page)

```

"image": "stateful-increment-contract:latest",
"imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
"contractName": "stateful-increment-contract",
"sender": "3PudkbvjV1nPj1TkuuRahh4sGdgfr4YAUV2",
"password": "",
"params": [],
"type": 103,
"version": 1,
}

```

Broadcasted JSON

```

{
  "type": 103,
  "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLLLZVj4Ky",
  "sender": "3N3YTjtNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
  "fee": 500000,
  "timestamp": 1550591678479,
  "proofs": [
    ↪ "yeCRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
  "version": 1,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "params": [],
  "height": 1619
}

```

11.2.17 104. CallContractTransaction

Warning: The byte composition of the signed transaction should not exceed more than 150 KB.

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type | Size(Bytes) |
|---------------------|--------------|------------------|------------------|--------------------|-------------|
| type | + | + | + | Byte | 1 |
| id | | + | | Byte | 1 |
| sender | + | + | | PublicKeyAccount | 3264 |
| sender's public key | | + | + | PublicKeyAccount | 3264 |
| fee | + | + | + | Long | 8 |
| timestamp | + (opt) | + | + | Long | 8 |
| proofs | | + | + | List[ByteStr] | 32767 |
| version | | + | + | Byte | 1 |
| contractVersion | + | + | + | Byte | 1 |
| contractId | + | + | + | ByteStr | 32767 |
| params | + | + | + | List[DataEntry[_]] | 32767 |
| height | | + | | | 8 |
| password | + (opt) | | | String | 32767 |

JSON to sign

```
{
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "fee": 10,
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "password": "",
  "type": 104,
  "params":
  [
    {
      "type": "integer",
      "key": "a",
      "value": 1
    },
    {
      "type": "integer",
      "key": "b",
      "value": 100
    }
  ],
  "version": 1,
  "contractVersion": 1
}
```

Broadcasted JSON

```
{
  "type": 104,
  "id": "9fBrL2n5TN473g1gNfoZqaAqAsAJCuHRHYxZpLexL3VP",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVlrqLcQouVrFZynjfoTEuPNV9GrdauNpgdWXLsq",
  "fee": 10,
  "timestamp": 1549365736923,
  "proofs": [
    ↪ "2q4cTBhdKEDkFxr7iYaHPAv1dzaKo5rDaTxPF5VHryyYTXxTPvN9Wb3YrsDYixKiUPXBnAyXzEcnKPFRCW9xVp4v" ],
  "version": 1,
  "contractVersion": 1,
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "params":
  [
    {
      "key": "a",
      "type": "integer",
      "value": 1
    },
    {
      "key": "b",
      "type": "integer",
      "value": 100
    }
  ]
}
```

11.2.18 105. ExecutedContractTransaction

Warning: The byte composition of the signed transaction should not exceed more than 150 KB.

| Field | Broadcasted JSON | Blockchain state | Type |
|---------------------|------------------|------------------|-----------------------|
| type | + | + | Byte |
| id | + | | Byte |
| sender | + | | PublicKeyAccount |
| sender's public key | + | + | PublicKeyAccount |
| fee | + | | Long |
| timestamp | + | + | Long |
| proofs | + | + | List[ByteStr] |
| version | + | + | Byte |
| tx | + | + | ExecutableTransaction |
| results | + | + | List[DataEntry[_]] |
| height | + | | |
| password | + (opt) | | String |

Broadcasted JSON

```
{
  "type": 105,
  "id": "38GmSVC5s8Sjeybzfe9RQ6p1Mb6ajb8LYJDcep8G8Umj",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
  "password": "",
  "fee": 500000,
  "timestamp": 1550591780234,
  "proofs": [
    ↪ "5whBipAWQgFvm3myNZe6GDd9Ky8199C9qNxBHqDnmVAUJW9gLf7t9LBQDi68CKT57dzmnP JpJkrwKh2HBSwUer6" ],
  "version": 1,
  "tx": {
    "type": 103,
    "id": "ULc9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLZZVj4Ky",
    "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
    "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
    "fee": 500000,
    "timestamp": 1550591678479,
    "proofs": [
      ↪ "yecRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
    "version": 1,
    "image": "stateful-increment-contract:latest",
    "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
    "contractName": "stateful-increment-contract",
    "params": [],
    "height": 1619
  },
  "results": [],
  "height": 1619
}
```

11.2.19 106. DisableContractTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | | + | + | Byte |
| contractId | + | + | + | ByteStr |
| height | | + | | |
| password | + (opt) | | | String |

JSON to sign

```
{
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "password": "",
  "contractId": "Fz3wqAwwcPMT4M1q6H7crLKtToFJvbeLSvqjaU4ZwMpg",
  "fee": 500000,
  "type": 106
}
```

Broadcasted JSON

```
{
  "type": 106,
  "id": "8Nw34YbosEVhCx18pd81HqYac4C2pGjyLKck8NhSoGYH",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
  "fee": 500000,
  "proofs": [
    ↪ "5GqPQkuRvG6LPXgPoCr9FogAdmhAaMbyFb5UfjQPuKdSc6BLuQsZ75LAWix1ok2Z6PC5ezPpjzqnr15i3RQmaEc" ],
  "version": 1,
  "contractId": "Fz3wqAwwcPMT4M1q6H7crLKtToFJvbeLSvqjaU4ZwMpg",
  "height": 1632
}
```

11.2.20 107. UpdateContractTransaction

Warning: The byte composition of the signed transaction should not exceed more than 150 KB.

| Field | JSON sign | to | Broadcasted JSON | Blockchain state | Type | Size(Bytes) |
|---------------------|-----------|-------|------------------|------------------|------------------|-------------|
| type | + | | + | + | Byte | 1 |
| id | | | + | | Byte | 1 |
| sender | + | | + | | PublicKeyAccount | 3264 |
| sender's public key | | | + | + | PublicKeyAccount | 3264 |
| image | + | | + | + | Array[Byte] | 32767 |
| imageHash | + | | + | + | Array[Byte] | 32767 |
| fee | + | | + | + | Long | 8 |
| timestamp | + | (opt) | + | + | Long | 8 |
| proofs | | | + | + | List[ByteStr] | 32767 |
| version | + | | + | + | Byte | 1 |
| contractId | + | | + | + | ByteStr | 32767 |
| height | | | + | | | 8 |
| password | + | (opt) | | | String | 32767 |

JSON to sign

```
{
  "image" : "registry.wvservices.com/we-sc/tdm-increment3:1028.1",
  "sender" : "3Mxxz9pBYS5fJMARJNQmzYUHxiWAtvMzSRT",
  "password": "",
  "fee" : 100000000,
  "contractId" : "EnsihTUHSNAB9RcWXJbiWT98X3hYtCw3SBzK8nHQRcWA",
  "imageHash" : "0e5d280b9acf6efd8000184ad008757bb967b5266e9ebf476031fad1488c86a3",
  "type" : 107,
  "version" : 1
}
```

Broadcasted JSON

```
{
  "senderPublicKey":
  ↪ "5qBRDm74WKR5xK7LPs8vCy9QjzzqK4KCb8PL36fm55S3kEi2XZETHFgMgp3D13AwgE8bBkYrzvEvQZuabMfEyJwW",
  "tx":
  {
    "senderPublicKey":
    ↪ "5qBRDm74WKR5xK7LPs8vCy9QjzzqK4KCb8PL36fm55S3kEi2XZETHFgMgp3D13AwgE8bBkYrzvEvQZuabMfEyJwW",
    "image": "registry.wvservices.com/we-sc/tdm-increment3:1028.1",
    "sender": "3Mxxz9pBYS5fJMARJNQmzYUHxiWAtvMzSRT",
    "proofs": [
    ↪ "3tNsTyteeZrxEbVsv5zPT6dr247nXsVWR5v7Kxh8spypgZQUdorCQZV2guTomutUTcyxhJUjnkQW4VmSgbCtgm1Z"],
    "fee": 0,
    "contractId": "EnsihTUHSNAB9RcWXJbiWT98X3hYtCw3SBzK8nHQRcWA",
    "id": "HdZdhXVveMT1vYzGTviCoGQU3aH6ZS3YtFpYujWeGCH6",
    "imageHash": "17d72ca20bf9393eb4f4496fa2b8aa002e851908b77af1d5db6abc9b8eae0217",
  }
}
```

(continues on next page)

(continued from previous page)

```

"type":107,"version":1,"timestamp":1572355661572},
"sender":"3HfRBedCpWi3vEzFSKEZDFXkyNwbLWQmmG",
"proofs":[
↪"28ADV8miUVN5EFjhqeFj6MADSXYjbxA3TsxSwFVs18jXAsHVAbczvnyoUSaYJsJRnmaWgXbpbduccRxpKGTs6tro"],
"fee":0,"id":"7niVY8mjzeKqLBePvhTxFRfLu7BmcwVfqaqtbWAN8AA2",
"type":105,
"version":1,
"results":[],
"timestamp":1572355666866
}
}

```

11.2.21 110. GenesisRegisterNodeTransaction

| Field | Broadcasted JSON | Blockchain state | Type |
|--------------|------------------|------------------|-------|
| type | + | + | Byte |
| id | + | | Byte |
| fee | + | | Long |
| timestamp | + | + | Long |
| signature | + | | Bytes |
| version | | + | Byte |
| targetPubKey | + | + | |
| height | + | | |

11.2.22 111. RegisterNodeTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | | Byte |
| sender | + | + | | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| fee | + | + | | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| version | | | + | Byte |
| targetPubKey | + | + | + | PublicKeyAccount |
| nodeName | + | + | + | String |
| opType | + | + | + | |
| height | | + | | |
| password | + (opt) | | | String |

JSON to sign

```

{
"type": 111,
"opType": "add",
"sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUGeytUUz",
"password": "",

```

(continues on next page)

(continued from previous page)

```
"targetPubKey": "apgJP9atQccdBPAGJPwH3NBVqYXrapgJP9atQccdBPAGJPwHapgJP9atQccdBPAGJPwHDKkh6A8",
"nodeName": "Node #1",
"fee": 500000,
}
```

11.2.23 112. CreatePolicyTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | + | Byte |
| sender | + | + | + | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| policyName | + | + | + | String |
| recipients | + | + | + | Array[Byte] |
| owners | + | + | + | Array[Byte] |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| height | | | + | Long |
| description | + | + | + | String |
| password | + (opt) | | | String |

JSON to sign

```
{
  "sender": "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
  "policyName": "Policy# 7777",
  "password": "sfgKYBFCF@#$fsdf()*%",
  "recipients": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T",
    "3NtNJV44wyxRXv2jyW3yXLxjJxvY1vR88TF",
    "3NxAooHUoLsAQvxBSqjE91WK3LwWGjiiCxx"
  ],
  "fee": 15000000,
  "description": "Buy bitcoin by 1c",
  "owners": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T"
  ],
  "type": 112
}
```


11.2.24 113. UpdatePolicyTransaction

| Field | JSON to sign | Broadcasted JSON | Blockchain state | Type |
|---------------------|--------------|------------------|------------------|------------------|
| type | + | + | + | Byte |
| id | | + | + | Byte |
| sender | + | + | + | PublicKeyAccount |
| sender's public key | | + | + | PublicKeyAccount |
| policyName | + | + | + | String |
| recipients | + | + | + | Array[Byte] |
| owners | + | + | + | Array[Byte] |
| fee | + | + | + | Long |
| timestamp | + (opt) | + | + | Long |
| proofs | | + | + | List[ByteStr] |
| height | | | + | Long |
| opType | + | + | + | |
| description | + | + | + | String |
| password | + (opt) | | | String |

JSON to sign

```
{
  "policyId": "7wphGbhqbmUgzun5wzggwqtViTiMdFezSa11fxRV58Lm",
  "password": "sfgKYBFCF@#$fsdf()*%",
  "sender": "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
  "proofs": [],
  "recipients": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T",
    "3NtNJV44wyxRXv2jyW3yXLxjJxvY1vR88TF",
    "3NxAoohUoLsAQvxBSqjE91WK3LwWGjiiCxx",
    "3NwJfjG5RpaDfxEhkwXgd7oX21NMFCxJHL"
  ],
  "fee": 15000000,
  "opType": "add",
  "owners": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T"
  ],
  "type": 113,
}
```

11.2.25 114. PolicyDataHashTransaction

When the user sends confidential data to the network using *POST /privacy/sendData*, the node automatically will create the 114 transaction.

| Field | Broadcasted JSON | Blockchain state | Type |
|---------------------|------------------|------------------|------------------|
| type | + | + | Byte |
| id | + | + | Byte |
| sender | + | + | PublicKeyAccount |
| sender's public key | + | + | PublicKeyAccount |
| policyId | + | + | String |
| dataHash | + | + | String |
| fee | + | + | Long |
| timestamp | + | + | Long |
| proofs | + | + | List[ByteStr] |
| height | | + | Long |

11.3 Network messages

This section describes the structure of network messages in the Waves Enterprise blockchain platform.

11.3.1 Network message

All network messages, except Handshake, are based on the following structure:

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Payload | Bytes | N |

Magic Bytes are 0x12, 0x34, 0x56, 0x78. Payload checksum is first 4 bytes of `_FastHash_` of Payload bytes. `FastHash` is hash function `Blake2b256(data)`.

11.3.2 Handshake message

Handshake message is intended for primary data exchange between two nodes. An authorized Handshake contains the node owner's blockchain address and signature. Unsigned Handshakes are not accepted.

Authorized Handshake

| Field order number | Field | Type | Field size in bytes |
|--------------------|---|-------|---------------------|
| 1 | HandshakeType | byte | 1 |
| 2 | Application name length (N) | Byte | 1 |
| 3 | Application name (UTF-8 encoded bytes) | Bytes | N |
| 4 | Application version major | Int | 4 |
| 5 | Application version minor | Int | 4 |
| 6 | Application version patch | Int | 4 |
| 7 | Consensus name length (P) | Byte | 1 |
| 8 | Consensus name length (UTF-8 encoded bytes) | Bytes | P |
| 9 | Node name length (M) | Byte | 1 |
| 10 | Node name (UTF-8 encoded bytes) | Bytes | M |
| 12 | Node nonce | Long | 8 |
| 13 | Declared address length (K) or 0 if no declared address was set | Int | 4 |
| 14 | Declared address bytes (if length is not 0) | Bytes | K |
| 15 | Peer port | Int | 4 |
| 16 | Node owner address | Bytes | 26 |
| 17 | Signature | Bytes | 64 |

11.3.3 GetPeers message

GetPeers message is sent to request network addresses of network participants.

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x01) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |

11.3.4 Peers message

Peers message is a response to a GetPeers request.

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x02) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Peers count (N) | Int | 4 |
| 7 | Peer #1 IP address | Bytes | 4 |
| 8 | Peer #1 port | Int | 4 |
| ... | ... | ... | ... |
| $6 + 2 * N - 1$ | Peer #N IP address | Bytes | 4 |
| $6 + 2 * N$ | Peer #N port | Int | 4 |

11.3.5 GetSignatures message

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x14) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Block IDs count (N) | Int | 4 |
| 7 | Block #1 ID | Bytes | 64 |
| ... | ... | ... | ... |
| 6 + N | Block #N ID | Bytes | 64 |

11.3.6 Signatures message

| Field order number | Field | Type | Field size in bytes |
|--------------------|----------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x15) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Block signatures count (N) | Int | 4 |
| 7 | Block #1 signature | Bytes | 64 |
| ... | ... | ... | ... |
| 6 + N | Block #N signature | Bytes | 64 |

11.3.7 GetBlock message

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x16) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Block ID | Bytes | 64 |

11.3.8 Block message

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x17) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Block bytes (N) | Bytes | N |

11.3.9 Score message

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|--------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x18) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Score (N bytes) | BigInt | N |

11.3.10 Transaction message

| Field order number | Field | Type | Field size in bytes |
|--------------------|---------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x19) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Transaction (N bytes) | Bytes | N |

11.3.11 Checkpoint message

| Field order number | Field | Type | Field size in bytes |
|--------------------|----------------------------|-------|---------------------|
| 1 | Packet length (BigEndian) | Int | 4 |
| 2 | Magic Bytes | Bytes | 4 |
| 3 | Content ID (0x64) | Byte | 1 |
| 4 | Payload length | Int | 4 |
| 5 | Payload checksum | Bytes | 4 |
| 6 | Checkpoint items count (N) | Int | 4 |
| 7 | Checkpoint #1 height | Long | 8 |
| 8 | Checkpoint #1 signature | Bytes | 64 |
| ... | ... | ... | ... |
| $6 + 2 * N - 1$ | Checkpoint #N height | Long | 8 |
| $6 + 2 * N$ | Checkpoint #N signature | Bytes | 64 |

SMART CONTRACTS

12.1 RIDE Smart Contracts

A smart contract is a script that checks transactions for compliance with conditions. These scripts can extend the logic of blockchain to meet your business tasks. The fee for a smart contract is fixed, and scripts can be published for both an account and token assets issued by the user.

For any given account, a check is performed on all transactions originating from the account's address. An account with a published script is called a smart account. For any given token assets, a check is performed on all transactions using that token asset. A token asset with a published script is called a smart asset. Only one script can be assigned to one account. Accordingly, any installed script replaces the previous one, including the default script.

12.1.1 RIDE

The RIDE language is used for creating scripts on the Waves Enterprise blockchain platform (you can read more about RIDE language on the [WAVES](#) portal). Scripts written in RIDE check conditions use the following data:

- Outgoing transaction details.
- Details of the account on behalf of which transactions are made.
- Details of the third accounts balance.
- Details of the blockchain height.

The principle of script operation is pattern matching. The script specifies transaction types and checks them for compliance with conditions under which corresponding transactions can be executed. Scripts can also permit or ban transactions regardless of conditions. Also there are such options:

- ban transaction regardless of conditions,
- permit regardless of conditions.

Operations with permitted and banned transactions specify transaction types and use the “everything but” principle. The script is set by the Setscript transaction, so permission, prohibition, or verification for compliance with conditions must be explicitly specified.

Important: Scripts do not modify transactions. They only verify that conditions are met.

12.1.2 Complexity of scripts

RIDE is not a Turing-complete language, which imposes limitations on how complex a script's logic can be. This helps guarantee network performance. For complex business processes, the mechanics of which do not fit into one script, a combination of several scripts for several addresses can be used, or a combination of scripts for token assets and addresses. The Waves team is actively developing RIDE features, and in the near future, nested functions that can facilitate more complex tasks will be available to developers.

12.1.3 Signatures and default script

Each transaction in the blockchain has a cryptographic proof of integrity based on the signature of the transaction by the sender's private key. This guarantees that transaction authorship is unalienable. For example, a script which is installed on each address by default verifies the only condition for each outgoing transaction — the signature of the sender's address.

Example of a default script code:

```
sigVerify(tx.bodyBytes, tx.proofs[0], tx.senderPk)
```

These script mechanics enhance proof verification capabilities. A transaction can be signed by another user or multiple users on behalf of the address from which it was sent. This is necessary because a contract can only check transactions originating from its own address. Accordingly, the user generates a transaction on behalf of the contract, signs it with his proof, and successfully passes the script test.

Important: If proof verification is not explicitly specified in your script, it is not executed. Accordingly, when a transaction's body is generated manually, it is possible to send transactions on behalf of an address using a script with another address proof.

12.1.4 Account data

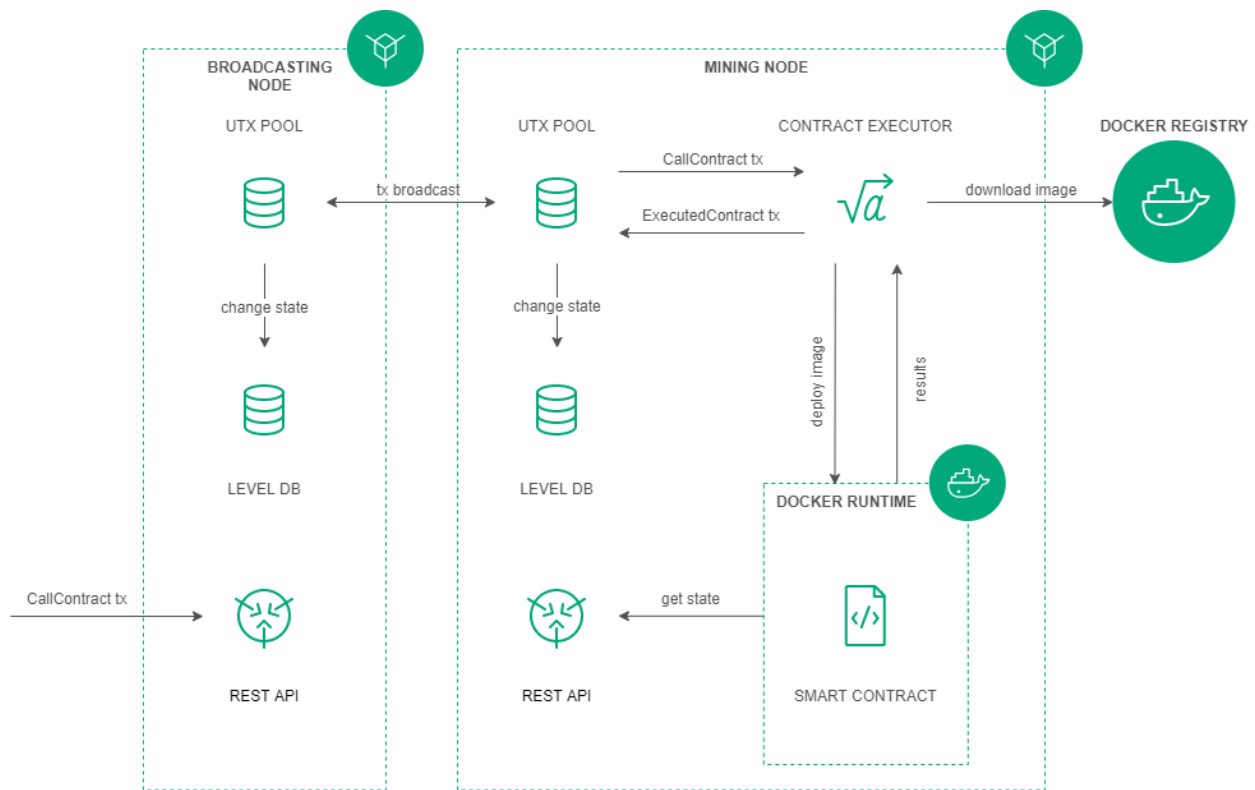
Data can be stored in the key-value format on addresses in the Waves Enterprise Blockchain. The data stored on the address is available for viewing using the request *return data from address by key*. The data is placed on the address when sending a data transaction. Since RIDE scripts are stateless, data transactions update the data stored, which the script addresses. Configuring proof verification on a smart account allows multiple users to collaborate on data on a smart account in different ways.

Important: Keys are unique for each address. Only one value corresponds to one address key. Publishing a new value for an existing key will result in the value being overwritten. The history and the author of changes can be tracked in the blockchain.

12.2 Docker Smart Contracts

In addition to contracts implemented on the basis of *RIDE* scripts for smart accounts and smart-assets, the Waves Enterprise platform provides the option to develop and use Turing-complete smart contracts. To implement Turing-complete contracts, applications are launched within an isolated Docker container environment. Inside this isolated environment, applications can be developed using any programming language. Each application is launched in a Docker container to ensure isolation and manage resources available to any particular application. To store smart contracts, a Docker Registry with read-only access (Docker images) to contracts is used for machines with nodes. The node state can be accessed through a REST API or gRPC framework.

Important: Users must run the Docker-engine and the Docker-daemon simultaneously on the node which is processing the Docker smart-contracts.



12.2.1 Creating a contract

Creating a smart contract starts with the preparation of a Docker image, which consists of the contract program code, the required environment, and the special scenario Dockerfile. A prepared Docker image is then assembled and sent to Docker Registry.

Dockerfile sample for REST API usage:

```
FROM python:alpine3.8
ADD contract.py /
ADD run.sh /
```

(continues on next page)

(continued from previous page)

```
RUN chmod +x run.sh
RUN apk add --no-cache --update iptables
CMD exec /bin/sh -c "trap : TERM INT; (while true; do sleep 1000; done) & wait"
```

Dockerfile sample for gRPC usage:

```
FROM python:3.9-rc-buster
RUN pip3 install grpcio-tools
ADD src/contract.py /
ADD src/protobuf/common_pb2.py /protobuf/
ADD src/protobuf/contract_pb2.py /protobuf/
ADD src/protobuf/contract_pb2_grpc.py /protobuf/
ADD run.sh /
RUN chmod +x run.sh
ENTRYPOINT ["/run.sh"]
```

The contract is created by publishing a special (CreateContractTransaction) transaction containing a link to the image in Docker Registry. To use the REST API or gRPC, please, specify the transaction version 103. After the transaction is received, the node downloads the image using the link specified in the “image” field, the image is checked and launched as a Docker container.

12.2.2 Executing a Contract

Smart contract execution is initiated by a special (CallContractTransaction) transaction containing the contract ID and call parameters. The transaction ID defines the Docker container. The container is executed unless it has been launched before. The contract launch parameters are transferred to the container. | Smart contracts change their state by updating the key-value pairs.

12.2.3 Updating Contract

Only the developer of the Docker smart contract can update this contract. The developer should keep the `contract_developer` role during the contract update and should be the `103` transaction creator. `107` transaction is using for the contract update. And it is necessary that the contract is active.

All the mining nodes download the contract image and run it for the checking after the `107` transaction includes into the block. Then the `105` transaction is issued within the `107` transaction inside it.

12.2.4 Contract Call Disabling

If necessary, the contract developer can disable calling the contract. To do this, a special (DisableContractTransaction) transaction is published specifying the Contract ID. The contract becomes unavailable after its disconnection, but you can get information about the contract from the the blockchain later.

12.2.5 Description of Transactions

The following transactions are implemented to ensure the interaction between the blockchain and the Docker Contract:

| Code | Transaction type | Purpose |
|------|------------------------------------|---|
| 103 | <i>CreateContractTransaction</i> | Initiates the Contract. Transaction is signed by a user with the role “ <i>contract_developer</i> ” |
| 104 | <i>CallContractTransaction</i> | Calls the Contract. Transaction is signed by the initiator of contract execution |
| 105 | <i>ExecutedContractTransaction</i> | Records the contract execution result in the contract state. Transaction is signed by the block generating node |
| 106 | <i>DisableContractTransaction</i> | Disables calling a contract. Transaction is signed by a user with the role “ <i>contract_developer</i> ” |
| 107 | <i>UpdateContractTransaction</i> | Updates a contract. Transaction is signed by a user with the role “ <i>contract_developer</i> ” Only the contract developer and <i>103</i> transaction issuer can update the contract |

12.2.6 Node configuration

Downloading and execution of Docker Contracts initiated by transactions with codes 103-107 are performed on nodes with enabled option `docker-engine.enable = yes` (for details see module “*Node configuration*” > “*Docker configuration*”).

12.2.7 REST API

The REST API methods description for the Docker contract usage is represented on the *API methods available to smart contract* page.

12.2.8 gRPC

The gRPC methods description for the Docker contract usage is represented on the *gRPC services available to smart contract* page.

12.2.9 Implementation examples

- *Creating a simple contract*

ANCHORING

In a private blockchain, transactions are processed by a certain number of participants known in advance. Thus, there is a threat of information spoofing, because the number of participants is quite small compared to a public blockchain where anyone can join the network. When using PoS consensus algorithm in a private blockchain, the threat of overwriting that blockchain becomes real.

The anchoring mechanism was developed to increase participant confidence in the data placed in a private blockchain. Anchoring checks the data in a blockchain for invariability, which is achieved by publishing data from a private blockchain to a public one, where data spoofing is unlikely due to the larger number of participants and blocks. Published data represents a signature and a height of blocks in a private network. This connectivity between two or more networks increases their resistance, because any attempt to forge or alter data using a [long-range attack](#) would require attacking all connected networks.

13.1 How does anchoring work in the Waves Enterprise blockchain

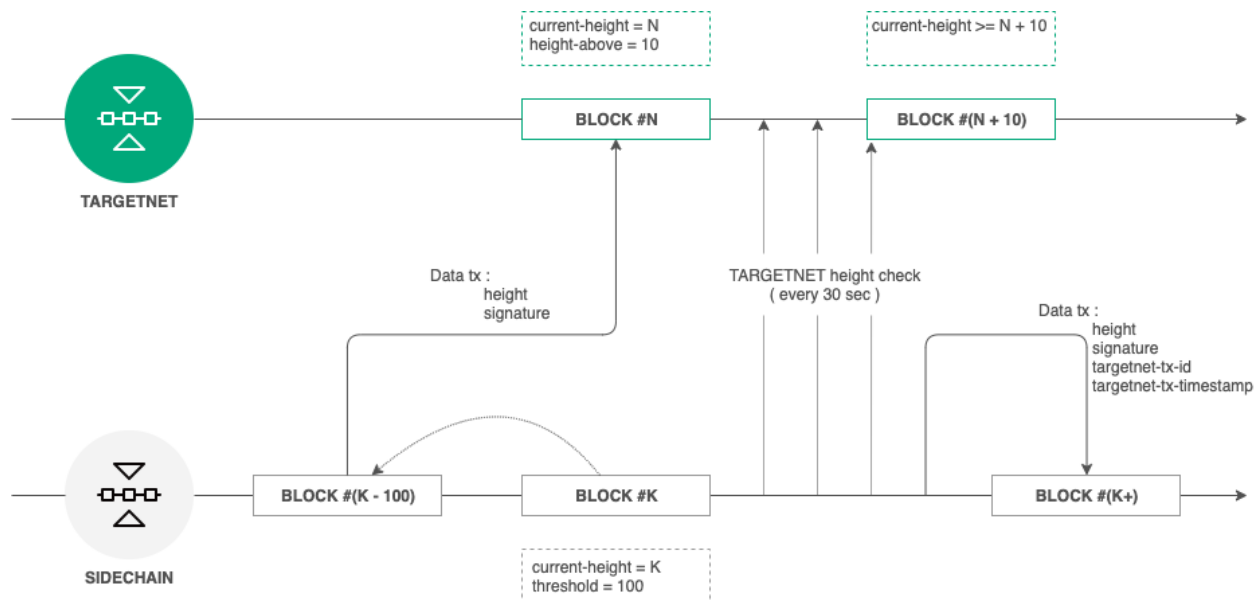


Fig. 1: Targetnet anchoring scheme

Anchoring process is shown below:

1. *Anchoring configurations* are set in the configuration file of the private blockchain node. Users should use recommended values for configurations to avoid anchoring malfunctioning.

2. Each `height-range` is an anchoring transaction that contains block data at `current-height - threshold` and is broadcasted to the Targetnet by the anchoring node. The *Data Transaction* with a `key-value` list is used as *an anchoring transaction*. The node then requests height of the broadcasted transaction.
3. The node then checks the Targetnet height each 30 seconds until its height reaches **the height of the created transaction + height-above**.
4. When the required Targetnet height is reached and the presence of previously created data transactions are confirmed, another anchoring data transaction is created in the private blockchain.

13.2 Transaction structure for anchoring

Targetnet transaction consists of the following fields:

- `height` - the height of the chosen block from the private blockchain.
- `signature` - the signature of the chosen block from the private blockchain.

The private blockchain transaction consists of the following fields:

- `height` - the height of the chosen block from the private blockchain.
- `signature` - the signature of the chosen block from the private blockchain.
- `targetnet-tx-id` - the Targetnet anchoring transaction ID.
- `targetnet-tx-timestamp` - the timestamp of the Targetnet anchoring transaction.

13.3 Errors during the anchoring

Errors can occur at any step during anchoring. In case of any error in the private blockchain the *Data Transaction* containing the error code and the description is always published. The error transaction includes the following data:

- `height` - the height of the chosen block from the private blockchain.
- `signature` - the signature of the chosen block from the private blockchain.
- `error-code` - the error code.
- `error-message` - the error message.

Table 1: Error types

| Code | Message | Possible cause |
|------|---|---|
| 0 | Unknown error | An unknown error occurred during the send of the transaction to the Targetnet |
| 1 | Fail to create data transaction for Targetnet | Creating of the transaction to be sent to the Targetnet failed |
| 2 | Fail send transaction to Targetnet | The transaction publication to the Targetnet failed (it could be a JSON request error) |
| 3 | Invalid http status of response from Targetnet transaction broadcast | The Targetnet has returned an HTTP code other than 200 after the transaction publication |
| 4 | Fail to parse http body of response from Targetnet transaction broadcast | The Targetnet has returned an unknown JSON after the transaction publication |
| 5 | Targetnet return transaction with id='\$TargetnetTxId' but it differ from transaction that we sent id='\$sentTxId' | The Targetnet has returned mismatched ID after the transaction publication |
| 6 | Targetnet didn't respond on transaction info request | The Targetnet has not responded to the request about the transaction info |
| 7 | Fail to get current height in Targetnet | Failed to get current Targetnet height |
| 8 | Anchoring transaction in Targetnet disappeared after height rise enough | The anchoring transaction has disappeared from the Targetnet after its height evened height-above value |
| 9 | Fail to create sidechain anchoring transaction | Fail to public the anchoring transaction in the private blockchain |
| 10 | Anchored transaction in sidechain was changed during Targetnet height arise await, looks like a rollback has happened | Anchored transaction in sidechain was changed during Targetnet height arise await, looks like a rollback has happened |

INTEGRATION SERVICES

14.1 Authorization service

The authorization service is an external service that provides authorization for all components of the blockchain network. This service is built using the [OAuth 2.0](#) authorization protocol. OAuth 2.0 is an open framework for realization of the authorization mechanism, allowing third parties limited access to protected resources without transferring credentials to the third party. The data flow scheme between participants sharing information using OAuth 2.0 is presented below.

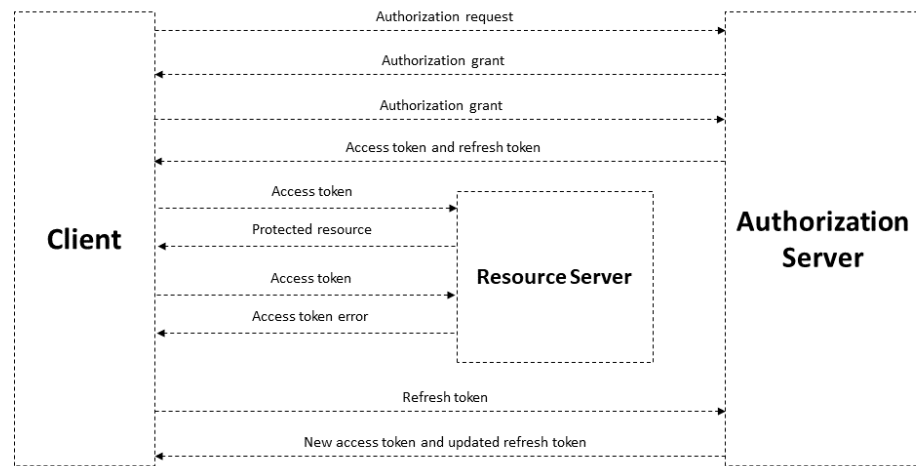


Fig. 1: Basic authorization scheme based on OAuth 2.0 protocol

A [JSON Web Token](#) is used to authorize each request from the client to the server and has a limited lifetime. The client can receive two types of tokens: access and refresh. The access token is used to authorize requests for access to protected resources and to store additional information about the user. The refresh token is used to obtain a new access token and to refresh the refresh token.

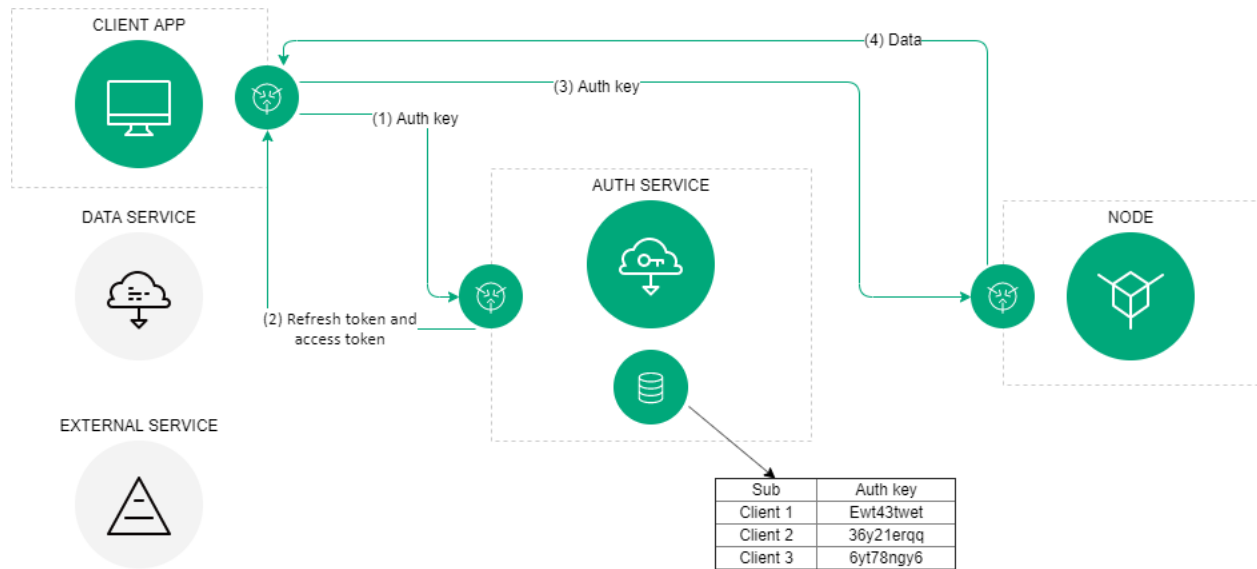


Fig. 2: The authorization scheme of the Waves Enterprise blockchain platform

In general, the authorization scheme includes the following operations:

1. The client (which could be any blockchain network component like the web client, data service, or an external application) provides its authentication data to the authorization service once.
2. If the initial authentication procedure is successful, the authorization service stores the client's authentication data in the database, generates and sends signed access, and refresh tokens to the client. Tokens include the lifetime info and basic customer data, such as an ID and a role. Client authentication data is stored in the authorization service configuration file. The client checks the lifetime of the access token each time before sending a request to a third-party service. In case the token is expired, the client refers to the authorization service to obtain a new access token. The refresh token is used for requests to the authorization service.
3. The client sends a request to receive data from a third-party service using the current access token.
4. The external application checks the lifetime of the access token and its integrity, then compares the previously obtained public key of the authorization service with the key contained in the signature of the access token. If the token is successfully verified, the service provides the requested data to the client.

14.2 Data preparation service

This service aggregates data from a blockchain into a relational database and provides an API to access that data. Service features are designed to meet the needs of the Waves Enterprise client. Specifying parameters are available for requests.

Deploy your client and node using the delivery set for service usage. Currently, access to the Data Preparation Service API is limited in the public network. The data service REST API is represented in the *Data service REST API* service.

SYSTEM REQUIREMENTS

System and hardware requirements are given below.

| Optional | vCPU | RAM | SSD | JVM Operation Mode |
|--------------------------|------|-------|--------|---------------------|
| Minimum requirements | 2+ | 2Gb | 50Gb | java -Xmx2048M -jar |
| Recommended requirements | 2+ | 4+ Gb | 50+ Gb | java -Xmx4096M -jar |

Hint: “Xmx” - flag defining maximum size of memory available for JVM.

Waves Enterprise platform environment requirements

- JRE 1.8 (64-bit) or OpenJDK 12.0.1
- Docker CE
- Docker-compose

INSTALLING AND RUNNING THE PLATFORM

Currently we support Unix-like systems (for example, popular Linux distributives and MacOS). However Waves Enterprise platform can be run under the Windows natively in experimental mode. Also you can you Unix virtual machines and the Docker environment for the installation and running the platform under the Windows.

Installation of the platform in the base delivery version assumes that [Docker Engine](#) and [Docker Compose](#) are installed in the deployment environment.

Depending on the purpose of the installation, you will need the following files:

1. `docker-compose.yml` – the configuration file used by Docker Compose to run applications in containers.
2. `generators-X.X.X.jar` - an auxiliary utility used in the Waves Enterprise platform to create key pairs, API keys, sign block genesis and other operations.

`docker-compose.yml` and `generators-X.X.X.jar` you can download by clicking on the [link](#).

3. Configuration files for `generators-X.X.X.jar` utility:
 - `accounts.conf` - he configuration file for the accounts creation;
 - `api-key-hash.conf` – the configuration file for the `api-key-hash` and `privacy-api-key-hash` values creation when you choose the `api-key` string hash authorization.
4. `node.conf` – the main node configuration file defining the operational principals and an option list. Below are some examples of node configuration files:
 - `mainnet.conf` - to connect to the Mainnet network;
 - `partnetnet.conf` - to connect to the Partnetnet network.

Examples of configuration files for the utility `generators-X.X.X.jar` and `node.conf` you can download from the [Waves Enterprise platform official page on GitHub](#).

Detailed information about configuration files can be found in *Data preparation service* module.

5. `node.license` - node license, not obligatory up to 30,000 blocks height.

You can find out about how to get `node.license` in the following *module*.

| Purpose of installation | <code>docker-compose.yml</code> | <code>generators-X.X.X.jar</code> | <code>node.conf</code> | <code>node.license</code> |
|--|---------------------------------|-----------------------------------|------------------------|---------------------------|
| Checking platform features | Required | It's not required | It's not required | It's not required |
| Connecting the node to the Mainnet network | Required | Required | Required | Required |
| Connecting the node to the Partner-net network | Required | Required | Required | Required |

16.1 Deploying the platform in Sandbox mode

The Waves Enterprise team offers a fully automated deployment mode to familiarize yourself with platform capabilities. In this mode, a blockchain network of three nodes will be installed as well as additional components - *authorization service*, *data preparation service* and *corporate client*. All key pairs used to sign transactions and blocks will be generated randomly.

In the trial mode you can interact with the blockchain through the client application, or REST/gRPC node interfaces: send transactions, receive data from the blockchain, set and call smart contracts, and transfer confidential data between nodes.

1. To install the platform in Sandbox mode, open the terminal and go to the directory where the file `docker-compose.yml` is located, and execute the following command:

```
docker run --rm -ti -v $(pwd):/config-manager/output wavesenterprise/config-manager:v1.2.1
```

Specify the latest version of the platform as the last three digits.

2. Wait for the results of the previous command and run the following command:

```
docker-compose up -d
```

Attention: On Linux, you may need to have root right to execute commands.

After launching the containers, the client application will be available at `http://localhost`, swagger host of the node - `http://localhost/node-0`.

To stop running nodes and services, execute the following command:

```
docker-compose down
```

16.2 Connecting a single node to the Mainnet network

Using the instructions below, you can connect the node to any existing network.

To connect the node to the Mainnet network you will need the following files: `docker-compose.yml`, `node.license`, `node.conf` and the key repository as a file `keystores.dat`.

Hint: The file `keystores.dat` is created when you generate a new member address.

1. Download the file `docker-compose.yml`.
2. Download the file `mainnet.conf`, rename it `node.conf` and edit the following options:
 - `owner-address`, `wallet.password` - the address of the new participant, on whose behalf the node will perform operations in the blockchain. The process of generating a new key pair and file `keystores.dat` using the utility `generators-X.X.X.jar` is described in section *Accounts creation*;
 - `node-name` - any name of the node;
 - `auth.api-api-key-hash`, `auth.privacy-api-key-hash` - hash from a secret phrase to access *REST API node*. The process of creating a hashed secret phrase using the utility `generators-X.X.X.jar` is described in section *Accounts creation*.

3. Create empty files: `postgres.env`, `node-0.env`, `nginx-proxy.env`, `frontend.env`, `data-service.env`, `crawler.env`, `auth-service.env`.
4. Open the file `my-node/env/node-0.env` and copy the text below to it:

```
LOG_LEVEL=DEBUG
WE_NODE_OWNER_PASSWORD_EMPTY=false
WE_NODE_OWNER_PASSWORD= /FILL
JAVA_OPTS=-Dwe.check-resources=false
```

5. In the field `WE_NODE_OWNER_PASSWORD` instead of `/FILL` enter the password from the key pair created when generating the address of a new participant by the utility `generators-X.X.X.Jar`.
6. Place the downloaded and previously created files according to the structure below:

```
my-node                                (directory with any name)
|- configs                             (directory)
|  |- nodes                            (directory)
|     |- node-0                        (directory)
|         |- node.conf                 (file)
|         |- keystores.dat             (file)
|         |- node.license              (file, optional)
|- env                                  (directory)
|  |- postgres.env                    (file)
|  |- node-0.env                      (file)
|  |- nginx-proxy.env                 (file)
|  |- frontend.env                    (file)
|  |- data-service.env                (file)
|  |- crawler.env                     (file)
|  |- auth-service.env                (file)
|- docker-compose.yml                  (file)
```

7. Run the command to start the node:

```
docker-compose up -d node-0
```

After the container is launched node REST API will be available at `http://localhost/node-0`.

Attention: If there are errors, make sure that no other competing containers or programs are running. To display a list of running containers and their status, type `docker ps -a`. To stop the selected container, enter `docker stop [myContainer]`. To stop all containers, you can enter `docker stop $(docker ps -a -q)`. The command `docker rm [myContainer]` will delete the selected one, `docker rm $(docker ps -a -q)` will delete all containers.

To stop running nodes and services, execute the following command:

```
docker-compose down
```


MANUAL NODE CONFIGURATION

The node configuration includes the following steps:

17.1 Preparation of configuration files

These following configuration files are used for the configuration:

- `accounts.conf` – the configuration file for the accounts creation.
- `api-key-hash.conf` – the configuration file for the `api-key-hash` and `privacy-api-key-hash` values creation when you choose the `api-key` string hash authorization.
- `node.conf` – the main node configuration file defining the operational principals and an option list.

17.1.1 `accounts.conf` configuration file for the accounts creation

When specifying a path, use the “forward slash” - / as a delimiting character for directory hierarchy levels. During Linux using the value `wallet` must match the directory structure of the operating system, for example `/home/contract/we/keystore.dat`. During node setting it is prohibited to use cyrillic symbols for specifying paths to the working directory, `keystore`, etc.

```
// accounts.conf listing

accounts-generator {
  waves-crypto = yes
  chain-id = V
  amount = 1
  wallet = "${user.home}"/node/keystore.dat"
  wallet-password = "some string as password"
  reload-node-wallet {
    enabled = false
    url = "http://localhost:6862/utils/reload-wallet"
  }
}
```

The description of the configuration file parameters is represented below.

- `waves-crypto` – the choice of a cryptographic algorithm (“yes” - use *cryptography Waves*, “no” - use *GOST-cryptography*);
- `chain-id` – an identifying byte of the network, the value will be necessary further on for entry in parameter `address-scheme-character` of the node configuration file;
- `amount` – a number of generated key pairs;

- `wallet` – the path to the key storage directory on the node, the value will be required further on for entry in parameter `wallet > file` of the node configuration file. For the Waves cryptography, the path to file `keystore.dat` is specified (example, `${user.home}/nodeName/keystore.dat`), for the GOST-cryptography - the path to directory (`${user.home}/nodeName/keystore/`);
- `wallet-password` – a password for access to closed node keys, the value will be necessary further for entry into the parameter `wallet > password` of the node configuration file;
- `reload-node-wallet` – an option to update the node keyStore without restarting the application, by default it is turned off (`false`). `url` parameter specifies the path to the `/utils/reload-wallet` method of the REST API node.

17.1.2 api-key-hash.conf configuration file

`api-key-hash.conf` configuration file is intended only for the `api-key-hash` and `privacy-api-key-hash` values creation when you choose the `api-key` string authorization.

```
// api-key-hash.conf listing

apikeyhash-generator {
  waves-crypto = no
  api-key = "some string for api-key"
}
```

Parameters description

- `waves-crypto` – the choice of a cryptographic algorithm (“yes” - use *cryptography Waves*, “no” - use *GOST-cryptography*);
- `api-key` – the key you need to come up with. The value of this key will need to be specified in requests to REST API node (for more details see page *REST API*).

17.1.3 node.conf node configuration file

If you are planning to connect the new node to the existing network, it will be more easy to request full configuration file from your network administrator or from any of net participants. When you are creating the configuration file from a scratch or connecting to the “Waves Enterprise Mainnet”, you can get the example of the file from our [GitHub](#) page. You can read on the *Changes in the node configuration file* page about changes in the node configuration file.

Warning: If your node’s version is 1.0 and higher you need to specify the following parameter in the `node` section of the node configuration file:

```
"features": {
  "supported": [100]
}
```

This option becomes active when the total quantity of blocks from `feature-check-blocks-period` = 15000 and `blocks-for-feature-activation` = 10000 parameters is achieved (25 000 of blocks). These parameters are stored in the `blockchain` section and can not be changed during Mainnet or Partnet connection. Nodes will not be able to connect to the network without activation of this option.

The example of the node configuration file is represented below. This file does not include such options like *anchoring*, *Docker* smart contracts and private data access *groups*. Also there are `api-key` authorization and Waves cryptography. You can find the fields description *here*.

Note: If you want to use additional options, set the `enable` field of the selected option to `yes` or `true` and configure the option section according to the description of its setting.

Warning: Please, fill **ONLY** the fields with the `/FILL/` word inside as a value.

```

node {
  # Type of cryptography
  waves-crypto = yes

  # Node owner address
  owner-address = " /FILL/ "

  # NTP settings
  ntp {
    server = "pool.ntp.org"

    # Maximum time without synchronization. Required for PoA consensus.
    fatal-timeout = 5 minutes
  }

  # Node "home" and data directories to store the state
  directory = "/node"
  data-directory = "/node/data"

  wallet {
    # Path to keystore.
    file = "/node/keystore.dat"

    # Access password
    password = " /FILL/ "
  }

  # Blockchain settings
  blockchain {
    type = CUSTOM
    fees.enabled = false
    consensus {
      type = "poa"
      round-duration = "17s"
      sync-duration = "3s"
      ban-duration-blocks = 100
      warnings-for-ban = 3
      max-bans-percentage = 40
    }
    custom {
      address-scheme-character = "E"
      functionality {
        feature-check-blocks-period = 1500
        blocks-for-feature-activation = 1000
        pre-activated-features = { 2 = 0, 3 = 0, 4 = 0, 5 = 0, 6 = 0, 7 = 0, 9 = 0, 10 = 0, 100 = 0 }
      }
    }

    # Mainnet genesis settings

```

(continues on next page)

(continued from previous page)

```
genesis {
  average-block-delay: 60s
  initial-base-target: 153722867

  # Filled by GenesisBlockGenerator
  block-timestamp: 1573472578702

  initial-balance: 1625000000000000

  # Filled by GenesisBlockGenerator
  genesis-public-key-base-58: ""

  # Filled by GenesisBlockGenerator
  signature: ""

  transactions = [
    # Initial token distribution:
    # - recipient: target's blockchain address (base58 string)
    # - amount: amount of tokens, multiplied by 10e8 (integer)
    #
    # Example: { recipient: "3HQSr3VFCiE6JcWwV1yX8attYbAGKTLV3Gz", amount:
↪3000000000000000 }
    #
    # Note:
    # Sum of amounts must be equal to initial-balance above.
    #
    { recipient: " /FILL/ ", amount: 1000000000000000 },
    { recipient: " /FILL/ ", amount: 1500000000000000 },
    { recipient: " /FILL/ ", amount: 5000000000000000 },
  ]

  network-participants = [
    # Initial participants and role distribution
    # - public-key: participant's base58 encoded public key;
    # - roles: list of roles to be granted;
    #
    # Example: {public-key: "EPxkVA9iQejsjQikovyakkY8iHnbXsR3wjkgE7ZW1It", roles:
↪[permissioner, miner, connection_manager, contract_developer, issuer]}
    #
    # Note:
    # There has to be at least one miner, one permissioner and one connection_manager for
↪the network to start correctly.
    # Participants are granted access to the network via GenesisRegisterNodeTransaction.
    # Role list could be empty, then given public-key will only be granted access to the
↪network.
    #
    { public-key: " /FILL/ ", roles: [permissioner, miner, connection_manager, contract_
↪developer, issuer]},
    { public-key: " /FILL/ ", roles: [miner]},
    { public-key: " /FILL/ ", roles: []},
  ]
}
}

# Application logging level. Could be DEBUG | INFO | WARN | ERROR. Default value is INFO.
logging-level = DEBUG
```

(continues on next page)

(continued from previous page)

```

# P2P Network settings
network {
  # Network address
  bind-address = "0.0.0.0"
  # Port number
  port = 6864

  # Peers network addresses and ports
  # Example: known-peers = ["node-1.com:6864", "node-2.com:6864"]
  known-peers = [ /FILL/ ]

  # Node name to send during handshake. Comment this string out to set random node name.
  # Example: node-name = "your-we-node-name"
  node-name = " /FILL/ "

  # How long the information about peer stays in database after the last communication with it
  peers-data-residence-time = 2h

  # String with IP address and port to send as external address during handshake. Could be set
  ↪ automatically if uPnP is enabled.
  # Example: declared-address = "your-node-address.com:6864"
  declared-address = "0.0.0.0:6864"
}

# New blocks generator settings
miner {
  enable = yes
  # Important: use quorum = 0 only for testing purposes, while running a single-node network;
  # In other cases always set quorum > 0
  quorum = 0
  interval-after-last-block-then-generation-is-allowed = 10d
  micro-block-interval = 5s
  min-micro-block-age = 3s
  max-transactions-in-micro-block = 500
  minimal-block-generation-offset = 200ms
}

# Nodes REST API settings
rest-api {
  # Enable/disable REST API
  enable = yes

  # Network address to bind to
  bind-address = "0.0.0.0"

  # Port to listen to REST API requests
  port = 6862

  auth {
    type: "api-key"

    # Hash of API key string
    # You can obtain hashes by running ApiKeyHash generator
    api-key-hash: " /FILL/ "
  }
}
    
```

(continues on next page)

(continued from previous page)

```

    # Hash of API key string for PrivacyApi routes
    privacy-api-key-hash: " /FILL/ "
  }
}

#Settings for Privacy Data Exchange
privacy {
  storage {
    enabled = false
    # url = "jdbc:postgresql://postgres:5432/node-1?user=postgres&password=wenterprise"
    # driver = "org.postgresql.Driver"
    # profile = "slick.jdbc.PostgresProfile$"

    # user = "postgres@postgres&password=wenterprise"
    # password = "wenterprise"

    # connectionPool = HikariCP
    # connectionTimeout = 5000
    # connectionTestQuery = "SELECT 1"
    # queueSize = 10000
    # numThreads = 20
    # schema = "public"
    # migration-dir = "db/migration"
  }
}

# Docker smart contracts settings
docker-engine {
  # Docker smart contracts enabled flag
  enable = no

  # Basic auth credentials for docker host
  #docker-auth {
  #  username = "some user"
  #  password = "some password"
  #}

  # Optional connection string to docker host
  docker-host = "unix:///var/run/docker.sock"

  # Optional string to node REST API if we use remote docker host
  # node-rest-api = "node-0"

  # gRPC server settings for docker contracts with the gRPC API
  grpc-server {
    # gRPC server port
    port = 6865
    # Optional node host
    # host = "192.168.65.2"
  }
}

# Execution settings
execution-limits {
  # Contract execution timeout
  timeout = 10s
}

```

(continues on next page)

(continued from previous page)

```

# Memory limit in Megabytes
memory = 512
# Memory swap value in Megabytes (see https://docs.docker.com/config/containers/resource_
↪constraints/)
memory-swap = 0
}

# Reuse once created container on subsequent executions
reuse-containers = yes

# Remove container with contract after specified duration passed
remove-container-after = 10m

# Allows net access for all contracts
allow-net-access = yes

# Remote registries auth information
remote-registries = []

# Check registry auth on node startup
check-registry-auth-on-startup = yes

# Contract execution messages cache settings
contract-execution-messages-cache {
# Time to expire for messages in cache
expire-after = 60m
# Max number of messages in buffer. When the limit is reached, the node processes all messages
↪in batch
max-buffer-size = 10
# Max time for buffer. When time is out, the node processes all messages in batch
max-buffer-time = 100ms
}
}
}

```

17.2 Changes in the node configuration file

This section provides information to help you identify changes in the configuration file depending on the node version.

Warning: If you are updating a node version, you must also update the node configuration file. The node will not run without updating the configuration file!

17.2.1 Changes in the node configuration file of the 1.2.0 version

docker-engine section

In the section `docker-engine` added parameter `grpc-server`, responsible for setting up gRPC server to work docker contracts with gRPC API:

```
grpc-server {
  # gRPC server port
  port = 6865
  # Optional node host
  # host = "192.168.65.2"
}
```

17.2.2 Changes in the node configuration file for earlier versions

Node version 1.1.2

Node version 1.1.0

17.3 Description of the node configuration file parameters and sections

Several types of values are used for parameters in the configuration file:

- Integer data which used to specify the exact number of elements. It can be the number of transactions, blocks or connections.
- Integer data including measuring units to specify the time periods or memory volume. You typically specify the time periods in days, hours, or seconds, or the cache memory volume, for example, `leveldb-cache-size = 256M` or `connection-timeout = 30s`.
- String which used to specify the addresses, directory paths, passwords and so on. The directory path is specifying in the acceptable format of your current OS and the value is quoted.
- Array for the list of values like addresses or public keys. The value is specified in square brackets separated by commas.
- Boolean `no` or `yes` which used for option activation.

An example of the node configuration file is represented on the *configuration files prepare* page. It includes the following sections:

- *node* - general section, which includes all sections of blockchain settings.
- *synchronization.transaction-broadcaster* - synchronization parameters settings for sending unconfirmed transactions to the blockchain.
- *ntp* - NTP server parameters settings.
- *blockchain* - common blockchain settings.
- *features* - network settings.
- *network* - network settings.
- *wallet* - settings of the private keys access.
- *miner* - mining settings.

- *rest-api* - REST API settings.
- *privacy* - confidential information access groups settings.
- *docker-engine* - Docker smart contracts settings.

17.3.1 node section

Additional section parameters:

- *waves-crypto* - *cryptography* type in the blockchain. Possible values: **yes** - Waves cryptography, **no** - GOST cryptography.
- *directory* - the main directory for the storage of the node software.
- *data-directory* - the main directory for the storage of the node software.
- *logging-level* - logging level. Possible values: **DEBUG**, **INFO**, **WARN**, **ERROR**, default value is **INFO**.
- *owner-address* - the node address, the future owner of the configuration file.

17.3.2 synchronization.transaction-broadcaster section

- *max-batch-size* and *max-batch-time* – technical parameters that allow you to adjust the speed of reducing the transaction queue.
- *min-broadcast-count* – a minimum number of connections that can be used to send each transaction to the blockchain. The value should not exceed the number of nodes in the network minus one (the sender should not be taken into account).
- *retry-delay* – an interval for resending a transaction if the number of current connections was not enough, or errors occurred during sending.

17.3.3 ntp section

- *server* - an NTP server addresses list. The recommended value is [`<0.pool.ntp.org>`, `<1.pool.ntp.org>`, ... `<10.pool.ntp.org>`].
- *request-timeout* - the timeout of the one request to an NTP server. The recommended value is 10 seconds.
- *expiration-timeout* - the timeout of the NTP server requests synchronization. The recommended value is 1 minute.
- *fatal-timeout* - the timeout of the connection to an NTP server. The recommended value is 1 minute.

17.3.4 blockchain section

- *type* - the blockchain type. Possible values are **MAINNET** or **CUSTOM**. The **MAINNET** value allows you to use the genesis block, consensus and Mainnet settings. When you select **MAINNET** in the configuration file of the node which connects to the Mainnet network, you do not need to specify the parameters of **custom**, **genesis** and **consensus** blocks.
- *consensus.type* - *consensus* type. Possible values are **pos** or **poa**. You can read more *here* about consensus settings.

fees unit

- **enabled** - the option of using fees for the *transaction* release. Possible values are **false** or **true**.

custom **unit**

- **address-scheme-character** - the address feature character which is used to prevent mixing up addresses from different networks. For the “Waves Enterprise Mainnet” - **V** and for the “Waves Enterprise Partnernet” - **P**. You can use any letter you like for the sidechain or test versions of the Waves Enterprise blockchain platform. Nodes must have the same network byte on the same blockchain network.
- **functionality** - main blockchain settings.
- **genesis** - genesis block settings.

functionality **unit**

- **feature-check-blocks-period** - the blocks period for feature checking and activation.
- **blocks-for-feature-activation** - the number of blocks required to accept feature.
- **pre-activated-features** - a set of blockchain options.

genesis **unit**

- **average-block-delay** - an average delay between the blocks creation. This parameter is used only for the *PoS* consensus.
- **initial-base-target** - an initial base number for the managing the mining process. This parameter is used for the *PoS* consensus . The frequency of the block creation depends on the parameter value therefore the higher the value, the more often blocks are created. Also, the value of the miner’s balance affects the use of this parameter in mining - the larger the miner’s balance, the less the value of **initial-base-target** is used. When setting a value for this parameter, it is recommended to take into account the combination of miners balances and the expected interval between blocks.
- **block-timestamp** - a time and data code. The time is specified in milliseconds and the value must consist of 13 digits. If you specify the standard value **timestamp** consisting of 10 digits, then you need to add any three digits at the end.
- **initial-balance** - an initial balance in smallest units. The parameter value affects on the mining process with the *PoS* consensus. The larger the miner’s balance, the smaller the **initial-base-target** value is used for the mining node determination for the current round.
- **genesis-public-key-base-58** - the public key hash of the genesis block, encrypted in Base58.
- **signature** - the genesis block signature, encrypted in Base58.
- **transactions** - a list of network participants with an initial balance, the creation of which will be included in the genesis block.
- **network-participants** - a list of network participants with specified roles, the creation of which will be included in the genesis block.

17.3.5 network section

- **bind-address** - the node network address.
- **port** - the port number.
- **known-peers** - a list of known nodes network addresses. This parameter should be filled in. The list of addresses is passed to the user by the network administrator before the new node is connected.
- **declared-address** - a string with IP address and port to send as external address during the handshake.

- `max-simultaneous-connections` - a maximum number of simultaneously supported connections. This parameter is limited by the number of nodes in the blockchain, i.e. the maximum number of simultaneous connections will not exceed the number of nodes in the network.
- `peers-request-interval` - an interval for requesting a list of peers. The value is specified in seconds or minutes. The recommended value is 1-2 minutes.

17.3.6 wallet section

- `file` - a path to the private keys storage.
- `password` - a password for the private keys file access.

17.3.7 miner section

- `enable` - a miner option activation.
- `quorum` - required number of connections (both incoming and outgoing) to attempt block generation. Setting this value to 0 enables offline generation. When you are specifying the value, it is necessary to consider that the own mining node is not summed with the parameter value, i.e., if it is `quorum = 2`, then you need at least 3 mining nodes in the network.
- `interval-after-last-block-then-generation-is-allowed` - enable block generation only if the last block is not older the given period of time.
- `micro-block-interval` - an interval between microblocks.
- `min-micro-block-age` - a minimal age of the microblock.
- `max-transactions-in-micro-block` - a maximum number of transaction in the microblock.
- `minimal-block-generation-offset` - a minimal time interval between blocks.

17.3.8 features section

- `supported` - a list of supported options.

17.4 Accounts creation

The user account includes an address and a key pair which consists of public and private keys. The address and public key are shown to the user during account creation on the command line. The private key is written to the `keystore.dat`.

17.4.1 Key pairs generating

Public and private keys for initial participants are creating by the generator. You can get the last version of the generator on our [GitHub](#) page. Before running the utility you need to specify the `accounts.conf` configuration file which contains parameters for keys creating. During the creation think up and enter a password, then save it for later configuration. The given password will be used at creation of a global variable `WE_NODE_OWNER_PASSWORD` further. Press `enter` key if you do not want to use this password. Use the following command to run the generator:

```
java -jar generators-x.x.x.jar AccountsGeneratorApp accounts.conf
```

17.4.2 Global variables

We recommend to use a password for the keys pair to increase security. The Waves Enterprise platform supports two ways of the password usage:

1. Enter the password manually at the each start of the node.
2. Create global variables in your OS.

If you are using the manual enter the password there is no need to create global variables. But when you are planning to use containers or any similar services to run the node then create the following global variables in the OS for your convenience:

1. `WE_NODE_OWNER_PASSWORD` - the keys pair password specified during the key pair creation.
2. `WE_NODE_OWNER_PASSWORD_EMPTY` - `true` or `false`, specify the `true` value if you do not want to use the keys pair password, in this case it is not necessary to create the `WE_NODE_OWNER_PASSWORD` variable. When you are using the password than specify the `false` value and write into the `WE_NODE_OWNER_PASSWORD` variable the keys pair password.

17.5 Signing the genesis block

Sign the genesis block using utility `generators-x.x.x.jar`. Command for signing: `java -jar generators-x.x.x.jar GenesisBlockGenerator node.conf`, where `Name.conf` is the edited in *this section* node configuration file. After signing `genesis-public-key-base-58` and `signature` fields of the configuration file will be filled with values of the public key and the proof of the genesis block.

Example:

```
genesis-public-key-base-58: "4ozcAj...penxrm"  
signature: "5QNVGF...7Bj4Pc"
```

17.6 Consensus settings

Waves Enterprise blockchain platform supports two types of consensus - *PoS* and *PoA*. The consensus settings are located in the *blockchain* section.

17.6.1 PoS configuration

The PoS consensus will be used by default if you have not specified the consensus type in the `consensus.type` field of the *blockchain* section. Here are the mining responsible parameters which are located in the `genesis` unit of the *blockchain* section:

- `average-block-delay` - an average delay between the blocks creation. The default value is 60 seconds. The value of this parameter is ignored if PoA consensus is selected.
- `initial-base-target` - an initial base number for the managing the mining process. The frequency of the block creation depends on the parameter value therefore the higher the value, the more often blocks are created. Also, the value of the miner's balance affects the use of this parameter in mining - the larger the miner's balance, the less the value of `initial-base-target` is used.
- `initial-balance` - an initial balance in smallest units. The greater the share of the miner's balance from the network initial balance, the smaller becomes the value of `initial-base-target` to determine the node miner of the current round.

We recommend to use the default parameter values specified in the configuration files examples which are represented on the [GitHub](#) page.

17.6.2 PoA settings

Please, uncomment or add the `consensus` unit of the `blockchain` section for the *PoA* consensus usage:

```
consensus {
  type = "poa"
  round-duration = "17s"
  sync-duration = "3s"
  ban-duration-blocks = 100
  warnings-for-ban = 3
  max-bans-percentage = 40
}
```

Represented in the `consensus` unit parameters are used only for the *PoA* consensus.

- `type` - the consensus type. Possible values are `pos` or `poa`. If you will specify the `pos` value, than other parameters will not be considered.
- `round-duration` - a round length of the block mining in seconds.
- `sync-duration` - a block mining synchronization period in seconds. The total time of the round is the sum of `round-duration` and `sync-duration`.
- `ban-duration-blocks` - a blocks quantity of the ban period for the mining node.
- `warnings-for-ban` - a number of rounds which is used for ban warnings for miner nodes.
- `max-bans-percentage` - a percentage of mining nodes from the total number of nodes in the network that can be placed in the ban.

Using the *PoA* consensus allows to adjust the order of blocks creation by limiting the mining function for certain nodes. The reason is to distribute evenly the network load, if any mining nodes left the network or became inactive. Mining node can get banned for the following reasons:

- if a node will miss its queue for mining;
- if a node provides an invalid block;
- if a node went offline.

Before getting into the `blacklist` the mining node receives warnings about the ban possibility during the number of rounds that is specified in the `warnings-for-ban` parameter. The mining node will be back to the mining after the `ban-duration-blocks` parameter value will end.

17.6.3 Consensus settings in the miner section

When you are configuring consensus settings, please, consider the following settings of the `miner` section:

- `micro-block-interval` - an interval between microblocks. The value is specified in seconds.
- `min-micro-block-age` - a minimal age of the microblock. The value is specified in seconds and should not be more than the `micro-block-interval` parameter value.
- `minimal-block-generation-offset` - a minimal time interval between blocks. The value is specified in milliseconds.

The values of the microblock creation parameters should not conflict with the parameters values of the `average-block-delay` for PoS and `round-duration` for PoA. The number of microblocks in a block is not limited, but depends on the transactions size in the microblock.

17.7 Docker configuration

Installation and execution of docker smart contracts configures in the `docker-engine` of the `node configuration file`.

```
# Docker smart contracts settings
docker-engine {
# Docker smart contracts enabled flag
enable = no
# Basic auth credentials for docker host
docker-auth {
  username = "some user"
  password = "some password"
}
# Optional connection string to docker host
# docker-host = "unix:///var/run/docker.sock"
# Optional string to node REST API if we use remote docker host
# node-rest-api = "https://clinton.wavesenterprise.com/node-0"
# Run for integration tests
integration-tests-mode-enable = no
# Execution settings
execution-limits {
  # gRPC contract startup timeout
  startup-timeout = 10s
  # Contract execution timeout
  timeout = 60s
  # Memory limit in Megabytes
  memory = 512
  # Memory swap value in Megabytes (see https://docs.docker.com/config/containers/resource_
↪constraints/)
  memory-swap = 0
}
# Reuse once created container on subsequent executions
reuse-containers = yes
# Remove container with contract after specified duration passed
remove-container-after = 10m
# Allows net access for all contracts
allow-net-access = no
# Remote registries auth information
remote-registries = [
{
  domain = "myregistry.com:5000"
  username = "user"
  password = "password"
}
]
# Check registry auth on node startup
check-registry-auth-on-startup = yes
# Authorization timeout for the contract
contract-auth-expires-in = 1m
# Contract execution messages cache settings
contract-execution-messages-cache {
```

(continues on next page)

(continued from previous page)

```

# Time to expire for messages in cache
expire-after = 60m
# Max number of messages in buffer. When the limit is reached, the node processes all messages
↳ in batch
max-buffer-size = 10
# Max time for buffer. When time is out, the node processes all messages in batch
max-buffer-time = 100ms
}
remove-container-on-fail = yes
grpc-server {
# host = "192.168.65.2"
port = 6865
akka-http-settings {
  akka {
    http.server.idle-timeout = infinite
    http.client.idle-timeout = infinite
    http.host-connection-pool.idle-timeout = infinite
    http.host-connection-pool.client.idle-timeout = infinite
  }
}
}
}

```

Parameters:

- `enable` - the Docker smart contracts option activation (yes/no).
- `docker-auth` - the authorization parameters with login/password section.
- `docker-host` - a Docker host URL address.
- `node-rest-api` - the REST API address if you are using the remote Docker host.
- `integration-tests-mode-enable` - the integration tests run option (yes/no).
- `execution-limits` - the Docker contracts run limits section:
 - `startup-timeout` - a timeout for creating a gRPC contract container and registering it in the node (in seconds);
 - `timeout` - a timeout for the smart contract execution;
 - `memory` - a memory limit for a smart contract in megabytes;
 - `memory-swap` - a memory swap value in megabytes.
- `reuse-containers` - reuse option for the existing Docker contract.
- `remove-container-after` - container remove option after contract execution (yes/no).
- `allow-net-access` - the option which allows network access for all smart contracts (yes/no).
- `remote-registries` - a list of remote registry repositories with credentials.
- `check-registry-auth-on-startup` - the option which checks the registry repositories authorization during the node start (yes/no).
- `contract-auth-expires-in` - a timeout for the Docker contract authorization token.
- `contract-execution-messages-cache` - the contract execution messages cache settings section. When the limit is reached, the node processes all messages in batch:
 - `expire-after` - a time period to expire for messages in cache;

- `max-buffer-size` - a maximum number of messages in buffer;
- `max-buffer-time` - a maximum time period in milliseconds of messages in buffer.
- `remove-container-on-fail` – deleting the container if an error occurred when starting it. This parameter can be useful during searching for errors when working with contracts (yes/no).

gRPC server

Section of gRPC server settings for working with smart contracts with the gRPC API.

- `host` – a node network address (optional parameter).
- `port` – a gRPC server port.
- `akka-http-settings` - a section of settings for the Akka HTTP framework used for the gRPC server.

17.8 Authorization type configuration for the REST API access

The Waves Enterprise blockchain platform supports the following two types of authorization for the node's REST API access:

- `api-key` string hash authorization;
- authorization via the authorization service.

The authorization type is specified in the REST API configuration section of the node configuration file. `api-key` string hash authorization type is a simple method of the access management to a node with a low level security. If the `api-key` hash is leaking out to the attacker, he is getting the full access to the node. When you utilize the separate authorization service with access tokens, you increase the security level of your blockchain network to the high level. You can read more information about the authorization service in the *Authorization service* section.

17.8.1 rest-api section of the node configuration file

The `rest-api` section allows to bound the node network address to the REST API interface, to choose and configure the authorization type, also to specify the limits for some REST API methods.

```
# Node's REST API settings
rest-api {
# Enable/disable REST API
enable = yes

# Network address to bind to
bind-address = "127.0.0.1"

# Port to listen to REST API requests
port = 6862

# Authorization strategy should be either 'oauth2' or 'api-key', default is 'api-key'
auth {
  type = "api-key"

# Hash of API key string
api-key-hash = "H6nsiifwYKYEx6YzYD7woP1XCn72RVvx6tC1zjjLXqsu"

# Hash of API key string for PrivacyApi routes
```

(continues on next page)

(continued from previous page)

```

privacy-api-key-hash = "H6nsiifwYKYEx6YZYD7woP1XCn72RVvx6tC1zjjLXqsu"
}
# For OAuth2:
# auth {
#   type: "oauth2"

#   # OAuth2 service public key to verify auth tokens
#   public-key: "AuthorizationServicePublicKeyInBase64"
# }

# Enable/disable CORS support
cors = yes

# Enable/disable X-API-Key from different host
api-key-different-host = no

# Max number of transactions
# returned by /transactions/address/{address}/limit/{limit}
transactions-by-address-limit = 10000
distribution-address-limit = 1000
}

```

Parameters description

- enable - REST API option activation.
- bind-address - a network address to bind the REST API interface.
- port - a port to listen to REST API requests.
- cors - enable/disable CORS support.
- transactions-by-address-limit - a maximum number of transactions returned by /transactions/address/{address}/limit/{limit} method.
- distribution-address-limit - GET /assets/{assetId}/distribution/{height}/limit/{limit}.

auth section for the api-key type

- auth-type - the authorization type, specify the api-key value - the string hash authorization.
- api-key-hash- a hash of API key string.
- privacy-api-key-hash - a hash of API key string for privacy methods.

auth section for the oauth2 type

- auth-type - the authorization type, specify the oauth2 value - the token authorization.
- public-key - a public key of the authorization service.

17.8.2 When you use the key string hash for the authorization

Specify the `api-key` value for the `auth-type` parameter. Create the `api-key-hash` for the REST API access by using the `generators-x.x.x.jar` utility. To run the utility, you need to specify the `api-key-hash.conf` file as one of the parameters, which defines the parameters of creating the `api-key-hash`. Use the following command to run the generator:

```
java -jar generators-x.x.x.jar ApiKeyHash api-key-hash.conf
```

Specify the value obtained as a result of the utility execution in the parameter `api-key-hash` in the node configuration file.

Create the `privacy-api-key-hash` by the same way as the `api-key-hash` to get the `privacy` methods access. Specify the value obtained as a result of the utility execution in the parameter `privacy-api-key-hash` in the node configuration file.

17.8.3 When you use the token authorization

Specify the `oauth2` value for the `auth-type` parameter, write the public key of the authorization service into the `public-key` parameter.

17.9 Anchoring settings

If you are using the `anchoring` option, please, configure the `anchoring` unit. `targetnet` is the blockchain network which will be used by the sidechain node to send anchoring transactions.

```
anchoring {
  enable = yes
  height-range = 50
  height-above = 10
  threshold = 1

  targetnet-authorization {
    type = "oauth2" # "api-key" or "oauth2"
    authorization-token = "PawC6b86r2pNRTR5e88wvcL3gfkG87w2Lqkvk4Jph2PUG3zPLedCTjnjh2ZTw3Rf
    ↪"
    authorization-service-url = "https://washington.testnet.com/authServiceAddress/v1/auth/
    ↪token"
    token-update-interval = "60s"
    # api-key-hash = "5M7C14rf3TAaWHvU6Kqo97iscd8fJFpuFwyQ3Q6vfztS"
    # privacy-api-key-hash = "5M7C14rf3TAaWHvU6Kqo97iscd8fJFpuFwyQ3Q6vfztS"
  }

  targetnet-scheme-byte = "K"
  targetnet-node-address = "http://node.weservices.com:6862/NodeAddress"
  targetnet-node-recipient-address = "3JWveBpXS1EcDpxcoAwVNAjFfUMrxaALgZt"
  targetnet-private-key-password = ""

  wallet {
    file = "node-1_mainnet-wallet.dat"
    password = "small"
  }

  targetnet-fee = 500000
}
```

(continues on next page)

(continued from previous page)

```
sidechain-fee = 500000
}
```

Anchoring parameters

- **height-range** - the number of blocks which is used as an interval between anchoring transactions to the Targetnet.
- **height-above** - the number of blocks in the Targetnet after which the private blockchain node creates the confirming data-transaction containing data from the first data-transaction. We recommend specifying this value that does not exceed the Targetnet maximum rollback depth **max-rollback**.
- **threshold** - the number of blocks subtracted from the current height of the private blockchain. The anchoring transaction sent to the Targetnet includes the data from the block at height **current-height - threshold**. When the value is 0, the current block is anchored. We recommend specifying this value close to the private blockchain maximum rollback depth **max-rollback**.

The distance between anchoring transactions may change depending on the mining settings in the Targetnet network. The specified value **height-range** sets the approximate interval between anchoring transactions. The real time of falling anchoring transactions into the mined block of the Targetnet may exceed the time spent on the mining of the **height-range** number of blocks.

Anchoring authorization parameters

- **type** - authorization type for anchoring. **api-key** - **api-key-hash** authorization, **auth-service** - authorization by a special security token.

For authorization by **api-key-hash** necessary a current key-value as **api-key**. For authorization by a special security token you must use a **type = "auth-service"** and comment config-file structure values:

- **authorization-token** - a constant authorization token.
- **authorization-service-url** - URL address authorization service.
- **token-update-interval** - data interval for a token refresh.

Targetnet access parameters

A separate **keystore.dat** file with a key pair for the Targetnet access is generated for the node that will send the anchoring transaction to the Targetnet.

- **targetnet-scheme-byte** - the Targetnet network byte.
- **targetnet-node-address** - the full node network address including the port number in the Targetnet for the sending of anchoring transactions. The address should be specified along with the connection type (**http/https**), the port number and the **NodeAddress** parameter as in the example **http://node.weservices.com:6862/NodeAddress**.
- **targetnet-node-recipient-address** - the node address in the Targetnet for the recording of anchoring transactions signed with a key pair of this address.
- **targetnet-private-key-password** - the node private key password for the anchoring transactions signing.

The network address and the port for the Targetnet/Partnernet networks anchoring can be obtained from Waves Enterprise technical support staff. If multiple private blockchains with mutual anchoring are used, you should use the appropriate private network settings.

Parameters of key pair file for the Targetnet anchoring transactions signing, wallet unit

- **file** - a file name and a path to the key pair file for the Targetnet anchoring transactions signing. The file is located on the private network node.

- password - a password of the key pair file.

Fee parameters

- targetnet-fee - the fee for the anchoring transaction issue in the Targetnet.
- sidechain-fee - the fee for the anchoring transaction issue in the private blockchain.

17.10 Privacy data access groups configuration

When using the *privacy* methods activate the option and fill in the `storage` block with database settings for storing the private data:

```
privacy {
  storage {
    enabled = true
    url = "jdbc:postgresql://" + ${POSTGRES_ADDRESS} + ":" + ${POSTGRES_PORT} + "/" + ${POSTGRES_DB}
    driver = "org.postgresql.Driver"
    profile = "slick.jdbc.PostgresProfile$"
    user = ${POSTGRES_USER}
    password = ${POSTGRES_PASSWORD}
    connectionPool = HikariCP
    connectionTimeout = 5000
    connectionTestQuery = "SELECT 1"
    queueSize = 10000
    numThreads = 20
    schema = "public"
    migration-dir = "db/migration"
  }
}
```

Parameters description

- enabled - the option activation;
- url - the PostgreSQL DB address;
- driver - the JDBC driver name;
- profile - a profile name for the JDBC access;
- user - a user name for the DB access;
- password - a password for the DB access;
- connectionPool - a connection pool name, default is HikariCP;
- connectionTimeout - a connection timeout;
- connectionTestQuery - a query name for the connection test;
- queueSize - a requests queue size;
- numThreads - a number of parallel connections;
- schema - an interaction scheme;
- migration-dir - a path to the data migration directory.

DB PostgreSQL is using as a database for the confidential data storage. The database should be installed on the same machine with the node and should have an DB access account. You can use the [PostgreSQL tutorial](#) for download and install the database according with your operation system type.

During the installation the system will offer to create an access account. These credentials must be entered into the appropriate `user/password` parameters.

Specify the URL for the PostgreSQL connection into the `url` parameter. URL consists of:

- `POSTGRES_ADDRESS` - адрес хоста PostgreSQL;
- `POSTGRES_PORT` - a PostgreSQL host port number;
- `POSTGRES_DB` - a PostgreSQL name.

You can specify the PostgreSQL credentials with the URL in the same string. The example is represented bellow, where `user=user_privacy_node_0@we-dev` is a login, `password=7nZL7Jr41q0WUHz5qKdypA&sslmode=require` - a password with require option during the authorization.

Example

```
privacy.storage.url = "jdbc:postgresql://vostk-dev.postgres.database.azure.com:5432/  
↪privacy_node_0?user=user_privacy_node_0@we-dev&password=7nZL7Jr41q0WUHz5qKdypA&  
↪sslmode=require"
```

You can download the latest distributives and configuration files examples from the [GitHub Waves Enterprise release page](#).

OBTAINING A LICENSE

The Waves Enterprise blockchain platform is commercial and is designed primarily for use in large companies and the public sector. To use the technology, you must purchase a license for the platform. Quick and easy access to the list of licenses is provided by the licensing service.

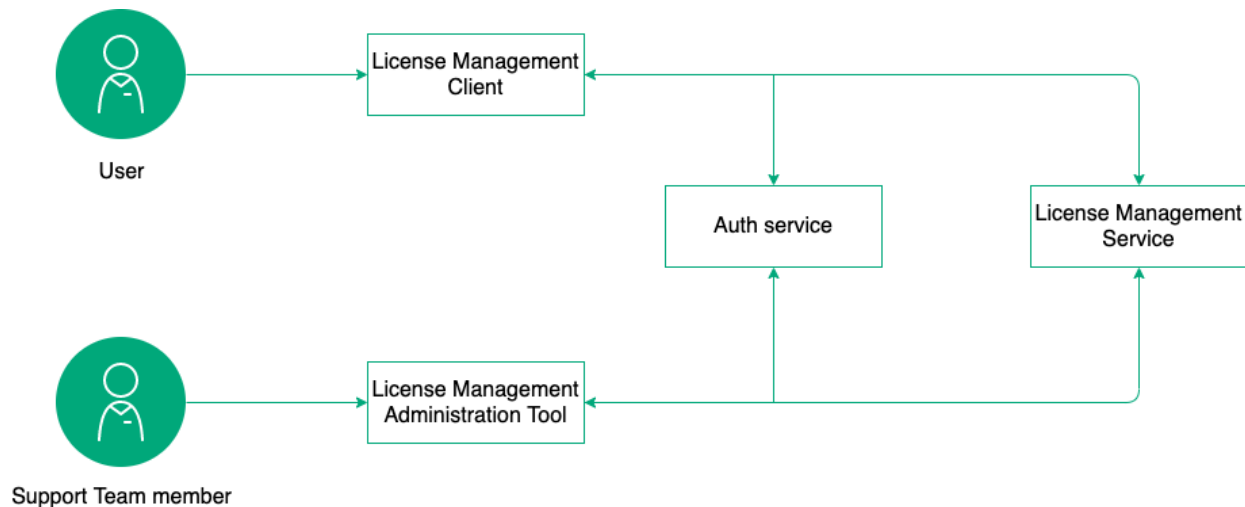


Fig. 1: Waves Enterprise blockchain platform license acquisition scheme

You do not need a product license to learn about the platform's features. The platform retains full functionality until the blockchain height of **30,000** blocks is reached, which at block round time of 30 seconds is 10 days of operation without restrictions.

Waves Enterprise blockchain platform users are offered the following license types:

- **Commercial license** - allows you to use the platform to implement commercial projects. It is issued for the period determined by the contractual relations with the partner.
- **Non-commercial license** - allows using the platform for implementing non-commercial projects. It is issued for the period determined by the contractual relations with the partner.
- **Trial license** - allows you to familiarize yourself with the platform and the technology. It is issued for the duration of the pilot project by contract, or for the time of product development and debugging.
- **The Mainnet network license** is a special license that allows you to run the node in the *Mainnet* network. To work in the network you should have at least **50,000 WEST** on your balance or in leasing. If the specified balance is reduced, restrictions on block formation and access to the node API are introduced. Sending an application for registration of new members is performed in the *Service Desk* system.

Attention: One license applies to one node!

To formalize a license request, follow these steps:

1. Go to [license management service](#) and create a new account, if it has not been created before.
2. Send your license request to [Waves Enterprise support](#). A support representative will contact you to agree on the details, create a company profile, and link the created account to it.
3. After activating the license, specify the address of your node (*node_owner_address*).
4. Send the specified license file as JSON in the request *POST /licenses/upload* to the node.
5. To view the license status, use the request *GET /licenses/status*.

MAINNET AND PARTNERNET CONNECTION

19.1 Working inside the “Waves Enterprise Mainnet”

19.1.1 Connection of the node to the “Waves Enterprise Mainnet”

Warning: The account balance must be at least **50,000 WEST** if you want to connect your node to the network “Waves Enterprise Mainnet” and do mining!

Follow these steps for the node connection to the “Waves Enterprise Mainnet”:

1. Go to the [Waves Enterprise website](#) and create an account following the web-interface hints.
2. Transfer tokens to the “Waves Enterprise Mainnet” network.
3. Transfer for leasing any number of tokens to the `3NrKDuhJUG7vSCiMMD259msBKcPRm4MvaJu` address and keep the transaction ID. Further you can withdraw tokens from the lease, because this operation is necessary to verify your ownership of this address and the balance.
4. *Deploy* a single node.
5. Perform the node *manual configuration*. An example of a node configuration file can be found on the project page on [GitHub](#). To add a node to the Mainnet network, the name of the configuration file is `mainnet-example.conf`. Please, fill only the fields with the **/FILL/** word inside as a value in the `mainnet-example.conf` node configuration file.
6. Go to the [Waves Enterprise support website](#) and perform the registration.
7. Select the type of request “Participant connection” for legal or natural person.
8. Register on the resource by filling in all the required fields of the form. If you want to mine, check the box **Please grant mining rights**.
9. Enter the transaction ID of the token lease transfer in the **Proof of WEST token ownership** field.
10. Please, wait for the connection application consideration. You can start working in the “Waves Enterprise Mainnet” after successful registration.
11. *Run* the node after obtaining permission to connect to the network “Waves Enterprise Mainnet”, public key of which you specified in the application.
12. Transfer or lease tokens to the address of the connected node for the mining and work in the network.

19.1.2 Fees in the “Waves Enterprise Mainnet”

| # | Transaction type | Fee | Description |
|-----|--|-----------|---|
| 1 | <i>Genesis transaction</i> | no fee | Initial binding of the balance to the addresses of nodes created at the start of the blockchain |
| 3 | <i>Issue Transaction</i> | 1 WEST | Tokens issue |
| 4 | <i>Transfer Transaction</i> | 0.1 WEST | Tokens transfer |
| 5 | <i>Reissue Transaction</i> | 1 WEST | Tokens reissue |
| 6 | <i>Burn Transaction</i> | 1 WEST | Tokens burn |
| 8 | <i>Lease Transaction</i> | 0.1 WEST | Tokens lease |
| 9 | <i>Lease Cancel Transaction</i> | 0.1 WEST | Cancel of the tokens lease |
| 10 | <i>Create Alias Transaction</i> | 1 WEST | Alias creation |
| 11 | <i>Mass Transfer Transaction</i> | 0.1 WEST | Mass tokens transfer. Minimum commission is specified |
| 12 | <i>Data Transaction</i> | 0.1 WEST | Transaction with the data in the key-value pairs format. The fee is always charged to the transaction author. Minimum commission is specified, the fee depends on data volume |
| 13 | <i>SetScript Transaction</i> | 0.5 WEST | Transaction which is binding a script with a RIDE contract to an account |
| 14 | <i>Sponsorship</i> | 1 WEST | Transaction which is signing a sponsorship asset |
| 15 | <i>SetAssetScript</i> | 1 WEST | Transaction which is binding a script with a RIDE contract to an asset |
| 101 | <i>Genesis Permission Transaction</i> | no fee | Assignment of the first network administrator for further distribution of rights |
| 102 | <i>Permission Transaction</i> | 0.05 WEST | Issuance/withdrawal of rights from the account |
| 103 | <i>Create-Contract Transaction</i> | 1 WEST | Docker-contract creation |
| 104 | <i>CallContract Transaction</i> | 0.1 WEST | Docker-contract call |
| 105 | <i>Executed-Contract Transaction</i> | no fee | Docker-contract execution |
| 106 | <i>Disable-Contract Transaction</i> | 0.05 WEST | Docker-contract disable |
| 107 | <i>Update-Contract Transaction</i> | 1 WEST | Docker-contract update |
| 110 | <i>GenesisRegisterNode Transaction</i> | no fee | Node registration in the genesis block with the blockchain start |
| 111 | <i>RegisterNode Transaction</i> | 0.05 WEST | A new node registration |
| 112 | <i>CreatePolicy Transaction</i> | 1 WEST | Access group creation |
| 113 | <i>UpdatePolicy Transaction</i> | 0.5 WEST | Update the access group |

19.1.3 Examples of the “Waves Enterprise Mainnet” configuration files

You can read *here* about the node configuration.

The `accounts.conf` file example

```
// accounts.conf listing

accounts-generator {
  waves-crypto = yes
  chain-id = V
  amount = 1
  wallet = ${user.home}"/node/keystore.dat"
  wallet-password = "some string as password"
  reload-node-wallet {
    enabled = false
    url = "http://localhost:6869/utills/reload-wallet"
  }
}
```

The `chain-id` parameter contains the identification network byte, for the “Waves Enterprise Mainnet” in is `V`.

The `api-key-hash` file example

```
// api-key-hash.conf listing

apikeyhash-generator {
  waves-crypto = no
  api-key = "some string"
}
```

The node configuration file example

```
node {
  # Type of cryptography
  waves-crypto = yes

  # Node owner address
  owner-address = ""

  ntp {
    fatal-timeout = "1 minute"
    server = "pool.ntp.org"
  }

  # Node "home" and data directories to store the state
  # directory = ${user.home}"/node"
  # data-directory = ${node.directory}"/data"

  # Settings for Privacy Data Exchange
  # Uncomment and fill to enable
  # privacy {
  #   storage {
  #     url = "jdbc:postgresql://"${POSTGRES_ADDRESS}":"${POSTGRES_PORT}"/"${POSTGRES_DB}"
```

(continues on next page)

(continued from previous page)

```
# driver = "org.postgresql.Driver"
# profile = "slick.jdbc.PostgresProfile$"
#
# user = ${POSTGRES_USER}
# password = ${POSTGRES_PASSWORD}
# connectionPool = HikariCP
# connectionTimeout = 5000
# connectionTestQuery = "SELECT 1"
# queueSize = 10000
# numThreads = 20
# schema = "public"
# migration-dir = "db/migration"
# }
# }

# Blockchain settings
# Mainnet blockchain settings (should match on all nodes for consistency)
blockchain {
  type = CUSTOM
  consensus.type = pos

  custom {
    address-scheme-character = "V"
    functionality {
      feature-check-blocks-period = 15000
      blocks-for-feature-activation = 10000
      pre-activated-features = {
        2 = 0
        3 = 0
        4 = 0
        5 = 0
        6 = 0
        7 = 0
        9 = 0
        10 = 0
      }
    }
  }
}

# Mainnet genesis settings
genesis {
  average-block-delay: 40s
  initial-base-target: 10000000000
  block-timestamp: 1559320391040
  initial-balance: 10000000000000000
  genesis-public-key-base-58: "D7tDsKd7DQ7H9m6fPRyk1GsNQxjAQXsETtuVgqSaaXDs"
  signature:
↪ "P7kwe3dWSWgUYL8FZu5kccPfPzoxGgLuKjTCkeapTxoDbdpo6EtcqndXoSjqKUUVS67xXfogGmaNroLgNocWcBg
↪ "
  transactions = [
    {recipient: "3Nnq14SGqeYETSd1SJ6z8LsgBRYB2ya1yRC", amount: 9999000000000000},
    {recipient: "3Nrystx7J1TN6vB1eYdHgug2nfxA7um918zy", amount: 1000000000000},
    {recipient: "3NuiCzDhmeSKL5QFa5sqZzzm9zTL4max4fZ", amount: 1500000000000},
    {recipient: "3NqaDwdEgGsqqJ1HjzndQMtk6v5KVxmRceg", amount: 2000000000000},
    {recipient: "3Nckru7f8Y8vS3PXGyy5iwoheRrKvqW5u8x", amount: 2500000000000},
    {recipient: "3NmHrYoC8S2SUosy6UJp47bBwq2Cr2X6Yq1", amount: 3000000000000}
  ]
}
```

(continues on next page)

(continued from previous page)

```

]
network-participants = [
  {public-key: "GasRtAUXMhifrUUmgU66rRZPii68tE4QxdQmtCcrV3xL", roles: [permissioner,
↪ connection_manager]},
  {public-key: "Er29kgV3yeumEAtPxBAk5fXPERYYa1wmAcPgzWw4mxHi", roles: [miner]},
  {public-key: "9eoVBycnr2m8bgu1WvYySoFJ1QqFLPAMzhnmErp291f6", roles: [miner]},
  {public-key: "9ngXJ3d1XSQgXcYbgZm2wH4QHS8CTc5mtf9M4XDoz5db", roles: [miner]},
  {public-key: "2cvrBT6jePt6mjinE1EdLLymoqRHFhWwepM3E5gRuSeL", roles: [miner]},
  {public-key: "87ZVwBTeBiKYdF2Q5hxGazwhR1pKy9VYgun8rLFMEmoW", roles: [miner]}
]
}

fees {
  genesis = 0
  genesis-permit = 0
  issue = 100000000
  transfer = 1000000
  reissue = 100000000
  burn = 5000000
  exchange = 500000
  lease = 1000000
  lease-cancel = 1000000
  create-alias = 100000000
  mass-transfer = 5000000
  data = 5000000
  set-script = 50000000
  sponsor-fee = 100000000
  set-asset-script = 100000000
  permit = 1000000
  create-contract = 100000000
  call-contract = 10000000
  executed-contract = 0
  disable-contract = 1000000
  update-contract = 100000000
  register-node = 1000000
  create-policy = 100000000
  update-policy = 50000000
  policy-data-hash = 5000000
  additional {
    mass-transfer = 1000000
    data = 1000000
  }
}
}
}

# Application logging level. Could be DEBUG | INFO | WARN | ERROR. Default value is 
↪ INFO.
logging-level = DEBUG

features {
  supported = [] # NG
}

# P2P Network settings
network {

```

(continues on next page)

(continued from previous page)

```

# Network address
bind-address = "0.0.0.0"
# Port number
port = 6864

# Peers network addresses and ports
# Example: known-peers = ["node-0.wavesenterprise.com:6864", "node-1.wavesenterprise.
↳com:6864"]
known-peers = [ ]

# Node name to send during handshake. Comment this string out to set random node name.
# node-name = "node"

# String with IP address and port to send as external address during handshake. Could↳
↳be set automatically if uPnP is enabled.
declared-address = "0.0.0.0:6864"
}

wallet {
# Path to keystore. In case of GOST cryptography keys stored in a './keystore/' folder.↳
↳In case of Waves-cryptography keys stored in a 'keystore.dat' file.
file = ${user.home}"/node/keystore.dat"
# Access password
password = ""
}

# Node's REST API settings
rest-api {
enable = yes
bind-address = "0.0.0.0"
port = 6862

# Hashed secret Api-Key to access node's REST API
api-key-hash = ""

# Api-key hash for Privacy Data Exchange REST API methods
privacy-api-key-hash = ""
}

# New blocks generator settings
miner {
enable = no
quorum = 2
interval-after-last-block-then-generation-is-allowed = 35d
micro-block-interval = 5s
min-micro-block-age = 3s
max-transactions-in-micro-block = 500
minimal-block-generation-offset = 200ms
}

# Anchoring settings
scheduler-service.enable = no

# Docker smart-contracts engine config
docker-engine {
enable = no
    
```

(continues on next page)

(continued from previous page)

```

execution-limits {
  timeout = 10s
  memory = 512
  memory-swap = 512
}
grpc-server {
  # gRPC server port
  port = 6865
  # Optional node host
  # host = "192.168.65.2"
}
}
}

```

19.2 Working inside the “Waves Enterprise Partnetnet”

19.2.1 Connection of the node to the “ Waves Enterprise Partnetnet”

Follow these steps for the node connection to the “Waves Enterprise Partnetnet”:

1. *Deploy* a single node.
2. *Create* the `accounts.conf` configuration file before the generator start.
3. Download the `current` release of the node and generator in the jar format.
4. *Generate* a key pair for the connected node using the generator. For your convenience it is recommended to create one key pair for one node, please, specify the number of nodes 1 in the `amount` field of the `accounts.conf` configuration file. Enter the node address password during the key pair creation and keep it for the following steps. Press `enter` key if you do not want to use this password.
5. Create the node configuration file using the template from the project [GitHub](#). Please, fill all the fields marked with `#FILL` string. If you want the node to be a miner specify the value `yes` of the `enable` parameter of the `miner` block and request the miner rights inside the connection application. Otherwise specify the `no` value. Also specify the PostgreSQL DB address as a value of the `url` parameter of the `privacy {storage {}}` block.
6. If you do not want to enter the password each time when node is starting, create the `WE_NODE_OWNER_PASSWORD` and `WE_NODE_OWNER_PASSWORD_EMPTY` global variables in your OS.
7. Go to the ‘Waves Enterprise support website <<https://support.wavesenterprise.com/servicedesk>>_ and perform the registration.
8. Select the type of request “Participant connection” for legal or natural person.
9. Register on the resource by filling in all the required fields of the form. If you want to mine, check the box **Please grant mining rights**.
10. Please, wait for the connection application consideration. You can start working in the “Waves Enterprise Partnetnet” after successful registration.
11. *Run* the node after getting the application approve.

19.2.2 Examples of the “Waves Enterprise Partnernet” configuration files

You can read [here](#) about the node configuration.

The accounts.conf file example

```
// accounts.conf listing

accounts-generator {
  waves-crypto = yes
  chain-id = P
  amount = 1
  wallet = ${user.home}"/node/keystore.dat"
  wallet-password = "some string as password"
  reload-node-wallet {
    enabled = false
    url = "http://localhost:6869/utills/reload-wallet"
  }
}
```

The `chain-id` parameter contains the identification network byte, for the “Waves Enterprise Partnernet” in is P. If you want to use the GOST cryptography specify the `no` value of the `waves-crypto` parameter inside all the configuration files. Also install the [CryptoPro JCP 2.0.40035](#) software before the node configuration. You can find full info about installation [here](#).

The api-key-hash file example

```
// api-key-hash.conf listing

apikeyhash-generator {
  waves-crypto = yes
  api-key = "some string"
}
```

The node configuration file example

```
node {
  waves-crypto = yes
  # Blockchain settings
  blockchain {
    type: CUSTOM
    consensus.type = PoS
    custom {
      address-scheme-character: "P"
      functionality {
        feature-check-blocks-period = 1
        blocks-for-feature-activation = 1
        pre-activated-features { 1 = 0, 2 = 0, 3 = 0, 4 = 0, 5 = 0, 6 = 0, 7 = 0, 8 = 0, 9 = 0, 10 = 0 }
        double-features-periods-after-height = 100000000
      }
    }
  }
  genesis {
    average-block-delay: 60s
  }
}
```

(continues on next page)

(continued from previous page)

```

initial-base-target: 153722867
block-timestamp: 1559260800000
initial-balance: 1625000000000000
genesis-public-key-base-58: "8RbU8qKWWxLuVk49LgeE39y83LUTVp1zHEJwMM7zKaMC"
signature:
↳ "2dKzduxL9bdWz1B9wBPnGALfowrPDSidEoGAQEoRogGuBB4sQanCr4JySXvWoAmpu1EmcU8MsCQTL3TaSMnFxG2U
↳ "
transactions = [
  { recipient: "3LWg4n6VmN6DKBSwGF1hwNaCzXdjMkQCFrn", amount: 1250000000000000 },
  { recipient: "3LPPZNhakdm9ZPiGShNvWGCshFqsQXFjUQ1", amount: 3000000000000000 },
  { recipient: "3LEpXfh7XmCRias92swo6LUJqyo9MA7SaFc", amount: 7500000000000000 }
]
network-participants = [
  {public-key: "CaFrRzAv7B3DrECR4i2Los1DwxHj4yKAEKCT3zEke9U4", roles: [permissioner,
↳miner, connection_manager]},
  {public-key: "Vxb6LQ8Qt9Afs6VJuyiMbMN5qm2pm1EEcWdoZo3WmkN", roles: [miner,
↳permissioner]},
  {public-key: "FmzyByBePwbKDjSdnYjwF9G12zGrQc7Gcr8WvQ5ybejC", roles: [miner]}
]
}
}
}
# Application logging level. Could be DEBUG | INFO | WARN | ERROR. Default value is
↳INFO.
logging-level = DEBUG
# P2P Network settings
network {
# Network address
bind-address = "0.0.0.0"
# Port number
port = 6864
known-peers = [
"node0-partnernet.wavesenterprise.com:6864",
"node1-partnernet.wavesenterprise.com:6864",
"node2-partnernet.wavesenterprise.com:6864"
]
# Node name to send during handshake. Comment this string out to set random node name.
# String with IP address and port to send as external address during handshake. Could
↳be set automatically if uPnP is enabled.
declared-address = "0.0.0.0:6864"
}
wallet {
file = "" #FILL
password = "" #FILL
}
# Privacy network settings: node owner address is used to sign handshakes
owner-address = "" #FILL

ntp {
fatal-timeout = "1 minute"
server = "pool.ntp.org"
}

# Matcher settings
matcher.enable = no
# Node's REST API settings

```

(continues on next page)

(continued from previous page)

```

rest-api {
  enable = yes
  bind-address = "0.0.0.0"
  port = 6862
  api-key-hash = "" #api-key for all api #FILL
  privacy-api-key-hash = "" #api-key for SendData api #FILL
}
# New blocks generator settings
miner {
  enable = yes
  interval-after-last-block-then-generation-is-allowed = 15d
  quorum = 1
  minimal-block-generation-offset = 200ms
}
# Anchoring
scheduler-service.enable = no

# For docker smart-contracts
docker-engine {
  enable = yes
  # Optional connection string to docker host
  # docker-host = "unix:///var/run/docker.sock"
  # Optional string to node REST API if we use remote docker host
  # node-rest-api = "https://clinton.weservices.com/node-0"
  execution-limits {
    timeout = 10s
    memory = 512
    memory-swap = 512
  }
  allow-net-access = yes
  grpc-server {
    # gRPC server port
    port = 6865
    # Optional node host
    # host = "192.168.65.2"
  }
}

privacy {
  # DB connection config
  storage {
    url = "" #FILL insert DB connection string here, example "jdbc:postgresql://db_
    ↪hostname:5432/____?user=_____&password=____"
    driver = "org.postgresql.Driver"
    profile = "slick.jdbc.PostgresProfile$"
    connectionPool = HikariCP
    connectionTimeout = 5000
    connectionTestQuery = "SELECT 1"
    queueSize = 10000
    numThreads = 10
    schema = "public"
    migration-dir = "db/migration"
  }
}
}

```


The Waves Enterprise blockchain platform provides an opportunity to interact with blockchain both in terms of receiving data (transactions, blocks, balances, etc.) and in terms of writing information to blockchain (signing and sending transactions) via RESTful API of the node. REST API allows users to interact remotely with the node using requests and responses in JSON format. HTTPS protocol is used to work with API and as an interface it is utilized the Swagger framework.

20.1 Node REST API methods

Full description of the REST API methods you can find on the [API Docs](#) page. Almost all REST API methods are closed by the *authorization*. If a method is opened, you'll see the badge .

20.1.1 Activation

Hint: The rules for generating requests to the node are given in module *How to use REST API*.

GET /activation/status

Returns the activation status of the new functionality in the node(s).

Method Response:

```
{ "height": 47041,
  "votingInterval": 1,
  "votingThreshold": 1,
  "nextCheck": 47041,
  "features": [
    { "id": 1,
      "description": "Minimum Generating Balance of 1000 WEST",
      "blockchainStatus": "ACTIVATED",
      "nodeStatus": "IMPLEMENTED",
      "activationHeight": 0 },
    { "id": 2,
      "description": "NG Protocol",
      "blockchainStatus": "ACTIVATED",
      "nodeStatus": "IMPLEMENTED",
```

(continues on next page)

(continued from previous page)

```

    "activationHeight": 0 },
  {"id": 3,
   "description": "Mass Transfer Transaction",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 },
  {"id": 4,
   "description": "Smart Accounts",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 },
  {"id": 5,
   "description": "Data Transaction",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 },
  {"id": 6,
   "description": "Burn Any Tokens",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 },
  {"id": 7,
   "description": "Fee Sponsorship",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 },
  {"id": 8,
   "description": "Fair PoS",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 },
  {"id": 9,
   "description": "Smart Assets",
   "blockchainStatus": "VOTING",
   "nodeStatus": "IMPLEMENTED",
   "supportingBlocks": 0 },
  {"id": 10,
   "description": "Smart Account Trading",
   "blockchainStatus": "ACTIVATED",
   "nodeStatus": "IMPLEMENTED",
   "activationHeight": 0 } ]
}

```

20.1.2 Addresses

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /addresses/info/{address}

Getting a public key by the address. The method returns only those public keys that are stored in the `keystore.dat` file of the node.

Method Response:

```
{
  "address": "3JFR1pmL6biTzr9oa63gJcjZ8ih429KD3aF",
  "publicKey": "EPxkVA9iQejsjQikovyxkkY8iHmbXsR3wjgkgE7ZW1Tt"
}
```

GET/addresses

Get all addresses of participants whose key pairs are stored in the node keystore.

Method Response:

```
[
  "3NBVqYXrapgJP9atQccdBP AgJPwHDKkh6A8",
  "3Mx2afTZ2KbRrLNbytyzTtXukZvqEB8SkW7"
]
```

GET/addresses/seq/{from}/{to}

Gets all addresses of participants whose key pairs are stored in node keystore in the specified range.

Method Response:

```
[
  "3NBVqYXrapgJP9atQccdBP AgJPwHDKkh6A8",
  "3Mx2afTZ2KbRrLNbytyzTtXukZvqEB8SkW7"
]
```

GET/addresses/balance/{address}

Get the balance for the address {address}.

Method Response:

```
{
  "address": "3N3keodUiS8WLEw9W4BKDNxgNdUpwSnpb3K",
  "confirmations": 0,
  "balance": 100945889661986
}
```

POST/addresses/balance/details

Get balances for the address list.

Method Query:

```
{
  "addresses": [
    "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ", "3N11u447zghwj9MemYkrkt9v9xDaMwTY9nG"
  ]
}
```

GET/addresses/effectivebalance/{address}/{confirmations}

Get the balance for the address {address} after a number of confirmations \geq value {confirmations}. Returns the total balance of the participant, including assets transferred to the participant for the leasing.

Method Response:

```
{
  "address": "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ",
  "confirmations": 1,
  "balance": 0
}
```

GET /addresses/effectiveBalance/{address}

Get the effective balance of the specified address.

Method Response

```
{
  "address": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
  "confirmations": 0,
  "balance": 1240001592820000
}
```

GET/addresses/balance/details/{address}

Returns detailed information about balance of address {address}.

Method Query:

```
{
  "addresses": [
    "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ"
  ]
}
```

Method Response:

```
[
  {
    "address": "3N65yEf31ojBZUvpu4LCo7n8D73juFtheUJ",
```

(continues on next page)

(continued from previous page)

```

    "regular": 0,
    "generating": 0,
    "available": 0,
    "effective": 0
  }
]

```

Response Options

- Regular - total balance of participant, including assets transferred for leasing
- Available - total balance of participant, except for assets transferred for leasing
- Effective — total balance of participant, including assets transferred to participant for leasing (Available + assets transferred to you for leasing)
- Generating - minimum balance of participant, including assets transferred to participant for leasing, for the last 1000 blocks (used for mining)

GET/addresses/scriptInfo/{address}

Get information about the script installed on the address {address}.

Method Response:

```

{
  "address": "3N3keodUiS8WLEw9W4BKDNxgNdUpwSnpb3K",
  "script":
  ↪ "3rbFDtbPwAvSp2vBvqGfGR9nRS1nBVnfuSCN3HxSZ7fVRpt3tuFG5JSmyTmvHPxyf34So cMRkRKFgzTtXXnnv7upRHXJzZrLSQo8tUW6yMtEiZ
  ↪",
  "scriptText": "ScriptV1 (BLOCK(LET(x,CONST_LONG(1)),FUNCTION_CALL(FunctionHeader(==,List(LONG,
  ↪LONG)),List(FUNCTION_CALL(FunctionHeader(+,List(LONG, LONG)),List(REF(x, LONG), CONST_LONG(1)),
  ↪LONG), CONST_LONG(2)),BOOLEAN),BOOLEAN))",
  "complexity": 11,
  "extraFee": 10001
}

```

Response Options

- “address” - address in Base58 format
- “script” - Base64 representation of the script
- “scriptText” - source code of the script
- “complexity” - complexity of the script
- “extraFee” - fee for outgoing transactions set by the script

POST/addresses/sign/{address}

Returns the message encoded in BASE58 format signed by address private key {address}, stored in node keystore. The message is first signed and then converted.

Method Query:

```
{
  "message": "mytext"
}
```

Method Response:

```
{
  "message": "wWshKhJj",
  "publicKey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "signature":
  ↪ "62PFG855ThsEHUZ4N8VE8kMyHCK9GWnvtTZ3hq6JHYv12BhP1eRjegA6nSa3DAoTTMammhamadvizDUYZAZtKY9S"
}
```

POST/addresses/verify/{address}

Validates signature of a message executed by address {address}, including the one created through POST method/addresses/sign/{address}.

Method Query:

```
{
  "message": "wWshKhJj",
  "publickey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "signature":
  ↪ "5kwwE9sDZzss0NaoBSJnb8RLqfYGt1NDGbTWWXUeX8b9amRRJN3hr5fhs9vHBq6VES5ng4hqbcUoDEsoQNauRRts"
}
```

Method Response:

```
{
  "valid": true
}
```

POST/addresses/signtext/{address}

Returns a message signed by address private key {address} stored in the node keystore.

Method Query:

```
{
  "message": "mytext"
}
```

Method Response:

```
{
  "message": "message",
  "publicKey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
```

(continues on next page)

(continued from previous page)

```

"signature":
↪ "5kVZfWfFmoYn38cJfNhdct5WCyksMgQ7kjqwHK7Zjnrzs9QYRwo6HuJoGc8WRMozdYcAVJvojJnPPArqPvu2uc3u"
}
    
```

POST /addresses/verifytext/{address}

Validates signature of a message executed by address {address}, including the one created through the POST method /addresses/signtext/{address}.

Method Query:

```

{
  "message": "message",
  "publicKey": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "signature":
  ↪ "5kVZfWfFmoYn38cJfNhdct5WCyksMgQ7kjqwHK7Zjnrzs9QYRwo6HuJoGc8WRMozdYcAVJvojJnPPArqPvu2uc3u"
}
    
```

Method Response:

```

{
  "valid": true
}
    
```

GET /addresses/validate/{addressOrAlias}

Validates correctness of specified address or its alias {addressOrAlias} in a network blockchain of operating node.

Method Response:

```

{
  addressOrAlias: "3HSVTtjim3FmV21HWQ1LurMhFzjut7Aa1Ac",
  valid: true
}
    
```

POST /addresses/validateMany

Checks the validity of addresses or aliases.

Method Query:

```

{
  addressesOrAliases: [
    "3HSVTtjim3FmV21HWQ1LurMhFzjut7Aa1Ac",
    "alias:T:asdfghjk",
    "alias:T:1nvAlidA11ass99911%~&$$$$ "
  ]
}
    
```

Method Response:

```
{
  validations: [
    {
      addressOrAlias: "3HSVTtjim3FmV21HWQ1LurMhFzjut7Aa1Ac",
      valid: true
    },
    {
      addressOrAlias: "alias:T:asdfghjk",
      valid: true
    },
    {
      addressOrAlias: "alias:T:invAlidAl1ass99911%~&$$$ ",
      valid: false,
      reason: "GenericError(Alias should contain only following characters: -.0123456789@_
↵abcdefghijklmnopqrstuvwxyz)"
    }
  ]
}
```

GET /addresses/publicKey/{publicKey}

Returns participant address based on its public key.

Method Response:

```
{
  "address": "3N4WaaaNAVLMQgVKTRSePgwBuAKvZTjAQbq"
}
```

GET /addresses/data/{address}

Returns all data recorded to address account {address}.

Method Response:

```
[
  {
    "key": "4yR7b6Gv2rzLrhYBHpgVCmLH42raPGTF4Ggi1N36aWnY",
    "type": "integer",
    "value": 1500000
  }
]
```

GET /addresses/data/{address}/{key}

Returns data recorded to address account {address} by key {key}.

Method Response:

```
{
  "key": "4yR7b6Gv2rzLrhYBHpgVCmLH42raPGTF4Ggi1N36aWnY",
  "type": "integer",
  "value": 1500000
}
```

20.1.3 Alias

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /alias/by-alias/{alias}

Gets participant address by its alias {alias}.

Method Response:

```
{
  "address": "address:3Mx2afTZ2KbRrLNbytyzTtXukZvqEB8SkW7"
}
```

GET /alias/by-address/{address}

Gets alias {alias} of participant by its address {address}.

Method Response:

```
[
  "alias:HUMANREADABLE1",
  "alias:HUMANREADABLE2",
  "alias:HUMANREADABLE3",
]
```

20.1.4 Anchoring

GET /anchoring/config

Hint: Rules of the creating requests to a node, see *How to use REST API* section.

Get the *anchoring* section of the node configuration file.

Method answer

```
{
  "enabled": true,
  "currentChainOwnerAddress": "3FWwx4o1177A4oeHAEW5EQ6Bkn4Lv48quYz",
  "mainnetNodeAddress": "https://clinton-pool.wavesenterpriseservices.com:443",
  "mainnetSchemeByte": "L",
  "mainnetRecipientAddress": "3JzVWCSV6v4ucSxtGSjZsvdiCT1FAzwpqrP",
  "mainnetFee": 8000000,
  "currentChainFee": 666666,
}
```

(continues on next page)

(continued from previous page)

```
"heightRange": 5,
"heightAbove": 3,
"threshold": 10
}
```

20.1.5 Assets

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET/assets/balance/{address}

Returns balance of all address {address} assets.

Method Response:

```
{
  "address": "3Mv61qe6egMSjRDZiiuvJDnf3Q1qW9tTZDB",
  "balances": [
    {
      "assetId": "Ax9T4grFxx5m3KPUEKjMdnQkCKtBktf694wU2wJYvQUD",
      "balance": 4879179221,
      "quantity": 48791792210,
      "reissuable": true,
      "minSponsoredAssetFee" : 100,
      "sponsorBalance" : 1233221,
      "issueTransaction" : {
        "type" : 3,
        ...
      }
    },
    {
      "assetId": "49KfHPJcKvSAvNKwM7CTofjKHZL87SaSx8eyADBjv5Wi",
      "balance": 10,
      "quantity": 10000000000,
      "reissuable": false,
      "issueTransaction" : {
        "type" : 3,
        ...
      }
    }
  ]
}
```

Method Parameters:

- “Address” - participant address
- “balances” - object with participant balance
- “assetId” - asset ID
- “balance” - asset balance

- “quantity” - number of issued assets
- “reissuable” - indicator whether asset can be reissued or not
- “issueTransaction” - asset creation transaction
- “minSponsoredAssetFee” - minimum value of fee for sponsorship transactions
- “sponsorBalance” - assets allocated for payment of sponsored asset transactions

GET /assets/balance/{address}/{assetId}

Returns address {address} balance by asset {assetId}.

Method Response:

```
{
  "address": "3Mv61qe6egMSjRDZiiuvJDnf3Q1qW9tTZDB",
  "assetId": "Ax9T4grFxx5m3KPUEKjMdnQkCKtBktf694wU2wJYvQUD",
  "balance": 4879179221
}
```

GET /assets/details/{assetId}

Returns description of asset {assetId}.

Method Response:

```
{
  "assetId" : "8tdULCMr598Kn2dUaKwHkvsNyFbDB1Uj5NxvVRTQRnMQ",
  "issueHeight" : 140194,
  "issueTimestamp" : 1504015013373,
  "issuer" : "3NCBMxgdghg4tUHEffsXy11L6hUi6fcBpd",
  "name" : "name",
  "description" : "Sponsored asset",
  "decimals" : 1,
  "reissuable" : true,
  "quantity" : 1221905614,
  "script" : null,
  "scriptText" : null,
  "complexity" : 0,
  "extraFee": 0,
  "minSponsoredAssetFee" : 100000 // null assume no sponsorship, number - amount of assets for
  ↪ minimal fee
}
```

GET /assets/{assetId}/distribution

Returns distribution of asset {assetId}.

Method Response:

```
{
  "3P8GxcTEyZtG6LEfnn9knp9wu8uLKrAFHCb": 1,
  "3P2voHxcJg79csj4YspNq1akepX8TSmGhTE": 1200
}
```

POST /assets/balance

Returns the assets balance for one or few addresses.

Method Response

```
{
  "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG": [],
  "3GRLFi4rz3SniCuC7rbd9UuD2KUZyNh84pn": []
}
```

20.1.6 Blocks

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

The last block may contain a different number of transactions during the period of its creation. It depends on the fact that while the block is not accepted by the nodes-miners, the number of transactions in it can constantly change. Therefore, when using methods that provide information about the last block, it should be kept in mind that the number of transactions in the last block may change.

GET /blocks/height

Returns block number of current blockchain state.

Method Response:

```
{
  "height": 7788
}
```

GET /blocks/height/{signature}

Returns height (number) of block by its signature.

GET /blocks/first

Returns contents of first block (genesis block).

GET /blocks/last

Returns contents of last block.

Method Response:

```
{
  "version": 2,
  "timestamp": 1479313809528,
  "reference":
  ↪ "4MLXQDbARiJDEAoy5vZ8QYh1yNnDhdGhGwkDKna8J6QXb7agVpFEi16hHBGUxxnq8x4myG4w66DR4Ze8FM5dh8Gi",

```

(continues on next page)

(continued from previous page)

```

"nextconsensus": {
  "basetarget": 464,
  "generationsignature": "7WUV2TufarAyiCPFDnAWbn2Q7Jk7nBmWbnnDXKDEeJv"
},
"transactions": [
  {
    "type": 2,
    "id":
    ↪ "64hxaxZvB9iD1cfRf1j8KPTXs4qE7SHaDWTZKoUvgfVZotaJUtSGa5Bxi86ufAfp5ifoNAGknBqS9CpxBKG9RNVR",
    "fee": 100000,
    "timestamp": 1479313757194,
    "signature":
    ↪ "64hxaxZvB9iD1cfRf1j8KPTXs4qE7SHaDWTZKoUvgfVZotaJUtSGa5Bxi86ufAfp5ifoNAGknBqS9CpxBKG9RNVR",
    "sender": "3NBVqYXrapgJP9atQccdBP AgJPwHDKkh6A8",
    "senderPublicKey": "CRxqEuxhdZBEHX42MU4FfyJxuHmbDBTaHmM3Uki7pLw",
    "recipient": "3N8UPtqiy322NVr1fLP7SaK1AaCU7oPaVuy",
    "amount": 1000000000
  }
],
"generator": "3N5GRqzDBhjVXnCb44baHcz2GoZy5qLxtTh",
"signature":
    ↪ "4ZhZdLAvAGneLU4K4b2eTgRQvbbjEZrtwo1qAhM9ar3A3weGEutbfNKM4WJ9JZnV8BXenx8JRGVNWpfx3prGaxd",
"fee": 100000,
"blocksize": 369
}
    
```

GET /blocks/at/{height}

Returns contents of block at height {height}.

GET /blocks/seq/{from}/{to}

Returns contents of blocks ranging from {from} to {to}.

GET /blocks/seqext/{from}/{to}

Returns contents of blocks with additional transactions info ranging from {from} to {to}.

GET /blocks/signature/{signature}

Returns contents of block by its signature {signature}.

GET /blocks/address/{address}/{from}/{to}

Returns all blocks generated (mined) by address {address}.

GET /blocks/child/{signature}

Returns block inherited from block with signature {signature}.

GET /blocks/headers/at/{height}

Returns block header at height {height}.

GET /blocks/headers/seq/{from}/{to}

Returns block headers ranging from {from} to {to}.

GET /blocks/headers/last

Returns header of last block in the blockchain.

20.1.7 Consensus

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /consensus/algo

Returns type of consensus algorithm used on the network.

Method Response:

```
{
  "consensusAlgo": "Fair Proof-of-Stake (FairPoS)"
}
```

GET /consensus/settings

Returns consensus settings specified in node configuration file.

Method Response:

```
{
  "consensusAlgo": "Proof-of-Authority (PoA)",
  "roundDuration": "25 seconds",
  "syncDuration": "5 seconds",
  "banDurationBlocks": 50,
  "warningsForBan": 3
}
```

GET /consensus/minersAtHeight/{height}

Returns miner queue at height {height}.

Method Response:

```
{
  "miners": [
    "3Mx5sDq4NXef1BRzJRAofa3orYFxlAnxmd7",
    "3N2EsS6hJPYgRn7WFJHLJNnrsm92sUKcXkd",
    "3N2cQFfUDzG2iujBrFTnD2TAsCNohDxYu8w",
    "3N6pfQJyqjLcMmbU7G5sNABLmSF5aFT4KTF",
    "3NBbipRYQmZFudFCoVJXg9JMkkyZ4DEdZNS"
  ],
  "height": 1
}
```

GET /consensus/miners/{timestamp}

Returns miner queue at timestamp {timestamp}.

Method Response:

```
{
  "miners": [
    "3Mx5sDq4NXef1BRzJRAofa3orYFxlAnxmd7",
    "3N2EsS6hJPYgRn7WFJHLJNnrsm92sUKcXkd",
    "3N2cQFfUDzG2iujBrFTnD2TAsCNohDxYu8w",
    "3N6pfQJyqjLcMmbU7G5sNABLmSF5aFT4KTF",
    "3NBbipRYQmZFudFCoVJXg9JMkkyZ4DEdZNS"
  ],
  "timestamp": 1547804621000
}
```

GET /consensus/bannedMiners/{height}

Returns a list of blocked miners at height {height}.

Method Response:

```
{
  "bannedMiners": [],
  "height": 1000
}
```

GET /consensus/basetarget/{blockId}

Returns value of 'base complexity' _ (basetarget) of creating block {blockId} .

GET /consensus/basetarget

Returns value of 'base complexity' _ (basetarget) of creating last block.

GET /consensus/generatingbalance/{address}

Returns generating balance available for minning node {address} - minimum participant balance including assets transferred to participant for leasing, for last 1000 blocks.

GET /consensus/generationsignature/{blockId}

Returns value of 'generation signature' _ of generating block {blockId}.

GET /consensus/generationsignature

Returns value of 'generation signature' _ of last block.

20.1.8 Contracts

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /contracts

Returns the contracts info.

Method Response

```
[
  {
    "contractId": "dmLT1ippM7tmfSC8u9P4wU6sBgHXGYy6JYxCq1CCh8i",
    "image": "registry.wvservices.com/wv-sc/may14_1:latest",
    "imageHash": "ff9b8af966b4c84e66d3847a514e65f55b2c1f63afcd8b708b9948a814cb8957",
    "version": 1,
    "active": false
  }
]
```

POST /contracts

Returns some parameters for the one or more contract IDs specified in the query.

Method Response

```
{
  "8vBJhy4eS8oEwCHC3yS3M6nZd5CLBa6XNt4Nk3yEEExG": [
    {
      "type": "string",
      "value": "Only description",
      "key": "Description"
    },
    {
      "type": "integer",
      "value": -9223372036854776000,
      "key": "key_may"
    }
  ]
}
```

GET /contracts/info/{contractId}

Returns current information about specified contract version, contract location, and the image hash.

Method Response

```
[
  {
    "contractId": "dmLT1ippM7tmfSC8u9P4wU6sBgHXGYy6JYxCq1CCh8i",
    "image": "registry.wvservices.com/wv-sc/may14_1:latest",
    "imageHash": "ff9b8af966b4c84e66d3847a514e65f55b2c1f63afcd8b708b9948a814cb8957",
    "version": 1,
    "active": false
  }
]
```

GET /contracts/status/{id}

Returns the contract execution transaction status.

Method Response

```
[
  {
    "sender": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
    "senderPublicKey": "4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
    "txId": "4q5Q8vLeGBpcdQofZikyrrjHUS4pB1AB4qNEn2yHRKWU",
    "status": "Success",
    "code": null,
    "message": "Smart contract transaction successfully mined",
    "timestamp": 1558961372834,
    "signature":
    ↪ "4gXy7qtzkaHHH6NkksnZ5pvn8juF65MvjQ9JgVztpgNwLNwuyyr27Db3gCh5YyADqZeBH72EyAkBouUoKvwJ3RQJ"
  }
]
```

(continues on next page)

(continued from previous page)

```

"sender": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
"senderPublicKey": "4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
"txId": "4q5Q8vLeGBpcdQofZikyrrjHUS4pB1AB4qNEn2yHRKWU",
"status": "Success",
"code": null,
"message": "Smart contract transaction successfully mined",
"timestamp": 1558961376012,
"signature":
↪ "3Vhqc9DvNhMvFFtWnBuV4XwQ62ZcTAvLNZYmeGc7mGzMcncGZ3RlshDs393fnQu1WTh8CmL58YnvnjyULEEi5yorV"
}
]

```

GET /contracts/{contractId}

Returns result of smart contract execution by its ID (contract creation transaction ID).

Method Response:

```

[
{
  "key": "avg",
  "type": "string",
  "value": "3897.80146957"
},
{
  "key": "buy_price",
  "type": "string",
  "value": "3842"
}
]

```

GET /contracts/executed-tx-for/{id}

Returns result of smart contract execution by ID of contract execution transaction.

Method Response:

```

{
  "type": 105,
  "id": "2UAHvs4KsfBbRVpm2dCigWtqUHuaNqou83CXy6DGDiaRa",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVLrqLCqouVrFZynjfoTEuPNV9GrdaunpgdWXLsq",
  "fee": 500000,
  "timestamp": 1549365523980,
  "proofs": [
    "4BoG6wQnYyZWyUKzAwh5n1184tsEWUqUTWmXMExvvcu95xgk4UFB8iCnHJ4GhvJm86REB69hKM7s2WLAwTSXquAs"
  ],
  "version": 1,
  "tx": {
    "type": 103,
    "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLLLZVj4Ky",
    "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
    "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqdsjMVT2M",
    "fee": 500000,

```

(continues on next page)

(continued from previous page)

```

    "timestamp": 1550591678479,
    "proofs": [
    ↪ "yecrFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fvj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
    "version": 1,
    "image": "stateful-increment-contract:latest",
    "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
    "contractName": "stateful-increment-contract",
    "params": [],
    "height": 1619
  },
  "results": []
}

```

GET /contracts/{contractId}/{key}

Returns smart contract execution value by its ID (contract creation transaction ID) and key {key}.

Method Response:

```

{
  "key": "updated",
  "type": "integer",
  "value": 1545835909
}

```

20.1.9 Crypto

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

POST /crypto/encryptSeparate

Encrypts the text separately for the each recipient with the unique key.

Method Query

```

{
  "sender": "3MCUfX4P4U56hoQwSqXnLJenB6cDkxBjisL",
  "password": "some string as a password",
  "encryptionText": "some text to encrypt",
  "recipientsPublicKeys": [
    ↪ "5R65oLxp3iwPekwirA4VwwUXaySz6W6YKXBKBRl352pwwcpsFcjRHJ1VVHLP63LkrkxsNod64V1pffeizZ5i2qXc",
    "9LopMj2GqWxBYgnZ2gxaNwxYqxXHuWd6ZAdVqkprR1fFMNvDUHYUCwFxsB79B9sefgxNdqwNtqzuDS8Zmm48w3S"]
  ]
}

```

Method Response

```

{
  "encryptedText": "IZ5Kk5YNspMWl/jmlTizVxD6Nik=",
  "publicKey":
    ↪ "5R65oLxp3iwPekwirA4VwwUXaySz6W6YKXBKBRl352pwwcpsFcjRHJ1VVHLP63LkrkxsNod64V1pffeizZ5i2qXc",
}

```

(continues on next page)

(continued from previous page)

```

"wrappedKey":
↪ "uWVoxJAzruwTDDSbphDS31TjSQX6CSWXivp3x34uE3XtnMqqK9swoaZ3LyAgFDR7o6CfkgzFkWmTen4qAZewPfbBwR"
},
{
  "encryptedText": "F9u010RGvSEDe6dWm1pzJQ+3xqE=",
  "publicKey":
↪ "9LopMj2GqWxBYgnZ2gxaNwxXqxXHuWd6ZAdVqkprR1fFMNvDUHYUCwFxsB79B9sefgxNdqwNtqzuDS8Zmm48w3S",
  "wrappedKey":
↪ "LdzoKadUzBTmwcZGYgu1AM4YrbbLr9Uh1MvQ3MPcLZUhCD9herz4dv1m6ssaVHPiBNUGgqKnLZ6Si4Cc64UvhXBbG"
}

```

POST /crypto/encryptCommon

Encrypts the data with a single CEK key for all recipients and the CEK wraps into a unique KEK for the each recipient.

Method Query

```

{
  "sender": "3MCUfX4P4U56hoQwSqXnLJenB6cDkxBjisL",
  "password": "some string as a password",
  "encryptionText": "some text to encrypt",
  "recipientsPublicKeys": [
↪ "5R65oLxp3iwPekwirA4VwwUXaySz6W6YKXBKBR352pwwcpsFcjRHJ1VVHLp63LkrkxsNod64V1pffeizZ5i2qXc",
  "9LopMj2GqWxBYgnZ2gxaNwxXqxXHuWd6ZAdVqkprR1fFMNvDUHYUCwFxsB79B9sefgxNdqwNtqzuDS8Zmm48w3S"]
}

```

Method Response

```

{
  "encryptedText": "NpCCig2i3jzo0xBnfqjfedbti8Y=",
  "recipientToWrappedStructure": {
    "5R65oLxp3iwPekwirA4VwwUXaySz6W6YKXBKBR352pwwcpsFcjRHJ1VVHLp63LkrkxsNod64V1pffeizZ5i2qXc":
    "M8pAe8HnKiWLE1HsC1ML5t8b7giWxiHfvagh7Y3F7rZL8q1tqMCJMYJo4qz4b3xjcuUiV57tY3k7oSig53Aw1Dkkw",
    "9LopMj2GqWxBYgnZ2gxaNwxXqxXHuWd6ZAdVqkprR1fFMNvDUHYUCwFxsB79B9sefgxNdqwNtqzuDS8Zmm48w3S":
    "Doqn6gPvBBesU2vdwgfYMBDHM4knEGMbqPn8Np76mRRoZXLdioofyVbSSaTTEr4cvXwzEwVMugiy2wuzFWk3zCiT3"
  }
}

```

POST /crypto/decrypt

Decrypts the data. The decryption is available only if the message recipient's key is in the node's keystore.

Method Query

```

{
  "recipient": "3M5F8B1qxSY1W6kA2ZnQiDB4JTGz9W1jvQy",
  "password": "some string as a password",
  "encryptedText": "oiKFJijfid8HkjsjdhKHhud987d",
  "wrappedKey": "M5F8B1qxSY1W6kA2ZnQiDB4JTGzA2ZnQiDB4JTGz9W1jvQy"
  "senderPublicKey": "M5F8B1qxSY1W6kA2ZnQiDB4JTGzA2ZnQiDB4JTGz9W1jvQy",
}

```

Method Response


```
{
  "decryptedText": "some string for encryption",
}
```

20.1.10 Debug

Hint: The rules for generating node queries are given in module *How to use REST API*.

GET /debug/blocks/{howMany}

Gets sizes and full hashes for last blocks. The blocks number is specified during the request.

Method Response

```
[
  {
    "226": "7CkZxrAjU8bnat8CjVAPagobNYazyv1HASubmp7YYqGe"
  },
  {
    "226": "GS3y9fUHAKCamq52TPsjizDVir8J7iGoe8P2XZLasxsC"
  },
  {
    "226": "B9LmhGGDdvcfUA9JEWvyVrT9sazZE6gibpAN13xUN7KV"
  },
  {
    "226": "Byb9MHtwYf3MFyi2tbhQ3GTdCct5phKq9REkjbQTzdne"
  },
  {
    "226": "HSxSHbiV4tZc8RaN6jxdhgtkAhjxuLn76uHxerMRUefA"
  }
]
```

GET /debug/info

Shows all information for the debugging and testing.

Method Response

```
{
  "stateHeight": 74015,
  "extensionLoaderState": "State(Idle)",
  "historyReplierCacheSizes": {
    "blocks": 13,
    "microBlocks": 2
  },
  "microBlockSynchronizerCacheSizes": {
    "microBlockOwners": 0,
    "nextInventories": 0,
    "awaiting": 0,
    "successfullyReceived": 0
  }
}
```

(continues on next page)

(continued from previous page)

```
  },
  "scoreObserverStats": {
    "localScore": 42142328633037120000,
    "scoresCacheSize": 4
  },
  "minerState": "mining microblocks"
}
```

POST /debug/rollback

Removes all blocks after given height.

Sample response

```
{
  "rollbackTo": 100,
  "returnTransactionsToUtx": true
}
```

Method Response

```
{
  "BlockId":
  ↪ "4U4Hmg4mDYrvxaZ3JVzL1Z1piPDZ1PJ61vd1PeS7ESZFkHsUCUqeeAZoszTVr43Z4NV44dqbLv9WdrLytDL6gHuv"
}
```

POST /debug/validate

Validates a transaction and measures time spent in milliseconds.

Query Parameters

```
"id" - Transaction ID
```

Method Response

```
{
  "valid": false,
  "validationTime": 14444
}
```

GET /debug/minerInfo

Shows all miner information for debugging.

Method Response

```
[
  {
    "address": "3JFR1pmL6biTzr9oa63gJcjZ8ih429KD3aF",
    "miningBalance": 1248959867200000,
    "timestamp": 1585923248329
  }
]
```

GET /debug/historyInfo

Shows all last block history for debugging.

Method Response

```
{
  "lastBlockIds": [
    "37P4fvexYHPUzNPRRqYbRYxGz7x3r5jFznck7amaS6aWnHL5oQqrqCzsSh1HvYKnd2ZhU6n6sWYPb3hxsY8FBfmZ",
    "5RRu1qtesz4KvrVp4fxzQHebq2fRanNsg3HJKwD4uChqySm7vFHCdHKU6iZYXJDVmfSxiE9Maeb6sM2JireaWlBx",
    "3Lo27JfjekcZnJsYEe7st7evDZ6TgmCUBtiZrSxUCobKL48DZQ4dXMfp89WYjEykh15HEHSXzqMSTQigE8vEcN2r",
    "r4RuxEXAqgfDMKVXRWmZcGMaWKDsAvVxfXDtw8d6bamLR61J1gaoesargYSoZQqRbDrBcefLprk7D78fA728719",
    "3F4Up46crZbpKVWUeieL6GeSrVMYm7JJ7aX6aHD6B8wedFggSKv8d3H39Qy9MLEauFBU9m3qZV1U8emhmqmLbg",
    "QSuBkEtVe9nik5T5S33ogeCbKy7ihBkS2pwYayK23m4ANier83ThpajEzvpbyPy9pPWZc5St8mYUKxXDscKuRC",
    "4udpNnz3e1M1GbVZxtwfg8gpf6EbiKxRCRBwi6iRMylsvh5J2Ec9Wqyu2sq2KYL75o12yiP8TszworeUfuxNmJ5g",
    "5BZYZ4RZAjM5KKCaHpyUsXnb4uunnM5kcfTojc5QzQo3vyP2w3YD4qrALizkkQQR4ziS77BoAGb56QCecUtHFFN",
    "5JwfLaF1oGxRXVCdDbFuKpxrvxgLCGU3kCFwxUHL8G3xV211MrKBuAuQ4MaC5uN574uV9U8M6HfHTMERnfr5jGJ",
    "4bysMhz14E1rC7dLYScfVVqPmHqzi8jdhnkruJmCNL86Tvw2cbF7G9YVchvTrv9qbQZ7JQownV59gRRcd26zm16"
  ],
  "microBlockIds": []
}
```

GET /debug/configInfo

Shows currently running node config.

Method Response

```
{
  "node": {
    "anchoring": {
      "enable": "no"
    },
    "blockchain": {
      "consensus": {
        "type": "pos"
      },
      "custom": {
        "address-scheme-character": "K",
        "functionality": {
          "blocks-for-feature-activation": 10,
          "feature-check-blocks-period": 30,
          "pre-activated-features": { ...
.....
        }
      }
    },
    "wallet": {
      "file": "wallet.dat",
      "password": ""
    },
    "waves-crypto": "yes"
  }
}
```

DELETE /debug/rollback-to/{signature}

Rollbacks the state to the block with a given signature.

Query Parameters

```
"signature" - Block signature
```

Method Response

```
{
  "BlockId":
  ↪ "4U4Hmg4mDYrvxaZ3JVzL1Z1piPDZ1PJ61vd1PeS7ESZfKhsUCUqeeAZosZTVr43Z4NV44dqbLv9WdrLytDL6gHuv"
}
```

GET /debug/portfolios/{address}

Gets current portfolio considering pessimistic transactions in the UTX pool.

Query Parameters

```
"address" - Node address
```

Method Response

```
{
  "balance": 104665861710336,
  "lease": {
    "in": 0,
    "out": 0
  },
  "assets": {}
}
```

POST /debug/print

Prints a string at DEBUG level, strips to 250 chars.

Sample response

```
{
  "message": "string"
}
```

GET /debug/state

Gets current state of the node.

Method Response

```
{
  "3JD3qDmgL1icDaxa3n24YSjxr9Jze5MBVVs": 4899000000,
  "3JPWx147Xf3f9fE89YtfvRhtKWBHy9rWnMK": 17528100000,
  "3JU5tCoSwHH7FKPBuOwySWBnQwpbZiYyNhB": 300021381800000,
}
```

(continues on next page)

(continued from previous page)

```

"3JCJChsQ2CGyHc9Ymu8cnsES6YzjjJELu3a": 75000362600000,
"3JEW9XnPC8w3qQ4AJyVTDBmsVUp32QKocGD": 5000000000,
"3JSaKNX94deXJkywQwTFgbigTxJa36TDVg3": 6847000000,
"3JFR1pmL6biTzr9oa63gJcjZ8ih429KD3aF": 1248938560600000,
"3JV6V4JEVc3a9uSqRmdUMvMKMfZa16HbGmq": 4770000000,
"3JZtYeGEZHjb2zQ6EcSEo524PdafPn6vWkc": 900000000,
"3JMMFLX9d1rmXaBK9AF7Wuwzu4vRkkoVQBC": 4670000000,
"3JJDpPDqSPokKp5jEmzwMzmaPUyopLZjW1C": 800000000,
"3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t": 994280900000
}

```

GET /debug/stateWE/{height}

Gets state at specified height.

Query Parameters

```
"height" - Block height
```

Method Response

```

{
  "3JWPx147Xf3f9fE89YtfvRhtKWBHy9rWnMK": 17528100000,
  "3JU5tCoswHH7FKPBuowySWBnQwpbZiYyNhB": 300020907600000,
  "3JCJChsQ2CGyHc9Ymu8cnsES6YzjjJELu3a": 750003506000000,
  "3JSaKNX94deXJkywQwTFgbigTxJa36TDVg3": 6847000000,
  "3JFR1pmL6biTzr9oa63gJcjZ8ih429KD3aF": 1248960085800000,
  "3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t": 994280900000
}

```

20.1.11 Leasing

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /leasing/active/{address}

Returns list of lease creation transactions, in which {address} was involved as sender or recipient.

Method Response:

```

[
  {
    "type": 8,
    "id": "2jWhz6uGYsgvfoMzNR5EEGdi9eafyCA2zLffkM4NP6T7",
    "sender": "3PP6vdkEwoif7AZDtSeSDtZcwiqSfhmwtTE",
    "senderPublicKey": "DW9NKL YeyoEWDqJKhWv87EdFfTqpFtJBWoCqfCVwRhS Y",
    "fee": 100000,
    "timestamp": 1544390280347,
    "signature":
    ↪ "25kpwh7nYjrUtfbAbWYRyMDPCUCoyMoUuWTJ6vZqrXsZYXbdiWHa9iGscTTGnPfyegP82sNSfM2bXNX3K7p6D3HD",

```

(continues on next page)

(continued from previous page)

```

"version": 1,
"amount": 31377465877,
"recipient": "3P3RD3yJW2gQ9dSVwVVDVCQiFWqALtZcyzH",
"height": 1298747
}
]

```

```

[
{
  "type": 8,
  "id": "2jWhz6uGYsgvfoMzNR5EEGdi9eafyCA2zLffkM4NP6T7",
  "sender": "3PP6vdkEwoif7AZDtSeSDtZcwiqSfhwttE",
  "senderPublicKey": "DW9NKLyeyoEWDqJKhWv87EdFfTqpFtJBWoCqfCVvRhsY",
  "fee": 100000,
  "timestamp": 1544390280347,
  "signature":
  ↪ "25kpwh7nYjRUtfbAbWYRyMDPCUCoyMoUuWTJ6vZQrXsZYXbdiWHa9iGscTTGnPfYegP82sNSfM2bXNX3K7p6D3HD",
  "version": 1,
  "amount": 31377465877,
  "recipient": "3P3RD3yJW2gQ9dSVwVVDVCQiFWqALtZcyzH",
  "height": 1298747
}
]

```

20.1.12 Licenses

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /licenses

Returns a list of all downloaded licenses.

Method Response:

```

[
{
  "license": {
    "version": 1,
    "id": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYSKG",
    "license_type": null,
    "issued_at": "2020-02-27T16:11:14.784Z",
    "node_owner_address": "4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
    "valid_from": "2020-02-20",
    "valid_to": "2020-02-27",
    "features": [
      "all_inclusive"
    ]
  },
  "signer_public_key": "dmLT1ippM7tmfSC8u9P4wU6sBgHXGYy6JYxCq1CCh8i",
  "signature":
  ↪ "ff9b8af966b4c84e66d3847a514e65f55b2c1f63afcd8b708b9948a814cb8957mLT1ippM7tmfSC8u",
}
]

```

(continues on next page)

(continued from previous page)

```

"signer_id": "ff9b8af966b4c84e66d3847a514e65f55b2c1f63afcd8b708b9948a814cb8957"
},
{
  "license": {
    "version": 1,
    "id": "49KfHPJcKvSAvNKwM7CTofjKHZL87SaSx8eyADBjv5Wi",
    "license_type": null,
    "issued_at": "2020-02-27T16:12:34.327Z",
    "node_owner_address": "3N4WaaaNAVLMQgVKTRSePgwBuAKvZTjAqBq",
    "valid_from": "2020-02-29",
    "valid_to": null,
    "features": [
      "all_inclusive"
    ]
  },
  "signer_public_key": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "signature":
  ↪"5kwwE9sDZzss0NaoBSJnb8RLqfYGt1NDGbTWWXUeX8b9amRRJN3hr5fhs9vHBq6VES5ng4hqbCUoDEsoQNauRRts",
  "signer_id": "8tdULCMr598Kn2dUaKwHkvsNyFbDB1Uj5NxivVRTQRnMQ"
}
]

```

GET /licenses/status

Returns the node license activation status

Method Response:

```

{
  "status" : "TRIAL",
  "description" : "Trial period is active. Blocks before expiration: '{num}'"
}

```

POST /licenses/upload

Adds a new license in JSON format in the node

Method request

```

{
  "license": {
    "version": 1,
    "id": "49KfHPJcKvSAvNKwM7CTofjKHZL87SaSx8eyADBjv5Wi",
    "license_type": null,
    "issued_at": "2020-02-27T16:12:34.327Z",
    "node_owner_address": "3N4WaaaNAVLMQgVKTRSePgwBuAKvZTjAqBq",
    "valid_from": "2020-02-29",
    "valid_to": null,
    "features": [
      "all_inclusive"
    ]
  },
  "signer_public_key": "C1ADP1tNGuSLTiQrfNRPhgXx59nCrwrZFRV4AHpfKBpZ",
  "signature":
  ↪"5kwwE9sDZzss0NaoBSJnb8RLqfYGt1NDGbTWWXUeX8b9amRRJN3hr5fhs9vHBq6VES5ng4hqbCUoDEsoQNauRRts",

```

(continues on next page)

(continued from previous page)

```
}
  "signer_id": "8tdULCMr598Kn2dUaKwHkvsNyFbDB1Uj5NxvVRtQRnMQ"
}
```

Method Response:

```
{
  "message": "License upload successfully"
}
```

20.1.13 Node

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /node/config

Returns main node configuration parameters.

Method Response:

```
{
  "version": "0.6.6",
  "waves-crypto": false,
  "chainId": "D",
  "consensus": "POS",
  "minimumFee": {
    "1": 0,
    "3": 10000000,
    "4": 100000,
    "5": 100000000,
    "6": 100000,
    "7": 300000,
    "8": 100000,
    "9": 100000,
    "10": 100000,
    "11": 100000,
    "12": 100000,
    "13": 1000000,
    "14": 100000000,
    "15": 100000000,
    "102": 0
  }
}
```


POST /node/stop

Query stops node.

GET /node/status

Returns main node configuration parameters.

Method Response:

```
{
  "blockchainHeight": 47041,
  "stateHeight": 47041,
  "updatedTimestamp": 1544709501138,
  "updatedAt": "2018-12-13T13:58:21.138Z"
}
```

GET /node/version

Returns version of application.

Method Response:

```
{
  "version": "Waves Enterprise v0.9.0"
}
```

GET /node/owner

Возвращает адрес и публичный ключ владельца ноды.

Method Response:

```
{
  "address": "3JFR1pmL6biTzr9oa63gJcjZ8ih429KD3aF",
  "publicKey": "EPxkVA9iQejsjQikovyxkkY8iHnbXsR3wjgkE7ZW1Tt"
}
```

20.1.14 Peers

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

POST /peers/connect

Request to connect a new host to the node.

Method Query:

```
{
  "host": "127.0.0.1",
  "port": "9084"
}
```

Method Response:

```
{
  "hostname": "localhost",
  "status": "Trying to connect"
}
```

GET /peers/connected

Returns a list of connected nodes.

Method Response:

```
{
  "peers": [
    {
      "address": "52.51.92.182/52.51.92.182:6863",
      "declaredAddress": "N/A",
      "peerName": "zx 182",
      "peerNonce": 183759
    },
    {
      "address": "ec2-52-28-66-217.eu-central-1.compute.amazonaws.com/52.28.66.217:6863",
      "declaredAddress": "N/A",
      "peerName": "zx 217",
      "peerNonce": 1021800
    }
  ]
}
```

GET /peers/all

Returns a list of all known nodes.

Method Response:

```
{
  "peers": [
    {
      "address": "/13.80.103.153:6864",
      "lastSeen": 1544704874714
    }
  ]
}
```

GET /peers/suspended

Returns a list of suspended nodes.

Method Response:

```
[
  {
    "hostname": "/13.80.103.153",
    "timestamp": 1544704754619
  }
]
```

POST /peers/identity

Gets the public key of the peer which is used by the node for the connection and the confidential data transfer.

Method Query:

```
{
  "address": "3NBVqYXrapgJP9atQccdBPAgJPwHDKkh6A8",
  "signature":
  →"6RwMUQcwrxtKDgM4ANes9Amu5EJgyfF9Bo6nTpXyD89ZKMAcpCM97igbWf2MmLXLdqNxdSUC68fd5TyRBEB6nqf"
}
```

Parameters:

- address - the blockchain address corresponding to the “privacy.owner-address” parameter in the node configuration file;
- signature - electronic signature of the “address” field value.

Method Response:

```
{
  "publicKey": "3NBVqYXrapgJP9atQccdBPAgJPwHDKkh6A8"
}
```

Parameters:

- publicKey - the peer public key associated with “privacy.owner-address” parameter in the configuration file. This parameter does not appear if the mode of the handshake checking turned off.

GET /peers/hostname/{address}

Gets the hostname and IP Address of the node by its address in the Waves Enterprise net.

Method Response:

```
{
  "hostname": "node1.we.io",
  "ip": "10.0.0.1"
}
```

GET /peers/allowedNodes

Gets the actual list of allowed participants at the request moment.

Method Response:

```
{
  "allowedNodes": [
    {
      "address": "3JNLQYuHYSHZiHr5KjJ89wwFJpDMdrAEJpj",
      "publicKey": "Gt3o1ghh2M2TS65UrHZCTJ82LLcMcBrxuaJyrgsLk5VY"
    },
    {
      "address": "3JLp8wt7rEUdn4Cca5Hp9jZ7w8T5XDAKicd",
      "publicKey": "J3ffCciVu3sustgb5vxmEHczACMR89Vty5ZBLbPn9xyg"
    },
    {
      "address": "3JRY1cp7atRMBd8QqoswRpH7DLawM5Pnk3L",
      "publicKey": "5vn4UcB9En1XgY6w2N6e9W7bqFshG4SL2RLFqEWEbWxG"
    }
  ],
  "timestamp": 1558697649489
}
```

20.1.15 Permissions

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

GET /permissions/{address}

Returns roles (permissions) assigned to specified address {address} which are valid at the moment.

Method Response:

```
{
  "roles": [
    {
      "role": "miner"
    },
    {
      "role": "permissioner"
    }
  ],
  "timestamp": 1544703449430
}
```

GET /permissions/{address}/at/{timestamp}

Returns roles (permissions) assigned to specified address {address} which are valid at the moment {timestamp}.

Method Response:

```
{
  "roles": [
    {
      "role": "miner"
    },
    {
      "role": "permissioner"
    }
  ],
  "timestamp": 1544703449430
}
```

POST /permissions/addresses

Returns roles (permissions) assigned to specified address list which are valid at the moment.

Method Query:

```
{
  "addresses": [
    "3N2cQFfUDzG2iuJBrFTnD2TAsCNoHDxYu8w", "3Mx5sDq4NXef1BRzJRAofa3orYFxlAnxmd7"
  ],
  "timestamp": 1544703449430
}
```

Method Response:

```
{
  "addressToRoles": [
    {
      "address": "3N2cQFfUDzG2iuJBrFTnD2TAsCNoHDxYu8w",
      "roles": [
        {
          "role": "miner"
        },
        {
          "role": "permissioner"
        }
      ]
    },
    {
      "address": "3Mx5sDq4NXef1BRzJRAofa3orYFxlAnxmd7",
      "roles": [
        {
          "role": "miner"
        }
      ]
    }
  ],
}
```

(continues on next page)

(continued from previous page)

```
    "timestamp": 1544703449430
  }
```

20.1.16 PKI

Warning: The PKI methods can be used only with GOST cryptography.

Digital signature formats listed in the table below is used in PKI. The digital signature number in the table is consistent for the `sigtype` field value.

Table 1: Digital signature formats

| # | Digital signature format |
|---|--------------------------|
| 1 | CADES-BES |
| 2 | CADES-X Long Type 1 |
| 3 | CADES-T |

POST /pki/sign

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

This method creates a detached digital signature. `inputData` is data for generating a digital signature as an array of bytes in the **Base64** coding, `keystoreAlias` is a name of the key container of the digital signature private key. Also you need to specify a password in the `password` string.

Request example

```
{
  "inputData" : "SGVsbG8gd29ybGQh",
  "keystoreAlias" : "key1",
  "password" : "password",
  "sigType" : "CADES_X_Long_Type_1",
}
```

Answer example

```
{
  "signature" :
  ↳ "c2RmZ3NkZmZoZ2ZkZ2hmZGpkZ2ZoamhnZmtqaGdmamtkZmdkZmdkZ2doZmQjVnksdnjfn="
}
```

GET /pki/keystoreAliases

This method returns all the keystore aliases based on the GOST cryptography.

Answer example

```
{
  [
    "3Mq9crNkTFf8oRPyisgtf4TjBvZxo4BL2ax",
    "e19a135e-11f7-4f0c-9109-a3d1c09812e3"
  ]
}
```

POST /pki/verify

This method checks the detached digital signature for the sent data. The `extendedKeyUsageList` is optional and may contain an array of object identifiers - OID. It is useful for the determination of the scope of the certificate. Any node with query parameters can check the certificate.

Request example

```
{
  "inputData" : "SGVsbG8gd29ybGGQh",
  "signature" : "c2RmZ3NkZmZoZ2ZkZ2hmZGpkZ2ZoamhnZmtqaGdmamtKZmdoZmdkc2doZmQ=",
  "sigType" : "CAAdES_X_Long_Type_1",
  "extendedKeyUsageList": [
    "1.2.643.7.1.1.1.1",
    "1.2.643.2.2.35.2"
  ]
}
```

Answer example

```
{
  "sigStatus" : "true"
}
```

Working with POST /pki/verify method

Using API `Post /pki/verify` method you can verify qualified digital signature. You need to install the root certificate on the node for proper using of API `Post /pki/verify`. The CA root certificate uniquely identifies the certification authority and is the basis in the chain of trust.

How to install a root certificate on a node

The root certificate is installing into the following Java directory:

```
-keystore /Library/Java/JavaVirtualMachines/jdk1.8.0_191.jdk/Contents/Home/jre/lib/
↔security/cacerts
```

The default password for the Java cacerts certificate store is `changeit`. You can change the password if you wish. Install certificates using the following command:

```
sudo keytool -import -alias testAliasCA_cryptopro -keystore /Library/Java/
↳JavaVirtualMachines/jdk1.8.0_191.jdk/Contents/Home/jre/lib/security/cacerts -file ~/
↳Downloads/cert.cer
```

20.1.17 Privacy

Hint: Rules of the creating requests to a node, see *How to use REST API* section.

POST /privacy/sendData

Writing the confidential data to the node store.

Method request:

```
{
  "sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUgEytUUz",
  "password": "apgJP9atQccdBPA",
  "policyId": "4gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaC",
  "type": "file",
  "info": {
    "filename": "Service contract #100/5.doc",
    "size": 2048,
    "timestamp": 1000000000,
    "author": "AIvanov@org.com",
    "comment": "some comments"
  },
  "data":
  ↳"TWFuIGlzIGRpc3Rpbmd1aXNoZWQsIG5vdCBvbmx5IGJ5IGhpcyByZWZzb24sIGJ1dCBieSB0aGlzIHNpbmd1bGFyIHBhc3Npb24gZnJvbSBvdGhl",
  ↳",
  "hash": "FRog42mzTA292ukng6PHoEK9Mpx9GZnrEHe cf vpwmta"
}
```

Parameters:

- sender - blockchain address for data broadcast (corresponds the “privacy.owner-address” parameter value in the node configuration file);
- password - access password to the private key of the node keystore;
- policyId - the group ID managing data forwarding;
- type - the type of the data;
- info - the information about the data;
- data - binary data;
- hash - data hash.

Method answer:

```
{
  "senderPublicKey": "Gt3o1ghh2M2TS65UrHZCTJ82LLcMcBrxuaJyrgrLk5VY",
  "policyId": "4gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaC",
```

(continues on next page)

(continued from previous page)

```

"sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUgEytUUz",
"dataHash": "FRog42mmzTA292ukng6PHoEK9Mpx9GZnrEHecfvpwmta",
"proofs": [
"2jM4tw4uDmspuXUBt6492T7opuZskYhFGW9gkbq532BvLYRF6RJn3hVGNLuMLK8JSM61GkVgYvYJg9UscAayEYfc"
],
"fee": 110000000,
"id": "H3bdFTatppjnMmUe38YWh35Lmf4XDYrgsDK1P3KgQ5aa",
"type": 114,
"timestamp": 1571043910570
}

```

GET /privacy/{policy-id}/recipients

Getting all addresses of participants, signed to the access group {policy-id}.

Method answer:

```

[
"3NBVqYXrapgJP9atQccdBPAgJPwHDKkh6A8",
"3Mx2afTZ2KbRrLNbytyzTtXukZvqEB8SkW7"
]

```

GET /privacy/{policy-id}/getHashes

Getting all addresses of participants, signed to the access group {policy-id}.

Method answer:

```

[
"3GCFaCWtvLDnC9yX29YftMbn75gwf dwGsBn",
"3GGxcmNyq8ZAHzK7or14Ma84khW8peBohJ",
"3GRLFi4rz3SniCuC7rbd9UuD2KUZyNh84pn",
"3GKpShrQRtdF1yYhQ58ZnKMTnp2xdEzKqW"
]

```

GET /privacy/{policy-id}/getHashes

Getting the array of identified hashes which are written with association to the {policy-id}.

Method answer:

```

[
"FdfdNBVqYXrapgJP9atQccdBPAgJPwHDKkh6A8",
"eedfdNBVqYXrapgJP9atQccdBPAgJPwHDKkh6A"
]

```

GET /privacy/{policyId}/getData/{policyItemHash}

Getting the confidential data package by its identified hash.

Method answer:

```
c29tZV9iYXN1NjRfZW5jb2RlZF9zdHJpbmc=
```

GET /privacy/{policyId}/getInfo/{policyItemHash}

Getting the metadata for the confidential data package by the identified hash.

Method answer:

```
{
  "sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUgEytUUz",
  "policy": "4gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaC",
  "type": "file",
  "info": {
    "filename": "Contract №100/5.doc",
    "size": 2048,
    "timestamp": 1000000000,
    "author": "AIvanov@org.com",
    "comment": "Comment"
  },
  "hash": "e67ad392ab4d933f39d5723aeed96c18c491140e119d590103e7fd6de15623f1"
}
```

POST /privacy/forceSync

Forced getting the confidential data package by the identified hash.

Method answer:

```
{
  "result": "success" // or "error"
  "message": "Address '3NBVqYXrapgJP9atQccdBPAgJPwHDKkh6A8' not in policy 'policyName'"
}
```

POST /privacy/getInfos

Getting the meta information array about private data according with the provided group ID and data hash.

Request example:

```
{ "policiesDataHashes":
  [
    {
      "policyId": "somepolicyId_1",
      "datahashes": [ "datahash_1","datahash_2" ]
    },
    {
      "policyId": "somepolicyId_2",
      "datahashes": [ "datahash_3","datahash_4" ]
    }
  ]
}
```

(continues on next page)

(continued from previous page)

```
]
}
```

Method answer:

```
{
  "policiesDataInfo": [
    {
      "policyId": "somepolicyId_1",
      "datasInfo": [
        {
          "hash": "e67ad392ab4d933f39d5723aeed96c18c491140e119d590103e7fd6de15623f1",
          "sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUgEytUUz",
          "type": "file",
          "info": {
            "filename": "Contract №100/5.doc",
            "size": 2048,
            "timestamp": 1000000000,
            "author": "AIvanov@org.com",
            "comment": "Comment"
          }
        },
        {
          "hash": "e67ad392ab4d933f39d5723aeed96c18c491140e119d590103e7fd6de15623f1",
          "sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUgEytUUz",
          "type": "file",
          "info": {
            "filename": "Contract №101/5.doc",
            "size": "2048",
            "timestamp": 1000000000,
            "author": "AIvanov@org.com",
            "comment": "Comment"
          }
        }
      ]
    }
  ]
}
```

20.1.18 Transactions

Hint: The rules for generating node queries are given in module *How to use REST API*.

GET /transactions/info/{id}

Query transaction information by its ID.

Query Parameters:

```
"id" - Transaction ID
```

Method Response:

```
{
  "type": 4,
  "id": "52GG9U2e6foYRkp5vAzsTQ86aDAABfRj7synz7ohBp19",
  "sender": "3NBVqYXrapgJP9atQccdBPagJPwHDKkh6A8",
  "senderPublicKey": "CRxqEuxhdZBEHX42MU4FfyJxuHmbDBTaHmM3Uki7pLw",
  "recipient": "3NBVqYXrapgJP9atQccdBPagJPwHDKkh6A8",
  "assetId": "E9yZC4cVhCDfbjFJCc9CqkAtkoFy5KaCe64iaxHM2adG",
  "amount": 100000,
  "fee": 100000,
  "timestamp": 1549365736923,
  "attachment": "string",
  "signature":
  ↪ "GknccUA79dBcwWgKjqB7vYHcnsj7caYETfncJhRkkaetbQon7DxbpMmvK9LYqUkirJp17geBJCRTNkHEoAjtSUm",
  "height": 7782
}
```

GET /transactions/address/{address}/limit/{limit}

Returns latest {limit} transactions from address {address}.

Method Response:

```
[
  [
    {
      "type": 2,
      "id":
      ↪ "4XE4M9eSoVWVdHwDYXqZsXhEc4q8PH9mDMUBegCSBBVHJyP2Yb1ZoGi59c1Qzq2TowLmymLNkFqjWp95CddnyBW",
      "fee": 100000,
      "timestamp": 1549365736923,
      "signature":
      ↪ "4XE4M9eSoVWVdHwDYXqZsXhEc4q8PH9mDMUBegCSBBVHJyP2Yb1ZoGi59c1Qzq2TowLmymLNkFqjWp95CddnyBW",
      "sender": "3NBVqYXrapgJP9atQccdBPagJPwHDKkh6A8",
      "senderPublicKey": "CRxqEuxhdZBEHX42MU4FfyJxuHmbDBTaHmM3Uki7pLw",
      "recipient": "3N9iRMou3pgmyPbFZn5QZQvBTQBkL2fR6R1",
      "amount": 1000000000
    }
  ]
]
```

GET /transactions/unconfirmed

Returns all unconfirmed transactions from node utx-pool.

Method Response:

```
[
  {
    "type": 4,
    "id": "52GG9U2e6foYRKp5vAzsTQ86aDAABfRJ7synz7ohBp19",
    "sender": "3NBVqYXrapgJP9atQccdBPAGJPwHDKkh6A8",
    "senderPublicKey": "CRxqEuxhdZBEHX42MU4FfyJxuHmbDBTaHmM3Uki7pLw",
    "recipient": "3NBVqYXrapgJP9atQccdBPAGJPwHDKkh6A8",
    "assetId": "E9yZC4cVhCDfbjFJCc9CqkAtkoFy5KaCe64iaxHM2adG",
    "amount": 100000,
    "fee": 100000,
    "timestamp": 1549365736923,
    "attachment": "string",
    "signature":
    ↪ "GknccUA79dBcwWgKjqB7vYHcnsj7caYETfncJhRkkaetbQon7DxbpMmvK9LYqUkirJp17geBJCRTNkHEoA jtsUm"
  }
]
```

GET /transactions/unconfirmed/size

Return the number of transactions available in UTX pool.

GET /unconfirmed/info/{id}

Query transaction details from UTX pool by its ID.

POST /transactions/calculateFee

Calculates fee amount for transferred transaction.

Query Parameters

```
"type" - Transaction type
"senderPublicKey" - Public key of sender
"sender" is ignored
"fee" is ignored
and all the other parameters appropriate for a transaction of the given type.
```

Method Query

```
{
  "type": 10,
  "timestamp": 1549365736923,
  "sender": "3MtrNP7AkTRuBhX4CBti6iT21pQpEnmHtyw",
  "alias": "ALIAS",
}
```

or

```
{
  "type": 4,
  "sender": "3MtrNP7AkTRuBhX4CBti6iT21pQpEnmHtyw",
  "recipient": "3P8JYPHrnXSfsWP1LVXySdzU1P83FE1ssDa",
  "amount": 1317209272,
  "feeAssetId": "8LQW8f7P5d5PZM7GtZEBgaqRPGSszS3DfPuiXrURJ4AJS",
  "attachment": "string"
}
```

Method Response

```
{
  "feeAssetId": null,
  "feeAmount": 10000
}
```

or

```
{
  "feeAssetId": "8LQW8f7P5d5PZM7GtZEBgaqRPGSszS3DfPuiXrURJ4AJS",
  "feeAmount": 10000
}
```

POST /transactions/sign

Signs a transaction with sender's private key stored in node keystore. After signing, method response must be sent to method input *Broadcast*.

It is necessary to enter the password into the `password` field in order to sign requests with the key from keystore node.

Sample queries

| ID | Transaction type |
|-----|--|
| 3 | <i>Issue</i> |
| 4 | <i>Transfer</i> |
| 5 | Reissue |
| 6 | Burn |
| 7 | Exchange |
| 8 | Lease |
| 9 | Lease Cancel |
| 10 | <i>Alias</i> |
| 11 | Mass Transfer |
| 12 | <i>Data</i> |
| 13 | <i>Set Script</i> |
| 14 | Sponsorship |
| 101 | Permission (for Genesis block) |
| 102 | <i>PermissionTransaction</i> |
| 103 | <i>CreateContractTransaction</i> |
| 104 | <i>CallContractTransaction</i> |
| 105 | <i>ExecutedContractTransaction</i> |
| 106 | <i>DisableContractTransaction</i> |
| 107 | <i>UpdateContractTransaction</i> |
| 110 | <i>GenesisRegisterNode Transaction</i> |
| 111 | <i>RegisterNode Transaction</i> |
| 112 | <i>CreatePolicy Transaction</i> |
| 113 | <i>UpdatePolicy Transaction</i> |
| 114 | <i>PolicyDataHash Transaction</i> |

3. Issue

```
{
  "type": 3,
  "version": 2,
  "name": "Test Asset 1",
  "quantity": 100000000000,
  "description": "Some description",
  "sender": "3FSCKyfFo3566zwiJjsFLBwKvd826KXUaqR",
  "decimals": 8,
  "reissuable": true,
  "fee": 100000000
}
```

4. Transfer

```
{
  "type": 4,
  "version": 2,
  "sender": "3M6dRZXaJY9oMA3fJKhMALyYKt13D1aimZX",
  "password": "",
  "recipient": "3M6dRZXaJY9oMA3fJKhMALyYKt13D1aimZX",
  "amount": 40000000000,
  "fee": 100000
}
```

10. Alias

```
{
  "type": 10,
  "version": 2,
  "fee": 100000,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "alias": "hodler"
}
```

12. Data

```
{
  "type": 12,
  "version": 1,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "senderPublicKey": "Fbt5fKHesnQG2CXmsKf4TC8v9oB7bsy2AY56CUopa6H3",
  "author": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "data":
  [
    {
      "key": "objectId",
      "type": "string",
      "value": "obj:123:1234"
    }
  ],
  "fee": 100000
}
```

13. Set Script

```
{
  "type": 13,
  "version": 1,
  "sender": "3N9vL3apA4j2L5PojHW8TYmfHx9Lo2ZaKPB",
  "fee": 1000000,
  "name": "faucet",
  "script": "base64:AQQAAAAHJG1hdGNoMAUAAAAcDHgG+RXSszQ=="
}

.. _tx-sponsorship:
```

14. Sponsorship

```
{
  "sender": "3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t",
  "assetId": "G16FvJk9vabwxjQswh9CQAhbZzn3QrwwjwnZB3qNVox",
  "fee": 100000000,
  "isEnabled": false,
  "type": 14,
  "password": "1234",
  "version": 1
}
```

102. PermissionTransaction

Sample query

```
{
  "type": 102,
```

(continues on next page)

(continued from previous page)

```

"sender": "3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG",
"senderPublicKey": "4WnvQPit2DiliYXDgDcXnJZ5yroKW54vauNoxdNeMi2g",
"fee": 0,
"proofs": [],
"target": "3GPtj5osoYqHpyfmsFv7BMiyKsVzbG1ykfL",
"opType": "add",
"role": "contract_developer",
"dueTimestamp": null
}

```

103. CreateContractTransaction

Sample query

```

{
  "fee": 100000000,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "sender": "3PudkbvjV1nPj1TkuuRahh4sGdgfr4YAUUV2",
  "password": "",
  "params": [],
  "type": 103,
  "version": 1,
}

```

Sample response

```

{
  "type": 103,
  "id": "ULcq9R7PvUB2yPmrmBdxoTi3bcRmQPT3JDLZZVj4Ky",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skQdsjMVT2M",
  "fee": 500000,
  "timestamp": 1550591678479,
  "proofs": [
    ↪ "yeCRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
  "version": 1,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "params": [],
  "height": 1619
}

```

104. CallContractTransaction

Sample query

```

{
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "fee": 10,
  "sender": "3PKyW5F5Sn4fmdrLcUnDMRHVyoDBxybRgP58",
  "type": 104,
  "version": 1,
  "contractVersion": 1,
  "password": "",
}

```

(continues on next page)

(continued from previous page)

```

"params": [
  {
    "type": "integer",
    "key": "a",
    "value": 1
  },
  {
    "type": "integer",
    "key": "b",
    "value": 100
  }
]
}

```

Sample response

```

{
  "type": 104,
  "id": "9fBrL2n5TN473g1gNfoZqaAqAsAJCuHRHYxZpLexL3VP",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVLRqLCqouVrFZynjfotEuPNV9GrdauNpgdWXLsq",
  "fee": 10,
  "timestamp": 1549365736923,
  "proofs": [
    "2q4cTBhdKEDkFxr7iYaHPAv1dzaKo5rDaTxPF5VHryyYTXxTPvN9Wb3YrsDYixKiUPXBnAyXzEcnKPFRCW9xVp4v"
  ],
  "version": 1,
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "params": [
    {
      "key": "a",
      "type": "integer",
      "value": 1
    },
    {
      "key": "b",
      "type": "integer",
      "value": 100
    }
  ]
}

```

105. ExecutedContractTransaction

Sample response

```

{
  "type": 105,
  "id": "2UAHvs4KsfBbRVPm2dCigWtqUHuanQou83CXy6DGDiRa",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVLRqLCqouVrFZynjfotEuPNV9GrdauNpgdWXLsq",
  "fee": 500000,
  "timestamp": 1549365523980,
  "proofs": [
    "4BoG6wQnYyZWYUKzAwh5n1184tsEWUqUTWmXMExvvcU95xgk4UFB8iCnHJ4GhvJm86REB69hKM7s2WLAwTSXquAs"
  ],
}

```

(continues on next page)

(continued from previous page)

```

"version": 1,
"tx": {
  "type": 103,
  "id": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVLrqlCqouVrFZynjfoTEuPNV9GrdauNpgdWXLsq",
  "fee": 500000,
  "timestamp": 1549365501462,
  "proofs": [
    "2ZK1Y1ecfQXeWsS5sfcTLM5W1KA3kwi9Up2H7z3Q6yVzMeGxT9xWJT6jREQsmuDBcvk3DCCiWBdFHaxazU8pbo41"
  ],
  "version": 1,
  "image": "localhost:5000/contract256",
  "imageHash": "930d18dacb4f49e07e2637a62115510f045da55ca16b9c7c503486828641d662",
  "params": []
},
"results": []
}

```

106. DisableContractTransaction

Sample query

```

{
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "password": "",
  "contractId": "Fz3wqAWwCpMT4M1q6H7crLKtToFJvbeLSvqjaU4ZwMpg",
  "fee": 500000,
  "type": 106
}

```

Sample response

```

{
  "type": 106,
  "id": "8Nw34YbosEVhCx18pd81HqYac4C2pGjyLKck8NhSoGYH",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPc59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
  "fee": 500000,
  "proofs": [
    "5GqPQkuRvG6LPXgPoCr9FogAdmhAaMbyFb5UfjQPUKdSc6BLuQsZ75LAWix1ok2Z6PC5ezPpjzqznr15i3RQmaEc"
  ],
  "version": 1,
  "contractId": "Fz3wqAWwCpMT4M1q6H7crLKtToFJvbeLSvqjaU4ZwMpg",
  "height": 1632
}

```

107. UpdateContractTransaction

Sample query

```

{
  "image" : "registry.wvservices.com/we-sc/tdm-increment3:1028.1",
  "sender" : "3Mxxz9pBYS5fJMARJNQmzYUHxiWAtvMzSRT",
  "password": "",
  "fee" : 100000000,
  "contractId" : "EnsihTUHSNAB9RcWXJbiWT98X3hYtCw3SBzK8nHQRcWA",
  "imageHash" : "0e5d280b9acf6efd8000184ad008757bb967b5266e9ebf476031fad1488c86a3",
}

```

(continues on next page)

(continued from previous page)

```

"type" : 107,
"version" : 1
}

```

Sample response

```

{
  "senderPublicKey":
  ↪ "5qBRDm74WKR5xK7LPs8vCy9QjzzqK4KCb8PL36fm55S3kEi2XZETHFgMgp3D13AwgE8bBkYrzvEvQZuabMfEyJwW",
  "tx":
  {
    "senderPublicKey":
    ↪ "5qBRDm74WKR5xK7LPs8vCy9QjzzqK4KCb8PL36fm55S3kEi2XZETHFgMgp3D13AwgE8bBkYrzvEvQZuabMfEyJwW",
    "image": "registry.wvservices.com/we-sc/tdm-increment3:1028.1",
    "sender": "3Mxxz9pBYS5fJMARJNQmzYUHxiWAtvMzSRT",
    "proofs": [
    ↪ "3tNsTyteeZrxEbVsv5zPT6dr247nXsVWR5v7Khx8spypgZQUdorCQZV2guTomutUTcyxhJUjNkQW4VmSgbCtgm1Z"],
    "fee": 0,
    "contractId": "EnsihTUHSNAB9RcWXJbiWT98X3hYtCw3SBzK8nHQRCWA",
    "id": "HdZdhXVveMT1vYzGTviCoGQU3aH6ZS3YtFpYujWeGCH6",
    "imageHash": "17d72ca20bf9393eb4f4496fa2b8aa002e851908b77af1d5db6abc9b8eae0217",
    "type": 107, "version": 1, "timestamp": 1572355661572},
    "sender": "3HfRBedCpWi3vEzFSKEZDFXkyNwbWLWQmmG",
    "proofs": [
    ↪ "28ADV8miUVN5EFjhqeFj6MADSXYjbxA3TsxSvFVs18jXAsHVAbczvnyoUSaYJsjrNmaWgXbpbduccRxpKGTs6tro"],
    "fee": 0, "id": "7niVY8mjzeKqLBePvhTxFRfLu7BmcwVfqaqtbWAN8AA2",
    "type": 105,
    "version": 1,
    "results": [],
    "timestamp": 1572355666866
  }
}

```

110. GenesisRegisterNode

Sample query

```

{
  "type": 110,
  "id": "2Xgbsqgfbp5fiq4nsaAoTkQsXc399tXdnKom8prEZqPW2Q7xZKNKCCqpkymtmJMgYLPvwybnxHPTFPFEfFdyLpJ",
  "fee": 0,
  "timestamp": 1489352400000,
  "signature":
  ↪ "2Xgbsqgfbp5fiq4nsaAoTkQsXc399tXdnKom8prEZqPW2Q7xZKNKCCqpkymtmJMgYLPvwybnxHPTFPFEfFdyLpJ",
  "targetPublicKey": "3JNLQYuHYSHZiHr5KjJ89wwFJpDMdrAEJpj",
  "target": "3JNLQYuHYSHZiHr5KjJ89wwFJpDMdrAEJpj"
}

```

Sample response

```

{
  "signature":
  ↪ "2Xgbsqgfbp5fiq4nsaAoTkQsXc399tXdnKom8prEZqPW2Q7xZKNKCCqpkymtmJMgYLPvwybnxHPTFPFEfFdyLpJ",
  "fee": 0,
  "id": "2Xgbsqgfbp5fiq4nsaAoTkQsXc399tXdnKom8prEZqPW2Q7xZKNKCCqpkymtmJMgYLPvwybnxHPTFPFEfFdyLpJ",
  "type": 110,
  "targetPublicKey": "3JNLQYuHYSHZiHr5KjJ89wwFJpDMdrAEJpj",
}

```

(continues on next page)

(continued from previous page)

```

    "timestamp": 1489352400000,
    "target": "3JNLQYUHYSHZiHr5KjJ89wwFJpDMdrAEJpj",
    "height": 1
}

```

111. RegisterNode

Sample query

```

{
  "type": 111,
  "opType": "add",
  "sender": "3HYW75PpAeVukmbYo9PQ3mzSHdKUGeytUUz",
  "password": "",
  "targetPubKey": "apgJP9atQccdBPAGJPwH3NBVqYXrapgJP9atQccdBPAGJPwHapgJP9atQccdBPAGJPwHDKkh6A8",
  "nodeName": "Node #1",
  "fee": 500000,
}

```

112. CreatePolicy

Sample query

```

{
  "sender": "3NkZd8Xd4KsuPiNVsuphRNCZE3SsqJycqv8d",
  "policyName": "Policy# 7777",
  "password": "sfgKYBFCF@#$fsdf()*%",
  "recipients": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SsqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T",
    "3NtNJV44wvxRXv2jyW3yXLxjJxvY1vR88TF",
    "3NxAooHUoLsAQvxBSqjE91WK3LwWGjiiCxx"
  ],
  "fee": 15000000,
  "description": "Buy bitcoin by 1c",
  "owners": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SsqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T"
  ],
  "type": 112
}

```

113. UpdatePolicy

Sample query

```

{
  "policyId": "7wphGbhqbmUgzun5wzggwqtViTiMdFezSa11fxrV58Lm",
  "password": "sfgKYBFCF@#$fsdf()*%",
  "sender": "3NkZd8Xd4KsuPiNVsuphRNCZE3SsqJycqv8d",
  "proofs": [],
  "recipients": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SsqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T",
  ]
}

```

(continues on next page)

(continued from previous page)

```

        "3NtNJV44wyxRXv2jyW3yXLxjJxvY1vR88TF",
        "3NxAoHULsAQvxBSqjE91WK3LwWGjiiCxx",
        "3NwJfjG5RpaDfxEhkwXgwd7oX21NMFCxJHL"
    ],
    "fee": 15000000,
    "opType": "add",
    "owners": [
        "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
        "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
        "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T"
    ],
    "type": 113,
}

```

114. PolicyDataHash

When a user sends confidential data to the network using the *POST /privacy/sendData* method, the node automatically generates the 114 transaction.

POST /transactions/broadcast

Sends a signed transaction to blockchain.

Method Query

```

{
  "type": 10,
  "senderPublicKey": "G6h72icCSjdW2A89QWDb37hyXJoYKq3XuCUJY2joS3EU",
  "fee": 100000000,
  "timestamp": 1550591678479,
  "signature":
  ↪ "4gQyPXzJFEzMbsCd9u5n3B2WauEc4172ssyrXCL882oNa8NfNihnpKianHXrHwnZs1RzDLbQ9rcRYnSqxKWfEPJG",
  "alias": "dajzmj6gfuzmbfnhamsbuxivc"
}

```

Method Response

```

{
  "type": 10,
  "id": "9q7X84wFuVvKqrdDQeWbtBmpsHt9SXFbvPPtUuKBVxxr",
  "sender": "3MtrNP7AkTRuBhX4CBti6iT21pQpEnmHtyw",
  "senderPublicKey": "G6h72icCSjdW2A89QWDb37hyXJoYKq3XuCUJY2joS3EU",
  "fee": 100000000,
  "timestamp": 1550591678479,
  "signature":
  ↪ "4gQyPXzJFEzMbsCd9u5n3B2WauEc4172ssyrXCL882oNa8NfNihnpKianHXrHwnZs1RzDLbQ9rcRYnSqxKWfEPJG",
  "alias": "dajzmj6gfuzmbfnhamsbuxivc"
}

```

POST /transactions/signAndBroadcast

Signs and sends a signed transaction to the blockchain.

Method Query

```
{
  "sender": "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
  "policyName": "Policy# 7777",
  "password": "sfgKYBFCF@#$fsdf()*%",
  "recipients": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T",
    "3NtNJV44wyxRXv2jyW3yXLxjJxvY1vR88TF",
    "3NxAoohUoLsAQvxBSqjE91WK3LwWGjiiCxx"
  ],
  "fee": 15000000,
  "description": "Buy bitcoin by 1c",
  "owners": [
    "3NkZd8Xd4KsuPiNVsuphRNCZE3SqJycqv8d",
    "3NotQaBygbSvYZW4ftJ2ZwLXex4rTHY1Qzn",
    "3Nm84ERiJqKfuqSYxzMAhaJXdj2ugA7Ve7T"
  ],
  "type": 112
}
```

Method Response

```
{
  "senderPublicKey": "3X6Qb6p96dY4drVt3x4XyHKCRvree4QDqNZyDWHzjJ79",
  "policyName": "Policy for sponsored v1",
  "fee": 100000000,
  "description": "Privacy for sponsored",
  "owners": [
    "3JSaKNX94deXJkywQwTFgbigTxJa36TDVg3",
    "3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t"
  ],
  "type": 112,
  "version": 2,
  "sender": "3JSaKNX94deXJkywQwTFgbigTxJa36TDVg3",
  "feeAssetId": "G16FvJk9vabwxjQswh9CQAhbZzn3QrwwjwnZB3qNVox",
  "proofs": [
    "3vDVjpb6UJeN9ahtNcQwt5WDVqC9KqdEsrr9HTToHfoXFd1HtVwnUPPtJKM8tAsCtby81XYQReLj33hLEZ8qbGA3V"
  ],
  "recipients": [
    "3JSaKNX94deXJkywQwTFgbigTxJa36TDVg3",
    "3JWDUsqyJEkVa1aivNPP8VCAa5zGuxiwD9t"
  ],
  "id": "EyyzmQcM2LrsgGDFFeGn8DhahJbFYmorcBrEh8phv5S",
  "timestamp": 1585307711344
}
```

20.1.19 Utils

Hint: The rules for generating queries to the node are given in module *How to use REST API*.

POST /utils/hash/secure

Returns secure (double) hash of specified message.

Method query:

```
ridethewaves!
```

Method response:

```
{
  "message": "ridethewaves!",
  "hash": "H6nsiifwYKYEx6YzYD7woP1XCn72RVvx6tC1zjjLXqsu"
}
```

POST /utils/hash/fast

Returns hash of specified message.

Method query:

```
ridethewaves!
```

Method response:

```
{
  "message": "ridethewaves!",
  "hash": "DJ35ymschUFDmqCnDJewjcnVExVkWgX7mJDXhFy9X8oQ"
}
```

POST /utils/script/compile

Response parameters:

```
"script" - Base64 script
"complexity" - script complexity
"extraFee" - the fee for outgoing transactions set by the script
```

Method query:

```
let x = 1
(x + 1) == 2
```

Method response:


```
{
  "script":
  ↪ "3rbFDtbPwAvSp2vBvqGfGR9nRS1nBVnfuSCN3HxSZ7fVRpt3tuFG5JSmyTmvHPxYf34So cMRkRKFgzTtXXnnv7upRHXJzZrLSQo8tUW6yMtEiZ
  ↪",
  "complexity": 11,
  "extraFee": 10001
}
```

or

Method query:

```
x == 1
```

Method response:

```
{
  "error": "Typecheck failed: A definition of 'x' is not found"
}
```

POST /utils/script/estimate

Decoding base64 script.

Method query:

```
AQQAAAAABeAAAAAAAAAAAAAQkAAAAAAAAACCQAAZAAAAAIFAAAAAXgAAAAAAAAAAAAEAAAAAAAAAAAAJdecYi
```

Method response:

```
{
  "script":
  ↪ "3rbFDtbPwAvSp2vBvqGfGR9nRS1nBVnfuSCN3HxSZ7fVRpt3tuFG5JSmyTmvHPxYf34So cMRkRKFgzTtXXnnv7upRHXJzZrLSQo8tUW6yMtEiZ
  ↪",
  "scriptText": "FUNCTION_CALL(FunctionHeader(=,List(LONG, LONG)),List(CONST_LONG(1), CONST_
  ↪LONG(2)),BOOLEAN)",
  "complexity": 11,
  "extraFee": 10001
}
```

GET /utils/time

Returns current node time.

Method response:

```
{
  "system": 1544715343390,
  "NTP": 1544715343390
}
```


POST /utils/reload-wallet

Reloads node keystore. Runs if new key pair was created in keystore without restarting node.

Method response:

```
{
  "message": "Wallet reloaded successfully"
}
```

20.2 Authorization service REST API methods

You can read more about working with REST API in *this* section. The authorization service REST API methods are accessed via HTTPS protocol. Methods are closed by authorization and are marked with the  icon.

20.2.1 GET /status

Getting the authorization service status.

Method answer

```
{
  "status": "OK"
}
```

20.2.2 POST /v1/user

Registering a new user.

Method request

```
{
  "username": "string",
  "password": "string",
  "locale": "string"
}
```

Method answer

```
{
  "access_token": "string",
  "refresh_token": "string",
  "token_type": "string"
}
```

20.2.3 GET /v1/user/profile



Getting user data.

Method answer

```
{
  "id": "string",
  "name": "string",
  "locale": "en",
  "addresses": [
    "string"
  ],
  "roles": [
    "string"
  ]
}
```

20.2.4 POST /v1/user/address



Getting an user address.

Method request

```
{
  "address": "string",
  "type": "string"
}
```

Method answer

```
{
  "addressId": "string"
}
```

20.2.5 GET /v1/user/doesEmailExist

Checking an user email address.

Method answer

```
{
  "exist": true
}
```

20.2.6 POST /v1/user/password/restore

Restoring an user account password.

Method request

```
{
  "email": "string"
}
```

Method answer

```
{
  "email": "string"
}
```

20.2.7 POST /v1/user/password/reset

Resetting an user password.

Method request

```
{
  "token": "string",
  "password": "string"
}
```

Method answer

```
{
  "userId": "string"
}
```

20.2.8 GET /v1/user/confirm/{code}

Entering a confirmation code to reset an user account password.

20.2.9 POST /v1/user/resendEmail

Resending a password recovery code to the specified email address.

Method request

```
{
  "email": "string"
}
```

Method answer

```
{
  "email": "string"
}
```

20.2.10 POST /v1/auth/login

Registering a new user in the authorization service.

Method request

```
{
  "username": "string",
  "password": "string",
  "locale": "string"
}
```

Method answer

```
{
  "access_token": "string",
  "refresh_token": "string",
  "token_type": "string"
}
```

20.2.11 POST /v1/auth/token



Registering external services and applications in the authorization service.

Method request

```
{
  "token": "string"
}
```

Method answer

```
{
  "access_token": "string",
  "refresh_token": "string",
  "token_type": "string"
}
```

20.2.12 POST /v1/auth/refresh

Getting a new refresh token.

Method request

```
{
  "token": "string"
}
```

Method answer

```
{
  "access_token": "string",
  "refresh_token": "string",
  "token_type": "string"
}
```

20.2.13 GET /v1/auth/publicKey

Getting the authorization service public key.

Method answer

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA7d90j/ZQTkkjf4UuMfUu
QIFDTYxYf6QBKMVJnq/wXyPYYkV8HVFFyzCaEciv3CXmBH77sXnuTlrEtV7zHB
KvV870HmZuazjIgzVSk0n0Y7F8UUUVNxn1zVD1dPs0GJ6orM41DnC1W65mCrP3bjn
fV4RbmykN/lk7McA6EsMcLEGbKkFhmeq2Nk4hn2CQvoTkupJU0CP1dh04bq1lQ7
Ffj9K/FJq73wSXDoH+qqdRG9sfrtgrhtJHerruhv3456eOzyAcD08+sJUQFKY8OB
SZMEndVzFS2ub9Q8e7BfcNxmTmQPM4PhH05wuTqL32qt3uJBx20I41u30ND44ZrDJ
BbVog73oPjRYXj+kTbwUZI66SP4aLcQ8sypQyLwqKk5DtLRozSN00IrupJJ/pwZs
9zPEggL91T0rirbEhG1f5U8/6XN8GVXX4iMk2fD8FHLFJuXCD70j4JC2iWfFDC6a
uUkwUfqfjJB8BzIHkncoq0ZbpidEE21TW1+svuEu/wyP5rN1yMiE/e/fZQqM2+o0
cH5Qow6HH35BrloCSZciutUcd1U7YPqESJ5tryy1xn9bsMb+On1ocZTtvec/ow4M
RmnJwm0j1nd+cc19OKLG5/boeA+2zqWu0jCbWR9c0oCmgbhucZChaHTBEAKDwCsC
VRz5qD6FPpePpTQDb6ss3bkCAwEAAQ==
-----END PUBLIC KEY-----
```

20.3 REST API methods for the data service

20.3.1 Transactions

GET /transactions

Returns a list of transactions matching the search query criteria and filters applied.

Important: It is returned a maximum of 500 transactions for the API `GET /transactions` method request.

Method Response:

```
[
  {
    "id": "string",
    "type": 0,
    "height": 0,
    "fee": 0,
    "sender": "string",
    "senderPublicKey": "string",
    "signature": "string",
    "timestamp": 0,
    "version": 0
  }
]
```

(continues on next page)

(continued from previous page)

```
}
]
```

GET /transactions/count

Returns the number of transactions matching the search query criteria and filters applied.

Method Response:

```
{
  "count": "string"
}
```

GET /transactions/id/{id}

Returns transaction by ID {id}.

Method Response:

```
{
  "id": "string",
  "type": 0,
  "height": 0,
  "fee": 0,
  "sender": "string",
  "senderPublicKey": "string",
  "signature": "string",
  "timestamp": 0,
  "version": 0
}
```

20.3.2 Token assets

GET /assets

Returns a list of token assets available in the blockchain (as token issue transactions).

Method Response:

```
[
  {
    "id": "string",
    "type": 0,
    "height": 0,
    "fee": 0,
    "sender": "string",
    "senderPublicKey": "string",
    "signature": "string",
    "timestamp": 0,
    "version": 0,
    "assetId": "string",
    "name": "string",

```

(continues on next page)

(continued from previous page)

```

    "description": "string",
    "quantity": 0,
    "decimals": 0,
    "reissuable": true
  }
]

```

20.3.3 Users

GET /users

Returns a list of users matching the search query criteria and filters applied.

Method Response:

```

[
  {
    "address": "string",
    "aliases": [
      "string"
    ],
    "registration_date": "string",
    "permissions": [
      "string"
    ],
    "balances": [
      {
        "assetId": "string",
        "amount": 0
      }
    ]
  }
]

```

GET /users/{userAddress}

Returns information about the user as per user's address.

Method Response:

```

{
  "address": "string",
  "aliases": [
    "string"
  ],
  "registration_date": "string",
  "permissions": [
    "string"
  ],
  "balances": [
    {
      "assetId": "string",
      "amount": 0
    }
  ]
}

```

(continues on next page)

(continued from previous page)

```
]
}
```

20.3.4 Blocks

GET /blocks/{height}

Returns the block at the specified height.

Method Response:

```
{
  "version": 0,
  "timestamp": 0,
  "reference": "string",
  "nxt-consensus": {
    "base-target": 0,
    "generation-signature": "string"
  },
  "features": [
    0
  ],
  "generator": "string",
  "signature": "string",
  "blocksize": 0,
  "transactionCount": 0,
  "fee": 0,
  "height": 0,
  "transactions": [
    {
      "id": "string",
      "type": 0,
      "height": 0,
      "fee": 0,
      "sender": "string",
      "senderPublicKey": "string",
      "signature": "string",
      "timestamp": 0,
      "version": 0
    }
  ]
}
```

20.3.5 Data transactions

GET /api/v1/txlds/{key}

Returns a list of data transaction ID's containing the specified key.

Method Response:

```
[
{
```

(continues on next page)

(continued from previous page)

```
[
  "id": "string"
]
```

GET /api/v1/txIds/{key}/{value}

Returns a list of data transaction ID's containing the specified key and value.

Method Response:

```
[
  {
    "id": "string"
  }
]
```

GET /api/v1/txData/{key}

Returns data transaction bodies containing the specified key.

Method Response:

```
[
  {
    "id": "string",
    "type": "string",
    "height": 0,
    "fee": 0,
    "sender": "string",
    "senderPublicKey": "string",
    "signature": "string",
    "timestamp": 0,
    "version": 0,
    "key": "string",
    "value": "string",
    "position_in_tx": 0
  }
]
```

GET /api/v1/txData/{key}/{value}

Returns data transaction bodies containing the specified key and value.

Method Response:

```
[
  {
    "id": "string",
    "type": "string",
    "height": 0,
    "fee": 0,
    "sender": "string",
    "senderPublicKey": "string",
```

(continues on next page)

(continued from previous page)

```

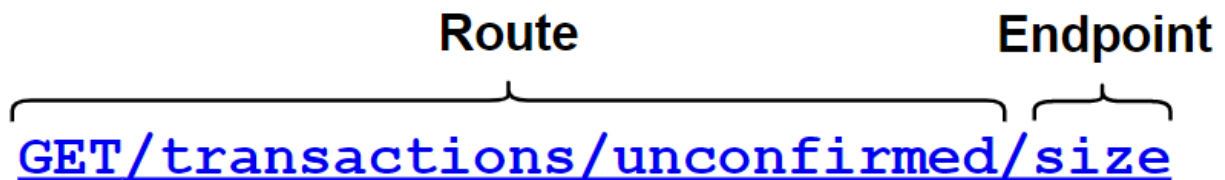
"signature": "string",
"timestamp": 0,
"version": 0,
"key": "string",
"value": "string",
"position_in_tx": 0
}
]

```

20.4 How to use REST API

All API methods are including GET, POST or DELETE HTTPS requests to URL <https://yournetwork.com/node-N/api-docs/swagger.json> using the set of parameters. The requests groups with routes and endpoints are selected in the Swagger interface. The route is the URL of the HTTP method, and the endpoint is the final part of the route, this is the access to the method. Example:

URL to the HTTP-method



For requests requiring the following actions, mandatory authorization by `api-key-hash` is required. The authorization type is specified in the node configuration file. If `api-key-hash` authorization type is selected, it is necessary to specify the value of the secret phrase, the hash of which is wrote in the node configuration file (`rest-api.api-key-hash` field).

- access to the node keystore (for example, sign method);
- access to operations with confidential data access groups;
- access to the node configuration.

When authorized by token, the value of `access` token is specified in the corresponding field. If token authorization is selected, then all REST API methods for node access are closed.

20.5 Authorization methods

Depending on the authorization method, different values are specified to get the access to the node REST API.

Available authorizations



OAuth2 Bearer (apiKey)

Name: Authorization

In: header

Value:

Authorize

Close

ApiKey or PrivacyApiKey (apiKey)

Name: X-API-Key

In: header

Value:

Authorize

Close

- OAuth2 Bearer (apiKey) - an **access** token value.
- ApiKey or PrivacyApiKey (apiKey) - **api-key-hash** value for both access to the node REST API and *privacy* methods.

20.5.1 api-key-hash authorization

The **api-key-hash** generation is happening during the *node configuration*. The value of the field **rest-api.api-key-hash** can be also generated using the */utils/hash/secure* method of node REST API. It is required to specify the access password to the keystore in the **password** field of the POST */transaction/sign* request for signing requests by the node keystore key.

Sample query:

```
curl -X POST
--header 'Content-Type: application/json'
--header 'Accept: application/json'
--header 'X-API-Key: 1' -d '1' 'http://2.testnet-pos.com:6862/transactions/calculateFee'
```

20.5.2 Token authorization

If the *authorization service* is used, the client receives a pair of tokens - **refresh** and **access** - for the node and other services access. Tokens can be obtained via the authorization service REST API.

DOCKER SMART-CONTRACTS

21.1 Smart contract run with REST API

Hint: Technical description of contracts implementation is given in module *Docker Smart Contracts*.

21.1.1 Description of program logic

This module reviews an example of how to create and run a simple smart contract. The contract performs increment the number transferred to the contract entry in *call-transactions*.

Program listing `contract.py` on Python:

```
import json
import os
import requests
import sys

def find_param_value(params, name):
    for param in params:
        if param['key'] == name: return param['value']
    return None

def print_success(results):
    print(json.dumps(results, separators=(',', ':')))

def print_error(message):
    print(message)
    sys.exit(3)

def get_value(contract_id):
    node = os.environ['NODE_API']
    if not node:
        print_error("Node REST API address is not defined")
    token = os.environ["API_TOKEN"]
    if not token:
        print_error("Node API token is not defined")
    headers = {'X-Contract-Api-Token': token}
```

(continues on next page)

(continued from previous page)

```

url = '{0}/internal/contracts/{1}/sum'.format(node, contract_id)
r = requests.get(url, verify=False, timeout=2, headers=headers)
data = r.json()
return data['value']

if __name__ == '__main__':
    command = os.environ['COMMAND']
    if command == 'CALL':
        contract_id = json.loads(os.environ['TX'])['contractId']
        value = get_value(contract_id)
        print_success([{"key": "sum",
                        "type": "integer",
                        "value": value + 1}])
    elif command == 'CREATE':
        print_success([{"key": "sum",
                        "type": "integer",
                        "value": 0}])
    else:
        print_error("Unknown command {0}".format(command))

```

Description of operation

- The program expects to get the data structure in json format with the field “params”.
- It reads the values of the “a” fields.
- Returns the result as a value of field “{a} + 1” in json format.

Example of incoming parameters

```

"params": [
  {
    "key": "a",
    "type": "integer",
    "value": 1
  }
]

```

21.1.2 Installing a smart contract

1. Download and install [Docker for Developers](#) for your operating system.
2. Prepare a contract image. In the `stateful-increment-contract` folder, create the following files:
 - `contract.py`
 - `Dockerfile`
 - `run.sh`

Listing of `run.sh` file

```

#!/bin/sh

python contract.py

```


Dockerfile File Listing

```
FROM python:alpine3.8
ADD contract.py /
ADD run.sh /
RUN chmod +x run.sh
RUN apk add --no-cache --update iptables
CMD exec /bin/sh -c "trap : TERM INT; (while true; do sleep 1000; done) & wait"
```

Important: It is required to install `iptables` into the smart contract container.

3. Install the image in Docker registry. Execute the following commands in the terminal:

```
docker run -d -p 5000:5000 --name registry registry:2
cd contracts/stateful-increment-contract
docker build -t stateful-increment-contract .
docker image tag stateful-increment-contract localhost:5000/stateful-increment-contract
docker start registry
docker push localhost:5000/stateful-increment-contract
```

4. Run the following command in the terminal to get the information about the container:

```
docker inspect 57c2c2d2643d
[
{
  "Id": "sha256:57c2c2d2643da042ef8dd80010632ffdd11e3d2e3f85c20c31dce838073614dd",
  "RepoTags": [
    "wenode:latest"
  ],
  "RepoDigests": [],
  "Parent": "sha256:d91d2307057bf3bb5bd9d364f16cd3d7eda3b58edf2686e1944bcc7133f07913",
  "Comment": "",
  "Created": "2019-10-25T14:15:03.856072509Z",
  "Container": "",
  "ContainerConfig": {
    "Hostname": "",
    "Domainname": "",
    "User": "",
    "AttachStdin": false,
    "AttachStdout": false,
    "AttachStderr": false,
```

The smart contract identifier `Id` is the value of the `imageHash` field and it is used in transactions with the created smart contract.

5. Sign a transaction to create a smart contract. In this example, the transaction is signed with the key stored in the node keystore.

Hint: To create a key pair and the participant address, use the utility `generators.jar`. The procedure for creating a key pair is given in item 1 of the module “Connecting to the Network”. The rules for generating queries to the node are given in the module *Node REST API*.

Query Body

```
{
  "fee": 100000000,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "sender": "3PudkbvjV1nPj1TkuuRahh4sGdgfr4YAUUV2",
  "password": "",
  "params": [],
  "type": 103,
  "version": 1
}
```

Sample query

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↳header 'X-Contract-API-Token' -d '{ \
  "fee": 100000000, \
  "image": "stateful-increment-contract:latest", \
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65", \
  "contractName": "stateful-increment-contract", \
  "sender": "3PudkbvjV1nPj1TkuuRahh4sGdgfr4YAUUV2", \
  "password": "", \
  "params": [], \
  "type": 103, \
  "version": 1 \
}' 'http://localhost:6862/transactions/sign'
```

Sample response

```
{
  "type": 103,
  "id": "ULcq9R7PvUB2yPmrmBdxoTi3bcRmQPT3JDLLLZVj4Ky",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhAv38Dws5skQDsJMVT2M",
  "fee": 500000,
  "timestamp": 1550591678479,
  "proofs": [
↳"yeCRFZm9iBLyDy93BDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
  "version": 1,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "params": [],
  "height": 1619
}
```

6. Send the signed transaction to the blockchain. The response from the sign method must be transferred to the input for the broadcast method.

Sample query

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↳header 'X-Contract-API-Token' -d '{ \
{
  "type": 103, \
  "id": "ULcq9R7PvUB2yPmrmBdxoTi3bcRmQPT3JDLLLZVj4Ky", \
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew", \
```

(continues on next page)

(continued from previous page)

```

"senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M", \
"fee": 500000, \
"timestamp": 1550591678479, \
"proofs": [
↪ "yecrFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ], \
"version": 1, \
"image": "stateful-increment-contract:latest", \
"imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65", \
"contractName": "stateful-increment-contract", \
"params": [], \
"height": 1619 \
}
}' 'http://localhost:6862/transactions/broadcast'
    
```

7. Use the transaction ID to check that the contract initiation transaction is placed in the blockchain.

Sample response

```

{
  "type": 103,
  "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLLLLZVj4Ky",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
  "fee": 500000,
  "timestamp": 1550591678479,
  "proofs": [
  ↪ "yecrFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
  "version": 1,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "params": [],
  "height": 1619
}
    
```

21.1.3 Smart Contract Execution

1. Sign a call-transaction to call (execute) the smart contract.

In the "contractID" field, specify the contract initialization transaction ID.

Query Body

```

{
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "fee": 10,
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "password": "",
  "type": 104,
  "version": 1,
  "params": [
    {
      "type": "integer",
      "key": "a",
      "value": 1
    }
  ]
}
    
```

(continues on next page)

(continued from previous page)

```

]
}

```

Sample query

```

curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↳header 'X-Contract-API-Token' -d '{ \
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2", \
  "fee": 10, \
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58", \
  "password": "", \
  "type": 104, \
  "version": 1, \
  "params": [ \
    { \
      "type": "integer", \
      "key": "a", \
      "value": 1 \
    } \
  ] \
}' 'http://localhost:6862/transactions/sign'

```

Sample response

```

{
  "type": 104,
  "id": "9fBrL2n5TN473g1gNfoZqaAqAsAJCuHRHYxZpLexL3VP",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVLRqLCqouVrFZynjfoTEuPNV9GrdauNpgdWXLsq",
  "fee": 10,
  "timestamp": 1549365736923,
  "proofs": [
    "2q4cTBhdKEDkFxr7iYaHPAv1dzaKo5rDaTxPF5VHryyYTXxTPvN9Wb3YrsDYixKiUPXBnAyXzEcnKPFRCW9xVp4v"
  ],
  "version": 1,
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "params": [
    {
      "key": "a",
      "type": "integer",
      "value": 1
    }
  ]
}

```

2. Send the signed transaction to the blockchain. The response from the sign method must be transferred to the input for the broadcast method.

Sample query

```

curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↳header 'X-Contract-API-Token' -d '{ \
  "type": 104, \
  "id": "9fBrL2n5TN473g1gNfoZqaAqAsAJCuHRHYxZpLexL3VP", \
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58", \
  "senderPublicKey": "2YvzcVLRqLCqouVrFZynjfoTEuPNV9GrdauNpgdWXLsq", \
  "fee": 10, \

```

(continues on next page)

(continued from previous page)

```

"timestamp": 1549365736923, \
"proofs": [ \
  "2q4cTBhDkEDkFxr7iYaHPAv1dzaKo5rDaTxPF5VHryyYTXxTPvN9Wb3YrsDYixKiUPXBnAyXzEcnKPFRCW9xVp4v" \
], \
"version": 1, \
"contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2", \
"params": [ \
  { \
    "key": "a", \
    "type": "integer", \
    "value": 1 \
  } \
] \
}' 'http://localhost:6862/transactions/broadcast'
    
```

3. Get the result of smart contract execution by its ID.

Sample response

```

[
  {
    "key": "1+1",
    "type": "integer",
    "value": 2
  }
]
    
```

21.2 API methods available to smart contract

Docker container-based smart contracts can use node *REST API*. Smart contract developers can use limited list of REST API methods. This list is represented below, these methods are available directly from the container.

Addresses methods

- *GET /addresses*
- *GET /addresses/publicKey/{publicKey}*
- *GET /addresses/balance/{address}*
- *GET /addresses/data/{address}*
- *GET /addresses/data/{address}/{key}*

Crypto methods

- *POST /crypto/encryptCommon*
- *POST /crypto/encryptSeparate*
- *POST /crypto/decrypt*

Privacy methods

- *GET /privacy/{policy-id}/getData/{policy-item-hash}*
- *GET /privacy/{policy-id}/getInfo/{policy-item-hash}*
- *GET /privacy/{policy-id}/hashes*

- *GET /privacy/{policy-id}/recipients*

Transactions methods

- *GET /transactions/info/{id}*
- *GET /transactions/address/{address}/limit/{limit}*

Contracts methods

A smart contract can use *Contracts* methods implementing the separated `/internal/contracts/` route, which is totally identical to the regular *Contracts* methods.

- *GET /internal/contracts/{contractId}/{key}*
- *GET /internal/contracts/executed-tx-for/{id}*
- *GET /internal/contracts/{contractId}*
- *GET /internal/contracts*

PKI methods

- *PKI /verify*

21.2.1 Docker contract authorization

A smart contract requires an authorization to use the node *REST API*. There are following steps for the correct REST API methods usage by the smart contract:

1. The following variables should be defined in the Docker contract environment:
 - `NODE_API` - an URL address to the node *REST API*.
 - `API_TOKEN` - an authorization token of the Docker contract.
 - `COMMAND` - commands for the Docker contract creation and call.
 - `TX` - a transaction which is required to the Docker contract for work (*103 - 107* codes).
2. The Docker contract developer assigns the value of the variable `API_TOKEN` to the request header `X-Contract-Api-Token`. The node specifies JWT authorization token into the variable `API_TOKEN` for the contract creation and execution.
3. The contract code should pass the received token in the request header (`X-Contract-Api-Token`) each time the node API is accessed.

21.3 Smart contract run with gRPC

In addition to using the REST API a smart contract can work with the node via the *gRPC* framework. *gRPC* is a high-performance remote procedure call (RPC) framework that runs over the HTTP/2 protocol. The *protobuf* protocol is used as a tool for describing of data types and serialization.

Hint: Technical description of contracts implementation is given in module *Docker Smart Contracts*.

gRPC framework supports 10 programming languages. You can find the list in [official gRPC docs](#). We use an example of creating a Python smart contract that performs an increment operation (increasing a given number by one).

21.3.1 Description of the smart contract

In our example *103* transaction initializes the initial state of the contract for the creation, keeping the numeric key `sum` with 0 value in it:

```
{
  "key": "sum",
  "type": "integer",
  "value": 0
}
```

Each next *104* call transaction increases the key value `sum` by one (`sum = sum + 1`).

How the smart contract works after the call:

1. After the program runs, it checks for the presence of environment variables. There are environment variables which are used by the contract:
 - `CONNECTION_ID` – connection ID passed by the contract when connecting to a node.
 - `CONNECTION_TOKEN` – authorization token passed by the contract when connecting to a node.
 - `NODE` – a node IP address or a node domain name.
 - `NODE_PORT` – a gRPC port of the service which is deployed on the node.

The values of the `NODE` and `NODE_PORT` variables are taken from `:ref:docker-engine.grpc-server <docker-configuration>` section of the configuration file. Other variables are generated by the node and passed to the container when creating a smart contract.

2. Using `NODE` and `NODE_PORT` variables values the contract creates gRPC connection to a node.
3. Then gRPC `ContractService` service's `Connect` method is called (see additional info in the `contract.proto` file). This method accepts `ConnectionRequest` parameter which is specifying the connection ID (`CONNECTION_ID` environment variable). Also in the methods metadata you need to specify the `authorization` head which contains an authorization token (`CONNECTION_TOKEN` environment variable).
4. In the case of successful result gRPC `stream` is return including the `ContractTransactionResponse` objects for the execution. The `ContractTransactionResponse` object contains two fields:
 - `transaction` – a contract creation or call transaction.
 - `auth_token` – an authorization token, specified in the `authorization` head of metadata of gRPC method being called.

If `transaction` contains a creation transaction (transaction type – *103*), the initial state is initialized for the contract. If `transaction` contains a call transaction (transaction type – *104*), the following actions are performed:

- the node receives a request of the value of the `sum` key (the `GetContractKey` method of the `ContractService` service);
- the key value increases by one, `sum = sum + 1`;
- a new key value is saved on the node (the `CommitExecutionSuccess` method of the `ContractService` service), i.e. the contract state is updated.

21.3.2 Smart contract creation

1. Download and install Docker for Developers (<https://www.docker.com/get-started>) for your operating system.
2. Prepare an image of the contract. The contract folder must contain the following files:

- `src/contract.py`
- `Dockerfile`
- `run.sh`
- `src/protobuf/contract.proto`
- `src/protobuf/common.proto`
- `src/protobuf/common_pb2.py`
- `src/protobuf/contract_pb2.py`
- `src/protobuf/contract_pb2_grpc.py`

`src/protobuf/common_pb2.py`, `src/protobuf/contract_pb2.py`, `src/protobuf/contract_pb2_grpc.py` files should be generated by the gRPC compiler using the `contract.proto` and `common.proto` protobuf files.

Important: After compiling the files you need to change the `import` directive in the generated files:

- it must be `import protobuf.common_pb2 as common__pb2` in the `contract_pb2.py` file;
 - it must be `import protobuf.contract_pb2 as contract__pb2` in the `contract_pb2_grpc.py` file.
-

3. Install the image in the Docker image repository. If you are using a local repository, run the following commands in the terminal:

```
docker run -d -p 5000:5000 --name registry registry:2
cd contracts/grpc-increment-contract
docker build -t grpc-increment-contract .
docker image tag grpc-increment-contract localhost:5000/grpc-increment-contract
docker start registry
docker push localhost:5000/grpc-increment-contract
```

4. Use `docker inspect` command to get more info about smart contract:

```
docker inspect 57c2c2d2643d
[
{
  "Id": "sha256:57c2c2d2643da042ef8dd80010632ffdd11e3d2e3f85c20c31dce838073614dd",
  "RepoTags": [
    "wenode:latest"
  ],
  "RepoDigests": [],
  "Parent": "sha256:d91d2307057bf3bb5bd9d364f16cd3d7eda3b58edf2686e1944bcc7133f07913",
  "Comment": "",
  "Created": "2019-10-25T14:15:03.856072509Z",
  "Container": "",
```

(continues on next page)

(continued from previous page)

```
"ContainerConfig": {
  "Hostname": "",
  "Domainname": "",
  "User": "",
  "AttachStdin": false,
  "AttachStdout": false,
  "AttachStderr": false,
```

Important: The smart contract identifier `Id` is the value of the `imageHash` field and it is used in transactions with the created smart contract.

5. Sign the *103* transaction for the smart contract creation. In our example the transaction is signed with a key stored in the node's keystore. See *REST API* section for a description of the rest API nodes and rules for generating transactions.

Request sample of the contract creation transaction:

```
{
  "fee": 100000000,
  "image": "localhost:5000/grpc-increment-contract",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "grpc-increment-contract",
  "sender": "3PudkbvjV1nPj1TkuuRahh4sGdgfr4YAUUV2",
  "password": "",
  "params": [],
  "type": 103,
  "version": 2,
}
```

Curl-request sample:

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↳header 'X-Contract-API-Token' -d '{ \
  "fee": 100000000, \
  "image": "localhost:5000/grpc-increment-contract", \
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65", \
  "contractName": "grpc-increment-contract", \
  "sender": "3PudkbvjV1nPj1TkuuRahh4sGdgfr4YAUUV2", \
  "password": "", \
  "params": [], \
  "type": 103, \
  "version": 2 \
}' 'http://localhost:6862/transactions/sign'
```

Response sample:

```
{
  "type": 103,
  "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLZZVj4Ky",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skQDsJMVT2M",
  "fee": 100000000,
  "timestamp": 1550591678479,
  "proofs": [
    ↳"ye cRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
```

(continues on next page)

(continued from previous page)

```

"version": 2,
"image": "localhost:5000/grpc-increment-contract",
"imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
"contractName": "grpc-increment-contract",
"params": [],
"height": 1619
}

```

6. Send the signed transaction to the blockchain. A response from the *sign* method should be passed to *broadcast* method input.

Request sample for sending a smart contract creation transaction to the blockchain:

```

{
  "type": 103,
  "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLLLZVj4Ky",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",
  "fee": 500000,
  "timestamp": 1550591678479,
  "proofs": [
    ↪ "yeCRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
  "version": 1,
  "image": "stateful-increment-contract:latest",
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
  "contractName": "stateful-increment-contract",
  "params": [],
  "height": 1619
}

```

Curl-request sample:

```

curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↪ header 'X-Contract-API-Token' -d '{ \
  "type": 103, \
  "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLLLZVj4Ky", \
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew", \
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M", \
  "fee": 100000000, \
  "timestamp": 1550591678479, \
  "proofs": [
    ↪ "yeCRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQQ8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ], \
  "version": 2, \
  "image": "localhost:5000/grpc-increment-contract", \
  "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65", \
  "contractName": "grpc-increment-contract", \
  "params": [], \
  "height": 1619 \
}' 'http://localhost:6862/transactions/broadcast'

```

Response sample:

```

{
  "type": 103,
  "id": "ULcq9R7PvUB2yPMrmBdxoTi3bcRmQPT3JDLLLZVj4Ky",
  "sender": "3N3YTj1tNwn8XUJ8ptGKbPuEFNa9GFnhqew",
  "senderPublicKey": "3kW7vy6nPC59BXM67n5N56rhhAv38Dws5skqDsJMVT2M",

```

(continues on next page)

(continued from previous page)

```

    "fee": 100000000,
    "timestamp": 1550591678479,
    "proofs": [
    ↪ "yeChRFZm9iBLyDy93bDVaNo1PR5Qkkic7196GAgUt9TNH1cnQphq4yGQq8Fxfj4BYA4TaqYVw5qxtWzGMPQyVeKYv" ],
    "version": 2,
    "image": "localhost:5000/grpc-increment-contract",
    "imageHash": "7d3b915c82930dd79591aab040657338f64e5d8b842abe2d73d5c8f828584b65",
    "contractName": "grpc-increment-contract",
    "params": [],
    "height": 1619
}
    
```

Compare transaction identifiers of both operations (id field) and make sure, that the initialization contract transaction has placed in the blockchain.

21.3.3 Smart contract call

1. Sign the *104* transaction for the smart contract call.

Request sample of the contract call transaction:

```

{
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "fee": 15000000,
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "password": "",
  "type": 104,
  "version": 2,
  "contractVersion": 1,
  "params": []
}
    
```

2. Send the signed transaction to the blockchain. A response from the *sign* method should be passed to *broadcast* method input.

Request sample for sending a smart contract call transaction to the blockchain:

```

{
  "type": 104,
  "id": "9fBrl2n5TN473g1gNfoZqaAqAsAJCuHRHYxZpLexL3VP",
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58",
  "senderPublicKey": "2YvzcVLRqLCqouVrFZynjfoTEuPNV9GrdaunpgdWXLsq",
  "fee": 15000000,
  "timestamp": 1549365736923,
  "proofs": [
    "2q4cTBhDkEDkFxr7iYaHPAv1dzaKo5rDaTxPF5VHryyYTXxTPvN9Wb3YrsDYixKiUPXBnAyXzEcnKPFRCW9xVp4v"
  ],
  "version": 1,
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2",
  "params": []
}
    
```

Curl-request sample:

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --
↳header 'X-Contract-Api-Token' -d '{ \
  "type": 104, \
  "id": "9fBrl2n5TN473g1gNfoZqaAqAsAJCuHRHYxZpLexL3VP", \
  "sender": "3PKyW5FSn4fmdrLcUnDMRHVyoDBxybRgP58", \
  "senderPublicKey": "2YvzcVLRqLCqouVrFZynjotEuPNV9GrdauNpgdWXLsq", \
  "fee": 15000000, \
  "timestamp": 1549365736923, \
  "proofs": [ \
    "2q4cTBhDkEDkFxr7iYaHPAv1dzaKo5rDaTxPF5VHryyYTXxTPvN9Wb3YrsDYixKiUPXBnAyXzEcnKPFRCW9xVp4v"
  ] \
  }, \
  "version": 1, \
  "contractId": "2sqPS2VAKmK77FoNakw1VtDTCbDSa7nqh5wTXvJeYGo2", \
  "params": [] \
}' 'http://localhost:6862/transactions/broadcast'
```

Response sample:

```
[
  {
    "key": "sum",
    "type": "integer",
    "value": 2
  }
]
```

Use the smart contract identifier to get info about an execution result.

21.3.4 Files samples

run.sh listing:

```
#!/bin/sh

eval $SET_ENV_CMD
python contract.py
```

Dockerfile listing:

```
FROM python:3.8-slim-buster
RUN apt install iptables
RUN apt update && apt install -yq dnsutils
RUN pip3 install grpcio-tools
ADD src/contract.py /
ADD src/protobuf/common_pb2.py /protobuf/
ADD src/protobuf/contract_pb2.py /protobuf/
ADD src/protobuf/contract_pb2_grpc.py /protobuf/
ADD run.sh /
RUN chmod +x run.sh
ENTRYPOINT ["/run.sh"]
```

Python smart contract listing:

```
import grpc
import os
```

(continues on next page)

(continued from previous page)

```

import sys

from protobuf import common_pb2, contract_pb2, contract_pb2_grpc

CreateContractTransactionType = 103
CallContractTransactionType = 104

AUTH_METADATA_KEY = "authorization"

class ContractHandler:
    def __init__(self, stub, connection_id):
        self.client = stub
        self.connection_id = connection_id
        return

    def start(self, connection_token):
        self.__connect(connection_token)

    def __connect(self, connection_token):
        request = contract_pb2.ConnectionRequest(
            connection_id=self.connection_id
        )
        metadata = [(AUTH_METADATA_KEY, connection_token)]
        for contract_transaction_response in self.client.Connect(request=request,
↳ metadata=metadata):
            self.__process_connect_response(contract_transaction_response)

    def __process_connect_response(self, contract_transaction_response):
        print("receive: {}".format(contract_transaction_response))
        contract_transaction = contract_transaction_response.transaction
        if contract_transaction.type == CreateContractTransactionType:
            self.__handle_create_transaction(contract_transaction_response)
        elif contract_transaction.type == CallContractTransactionType:
            self.__handle_call_transaction(contract_transaction_response)
        else:
            print("Error: unknown transaction type '{}'.format(contract_transaction.type),
↳ file=sys.stderr)

    def __handle_create_transaction(self, contract_transaction_response):
        create_transaction = contract_transaction_response.transaction
        request = contract_pb2.ExecutionSuccessRequest(
            tx_id=create_transaction.id,
            results=[common_pb2.DataEntry(
                key="sum",
                int_value=0)]
        )
        metadata = [(AUTH_METADATA_KEY, contract_transaction_response.auth_token)]
        response = self.client.CommitExecutionSuccess(request=request, metadata=metadata)
        print("in create tx response '{}'.format(response))

    def __handle_call_transaction(self, contract_transaction_response):
        call_transaction = contract_transaction_response.transaction
        metadata = [(AUTH_METADATA_KEY, contract_transaction_response.auth_token)]

        contract_key_request = contract_pb2.ContractKeyRequest(
            contract_id=call_transaction.contract_id,

```

(continues on next page)

(continued from previous page)

```

        key="sum"
    )
    contract_key = self.client.GetContractKey(request=contract_key_request, metadata=metadata)
    old_value = contract_key.entry.int_value

    request = contract_pb2.ExecutionSuccessRequest(
        tx_id=call_transaction.id,
        results=[common_pb2.DataEntry(
            key="sum",
            int_value=old_value + 1)]
    )
    response = self.client.CommitExecutionSuccess(request=request, metadata=metadata)
    print("in call tx response '{}'.format(response)")

def run(connection_id, node_host, node_port, connection_token):
    # NOTE(gRPC Python Team): .close() is possible on a channel and should be
    # used in circumstances in which the with statement does not fit the needs
    # of the code.
    with grpc.insecure_channel('{}:{}'.format(node_host, node_port)) as channel:
        stub = contract_pb2_grpc.ContractServiceStub(channel)
        handler = ContractHandler(stub, connection_id)
        handler.start(connection_token)

CONNECTION_ID_KEY = 'CONNECTION_ID'
CONNECTION_TOKEN_KEY = 'CONNECTION_TOKEN'
NODE_KEY = 'NODE'
NODE_PORT_KEY = 'NODE_PORT'

if __name__ == '__main__':
    if CONNECTION_ID_KEY not in os.environ:
        sys.exit("Connection id is not set")
    if CONNECTION_TOKEN_KEY not in os.environ:
        sys.exit("Connection token is not set")
    if NODE_KEY not in os.environ:
        sys.exit("Node host is not set")
    if NODE_PORT_KEY not in os.environ:
        sys.exit("Node port is not set")

    connection_id = os.environ[CONNECTION_ID_KEY]
    connection_token = os.environ[CONNECTION_TOKEN_KEY]
    node_host = os.environ[NODE_KEY]
    node_port = os.environ[NODE_PORT_KEY]

    run(connection_id, node_host, node_port, connection_token)

```

contract.proto listing:

```

syntax = "proto3";
package wavesenterprise;

option java_multiple_files = true;
option java_package = "com.wavesplatform.protobuf.service";
option csharp_namespace = "WavesEnterprise";

import "google/protobuf/wrappers.proto";
import "common.proto";

```

(continues on next page)

(continued from previous page)

```

service ContractService {

    rpc Connect (ConnectionRequest) returns (stream ContractTransactionResponse);

    rpc CommitExecutionSuccess (ExecutionSuccessRequest) returns (CommitExecutionResponse);

    rpc CommitExecutionError (ExecutionErrorRequest) returns (CommitExecutionResponse);

    rpc GetContractKeys (ContractKeysRequest) returns (ContractKeysResponse);

    rpc GetContractKey (ContractKeyRequest) returns (ContractKeyResponse);
}

message ConnectionRequest {
    string connection_id = 1;
}

message ContractTransactionResponse {
    ContractTransaction transaction = 1;
    string auth_token = 2;
}

message ContractTransaction {
    string id = 1;
    int32 type = 2;
    string sender = 3;
    string sender_public_key = 4;
    string contract_id = 5;
    repeated DataEntry params = 6;
    int64 fee = 7;
    int32 version = 8;
    bytes proofs = 9;
    int64 timestamp = 10;
    AssetId fee_asset_id = 11;

    oneof data {
        CreateContractTransactionData create_data = 20;
        CallContractTransactionData call_data = 21;
    }
}

message CreateContractTransactionData {
    string image = 1;
    string image_hash = 2;
    string contract_name = 3;
}

message CallContractTransactionData {
    int32 contract_version = 1;
}

message ExecutionSuccessRequest {
    string tx_id = 1;
    repeated DataEntry results = 2;
}
    
```

(continues on next page)

(continued from previous page)

```

message ExecutionErrorRequest {
  string tx_id = 1;
  string message = 2;
}

message CommitExecutionResponse {
}

message ContractKeysRequest {
  string contract_id = 1;
  google.protobuf.Int32Value limit = 2;
  google.protobuf.Int32Value offset = 3;
  google.protobuf.StringValue matches = 4;
  KeysFilter keys_filter = 5;
}

message KeysFilter {
  repeated string keys = 1;
}

message ContractKeysResponse {
  repeated DataEntry entries = 1;
}

message ContractKeyRequest {
  string contract_id = 1;
  string key = 2;
}

message ContractKeyResponse {
  DataEntry entry = 1;
}

message AssetId {
  string value = 1;
}

```

common.proto listing:

```

syntax = "proto3";
package wavesenterprise;

option java_multiple_files = true;
option java_package = "com.wavesplatform.protobuf.common";
option csharp_namespace = "WavesEnterprise";

message DataEntry {
  string key = 1;
  oneof value {
    int64 int_value = 10;
    bool bool_value = 11;
    bytes binary_value = 12;
    string string_value = 13;
  }
}

```


21.4 gRPC services available to smart contract

You can use the official [GitHub](#) page for to download all required protobuf files. The list of all files is as follows:

- `address.proto` - addresses methods.
- `common.proto` - a common file for proper work of others protobuf files.
- `crypto.proto` - methods for working with data encryption.
- `permission.proto` - permission methods.
- `pki.proto` - PKI methods.
- `privacy.proto` - privacy methods.
- `util.proto` - methods for utility tools.

Every protobuf file (except `common.proto`) contains a set of small blocks (message) that include a set of key-value fields. A list of such blocks for each file is provided below.

address.proto

- `GetAddresses` - getting all addresses of participants whose key pairs are stored in the node keystore.
- `GetAddressData` - getting all data recorded to address account {address}.

contract.proto

- `Connect` - connecting a contract to a node.
- `CommitExecutionSuccess` - getting the result of successful contract execution and sending the results to the node.
- `CommitExecutionError` - getting a contract execution error and sending the results to the node.
- `GetContractKeys` - getting the contract result execution by its ID (contract creation transaction ID).
- `GetContractKey` - getting a contract execution value by its ID (contract creation transaction ID) and key {key}.

crypto.proto

- `EncryptSeparate` - data encryption separately for the each recipient with the unique key.
- `EncryptCommon` - data encryption with a single CEK key for all recipients and the CEK wraps into a unique KEK for the each recipient.
- `Decrypt` - data decryption. The decryption is available only if the message recipient's key is in the node's keystore.

permission.proto

- `GetPermissions` - getting roles (permissions) assigned to specified address {address} which are valid at the moment.
- `GetPermissionsForAddresses` - getting roles (permissions) assigned to specified address list which are valid at the moment.

pki.proto

- `Sign` - a creation a detached digital signature for sent data.
- `Verify` - check the detached digital signature for sent data.

privacy.proto

- `GetPolicyRecipients` - getting all addresses of participants, signed to the access group {policy-id}.
- `GetPolicyOwners` - getting all addresses of owners, signed to the access group {policy-id}.
- `GetPolicyHashes` - getting the array of identified hashes which are written with association to the {policy-id}.
- `GetPolicyItemData` - getting the confidential data package by its identified hash.
- `GetPolicyItemInfo` - getting the metadata for the confidential data package by the identified hash.

util.proto

- `GetNodeTime` - getting current node time.

ROLE MANAGEMENT

The list of possible roles in the blockchain platform is given in module *“Authorization of participants”*.

Important: The prerequisite for changing permissions of participants (adding or deleting roles) is the availability of the participant’s private key with the “permissioner” role in the node keystore from which the query is made.

22.1 Option 1 (through REST API)

Participant permissions are managed by signing (sign method) and broadcasting (broadcast method) of permission transactions through *Node REST API*.

Query object for sign method:

```
{
  "type":102,
  "sender":3GLWx8yUFcNSL3DER8kZyE4TpyAyNiEYsKG,
  "senderPublicKey":4WnvQPit2Di1iYXDgDcXnJZ5yroKW54vauNoxdNeMi2g,
  "fee":0,
  "proofs":[""],
  "target":3GPtj5osoYqHpyfmsFv7BMiyKsVzbG1ykfL,
  "opType":"add",
  "role":"contract_developer",
  "dueTimestamp":null
}
```

Query fields:

- type - the type of the transaction for the participant permission management (type = 102);
- sender - the participant address with the permission to issue permission transactions;
- proofs - the transaction signature;
- target - the participant address, for which permissions are required to be assigned or deleted;
- role - participant permissions to be assigned or removed. Possible values: “miner”, “issuer”, “dex”, “permissioner”, “blacklister”, “banned”, “contract_developer”, “connection_manager”;
- opType - the type of the operation “add” (add permissions) or “remove” (delete permissions);
- dueTimestamp - the permission validity date in the timestamp format. The field is optional.

Transfer the response from the node to the broadcast method.

22.2 Option 2 (using the utility)

Using the Generators utility the process can be automated.

Example of console launching:

```
java -jar generators.jar GrantRolesApp [configfile]
```

Example of configuration:

```
permission-granter {
waves-crypto = no
chain-id = T
account = {
  addresses = [
    "3N2cQFfUDzG2iujBrFTnD2TAsCNohDxYu8w"
  ]
  storage = ${user.home}"/node/keystore.dat"
  password = "some string as password"
}
send-to = [
  "devnet-aws-fr-2.we.wavesnodes.com:6864"
]
grants = [
  {
    address: "3N2cQFfUDzG2iujBrFTnD2TAsCNohDxYu8w"
    assigns = [
      {
        permission = "miner",
        operation = "add",
        due-timestamp = 1527698744623
      },
      {
        permission = "issuer",
        operation = "add",
        due-timestamp = 1527699744623
      },
      {
        permission = "blacklister",
        operation = "add"
      },
      {
        permission = "permissioner",
        operation = "remove"
      }
    ]
  }
]
txs-per-bucket = 10
}
```

The field “due-timestamp” limits the role validity; Fields “nodes”, “roles” are mandatory.

If the node is already assigned any of the roles specified in the config, then the case is handled in accordance with the rules:

| Current node status | Status received from transaction | Processing result |
|------------------------------------|----------------------------------|--|
| No role assigned | New role | Success - role assigned |
| Role assigned without dueDate | Role with dueDate | Checking dueDate; if less than current, then IncorrectDateTime, otherwise Success - role assigned with dueDate |
| Role assigned with dueDate | Role with dueDate | Checking dueDate; if less than current, then IncorrectDateTime, otherwise Success - updating dueDate |
| Role assigned with dueDate | Role without dueDate | Success - role assigned without dueDate |
| Role assigned with/without dueDate | Role removal | Checking node address; if <> for genesis address, then Success - role removed |

PARTICIPANTS CONNECTION TO THE NETWORK

The moment of the first node *running* is the beginning of the new blockchain net creation. You can create the blockchain net from the starting only one node, further you can add new nodes as required.

- *Connect* a new node into the existing network.
- *Delete* unnecessary nodes from the network.

23.1 Connection of a new node to the existing net

You can add new nodes into the net at any time. The configuration files setting is described in the section *Installing and running the Waves Enterprise platform*. Perform all these actions and *run* the node. The following steps are making:

1. The new node user gives the public key and the node description to the net administrator.
2. The network administrator (the node with “Connection-manager” role) uses the received public key and description for the *111 RegisterNode* transaction creation with the "opType": "add" parameter.
3. Transaction falls to the block and further into the nodes states of network participants. As a result of the transaction among the stored data, each participant of the network stores the public key and the address of the new node.
4. If necessary, the network administrator can add additional roles to the new node using the transaction *102 Permit*.
5. The user *runs* the node.
6. After starting, the node sends *handshake-message* with its public key to the participants from the “peers” list of its configuration file.
7. Network participants compare the public key from the *handshake message* and the key from transaction *111 RegisterNode* sent earlier by the network administrator. If the check is successful, the network participant updates its database and sends the Peers Message message to the network.
8. Having successfully connected, the new node synchronizes with the network and receives the address table of the network participants.

23.2 Deleting the node

1. The network administrator creates the *111 RegisterNode* transaction with the parameter "opType": "remove" and the public key of the removed node within.
2. This transaction is fell into the block and approved by other nodes.
3. After accepting the transaction the nodes find the public key specified in the transaction *111 RegisterNode* in their state and delete it from there.
4. Then nodes delete the network address of the removed node from the `network.known-peers` of the node configuration file.

CONFIDENTIAL DATA EXCHANGE

Before you can share the confidential data, you need to create access groups. Using transactions, you can *add* or *change* access groups to the confidential data.

24.1 Creation of the confidential data access group

The confidential data access group can be created by any network participant. You need to specify the range of participants, which will get the data. Then any of participant will perform the following actions:

1. The network participant, the future owner of the group, is creating the *112 CreatePolicy* with the following parameters:
 - sender - the public key of the access group creator.
 - description - the description of the access group.
 - policyName - the name of the access group.
 - recipients - public keys of access group participants, which will have the access to the confidential data.
 - owners - public keys of access group participants, which, in addition to the data access, can change the lineup of the group participants.
2. This transaction is fell into the block and approved by other nodes.
3. After accepting the transaction the nodes which are the access group participants will get the access to the confidential data.

24.2 Changing the access group

Access groups can only be changed by their owners. The following actions are performed to change the list of participants in the access group:

1. The group owner creates the *113 UpdatePolicy* transaction with the following parameters:
 - policyId - identifier of the access group;
 - sender - the public key of the access group owner;
 - opType - the option of the adding (**add**) or the removing (**remove**) the group participants;
 - recipients - public keys of access group participants, which are added or removed from the access group;
 - owners - public keys of access group participants, which are added or removed from the access group.
2. This transaction is fell into the block and approved by other nodes.

3. After accepting the transaction the information about participants of the changed access group will update.

24.3 Exchanging the confidential data

Important: The size of the transferred data via API method *POST /privacy/sendData* to the network is up to 20 MB.

1. Using the API *POST /privacy/sendData* tool the client sends the data to the network (API parameters: sender, password, policy ID, data type, data information, data and hash).
2. Access group participants use the *GET /privacy/{policyId}/getData/{policyItemHash}* tool for getting information about data and its further download.

Follow these steps for the values creation of the **data** and **hash** fields:

1. Translate the data byte sequence into the **Base64** encoding.
2. Place the result of the data conversion to the "data": "29sCt...RgdC60LL" field of the API *POST /privacy/sendData*.
3. Specify the data hash sum according to the **SHA-256** algorithm in the "hash": "9wetTB...SU2zr1Uh" field. You need to specify the hash result in the **Base58** encoding.
4. Send the data to the network by pressing the **Try it out!** button.
5. Node automatically will create the *114 PolicyDataHash* transaction as a result of the data sending.

DATA ENCRYPTION OPERATIONS

Symmetric CEK and KEK keys are used to encrypt/decrypt data. CEK (Content Encryption Key) is the key for the encrypting text data, KEK (Key Encryption Key) is the key for encrypting the CEK. The CEK key is generated by a node randomly using the appropriate hashing algorithms. The KEK key is generated by a node based on Diffie-Hellman algorithm, using public and private keys of sender and recipients, and is used to encrypt the CEK key.

The symmetric CEK key is unreachable and does not appear in the encryption process. It is transmitted from the sender to the recipient in the encrypted form (wrappedKey) via open communication channels along with the encrypted message. One of such channels can be a record to the blockchain — a DataTransaction or a smart contract state. The KEK key does not transmit from the sender to recipients, it is restored by the recipient based on its private key and the known public key of the sender (Diffie-Hellman key exchange algorithm).

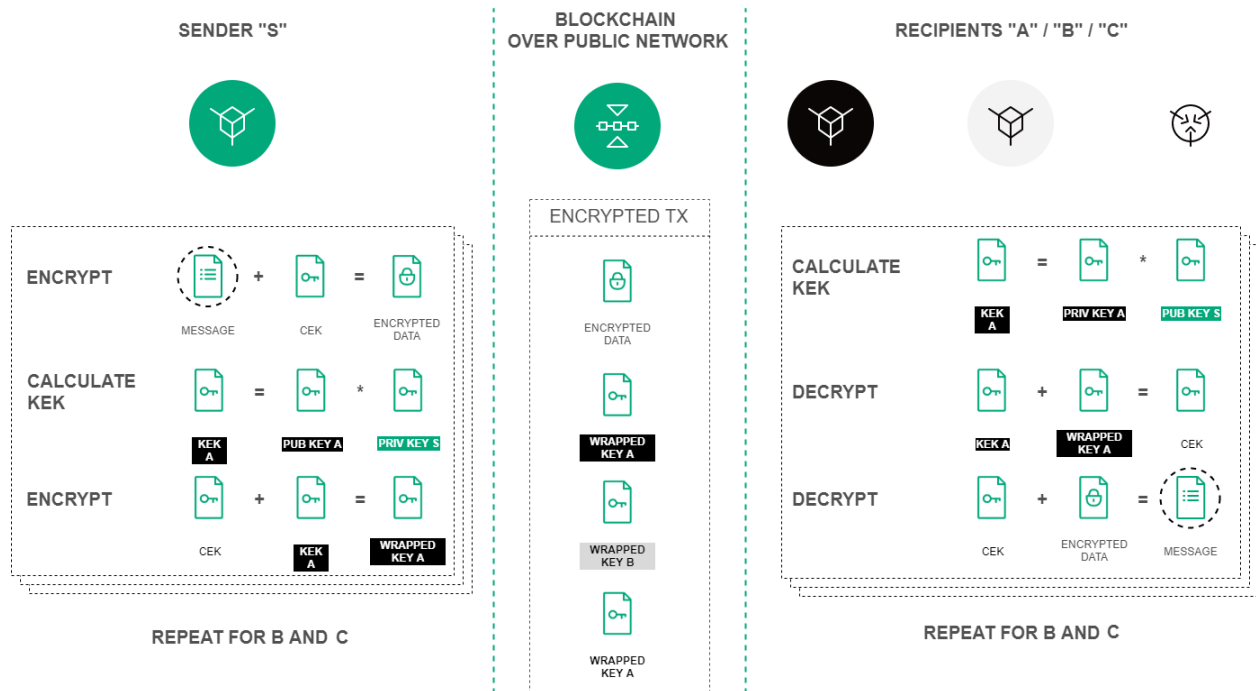


Fig. 1: Encryption procedure of the text data based on the Diffie-Hellman algorithm

Encryption/decryption process includes the following actions:

1. Use the *POST /crypto/encryptSeparate* method to encrypt data for each recipient separately. Parameters in the request object:
 - **sender** - the sender address;
 - **password** - a key pair password of the sender, which is generated at the same time as the account itself;
 - **encryptionText** - the text for the encryption;
 - **recipientsPublicKeys** - an array with recipients public keys list inside.
2. Use the *POST /crypto/encryptCommon* method to encrypt data for all recipients with a single CEK key.
3. Use the *POST /crypto/decrypt* method for the decryption. Parameters in the request object:
 - **recipient** - the recipient address.
 - **password** - a key pair password of the recipient, which is generated at the same time as the account itself.
 - **encryptedText** - the encrypted text data.
 - **wrappedKey** - the wrapped key obtained by encoding the data.
 - **senderPublicKey** - the sender public key.

GLOSSARY

Account

A client data set which is stored in database and used for client identification

Alias

A user's login associated with his address as a result of the transaction, the result of which is used to record the alias address matching in the database, and it is possible to specify this alias in the subsequent transactions

Anonymous network

Unpermissioned public blockchain which can be accessed by any participant as an anonymous person

Blockchain

A decentralized, distributed and public digital ledger that is used to record in such way that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks

Genesis block

The first block in the blockchain which contains special genesis transactions distributing the initial balance and permissions

Access group

A table inside the node state containing the net participants list which can exchange the privacy data according to this policy

Cryptocurrency

A form of digital currency based on encryption algorithms and ran inside decentralized platforms built on the blockchain

Consensus

The way to agree on a single point of the data value in a network between participants

Mining

The process by which transactions are verified and added to a blockchain

Mainnet

A real network where transactions are executing, tokens are issuing and storing

Node

A computer which is ran the node software and connected to the blockchain network

Peer

A net address of the node

Private key

A privately held string of data that allows you to sign transactions and to get access to tokens. The private key is inextricably bound to the public key

Public network

Permissioned public blockchain where each participant is known and registered in the network

Public key

A string of data bound with the private key and used for interactions with net participants. The public key is applied to transactions to confirm the correctness of the user's signature made on the private key

Public address

A public address is the cryptographic hash of a public key and a net byte. They act as email addresses that can be published anywhere, unlike private keys

Swagger

API tool

Seed phrase

A set from 24 accidentally chosen words for restoring the access to the tokens

Smart account

An account with specified features for creating and running smart-contracts

Smart asset

A token with an attached script, during each new transaction with such a token the transaction will be confirmed first by the script, then by the blockchain

Smart contract

A computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement between participant

State

The full history of transactions which is stored in the node DB

Token

An account unit, a blockchain asset, which is not a cryptocurrency and is intended to represent the digital balance, it is an equivalent of the company's shares

Transaction

An operation that participants on the blockchain network use to interact with each other

Participant

A blockchain participant who send transactions to the net for getting approve

Hash

A unique configuration of the symbols (letters and digits), it is a result of the hash function performing over the data according with the specified algorithm. Hash uniquely identifies the object

Private network

Permissioned private blockchain where all transactions are controlled by a central authority

Gateway

The app for tokens transfer from one blockchain net to another one

Airdrop

A distribution of cryptocurrency to users, entirely for free

PoS (Proof-of-Stake)

A consensus algorithm based on the stake which is used for choosing the node for checking transactions and generating a new block

PoA (Proof-of-Authority)

A consensus algorithm in a private blockchain that grants to the most authority nodes the right to check transactions and generate a new block

WHAT IS NEW IN THE WAVES ENTERPRISE

27.1 1.2.1

The following pages have been added:

- REST API *Debug* methods
- Full REST API description on the [API Docs](#) page

The following sections have been rebuilt:

- *Installing and running the Waves Enterprise platform*

27.2 1.2.0

The following pages have been added:

- A new section *Integration services*, which includes *Authorization service* and *Data preparation service*
- *Obtaining a license* section was added
- A new REST API *Licenses* method was added
- A new *Smart contract run with gRPC* section was added
- A new *gRPC services available to smart contract* section was added

The following sections have been rebuilt:

- *Installing and running the Waves Enterprise platform*
- The *Cryptography* section was renovated. Part of information was moved into *Data encryption operations* section
- *Changes in the node configuration file*
- *Transactions*

27.3 1.1.2

The following sections have been rebuilt:

- Sandbox
- *Changes in the node configuration file*
- *Node installation* was converted into “Installing and running the Waves Enterprise platform”
- *Participants connection to the network*
- *Anchoring settings*
- *Authorization type configuration for the REST API access*
- *Connection of the node to the “Waves Enterprise Partnetnet”*
- *Connection of the node to the “Waves Enterprise Mainnet”*
- *System requirements*

27.4 1.1.0

The following pages have been added:

- *API methods available to smart contract*
- Sandbox
- *Changes in the node configuration file*

The following sections have been rebuilt:

- *Docker Smart Contracts*
- *Example of starting a contract*
- *Node installation*
- Additional services deploy

27.5 1.0.0

The following pages have been added:

- *Authorization service*

The following sections have been rebuilt:

- *Node configuration*
- *Mainnet and Partnetnet connection*
- *REST API*
- *Node installation*

Changes in the node configuration file node.conf

- The *NTP server* section is added
- The *auth* section is added into the authorization type selection of the *REST API* section