OEX White Paper

OPEN DEX (Open-source Decentralized Exchange)

OEX Chain—To Build the Safe, Convenient DeFi Application Infrastructure

Catalog

Abstract:

Bitcoin redefines the currency and truly realizes the digitization of the currency, and also redefines the decentralized issuing Mechanism, and the asset circulation realized by decentralized institutions. Blockchain-based Digital assets change rapidly, resulting in the needs of a variety of digital assets and financial derivative products, like digital assets issuance, digital assets transaction, digital bonds, options, digital fund, P2P lending, assets management, mortgage, digital asset custody, fundraising, etc..

Digital finance and its derivative products are with huge potential market and bright prospects, but still trapped by blockchain technology bottleneck, and quite a gap for large-scale application, which technical innovation is needed badly for driving the upgrade of the whole industry. Take Ethereum network as an example, we’ ve known most of the Decentralized Finance (DeFi) applications are based on Ethereum, while the network congestion keeps getting serious, which the upgrades and capacity expansion are

needed urgently to meet the development of the diversified and complicated contracts, and also the higher liquidity.

1. Overview of CeFi (Centralized Finance) Protocol

Usually when we tend to engage in a certain type of financial industry in the real world, a series of permits signed or issued by the Country are usually needed, to ensure the security of the financial industry, and the stability and security of the economy by restricting permits review and high access threshold to restrict and supervise the whole industry. However, there might be two extremes of financial resources configuration by state power, and the financial license almost means monopoly, because the majority of the financial assets and capitals pour in the few licensed institutions; the financial and capital resources configuration by the centralized financial institutions also leaves larger space centralized operation to do evil, as well as the space for power-seeking.

On the other hand, centralization completely took the throat of market innovation, and cut the resources with one- size- fits- all.

It’s known that market innovation is based on market liberalization, and the competition brought by liberalization will lead to open, transparency, and altruism, and benefit both individuals and the entire economy.

2. Decentralized Finance.

The emergence of DeFi (Decentralized Finance) provides another possibility for the circulation of financial products. Along with the development of more blockchain-based smart contracts, the decentralized financial products are now more plentiful, with more choices and higher liquidity.

The significance of blockchain technology for financial innovation is that the circulation of financial assets is completely dependent on ledgers, and the distributed ledgers by the blockchain-based decentralized accounting mechanism make the tamper impossible through centralized means. Through code, the decentralization by blockchain technology prevents the adverse impact brought by “human” - the most unstable factor.

The blockchain assets led by Bitcoin have behaved well in the distributed ledgers for the last decade, the consensus and incentive mechanism of the whole network brought new opportunity and the possibility to the innovation cored by blockchain technology, the exploration of decentralized finance will be the top priority for future digital finance.

So in conclusion, we can roughly divide digital assets into three stages: first is the generation of digital assets, also the issuance of digital assets based on blockchain technology; The second stage is the right confirming of digital assets, to complete the right confirming of digital assets through the blockchain technology; The third is the digital asset circulation, to complete the asset circulation through the centralized or decentralized exchanges. The whole process is essentially a kind of financial behavior of the digital assets.

3. Current DeFi Market

3.1 Market Description

Many people believe DeFi was originated in 2018 and developed in 2019. Currently, DeFi ecology map has been expanding continuously, with cases and scenarios in multiple areas such as the lending platform, DEX, Stable coins, derivatives, oracles and insurances.

DeFi keeps hitting new records since June 2020. According to DeFi MarketCap, the total market value of the top 100 DeFi tokens was 1 billion USD on April 14th and became 2 billion USD on June 9th. Until 12 on June 21, the total market value of the top 100 DeFi tokens has risen to 6.1 billion USD, and continue to soar.

3.2 About DeFi Protocols

Here we will introduce the three most popular DeFi products on the current Ethereum network:

➢ MakerDAO

Maker (built on the Ethereum blockchain). The Maker Protocol is one of the largest decentralized applications on the Ethereum blockchain. Designed by a disparate group of contributors, including developers within the Maker Foundation, its outside partners, and other persons and entities. It is the first decentralized finance (DeFi) application to see significant adoption.

The Maker Protocol is managed by people around the world who hold its governance token, MKR. Through a system of scientific governance involving Executive Voting and Governance Polling, MKR holders govern the Protocol and the financial risks of Dai to ensure its stability, transparency, and efficiency. One MKR token locked in a voting contract equals one vote.

➢The Dai Stablecoin

The DAI stablecoin is a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. DAI has been issued on Ethereum and other popular blockchains; DAI is held in cryptocurrency wallets or within platforms.

DAI is easy to generate, access, and use. Users generate DAI by depositing collateral assets into Maker Vaults within the Maker Protocol. This is how DAI is entered into circulation and how users gain access to liquidity. Others obtain DAI by buying it from brokers or exchanges, or simply by receiving it as a means of payment.

Every DAI in circulation is directly backed by excess collateral, meaning that the value of the collateral is higher than the value of the DAI debt, and all DAI transactions are publicly viewable on the Ethereum blockchain.

No matter it has been generated, bought, or received, DAI can be used in the same manner as any other cryptocurrency: it can be sent to others, used as payments for goods and services, and even held as savings through a feature of the Maker Protocol called the Dai Savings Rate (DSR).

Every DAI in circulation is directly backed by excess collateral, meaning that the value of the collateral is higher than the value of the DAI debt, and all Dai transactions are publicly viewable on the Ethereum blockchain.

➢ Compound

Compound operates similarly to the traditional bank model, which collects the deposited capital in a liquid capital pool and lent to borrowers. Compound are pools of assets with algorithmically derived interest rates, based on the supply and demand for the asset. Compound is designed with no Counterparty Risk, it allows users to deposit cryptocurrencies and earn interest, or borrow other cryptocurrencies against them. Therefore, nobody has to wait for a counterparty to repay what they have borrowed.
Each token has a separate pool of assets on the Compound platform. The corresponding pool of assets will increase when a borrower deposits some token as collateral, while will decrease when borrowing out. Therefore, the separate matching between two parties is no longer needed because of the asset pool, and no Counterparty Risk, which improves the transaction efficiency.
Deposit on Compound platform is very similar to the bank deposit, where users deposit their encrypted assets into smart contracts and earn the interest that comes from them. In addition, depositors can withdraw the principal and interest from Compound at any time.

As for borrowing from Compound, a borrower needs to deposit overcollateralized assets (collateral) that the platform supports, to earn the borrowing quota and borrow other crypto tokens.
Over-collateralization is used to lower the risk of the breach by the borrower in some way. The borrower will redeem his/her collateralized assets automatically after paid off the debts and interests. Users need to add more collateralized assets if the value declines below the borrowed assets, or will trigger the smart contract liquidation, in this case, the borrower will still have the borrowed assets but lose colleterial assets.

➢ Uniswap

Uniswap is an Ethereum based protocol that is designed to facilitate automatic digital asset exchange between ETH and ERC20 tokens. Uniswap is completely on-chain, and individuals can make use of the protocol via the DApp browser in Decentralized Wallet. Uniswap can also be thought of as being a DeFi (decentralized finance) project, because it seeks to leverage its decentralized protocol in disintermediating middle-men that are involved in the financial process of digital asset exchange.

The design architecture of the Uniswap protocol differs from the model found within traditional digital asset exchanges. Most traditional exchanges maintain an order book and use that to match buyers and sellers of a given asset. Uniswap on the other hand, utilizes liquidity reserves in facilitating the exchange of digital assets on its protocol.

The invariant formula that is used by Uniswap in determining the exchange rate between tokens is taken from a post published by Vitalik Buterin in March 2018. In this post, the exchange rates for an ERC20 token are calculated in accordance with the following formula:

$x*y=k$

k is a constant that does not change

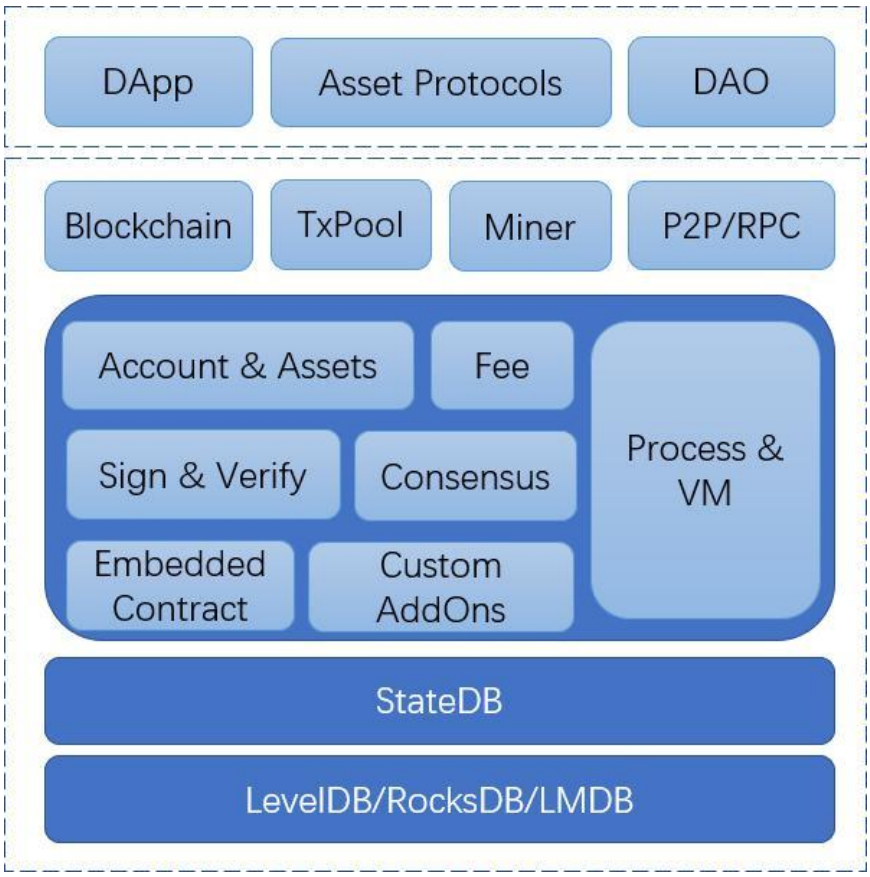
x and y signify the quantity of ETH and ERC20 tokens that are available on a particular exchange, which in the case of Uniswap, would be the amount of ETH and ERC20 tokens that are available in a given exchange contract. With this formula, the exchange rate of a given token will always be at a particular point on the resulting curve of the above formula.

4. Overview of OEX Chain

Based on the deep understanding of blockchain and digital assets, OEX Chain has developed a large number of innovative features. On the consensus level, it modified the transaction fee allocation model of the traditional blockchain and improved the consensus agreement, which not only improves the performance and security, but also set a solid foundation for the healthy development of the dapp ecology; on the economic model level, it realized the on-chain issuance and management, made the issued assets to become the overachievers on blockchain which may enjoy equal status with platform tokens. It fundamentally ensures the asset safety of users, and also lower the threshold of blockchain for users in traditional finance area, which will eliminate the obstacles for the overall prosperity of OEX ecology.

Please see the overall architecture diagram as follows:

OEX Chain Structure



5. Advantages of developing DeFi protocols on OEX

As described above, OEX Chain is specially designed for digital assets in terms of security and convenience, with Token-minting contract, parent-child accounting system, and the TPS higher CB-DPOS consensus mechanism embedded on the chain. We will explain the features of these functions in detail below:

➢ Token-minting Contract

The underlying native elements of OEX Chain are open source, which allows users to issue their own "native assets" on OEX chain. Smart contracts are no longer required when issuing assets, but the one-click issuance by filling in the asset information on the wallet page.

OEX Chain is permitted to define and restrict assets by native elements, so the digital assets issued by users are no long the state data on contract, but the account data as native tokens on the public chain, that’ s why we could native assets. Protected by native elements, the safety of the native assets is greatly improved by the functions the native elements provided, which can completely eliminate the safety risks for ERC 20 typed assets brought by contracts and allow users to fully control their tokens.

All assets on OEX Chain are equal, and no main and affiliate assets distinction between them. Meanwhile, all assets on OEX Chain are easily processed the same by applications like wallet browsers, to facilitate the use of smart contracts on chain.

Independent DeFi protocol can be introduced to native assets for adapting to more application scenarios during circulation, which could intergrade native assets with DeFi business logic, to meet the requirements of users. You only need to upgrade the circulation protocol the native assets bound if DeFi business logic needs to be upgraded in the future, which to the greatest extent to meet the different needs of the finance area.

➢ Parent-Child Account System

OEX Chain is similar to EOS on the account model, which account name is the customized string with better readability. Multiple tokens, smart contracts and public keys bound can be in an account, and the private keys are needed for signing the transaction during operating the account, because only the transactions with the legal signature can be processed by chain. Therefore, this typed account model is easier to understand and remember no matter for traditional network or blockchain users, and its expandability is more favorable for the popularization of DeFi protocols.

Considering that most crypto traders are users from traditional centralized exchanges, who may be not familiar to the high- threshold concepts like public & private keys, signature, and mnemonic words involve in blockchain account, OEX chain innovatively creates the Parent-child account function, which can greatly lower the threshold for average users on DeFi protocols. We will introduce the creation method, the basic features and the relationship between Parent-child account as follows:

a. The child account can only be created by the superior account, for example, if the parent account is google, the child account can be the first-level account google.chrome, or the second-level account google.chrome.bookmark. OEX Chain can support second-level child account by far.

b. The child account owns all the transaction permits, which is no difference with average accounts.

c. The parent account can replace the child account to send transaction, and the transaction signer will leave proof on chain. The parent account can sign the transactions for google.chrome and google.chrome.bookmark;

With child account, traditional exchange users can not only enjoy the transparency brought by blockchain itself, but also the interactive experience almost the same with traditional exchanges during DeFi protocol tradings.

➢ CB-DPoS Consensus Protocol

It has always been an issue for DPoS Consensus mechanism on how to bring more votes to the supernodes with higher stability. The actual bookkeeping performance of the blockchain system with DPoS is far worse than laboratory data, except for network, there is another important reason: the instability of the bookkeeping supernodes. However, the innovative DPoS Mechanism of OEX Chain-CB-DPoS resolves the issue successfully. CB here stands for Community Based, which means OEX Chain will use its Voting Incentive Mechanism, select the supernodes with high stability, to improve the actual bookkeeping performance of the whole system. See detailed procedure as follows:

- The CB-DPOS defines every 7 days as a bookkeeping cycle;
- An initial ranking of the 28 supernodes is based on votes they got;
- The top 21 supernodes take charge to bookkeepin turns, and the remaining seven will be as candidate super nodes which will replace these supernodes when they got wrong during bookkeeping;
- The bookkeeping supernodes will be replaced by candidates for violations or malfunction
- Voting incentive system can avoid the blindness of voting, benefits voters with rational choices;
- Voters can vote according to the candidate's bookkeeping history, collateral OEX tokens, and other public information of the participating institutions, elect the bookkeeping nodes and candidate nodes of the next cycle;

  The incentive mechanism plays an important part in the whole process. First, the supernodes are selected by voting, voters will be rewarded only when the nodes are selected as supernodes. Second, the incentive amount is depended by the stability of the super nodes during its bookkeeping cycle, and the incentive of the stable nodes may be many times of the unstable ones.

  Only motivating community users to participate in community governance can improve the operation stability and security of the chain during the governance of the public chain, which is also the foundation to ensure the security and speed of transactions for DeFi protocols.

➢ DeFi Protocol liquidity mining incentive

In traditional blockchain ecology, all the transaction fees on chain are rewarded to bookkeepers, such as the miner and supernodes, but no incentive for the token issuers and contract developers even though they contributed to the whole ecology. OEX Chain will allocate 80% of the transaction fee to the native assets' issuers and DeFi protocol developers, so they can gain the platform incentives without designing the profit model themselves. Take Uniswap on Ethereum as an example, protocol developers couldn't obtain the incentives without providing liquidity, which is not fair. While on OEX chain, Uniswap developers can obtain most of the gas fees from the large volume, which can solve the income issue for developers.

6. Mapping mechanism of the digital currencies

Most of the digital assets in the blockchain industry are on traditional exchanges, Bitcoin and Ethereum chains based on reality, so how to map these digital assets on OEX chain will be our priority. Currently we can map these assets in two ways:

6.1 Map digital assets on other public chains to OEX Chains by the cross-chain protocols;

Take the mapping of Ethereum tokens to OEX Chain as an example, to explain to execution procedure of the asset mapping:

- To deploy asset mapping contracts both on Ethereum and OEX Chain

- Users can send their ERC tokens to Ethereum contract, then lock, and specify the account name on OEX Chain for mapping ETH or ERC-20 tokens on Ethereum to OEX Chain:
- When the external decentralized oracles received the ERC token mapping requests, contracts on OEX Chain will be called, to deposit the accordingly number of tokens into the account specified before;
- Deploying asset mapping contracts on both Ethereum and OEX;
- The same process occurs when the user needs to remap the mapped tokens from the OEX chain to Ethereum.

6.2 Carry out asset mapping through the centralized exchange as an intermediate institution

The asset mapping process can be achieved if the centralized exchange supports the deposit and withdrawal of a certain token (in exchange account) to different public chains. The following is an example of the procedure, on the token mapping between Ethereum and OEX Chain:

- Users deposit the Ethereum tokens into exchange wallets
- Then withdraw the token from the wallet to OEX Chain, so that the token mapping from Ethereum to OEX chain is complete
- The same process occurs when papping tokens from OEX Chain to Ethereum

7. OEX Token Allocation Mechanism

The total supply of OEX tokens is 1 billion, see the allocation plan as follow:

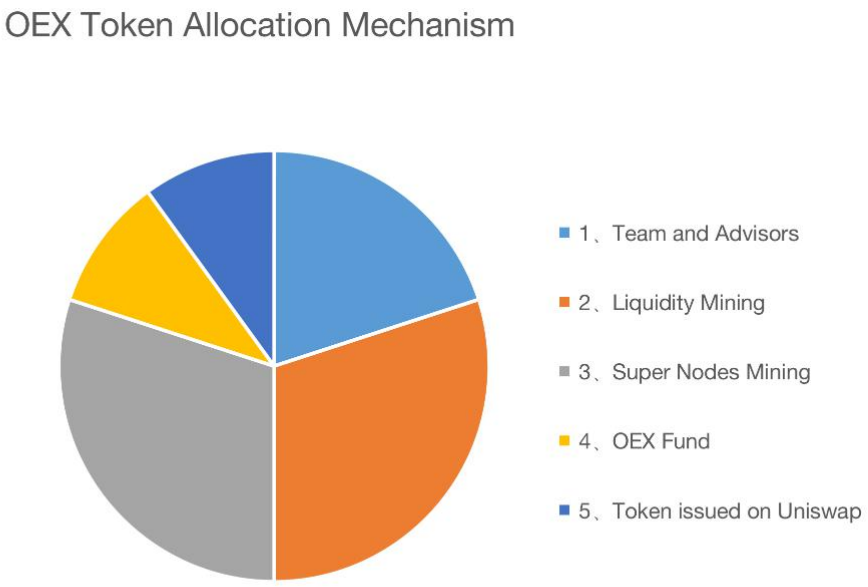
1. Team and Advisors 20%

2. Liquidity Mining 30%

3. Super Nodes Mining 30%

4. OEX Fund 10%

5. Token issued on Uniswap 10%



OEX Token Release Schedule:

a. Tokens for Team and Advisors: 1-year lock-up period, with linear release plan from the second year along with release token on the secondary market;

b. Liquidity mining will be used but not limited to: incentive in mining pool for liquidity mining of OEX Chain and OEX ecology, incentive for adding liquidity to DeFi Applications such as staking mining, lending mining. The detailed release rules will be realized on chain by smart contract after full analysis.

c. Supernode mining incentive plan is as follow which will be realized by smart contract:

c. Supernode mining incentive will be realized by smart contract as follows:

1)15% of the DPoS mining quota will be released for the first year, 7.5% for the second year, 3.75% for the third year, and 1.875% annually from the fourth year, until all been released;

2)The total tokens to be released for each cycle (21*6 blocks, 126*3=378 seconds=6.3 minutes) can be calculated by release ratio, and then allocated according to ranking of the miners (supernodes), the weighting coefficient of the 21 miners are:
100,95,94,93,92,91,90,85,80,75,70,65,60,55,54,53,52,51,50,49,48, and the total weighting is: 100+95+90+。。。+50+49+48= 1502

Take the first year (52 cycles) as an example: the total tokens to be released are 45 million, which will be ended at the 83200th epoch (each epoch generates 126 blocks), the tokens to be released in each epoch are:
45000000 / total epoch = 45000000 / (52 * 7 * 24 * 3600 / (126 * 3)) = 45000000 / 83200 = 540.865 OEX≈ 540 OEX tokens

Therefore, the top 1 miner of each epoch will receive: 540 * (100/1502) = 35.962 ≈36 OEX
Each miner is supposed to generate 6 blocks in each epoch, and the top 1 miner can receive 36/6=6 OEX from each block generated.
d. OEX Fund tokens: will be used as the staking mining of the 21 supernodes at the early stage, the released tokens also belong to the community Fund. All incentive tokens can be used for public biding, or institution investment at the primary market, and the profits will be used for project developing; the fund will be determined by community voting in the future;

e. Allocation Mechanism of AMA (Automated Market Maker) based token pools on Uniswap is open and transparent, 10% to be released will enter to secondary market;

8 Risk Disclaimer: Digital Asset Trading can be challenging and unpredictable, none of the above constitutes investment advice. OEX has never committed to any investment, fundraising on public market. Users are strongly encouraged to carefully consider their investment objectives, level of experience, and risk appetite, any losses, or liabilities shall be borne by the users.