SMARTBOARD

Technical Drawing

Technical documentation

Table of Contents

1. General description of the blockchain network of the platform

1.1. Description of the blockchain network of the platform

For project implementation, a public blockchain based on the source code of the izzz.io. The consensus algorithm is based on the confirmation of the generation time of a block (Dynamic Limited Confidence Proof-of-Activity, DLCPoA), which does not require significant computational resources, and is also based on a system of trusted nodes (Proof-of-Authority) to accelerate the network.

1.2. Technical Details of the Blockchain

Confirmation Method	DLCPoA (Dynamic Limited Confidence Proof of Activity) + Proof-of-Authority
Software Platform	Node.js 10
Hashing	Filtered SHA256
Digital Signatures	ECDSA-secp256k1 based on на bitcore-lib
CSP	bitcore-lib 1.0.4
Structure of the main chain of blocks	JSON blocks with up to 2 megabytes of content (reconfigurable)
Data Base	LevelDB 1.20, Sqlite3 3.24.0
Smart Contracts	EcmaContracts V8: JavaScript ES6, with manageable condition
p2p Protocol	WebSocket Based + DNS-SD Multicast Discovery

The main chain consists of JSON blocks with the following structure:

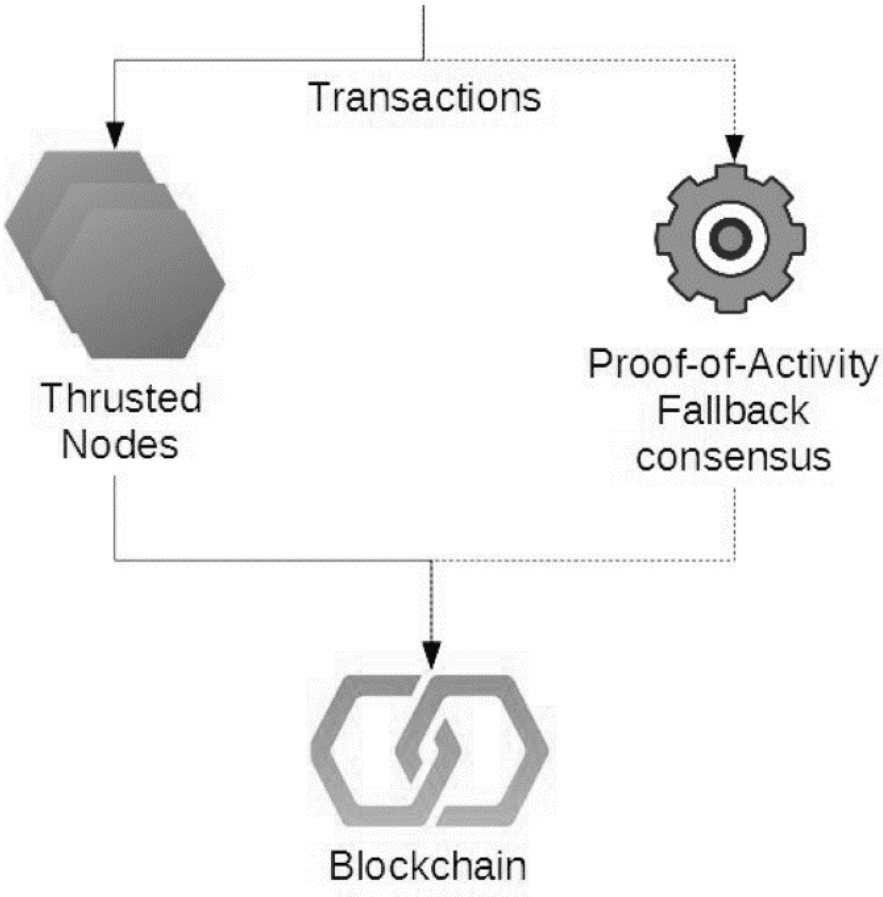
— Hash block SHA256.
— The sequence number of the block.
— Block generation start time.
— Time of block generation completion.

— Digital signature.
— Data of the block.

1.3. Features of the blockchain

— One-dimensional blockchain (1 transaction – 1 block).
— DLCPoA block generation algorithm securely protects the network from spam and fake transactions, while not requiring significant computing resources.
— Absence of mining in the system.
— Transactions in the platform network are free of charge.
— Network speed: up to 1000 smart contract requests per second.

1.4. The scheme of work of the transaction system



Proof of Authority are nodes that work with keys issued at the launch of a blockchain network. They are used to speed up transactions by the absence of distributed consensus (blocks are considered valid if signed with the key of one of the Trusted Nodes).

Proof-of-Activity Fallback Consensus is an additional system of consensus in the network. Completely decentralized, used for the first launch of the network.

Time-dependent DLCPoA is used for distributed consensus..

DLCPoA (Dynamic Limited Confidence Proof of Activity) is a modification of the LCPoA algorithm with a configurable complexity of block generation.

LCPoA (Limited Confidence Proof of Activity) is a hybrid algorithm of a blockchain network consensus that consists of two technical elements:

1. Proof of Activity – a principle that aims at a task similar to the Proof of Work principle, but with significantly reduced complexity, due to which the process of solving a task takes from a fraction of a second to several minutes.
2. Limited Confidence – a system of automatic creation of «control points» in a blockchain network.

1.5. Advantages of LCPoA Consensus Algorithm

— The average speed on devices of different classes is 1 block in 5 seconds.
— The limit of maximum block selection speed for all devices is 1000 hashes per second, which makes the use of miners senseless.
— Block generation can be easily performed by a device of any power.
— Completely decentralized algorithm; all that is required to generate a new block is information about the last block of the network.
— No tokens or rewards are required in the network for operation.

1.6. Security and a 51% Attack

Basically, with no defense by the Limited Confidence mechanism, the described option of Proof of Activity itself is highly vulnerable to a 51% attack. With the use of Limited Confidence – a 51% attack is possible only on very few blocks, which makes it pointless in most cases.

DLCPoA is a consensus algorithm that allows adjusting the speed of the network. A corresponding hash - the validity of which is determined by certain filters – must be found to generate a hash of a new block in the network. With the LCPoA algorithm, filters are set in the configuration, while with the DLCPoA, filters are determined automatically by the formula based on the speed of the network. If the speed is close to the target, the filter becomes more complex; if it is far from the target, the filter becomes less complex, up to zero complexity when any hash fits.

Formula that determines the complexity of a network

$$\sum \text{abs(log10(1000 — distance between the blocks in ms) / (1000/ target speed of the network)}$$

Formula that determines the selection of a hash

$$\sum \text{hashSigma* <= round(allowed number of hash variables — (allowed number of hash variables * complexity)}$$

**hashSigma: the latter 6 or more hash characters in hexadecimal representation, i.e. 6 bytes*

Dynamic configuration of the algorithm's complexity enables preventing attacks on the speed of the network and maintaining the network operable under any loads.

1.7. Description of the work of System's blockchain network

Blockchain of the System will use smart contracts running in a special execution environment called EcmaContracts, which uses JavaScript engine V8 for creating a virtualized execution environment for the

code of contracts. Thus, it will completely isolate arbitrary contract code from both the system and other contracts, and control the availability of resources (RAM, CPU time, request limits) for each entity of a virtual machine.

EcmaContracts implements the principle of contract entity state management, where only data about requests to smart contract methods and their arguments is stored in the blockchain. The results of smart contracts' performance are stored locally on the user's node and loaded the next time the contract is triggered. All nodes in the network simultaneously repeat each transaction in the chain from the first block to the last existing one, resulting in complete synchronization of contract states on every node.

1.8. Language of smart contracts

The smart contract execution system allows creating contracts using JavaScript ES6 language. Smart contracts are Turing-complete and have a wide range of features. Most standard methods and classes are available.

1.9. EcmaContracts

EcmaContracts provides an environment to manage and execute smart contracts.

EcmaContracts monitors the state, running virtual machine entities, resource usage, and provides contract execution environments with the necessary methods and objects to operate. Interaction with such objects enables the deployment of efficient and functional decentralized systems.

1.10. DApp

The use of Decentralized Applications (DApp) in the network enables additional functionality for the node. DApp applications have wide functionality:

1. Interaction with a chain of blocks, pre-processing, reaction to changes in a chain.
2. Interaction with smart contracts, including the launch of new ones.
3. Interaction with other decentralized applications through built-in protocols.
4. Integration of centralized applications with decentralized ones.

2. General platform description

2.1. Glossary

SmartBoard Coin (SBC) – Utility-token for making payments for internal services of the platform.

Currency token (hereinafter referred to as «T-Token» / «T-Currency» or «Currency token») – a token that substitutes the real cryptocurrency intended for transactions within the ecosystem. Behind each unit of currency tokens lies the original cryptocurrency stored in a controlled wallet.

DAC – decentralized autonomous company. Collective account for storage and management of digital assets (SBC + 1 currency of choice). It can emit crypto shares, backed by the balance of the organization.

Member (DAC) – a member of a company (DAC). Eligible to submit different actions for voting and sign other votings. A member of a DAC may not be a shareholder.

Shareholder (DAC) – a user who bought DAC crypto shares. Can take part in voting (if the rules stipulate so). Can not initiate voting.

DAF – decentralized autonomous fund. Collective multi-currency account for storage and management of digital assets (SBC + 1 currency of choice at the beginning, and the rest could be unlocked after creation) and crypto shares of other companies (DAC). It can issue its crypto shares backed by the fund's balance. The fund's shareholders can participate in the management of other organizations, which crypto shares are held on the fund's balance; they can also propose and sign actions on behalf of the fund.

Shareholder (DAF) – a user who bought DAF crypto shares. Can participate in and initiate votings.

The right for voting – the right to initiate votes. Members of the DAC and shareholders of the DAF have the right to initiate votings.

Signature right – the right to sign votings. In DAC, the signature right is possessed by members and shareholders (including funds). In DAF, the signature right is given to the shareholders of the fund.

Digital shares of funds and organizations – crypto shares establish rights to the property of organizations and can be used as a management tool in voting.

SBC (SmartBoard Coin) token – a token for payments for internal services of the platform.

Digital Signature – password to confirm actions.

2.2. Digital assets

Digital assets are internal tokens used for various purposes in the ecosystem.

Cryptocurrencies accepted in the system:

— Bitcoin.
— Ethereum.
— USDT (ETH).

The emission of T-currency tokens is carried out by a service contract that creates T-currency tokens in an equivalent amount to convertible funds.

T-currency tokens transfers

T-currency tokens can be freely transferred between organizations and users within the ecosystem, and operations about these movements are recorded in the blockchain.

Types of T-currencies in the ecosystem (internal system tokens - analogs of cryptocurrencies):

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

Rules of exchanging cryptocurrencies into T-currencies

The exchange is made in a ratio of 1:1 excluding the fee that is charged from users.

In the process of the return conversion, T-currency tokens are eliminated, releasing an equal part from the platform's wallet to the user's personal wallet on the platform in a 1:1 ratio, without including the fee charged from users.

The conversion for deposit and withdrawal is performed automatically.

Exchange of currencies within the System is performed through integration with a third-party service – CoinPayments.

Internal purchases

All internal purchases can be made from the balance of T-currency tokens (T). They are used for buying company shares.

Internal purchases are made without any additional information, but if a digital signature is enabled in the settings, signature confirmation is requested when performing actions (crypto shares purchase/elimination; buying SBC; transactions; voting signature).

In order to emit SBC, users have to top up their T-currency balance first and then convert into SBC with:

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

Digital shares of an organization may be acquired with currency tokens. 1% crypto shares = 1% of the company's property (currency tokens). Crypto shares can be eliminated, and your stake can be withdrawn from the balance of the organization to your personal account.

In case of obtaining an irrational figure in the system, such figures are rounded to 2 decimals (to the lesser side).

Members buy back crypto shares after the organization is created.

In case of crypto share elimination, currency tokens equal to their shares are destroyed, and T-tokens are transferred to the user's personal wallet.

Exiting an organization entails the destruction of crypto shares, signature rights, and allocation of equal shares to the user's personal wallet. It is impossible to eliminate without owning the signature token (in case of its transfer).

2.3. Tokenomics

Emission limit: 1 billion SBCs.

Emission: circulation of new coins is generated by users exchanging cryptocurrencies to SBC at a fixed rate, according to the PFP algorithm.

Emission algorithm: Proof Freeze Provision – platform users create new coins by exchanging cryptocurrencies to SBC at a fixed rate of $ 1. The exchange process takes place inside the personal cabinet on the platform. The funds received for the SBC exchange will be frozen in an open account. All accounts will be available for auditing.

Initial emission: 150 million SBCs.

Rules for selling tokens after the initial emission: other tokens will be sold at the rate of SBC. Funds from the sale will be frozen; in the future, it is planned to provide the possibility of SBC buy-back.

SBC exchange rate: initially equal to $ 1. After being placed in the market, it may change. The indicator is dynamic.

Elimination: the number of SBCs decreases as users pay for the platform's internal services (tokens are burnt). Internal services paid for in SBC – this is the creation of DAC, DAF, as well as unlocking additional accounts for T-currencies in DAF.

2.4. User registration

At registration in the system, users create a login and password. Also, the user ID for identification in the system is set (can be set in the personal cabinet after registration).

During registration, every user gets a generated account/wallet for operations inside the system:

— SmartBoard Coin.
— (T) Bitcoin.
— (T) Ethereum.

— (T) USDT (ETH).

These accounts are linked to the user account. With balance funds, it is possible to make direct purchases with SmartBoard Coin using a password and two-factor authentication (if enabled).

For Ethereum, Bitcoin, and USDT (ETH) cryptocurrencies, input/output processing is performed via CoinPayments service integrated into the system.

2.5. Wallet

Each wallet has an internal address to which all digital assets within the ecosystem are linked. It is possible to send tokens to the internal address inside the network with no fee.

The system automatically separates internal addresses from external (other blockchains) and performs the required transaction.

The following cryptocurrencies are available for storage in the wallet:

— SmartBoard Coin.
— (T) Bitcoin.
— (T) Ethereum.
— (T) Tether (ETH).
— Криптоакции.
— Права подписи.

3. DAC – decentralized autonomous company

Decentralized autonomous company – collective cryptocurrency account with a detailed configuration of internal rules.

3.1. Company configuration

3.1.1. Currency selection

In addition to SmartBoard Coin, DAC can store one currency of choice:

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

3.1.2. Team settings

Members are invited through an internal @ID. Each member receives an invitation when all rules have been configured by the creator of the organization. After creation, members receive the signature rights in the wallet.

Signature right provides an opportunity to take part in voting. Transfer of signature rights is determined at creation.

Removal of members: the vote of an excluded member is not taken into account at voting. The removal leads to alienation of the signature right.

3.1.3. Configuration of crypto shares

The emission of crypto shares is set during creation. The initial amount of the emission is limited by the range from 10 to 1000 crypto shares. Crypto shares have to be bought back after the creation of the organization. Crypto shares can be bought by any user of the platform.

Crypto shares can be transferred freely within the ecosystem.

The price of crypto shares is set in the selected currency, and payment is made in currency tokens.

3.1.4. Configuration of transactions

Transactions in the system are any transfers of digital assets (internal purchases, direct transfers, external transfers). These settings regulate the rules of execution of all actions.

There are 2 types of rules in transaction settings: general and private.

The general rule is mandatory and applies to all transactions that are not covered by private rules. Private rules allow creating a distinct rule for transfers that exceed a certain amount. There can be several private rules, but only one general rule.

Example. If a general rule is set for all transactions and a private rule is set for transactions of >100 USDT, then when sending transactions of less than 100 USDT, a general rule will be applied; when sending transactions of more than 100 USDT, a private rule will be applied. Besides, you can set one more private rule >1000, then within the range from 100 to 999, the first private rule will take effect, and within the range from 1000, the second private rule will be applied.

3.1.5. Creation of a company

After all rules are configured, the creator of the organization sends an invitation to the selected members. To create a company, you need to obtain consent from all members. The fee for creation is paid by the creator. The creator gets the right to change the description of the organization and its logo.

3.2. Rules Constructor

The Rules Constructor allows configuring execution conditions in detail for different actions.

The constructor has 3 types of different signatures:

1. Signature of a particular member.
2. Shareholders voting.

3. Members voting.

Members and shareholders – 2 different types of roles in the company. A member may be a shareholder, and a shareholder may be a member. However, there may be members of the company that belongs to only one category. They are members but have no crypto shares or vice versa.

In case a user is both a member and a shareholder, they vote once.

Signature approval procedure

All types of signatures are obligatory for execution if they are placed in one “book”.

Alternative rule

An alternative rule allows you to set an additional condition for the execution of an action. It acts on a par with the general rule.

3.3. Company management

3.3.1. Voting process

To confirm the action, it is necessary to meet the condition of the general or alternative rule.

Voting is held within 24 hours. During the voting, the opportunity to transfer signature rights is locked.

3.3.2. Management of crypto shares

Additional emission is made at a determined fee. DAC crypto shares can be purchased by users and autonomous funds.

3.3.3. Team management

Adding new members can be done by internal @ID. New members obtain the right to vote in “members votings”.

Removal of team members causes alienation of signature rights. If a team member has crypto shares, after the removal from the team, they remain as an investor, but without the authority of a member.

3.3.4. Exiting from the organization

A shareholder that owns crypto shares in the company may exit from the company. Exiting the DAC entails the elimination of the crypto shares and the allocation of an equal stake from the company's balance sheet to a personal account.

4. DAF – decentralized autonomous fund

Decentralized autonomous fund – a collective cryptocurrency account with a multicurrency wallet and the option of purchasing crypto shares of other DACs.

4.1. Fund configuration

4.1.1. Currency choice

Besides SmartBoard Coin, DAF can store 3 currencies, one is selected at the creation, 2 others are unlocked after the creation:

— (T) Bitcoin.
— (T) Ethereum.
— (T) USDT (ETH).

4.1.2. Team settings

Members cannot be defined in the autonomous fund at the creation. All members of the fund are shareholders who buy crypto shares of the fund after its creation.

4.1.3. Configuration of crypto shares

Emission of crypto shares

It is set at the time of creation. is set during creation. The initial emission is limited from 10 to 1000 crypto shares. Crypto shares have to be bought back after the creation of the organization. Crypto shares can be bought by any user of the platform.

Crypto shares can be transferred freely within the ecosystem.

The price of crypto shares is set in the selected currency, and payment is made in currency tokens.

4.1.4. Configuration of transactions

Transaction types:

1. Direct transaction (internal, external).
2. Buying DAC crypto shares.
3. Buying SBC.
4. Unlocking of additional accounts.

4.1.5. Management configuration

a) The rule for selling crypto shares shall be defined for all operations with crypto shares on the fund balance:
    1. Listing for sale.
    2. Removal from sale.

Funds from sales are transferred to the general account.

b) Decision-making rule in subsidiaries stipulates the condition for a proposal to act on behalf of the fund.

4.1.6. Fund creation

After all rules are configured, the creator of the organization buys at least 1 crypto share and creates a fund. Other members of the fund buyback crypto shares after the fund is created.

4.2. Fund management

4.2.1. Voting process

The established consensus of shareholders must be respected to confirm the action.

Voting is held within 24 hours.

4.2.2. Management of crypto shares

a) Management of own crypto shares: additional emission is made at a set fee. DAF crypto shares can only be purchased by users.
b) Management of third-party crypto shares: fund shareholders may offer to purchase crypto shares of other DACs. Any shareholder can offer the purchase. The rule of purchase is regulated by the transaction rule.

Sale and removal from the sale of crypto shares are regulated in the management settings by a special rule. Crypto shares can be bought from funds by users or other funds. Funds from sales are transferred to a general account.

4.2.3. Management of subsidiaries

Any shareholder of the fund holding crypto shares in the company may offer to make an action in the company on behalf of the fund.

Types of action

1. To propose a voting.
2. Vote for.
3. Vote against.

The proposed action shall first go to the fund and shall be voted on. If it is accepted, it is submitted to the voting in the subsidiary company.

4.2.4. Exit from the fund

Exiting the fund entails the elimination of crypto shares and the allocation of an equal part of all funds from the fund balance. SBC, currency tokens, DAC crypto shares may be among the fund's funds.