Difirst Protocol – 白皮书

Difirst 基金会

2020.7

概述

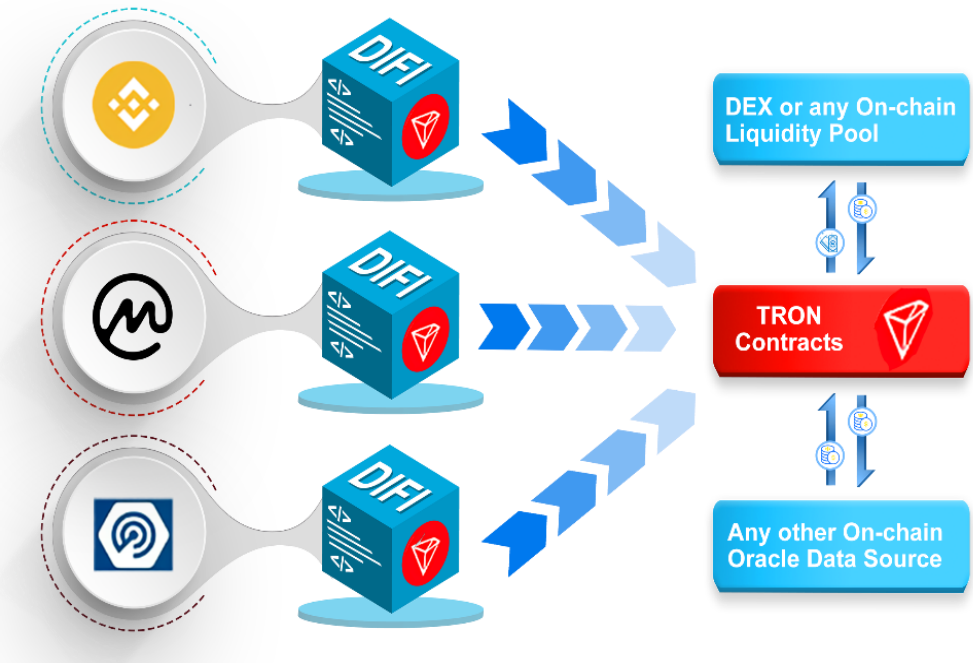
Difirst Protocol 是第一个基于 TRON 公链的去中心化预言机网络。Difirst Protocol 通过搭建一个人人皆可参与、验证报价、交易的网络协议，为 TRON 生态的 DEFI 应用提供去中心化的数据获得方式。对于包括 DEX（去中心化交易所）在内的大多数 DEFI 产品，都是采用基于哈希时间锁定合约（HTLC）的原子互换协议实现交易和清算，从而无差别地在点对点环境下完成数字货币的交割。一旦数据提供方利用中心化的方式存在潜在作恶机会，所有的 DEFI 产品都面临着系统性风险。

一、预言机定义

在互联网世界里，定义预言机的方式随着物理环境、网络环境的不同而有所差别。在区块链环境中，我们将预言机理解成从数据源抓取数据并上传的工具，以用作智能合约和其他外部数据源之间的桥梁。

更具体地说，预言机是一种代理组织，它不仅负责与外部数据源进行通信，并且验证所提供的数据是否准确。因此，在区块链世界里，预言机负责向智能合约提供重要而可靠的信息，而帮助智能合约执行某些任务。

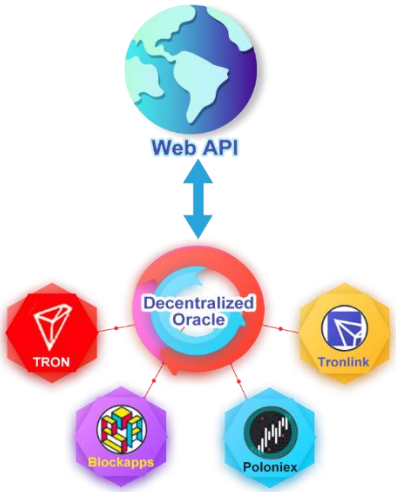
预言机的重要性取决于以下事实：区块链智能合约只能访问其自身数字网络中包含的数据。因此，需要使用预言机作为一种通信工具，将现实世界的事件（非确定性数据）“转换”为智能合约可以识别的数字和信息（确定性数据）。



可以根据具体应用场景对区块链预言机进行分类。常见的类型有：
硬件预言机：实现物理系统与技术相集成，为智能合约提供真实数据。例如，硬件预言机可以与各种行业（汽车，制药，供应链等）中使用的 RFID 传感器进行通信。
软件预言机：最常用的一种。从外部程序和 Web API 检索在线数据，例如市场价格，航班状态和天气数据等。
共识型预言机：一种去中心化的预言机系统，遵循特定的方法来确定所收集数据的有效性和准确性。这些去中心化的预言机从其他数据源甚至是其他预言机中收集大量数据。共识型预言机已被用于预测市场，例如 Augur 和 Gnosis。
输入型预言机：将外部数据传输到智能合约或软件预言机。可以配置为一组满足“如果”准则的条件命令（例如“如果某资产达到特定价格，则下达买单”）。
输出型预言机：将智能合约数据传输到外部系统，从而使智能合约可以与非区块链数据源进行通信。
通常，区块链预言机从第三方数据源调用数据，该第三方数据源依赖于外部权限才能正常工作，这意味着它们通常是中心化实体提供的工具。因此，大多数预言机最终牺牲了智能合约的去中心化属性。

二、去中心化预言机

对于公链上的智能合约而言有一个重要的限制，即它们仅对区块链上的数据进行操作。因此作为外部数据传输者的预言机必须严格受信任从而提供的强大安全性保证。但随着链上资产和价值的提升，中心化预言机的操纵方有更大的经济激励来作恶。
因此，一个去中心化的预言机系统是必要的。去中心化预言机的设计思想和公链的设计思想一致，即在不控制准入条件的情况下，通过合理的经济激励模型，并增加、分散提供数据的节点，从而通过竞争留下正确的数据，剔除错误的数据，增强整个预言机系统的容错能力。
由于去中心化预言机涉及的每个单个节点都无法证明是可信的，因此在整个系统搭建时我们需要关注以下几点 ：
（1）数据内容的私密性。这一点不同于零知识证明等常见解决方案，节点调用并向预言机传输数据时有所局限，
（2）数据获取的即时性。考虑到不同节点间“数据竞争”的每个周期都需要时间验证或证伪，因此数据获取的时间周期制定需要仔细论证。
（3）女巫攻击引发数据腐败。考虑到数据提供方可以创造多个节点，因此向预言机提供数据的节点需要准入门槛。
（4）节点恶意复制其他节点数据问题。除了应用技术手段对上传数据的节点进行保护外，还需要设置合理的竞争机制保证上传数据的节点相对于恶意复制数据的节点有优势或优先权。



三、Difirst 预言机的解决方案

1、Difirst 预言机是什么

简单来说，Difirst 是一个面向加密数字货币的价格预言机。不同加密数字货币之间的价格问题几乎是所有加密数字货币用户最关心的问题，不同于法币（USDT，DAI）等的价值波动，加密数字货币之间的价格波动几乎完全由交易意愿或者说供需关系决定。虽然有中心化交易所及去中心化交易所的存在，但是其中的成交规模、信息不对称性以及中心化特性都不能完美的反映加密数字货币之间的价格变化。Difirst 提出了一种全新的思路，将加密数字货币的价格作为核心要素，通过捕获用户的交易意愿在链上形成不同加密数字货币之间的价格，即预言机。

2、Difirst Protocol 的价格形成机制

为了形成不同加密数字货币之间的价格，多个不同的 Difirst 用户需要在 Difirst 智能合约中给出自己所认可的价格，如果这些用户给出的价格是理性的，那么综合足够多的用户提出的价格所得出的最终价格，就是合理的。更进一步的，可以通过合理的机制设计保证用户的理性，即，当用户给出的价格是非理性的时候（偏离实际的市场价），那么用户的收益是负的；而当用户给出的价格是理性的时候（符合实际的市场价），那么用户的收益是正的。Difirst 引入了 Difirst Token（代币名 DIFI）以激励用户价格的理性行为。

下面我们给出 DIFI 的价格形成机制，假设两个加密数字货币 M，N，其价格表示为一个二元组 (m, n)，即 m 个加密数字货币 M 等价于 n 个加密数字货币 N，不同的二元组可能表示相同的价格，例如(m, n), (2m, 2n), (3m, 3n)... 表示的价格是相同的。

我们给出 DIFI 持币用户的两种行为：

- 报价：用户 a 通过将 Ma 个 M 以及 Na 个 N 存入 DIFI 智能合约的方式出示自己认可的价格（Ma, Na)；
- 吃单：用户通过向智能合约存入 M 或 N，以指定的价格换取 N 或 M，需要的注意的是，吃单时指定的价格必须是 Difirst 系统中已经存在的报价；当进行吃单时，用户需要给出新的价格，即进行新的报价行为，新的报价行为的数量至少为吃单数量的\alpha 倍，我们称\alpha 为**吃报系数**。

DIFI 的价格形成机制按照周期进行，每个周期可以描述为如下的有限状态机：

初始状态：此时系统中没有形成有效的价格，在这种状态下，任意用户可以进行报价，系统进入有价状态；任意用户可以取回上个周期未被吃单的加密数字货币。

- 有价状态：系统中存在一个或多个报价行为，此时有两种情况，1）系统接受到了新的报价行为，此时系统仍然为有价状态；2）系统接受到了吃单行为，当所有的报价都被吃单完成时，系统进入初始状态；否则，系统仍为有价状态。
- 结算状态：当系统达到一段时间后，系统进入结算状态，增发一定数量的 DIFI，当系统是由初始状态进入结算状态时，系统增发的 token 进入下一个周期；当系统由有价状态进入结算状态时，系统按照未被吃单的所有的报价平均得到周期内的价格，增发的 token 发送给矿工。系统进入下一个周期的初始状态。

下面我们给出更详细的参数，以 TRX、USDT 为例

- 报价：TRX 的数量不能低于 100,000TRX，或者 USDT 的数量不能低于 2000USDT，报价时收取 TRX 规模的 0.5%作为手续费；当本次报价偏离上次报价超过 10%时，本次报价的规模不能低于上次报价的 10 倍。
- 系统周期为 100 个区块（大约 5 分钟）
- 吃单行为：吃单数量为 X*100,000TRX，其中 X 为任意整数；当进行吃单时，系统收取 1.5%TRX 作为吃单手续费；吃报系数\alpha 取值为 2。

不难注意到，上述价格形成机制在没有 DIFI 的情况下，存在一定的非理性行为。为此，我们进一步引入 DIFI。

3、Difirst Token（DIFI） 挖矿释放规则：

1）DIFI 总量为 52.5 亿。
2）DIFI 预挖 2.5 亿，为基金会所有，用于市场运营，早期资金募集，包括 IEO 等
3）矿池产出起始区块为波场的第 22811888 块，起始每个区块产出 DIFI 为 62.5；
4）每隔 800000 个区块(约为 4 周)衰减一次, 新周期每个区块的 DIFI 产出是原周期的 99%；
5）第一年挖矿产出约为 12.5%，大约在 2090 年，挖矿不再产出。

DIFI 区块奖励明细

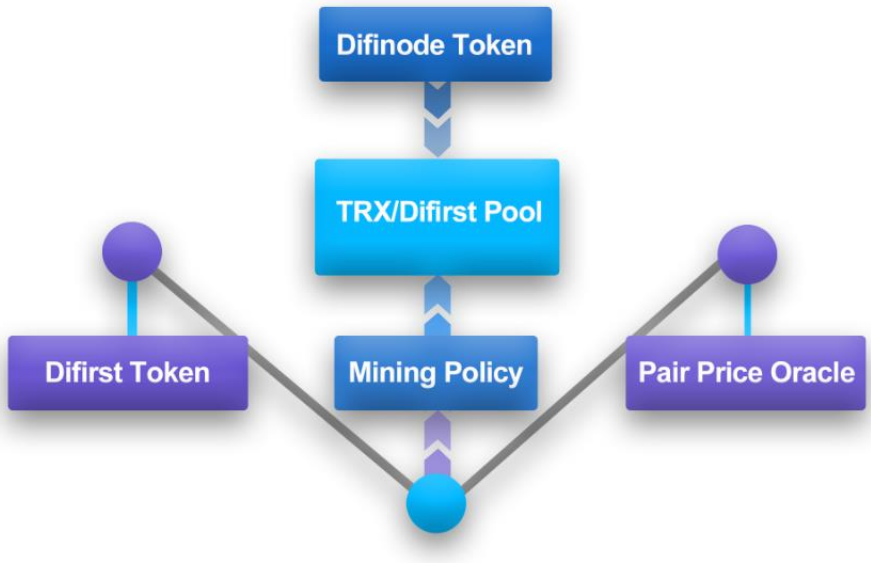
TRON 区块高度	时间跨度	单个区块奖励/DIFI
22811888——23611888	第 1-28 天	62.5
23611888——24411888	第 29-56 天	62.5*99%
24411888——25211888	第 56-84 天	62.5*99%*99%
25211888——26011888	第 85-112 天	62.5*99%*99%*99%
26011888——26811888	第 113-140 天	62.5*99%*99%*99%*99%
如上，以此类推。 注：此处时间标准指的是以 DIFI 开始挖矿的起始区块 22811888 产生时，为第一天。TRON 的区块产出时间平均为 3 秒。		

每次 DIFI 出矿分配:
A．报价矿工： 80%
B．超级节点：18%
C．Difirst 技术团队：2%

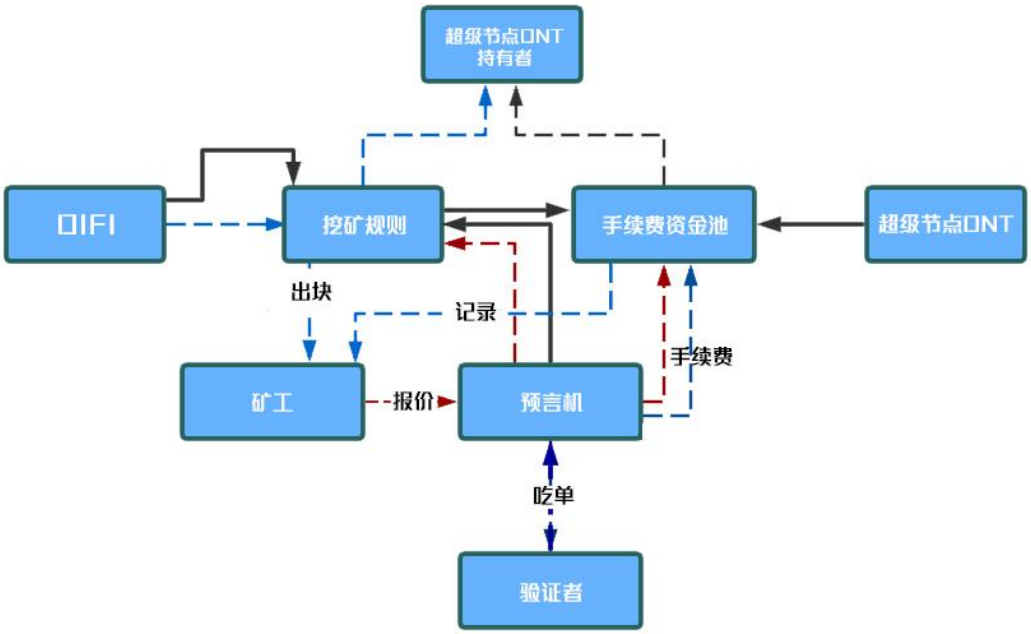
4、报价挖矿：

为了规避系统中的非理性行为，我们引入报价挖矿，即通过激励 DIFI 的方式激励报价行为，从而维护 Difirst 预言机的有效性。
假设该区块中报价手续费之和是 T，其中某一笔报价付出的手续费是 t，那么该笔报价的 DIFI 挖矿数量为 N:
N = （t / T）* M
其中 M 为累计的 DIFI 挖矿奖励。

5、智能合约架构：



如上图所示，为 Difirst 协议的智能合约框架。其中 Difirst Token、Difinode Token（详见下文治理模块）合约为 TRC-20 合约；Pair Price Oracle 合约为报价-吃单合约，用于接收报价吃单，并存放用户报价时质押的代币；Mining Policy 用于执行实际的挖矿逻辑，并进行手续费的计算；TRX/Difirst Pool 存放挖矿、吃单过程中产生的手续费，并进行相应的分发。



上图表示了矿工进行报价、以及验证者进行吃单的合约调用过程，以及出块时从 Difirst Token 合约进行铸币以及分发收益的过程。

四、 Difirst Token 代币经济模型

1、Difirst Token 介绍

DIFI（Difirst Token）是去中心化协议 Difirst Protocol 基于波场网络发行的 TRC20 Token。Difirst Token 最大量上限为 52.5 亿枚。其中 50 亿通过 Difirst 预言机【报价挖矿】的方式进行释放，2.5 亿为基金会预留，用于市场和运营之用，包括早期资金募集，IEO 等。

Difirst Token 合约地址：有待确定

挖矿分配机制：

- 报价矿工：指参与 Difirst 预言机报价的矿工；
- Difirst 技术团队：指 Difirst Protocol 开发团队；
- 超级节点：指 Difinode 持有者，他们是 Difirst Protocol 的早期投资者和支持者。
- 对于超级节点而言，初始 600 美金为一个节点，一共 2100 个。若 DIFI 上线前节点未完全认购完成，即使 DIFI 已在二级市场流通，社区节点依旧可以继续认购，认购价格根据 DIFI 在二级市场上的价格依照一定算法自动进行动态调整。总共 9 亿代币，初始价格 0.1 美分。
- 假设这一笔报价 DIFI 挖矿数量是 100 枚，那么报价矿工得 80 枚，Difirst 技术团队得 2 枚，超级节点得 18 枚。

2、 Difinode Token 介绍

（1）Difinode Token 是 Difirst 治理方案的权益代币，是 DAO（去中心化治理方式）在 TRON 生

态的延伸，代币名简称为 DNT。Difinode Token 代表着 Difirst 生态超级节点的符号，是权利和义务相统一的权益代币。

（2）同时，DNT 也具有流通性，分为一级市场和二级市场。在一级市场，即首次发行市场，由 Difirst Protocol 基金会授予满足条件的超级节点。未来超级节点可以通过 P2P 的方式将 DNT 转出给其他用户，或者在 Difirst Protocol 公开拍卖市场进行交易，即二级市场。

（3）DNT 总量为 2100 枚。每个超级节点母节点拥有 1 枚。DNT 也是一种基于波场 TRC20 协议发行的 Token。其数量精度为 0.0001，即，最多有 2100 万个子节点。

（4）DNT 转出后即视为对 Difinode 权益的放弃，其权益主要为以下两点：

1）Difirst Token 收益权：超级节点不会提前拥有 Difirst Token，而是在报价矿工的挖矿环节和其他矿工同步获得 Difirst Token 释放。Difirst Token 通过报价挖矿释放的部分共有 50 亿代币，其中 80%为矿工所有，18%为超级节点所有，2%为技术团队所有。这意味着，在报价矿工的挖矿过程中，每释放 100 枚 Difirst Token，就有 18 枚分配给了超级节点。

2）Difirst Protocol 治理权：DNT 持有人拥有 Difirst Protocol 大小事务和事件发生的治理权（包括但不仅限于发起投票权和执行投票权）。

（5）关于 DNT 治理机制和发起、执行投票的详细步骤，将会在下文详细展开。

DifiNode Token 合约地址：有待确定

3、Difirst Token 持有人收益分配机制

系统收益来源

1）报价矿工挖矿过程中付出的手续费：报价 TRX 规模的 0.5%

2）验证者吃单手续费：验证者在吃单时，需要向系统支付吃单 TRX 数量 0.1% 的手续费

3）TRX/USDT 价格预言机被下游 DEFI 调用所产生的收益：当有 DeFi 产品调用 Difirst 预言机价格数据时，需要向 Difirst 系统支付一定数额的 TRX 费用，该部分收入 50% 进入系统收益池。（注：另外 50% 奖励给报价矿工）

- 用户收益分配方案：

Difirst 系统收益合约根据每位用户锁仓 Difirst Token 的占比来计算与之对应的 TRX 收益数量，每周六纽约时间上午 8 点分配一次。只有在上周六纽约时间上午 8 点至本周六纽约时间上午 7 点 59 分锁仓的 Difirst Token 才能参与 TRX 分配。

- 系统收益获取方式：个人主动领取
- Difirst Token 锁仓：Difirst 收益合约主要用来在系统收益领取期间统计 Difirst Token 持仓量，锁仓 Difirst Token 的数量用来计算领取系统收益时的持仓占比和可领取系统收益 TRX 的数量。
- 其中本期可领取收益为：

个人可领取收益 = （个人已锁仓 Difirst Token 数量/ Difirst Token 总流通量） * 本期系统可分配收益

- Difirst Token 可锁仓时间：纽约时间 周一 00:00 至 周五 23:59 ，所以要想拿到上周六到这周六的分红，需要在上周五 23:59 之前就开始锁仓。
- Difirst Token 可取出时间：任意时间
- TRX 收益领取时间：纽约时间周六 10:00 至 周日 23:59
- 最终解释权以官网说明为准