ZENTADEX BLOCKCHAIN BASED DECENTRALIZED EXCHANGE

Abstract:

A pure peer to peer version of the exchange system would allow all parties access to the market without relying on any central organization for market access. Paper proposes a solution for the problem of maintain an order book and determine the execution rate in the peer to peer network. Like cryptocurrencies, the network relies on the blockchain of transaction. The digital signature system would be the core of the decentralized marketplace. The paper defines basic ground rules for the working of a decentralized exchange. The major components of the decentralized exchange are issuing process, co-existence of blockchain, order books and functions of the miner. Unlike other cryptocurrencies, decentralized exchange would have a trust-based issuing process which in long run would be a sum zero game. A Decentralized Exchange have 3 types of entities namely – Issuer, Trader and Miner.

1. Introduction

Traditionally exchanges have been a place where buyers and sellers of a commodity meet to decide on a specific price for the commodity based on demand and supply. Initially, an exchange was a common marketplace, later it evolved into an organized market place regulated by defined rules. The decentralized exchange which can facilitate the functions of exchange without relying on central point of authority embedding all the basic principles of exchange in an autonomous technical protocol by extending the capabilities of blockchain.

2. Functions of exchange

The exchange by very definition is an organized market place where various commodities, currencies, financial securities and derivatives are traded. The Basic Components of any exchange are the Entities (buyer and seller), A pair of Financial Instrument (Commodity, Security, Currency or Derivatives), Quantity in trade and Price for the Financial Instrument against another Financial instrument. For this paper, Currency has been considered as a financial instrument. Each Financial instrument has a finite unit of exchange. (I.e. 1 oz of gold is a basic unit of exchange or 1 unit of share is a basic unit for exchange.). In exchange, the entities bring in their respective financial instrument for trade with other financial instrument and based on demand and supply between two financial instruments the price is determined.

3. Zentadex exchange

The Zentadex exchange relies on the fundamentals of blockchain for storing transactions over a peer to peer network. Unlike cryptocurrencies, the decentralized exchange has three types of entities (i.e. Issuer, Trader [User] and Miner). The network relies on issuing process (Definition, issue, and withdrawal), orders (Open order and execution order) and blockchain. The miner would verify the

transaction for validity as well as match the execution orders and upon successful confirmation would generate a block using proof of work as followed by the Bitcoin protocol.

a) Issuer:
Issuer is the entity who is the initial starting point for the decentralized exchange. The issuer has Private Key [IPv], Public Key [IPu] and Issuing Token [In]. Only Issuers can generate financial instruments in the decentralized exchange and can delegate the right of being an issuer to another entity by generating new issuing token. The Issuer defines / issues /withdraws, which facilitates the entry and exit point for the market there making a sum zero game among Issuers and Trader. By definition, issuer is a custodian for all the Issued within the marketplace. (I.e. amount of a Flx held by issuer in custody should be amount of a Flx in circulation inside the decentralized marketplace.) The Issuer is entitled for an issuing cost via discounting methods.

b)Trader:
A trader is an entity that places the order to either buy/sell a defined quantity of Flx in lieu defined quantity of Fly upon finding a successful match (i.e. countering order) an execution order is broadcasted by trading entity which determines the price and is subject to verification by mining entity. Trader has private key [TPv] and Public Key[TPu]. The Trader places open order on the network as a broadcast to all the nodes. Each order has an exactly opposite countering order which would result in execution order. The trading entity constantly monitors the network for countering order for the orders placed by itself to generate the execution order. The execution order determines the notional price for a specific market (i.e. market between Fix and Fly). The trading entity can cancel the order which has been issued by itself. The trading entity has the option to select the market it wills to be active on (I.e. Pair of FI market where trader wills to be active on), so that only open orders relating to a particular market are only being accessed by that node.

c)Miner:
Miners are entities who constantly listen to the network for successful transaction broadcasted by the nodes. The transactions monitored are issue token transfer transaction, FI Definition transaction, FI issue transaction, Execution orders, and FI withdrawal Transaction. The mining nodes have the function of validating all the transactions. By validating issue related transaction (Token transfer Tx, FI definition Tx, FI issue Tx and FI withdrawal Tx) miner brings trust into the marketplace. By validating execution order the miner determines the actual price between two FI's. The validates all the transactions by using proof of work and generates a block which is stored sequentially in blockchain upon consensus by other nodes. The transaction cost associated with all transaction is accumulated by the miner and is the incentive point for miner. The mining node must listen to all events happening across markets (i.e. All Pair of Financial instrument).

Transactions in the decentralized exchange.

The Transaction in a decentralized exchange are of many types but all of the transactions are linked to Genesis transaction.

Token transfer Tx:
All issuers have a token which serves the function of limiting the number of FI's being floated in the decentralized exchange. Only the Issuer can generate an Issuing token which can be passed down to another issuer using a token transfer transaction. Issuing token is the hash of the new token owner's public key and a previous token which is signed by previous token owner's private key, forming a block chain of issuing token thereby providing the trust relationship amongst issuers.

Price Discovery using the blockchain and mining

Notional Price:
In the decentralized exchange, price is determined by executive orders. Notional price is determined when a node in the network broadcast's an execution order. However, the notional price of exchange for two FI's is subject to validation by a miner since it can include bogus transaction (i.e. Double Spend transaction, etc). Notional price is the real-time price of a commodity but not the real/actual price of exchange for two FI's.

Actual Price:
Actual Price of exchange for two FI's is determined by successful confirmation of execution order in the block. Actual price is calculated on the basis of the valid execution transaction in block broadcasted in the network by the miner. Actual price is the real price of exchange prevalent in the market. All nodes update their open order books/ buffer upon receiving the new block.

Mining:
The purely decentralized exchange is coinage independent but dependent more on a network for optimal functionality. Decentralized exchange can be implemented in either of the methods. (i.e Proof of stake or Proof of work). **Proof of stake would be Ideal implementation for a completely decentralized exchange, however, the method of implementation is subject to debate. The ideal block generation rate would be by 1-60 seconds for a decentralized exchange.**

Incentivization in the blockchain

For Issuer:
The issuer is entitled to issuing/withdrawal fee and is directly allocated to the issuer as a direct percent of Transaction and is at the discretion of the issuer.

For Miner:
The decentralized exchange is coinage free thereby not depending on any specific coin for its stability but issuer generates various FI's which act as coins. Each transaction in the decentralized exchange is subject to transaction fee except for token transfer transaction and definition transactions. The transaction fee is mandatory for all the parties in the decentralized exchange.

For a transaction to be executed, it must meet the following requirements:

-The transaction must be a well-formatted RLP.
-The transaction signature is valid.
-The transaction nonce is valid.
-The gas limit is at least as big as the intrinsic gas required for the transaction.
-The sender has enough Ether to cover the upfront payment, which consists of the gas fee and the value to be sent.

Execution transaction:

Each and every open order has an equal and opposite open order which makes the exchange transaction between two parties complete. Theoretically, execution order is a collision point for two

opposite orders and is recorded in the blockchain. Execution order can only broadcasted by the nodes who broadcasted initial open orders. Execution order is subject to split transactions (i.e. – Large open order can be fulfilled by multiple smaller countering open orders.), thereby making a partial execution of the order. Technically execution order includes the both countering open order signed by issuer of the either of the order. For any open order, there can be a minimum two execution order. At node level, the execution order are broadcasted only if they meet the execution conditions. Following are the execution conditions. If the countering open order matches the specification of broadcasted open order, then broadcast the entire amount as execution order. Else calculate the difference between the orders and broadcast the execution order of appropriate measure leaving the rest as open order. Execution transaction confirms the transfer of ownership of one FI to another.

Gas Fee and Miners:

In order to prevent users from abusing the network, all computations on the Ethereum network are charged a certain amount of fees measured in units of gas. Every transaction on the Ethereum network comes with gas fee, which is determined by gas price and gas limit.

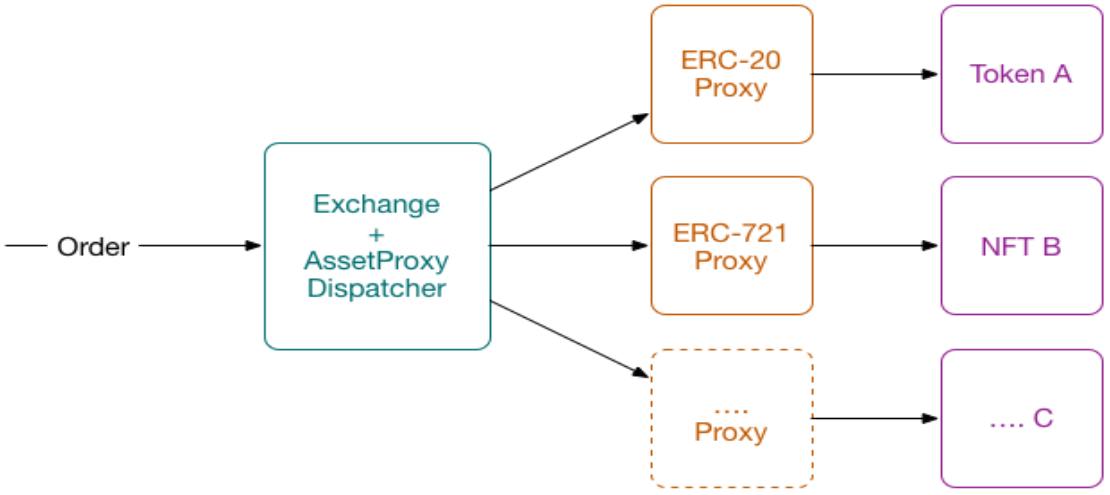
Gas price is the number of Wei per unit of gas. Gas limit is the maximum amount of gas the sender agrees to spend on executing this transaction. The product of the two represents the maximum amount of Wei the sender is willing to pay. If the sender wants his/her transaction to be mined first, he/she usually sets a high gas price to attract miners to prioritize his/her transaction. Thus, the sender has a trade-off to make between minimizing the gas price and maximizing the chance of his/her transaction being mined in time.

Metamask:

Metamask is a popular Google Chrome application connecting the web browser and the Ethereum wallet, and it is used by most of the decentralized exchanges. Although Metamask provides a strong and reliable connection between the Ethereum wallet and the decentralized exchange.

How to use Metamask, for more information please check:

Link to Metamask:https://metamask.io



Summary:

On an architectural level, decentralization means that there is no centrally-controlled server(s), and the networks' nodes are distributed.

The Two Types of Decentralized Exchanges

As exchanges revolve around transacting currencies, there are two fundamental exchange models: currency-centric and currency-neutral. Either of these models can be centralized or decentralized, depending on how the four key functions of the exchange are handled.

Currency-centric exchanges are built on top of singular blockchain platforms, such as Ethereum. A currency-centric exchange is limited to escrowing only the currency of the platform it is built on, such as ERC20 assets and other contracts if the exchange is built on top of Ethereum. This is the way traditional exchanges are built.

The newer model is currency-neutral, which is architected to connect different native cryptocurrencies, meaning that users do not have to adhere to any specific currency ecosystem. These systems allow users to trade cryptocurrencies without a coin underlying that exchange, which acts as a sort of additional "middleman" to go through since it is no longer fully peer-to-peer.

These newer projects allow for securely matching and handling order books and not just asset exchange, in a decentralized manner, which is done using the blockchain. Because the exchange is a community of users, there has to be a way to broadcast and match orders. One way of trustless trading is through "atomic swaps" for order matching, but atomic swaps alone cannot create a trustless marketplace, as it is done from one specific peer to another, rather than as a broadcast to anyone on the network. Anatomic swap is when a trade is done in a single, or atomic, operation, as opposed to two separate transactions (such as first sending one coin, then waiting for the receiver to

send their coin). This is facilitated through smart contracts that act as a trustless escrow holding onto one currency until the other user sends their currency as well when both currencies can be released.

The Pros and Cons of Decentralized Exchanges

The most obvious benefit of a DEX is the same as with any decentralized application, which revolves around the philosophy of cutting out the middlemen and returning interactions to peer-to-peer, permissionless models without central authorities. More specifically, decentralization creates censorship-resistance, which in the case of decentralized exchanges means that no central authority could forcefully impose regulations, or even ban currencies and/or the exchange itself. This is especially important considering that many countries are clamping down on cryptocurrency trading. For example, the two most populous countries on earth, China, and India have banned cryptocurrency exchanges, while countries including Mexico, Russia, Saudi Arabia, and Brazil have restricted cryptocurrencies.

Without Decentralized Exchanges, the people's ability to invest in a crypto is subject to governments, so cryptocurrency becomes hardly more democratic than traditional asset markets. Governments can exert control over centralized exchanges and users are subject to authorities who may at any moment track and tax users, or ban currencies.

Other merits of a DEX include heightened security. Massive security attacks, such as the roughly $470 million that was stolen from Mt. Gox, were only possible because the centralized hot wallets of the exchange were targeted, which presented a single point of failure. In a DEX, each user is in private control of their own funds, so there is no central point of attack. However, as we'll get to later, many exchanges claim to be decentralized, such as Bancor, but are truly hybrid, and their centralized aspects present vulnerabilities. For instance, around $23 million was recently stolen from Bancor, and Bancor responded with a freeze attempt built into their protocol, which is only possible with at least a partially-centralized architecture.

As we'll see, DEXs use Smart Contracts to facilitate transactions, such as using contracts as an escrow for peer-to-peer transactions. If the contracts themselves are highly secure, then the exchange benefits from the cryptographic security of the underlying blockchain. However, this is often not the case, and Smart Contracts can contain many vulnerabilities, including underflows, overflows, reentrancy attacks, and many more.

Further, a DEX could facilitate faster and cheaper transactions than a centralized exchange, since there is no third party authenticator. Currently, this is just theoretical and has yet to be proven by exchanges on a large scale, as DEXs have not achieved the "network effect" of reaching enough users for critical mass.

The application of decentralized exchange to other normal business functions like online ticketing or commoditizing of various daily products using decentralized exchange is a matter of debate for the future as well as a definition of time driven and other such complex financial instruments are a matter of research for the future.

The largest drawback of current DEXs is the lack of functionality and this will cover Zentadex.

References:

Hashcash - a denial of service counter-measure http://www.hashcash.org/papers/hashcash.pdf.

Merkle, R. (April 1980). Protocols for public key cryptosystems. Symposium on Security and Privacy, IEEE Computer Society, 122-133.

“Decentralized Cryptocurrency Exchanges”
“Atomic Swaps and Trustless Cross-Chain Trading”
“The Trouble With Centralized Exchanges”

Nakamoto, S. (2011). Bitcoin: A Peer-to-Peer Electronic Cash System.