ORACLE CHAIN

欧链技术白皮书

ORACLECHAIN TECHNICAL WHITE PAPER

目录

摘要

OracleChain（欧链）作为全球第一个在 EOS 生态圈上构筑的应用，将直面该生态的 Oracle（预言机）需求，将区块链技术服务和现实生活中的多种需求场景直接高效对接，深耕这个百亿美金估值的巨大市场。作为一个基于 EOS 平台的去中心化的 Oracle 技术平台，我们采用自主的 PoRD 机制，将现实世界数据引入区块链，并将此作为基础设施为其他区块链应用提供服务。除了在区块链上提供现实世界数据的 Oracle 服务，同时还可以提供跨链数据的 Oracle 服务。基于 OracleChain 除了能实现 Augur、Gnosis 等预测市场（Prediction Market）应用的功能之外，还能支撑对链外数据有更高频率访问需求的智能合约业务，比如智能投顾等场景。OracleChain 将改变当前区块链应用的开发模式，建立全新的生态圈，培育并服务真正能改变现实世界的区块链应用。我们的使命是“让世界与区块链互联”，立志成为链接现实世界与区块链世界的基础设施，通过把外部数据引入区块链来实现链内链外的数据互通，打造未来区块链世界中最高效的获取链外数据的服务提供平台。

第一章、 OracleChain 设计理念

1.1 行业背景

区块链上的应用场景按照链内与链外信息是否存在交互，大体可以分为两类。第一种类似比特币这样单一货币系统，系统功能主要是支撑货币在链内的流通，这样整个业务流程只需存在于区块链之内，无需与链外信息的进行交互。目前大

部分的公有链项目都属于这类应用，局限于自己的数据闭环机制，参与方只在这条区块链上生成数据、消费数据。但在区块链技术尤其是智能合约技术发展过程中我们发现，很多应用需要进行链内链外数据的交互，这就形成了对链外数据有依赖的第二类应用场景。

以金融领域为例，把金融合约实现为区块链上的智能合约，合约状态的判断不可避免需要使用到链外金融系统里的信息。这种链外业务流程和链内智能合约相结合的模式，需要一个实现链内链外数据打通的渠道。对于立志服务现实世界的区块链应用，必须获取链外数据，才能触发智能合约的逻辑判断。属于此类的区块链应用包括去中心化交易市场系统、去中心化的保险系统、各种预测市场系统、航班晚点的即时赔偿系统等。这些都需要使用 Oracle 预言机来获得链外真实数据以执行智能合约。

如果说 EOS 平台为高效的区块链提供了一种可能，那么 OracleChain 就是在这种基础上再造出一双翅膀，通过为区块链应用提供链外数据来跨越现实世界与区块链世界之间的数据鸿沟，打破不同区块链应用之间的数据隔阂，使得区块链社会变得更有活力，并产生更多丰富的可能性。

1.2 创新之处

A. 基于 EOS 区块链平台

EOS 区块链平台是基于经过普遍证实、并通过长期实践考验的概念来设计的，代表着区块链技术的根本性进步。EOS 区块链平台的目标是能做到支持百万级别用户、免费使用、轻松升级和 Bug 恢复、低延迟以及良好的串行性能和并行性能的结合。借助于 EOS 的优良特性，OracleChain 可以做到高吞吐率和高效地处理

预言机请求，为区块链应用提供高处理能力和低延迟的数据服务，使得诸如智能投顾等金融性应用成为可能。

B. 参与者激励及 OCT 的闭环

OracleChain 将使用一个有效的奖惩机制，旨在鼓励数据源节点（data feeder）提供有效的 data feed 服务，所有正常参与 data feed 的节点都将会得到声誉提升，同时获得 OracleChain 的代币 OCT（Oracle Chain Token），反之，非正常的数据源节点会同时失去声誉和抵押给 OracleChain 平台的 OCT 风险金。通过这种我们称之为 Proof-of-Reputation&Deposit(PoRD) 的双效机制，OracleChain 将有效抵御怀有敌意的数据源节点通过恶意 data feed，影响 Oracle 的实际结果。而用户需要支付 OCT 来获得 Oracle 服务，从此实现 OCT 在 OracleChain 上的闭环流动。

C.世界的桥梁

OracleChain 将数据作为连接世界的桥梁，彻底打破了目前现实世界、区块链应用之间的数据鸿沟，实现现实世界、区块链世界数据的互联互通，促进区块链生态圈的整体繁荣。

D.更科学的数据观

OracleChain 在区块链领域提出了数据的价值概念，以收费的方式向区块链应用提供数据服务，体现数据的价值。

1.3 使命陈述

我们的使命是“让世界与区块链互联”。基于性能优越的区块链底层平台 EOS，OracleChain 把自身定位为链内链外数据打通服务平台，为大规模商用级别的区块链应用提供公共的数据服务。虽然 EOS 项目还在初期，但已经吸引到区块链行

业的大量关注。OracleChain 计划积极参与生态圈建设，建设好数据打通这一公共服务，并以此为基础促进更多应用的落地，实现生态圈的共同繁荣。

OracleChain 的核心目标是成为链接现实世界与区块链世界的基础设施，通过把外部数据引入区块链来实现链内链外的数据互通，打造未来区块链世界中最高效的获取链外数据的服务提供平台。

第二章、 OracleChain 技术架构

2.1 平台模型

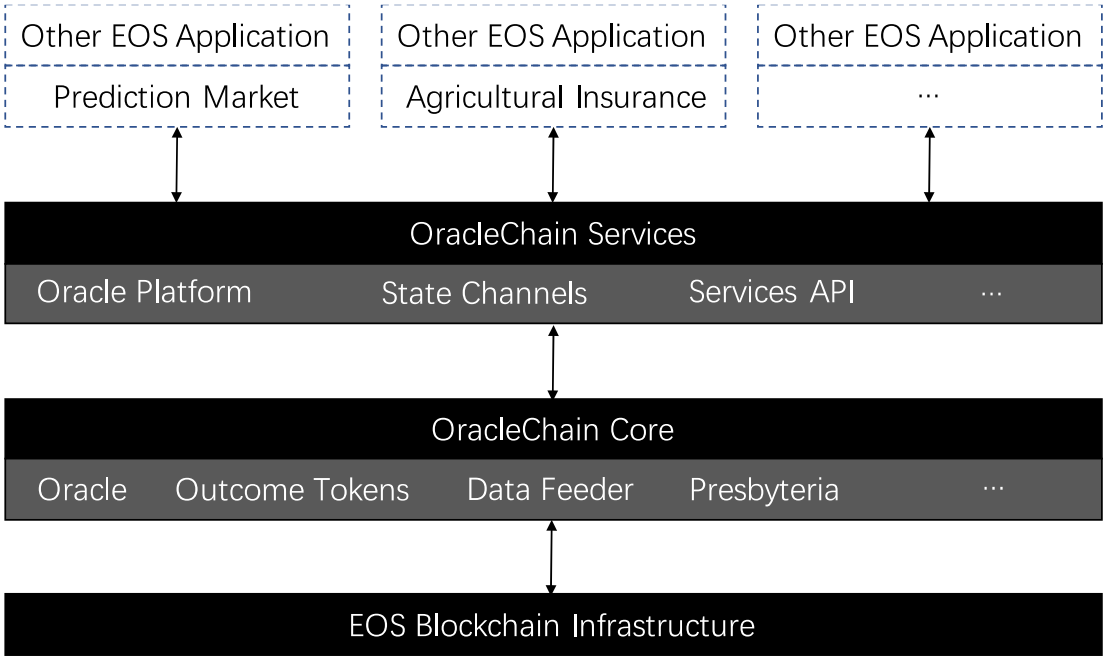

图 2.1 OracleChain 平台模型

OracleChain 平台主要由两个层次组成：核心层和服务层。核心层基于 EOS 框架搭建 OracleChain 的基础服务和运作机制，服务层则在核心层的基础上将 Oracle 平台包装成 API 接口对外提供 Oracle 服务。

核心层

OracleChain 核心层提供 Oracle 实例的创建，实例数据输出令牌的管理，Data Feeder 节点的管理等基础服务。在这一层，OracleChain 实现了对 Oracle 实例和 Data Feeder 节点的管理。Data Feeder 节点将根据 Oracle 的需求读取数据并和其他 Data Feeder 节点共同完成此 Oracle 答案。特别的，OracleChain 引入了声望（Reputation）的奖惩机制、风险金（Deposit）的惩罚机制和 Oracle 费用的奖励机制来完成 data feed 过程，最终回答 Oracle 答案。

Data Feeder 节点通过相互协作来完成一次 Oracle 并共享此次收益，并能通过自组织的方式发现那些异常的 Data Feeder，并触发惩罚机制。同时举报者可以举报 Data Feeder 节点那些不易被发现的不诚实行为。

为了防止恶意的 Data Feeder 节点组织（不会自我惩罚组织成员）和恶意的举报者，OracleChain 特别设置了长老会（Presbyteria）机制，由全网声望最高的 Data Feeder 节点组成最终裁判团，对恶意 data feed 和举报行为进行裁决，并触发惩罚机制。

服务层

OracleChain 服务层提供 Oracle 实例平台、状态通道和服务 API 等对外服务。在这一层，OracleChain 实现了对 Oracle 服务的撮合、计费等对外服务，真正实现了 OracleChain 的基础设施能力。

Oracle 平台将会撮合 Oracle 需求方和 Data Feeder 组织。Data Feeder 组织有可能是松散的临时团体，也可能是提供专业服务的组织。每一个 Oracle 实例里面会申明该实例的费用，需要的 Data Feeder 组织方式以及参与门槛，例如需要 100 个高声望的 Data Feeder 并在其中 80 个节点达成共识的情况下完成 data feed。Services API 将被设计得更加通用，既符合 EOS 跨链的设计理念，也符合便捷开

发的使用需求。

在 OracleChain 的平台模型上，任何的 EOS 应用都可以使用 Oracle 服务。无论是高频次的预测市场，还是低频次的农业保险，都可以借助 OracleChain 的服务变成可能，真正将区块链技术服务于现实生活中。

2.2 data feed 机制

在传统的集中式系统中，数据通常直接从数据源（Data Source）以数据输入（Data Input）的方式获得。这个数据源既可能是来自于集中式系统内部，也可能来自于第三方，系统的运行信任且依赖于数据源所输入的数据。此时数据源是作为一个正直、不带偏见、永不犯错的法官一样的角色，因为或者这个数据源是系统内部可以严密控制的模块，或者是由绝对可信的第三方来担任，系统在数据源的驱动下实现有效运转。

回到去中心化的区块链环境下，这个简单的问题变得非常复杂，会引发诸多问题，比如“谁有资格得到区块链上的所有人的信任担当这个信息源？”、“谁有资格来判断参与者是否可信？”等等。而且信任的可持续性也存在着问题，一个之前持续遵守规则的参与者在逐步累积信用，从而获得较大权力后其实也存在着作恶的可能。

为了解决区块链在去中心化的大背景下完成数据采集和取信的过程，OracleChain 提出了一种 data feed 机制。这种机制将使用一个有效的奖惩手段，旨在鼓励数据源节点（Data Feeder）提供有效的 data feed 服务，所有正常参与 data feed 的节点都将会得到声望提升，同时获得 OracleChain 的代币 OCT（Oracle Chain Token），反之，非正常的数据源节点会同时失去声望和抵押给 OracleChain

平台的 OCT 风险金。通过这种我们称之为 Proof-of-Reputation&Deposit(PoRD) 的双效机制，OracleChain 将有效抵御怀有敌意的数据源节点通过恶意 data feed，影响 Oracle 的实际结果。而用户需要支付 OCT 来获得 Oracle 服务，从此实现 OCT 在 OracleChain 上的闭环流动。

在 PoRD 机制中，每个 Oracle 实例对应一个智能合约。对每个 Oracle 实例，会存在一个声望（Reputation）和保证金（Deposit）的阈值，OracleChain 区块链网络的活动节点只有声望和保证金超过这一阈值，才能参与该 Oracle 实例的 data feed 服务。然后当指定条件触发 Oracle 实例进入结算阶段时，Oracle 实例所对应的智能合约会依据其处理逻辑和参数设置，评判出善意的 data feed 和恶意的 data feed，对善意 data feed 节点提供声望提升和 OCT 代币奖励，对恶意 data feed 节点进行声望减值和 OCT 保证金扣除，以该双效机制保证整个体系的 data feed 工作可以正常运行。

2.3 技术优势

OracleChain 平台具有四大技术优势，分别是高效、兼容、参与和便利。

高效

借助于基层区块链基础设施的对区块数据的细粒度控制和良好的并行处理优化，通过 OracleChain 的架构可支持秒级的确认时间和强大的事务处理吞吐率。

兼容

基于基层区块链基础设施的的跨链机制，OracleChain 可以面向整个 EOS 生态圈提供数据服务，实现链内链外数据转移和互通。

参与

用户可以通过data feed参与全球范围内的Oracle共识体系和OCT生态运转。独特的治理策略可以促使节点遵守社区规则，并利用 PoRD 双效机制保证OracleChain 的正常运行。

便利

OracleChain 提供更高效实用的 Service API，方便其他区块链应用来使用Oracle 服务。

第三章、 OracleChain 治理架构

基于区块链系统的治理一直是一个比较困难的问题。每当需要升级系统时，都需要实施硬分叉,这通常会导致所有区块链利益关联方之间的大量争论和博弈。即使是像修改源代码中任意设定的变量这样简单的事情,由于没有明确的升级路径，比如在比特币社区对区块大小和隔离见证机制的争论不决。尤其在最终使用用户和决策决定者的利益并不一致的情况下,要达成这样的一致会变得更加困难。事实上也存在着一些更为复杂的治理决策，比如在“The DAO”中修复单一的智能合约错误，这甚至会导致更大的问题，引起社区的分裂。

引起这些问题的最大原因是协议升级或更改的决策过程定义不够明确，缺乏透明度。为解决这一问题，OracleChain 把其自身的管理作为其整体共识的一部分。它使用 OracleChain 自身提供的 Oracle 机制尽可能让争议和协商的过程有效和透明地运作。此外，OracleChain 的共识机制可以由多个变量来定义，这些变量决定了系统的功能，或者对系统某个参数的调整，比如使用 Oracle 服务的基础成本等等。

OracleChain 对社区治理的一个基本认识是治理的策略是将权力交给 OracleChain 网络上的高声望节点（用户）。也就是不同重要程度的治理活动需要节点达到不同的声望级别才能参与,即用户会根据不同的声望级别对 OracleChain 实施不同的影响。对于最高阶的节点，可能被授予有限的和被监督的权限来冻结帐户，更新有缺陷的应用程序，甚至提出对底层协议的变更。

通过把待协商的变量设置为 Oracle 并在全社区分级别进行投票协商，OracleChain 用户也可以学习如何有效地改进协议。OracleChain 的治理策略，可以促使节点遵守社区的 data feed 规则，尽可能保证维持更高的声望值，以保持对社区治理更大的话语权。通过对潜在的难题进行构建 Oracle 实例进行运行，我们可以帮助社区就选择哪个版本代码进行使用达成一致。每个用户会为自己选择寻求优化的度量，但是简单的默认策略将是最大化其持有价值，众多用户借由每个用户的理智决策会为整个 OracleChain 社区提供正确的演进方向。

第四章、 OracleChain 实施及迭代

4.1 发展路线图

OracleChain 于 2017 年 6 月正式启动中国路演以及项目 ICO。在 ICO 期间同步启动项目的研发计划，并预计在年底上线第一个 Demo 系统。同时在 2018 年 6 月上线第一个预测市场 demo 系统，并在当年底正式上线预测市场。在整个项目研发过程中，OracleChain 团队会紧密追踪 EOS 项目的开发进度，同步推动项目前进。

4.2 生态圈建设

OracleChain 自身定位为 EOS 生态圈中打通链内链外数据的重要一环,并以此为基础培育更多上层应用。一个生态圈的繁荣，需要吸引更多的人才积极参与。出于这个目的，在 OCT 分配方案中配置了 10%的社区推广基金。该部分资金会用于支持诸如黑客马拉松等社区活动，以便培育更多开发成员。在举办这些活动中还希望能挖掘优秀的的创意和团队，围绕 OracleChain 的数据基础服务培育出更多更多区块链应用，积极推动生态圈的全面繁荣。

第五章、 OracleChain 应用

5.1 预测市场

OracleChain 可应用于预测市场。基于 OracleChain 基础服务去构建的预测市场类应用，将为本地和全球经济提供独特的价值发现功能。在区块链领域，涉及了链外链内数据打通主要有 Augur 和 Gnosis 两个项目。这两个项目均采用预测市场的架构，这就意味着为了把一个链外数据导入链内，需要经过社区的投票等一系列过程才能在区块链上形成一个公允数据。预测市场的架构足以支撑那些与链外数据交互频次很低的场景里,比如对一场足球赛事比赛结果的对赌智能合约。但在那些交互频次很高的场景里,对链内链外数据通道的实时性提出了更高的要求。OracleChain 既可以以传统的方式支持低频预测市场的运作，也可以支持由众多节点实时从线下抓取链外数据,并根据节点们所提供的喂价数据折中选择出一个结果同步到区块链上。在一个包含了各种应用场景的 EOS 区块链生态圈里，需

要一个更高效的策略来替代低效的线下监督。瞄准这一问题 OracleChain 会基于 PoRD 机制的自治架构，来保证链内链外数据打通服务的实时和准确。

5.2 保险市场

OracleChain 可用于组织去中心化的农产品价格和收入保险市场，响应国家号召服务四农。

在传统的保险行业中，保险公司承担着吸收风险、消费风险的中介身份。区块链的出现让大家看到大规模的互助保险成为了一种可能。但是这种自组织的保险模式受困于效率和定险，很难推广。OracleChain 提供一种对事件定险的可能，尤其是在农产品价格和收入方面。

2017 年 6 月 1 日，中共中央办公厅、国务院办公厅印发《关于加快构建政策体系培育新型农业经营主体的意见》（下称《意见》）。《意见》提出，积极开展天气指数保险、农产品价格和收入保险、“保险+期货”、农田水利设施保险、贷款保证保险等试点。对于农产品价格这种集中式风险，保险公司很难使用传统的“空间+时间”的风险分担模式降低自己的风险，只能采用“时间”的风险分担模式，缺很难找到对应的风险分销机构。

基于 OracleChain 可以开发专门针对农产品价格的各类智能保险种类，直接将承包人和风险承担者对接，基于智能合约的购买、赔付方式将大大降低保险的成本，也将保险公司的集中风险直接分摊到风险承担者个人身上。

5.3 智能投顾

区块链的预言机有不少应用场景，在智能合约能够真正自动地执行现实生活

中的业务逻辑判断之前，首要的工作是能够获取外部数据，其后才能用基于区块链上智能合约的自动执行代替传统社会通过人为参与执行逻辑事务。智能投顾又称机器人理财，是虚拟机器人基于客户自身理财需求，通过算法和产品来完成以往人工提供的理财顾问服务。在区块链领域，智能投顾的功能主要通过智能合约来实现。利用 Oracle 智能合约机制，OracleChain 可用于链内和链外投资标的价格的发现与处理，可以建立起去中心化的智能投顾应用，投资目标既可以是传统金融标的，也可以是区块链资产。

5.4 体育竞猜

OracleChain 可为体育竞猜提供一种去中心化的数据组织和处理方案。根据 Gnosis 的资料，全球在线体育博彩是一个庞大的市场，受监管市场的博彩金额至少高达数十亿美元，而有些估计显示未受监管市场的博彩额是是受监管的 10 倍。尽管有这么大的机会，公司和政府在现有模式下的创新速度也还是十分缓慢。在孤立数据和流动性池中运行的现有应用程序可访问性有限，并且将新产品推向市场的速度很慢。此外，通过中心化的服务，用户会遇到额外的风险，例如盗窃或其他故障，以及付款处理器的意外问题。

这种中心化的体育竞猜服务的主要障碍就是上述的数据孤立和访问性差的问题。没有公开，公平，透明的市场访问方式，产品不能提供一个能够促进创新的平台模式，而且可能反而会受到损害。

OracleChain 是以开放平台的方式运行的，而且整个竞猜结果的组织是去中心化、公平无偏见和透明的。这样新旧参与者在同一平台上可以安全地获得经营回报，例如增加流动性转化为更好的赔率。

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[2] block.one,” EOS.IO Technical White Paper”, 2016.[Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
[3] block.one(赵微、谭智勇、宋承根@OracleChain，梓岑@YOYOW 译),” EOS.IO Technical White Paper(EOS 白皮书-中文版)”, 2016.[Online]. Available: http://btsabc.org/article-978-1.html
[4] V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform,” 2014. [Online]. Available:https://github.com/ethereum/wiki/wiki/White-Paper.
[5] M. Liston and M. K¨ oppelmann, “A visit to the oracle,” 2016. [Online]. Available: https://blog.gnosis.pm.
[6] J. Peterson and J. Krug, “Augur: A decentralized, open-source platform for prediction markets,” 2014. [Online]. Available: http://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platformfor-Prediction-Markets.pdf.

赵微、谭智勇、宋承根@OracleChain

初稿于 2017 年 6 月 12 日周一凌晨 3：00 东方渐白

修订稿于 2017 年 9 月 27 日周三下午 3：00 日暮西山