MEMBRANA

TRUST MANAGEMENT OF DIGITAL ASSETS

WHITEPAPER

ABSTRACT

Membrana is a blockchain platform for concluding mutually beneficial and secure contracts, between investors and traders for trust management of cryptocurrency assets.

Links: alpha.membrana.io, demo.membrana.io, membrana.io

Related documents: Membrana Business Overview

Cryptocurrency Market

Thanks to blockchain technology, a large number and new types of assets — cryptocurrency — have appeared on the market: Bitcoin, Litecoin, Ether, Ethereum token, etc. These assets are decentralized digital currencies, each of which allows their owners to carry out transactions between wallets.

There are cryptocurrency exchanges based on market economy principles for the exchange of various cryptocurrencies. Many exchanges, such as Bittrex, Kraken, Bitfinex, Hitbtc, offer their users the ability to trade a large number of cryptocurrency pairs, which enables traders to use different trading strategies and generate profit from rate changes. More and more traders have done it successfully, showing a stable and high yield that reaches hundreds or even thousands of percent per year. For example, the Alternative Money Fund in 2017 has achieved a gain of more than 3,000%, and the Blue Magic Capital Fund with more than 10,000%.

Modern market of cryptocurrencies is highly volatile. On one hand, it enables successful traders to display extremely high yield. On the other hand, it brings great risks to all market participants, but first of all to beginners. Unlike traditional exchanges such as Forex, in cryptocurrency trading one can easily lose a significant portion of their assets in one day, even without a leverage.

Trust Asset Management

Trust management of assets is a sphere that has always been in demand. Investors are ready to entrust their assets to successful traders in order to generate income. Cryptocurrency market is no exception and is of increasing interest to investors and traders. By transferring their assets to experienced traders, investors retain the possibility of obtaining super-high income in the cryptocurrency market and, at the same time, minimize the risks of significant loss common to inexperienced players.

However, at the moment, there is no convenient and safe tool on the market for the conclusion of contracts between investors and traders for the trust management of cryptocurrencies. Nevertheless, such contracts are active in words, forums, and chats. This leads to a lot of fraudulent acts, for example, when traders disappear with investors' fund.

Membrana Platform

Membrana.io platform is intended to bring investors and traders together for concluding mutually beneficial and blockchain-protected contracts. Membrana.io provides investors and traders with a transparent, decentralized and secure system, which controls the process of concluding and executing a contract up to the point of revenue gained by both parties.

CONCEPT

Users of Membrana

Traders

Trader is a participant in the market of cryptocurrencies trading on the exchange, and potentially willing to receive digital assets in trust management for remuneration, paid in the event of profitable transactions and increase of an investor's assets. A trader is interested in being a notable investor and possessing all tools for trading on different cryptocurrency exchanges — both at their own expense and with the funds transferred to them in management.

Investors

Investor is a participant in cryptocurrency market with digital assets, and potentially willing to transfer these assets in trust management to a successful trader for profit purpose. An investor is interested in fund safety and obtaining complete and reliable information on traders.

Current Task

The main objective of Membrana.io platform is to directly connect an investor and a trader to conclude a mutually beneficial, secure, and reliable contract.

To avoid risks for an investor and a trader, and to make cooperation under trust management more profitable and safe, here at Membrana.io we have developed a unique algorithm to solve the following problems:

- The need for involvement of an intermediate party, guaranteeing the safety of funds and the fulfilment of contract terms
- Loss of control over invested fund (transfer of fund to a third party)
- Lack of trust between both parties
- Lack of opportunity to check the exact yield of a trader in the past
- Risk of violation of contractual terms
- Lack of a convenient tool for trading on different exchanges at the same time

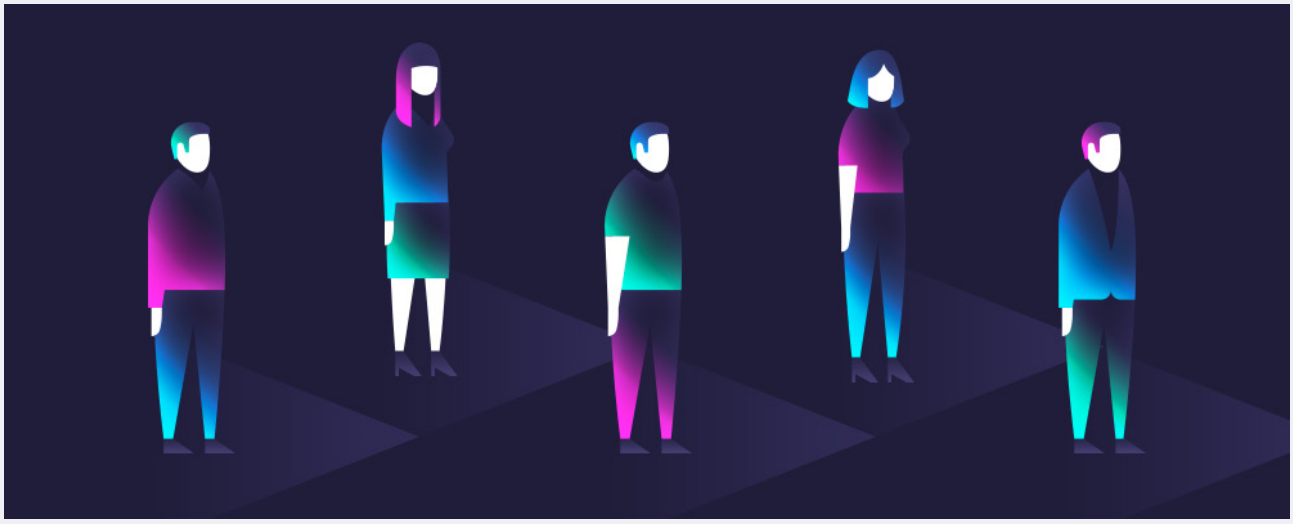
Opportunities for Traders

Membrana.io platform offers traders the following opportunities:

- Trading on different cryptocurrency exchanges through a single interface
- Trading from both of their exchange accounts, and accounts transferred to traders in trust management by investors

- Offering their services on trust management to potential investors. Setting parameters for future contracts, such as contract duration, target profit, and remuneration amount
- Conclusion of contracts for trust management of cryptocurrency assets with investors
- Fixing the terms of concluded contracts with Ethereum Smart Contract technology to guarantee the completion of these conditions

Opportunities for Investors



Membrana platform offers investors the following opportunities:

- Choosing suitable traders based on complete and definitive information of traders who offer their services on trust management
- Getting reliable data on past profitability of traders' commercial activities confirmed by a hash sum of transactions saved in blockchain
- Concluding a contract with a trader for the trust management of cryptocurrency assets located on various cryptocurrency exchanges in an investor's account
- Transferring own funds to the trust management by traders without transferring these funds directly to them. Membrana.io platform allows an investor to give traders an opportunity to manage funds, but not possessing the funds. Traders get the opportunity to trade with the investors' exchange accounts but they do not own these funds. Also, investors do not transfer their funds to Membrana platform
- Setting restrictions on trading with an exchange account transferred to trust management, such as a set of allowed trading currencies, and maximum trading loss (stop loss)
- Obtaining information on the progress of the execution of concluded contracts

Membrana Technology

Safe Transfer of Funds in Trust Management

For the purpose of transfer of an investor's exchange account to a trader in trust management, an API key provided by the exchange is used. The API key is not transferred to the trader, but stored on Membrana.io platform. The trader trades on exchange via the Membrana.io single trading terminal. As a result, the trader does have access to the investor's assets. All investor's funds remain on its exchange account, and are not transferred to the trader. Membrana.io also maintains the restrictions set at the contracting stage: currency basket permitted for trade, stop loss, time period for trading by the API key, etc.

Contract Between Investors and Traders

To conclude the transaction between investors and traders, Ethereum Smart Contract is used. Traders' consideration is reserved in Smart Contract in advance, and is automatically paid upon reaching the target profit set in percent of the amount transferred in trust management, or upon expiration of Smart Contract term.

Confirmation of Past Trader's Profitability Using Blockchain

All contracts concluded by traders via Membrana.io platform will be saved in the database. This information is further used to calculate traders' success indicators, such as ROI. These indicators of all traders will be provided to investors to enable investors to select suitable traders.

Membrana.io platform uses blockchain to validate traders' details. To do this, the hash sum of traders' transactions for the day is saved in Ethereum Smart Contract. The block, where the hash sum is saved, is dated and cannot be counterfeited. Therefore, the validity of all data on traders' transactions of exchange is confirmed by their hash sum in the blockchain — in the block dated with the respective date of transaction. It is not possible to save only profitable transactions in the database and their hash sum externally as far as at the moment of saving, because it is not known which transactions are profitable.

Income of Membrana

0.5% of the amount is transferred into trust management. For more detail information look Membrana Business Overview.

Advantages of Membrana

For Traders:

- Possibility to attract investments in trust management
- Single trading terminal inside the platform supporting various exchanges
- Support of all major cryptocurrency exchanges in one terminal
- Rating system based on auction bidding results
- Conditions of transaction are set in Smart Contract and are unchangeable
- Trader's commission fee is set for transaction at the moment of contracting
- Possibility to configure trading strategies (to be developed)

For Investors:

- Safety and transparency of all transactions
- Funds are always in investors' accounts
- Possibility to select the most successful trader for investment
- Guaranteed result accuracy of traders
- All conditions of transaction are set in Smart Contract and are unchangeable
- Currency selection to calculate profit: BTC, ETH, and USD
- Convenient interface to work with several contracts with traders

For Cryptocurrency Trading Ecosystem:

- Additional possibilities for investments
- Inflow of assets on the market from new investors
- Increased number and volume of transactions on cryptocurrency exchanges
- Relaxation in requirements for entering cryptocurrency trading, it is sufficient to just select traders and transfer assets to them.
- Increase in traders' income, and their quantity
- Improvement of trust management reputation on cryptocurrency market

TECHNOLOGIES

Ethereum Smart Contract

To conclude a transaction for trust management between investors and traders, Ethereum Smart Contract is used. A Smart Contract contains all the agreement details. An investor reserves a trader's consideration in advance on the Smart Contract account in the amount to be paid, upon reaching the target profit. The consideration is automatically paid to the trader upon the expiration of contract term, and the receipt of income by the trader. The contract may be terminated ahead of time, if the target profit is received by the trader, as well as if the investor commits a prohibited action. For example, if the investor withdraws money from the exchange account, or carries out a transaction on this account on their own. To get information on the current state of exchange account, Smart Contract uses Oracles described below.

Exchange API

Most cryptocurrency exchanges provide an API (Application Programming Interface) for automatic transaction. The API is accessed by a certain exchange account using the API key, which can be obtained by the account owner on the exchange website.

Membrana.io platform provides traders with the single trading terminal to carry out a transaction on any supported exchange. Traders carry out the transaction on Membrana.io platform. Membrana.io translates each transaction via the exchange API

using API keys owned by the trader, or transferred to traders in trust management. API keys are stored in the protected database on Membrana.io platform.

Fund Security for Investors

The technology implemented on Membrana.io platform provides fund security for investors — funds are transferred to traders in trust management. The funds will not be transferred directly to traders under any circumstances. Traders do not have access to investors' API keys as well. API keys are stored on Membrana.io platform. Traders carry out transactions via the single trading terminal on Membrana.io platform. Each trust management contract has particular currency restrictions which are available for trading. Thus, it is not possible for traders to make use of investors' funds for a dummy currency.

Protection of Investor's API Keys

Security of original API keys is ensured as the backend system. Backend system manages the functionality of personal account and trading terminal, and does not have access to the server directly interacting with the exchange. The trading system has an isolated environment. The access to transactions via this system is possible only in case of signature authorization session, using the ECDSA algorithm.

Oracles

Oracle is a software component providing data to Ethereum from the external world. These data can be further used by Smart Contracts.

On Membrana.io platform, oracles are used by the backend system to obtain and record information in blockchain, data on currency balance on the exchange account, transactions of certain exchange account, cryptocurrency exchange rates, and transactions of certain traders.

MetaMask

User authorization on Membrana.io platform is executed using MetaMask. MetaMask is a plug-in for web browser (currently supported by Chrome and Firefox), enabling users to carry out blockchain transactions in Ethereum via JavaScript web3 object without a private key. Membrana.io platform uses web3 to work with Smart Contract.

ALGORITHM OF MEMBRANA SYSTEM OPERATION

Authorization

A user installs the MetaMask plug-in to the Internet browser and logs into Ethereum using Metamask.

Addition the API Key

A user logs into the cryptocurrency exchange website and requests for an API key for automatic transactions. In addition, an option of adding the API key is used on Membrana.io.im website, where the key itself and its name are entered for a better understanding of key assignment. For example, "own funds' trade". It is also possible to limit the currency basket for trading with this API key. In this case, the currencies USD, BTC, and ETH should be available at all times.

After adding the API key to Membrana.io, the possibility of self-trade through this key emerges via the single trading terminal (for traders). It also becomes possible to use this API key to conclude contracts for trust management of funds on the exchange account, to which this key belongs (for investors).

Trust Management Offer from Traders

A trader who is willing to receive funds in trust management, sets the parameters of future contract with an investor:

- Target profit to close out the contract as a percentage of the amount transferred into trust management

- Minimum investment amount
- Contract term
- Stop loss: the maximum allowable loss (as a percentage of the initial amount of assets)
- Amount of trader's commission (as a percentage of the target profit)
- Currency of settlement under the contract

Trader Selection by Investors

An investor who is willing to transfer funds in trust management, looks through the list of active offers from traders in a convenient way with the exclusion of unsuitable options, and the help of various filters—such as trader's reputation, profitability, contract amount, contract duration, etc.

The investor and the trader have the opportunity to exchange messages to discuss terms of a forthcoming transaction.

Conclusion of a Contract

Having chosen a suitable offer, the investor sends an application to the trader for the conclusion of a contract. In order to do this, the investor should already have an account on the cryptocurrency exchange, and an API key added to Membrana.io platform to manage this account. The exchange account should not contain currencies other than BTC, ETH, or USD. The trader then accepts the application. The concluded contract is recorded in Ethereum Smart Contract. The maximum commission is transferred from the investor's Ethereum wallet to the Smart Contract, and is reserved there for payment to the trader in the future.

Contract Closeout

Achievement of Target Profit

The contract is automatically completed if the target profit recorded at the time of transaction conclusion is achieved. The reserved trader's consideration shall be paid in full.

Expiration of a Contract

After the contract expires, it is completed. The reserved trader's consideration shall be paid partially. The share is calculated as a ratio of the reached profit to the targeted one. If the profit is negative, then the share is zero. The part of consideration that has not been paid to the trader is returned to the investor. All currencies that are on the exchange account are sold for accounting currency.

Stop Loss

In order to protect the investor from large losses, a stop loss value as a percentage of the initial amount in the accounting currency is fixed in the Smart Contract. In case of the decrease of total amount of funds to a certain value—as a result of transactions made by the trader—the contract is then automatically completed. Thus, the consideration is not paid to the trader, and is returned to the investor's Ethereum wallet. All currencies are automatically sold for the accounting currency at the exchange price.

Prohibited Investor Action

It is prohibited for the investor to withdraw funds from the exchange account used in the applicable contract, and to bring them to the exchange account. If this happens, the smart contract finds out through Oracle and terminates automatically. In this case, the reserved commission shall be paid to the trader in full. All currencies that are on the exchange account are sold for the accounting currency. Likewise, the investor is not allowed to conduct a transaction independently from the exchange account transferred in trust management.

Settlement Between Investors and Traders

When concluding a transaction for trust management, the currency of settlement is fixed. There is an option to choose among BTC, ETH or USD. To make any settlement under the contract, for example, the calculation of profit or loss achieved, all currencies on the investor's exchange account are converted into the accounting currency at the exchange price at the time of settlement.

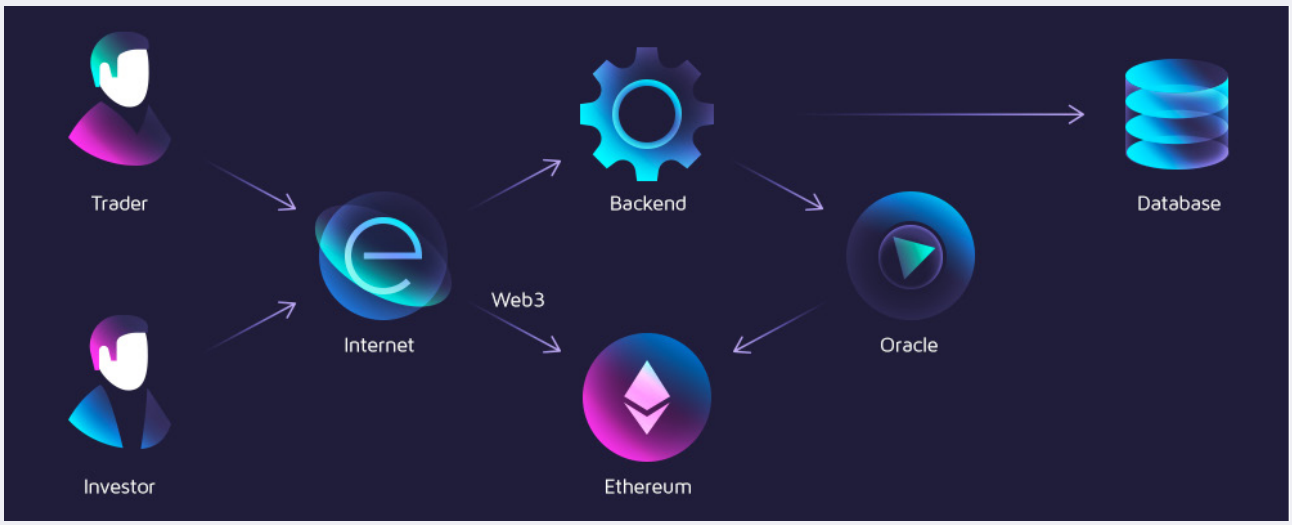
The assets transferred in trust management must be nominated in BTC, ETH, or USD. The investor is prohibited from having other currencies on the exchange account at the time of transfer in trust management.

In order to complete the contract upon the achievement of a target profit, the trader must sell all currencies on the exchange account for the accounting currency (BTC, ETH or USD).

Often, there will be a situation when the trader receives a profit exceeding the target profit, due to the fact that the probability of the last transaction and the exact hit in the value of the target profit, is very small. In this case, as well as when the target profit is achieved, the contract is closed out. In addition, the investor is invoiced to pay for the trader's services while receiving additional profit. The amount of this consideration has been already determined in the contract, as a percentage of the profit received.

It is planned in the future release for Membrana.io, to allow the investor to choose currencies that must be sold necessarily for any reason at the time of the contract closeout — which can be saved on the exchange account.

THE HIGH-LEVEL PLATFORM ARCHITECTURE (ALPHA VERSION)



Frontend

The frontend subsystem of Membrana.io platform, which interacts with users, is a dynamic web page created using React technology.

The Internet browser uses MetaMask plug-in, allowing users to make transactions from their Ethereum wallets. MetaMask also provides a web3 object to work with Ethereum automatically.

Backend

The server part of Membrana.io platform is responsible for processing user requests made through the web site. Backend is created using Node.js.

Database

In order to store all necessary information in the system, MongoDB database is used. The database interacts with the backend.

Ethereum Blockchain

Membrana.io platform uses Ethereum blockchain. The technology of smart contract is used to consolidate all terms of transaction between investors and traders for trust asset management. Also, in the process of initiating transactions by traders, data (hash sums) on these transactions are stored in blockchain to confirm the reliability of data in the future.

Ethereum interacts with the platform's frontend. All transactions are signed by a key of a specific user. This is possible, as far in order to log onto Membrana.io platform, users log in using MetaMask.

Oracles

On Membrana.io platform, oracles are used by the backend to obtain and record in blockchain with data of transactions of a certain exchange account, cryptocurrency rates, and transactions of a specific trader.

SMART CONTRACT CODE

Smart contracts of Membrana.io platform can be found in the official GitHub repository: github.com/MembranaPlatform.

An example of the code of Membrana.ioInstance.sol (alpha version) — the main smart contract, is shown below. The code implements the functionality of concluding and executing a trust management transaction between an investor and a trader.

```
pragma solidity ^0.4.15;
contract MembranaInstance {
    address public be = 0x10367bD202112F862d715D093C0B78E26BEcdc9C;
    enum state { paid, verified, halted, finished }
    state public currentState;
    uint256 public start;
    uint256 public deadline;
    uint256 public maxLoss;
    uint256 public startBallance;
    uint256 public targetBallance;
    uint256 public amount;
    string public investor;
    address public investorAddress;
    string public trader;
    address public traderAddress;

    function MembranaInstance(uint duration, uint _maxLoss, uint _
startBallance,
            uint _targetBallance, uint256 _amount,  string _investor,
            address _investorAddress, string _trader, address _traderAddress)
{
        start = now;
        deadline = start + duration * 86400;
        maxLoss = _maxLoss;
        startBallance = _startBallance;
        targetBallance = _targetBallance;
        amount = _amount;
        investor = _investor;
        investorAddress = _investorAddress;
        trader = _trader;
        traderAddress = _traderAddress;
        currentState = state.paid;
```

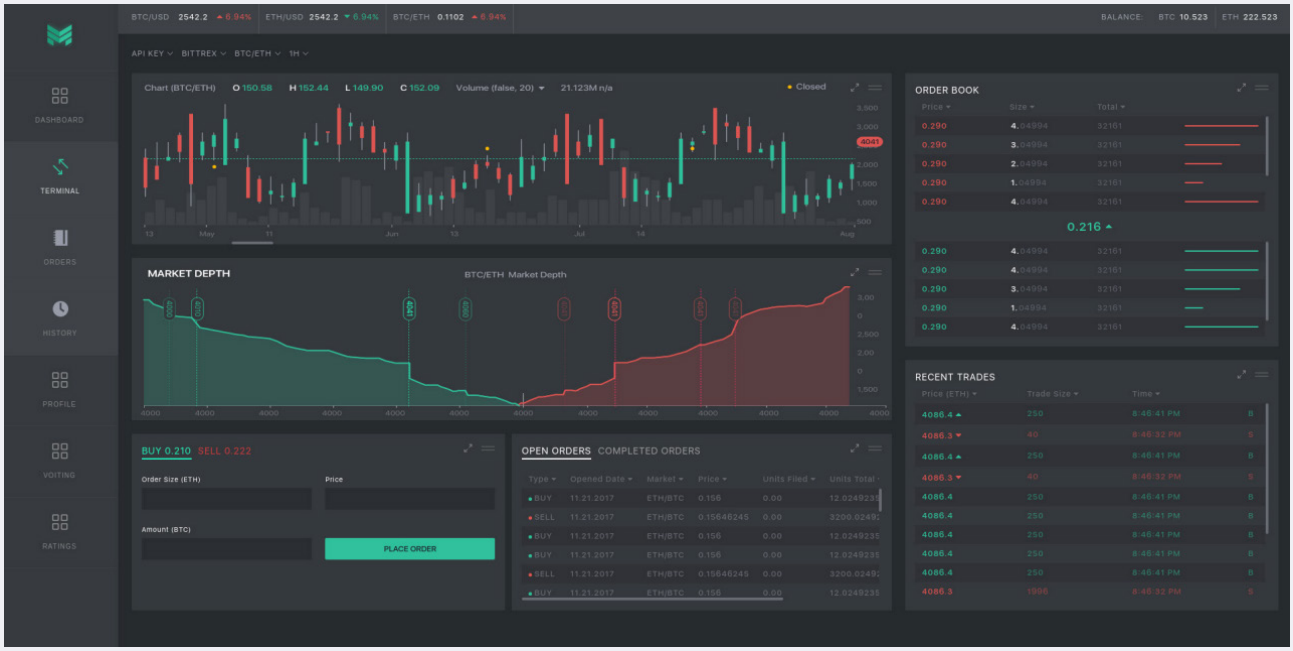
```
    }
    function myAddr() public constant returns(address) {
      return this;
    }
    modifier onlyBe() {
        require(msg.sender == be);
        _;
    }
    modifier inState(state s) {
        require(currentState == s);
        _;
    }
    function getState() public constant returns (uint)  {
        return uint(currentState);
    }
    function setVerified() external onlyBe inState(state.paid) {
        currentState = state.verified;
    }
    function setHalted() external onlyBe returns(state) {
        require(currentState == state.paid || currentState == state.verified);
        traderAddress.transfer(this.balance);
        currentState = state.halted;
        return currentState;
    }
    function setFinished(uint finishAmount) external onlyBe inState(state.
verified) {
        require(now < deadline);
        if (finishAmount<=startBallance) {
          investorAddress.transfer(this.balance);
        } else if (finishAmount>targetBallance) {
          traderAddress.transfer(this.balance);
        } else {
          traderAddress.transfer(((finishAmount-startBallance)/
(targetBallance-startBallance))*this.balance);
          investorAddress.transfer(this.balance);
        }
        currentState = state.finished;
   }
   function () public payable {
   }
}
```

MEMBRANA PLATFORM INTERFACE (ALPHA VERSION)

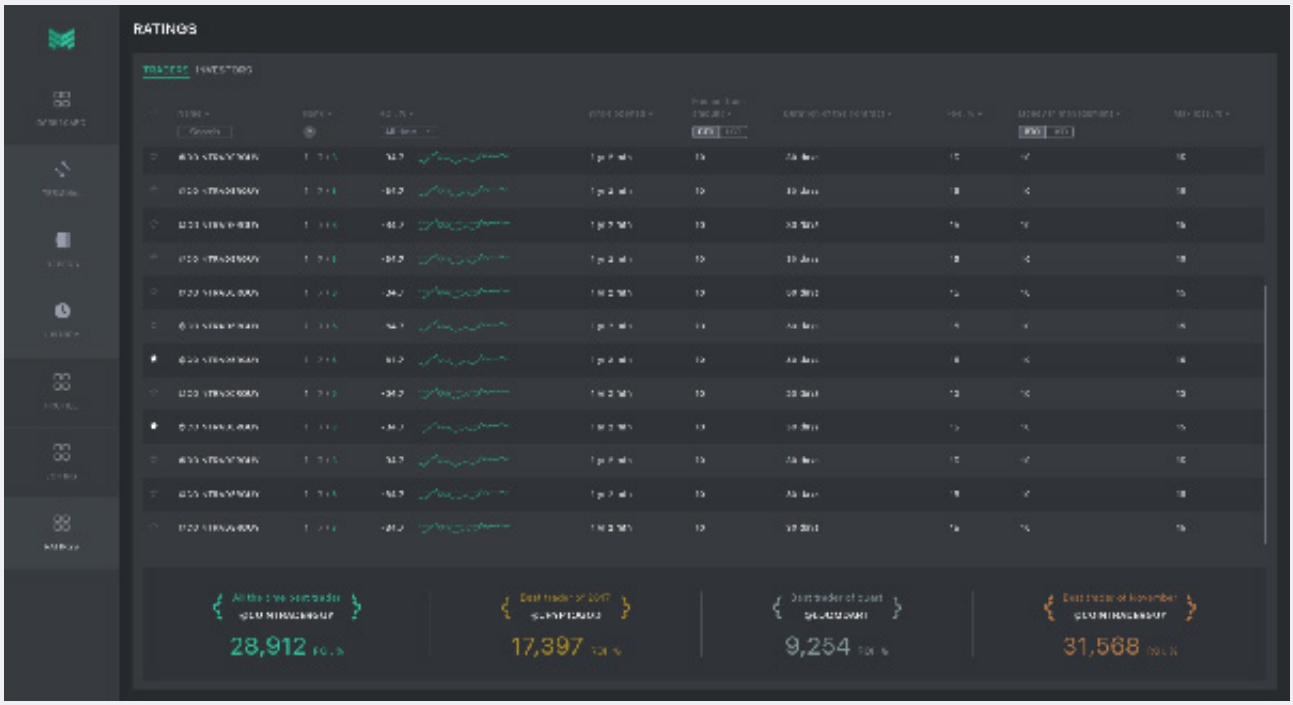
At current state Alfa version of Membrana.io platform is available for open testing: alpha.membrana.io

Below there are screenshots of its interface.

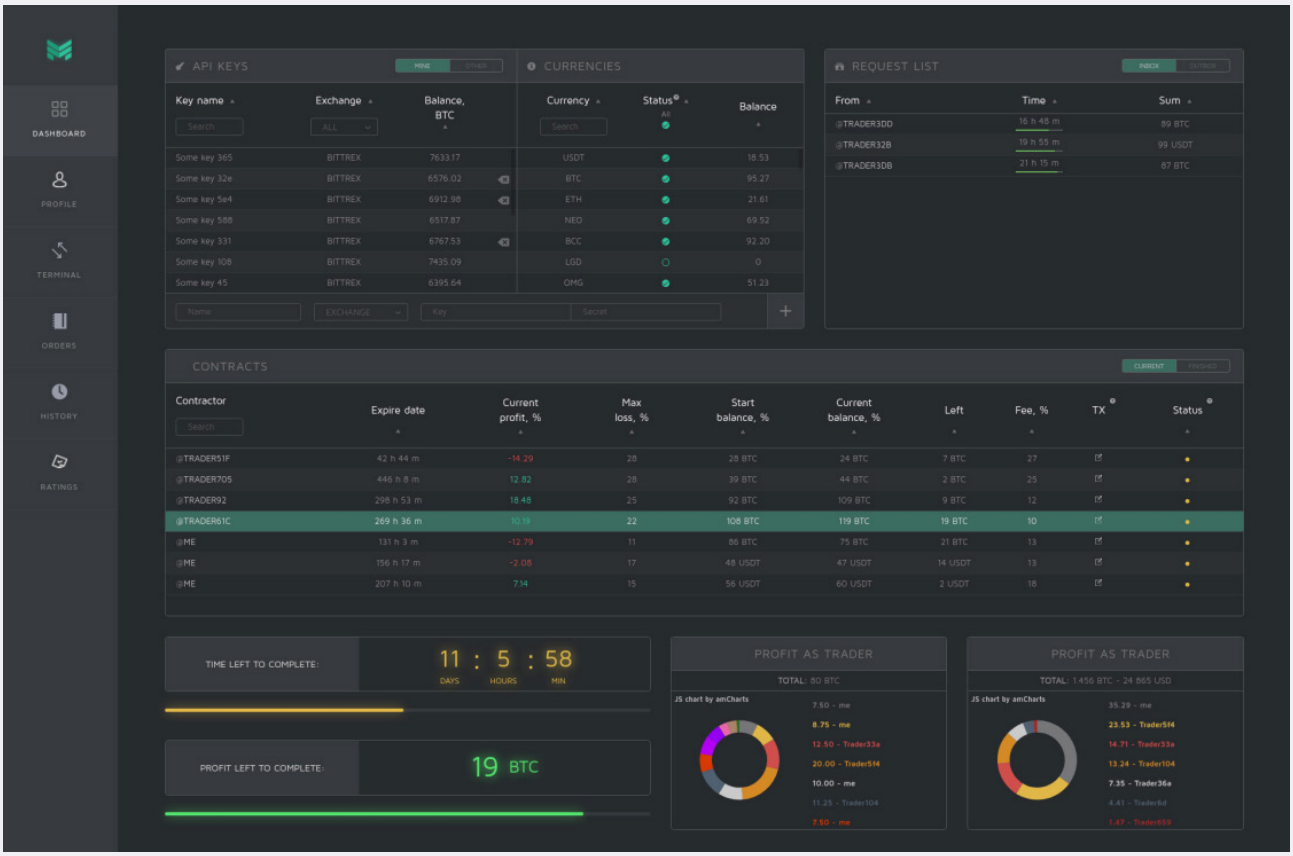
Single Trading Terminal for Traders



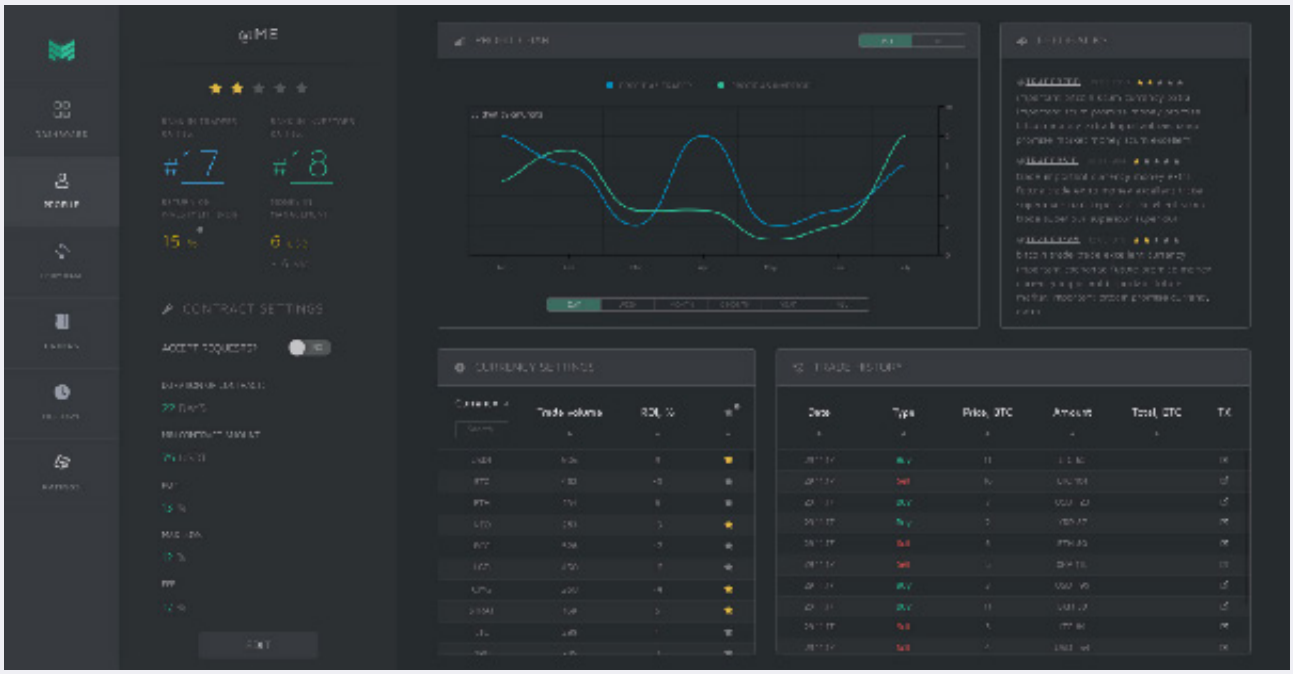
Trader's Rating



Investor’s Personal Account



Trader's Profile



PROJECT ROADMAP

Below you can read Membrana.io project roadmap

Q1 2017 Concept Development

This quarter started with the concept development of cryptocurrency asset trust management. We searched for solutions to main problems of trust management market:

- Loss of control over investment capital
- Risks associated with the participation of intermediary in transaction
- Lack of trust between investors and traders
- Lack of assurance of the validity of a trader's past trading results
- Possible falsification of trading results
- Q2 2017 Verification of Concept Viability

In the 2nd quarter, we focused on the complete verification of concept viability under different scenarios of participant's behaviour. Besides, additional audit was conducted to ensure the safety of investor's assets, with the study and analysis of all possible risks. Optimization of internal processes was performed to eliminate risks.

Q3 2017 Creation of Interfaces

Development of platform interfaces was carried out in this quarter.

Q1 2018 Alpha Version

The last quarter of 2017 has its focus on the development of platform architecture, implementation of its alpha version with the following functionality:

- Authorization using MetaMask
- Addition of API keys of Bittrex cryptocurrency exchange
- Sending, receiving requests for trust management
- Viewing contract conditions in Etherscan system
- Providing access to trading through API key
- Q4 is concluded with closed testing of alpha version.

Q2 2018 Beta Version

This quarter starts with the open testing of beta version with updated functionality:

- Updating trader's rating based on contract deliverables
- Placement of orders on cryptocurrency exchange through internal trading terminal
- Recording results of trades in blockchain
- Adjustment of Oracle's performance
- Performing a smart contract in any scenarios
- Checking the operation of all systems and algorithms

Q3 2018 RTM Release

Membrana.io platform is released with full functionality, and is ready to enter the market:

- Supporting most cryptocurrency exchanges with API keys
- Release of mobile version platform
- Correcting bugs and working out feedback received

AI Q4 2018 Release of Prediction AI

The development of artificial intelligence (AI) begins, in order to predict the expected profitability of traders.

Working to create a hybrid intelligence, which consists of self-learning AI, and a system based on human predictions. This will not only allow the prediction of traders' expected profitability, but also increase the accuracy and profitability of investment processes.

Q1 2019 Funds

Release of toolkit that allows traders and investors to unite in funds.

Release of the first DAO voting system within funds.

Customizable funds for traders and investors, for which decisions are made jointly through equity voting.

Q2 2019 ICO Funds

A system that allows users to link an investor and an ICO manager through a smart contract.

Asset management for participation in the ICO on Ethereum blockchain. Payments are made in ICO tokens under conditions recorded in a smart contract. The manager's efficiency is estimated by the difference in the value of invested ETH at the time of ICO, and the value of tokens at the time of contract conclusion.

Q4 2019 Trading Algorithms

Built-in system for the creation of user's own trading algorithms.

The ability to create their own dynamic trading algorithms that will be executed according to data taken, with the help of tracking systems.

The algorithms will be built on formulas based on the following parameters:

- Capitalization of cryptocurrency
- Exchange rate on a certain cryptocurrency exchange
- Trading volumes (per hour, per day, and per month)
- Cross-rate with another cryptocurrency
- Sale / purchase order books
- and about 100 other parameters.

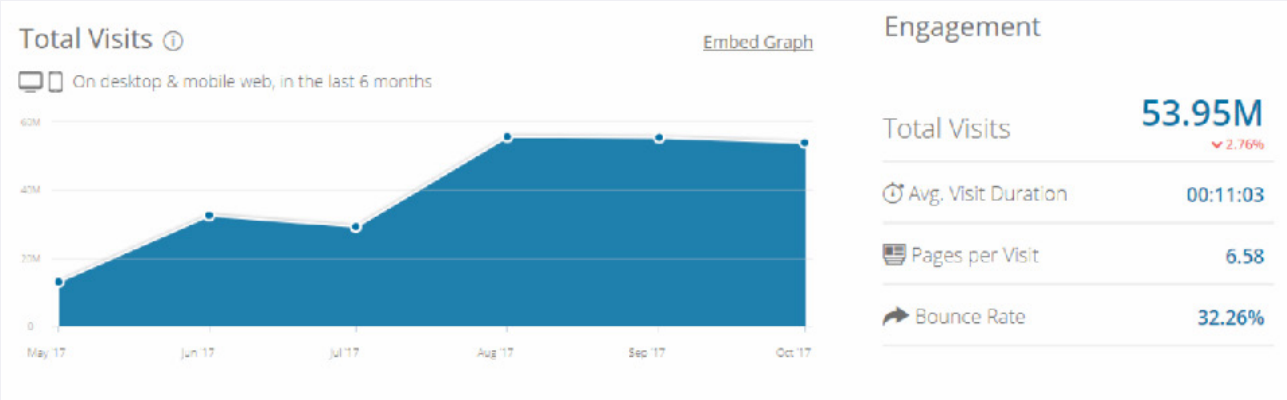
The system will allow users to create their own trading algorithms and manage their portfolios using the formulas. Each user, without the knowledge of programming, could create their own robots that will work on several exchanges at the same time.

BUSINESS MODEL

Membrana.io platform is made to provide an opportunity to traders and investors for the
conclusion of mutually beneficial and safe trust management contracts. For services rendered, platform will charge a commission fee from investors.

The platform commission is 0.5% of the contract amount. The specific pricing policy will be further developed and may include the following:

The platform commission fee is regressive as it decreases depending on the contract amount.



According to SimilarWeb service worldwide, visitor traffic is 53 million people per day.
Trade volume on Bittrex exchange is equivalent to 90 thousand Bitcoins per day.
The price of one Bitcoin is $10 000 on the day of document creation.

Let's calculate the income at Membrana.io platform, based on different daily contract volume.

For the sake of calculation simplicity, operation costs won't be included. Also, the

commission fee will be counted as 0.5% for all contracts.
The calculation is in the table below.

Share from the trading volume	0.03%	0.05	0.1%	0.25%	0.5%
Contract volume in BTC	9	45	90	225	450
Daily profit in BTC	0.045	0.225	0.45	1.125	2.25
Monthly profit in BTC	1.35	6.75	13.5	33.75	67.5
Monthly profit in USD	13,000	67,500	135,000	337,500	675,000

This example illustrates the potential of Membrana.io platform for one Bittrex exchange

Let's examine the income growth of Membrana.io platform when implemented on following
exchanges:
Bitfinex - daily trading volume 250,000 BTC
Poloniex - daily trading volume 80,000 BTC

For the calculation, we will use contract share equal to 0.05% from the exchange volume.

Exchange	Bitfinex	Polonex
Contract volume in BTC	125	40
Daily profit in BTC	0.625	0.2
Monthly profit in BTC	18.75	6
Monthly profit in USD	187,500	60,000

Consolidated monthly income is based on a contract share of 0.05% from the trading volume of 3 exchanges - Bittrex, Bitfinex, and Poloniex. It will be 315,000 USD.

Evgeniy Buev, CEO

Serial entrepreneur
Trader of cryptocurrency assets since 2015

Maxim Khukhro, CTO

Expert in machine learning and Java
AI researcher
8 years at Intel Corporation

Yuriy Gerasimov, CMO

Marketing in SxS corporation
Launched several business start-ups
Cryptoanalyst

Igor Knyazev, Backend and Solidity Developer

Developed his own trading platform
Developer of Solidity since 2016

Kirill Romanov, COO

Digital-agency founder
Serial entrepreneur
Marketing since 2009

Vyacheslav Mychkin, Frontend Developer

JS and mobile applications' developer (Android, iOS)

ADVISORS

Alexander Noxon, Technical Advisor

CTO at dao.casino
Expert in ethereum dapps
In 2015 developed own trading platform connectivity
Thomson Reuters.

Salus, Advisor

The founder of SaluS (SLS)
Crypto trader since 2013
Oldschool and trustable bitcointalk member.

Website

Platform Demo Version

Platform Alpha Version

GitHub

Telegram

Medium

info@membrana.io