DSP

Decentralize Social Platforms

The purpose of this document is to present some technical aspects of our DSP blockchain-based platform. The first version is designed to give the DSP community the possibility to evaluate and give feedback for the selected implementation details. Please note that they can still change. We are going to work with this document further and evaluate new technical possibilities that might come during the fourth quarter of 2017.

C
O
N
T
E
N
T
S

T A B L E O F

DSP PLATFORM BACKGROUND

The DSP Marketplace is a platform that will unite safe trading and social interaction between users. The business functionalities that are required here will make the difference in trading sector demand secure and reliable technology. The goal is to utilize the Ethereum open-source blockchain-based platform and its smart contract functionality to implement a patent-pending interactive item card, secure payments and DSP social rewarding system. More information about DSP Marketplace concerning those crucial functionalities of the platform from the business perspective (and ICO details) can be found in the DSP Whitepaper accessible at.

ARCHITECTURE DIAGRAM

There are many ways (some still in development or alpha version) of building an Ethereum node network. Two leading solutions are:

- installing full Ethereum nodes on users devices,
- using other, lighter programs/solutions that allows to sign transactions (like MetaMask [1]) and running them against a hosted node cluster (like INFURA [2]).

In order to let users run the application without requiring users to install their own full Ethereum node, we are going to use a hosted Ethereum node cluster. The blockchain architecture will be used to handle the DSP digital currency and to ensure durability and immutability of the product and its history.

Processing and storing data in DSP will be provided by DSP REST API. This solution allows access to data over the network, regardless of device type (through a web application or dedicated mobile app). Applications will communicate with DSP REST API over HTTPS (secure communication protocol), using JSON as message format.
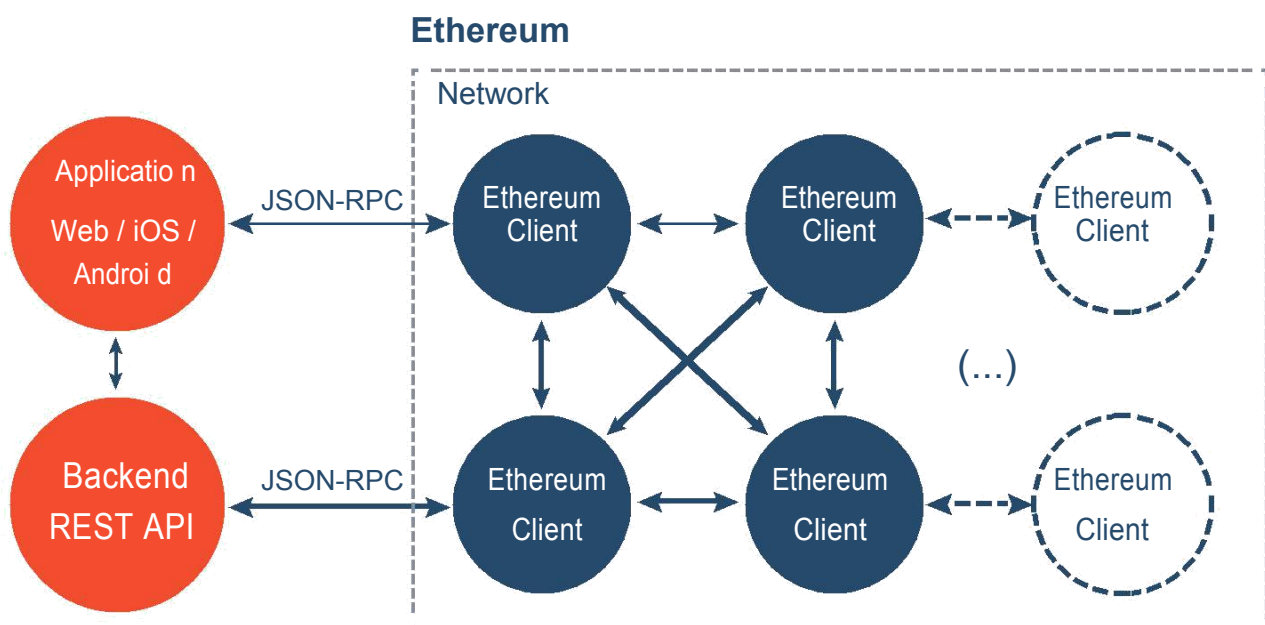
SECURITY

BLOCKCHAIN LEVEL SECURITY

Decentralization through the use of blockchain technology has many security-related advantages, like:

- **Immutability** - blockchain keeps track of all the changes that have been made,
- Protection against data corruption - each computer has a copy of the database, therefore it would be necessary to simultaneously corrupt data on more than 51% of the participating computers.
- **Reliability** - it is highly unlikely to simultaneously stop all the computers participating in the Ethernet blockchain.

CONTRACT LEVEL SECURITY

What can be done on developer-side is to write secure Ethereum contracts, following the Best Practices [3] for smart contracts which describe particular security techniques and tips. For the same reason, we are planning to build contracts using the OpenZeppelin [4] library which greatly aids in writing secure smart contracts on Ethereum. This open source library provides tested and community-audited code that can be implemented and extended by developers so that they can write their own secure contracts. Before implementation, each piece of code will need to pass a code review and tests (read more in Tests chapter). In order to increase trust and maximize security, code audits are also planned.

[3] https://github.com/ConsenSys/smart-contract-best-practices
[4] https://openzeppelin.org
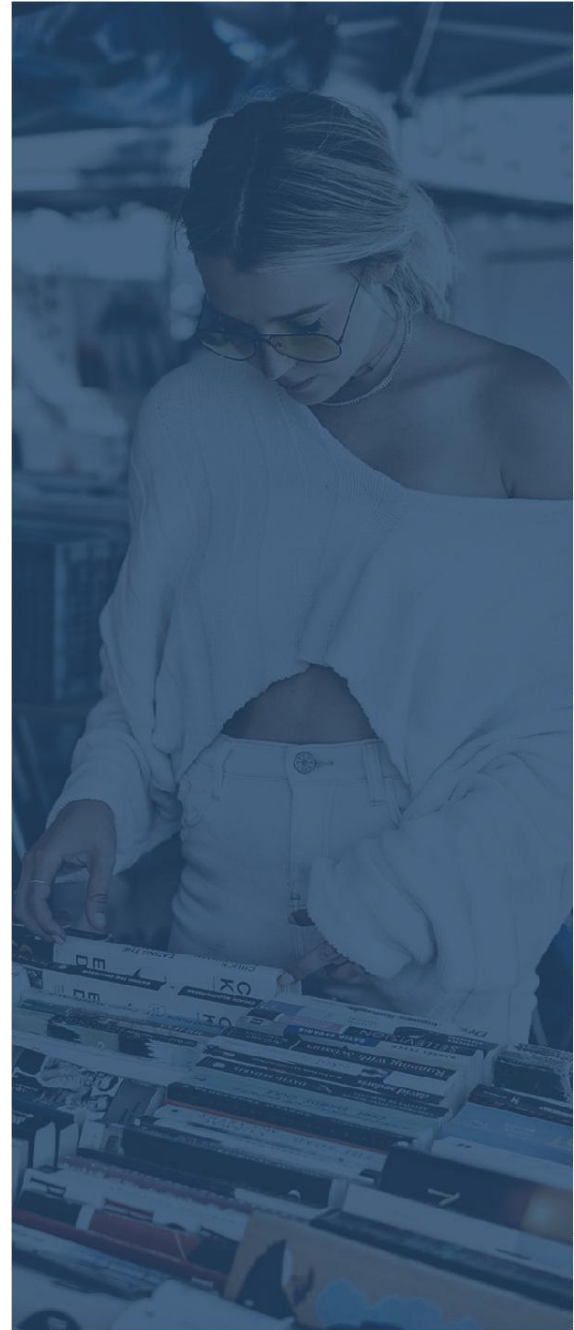
DSP COMMUNITY TOKEN

DSP Community Token, called DSP, is an internal digital currency, which will be used in DSP Decentralized Social Marketplace. It is planned that all transactions will eventually be paid in digital currency.

All users of the DSP platform will be able to gain DSP in various ways:

- By buying them for Ether during the ICO (read the ICO Specs Whitepaper for details).
- Exchanging Ether to DSP using DSP Exchange (read more in Buying DSP chapter).
- As a payment after a successful purchase transaction.
- As a reward or compensation after promoting a product (read more in Promoting item using DSP chapter).

IMPLEMENTATION OF DSP

DSP is an ERC20 Token implemented as a contract in the Ethereum blockchain app platform. The Ethereum Contract for DSP Community Token and all other contracts will be written in Solidity (programming language), as it is "currently the flagship language of Ethereum and the most popular" [5] . All Decentralized Social Marketplace users will collect their DSP in Ethereum Wallet.

BUYING DSP

DSP Community Tokens can be acquired (in exchange for Ether) during the ICO. After the completion of the ICO, purchasing DSP for Ether will be available via the DSP platform. The price of DSP will be set according to its current price on the stock exchanges.

DSP will provide a "liquidity reserve" of DSP, which will only be utilized in a theoretical situation, for instance, if after the ICO the DSP is not liquid enough to support the functioning of the DSP platform.

[5] http://www.ethdocs.org/en/latest/contracts-and- transactions/contracts.html#ethereum-high- level-languages

DSP INTERACTIVE ITEM CARD

DSP Interactive Item Card (IIC) is a digital representation of the physical item. It includes information about the ownership data, the condition of the physical item, the genuineness of the item and the price history. Once created, IIC can be modified or can change its owner (be bought), but every state and every change will remain in its history.

To achieve what is promised above, IIC data will be stored in two areas:

- all data (and history) will be stored in database (eg. with use of Event Sourcing) and server space (eg. to keep photos)
- item key information, link to database data and data signature will be kept in the blockchain.

The DSP, IIC contracts will be written in the Solidity programming language.
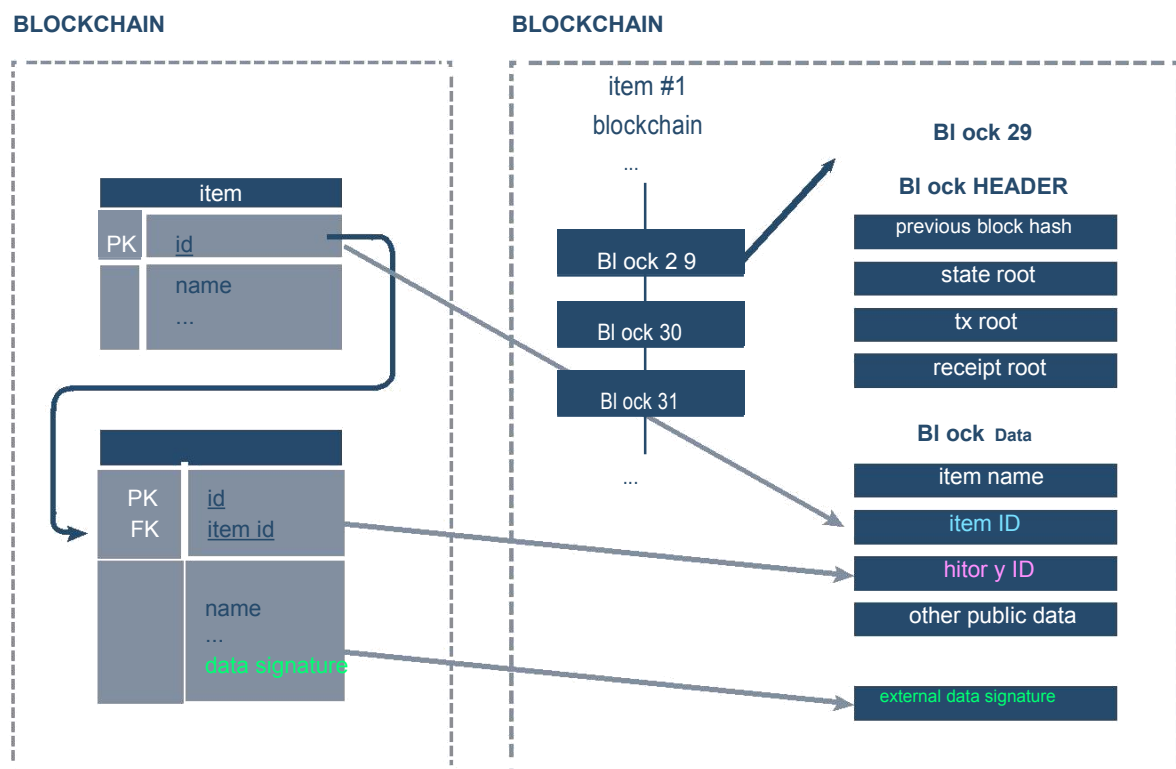
PROMOTING ITEMS USING DSP

An item owner will have the possibility to involve other community members in promoting their product and, consequently, increase interest and trust in it.

Users that were chosen by the item owner to engage in its promotion will, after a successful transaction, be rewarded with DSP by the seller. Please note that DSPs for prizes will come from the owner's wallet. This means that item owner will need to have DSP on his account to make his product promotable.

When a seller orders a promotion, his DSP will be transferred to the prize contract, and will remain there until a successful buying transaction occurs or when the promotion is cancelled. In case the promotion is cancelled, the DSP will return to the item owner's wallet, after paying compensation.
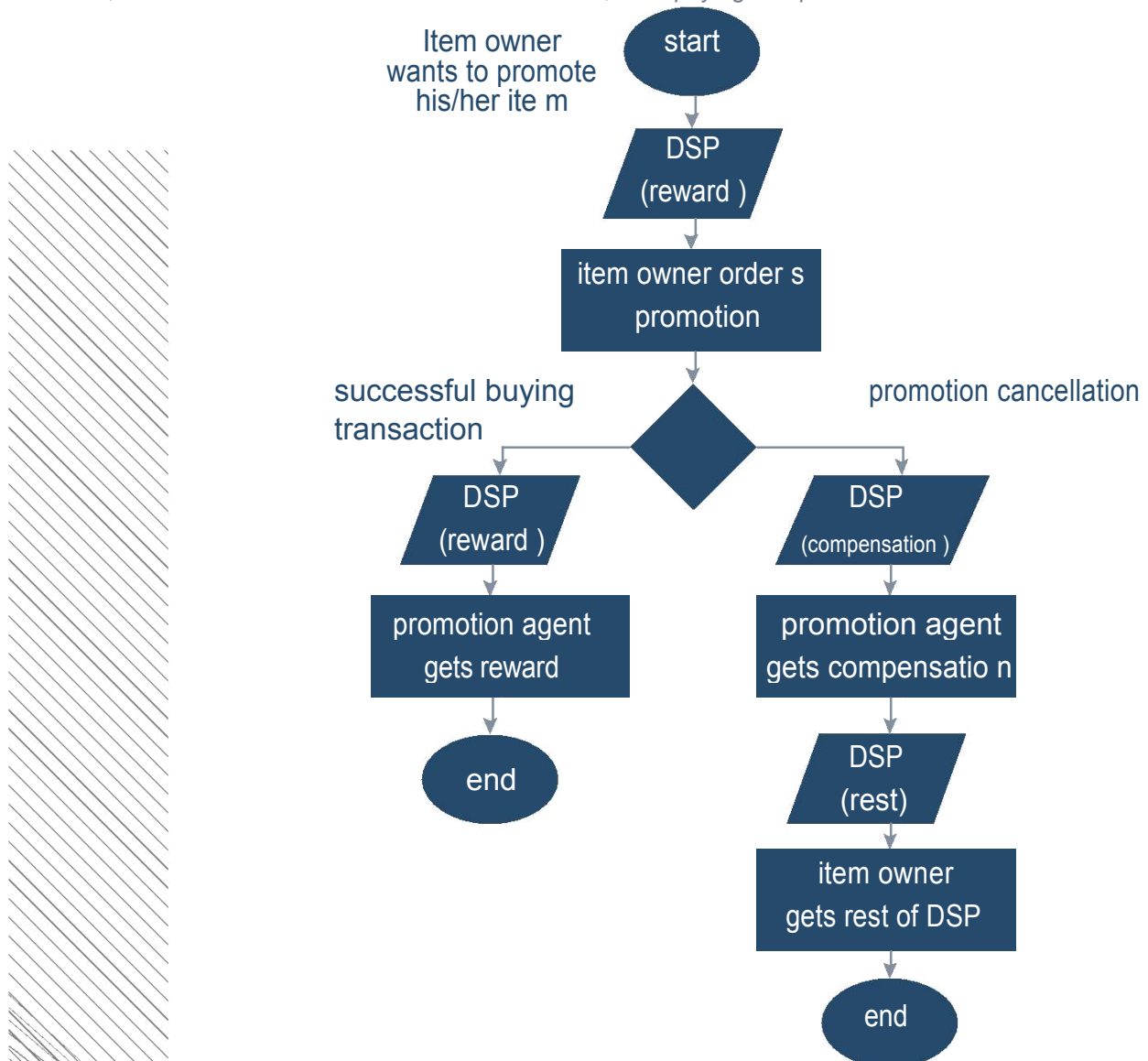
TESTING CONTRACTS

All contracts will be tested with one or more of the following methods:

- going through test scenarios in manual testing
- automated functional tests
- automated unit tests

It is planned that all contract functions will be tested with unit tests. Using solidity-coverage [6] to measure code coverage, we plan to have a full test suite, close to 100%. For test writing and their automation, we plan to use Truffle [7], which comes with an automated testing framework. Thanks to this, developers have the possibility to test contracts in two important ways:

- make advanced unit tests using Solidity language, so the whole test suite can be build,
- make contracts to be tested from the outside world. These tests needs to be written in JavaScript. Truffle integrates with Mocha [8] framework, that allows for running these tests asynchronously and serially.

In order to test contracts and transactions without additional costs (gas), tests in the development process will run on a test Ethereum network. For this purpose, we plan to use public testnet Ropsten. Before deploying, smoke tests will run on Mainnet (real-world Ethereum network).

[6] https://github.com/sc-forks/solidity- coverage
[7] http://truffleframework.com
[8] https://mochajs.org
[9] https://raiden.network
[10] https://raiden.network/faq.html

GAS

When a contract is executed, as a result instruction is executed on every node of the network. This has a cost: gas is the name for the execution fee that senders of transactions need to pay for every operation made on an Ethereum blockchain. This fee is paid in Ether and will be covered by DSP in most of the transactions. Users Wallets will be topped up by a small amount of Ether - enough to be able to perform one transaction. After each transaction, the user's wallet will be refilled, so they can perform the next operation. It is also planned to implement solutions that reduce transaction costs, like The Raiden Network [9] or other. The main idea of The Raiden Network is to run some transactions off-chain, without involving the Ethereum blockchain for every transfer. Although running off-chain, the Raiden Network promises to ensure transfers with guarantees of finality, security, and decentralization similar to those known from blockchains. Ethereum transactions are public, whereas Raiden transfers are private between the payer, the payee, and the nodes forwarding the transfer. When channels are settled, only the sum of transactions will become visible to the world. [10]

DEVELOPMENT PLAN

CLOSED ALPHA RELEASE

For the Alpha release planned for Q3 2017, the DSP platform with the most important functionalities is developed. In the same time UX/UI for iOS application is designed. The DSP - A application for iOS is accessible in TestFlight application in external testing mode. The application allows for:

• managing Item cards

• searching, listing and viewing Items

• give opportunity to real time chat in the context of selling and buying items

• provide social actions like giving product 'a like'.

DSP MVP

The release of the minimum viable product is scheduled for the Q2 of 2018. The most important goal for the MVP is to integrate the DSP platform with the blockchain.
The functionalities that are planned to be implemented :

• Extending DSP backend API

• Extending social functionalities in DSP backend

• Possibility to connect to Ethereum network.

• Ether transfer for gas payments.

• Make exchange Ether to DSP available.

• Provide the ability to pay for the product using DSP

• Web interface release

• Extension of iOS application

Development of the infrastructure and the safety plan implementation will follow the MVP phase and will continue in parallel to platform growth. The plan is for the DSP platform to be available to the widest possible audience - for this purpose, solutions for a variety of devices are being considered.

DSP PLATFORM Q2018 4

• DSP Secure payment

• Implement an interactive item card with smart contract

• Provide product promoting (with DSP payment)

• Android app release

DSP PLATFORM 2019

• Reselling items

• Rewarding system

DSP PLATFORM 2020

• Modules prepared for Business accounts

• Integration with Internet of Things