Dex DEX (Decentralized Exchange)

General description

DEX – a new exchange, based on the blockchain technology BitShares 2.0 (Graphene), representing decentralized platform for highly effective financial operations based on Smart contracts.

DEX is a decentralized trading platform, which has all the pros of standard centralized exchanges excluding their inherent drawbacks, the main ones being vulnerability to direct hacking and practically full control over clients' funds by a third party (exchange representatives and government officials).

Structure and functionality of DEX is standard for the exchanges built on Bitshares:

The main functionalities include:

- Registration/Authentication of users;
- Trading;
- Transfer of funds;
- Voting; Token creation;
- Observer.

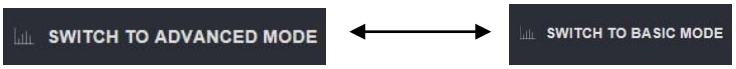
The main distinctions of DEX are:

- Personal gateways for deposit/withdrawal of 10 cryptocurrencies; Possibility of customizing UI (User Interface configuration)

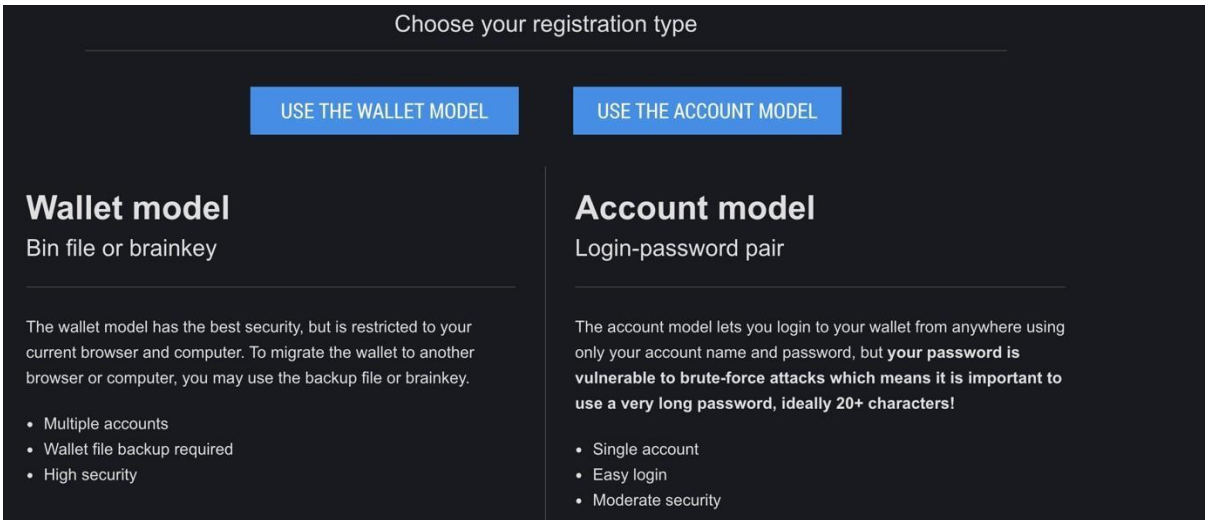
1. Accounts

Authorization and registration are done directly in the BitShares blockchain. There are two types of supported accounts: Regular and Multi-sign. All the balances of each account could be used on DEX as well as in the whole Bitshares network. View of the initial page of DEX is as follows. The view of upper panel menu for unauthorized user:

Switching between ADVANCED/BASIC modes is carried out by clicking on corresponding element of the panel.



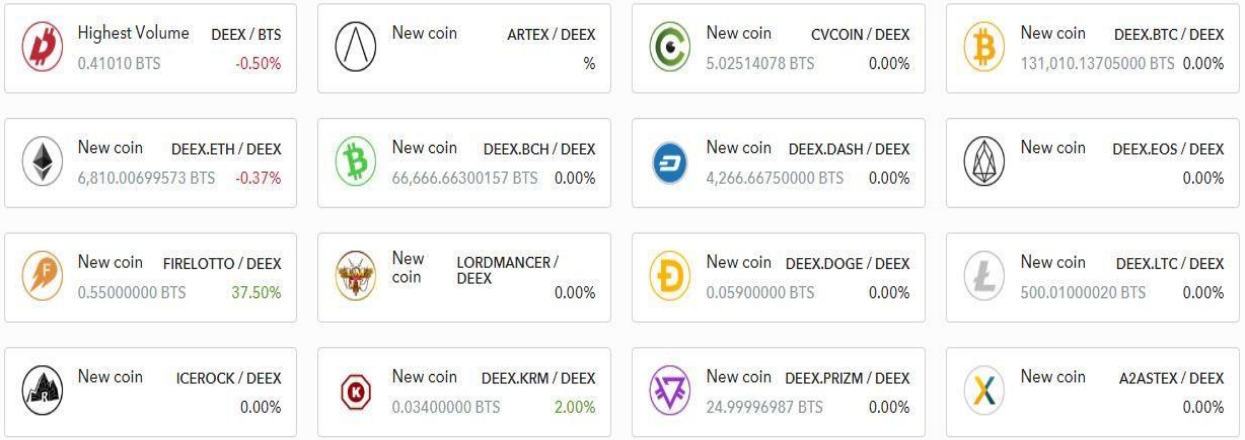
The view of central part of the initial web page with choice of account model for subsequent creation.



2. Main page

The view of upper menu for authorized user is as follows:

The view of main page for authorized user in Advanced mode:



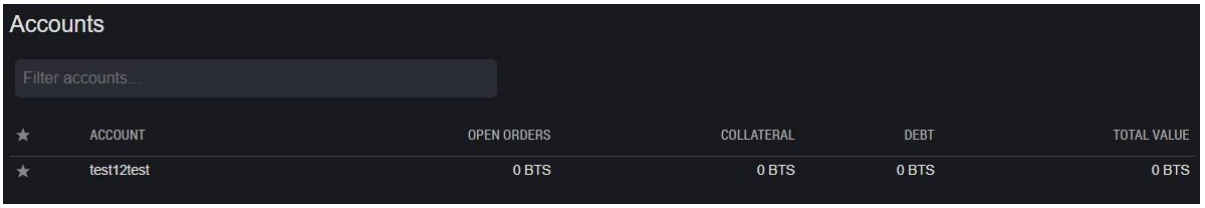
The main page includes information about given currency pairs and consists of following elements:

- Currency icon;
- Name of currency;
- Price;
- Volume;
- Growth rate change in %.

After authorization on the main page, a user is additionally displayed: a table with list of accounts in a wallet, a table with history of recent activity (on every account in a wallet) and also advanced upper menu.

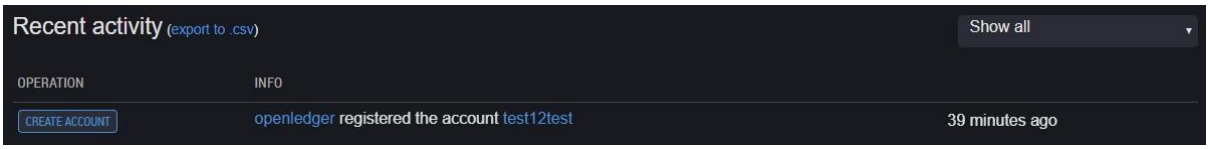
The table with a list of accounts in a wallet:

- Name;
- Open orders;
- Collateral;
- Total value.



The recent activity table (sorted from new to old):

- Operations;
- Information.



The upper menu includes following elements:

 Logo (transition to main page);

- Account (only for authorized users);
- Send (only for authorized users);
- Exchange;
- Deposit/Withdraw funds;
- Balance (only for authorized users);
- Name of account (only for authorized users);
- Language of interface;
- Settings;
- Lock down icon (only for authorized users); Create an account (only for authorized users).

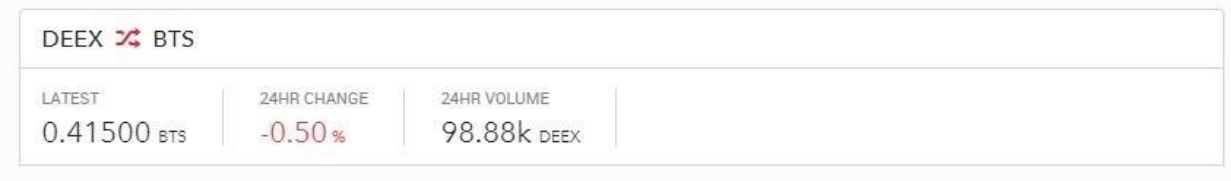
3. Exchange and its functionalities

Functionality of the exchange will include all the functionality of the BitShares. Separately created gateway allows to deposit and withdraw funds only in the chosen currency. On the exchange itself all sorts of tokens can be used that are available in the BitShares network. There is a possibility of market analysis for a given trading pair on a trading graph of the exchange and buy/sell trade execution. Also lending of necessary quantity of tokens are possible for short positions.

3.1. The Main market indicators

On the corresponding panel, current main indicators of the chosen trading pair are shown:

- Current price;
- Change tendency;
- Percentage growth in the last 24 hours;
- Volume for the last 24 hours on each trading pair;
- Current market price.

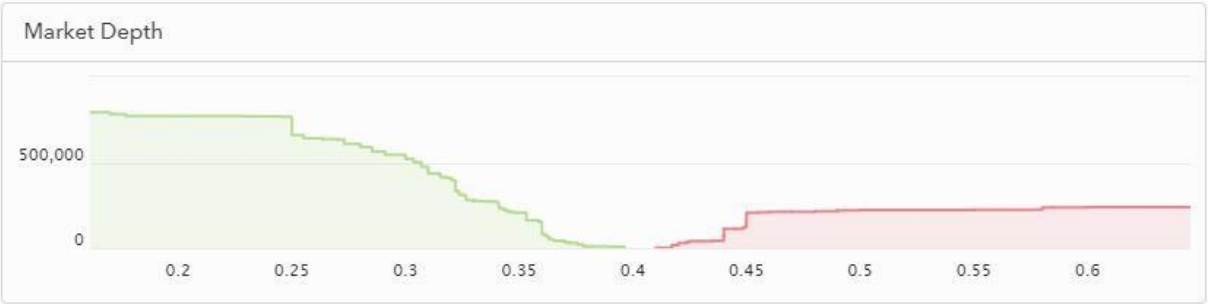


3.2. Price Chart

Graph of market price change of chosen trading pair. Graphs include possibility to choose displayed time interval (6 h, 2 days, 4 days, 1 week, 2 weeks, 1 month, 3 months, all) with adjustments to every value (5 minutes, 1 hour, 1 day). Also options of manual adjustments are present.

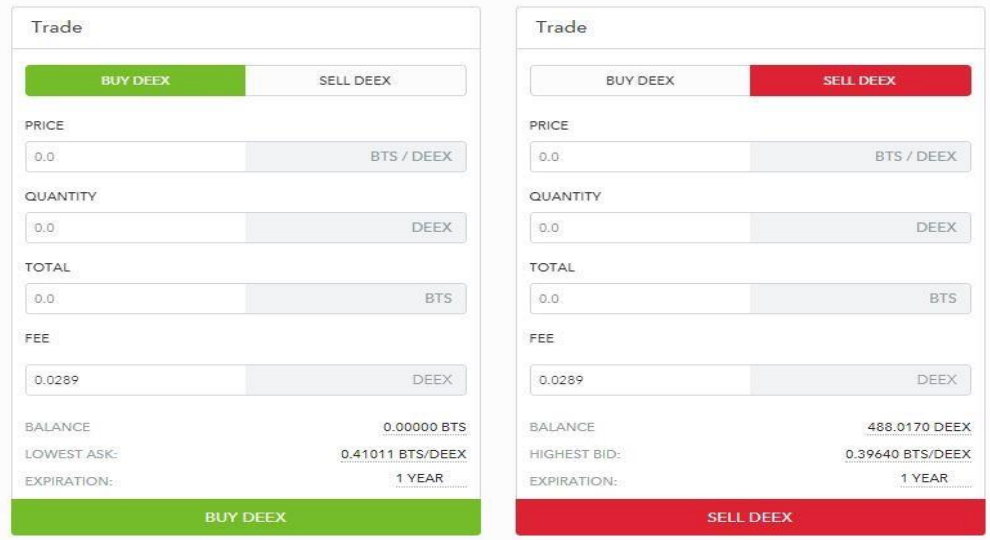
3.3. Market Depth graph

Graph of purchase/sell price and volume change from market price. Maximum prices of purchase and sell are displayed. Identification of current estimated market price is installed.



3.4. Blocks for conducting trades

There are two trading blocks for executing sale and purchase trades for given currency. In each block current balance of currency available for trade and current price (the highest for sale and the lowest for purchase) are shown.



It is possible to lend necessary currency for execution of quick trades. In each trading block, data entry section, desired amount of a trade and coefficient of debt's coverage by personal funds (collateral ratio) are displayed on the basis of current balance. Validation (confirmation) regarding optimal coefficient of 1,75 or 175% is accessible «below» coefficient.

Two blocks with a list of existing requests to trade in chosen currency pair:

- Open trades for purchase;
- Open trades for sale.

When an existing sale trade is chosen, the purchase trade block is auto filled with the same parameters and vice versa.
Price sorting is available in descending order for purchase and in ascending order for sale. Scrolling and options «Fold/Unfold» can be helpful in extending overview of all possible trades if there are too many of them to fit in the block.

A block with completed trades on chosen trading pair separated on my and market exchange trades presented in form of tabs consists of following options:

- Price;
- Trade volume on each currency;
- Date and time of execution.

A block with open requests on trade in chosen trading pair (waiting to get filled) is presented by following parameters:

- Price;
- Trade volume on each currency;
- Expiration date of a trade.

All prices are highlighted with green (for purchase) and red (for sale).

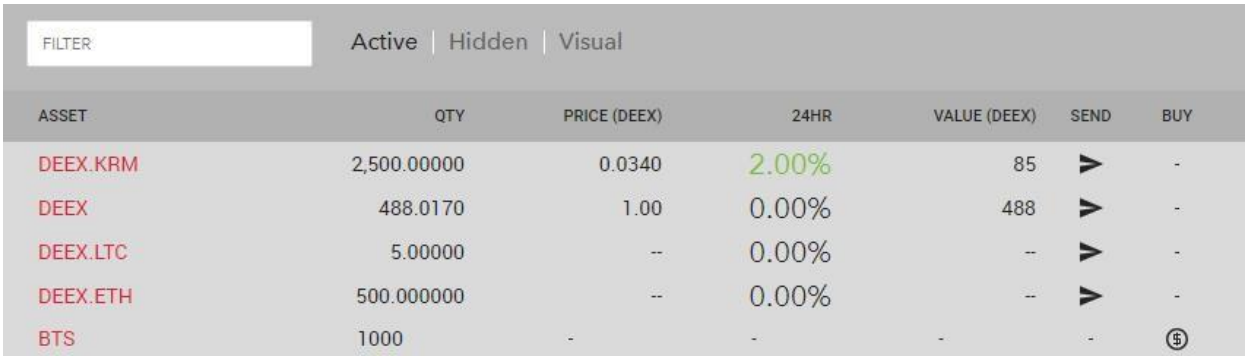
3.5. Block with market information

A block with current market rate is displayed for each currency pairs with search and filter options. There also possibility to choose trading pair by market and name of currency along with opportunity to add currency to favorites. Overview in table of current volume, price and price change is available for period of last 24 hours.
All tables and graphs change dynamically without necessity to press on any button for updating information and indicators.

4. Balance management

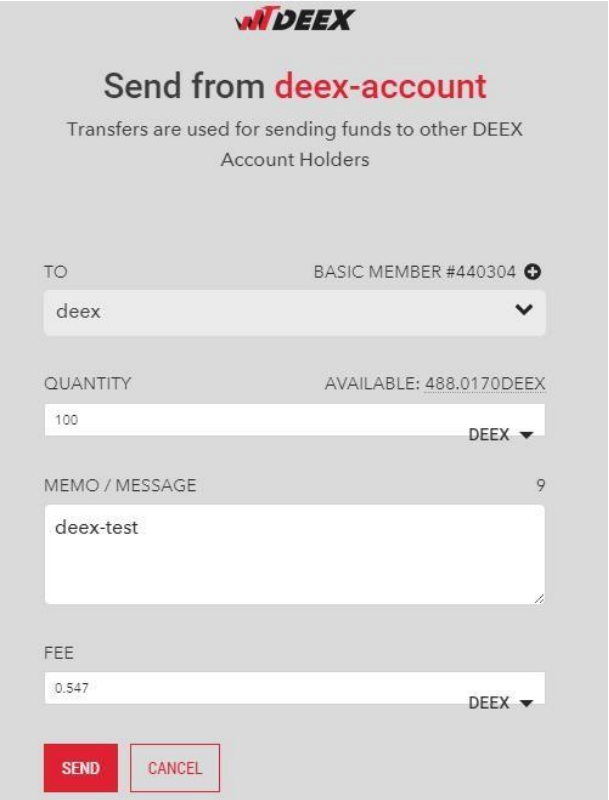
4.1. Account balance

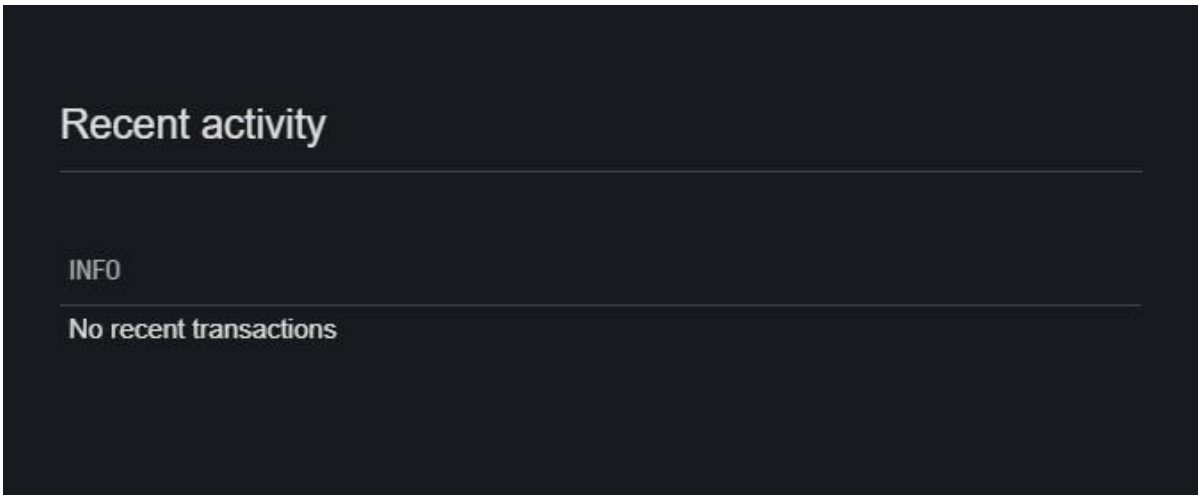
On «Account» tab disposable balance on each currency is displayed. Also for each currency following buttons may be used: «Deposit», «Buy», «Trade».



4.2. Dispatch of money

This option allows send money on every other network account. The box «From» automatically fills with account data of user, in the box «To» receiver-account has to be indicated. In the box «MEMO» desired sum of transfer has to be stated. In the box «FEE» commission on a transfer is written. To the right a block with information about last transfers is situated. Button «SEND» becomes inactive in case when desired sum and commission exceed disposable balance of user.

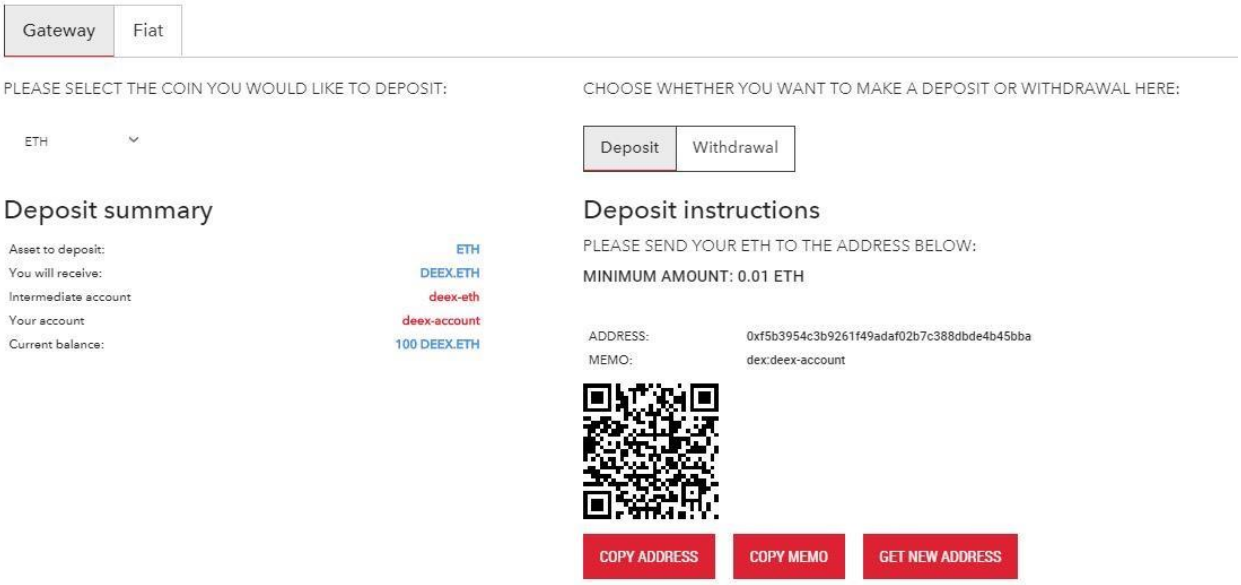




4.3. Money deposit/withdrawal

Option of deposit is available in any currency accepted on the exchange with indication of wallet address of chosen currency. The list of available currencies contains 10 positions. Also any deposit operation always goes with indication of intermediate DEX account.

For withdrawal, it is necessary to specify wallet address of chosen currency. (below in section «currency listing» will be showed a more detailed description of the matter) For receiving funds, it is necessary to send name of your account to a sender.



5. Account settings

When working with the exchange, it is obligatory to backup and configure passwords. Option of password change is carried out with the help of automated password generator (with choice of password type: active, owner, memo).

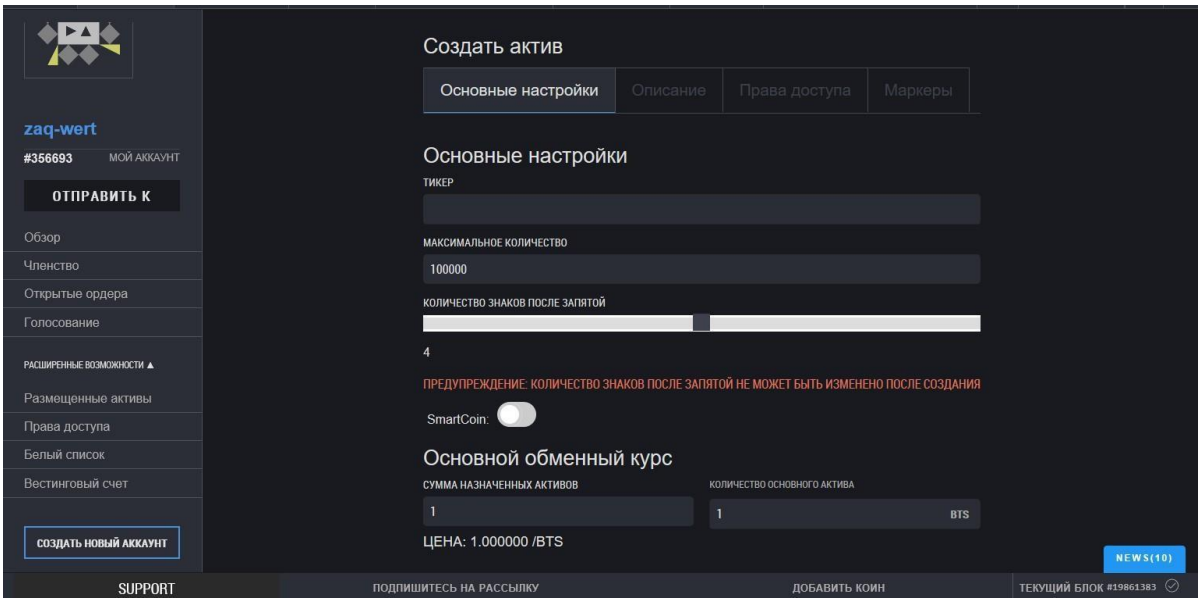
Overview of recent account activity with filter on following operation types:

- All
- Transfer
- Place order
- Cancel order
- Fill order
- Create account
- Update account
- Create asset
- Witness pay withdrawal
- Withdrawal vesting balance
- Feed publication Type of operation, description, name of account and date are displayed.

An Option of adding an account to «white» or «black list». For that, it is necessary to enter account name and confirm a transaction. Validation of decent quantity of funds for fee payment is on the «Ok» button. Overview of an account being added to black or white list.

6. Token creation

BitShares allows certain indiviuals and companies create and issue personal tokens based on BTS for wide variety of distinct purposes. Potential scenarios for use of so called User Issued Assets (UIA) is quite diverse.
For creation, one has to go to section «Account» - «Issued assets» - «Create an asset».



- Main settings (Symbol, maximum quantity, precision, SmartCoin option, sum of confirmation from user balance);
- Description (general description, concise and limited to 32 symbols, desired market currency pair);
- Allowance (strict obligation of being in the white list of owner, possibility to selfsend tokens, turn off confidential transactions);
- Flags (connection of market commission with indication % and maximum sum)

7. Voting

7.1. Proxy

With Proxy turned on, user cannot vote for Witnesses, Committee members, Working Proposals. Only account that is registered as Proxy can participate in a voting which means the weight of his vote will be taken into account. Add list of users for voting and field for search by the name of an account. If account is proxy registrated then voting buttons will be inaccessible.

7.2. Witnesses

Voting for list of users who will serve as Witnesses - To be clear, users who become a part of the blockchain ecosystem by being able to produce blocks and verify transactions.

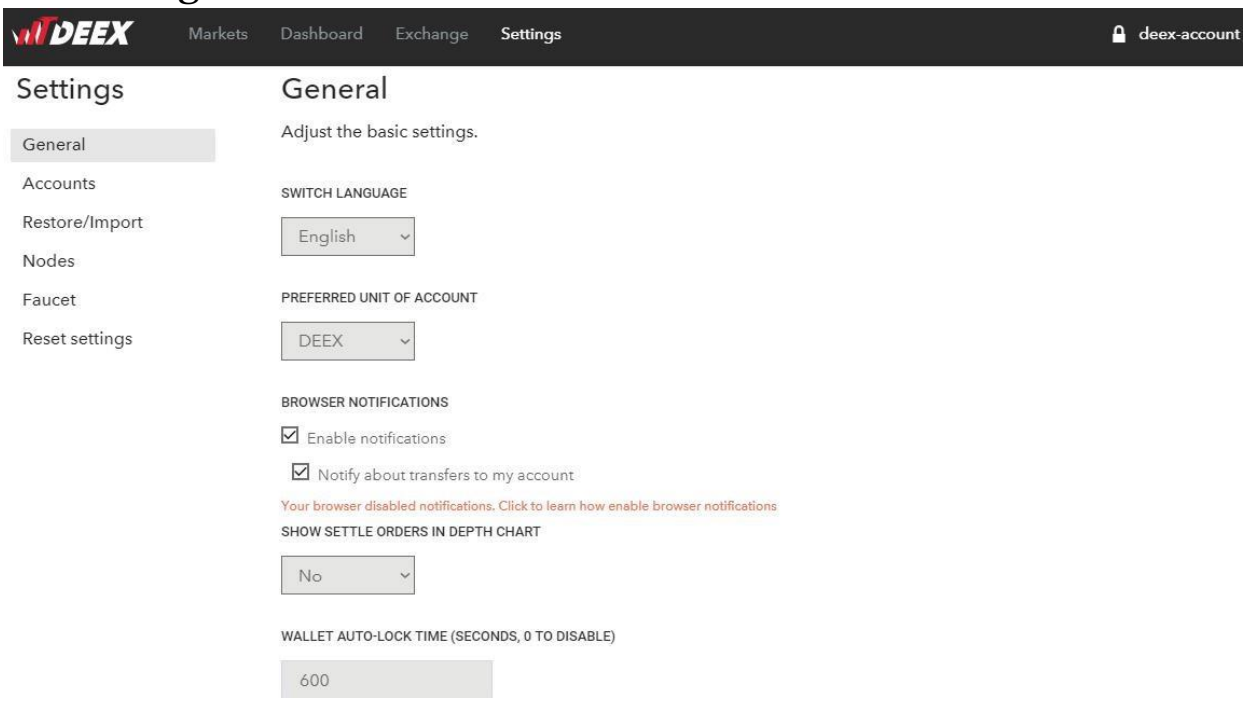
7.3. Committee members

Voting for list of users who will be responsible for taking decisions on any ecosystem developments.

7.4. Proposals

Proposals of offering valuable for system services for payment from Bitshares. Every candidate has to score decent amount of votes for their proposal confirmation. Add possibility to create your own worker and fill out details of a proposal.

8. Settings

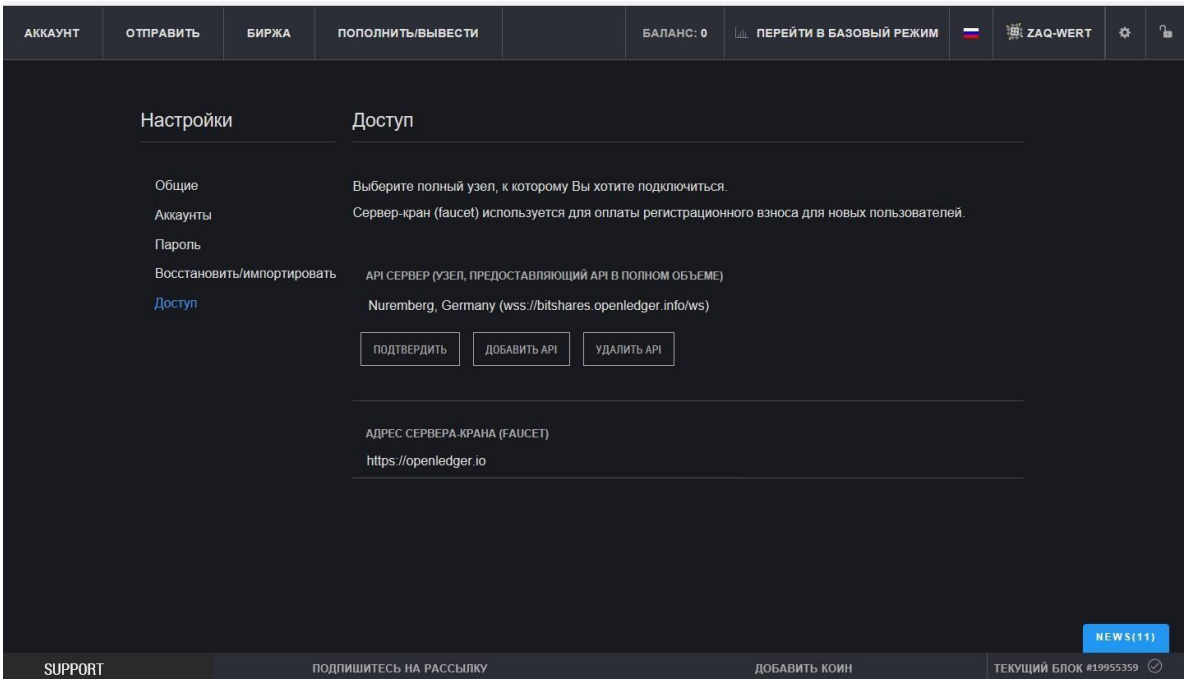


8.1. Language

Option of switching between languages in the form of flags of corresponding countries in the upper control panel.

8.2. Access configuration

Configuration of faucet and API access. On the screen of connection access settings, it is necessary to enter new connection link to faucet (faucet server is a server which pays registration fees for new coming users) or choose from list of available ones. When entering new link after pressing «Add» button, link has to be in drop-down menu of available links.



8.3. Wallet recovery

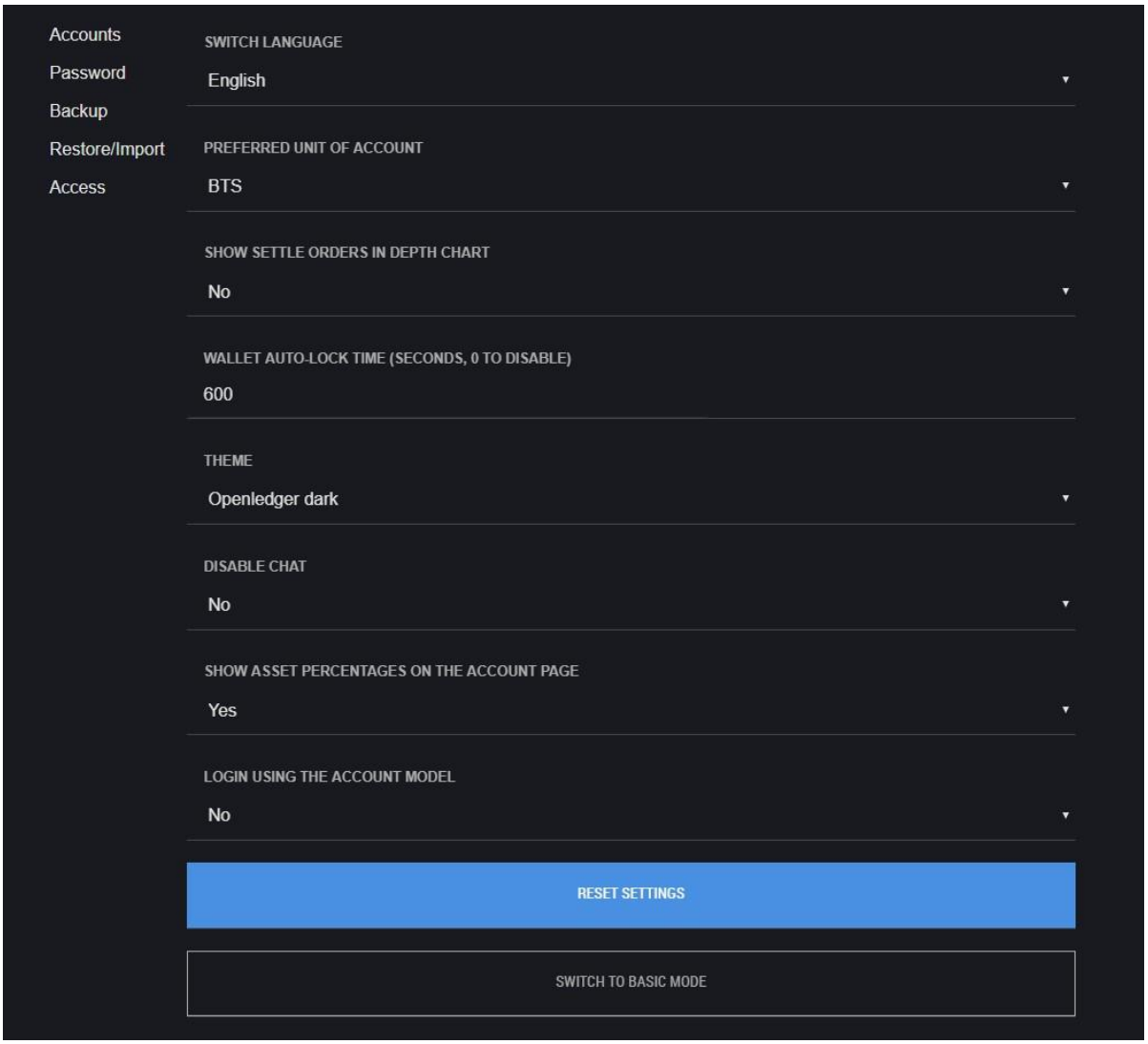
For accounts of wallet or multi-sign type, wallet recovery is carried out with help of:

- .bin file format
- Private key
- Brain key JSON file with key

8.4. Main wallet settings

As main settings following can be added and used:

- Choice of main currency
- Setup of time limit for account blockage
- Choice of type of account for authorization
- Choice of type of decentralization of the exchange (simple and advanced)
- Option to display assets in % on the screen of the exchange
- Option to display settlement transactions on Market Depth graph



9. Connection of currencies

The exchange allows to trade (BTC, ETH, LTC, BTS, DASH, STEEM, ZEC, XRP, BCH, ETC).
As was mentoned above, there exist two options of depositing funds on a balance: with fiat and with cryptocurrency.
In example №1, USD/btc is used and corresponding pair btc/dex.btc and in example №2, eth/dex.eth is utilized.

Account deposit is carried out by following scheme.

1. An account's user initiates process of receiving cryptocurrency, a form where desired amount of chosen currency and corresponding bank's account of exchange have to be stated is sent to him. An exchange's operator manually checks amount received as it can vary from stated amount in deposit order. An operator inputs to the blockchain actually received sum. On the exchange exists already issued token – dex.usd in decent for future deposits amounts. That's

why on one real dollar received through bank account, an operator gives out virtual dex.usd. On top of that deposit commission stated by account's owner is substracted. A deposit operation is done manually. This option is not heavily demanded that's why an operator wont be loaded with work.

2. Because we deal with the Bitshares blockchain, there are no other currency except its own currency and existing tokens. Thus, it is necessary to have par btc/dex.btc and they have to be in decent amounts. Later once real btc have been received on user's account, issued dex.btc are sent, however in this case the deposit process is automated and certainly with intervention of an operator when needed.

For each chosen currency gateway has to be written for connection to the exchange. A gateway works through embedded private keys and immediately deposits with dex.btc accounts once dex token is received which is used for trading on the exchange and has to be in advance registered as being tied to DEX.
With the help of a gateway currency will be transferred to internal token address of a currency (unique for each user) in 1 to 1 ratio (there is also possibility to take fees). Then with the help of functional as in bitshares through the exchange a user can exchange dex tokens on every other available dex.currencies which will be received on an internal address of chosen dex.currency (unique for every user).
If user desires to transfer chosen currency from DEX account on a personal wallet, he has to enter all the specific details for each currency. With the help of a gateway from an internal address sum equivalent to chosen currency will be transferred. For each user and currency unique address will be created. This operation may also include a fee for user. For each gateway, logic of deposit and withdrawal may vary depending on specifics of a currency. For example, for BTS MEMO box is used instead of Amount. For maintenance of work of each gateway, there will be separate dedicated node.

10. Centralization\Decentralization and security of the exchange

Mechanism of the exchange implies only centralization of gateways which is linking element between different blockchains. This linking element cannot be decentralized and be under owner's security.

Arrangement of a model of the exchange has to be in following manner:
- Server on which engine of the exchange is stored, - Gateways
with hot wallets for deposit and withdrawal of funds.

Only one risk of funds theft follows from this – a theft from hot wallet that holds all private keys. They (keys) cannot be hidden in some other place as there wouldn't be enough automation, thus these wallets have to be strictly online. Potential danger can come from «offended» admin/developer. If we talk about hacker attack, he needs to hack a server, find dat file of the exchange, figure out which key belongs to which wallet

and transfer funds from wallet. This type of danger exists on every exchange with no exceptions. The limit of a hot wallet has to be minimized in order to excluded any leakages which leads to frequent maintenance. Moreover, hot wallets are paired with a cold storage (cold wallet) which is the main storage of the funds and this wallet shouldn't have online access. The connection has to be one-sided – once limit is exceeded on a hot wallet, all the excesses are automatically redirected to the cold storage. A deposit of hot wallet happens in manual mode. This type of pair is reasonable to create only for those hot wallets which store large amount of cryptocurrency. A Mechanism of transfer from hot to cold wallets has to be completed in gateway of a currency, CAP (limit). The necessity of the transfer mechanism is negotiated with each client separately on each currency.
Requirements for cold storages are stipulated separately with each client. There is possibility of storing directly on blockchain or by saving private keys. How they will be stored and on which carrier is determined independently. Perhaps it will be stored on external drive, USB flash, laptop or paper.

As all the trades happen directly through blockchain and as each token is a real substance, deception and hacker «injections» in any trades are practically ruled out. Significant protection is gained by decentralization.

11. Observer

A blockchain observer with main data on blocks, markets, accounts. Tabs enable to create following blocks:

- Chain of blocks
- Assets
- Accounts
- Witnesses
- Members of the committee
- Markets
- Price list of transaction fees

11.1. Chain of blocks

The main statistics of the blockchain is displayed on top of the screen. There are indicated a number of the last block, generation time of the last block, quantity of active witnesses, quantity of active members of the committee, transactions per second, transactions per block, mean time of confirmations, quantity of recently missed blocks, current volume of the main currency BTS, the graph of block generation, transaction per block graph, quantity of stealth transactions.

It is necessary to add below block «Recent activity» where a list with types of activity, details of activity and time of activity. The newest ones are the first to be displayed.

In the block «Recent blocks», it is obligatory to include Block ID, date-time generation, name of observer and quantity of transactions.

Every block is a link which leads to a screen of a block's details. In a block's details, date, time, name of observer with a link, quantity of transactions, links to preceding and subsequent block also details of trades included in that block are all should be stated.

11.2. Assets

The main lists of assets existing on the exchange. There exist 3 main sections in the form of tabs: SmartCoin User issued assets Assets of prediction market

In the section SmartCoin, it is necessary to display the list of assets available on the exchange, state their name with a link, name of issuer with a link to an account, current supply and link on the exchange. On the top there has to be available place for input box for name of a filter.

In the section "User issued assets", assets that issued by authorize users are displayed. In case user is not authorized, show all available assets.

In the section Prediction market assets, assets that predict one or the other event. Every asset contains name with a link to the market, description and links to the exchange.

11.3. Accounts

In this section account search is carried out by name in the input box. The search functionality works dynamically after every entered symbol. Results of the search are displayed in a table:

- Identification
- Account name
- Current residual on account
- Percent from total

Each name of account is a link to the page of an account.

11.4. Witnesses

In the section «Witnesses», following statistics is displayed:

- Current witness (who validated the last block)
- Active witnesses (quantity)
- Level of participation

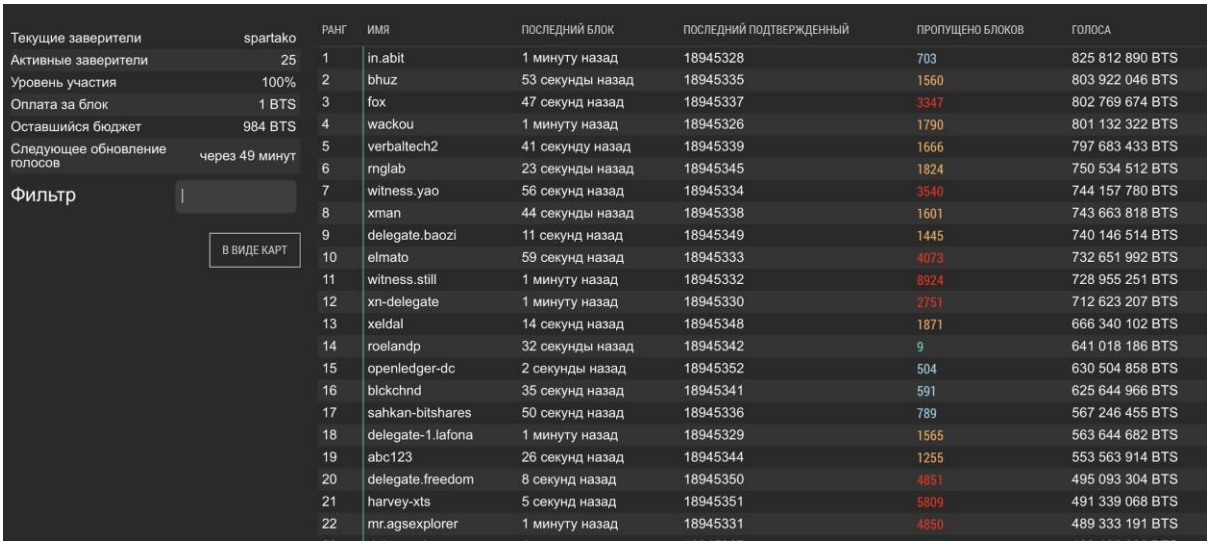
- Payment for a block (in BTS)
- Remaining budget (in BTS)
- Next update of votes (countdown)

There are also options to filter a list of witnesses by manual entry. The search functionality works dynamically after every entered symbol.

Option of switching between a table of list and a table of cards.

In the list of witnesses following columns are displayed:

- Name
- The last block (who much time passed since it was created)
- The last validated (a number of the last validated block)
- Blocks missed (quantity is to be highlighted: blue if quantity is under 1000, orange – under 2000 and red – over 2000)
- Votes (in BTS)



Текущие заверители	spartako
Активные заверители	25
Уровень участия	100%
Оплата за блок	1 BTS
Оставшийся бюджет	984 BTS
Следующее обновление голосов	через 49 минут

Фильтр

В ВИДЕ КАРТ

РАНГ	ИМЯ	ПОСЛЕДНИЙ БЛОК	ПОСЛЕДНИЙ ПОДТВЕРЖДЕННЫЙ	ПРОПУЩЕНО БЛОКОВ	ГОЛОСА
1	in.abit	1 минуту назад	18945328	703	825 812 890 BTS
2	bhuz	53 секунды назад	18945335	1560	803 922 046 BTS
3	fox	47 секунд назад	18945337	3347	802 769 674 BTS
4	wackou	1 минуту назад	18945326	1790	801 132 322 BTS
5	verbaltech2	41 секунду назад	18945339	1666	797 683 433 BTS
6	rnglab	23 секунды назад	18945345	1824	750 534 512 BTS
7	witness.yao	56 секунд назад	18945334	3540	744 157 780 BTS
8	xman	44 секунды назад	18945338	1601	743 663 818 BTS
9	delegate.baozi	11 секунд назад	18945349	1445	740 146 514 BTS
10	elmato	59 секунд назад	18945333	4073	732 651 992 BTS
11	witness.still	1 минуту назад	18945332	8924	728 955 251 BTS
12	xn-delegate	1 минуту назад	18945330	2751	712 623 207 BTS
13	xeldal	14 секунд назад	18945348	1871	666 340 102 BTS
14	roelandp	32 секунды назад	18945342	9	641 018 186 BTS
15	openledger-dc	2 секунды назад	18945352	504	630 504 858 BTS
16	blckchnd	35 секунд назад	18945341	591	625 644 966 BTS
17	sahkan-bitshares	50 секунд назад	18945336	789	567 246 455 BTS
18	delegate-1.lafona	1 минуту назад	18945329	1565	563 644 682 BTS
19	abc123	26 секунд назад	18945344	1255	553 563 914 BTS
20	delegate.freedom	8 секунд назад	18945350	4851	495 093 304 BTS
21	harvey-xts	5 секунд назад	18945351	5809	491 339 068 BTS
22	mr.agsexplorer	1 минуту назад	18945331	4850	489 333 191 BTS

11.5. Members of the committee

In the block «Committee members», current number of committee members is depicted as well as a list which includes rang, name, votes (in BTS) and link on corresponding web-site.

There is also a possibility to filter a list of committee members by names in the corresponding box for entry. The search functionality works dynamically after every entered symbol.

Option of switching between a table of list and a table of cards.

11.6. Markets

In the section «Markets» a table with all available markets is displayed. It is separated on tabs «My markets» and «Find markets». On each tab following columns are available:

- Market
- Appoint reserve
- Volume
- Price
- Change (price changes are in % for the last 24 hours displayed in following colors:
  red for decrease, green for increase)

On the tab «Find Markets» two filters are used: «Base currency» and «Name of an asset». Market search for currency pair is conducted by these two filters.

On the tab «My Markets» there is possibility to see favorites and also adjust filtration by main markets and their name.

11.7. Price list of transaction fees

Presented as a grouped list of fees

12. The token of the exchange

This token is created as a substance (UIA) on the Bitshares (needed amount is not hard to issue).
It is needed to agree upon the name and initial settings. Dividend accruals are manually distributed according to agreement with token holders. Rules of payment and commission percentage from each trade is determined separately.

13. Optimal requirements for the system

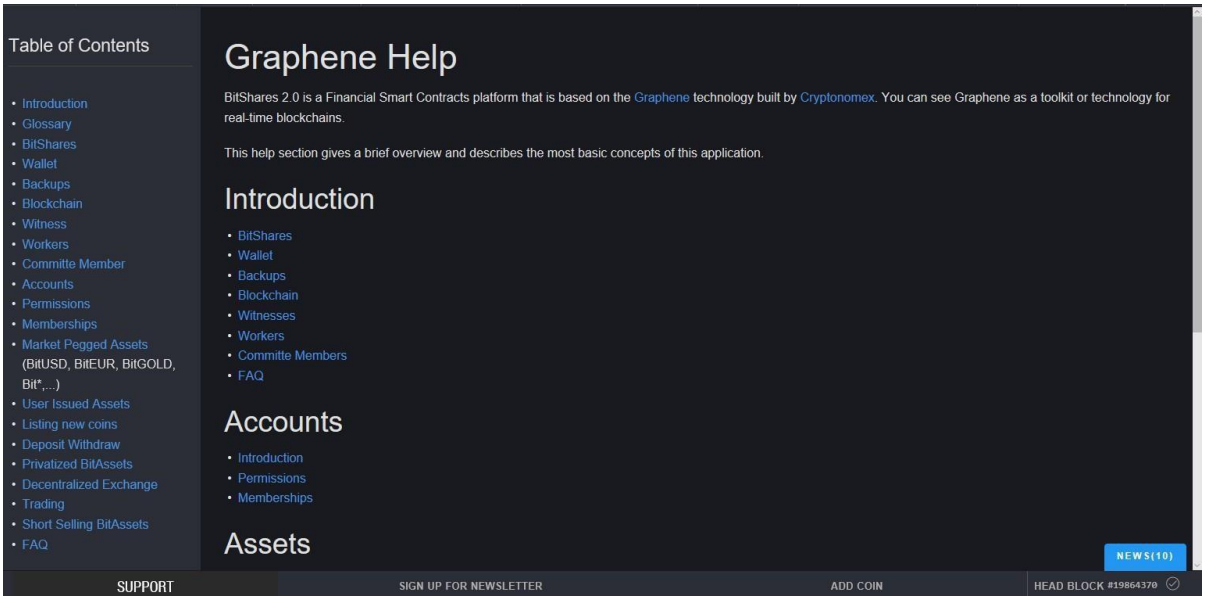
Hardware: two servers minimum. Intel® Xeon® E5-1650 v3 Hexa-Core 128 GB DDR4
ECC RAM 2 x 2 TB SATA 6 Gb/s Enterprise HDD; 7200 rpm (Software-RAID 1)
Bandwidth - 1 Gbit/s
OS: Linux Ubuntu 16 / Debian 8 DBMS:
for gateways Postgres 9.4.5

14. Glossary

- Dex – the name of the exchange
- BitShares 2.0 - a financial smart-contract platform built on blockchain technology Graphene created by Cryptonomex.
- UI – User interface.
- UIA – User Issue Assets, tokens created on the Bitshares platform.
- Bts – cryptocurrency of the Bitshares platform.
- BTC, ETH, LTC, BTS, DASH, STEEM, ZEC, XRP, BCH, ETC – cryptocurrencies.
- Workers - Workers who complete proposed work and in exchange for their service get paid from the BitShares blockchain.
- Witness (delegate) - an analog of a miner who works for the BitShares blockchain by creating new blocks. aEvery delegate is chosen by token holders; he creates and verifies blocks with current transactions. Each complete transaction in the network, eventually, has to be verified by every delegate.
- Committee Members – delegates chosen by token holders who determine certain blockchain processes and how they should be carried out.
- Proposals – propositions to advance the Bitshares.
- DEX - decentralized exchange.
- Faucet – server used for registration payment for newcomers.
- API server – node providing full functions of API.
- Accounts Regular/Multi-sign – types of accounts/wallets:
- Regular - fully administered by one user
- Multi-sign – multi-user (administered by many users)
- JSON - JavaScript Object Notation, textual format of data exchange, built on JavaScript. As many other textual formats, people can easily comprehend JSON.
- Gateway – gate-link of cryptocurrencies between blockchains. CAP – upper limit, used in the context of hot wallet.

15. Help section

In order for this section to work, a page with general explanations, instructions and links adjustments to needed points of main operations. Also pop-up hints for each market with their general description are added.



Section is presented as a small tree with section branches with 4 base blocks of brief reference information. The 4 blocks contains all the key definitions and terminology of the Bitshares blockchain.

Introduction

- ☐ BitShares
- ☐ Wallet
- ☐ Backups
- ☐ Blockchain
- ☐ Witnesses
- ☐ Workers
- ☐ Committe Members
- FAQ

Accounts

- ☐ Introduction
- ☐ Permissions
- ☐ Memberships

Assets

- ☐ Market Pegged Assets (BitUSD, BitEUR, BitGOLD, Bit*,...)
- ☐ User Issued Assets
- ☐ Privatized BitAssets

Decentralized Exchange

- ☐ Introduction
- ☐ Trading
- ☐ Short Selling BitAssets

16. Additional changes of system functionality

In the process of system development, it is possible to add further functionalities which can facilitate work of a user and advance perception of the exchange in general.

Creation of flexible and user-friendly interface. This objective is carried out through increase of color schemes for depiction of interface elements.

Addition of rotating element of «hourglass», when there is delay in the processing of data while working with the system. ПWhen connection is weak or when there are other problems with depiction of data, this functionality will be able to show a user that the system is in the processing mode and certain actin will be carried out after certain period of time will pass. This will secure a user from spontaneously clicking on the elements of the interface.

Addition of possibility to change width and height of windows (analogous to adjustment of height and width of windows in an operational system). This will also bring more flexibility to the interface for individual user.

Addition of documentation materials with description of functionality of the exchange for easier and faster introduction with all the options and possibilities available. It is possible to turn on demonstrable visual elements, textual blocks and pop-up windows.