OEX白皮书

OPEN DEX（开放式去中心化交易）
OEX公链——打造安全便捷的DEFI应用基础设施

目录

前言

比特币重新定义了货币，真正实现了货币的数字化，也重新定义货币的去中心化发行机制，资产流转方式，通过非中心化机构来处理资产流转。基于区块链技术的数字资产日新月异，从而带来了数字衍生资产的多样性需求，在数字资产发行、数字资产交易、数字债券、数字股权、数字基金、数字资产 P2P 借贷、理财、数字资产抵押、数字资产托管、数字资产募资、等等一系列金融以及金融衍生类数字金融产品。

数字金融及衍生品前景广阔，市场巨大。困于目前区块链技术瓶颈与大规模应用之间还有相当差距。急需市场技术革新驱动行业或者产业升级。以以太坊网络为例，目前绝大多数去中心化金融 DEFI 应用于合约开发都是基于该网络，于此同时该网络的拥堵一直在持续，网络急需扩容升级来满足更多样性复杂的合约开发以及更高的流动性。

1. 中心化金融产品内容概述

现实世界中，我们需要从事某一类金融行业时，通常需要该主权国家颁发或签署一系列许可，通过严格准入审查和非常高的准入门槛来限制和监督行业，以确保金融行业安全和该主权国家经济平稳安全。但是主权国家通过权力配置金融资源往往会出现两个较为极端的结果，一旦拥有从事该金融类型牌照几乎意味着垄断，因为牌照的极少数机构获得了大多数人金融类资产以及资金涌入，通过中心化的金融机构来配置金融资源和资金资源，给予中心化运营作恶的空间更大。其中权力寻租空间也是亦然。

另外一方面是完全限制了市场创新的咽喉，几乎一刀切式的完成了资源的切割。市场的创新基石是市场自由化，自由化带来的竞争会向公开、透明、利他化方向发展以普惠个人和利于整体市场经济

2. 去中心化金融概述

DeFi（Decentralized Finance 去中心化金融）的出现，让金融产品流转有了另外一种可能。随着越来越多的基于区块链智能合约的开发，去中心化金融产品也会越来越丰富，提供的可选择性也会越来越多，流动性也会越来越好。

区块链技术对于金融创新的意义在于，金融资产的流转完全依赖账本，区块链技术以去中心化记账机制所带来的分布式账本应用使得很难通过中心化手段篡改账本。

通过区块链技术带来的去中心化通过代码实现了防止“人”这个最不稳定因素带来不利影响。以比特币为首的区块链资产在过去十年间分布式账本一直记账良好，整个网络的共识机制和激励机制给以区块链技术为核心的革新带来了新的机遇和可能。我们有理由相信在数字化金融已然进入了新的发展轨道，去中心化金融的不断探索亦是未来数字化金融重中之重。

总结来说，大体上我们可以将数字化资产分为三个阶段：一是数字资产的产生，基于区块链技术发行数字资产；二是数字资产的确权，同时通过区块链技术完成数字资产确权；三是数字资产流转，通过中心化或去中心化场所完成资产流转。整个过程本质上都是一种数字资产的金融行为。

3. 目前 DeFi 市场简介

1、市场情况

业界普遍认为，DeFi 发端于 2018 年，过去的 2019 年是其发展元年。目前，DeFi 生态版图持续扩大，出现了借贷平台、DEX、稳定币、衍生品、预测市场、保险等多领域用例。

进入 2020 年 6 月后，DeFi 连创新高。DeFi MarketCap 数据显示，4 月 14 日，DeFi 代币名前100 的总市值为 10 亿美元，而到 6 月 9 日，这一数字变成 20 亿美元。截至 6月 21 日 12 时，DeFi 代币排名前 100 的总市值已升至 61 亿美元，并将持续攀升。

2、产品介绍

下面介绍下目前以太坊上最流行的三个 DeFi 产品：

- ## MakerDAO

Maker（基于以太坊网络的），Maker 协议是以太坊区块链上最大的去中心化应用之一，参与设计该协议的人员非常多样化，包括 Maker 基金会的开发者、外部合作伙伴，以及其他个人和实体。Maker 协议是首个获得大规模采用的去中心化金融（DeFi）应用。

Maker 协议由世界各地的治理型代币 MKR 持有者管理。通过由执行投票（Executive Voting）和治理投票（Governance Polling）组成的科学型治理系统，MKR 持有者可以管理 Maker 协议及 DAI 的金融风险，从而确保该协议的稳定性、透明性和高效性。投票合约中锁定的每一个 MKR 代币均等同于一票。

- ## 稳定币 DAI

稳定币 DAI 是一种软锚定美元的资产担保型加密货币，其发行是去中心化、无偏见的。DAI 已在以太坊区块链和一些其他流行的区块链上发行；持有 DAI 需要用到加密货币钱包或者加密资产平台。

DAI 的生成、访问和使用门槛都很低。用户通过使用 Maker 协议来创建叫做 “Maker Vault （Maker 金库）"的智能合约并存入资产来生成 DAI。这个过程既是 DAI 进入流通领域的过程，也是用户获得流动性的过程。此外，用户也可以从中介或交易所处购买 DAI；或者更简单一点，只要愿意接受 DAI 来支付，那就能得到 DAI。

无论是你自己生成的、买到的还是收到的 DAI，用起来都跟别的加密货币没有区别：你可以将 DAI 发送给其他人，用它来购买商品和服务，甚至可以通过叫做 “DAI 存款利率（DAI Savings Rate, DSR）” 的 Maker 协议功能，把 DAI 转入储蓄账户。

流通中的每个 DAI 都是由超额资产背书的 —— 担保物的价值总是高于 DAI 债务的价值 —— 而且所有 DAI 交易都在以太坊区块链上公开可见。

➢ Compound

Compound 的运营模式接近于传统的银行模式，以流动的资金池方式聚集存款人存入的资金，并将资金贷给借款人，通过算法平衡供求、设定利率。Compound 平台被设计为不具有交易对手风险，存款人向资金池供应加密资产获得利益，借款人向资金池借出代币并支付利息。因此，存款人不需要等待其交易对手偿还借款。

在Compound 平台中，每种代币拥有独立的资金池。当借款人以某一代币进行抵押时，相应资金池会增加；当借款人借出某一代币时，相应资金池会减少。资金池的存在使得交易双方不需要单独撮合，不存在交易对手风险，提高了交易效率。

对于存款而言，在 Compound 平台上存款与在银行存款非常类似，存款人将其加密资产存入智能合约，并赚取由此产生的利息。此外，存款人可以随时从 Compound 中提取其存入的本金和利息。

对于借款而言，从 Compound 借款需要借款人超额抵押该平台支持的代币，获得贷款额度，并借出其他代币。超额抵押的方式在很大程度上降低了借款人违约的风险。当借款人返还借款及利息后，将会自动收回锁定的抵押资产。由于抵押资产的价格存在波动，一旦其价格低于贷款水平的阈值，则需要借款人补仓，或者会触发智能合约自动清算，此时借款人会持有借款，但会失去抵押资产。换言之，如果借款人的借款能力不足，他们的抵押品将拍卖出售，用以偿还债务。

➢ Uniswap

Uniswap 是一种基于以太坊的协议，旨在促进ETH 和ERC20 代币数字资产之间的自动兑换交易。Uniswap 完全部署在链上，任何个人用户，只要安装了去中心化钱包软件，都可以使用这个协议。Uniswap 也可以被认为是一个 DeFi 项目，因为它试图利用去中心化协议来让数字资产交易过程中彻底实现去中介化。

Uniswap 协议的设计结构体系与传统数字资产交易所中的交易模型完全不同。大多数传统交易所都是通过维护一个“订单簿”，来匹配一种数字资产的买卖双方。Uniswap 则完全不同，它是利用储备金流动性来实现协议上的数字资产交易兑换。

Uniswap 用来确定 token 交易汇率的恒定乘积公式，最初来源自 2018 年 3 月 Vitalik Buterin 发表过的一篇文章中。此文中表述，根据以下公式来计算ERC20 代币的交易汇率:

$$x * y = k$$

k 表示一个不变的常数

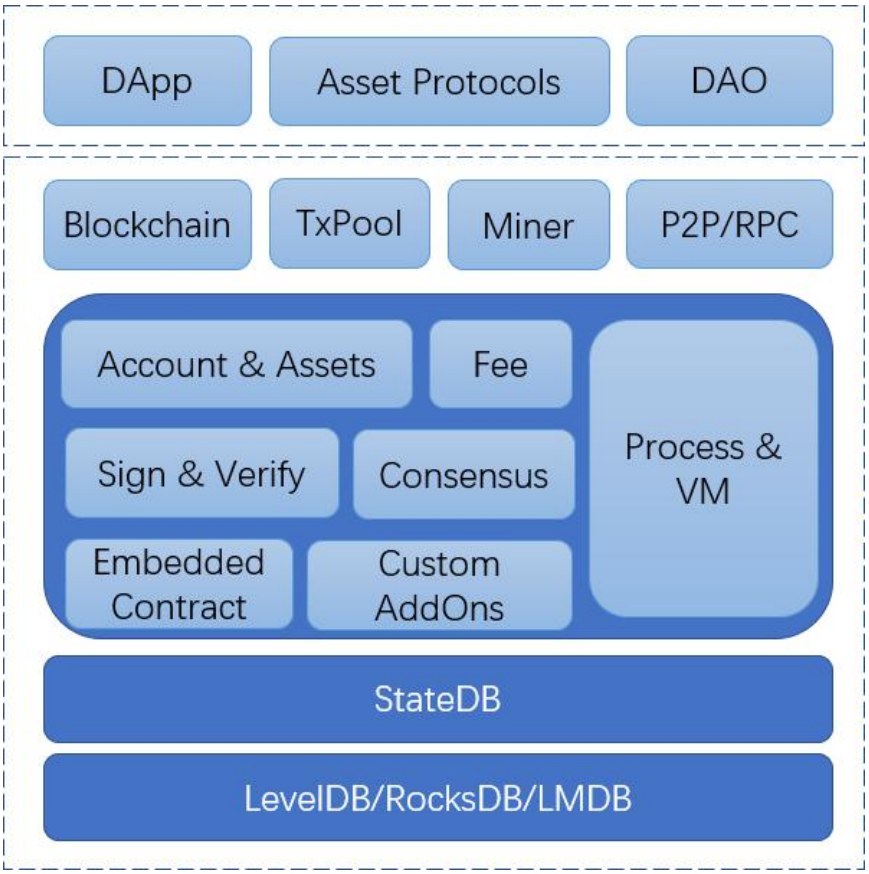
x 和 y 表示特定交易对中 ETH 和 ERC20 代币的可用数量。

对于 Uniswap 而言，则是该 ERC20 代币和 ETH 的交易合约中 ETH 和该 ERC20 代币的流动性池的储备量。在这个公式中，该 ERC20 代币和 ETH 的兑换汇率，将始终处于此公式结果曲线上的某一点。

4. OEX 公链介绍

OEX 公链基于对区块链和数字资产的深刻理解，开发了大量创新性的特性，在共识层面改造了传统区块链上的手续费分配模式并改进了共识协议，不仅提高了性能和安全性，同时对未来去中心化应用生态的健康发展奠定了良好的基础；在经济模型层面，实现了在链内发行和管理资产的功能，让用户发行的资产真正成为区块链上的一等公民，使其享有同平台币几乎相同的地位，从根本上上保障了用户资产的安全，同时还借鉴了中心化交易所的父子账户模型，降低传统用户进入区块链行业的门槛，将为 OEX 生态的整体繁荣消除障碍。

OEX 公链的整体架构如下图所示：



OEX 公链架构

5. DeFi 产品运行于 OEX 公链上的优势

如上所述，OEX 公链针对数字资产，在安全性和便利性方面进行了特别的设计，在链内嵌入了铸币合约、父子账户体系以及 TPS 更加的 CB-DPoS 共识机制。下面我们详细解释下这几种功能的特性：

- 铸币协议

OEX 公链将底层原生组件开放出来给用户使用，用户可以在 OEX 公链上发行属于自己的“原生资产”。用户在 OEX 公链上发行资产时可不再编写 ERC20 合约。只需要在钱包界面填写资产信息便可做到一键发行。

OEX 公链用原生组件对资产进行了定义和约束，用户发行的数字资产不再是合约中的状态数据，而是和公链原生代币一样的账户数据，因此我们称之为原生资产。原生资产使用原生组件提供的功能，受原生组件的保护，安全性获得了极大的提升，可彻底消除如 ERC20 资产中由合约引入的安全风险，让用户完全掌握自己代币的所有权。

在 OEX 公链中所有资产一律平等。没有主资产和附属资产的区别。同时，由于标准统

一，OEX 公链上的资产也很容易被钱包浏览器等应用统一处理，也方便链上的智能合约统一使用。

为了让原生资产在流通过程中适应更多的应用场景，可以为原生资产绑定独立的 DeFi 协议，将原生资产同 DeFi 的业务逻辑相结合，来满足用户的需求。如 DeFi 业务逻辑今后需要升级，也仅仅需要改变原生资产绑定的流通协议即可，能够最大程度的满足金融领域的需求。

- 父子账户体系

OEX 公链在账户模型上同 EOS 比较接近，账户名是用户自定义的可读性更好的字符串，账户里可包含多个 token、智能合约和绑定的公钥，操作账户时需要获取钱包中的私钥给交易签名，具有合法签名的交易才能被链处理。此类账户结构无论是对传统互联网用户还是区块链用户，都更容易理解和记忆，扩展性也更强，对 DeFi 产品的普及更为有利。

考虑到目前大量的数字货币交易用户都是传统中心化交易所的用户，这些用户对区块链账户所涉及的公私钥、签名、助记词等概念并不熟悉且入门门槛高，OEX 公链创造性的设计了父子账号功能，可以大大降低传统交易所用户使用DeFi 产品的门槛。下面介绍下子账户的创建方式、基本特性，以及父子账户的关系：

1. 子账户只能由上级账户创建，如父账户是 google，子账户则可以是一级子账户 google.chrome，也可以是二级子账户 google.chrome.bookmark。目前，OEX 公链最多只能使 用二级子账户。

2. 子账户拥有所有交易权限，这点跟普通账户无差异；

3. 父账户可代子账户签名发送交易，交易的签名者在链上留有存证，如父账户 google 可以为 google.chrome 和 google.chrome.bookmark 的交易签名；

有了子账号后，传统交易所用户在DeFi 产品上进行交易过程中，除了能够获得区块链本身所带来的公开透明的特性外，还能获得同传统交易所几乎一致的交互体验。

- CB-DPoS 共识协议

在 DPoS 共识机制中，如何让稳定记账出块的超级节点能够得到更多投票者的支持，一直是个难题。目前采用 DPoS 共识机制的区块链系统的实际记账性能通常远远低于实验室数据，除了网络原因以外，另一个重要的原因就是实际记账的超级节点的稳定性不佳。OEX 公链以创新型的 DPoS 机制—CB-DPoS—有效地解决了这个问题。CB-DPoS 中的CB 是 community based 的意思。OEX 公链利用投票奖励机制，甄别出稳定性高的超级节点，从而升整个系统的实际记账性能。具体流程如下：

- CB-DPoS 规则规定每 7 天为一个记账周期；
- 28 个超级节点会根据得票获得初始排名；
- 排名靠前的 21 个轮流记账，其余 7 个替补超级节点会在记账节点出错时替补记账；
- 当记账者违规或者出现故障不能记账，由替补记账者顶替该记账位置；
- 投票奖励机制可以避免投票的盲目性，让理性选择超级节点的投票人获益；
- 投票者会根据候选人的记账历史、OEX 抵押量以及参选机构的信息等公开的数据进行投票， 选举出下一个周期的记账节点和备用节点；

在这个过程中，奖励机制起了重要的调节作用。首先，OEX 公链的超级节点由投票产生，投票者选择的节点入选超级节点，投票者才有机会获得奖励。其次，奖励的数量取决于超级节点在记账周期内的稳定性，稳定节点产生的奖励可能数倍于不稳定节点。

在一条公链的治理过程中，只有最大程度的调动社区用户参与治理的积极性，才能让一条

链运行的更加稳定和安全，而这也是 DeFi 产品能同时满足安全和高速交易的基础。

- DeFi 产品流动性挖矿激励

传统区块链生态中，链上产生的交易手续费全部由记账者获得，例如矿工和超级节点。Token 的 发行方和合约的开发者虽然对整个生态作出了贡献，本身却没有任何激励。

OEX 公链将记账手续费的 80%分配给原生资产的发行方以及开发 DeFi 产品的开发者，使得这些为生态发展做出重要贡献的参与者无需自行设计盈利模式也可获得来自平台底层的激励。以以太坊上的 Uniswap 为例，产品的开发者如果不去为交易对提供流动性，那是无法获得激励的，这无疑是不公平的，而在 OEX 公链上，Uniswap 的开发者完全可以从庞大的交易量中获取大部分的交易 gas 费作为收入，从而解决开发者的营收问题。

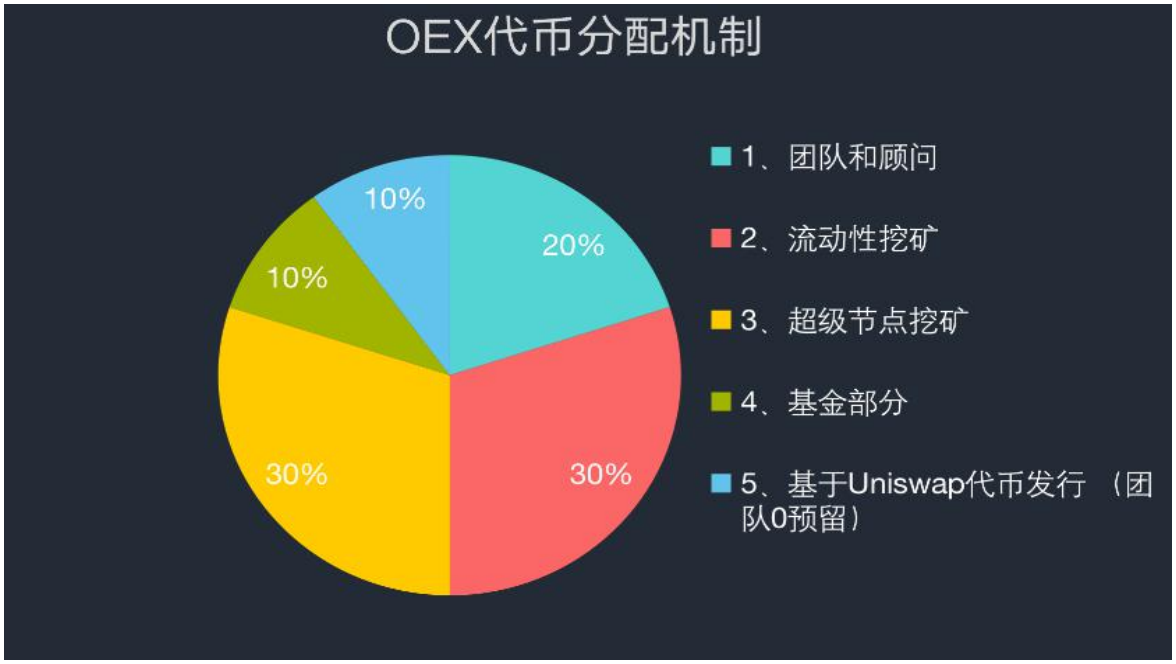
6. 数字货币映射机制

基于现实情况，目前区块链行业大量的数字资产都位于传统交易所和比特币、以太坊两条链上，因此能否将它们上面的数字资产映射到 OEX 公链上，成了我们必须要解决的问题， 目前我们采用两种方式进行映射：

1) 通过跨链协议将其它公链上的数字资产映射到 OEX 公链上
   下面以以太坊同 OEX 公链的映射为例，来简单说明此种资产映射方式具体执行过程：
   - ✧ 在以太坊和 OEX 上同时部署资产映射合约；
   - ✧ 当用户需要从以太坊上将 ETH 或 ERC20 代币映射到 OEX 公链上时，先将以太坊上的代币发到以太坊合约里进行锁仓，并指定需要映射到的 OEX 公链上的账户名；
   - ✧ 外部的准去中心化预言机获取到以太坊上的代币映射请求后，便调用 OEX 公链上合约，向对应的账户充入跟以太坊上锁定数量相同的代币量；
   - ✧ 当用户需要从 OEX 公链将映射过来的代币重新映射回以太坊上时，其过程同上。
2) 通过中心化交易所作为中间机构，进行资产映射
   如中心化交易所支持将一种代币（在交易所账户里）跟不同公链进行充提币的时候，便可完成此资产映射过程，下面以以太坊和 OEX 公链的代币映射为例，介绍具体过程：
   - ✧ 用户将以太坊上的代币充值到交易所钱包中
   - ✧ 用户将钱包中的代币提币到 OEX 公链，这样从以太坊到 OEX 公链的代币映射即完成
   - ✧ 从OEX 公链映射代币到以太坊，同上面过程

7. OEX 代币分配机制：

1、团队和顾问　20%
2、流动性挖矿　30%
3、超级节点挖矿　30%
4、OEX基金部分　10%
5、基于Uniswap等swap池代币发行　10%



OEX代币释放细则：
a、团队及顾问代币第一年锁仓，第二年开始随二级市场代币释放线性解锁
b、流动性挖矿将用作但不限于：OEX公链及OEX生态流动性挖矿池激励，抵押合约挖矿，借贷挖矿，等为DEFI应用增加流动性作出的激励，详细释放规则将充分论证后以智能合约在完全在链上实现。
c、超级节点挖矿激励将通过智能合约实现如下：
　1、第一年释放DPOS挖矿份额总量的15%，第二年释放7.5%，第三年释放3.75%，第四年之后每年释放DPOS挖矿份额的1.875%，直到释放结束
　2、通过释放比例可计算出每一轮（21*6个块，126*3=378秒=6分钟多一点）需要释放的代币总量，并按照矿工排名进行代币分配，21个矿工权重系数如下：
　100,95,94,93,92,91,90,85,80,75,70,65,60,55,54,53,52,51,50,49,48
　总权重之和：100+95+90+。。。+50+49+48 = 1754 - 252 = 1502
　以第一年为例（52周），总释放量是0.45亿代币，到第83200个epoch结束（1个epoch出126个块），其中每个epoch需要释放的代币数量为：
　45000000 / 总的epoch数量 = 45000000 / (52 * 7 * 24 * 3600 / (126 * 3)) = 45000000 / 83200 = 540.865个OEX ≈ 540 个OEX
　排第一的矿工在每个epoch里总共能分到：540 * (100/1502) = 35.962 个OEX ≈36 OEX
　每个矿工在每一个epoch里总共应该出 6 个块
　则排第一的矿工在每个自己的出的块能分到的OEX数量为 36 / 6 = 6

3. 成为矿工需抵押至少10万OEX，账户快照中需20万OEX方能被投票

d、 基金部分：早期将用作21个超级节点抵押挖矿，释放的代币同样属于社区基金所有。所有获得的代币将不向二级市场投放流通，但可以在一级市场以公开招标或者名单方式引入投资机构释放代币，所获得的投资收益早期将作为项目发展费用支出激励，未来将通过社区治理投票方式来决定如何使用该基金。
e、通过uniswap基于自动做市商（AMM）兑换池代币分发机制公开，透明释放代币总量的10%份额进入二级市场。

8、免责申明:
数字资产市场风险无法预估，以上均不构成投资建议，OEX代币从未在公开市场进行过投资、募资行为，相关责任用户自行承担。