FundPlaces Distributed Asset Ledger (FuDAL) Version 1.0

08 Nov 2017

FundPlaces

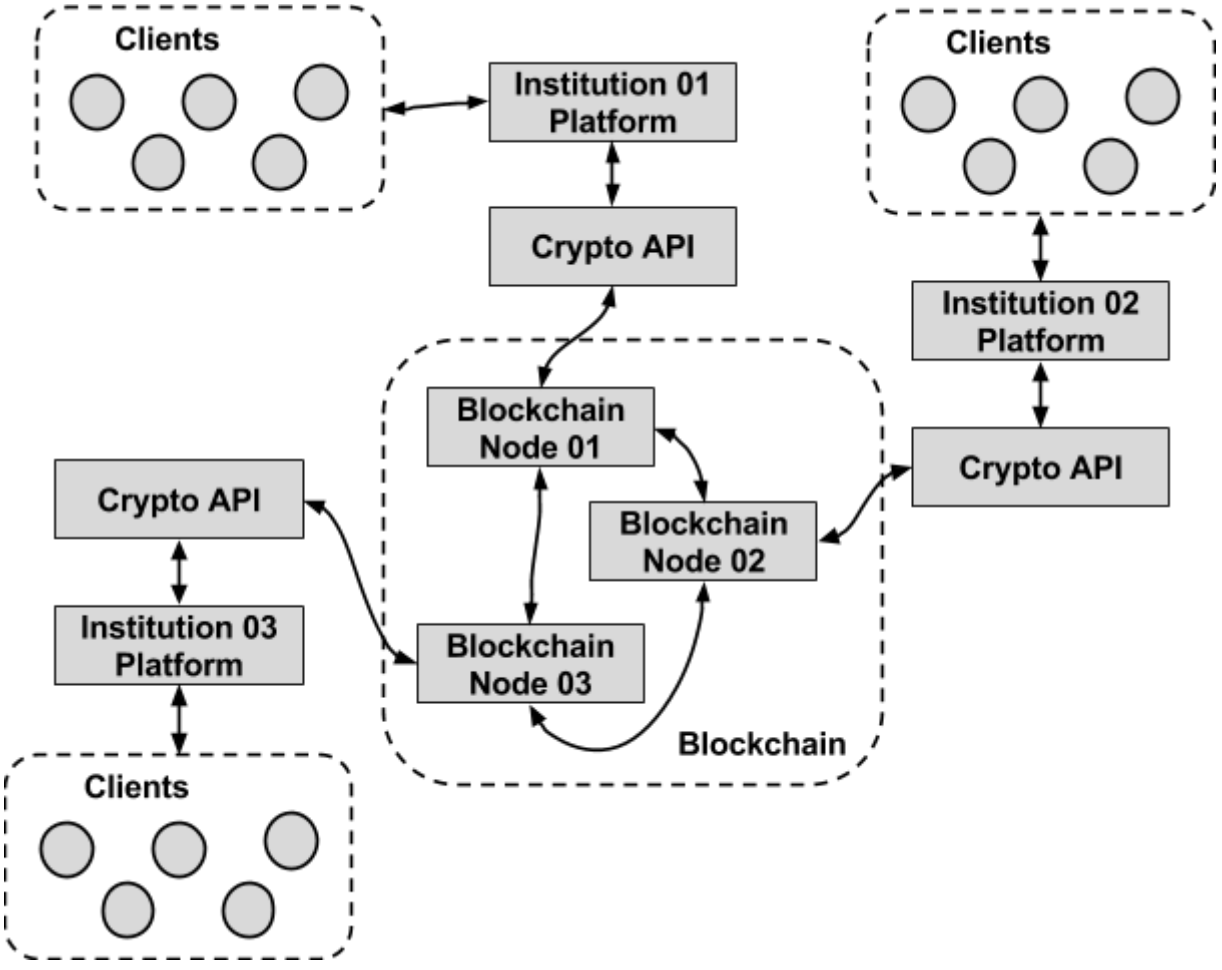
Contents

Introduction

The FundPlaces Distributed Asset Ledger (FuDAL) is a permissioned blockchain platform that allows participants to issue their own assets, distribute returns, trade atomically and redeem assets. Each asset has a voting mechanism so that owners can make decisions regarding their investment with critical information being recorded on the immutable blockchain.

The current incarnation of FuDAL is aimed at 3rd party institutions who want to allow their clients to issue, buy, sell and redeem assets within and across institutional boundaries. Clients' personal information will remain private and kept confidential by their institutions. On the blockchain, clients' accounts will only be known by their addresses.

FuDAL is being used in production as the key innovation underlying FundPlaces, a real estate investment platform that allows property developers to easily issue TILES (assets), distribute the economic benefits and redeem those TILES at the conclusion of the investment. TILES owners can also make decisions regarding their investment through the blockchain voting mechanism.



FuDAL Architecture

Overview

FuDAL is a RESTful API which wraps around the FundPlaces permissioned blockchain and has its own datastore. This datastore acts like a horizontally scalable wallet which organizes and caches blockchain data so that it can be queried efficiently. Each institution runs their **own instance** of FuDAL which includes the API, datastore and blockchain node. The API, datastore and blockchain nodes are horizontally scalable.

The API allows an institution to create single-signature and multi-signature accounts on the blockchain, encrypt and manage keys, manage balances, issue assets, distribute returns, redeem assets and perform atomic exchange transactions for trading etc. By translating blockchain operations into an easy to use RESTful API, the institution can use its existing web and mobile development teams to create blockchain applications.

Blockchain

The Multichain (https://www.multichain.com/) permissioned blockchain is the basic technology underlying the platform and the Crypto Assets API. It is a fork of bitcoin core but with added support for:

1. Permission management
2. Asset Issuance
3. Streams which are like key-value storage
4. Rich metadata with each "operation" (also known as transactions in blockchain parlance)

As the blockchain is permissioned, only entities which have been given explicit access can connect to the blockchain and engage in activities such as: sending and receiving assets, issuing assets, writing to streams and mining.

Since all participants are "trusted", a much less resource intensive mechanism can be used for the blockchain to reach consensus (Proof-of-Work is not needed). This means that the throughput of the chain can be a lot higher than that of the public blockchains.

Only critical information is stored on the blockchain. Since anyone who is allowed to connect to a blockchain can see all the information on it, no personal identifying information is stored. Other than asset ownership data, the only other things stored in streams on the blockchain are: address relationships, asset information, asset booking data and trading order data.

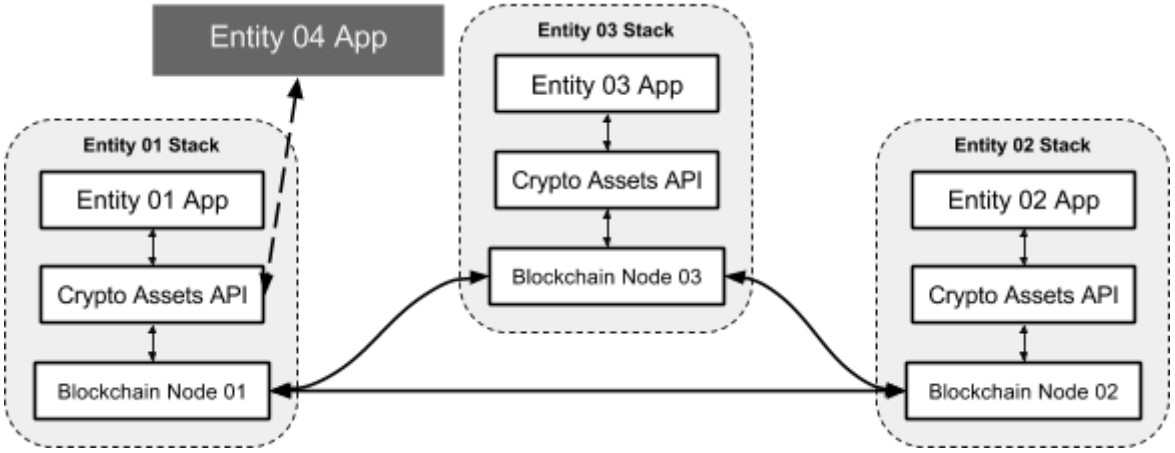
FuDAL API

The interface to the blockchain is powerful, but low-level and allows all sorts of applications to be built on top. Hence, we have created the FuDAL API. This is a micro-service which presents the programmer with a friendly RESTful API interface for managing assets, taking trades etc. Programmers only need to be familiar with RESTful APIs to do the integration, no blockchain development experience is necessary.

There are 2 ways in which a partner institution can use the FuDAL API, they can connect to it through an existing institution partner or they can run a separate FuDAL technology stack which includes their own blockchain node.

Connecting through an existing partner is the easiest way and there is no need to run any infrastructure. However, some customer information like names, email addresses and mobile numbers will need to be shared.

If a partner runs their own blockchain node and version of the FuDAL stack, they can achieve complete customer data segregation from other entities utilizing the same chain. This allows them to more easily conform to local data privacy and banking secrecy regulations, while implementing jurisdiction appropriate KYC measures for their customers.



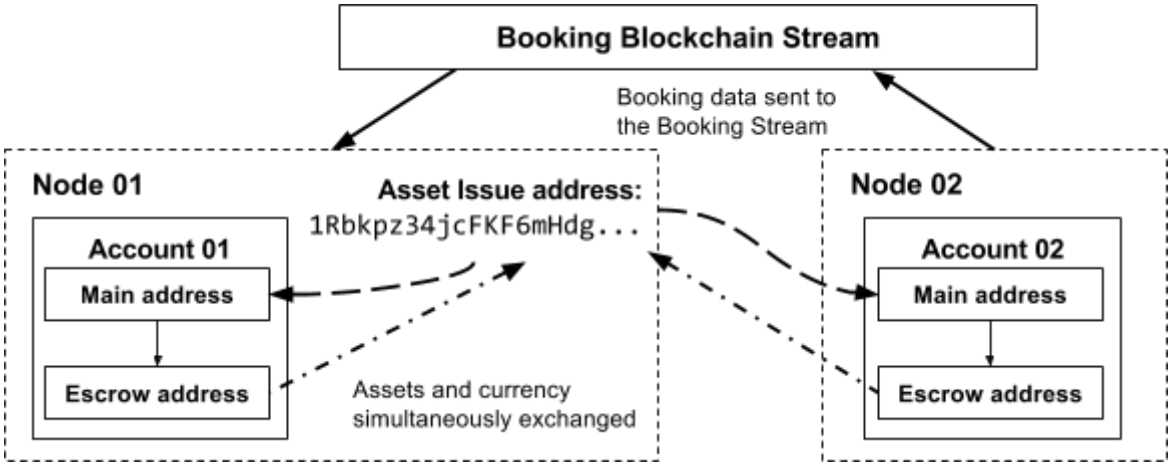
In this example, Entity 01, Entity 02 and Entity 03 run their own separate stacks, while Entity 04 connects to the blockchain through Entity 01's Crypto Assets API. Some Personally Identifying Information of Entity 04's customers will need to be shared with Entity 01.

Blockchain Operations

Issuing Assets

Each node has the ability to issue assets (in FundPlaces case, we call them TILES) and grant that ability to any addresses it generates. Every unique asset has a unique asset address that is allowed to issue it. No other address will be able to issue that asset.

To issue an Asset, a node will first "reserve" the Asset by creating a single genesis token and then "burning" it (sending it to an address whose private key is not known). Then, it will broadcast the presence of this new token over a blockchain stream for all other nodes to pick up. Other nodes can then take bookings for the token from their members.



There is a 4 step process in the booking and issuing process.

1. The account transfers currency tokens (currency), to their Escrow address. Anything in this Escrow address still "belongs" to them but is earmarked for a future transaction. Metadata containing some of the Booking data is also recorded with the transfer to tie them together.

2. The account then prepares an atomic exchange instruction. This is an instruction to transfer ***x*** currency for ***y*** asset. This instruction is incomplete as it only has one leg, which has been authorized by the account. Only when the issuer provides the asset issuance leg and authorizes it will the instruction be complete and can be sent to the blockchain.

   The account also prepares a refund instruction. Both the exchange and refund instructions are encrypted using the Issue Address' public key and attached to the Booking.

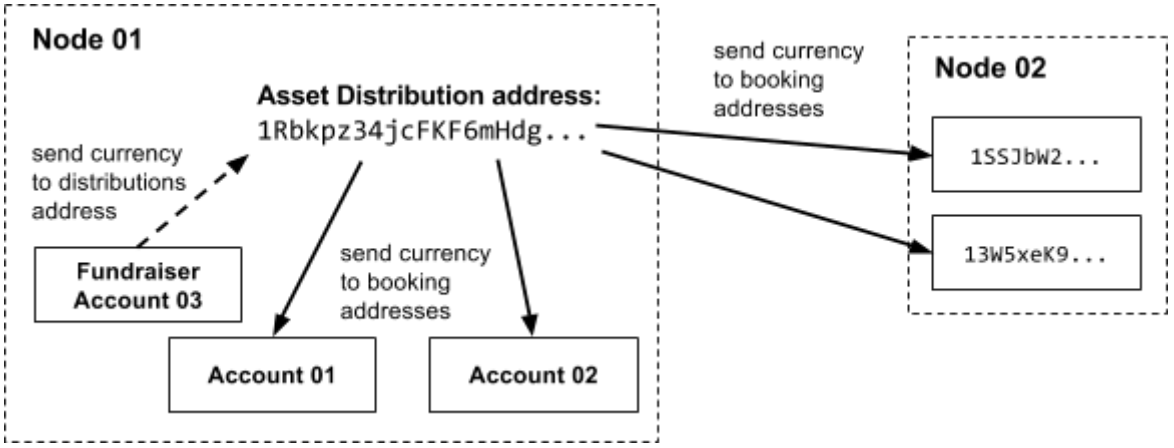
3. The Booking is broadcast on the Booking Stream and can be picked up by the issuing node. The issuing node will decrypt the booking and make sure that the

exchange instructions are correct. If not, it will reject the booking and execute the refund instruction.

4. Once the booking period is over, then the issuing node can allocate the Assets to be issued according to various algorithms. For each booking, an asset is allocated and the exchange instructions are completed and broadcast to the blockchain.

Distributing Returns

Distributing returns is a relatively straightforward process. The fundraiser will send currency tokens to the Token Distribution Address and then those funds will be distributed to the addresses which contain the Tokens.

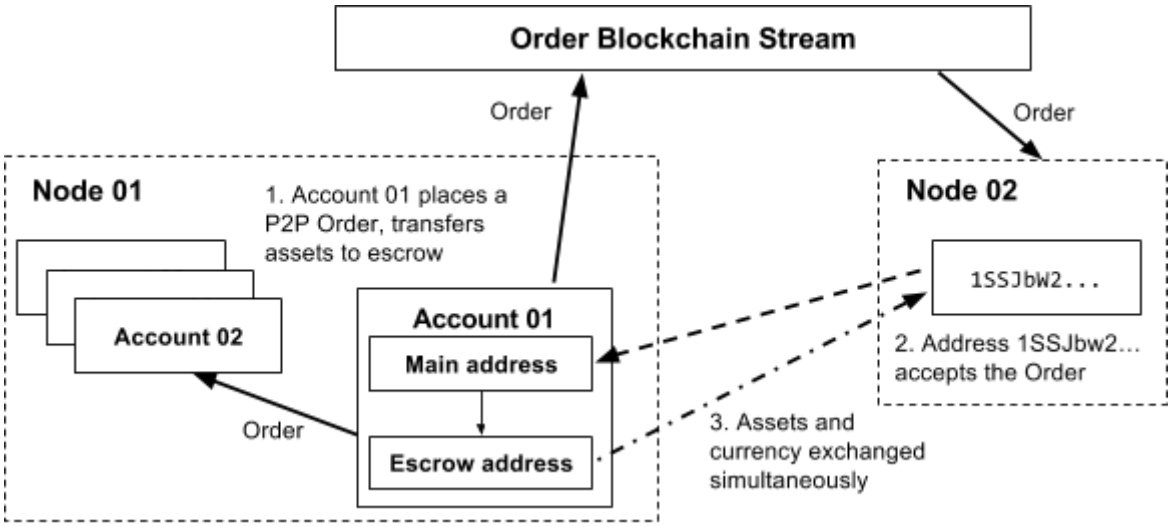


Trading

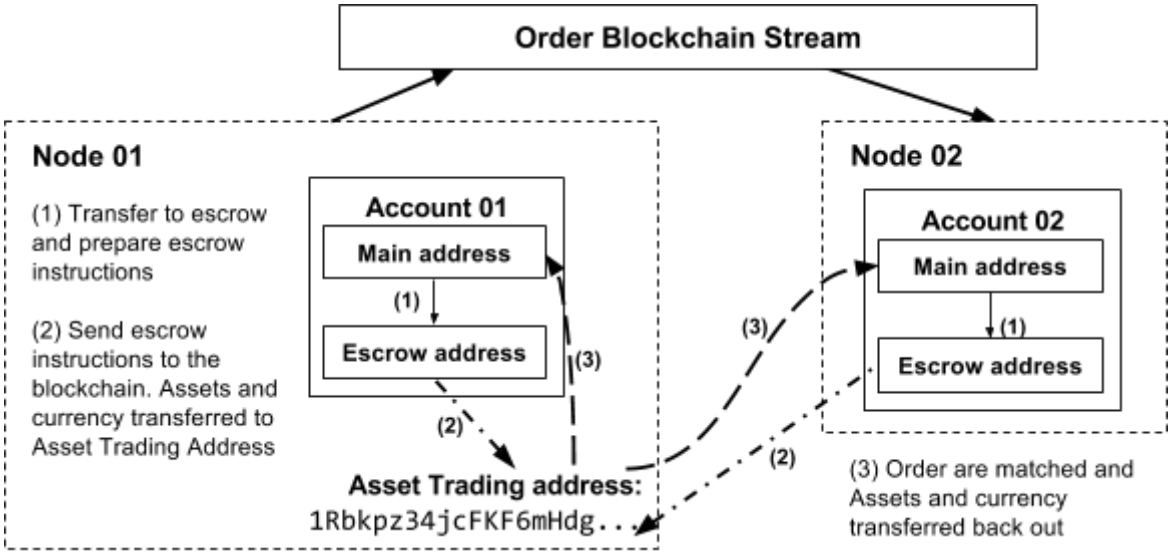
There are 2 types of trading, Peer-to-Peer (P2P) trading and automated trading.

In **P2P trading**, an investor makes an offer to sell ***x*** of an Asset for ***y*** currency (or vice-versa). The seller will transfer their asset to their escrow address and prepare an atomic exchange transaction instruction.

The incomplete instruction is sent with the order to the Order Stream. All the nodes will receive it and can offer it to their users. Any potential buyer can view the instructions and if they agree with the trade, add their leg of the instructions. They will then send this to the blockchain to be confirmed as a transaction.



For **Automated trading**, an investor makes an offer to sell ***x*** of an Asset for ***y*** currency (or vice-versa) with the possibility of partial fulfillment but with the promise of more liquidity and quicker execution of the trade. The issuer of the asset will facilitate trading by acting as a market maker or matching orders directly.



The seller will transfer their asset from their main address to their escrow address and then prepare an escrow instruction that will transfer the assets from their escrow address to the Asset Trading address. This instruction is signed but not broadcast to the blockchain yet. The order is generated and the instruction is added to it. Then the entire order is encrypted using Asset Trading address' public key, after which the order is sent to the Order Stream.

The order can be picked up from the Order Stream by any node, but it can only be decrypted by the node that manages the Asset Trading address. Other nodes will just ignore this particular order. Once sufficient orders are received, an order matching algorithm is run for that particular Asset.

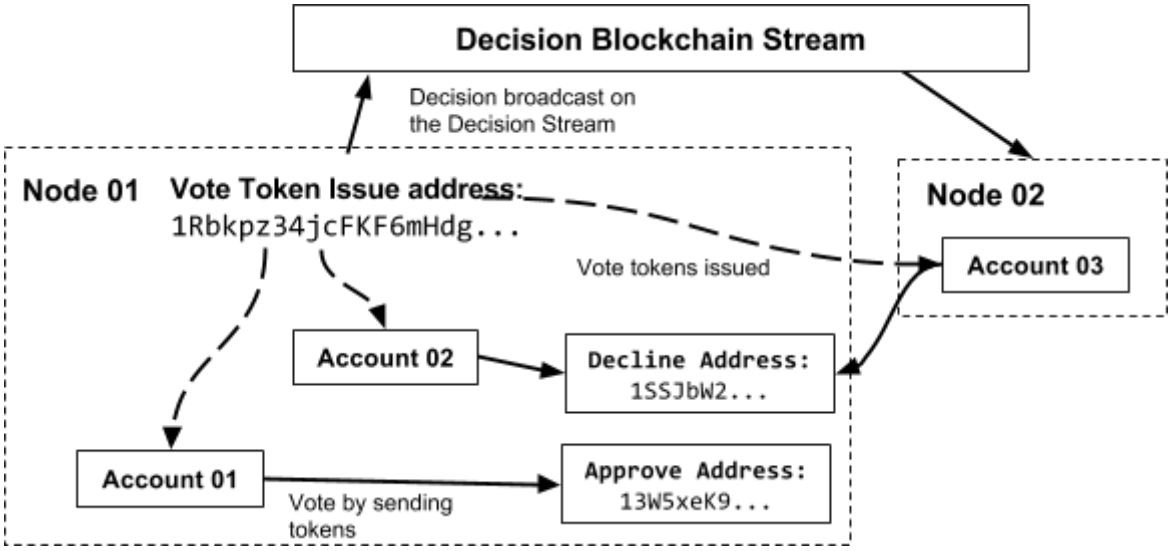
Once the algorithm has matched the orders, the matching orders' escrow instructions are broadcast to the blockchain. This results in currency and tokens being transferred from the escrow addresses of accounts that have placed orders to the Asset Trading address. Then those assets and currency are transferred out to fulfill the orders.

Voting on Decisions

Periodically, token holders can vote on whether various decisions will affect the investment underlying their token. The votes are basically tokens and each decision will have its own unique vote token. For the vote to be conducted, vote tokens will be issued in a 1:1 ratio to those addresses which hold the assets.

Voters can either approve or decline the decision by sending their tokens to either an **Approve** address or a **Decline** address. Voting will be open for a certain time period and when either an Approve or Decline address contains 50% + 1 of the voting tokens by the end of the voting period, then that choice "wins". If no choice has a majority, then the decision is considered to be declined.

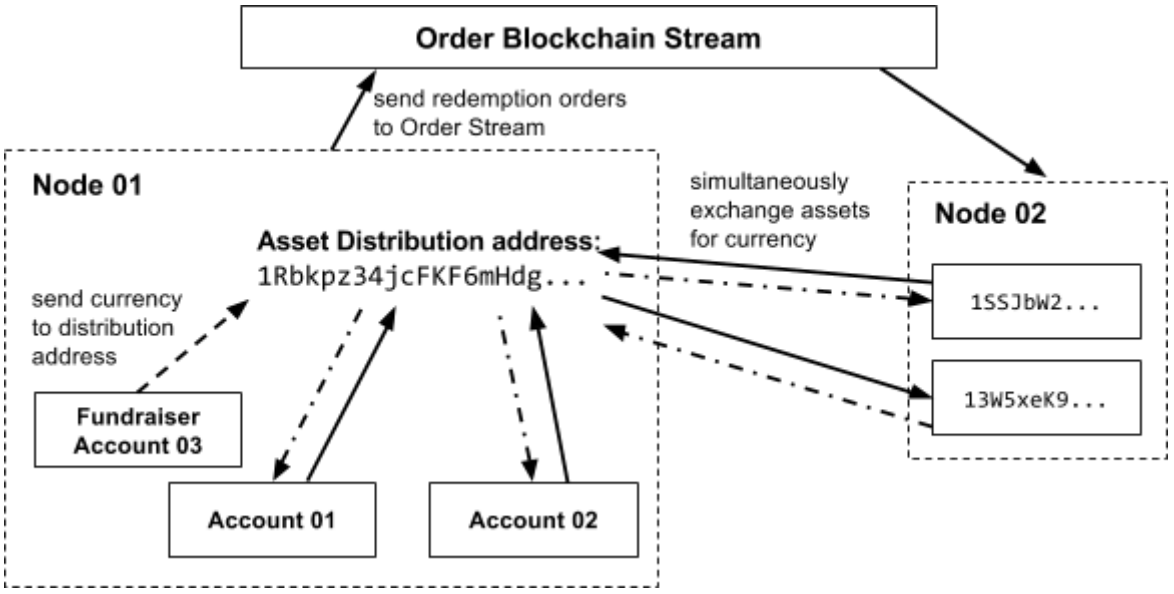
Additionally, once vote tokens are issued, they can be traded like any other token.



Redeeming Tokens

At the end of the lifespan of the investment, the Assets can be redeemed by the issuing address. Automated trading is shut down and all tokens and currency are returned to the originating addresses.

Currency for the redemptions are placed in the Asset Distribution Address and atomic exchange transaction instructions are prepared for each address that contains the Asset. Each instruction is encrypted with destination address' public key and broadcast on the Order Stream. The order can then be picked up, decrypted and accepted.



Ethereum Integration (Future Roadmap)

Ethereum integration will allow assets and currency issued by FundPlaces and partners to be pushed from the private blockchain to the public Ethereum blockchain and vice-versa. Accounts on the platform will send their tokens to a holding address on the private chain, while specifying the destination Ethereum address.

Tokens in this holding address will be mirrored on the Ethereum blockchain in the form of ERC 20 tokens and credited to the destination Ethereum address. These tokens can be traded on the Ethereum blockchain, but they can only be redeemed if they are pushed back to the private chain into an account.

This ensures that all beneficial owners of assets will need to go through appropriate KYC measures to claim the benefits.