DeOracle

无需许可的去中心化预言机

2021.1.1　v2.3.8

摘　要

随着 DeFi 生态和去中心化交易所的蓬勃发展，区块链上所有的应用程序对 Token 项目方价格数据的需求越来越大，需求类型越来越多，而目前市场上现有的预言机产品，全部诞生于 DeFi 火爆之前，其产品受制于设计架构，造成扩展性有限，安全度低等缺陷，并且在数据来源、交易对数量、防止闪电贷攻击等多方面无法满足现在 DeFi 生态庞大的要求，市场上迫切需要一种新型预言机满足日益增长的 DeFi 需求。

本文介绍一种全新的预言机产品—DeOracle：一种无需许可的去中心化预言机，可以满足市场上 DeFi 生态对价格数据的各种需求，通过本文您将了解到 DeOracle 预言机的特性、产品架构、商业模式以及未来的发展规划等信息。

目录

一、 引言

1.1 背景

自从中本聪在 2008 年创建比特币以来，至今已经 12 年，比特币因其解决了“双花”问题，对世界货币产生了深远的影响，引起各国央行的高度重视，促使各个主权国家也在发行各自的数字货币。截止到 2021 年 1 月比特币最高价格突破了 40000 美元，市值也达到了 7550 亿美元，超过了 FACEBOOK，特斯拉，俄罗斯卢布的市值。

根据比特币白皮书的介绍，比特币是一种点对点电子现金系统。比特币基于密码学的挖矿模式创造了区块链技术，从而实现了去除第三方信任，构成去中心化，创造了一个无需任何的信任背书，还能正常运转的支付系统。比特币依托互联网、匿名技术，逐步实现了在全球各地流通，并且在消费市场做为支付工具。

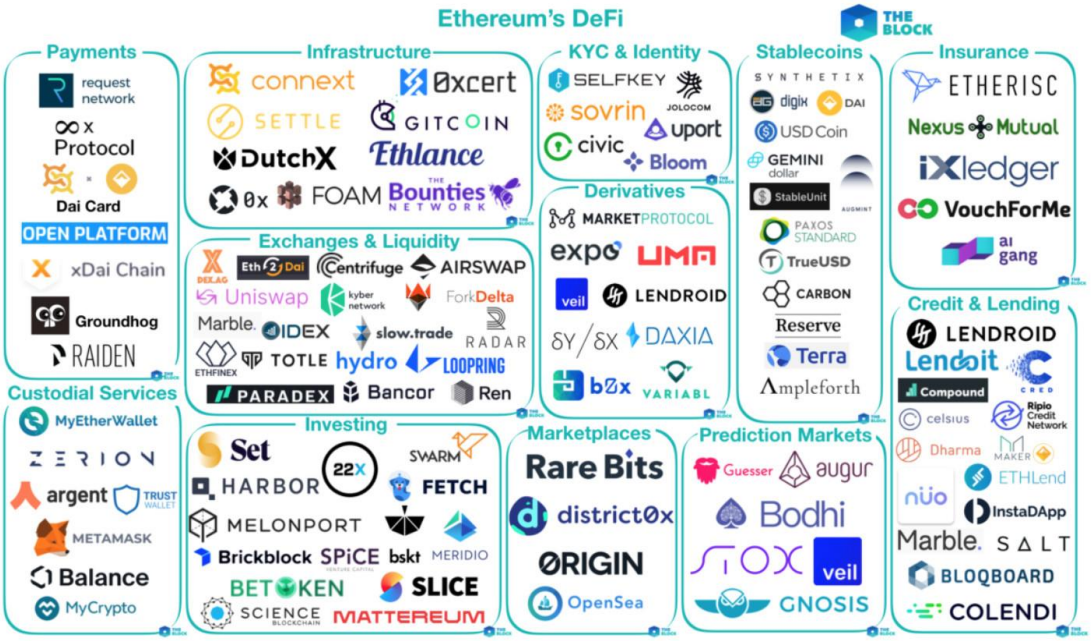
比特币首创的区块链技术，为了增强支付的安全性，采用了图灵非完备技术，但是同时也造成比特币智能合约的功能受限。于是，Vitalik 在 2014 年创立了以太坊，基于比特币的原理，采用了图灵完备技术，增强了智能合约的功能，进而在以太坊的区块链上迅速产生了一批应用程序的 DApp（比如：ICO、预测市场、以太猫、DAO、博彩）等流行产品。

以太坊的疯狂造势创造了 2017 年的牛市，币圈的市场也增加了 2000 万参与者，以太坊价格从当初 ICO 的 0.26 美元，最高涨到了 1400 美元。

1.2 DeFi 简介

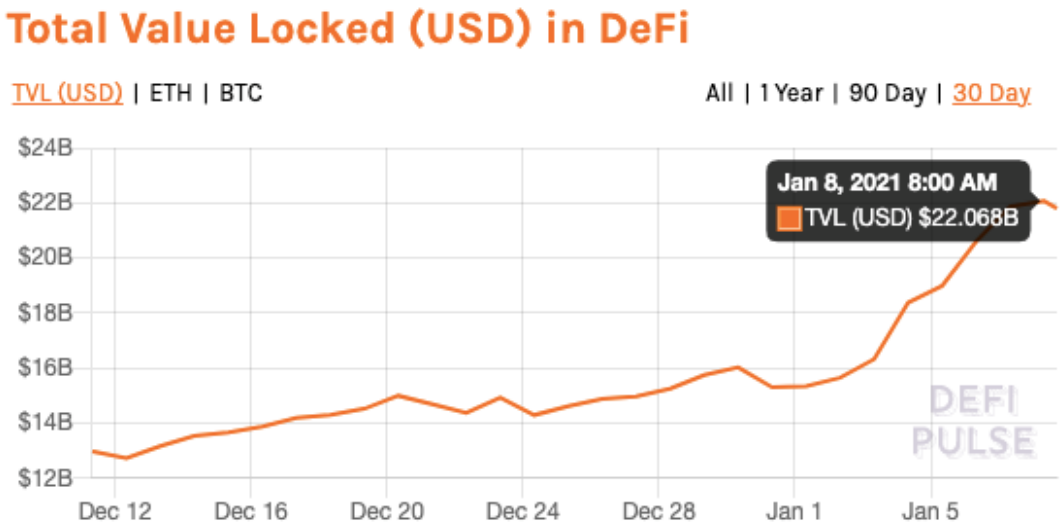
在 2018 年的熊市里，在以太坊中诞生了 DeFi（Decentralized Finance）即去中心化金融应用。通过区块链的智能合约技术，开发了一系列的金融产品，比如：借贷、抵押、理财、去中心化交易所、合成资产、金融指数等产品，形成了一个无需准入、无需信任、可抗审查的、资产在链上的全球性自由流动的金融体系。

因为智能合约之间是可以互操作的，所以 DeFi 产品也可以交互，像搭积木一样，拼接成多样化的产品。



上图是以太坊上的 DeFi 产品图

进入 2020 年以来，DeFi 成为了市场的热点，DeFi 生态上的资金、用户都爆炸式增长，甚至比特币社区都在宣称“比特币也是 DeFi”。目前 DeFi 生态上的锁定资金已经达到 220 亿美元，再加上用户量最多的 Uniswap 去中心化交易所的推波助澜，使得 DeFi 生态的用户在短时间内迅速的达到了 100 万。



DeFi 不断增长的锁定资金

DeFi 热潮才刚刚开始，从 Compound 开创了借贷挖矿，到其他项目竞相模仿；再到陆续产生了聚合挖矿、流动性挖矿等模式产品，再到 Uniswap 开创了 AMM、无需许可的交易模式，去中心化交易所占领越来越多的交易市场份额。可以预见的到，未来的 DeFi 生态竞争将更加激烈，产品也更加完善。

1.3 预言机介绍

随着 DeFi 生态的崛起，作为 DeFi 领域重要的基础设施--预言机，也迅速发展起来。

预言机是把链下的数据保存到链上，以供区块链上的应用程序使用，基于以太坊的智能合约技术，从而实现了现实世界与区块链世界的数据交互。

目前市场上所有的 DeFi 产品都需要使用预言机，需要预言机提供 Token 的价格数据，才能让 DeFi 产品实现挖矿、借贷、抵押、合成资产等功能。

预言机的代表项目是 ChainLink，这个项目是在 2017 年启动，募资价格是 0.1 美元，经历了 2 年的熊市，迅速发展起来，最高币价达到了 20 美元，产品市值 60 多亿美元，升值 200 多倍，目前在整个 Token 项目中市值排名在第九位，也是 DeFi 领域市值最高的产品。

在这波 DeFi 热潮中，还陆续产生了一些其他的预言机团队，大多是基于 chainlink 产品做些改动，比如：API3、NEST、band 等。

近来随着闪电贷攻击的事件频发，预言机的重要性受到了越来越多的重视，Uniswap、compound、YFI、MakerDAO 等 DeFi 项目团队也开始开发自己的预言机，在通用预言机的基础上，增加一些定制的服务。

目前市场上的预言机团队都是诞生于 DeFi 火爆之前，受到产品设计、技术框架等原因的限制，在扩展性、安全性上无法满足 DeFi 新时代市场需求，综上所述，DeOracle 团队开发了新一代的预言机，满足日益增长的市场需求。

二、预言机的问题

目前市场上的预言机产品主要有 Chainlink、Band、NEST、API3 等，但这些预言机存在一些设计缺陷，无法满足现在的区块链应用程序的需求。

2.1 扩展性差

现有的预言机需要数据提供者喂价，但是数据提供者数量少，最多的预言机数据提供者仅为十几个，预言机很难找到更多合格的数据提供者。

产品架构体系决定了增加一个交易对流程比较繁琐，交易对的数量很难做到大幅度增加，基本不支持新币种、小币种。这很难适应 DeFi 快速庞大的发展需求，目前市场上所有的预言机产品加起来总共支持不到 70 种 Token 的价格，这明显不能满足 DeFi 生态的数量需求。

如果想支持更多的交易对，就需要更改产品的设计架构，这对目前市场上的预言机团队来说，难度太大，成本太高，相当于重构产品，因此基本做不到。

2.2 安全度低

市场上预言机获取价格数据的流程有采集数据、发送数据、聚合数据等几个环节。

采集数据是从中心化交易所获取，而中心化交易所为了私利是有操控、伪造价格数据的可能性。

喂价者发送数据到合约，喂价者并不十分可信，如果利益足够，也会有作恶的可能性。

最近频繁发生的多起闪电贷攻击事件，就是利用了预言机价格的漏洞，造成了产品用户的巨额损失。

2.3 团队中心化

目前的预言机团队大都是公司中心化体系，未获得主权国家的法律许可文件，如果再次发生 SEC 调查，很可能将步瑞波 XRP 后尘。

2.4 审核许可权

市场上的预言机，需要提供某个 Token 项目方的交易对，是需要该项目方官方同意的，如果项目方官方不同意，就无法提供该 Token 项目的交易对，比如：目前的预言机没有提供火币和 okex 的代币（HT、Okb）的价格数据。

除此之外，如果用户想提供预言机需要的价格数据，要经过预言机团队审核同意，如果预言机团队不同意，用户就不能为预言机提供价格数据。

预言机团队凭借自己的主观性，从市场上选择、定义各个 Token 项目方的币是否有价值、Token 项目方名声好不好、Token 项目有没价值，属不属于垃圾币等。预言机团队自主筛选、判断审核是否提供该 Token 项目方币的价格数据，人为设置了准入门槛，把很多 Token 项目方挡在门外，造成某些想用预言机的项目方无法使用。

预言机团队自己是裁判，权力过于集中，判断性过于主观，这并不符合区块链去第三方审核、去权力化、降低门槛的理念。

三、产品介绍

区块链上的 DApp、DeFi 产品（比如：借贷、抵押、生成稳定币等）都需要区块链上的 Token 价格数据。随着区块链上的应用程序越来越多，数据使用的需求将会越来越强烈。

目前市场上主要有 Chainlink、Band、NEST、API3 等几种预言机，与这些预言机相比，DeOracle 具有如下 6 个特点：

3.1 无需许可

Uniswap 开创了无需许可的创新模式，任何人都可以创建任何 Token 的交易对，无需 Uniswap 官方同意，这给了用户极大的自由，各种类型的 Token，无论是否 Token 项目官方同意、“热门币”、“优质币”、小币种、新币都可以上线，也正是这种模式促使 Uniswap 的成功，DeOracle 产品也采用此种模式。

目前市场上预言机的价格提供者都需要官方许可效验的，用户只有通过预言机团队的审核才有资格进行更新价格数据，这样的模式导致不是任何用户都可以提供更新数据，仅有十几个数据提供者为近 70 种 Token 喂价。

做为新一代预言机产品，DeOracle 预言机是无需许可的，任何用户都可以更新任何 Token 的价格数据，不需要经过团队的审核许可，极大的拓宽了预言机的广度和深度，满足了市场的需求。

3.2 交易对种类数量最全

目前市场上所有的预言机产品总共提供不到 70 种 Token 交易对的价格，由于产品设计架构的初衷没有考虑到 DeFi 目前的生态发展，导致产品无法扩充太多 Token 的交易对；并且市场上所有的预言机都需要喂价者提供数据，没有广泛的数据提供者也是这些产品的重大缺陷；除此之外产品更新价格数据是需要向产品团队支付费用，而预言机团队中心化管理，主观性判断，审核同意后才能增加新的交易对数据，导致很多项目方的价格数据无法加入其中。综上所述，市场上预言机产品是无法在短时间内满足 DeFi 生态的需求，DeFi 市场迫切需要一种新的预言机产品。

DeOracle 产品就此孕育而生，一种完全开放给所有用户、所有 Token 项目方任意添加 Token 交易对和更新价格的预言机产品。

不管做为 Token 项目方还是个人用户，完全交由市场行为才是 DeFi 生态发展到现在强大的源泉。用户自主想支持哪个 Token 就添加哪个 Token，不需要与 DeOracle 团队沟通获得审核同意，也只有这样才能支撑得起未来庞大 DeFi 生态的需求。

随着产品的上市，“主流热门”币种，小币种、新币种等，只要在去中心化交易所上有这个 Token 的交易对，全部可以支持。DeOracle 目前已经支持了 Uniswap 的所有 Token 交易对，后续将支持 balancer、sushiswap 等市场上所有的去中心化交易所。

3.3 价格数据可信

目前市场上预言机大部分是把中心化交易所的价格数据发送到到区块链上，让用户使用，这叫数据提供者。然而数据提供者并不是可信的，可能提供错误的、虚假的数据，因此预言机产品的数据不是 100%可信的。

NEST 预言机提出了一种解决方案，是需要用户提供价格数据的同时，提供两种 Token，让套利者验证价格数据的真假，如果数据是恶意作假的，套利者可以直接套利，那么数据提供者将会损失资金，让数据提供者付出代价，保证数据正确。

做为全新一代 DeOracle 预言机产品，使用更加符合区块链理念的解决方案，其数据来源不需要提供者发送价格数据，而是直接从去中心化交易所获取交易的价格数据（比如：Uniswap、balancer 等），去中心化交易所本身就是用户间直接交易，从去中心化交易所获取价格数据，价格数据来源真实、可靠，杜绝了数据造假、数据错误，从根本上解决了数据可信的问题。

市场上所有的预言机都是把数据从链下发送到链上，DeOracle 重新定义了预言机，是把链上的数据整合保存到链上。早期优先满足 DeFi 产品需要价格数据的需求，随着项目的发展，未来将保存更多市场上需求的各种数据（如 Token 的投资回报率等）。

3.4 价格数据透明且安全

市场上的预言机，很容易受到闪电贷的攻击，自从 6 月份以来已经爆发了多起闪电贷攻击案例，套取了 DeFi 产品上的用户资金，给产品、用户带来了巨额损失，更为严重的直接造成了产品失败、用户倾家荡产。

这类闪电贷的攻击是黑客利用了预言机的价格数据只采用当前数据的特点，用大额交易改变了价格，产生了套利行为。

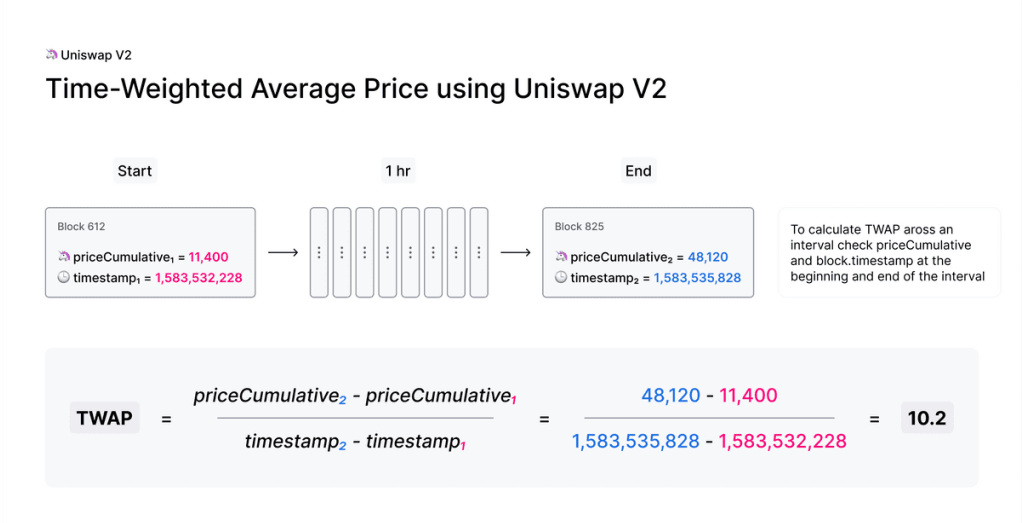
某些预言机产品数据是不透明不公开的，未公布数据来源于哪些交易所，防止黑客攻击。

DeOracle 预言机的数据来源是公开透明的，全部来自去中心化交易所，所有信息都是公开可查，技术上采用了去中心化交易所的 TWAP 价格，不会被黑客操控价格，避免了闪电贷的攻击。

3.5 TWAP 介绍

时间加权平均价格，time-weighted average prices 的简写，基于交易对的价格历史数据，再以时间加权，计算价格。先计算任意时间间隔的价格，两个时间点的价格差，除以时间间隔，就是时间加权平均价格。

时间间隔可以是一个以太坊区块确认时间（约 15 秒），也可以是每小时、每天、每周等，从而可以计算出每个区块、每小时、每天、每周的价格。



如果黑客想攻击影响 TWAP 价格，是需要支付巨额的攻击成本，由于攻击成本过高，黑客将会放弃攻击。这是 Uniswap 交易所设计的防止黑客攻击的技术。

TWAP 价格是按时间段计算的，想让价格波动 5%，需要支付的成本是这段时间内套利损失的费用和手续费之和。因此用这种方式计算价格，黑客是无法通过短暂的操作来影响价格，所以安全可靠，完全避免了闪电贷的攻击。

3.6 价格更新策略

市场上所有预言机产品对 Token 的价格更新策略，是由其预言机团队自主决定，比如某预言机产品 Token 的价格数据是 3 小时更新一次，或 Token 的价格波动超过 0.5%更新，这并不能准确的满足市场上各种用户的定制化需求。

做为全新一代 DeOracle 预言机产品，所有的价格数据是由用户自主决定更新策略，用户可以根据市场动态，自己确定更新时间间隔，或者波动范围大小，甚至可以自己来更新价格数据，从而满足市场上各种用户的个性需求。

3.7 跨链

目前市场上的预言机主要是在以太坊公链开发的，并不支持其他公链。但随着市场的发展，其他公链的生态也在扩大（比如：币安智能链、波卡等），支持其他公链是未来的发展趋势。

DeOracle 将做为首个支持多个公链的预言机产品，将开发自己的节点网络，推出首个预言机公链产品。

3.8 预言机的特点对比

目前市场上预言机主要有 Chainlink、Band、NEST、API3 等几种，这些预言机和 DeOracle 预言机的特征做一些比较，如下图：

	Chainlink	Band	NEST	API3	DeOracle
官方许可	需要	需要	不需要	需要	不需要
交易对数量	约 70 种		50 种+		所有交易对
数据来源	中心化交易所	中心化交易所	中心化交易所	中心化交易所	去中心化交易所
公开透明	不公开不透明	不公开不透明	公开透明	公开透明	公开透明
闪电贷攻击	能防止	能防止	不能防止	不能防止	能防止
更新策略	3 小时或波动 0.5%		用户自己提交		用户自定义
跨链	不能跨链	不能跨链	不能跨链	不能跨链	能跨链
数据提供者	审核通过的企业	审核通过的企业	个人用户	互联网企业	个人用户

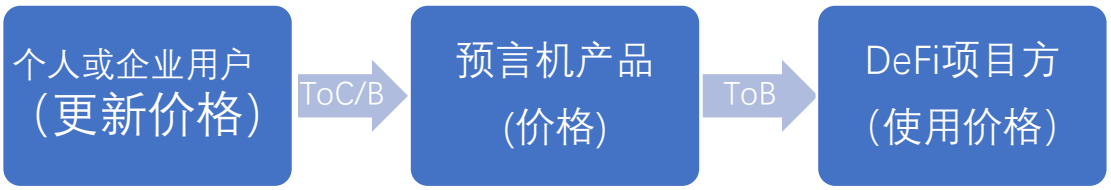
四、产品设计架构

预言机产品的核心是价格数据。因此想让更多的 DeFi 项目方使用 DeOracle 预言机的价格，预言机的价格必须是及时更新，交易对的种类越多越好。

做为全新一代预言机产品，与其他的预言机产品有根本上的差别，市场上其他预言机产品面对的客户全部是 B 端用户，由 B 端客户更新价格，再由 B 端客户来使用更新价格的数据。

DeOracle 的预言机则调整为面向 B 端和 C 端用户相结合共同参与的产品，不仅仅依靠团队来进行数据价格的更新，而是更广泛的让社区中的每个用户参与，让更多的 C 端和 B 端用户来参与其中，也只有这样才能做到 DeFi 项目方使用到的是最及时最更新的市场价格。

整体示意图如下：



4.1 个人用户

个人用户的权利：可以添加任何一个交易对，更新一个对或多个交易对的价格。

更新价格是指把价格数据保存到区块链上，需要发送一笔以太坊交易，这需要付出一定的 gas 费。

DeOracle 产品的用户更新价格同样也需要支付 gas 费，但为了弥补用户支付 gas 费的成本损失，团队将发行预言机的代币 Token，通过代币弥补用户的 gas 费用，激励用户不断更新价格。

用户可以自定义价格更新策略：比如更新价格的时间、更新价格的波动范围等。

为提升用户更新价格的效率，团队将开发去中心化交易所监控工具，提醒用户及时更新价格，提醒用户有新的价格产生再更新价格，没有新的价格则不用反复更新价格。

团队未来将开发自动化工具，用户仅需做简单的配置，就可以实现自动化的更新价格。

4.2 企业用户

区块链上的应用程序可通过 DeOracle 产品获取预言机的价格数据，满足自己项目的应用需求。

企业用户获取数据是收费的，支付方式为产品的 Token，企业用户以 ETH 地址作为付费企业的身份，管理员负责管理付费企业。

获取价格数据是通过智能合约的接口，团队会将所有智能合约的接口代码公布在 github 上，做为 DeFi 生态强有力的基础支持工具，完全符合区块链技术的要求，开源透明，支持所有社区用户查看与审阅代码。

4.3 管理员

DeOracle 预言机的管理员，负责管理产品的商业模式。

对于付费企业会员，管理员可以添加会员，移除会员等，并且根据市场行情来进行调整收费策略，开启、关闭收费模式、折扣模式等。

对于个人用户，管理员可以根据市场行情、gas 费用的成本来调整弥补用户更新价格所支付的成本，以及解决用户的反馈意见。

预言机早期需要管理员进行辅助管理，随着项目的发展，逐步减少和削弱管理员的权限工作，将管理模式进化为社区治理模式 DAO。例如在项目初期管理员来负责管理付费企业会员，随着项目的发展，未来将管理更改为自动化操作，项目方通过合约转账将自动成为付费企业会员，根据转账的金额自动计算付费有效期限，减少管理员的干预，让项目更健康的发展。

五、长期开发计划

5.1 降低 gas 费用

目前市场上的预言机产品都是在以太坊主链上更新价格数据，因此每次更新是需要支付 gas 费用。

根据以太坊主链正常交易时进行的价格测试，更新一次价格，需要 7 美元，如果更新次数频繁，gas 费用将呈倍数增加，所有用户都无法承受。

DeFi 产品同样也面临 gas 费用过高的问题，某些产品会采取发行 Token 的方式来弥补 gas 费的成本，比如 1inch 发行了 Chi GasToken，目的就是用来减少用户的损失。

DeOracle 产品也将推出自己的项目代币，来弥补付出 gas 费用成本的用户，并且在未来推出的新版本中，也会逐渐降低 gas 费用，降低用户更新价格所支付的成本。

5.2 聚合所有的去中心化交易所

DeOracle 预言机产品目前的版本数据来源仅仅支持了 Uniswap，她是 DeFi 领域最大的去中心化交易所，用户超过了 50 万，超过 68000 个唯一地址，为 27000 个唯一交易对提供流动性，同时是 AMM 模式的开创者。

预言机未来将集成更多的去中心化交易所（比如：SushiSwap、Balancer 等），届时将有利于增加更多的交易对种类数量，还能提升价格数据的安全性，避免被操控、被攻击等风险。

5.3 支持以太坊二层的预言机

目前市场上所有的预言机都是基于以太坊主链上的产品，当主链网络拥堵的时候，gas 费用将会变的非常高，交易无法及时确认，这些客观原因都会提高用户的成本，降低产品的体验。

随着主流 DeFi 产品都在开发以太坊的二层版本，DeOracle 团队一直也在跟进以太坊二层技术的发展（Optimisic、matic、OMG 等），预言机也将迅速支持引入以太坊二层的网络技术，通过版本的升级不仅可以大大降低用户的 gas 费用，也会提升速度效率，使得产品的用户体验度提高。

5.4 支持以太坊 2.0 的预言机

以太坊开发团队正在开发以太坊 2.0 版本，未来将采用 POS、分片等技术，提升网络交易处理能力，DeOracle 团队也将开发支持以太坊 2.0 版本的预言机，支持以太坊的新区块链网络。

5.5 跨链预言机

除了比特币、以太坊，其他公链也正在发展壮大，比如：波卡、币安智能链等，团队也将开发支持各种公链的预言机，未来也会推出 DeOracle 预言机的公链。

5.6 期货预言机

DeFi 行业正在尝试做区块链上的期权期货产品，这类产品依然需要预言机提供各种任意时间段的 Token 价格，每隔多少分钟、多少小时、多少天，都可以定制服务，YFI 创始人 andre 的期货产品已经发布测试，未来 DeOracle 预言机同样也会支持期权期货的价格数据的更新。

六、产品治理

随着去中心化交易所 DEX 的兴起（如 Uniswap、balancer 等），Token 价格数据可以直接从去中心化交易所 DEX 里获取，完全取代从中心化交易所 CEX 获取。正是基于这个共识，DeFi 社区一些小伙伴聚集在一起，开发了 DeOracle 预言机产品，实现了这个目标。团队采用的是社区模式，打破传统的公司式管理架构。

产品的治理，最终将采用 DeFi 社区普遍认可的 DAO 模式，让代币持有者更多的参与产品的工作，且能获得更多的利益回报，与产品实现利益共享。

治理模式将写进智能合约，部署在以太坊区块链上，无法随意修改治理模式，让产品增加更多的共识方案。

DAO 治理大致分几个步骤：

6.1 提出议案

拥有 DeOracle 产品代币当前流通数量 1%的持有用户可以提出议案，低于 1%持有用户无法提出议案。

议案可以是对产品的建议、可执行代码等各个方面，团队期望最好的是代码上的提案。

6.2 议案与投票

社区提出的议案，将会由代币持有用户进行投票（赞成、反对），决定是否采用，不持有代币的用户，无法投票。用户可以选择自己进行投票，也可以将自己的投票权委托给他人，代替自己投票。

产品的投票期为 7 天，在投票期间，提案发起用户持有代币数量不能低于 1%，否则产品的提案将被自动取消。

6.3 投票结果

根据社区的投票结果，决定议案是否执行。

若社区投票结果为议案赞成执行，还需要符合另外一个条件，即投赞成票的数量，需要达到当前代币流通数量的 4%以上；如果低于 4%，议案将不会被通过，议案无法执行。

6.4 时间锁

社区投票通过的提案将进入时间锁内，根据议案轻重缓急的程度，判断各个议案的执行时间。普通议案将在 3 天后执行，用户有 3 天的缓冲期，为新议案的执行做准备工作。但是如若发生特别重要的议案，将会立即执行。

七、代币经济

为了 DeOracle 预言机的产品能够长期正常经营，团队将发行产品代币。

代币简写：DOE。鹿驰走，无顾，六马不能望其尘。

团队正是追求将产品做到极致，使其他预言机或者同类产品不能同日而语。

7.1 代币奖励与支付方案

代币将会为推广 DeOracle 预言机生态做出杰出贡献的用户作为奖励；代币将会激励更多的参与者更新价格数据；代币将会鼓励更多的开发者贡献代码；并且持有代币还可以参与治理。

做为使用预言机价格数据的 DeFi 项目方，需要支付产品代币才能获取到 Token 价格数据。项目方支付代币后，自动成为付费成员，且智能合约会根据支付代币的数量，自动计算付费会员的有效日期，整个过程无需管理员参与许可。

预言机代币是符合 ERC20 标准的 Token,凡是目前市场上支持 ERC20 的产品都能兼容支持预言机代币。

7.2 代币分配方案

预言机的代币总量 10 亿枚，前 4 年逐月释放，4 年内不增发，4 年后每年增发 2%。为了能让持币者收益提升，团队也将采用流量挖矿、锁仓激励等多种组合方式来提高 DOE 收益的增值服务，具体方案的详细细节，将会在官网进行详细说明。

具体分配方案：

(1) 团队持有 20%，共计 2 亿枚，分 4 年逐月解锁。

1）第一年解锁 0.8 亿枚

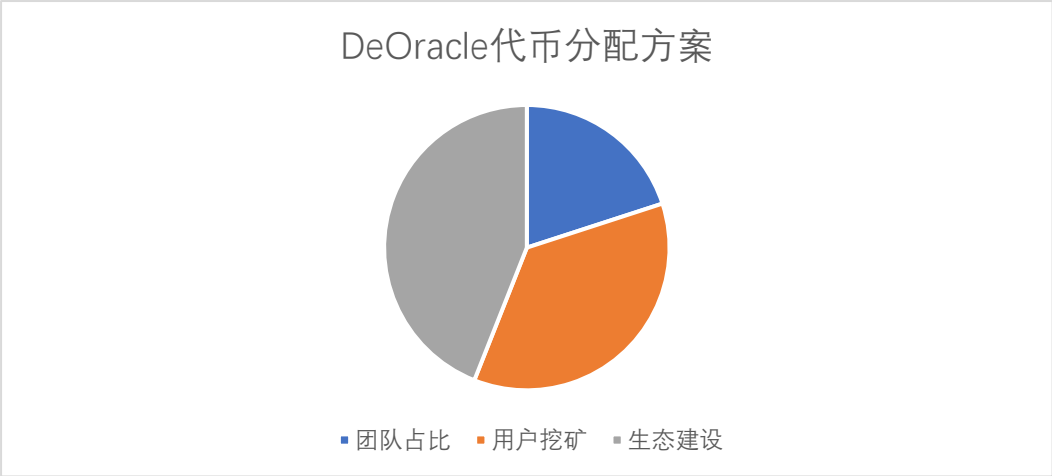
2）第二年解锁 0.6 亿枚

3）第三年解锁 0.4 亿枚

4）第四年解锁 0.2 亿枚

(2) 用户挖矿 36%，共计 3.6 亿枚，激励用户更新价格，每天释放 2 万枚，分 50 年挖完。

（3） 社区生态建设 44%，共计 4.4 亿枚，用于激励开源社区、生态扩展等。



目前市场上预言机主要有 Chainlink、Band、NEST、API3，与这些项目的代币做比较，如下图：

	Chainlink	Band	NEST	API3	DeOracle
总量	10 亿枚	1 亿枚	100 亿枚	1 亿枚	10 亿枚
ICO 价格	0.1 美元			0.3 美元	
单价	20 美元	10 美元	0.02 美元	2 美元	
市值	65 亿美元	1.7 亿美元	5000 万美元	5000 万美元	
发布日期	2017.9.21	2019.9.19	2018.12.19	2020.11.30	

数据来自 coinmaketcap

参考文献

[1] Satoshi Nakamoto 比特币白皮书 https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin 以太坊白皮书 https://ethereum.org/en/whitepaper

[3] ChainLink 白皮书 https://link.smartcontract.com/whitepaper

[4] Band Protocol 白皮书 https://docs.bandchain.org/whitepaper

[5] NEST protocol 白皮书 https://nestprotocol.org/doc/ennestwhitepaper.pdf

[6] API3 白皮书 https://raw.githubusercontent.com/api3dao/api3-whitepaper/master/api3-whitepaper.pdf

[7] Hayden Adams Uniswap V2 Core 白皮书 https://Uniswap.org/whitepaper.pdf

[8] SushiSwap Project https://sushiswapchef.medium.com/the-sushiswap-project-dd6eb80c6ba2

[9] Andre Cronje Deriswap: Capital efficient swaps, futures, options, and loans https://andrecronje.medium.com/deriswap-capital-efficient-swaps-futures-options-and-loans-ea424b24a41c

[10] Andre Cronje Keep3r Network: On-chain Oracle price feeds https://andrecronje.medium.com/keep3r-network-on-chain-oracle-price-feeds-3c67ed002a9

[11] AAVE 闪电贷 https://docs.aave.com/developers/guides/flash-loans

[12] Andre Cronje Uniquote, Unihedge, and UniswapV2Oracle https://andrecronje.medium.com/uniquote-unihedge-and-Uniswapv2oracle-f120838aabb8

[13] Uniswap oracle TWAP 介绍 https://Uniswap.org/docs/v2/core-concepts/oracles

[14] 1inch introduces Chi GasToken https://1inch-exchange.medium.com/1inch-introduces-chi-gasToken-d0bd5bb0f92b

[15] 币安智能链 https://www.binance.org/en/smartChain

[16] Gavin Wood 波卡网络 https://polkadot.network/PolkaDotPaper.pdf

[17] CoinMarketCap https://coinmarketcap.com

[18] DeFipulse https://www.DeFipulse.com

[19] Dune Analytics https://duneanalytics.com

[20] Compound 治理 https://medium.com/compound-finance/compound-governance-5531f524cf68

[21] Compound 代币 https://compound.finance/governance/comp

[22] Uniswap 治理 https://Uniswap.org/docs/v2/governance/governance-reference

[23] Uniswap 代币 https://Uniswap.org/blog/uni