**预言机介绍**

**Oracle**

**定义**

预言机（Oracle）的主要功能是将外部数据引入区块链智能合约，使得这些合约能够与现实世界进行互动（读取到外部世界的数据）。由于区块链的本身是封闭的系统，无法访问外部数据，预言机在信息传递中扮演着桥梁的角色，它可以从外部世界获取信息并将其传递给区块链。

例如，如果智能合约要获取天气预报、金融市场价格、体育比赛结果等数据， 都需要通过预言机来获取源数据然后传递给合约。

将链上和链下世界连接需要通过一个中间层，那就是“预言机”。

**作用**

区块链预言机是将区块链安全连接至链下系统的中间层，区块链可以通过预言机连接至数据提供商、web API、企业后端、云服务商、物联网设备、电子签名、支付系统以及其他区块链等各种链下环境。预言机具有几大关键功能：

* **等待响应**——监控区块链网络，扫描网络中是否有来自于用户或智能合约的链下数据请求。
* **获取数据**——从一个或多个链下系统获取数据（比如由第三方web服务器运行的链下API）
* **格式化**——将来自API的数据转换成区块链可读的格式，并将链上数据转换成外部API兼容的格式，以此打破链上链下的交流屏障。
* **验证**——使用数据签名、区块链交易签名、TLS签名、可信执行环境（TEE）证明以及零知识证明等各种工具为预言机服务提供加密证明。
* **计算**——对数据进行运算，比如基于多个预言机提交的数据计算出中位数，或基于不同类型的数据（如：个人风险情况、市场费率和资金成本等）生成保险报价。
* **广播**——通过在区块链上签名并广播交易将数据和相关证明发送至链上智能合约。
* **数据输出（可选）**——在智能合约执行时向链下系统发送数据，比如将支付指令发送至传统支付网络，或与信息物理系统进行交互。

为了实现上述功能，预言机系统必须要在链上和链下同时运行。**链上模块**的作用是与区块链交互（等待数据响应）、广播数据、发送证明、获取区块链数据以及有时在链上进行运算。**链下模块**的作用是处理数据请求、获取链下数据并转换格式、将区块链数据发送至链下系统以及在更高级的预言机网络中进行运算。

**分类**

**软件预言机**：从在线数据源（如API）获取数据，适用于公共和可访问的信息。

**硬件预言机**：通过传感器等设备获取物理世界的数据，如温度、湿度等。

**中心化预言机**：由单一实体控制，虽然实现简单，但存在信任问题和潜在的单点故障风险。

**去中心化预言机**：通过多个独立节点提供数据，降低单点故障的风险，增强数据的可靠性。

**挑战**

* **数据源可信**
* 数据源选取和可信认证。预言机需要谨慎选择外部数据源，必须保证对每个选取的外部数据源，都可以验证是可信的
* 数据获取有标准流程。开发者必须明确执行引擎、用户、外部数据源与预言机的数据交换流程，且对于不同的数据源类型要能够统一或明确区分数据的交互流程，确保交互方案可执行可落地
* 数据交互格式统一。不同的数据源类型有不同的数据交互格式，以传感器作为数据源和以Web作为数据源获取到的数据格式是不一样的，针对不同情况，明确统一的数据编解码层，以对不同数据源的数据进行请求和解释。
* **数据传输的安全性**
* 数据从网上到本地，采用HTTPS协议（底层采用TLS协议）去保障连接和数据的正确性、完整性。
* 数据从本地到链上，预言机采用可信执行环境 ( TEE ) 技术，TEE是CPU内一块安全区域，和操作系统独立运行

**赛道**

**发展历程**



* 2014 及以前

Augur 是一个去中心化预测市场，使用户能够将数字资产押在现实世界事件的结果上。预言机需求初现。Vitalik 是该项目的顾问。

* 2015-2016 阶段

以太坊联合创始人 Vitalik Buterin 提出预言机概念，强调其作为智能合约获取外部数据的关键作用。2015 年，Oraclize（现为 Provable）推出首个去中心化预言机服务，支持以太坊智能合约获取外部数据。同年，以太坊主网上线。

* 2017-2018 阶段

Chainlink 项目在 2017 年成立，提出去中心化预言机网络（DON）的概念，旨在解决单点故障问题。去中心化金融（DeFi）尚未爆发，预言机需求主要集中于简单数据调用。

* 2019-2021 阶段

2020 年 DeFi Summer 来临，预言机作为 DeFi 最核心的外部数据服务商，为去中心化应用提供喂价服务。由于需求的爆发，Chainlink 之外的预言机项目如 Band Protocol、Tellor 相继推出，竞争格局初现。

* 2022-2023 阶段

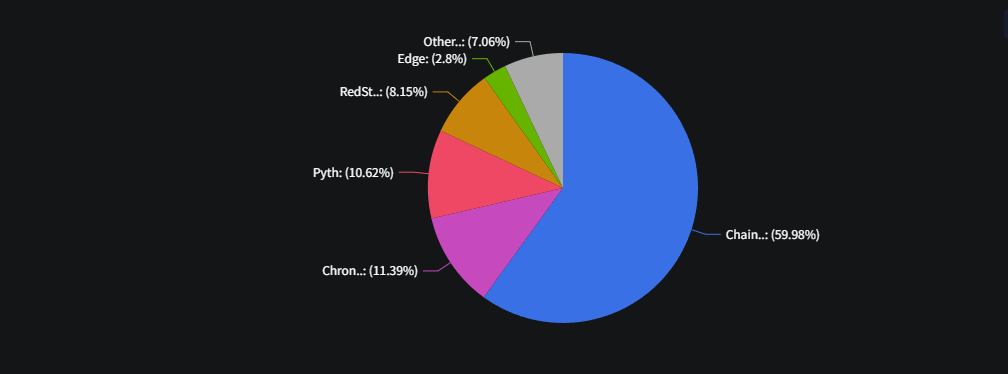
DeFi 市场进入调整期，但预言机赛道持续创新。跨链互操作性和模块化区块链成为行业趋势，预言机服务向多链、多场景扩展。Chainlink 推出跨链互操作性协议（CCIP），支持跨链数据传输和智能合约交互。Pyth Network（专注于金融数据的预言机）主网上线，吸引多家传统金融机构参与。

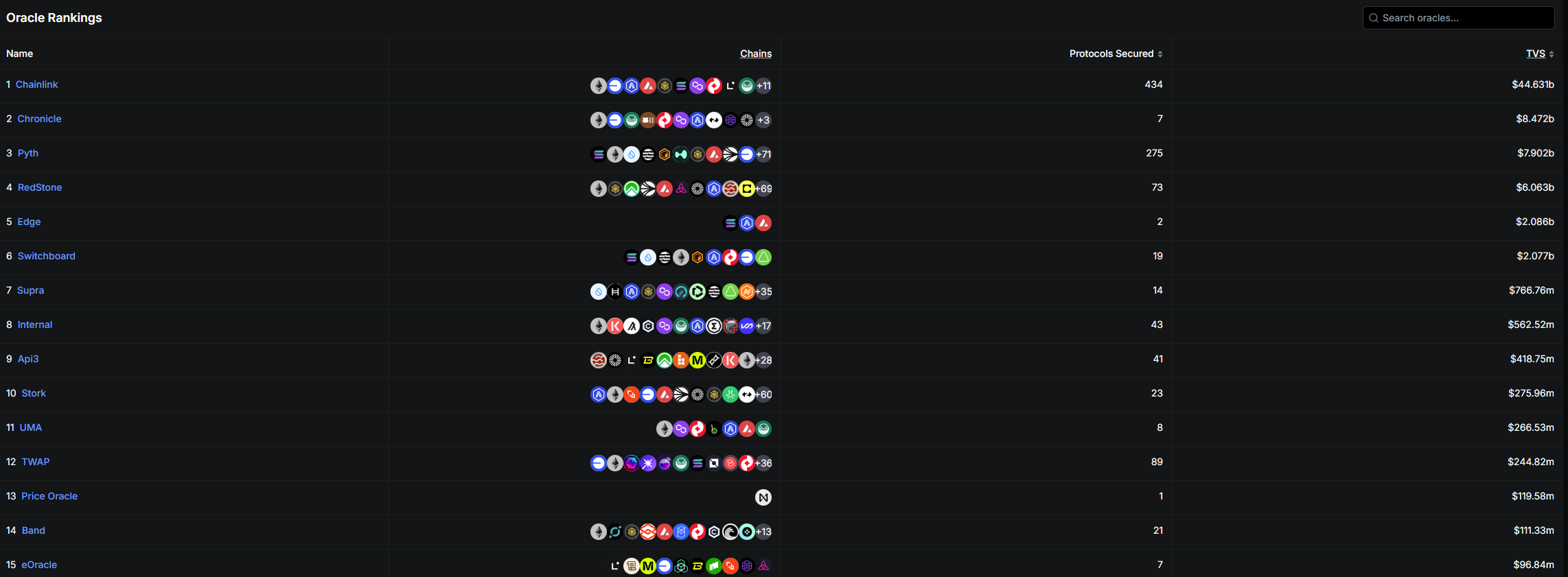
* 2024-2025 阶段

预言机服务从 DeFi 扩展到游戏、NFT、保险等领域。DePIN 应用开始对物联网预言机有更多的需求。AI 与预言机结合，探索智能合约自动化执行的新场景。

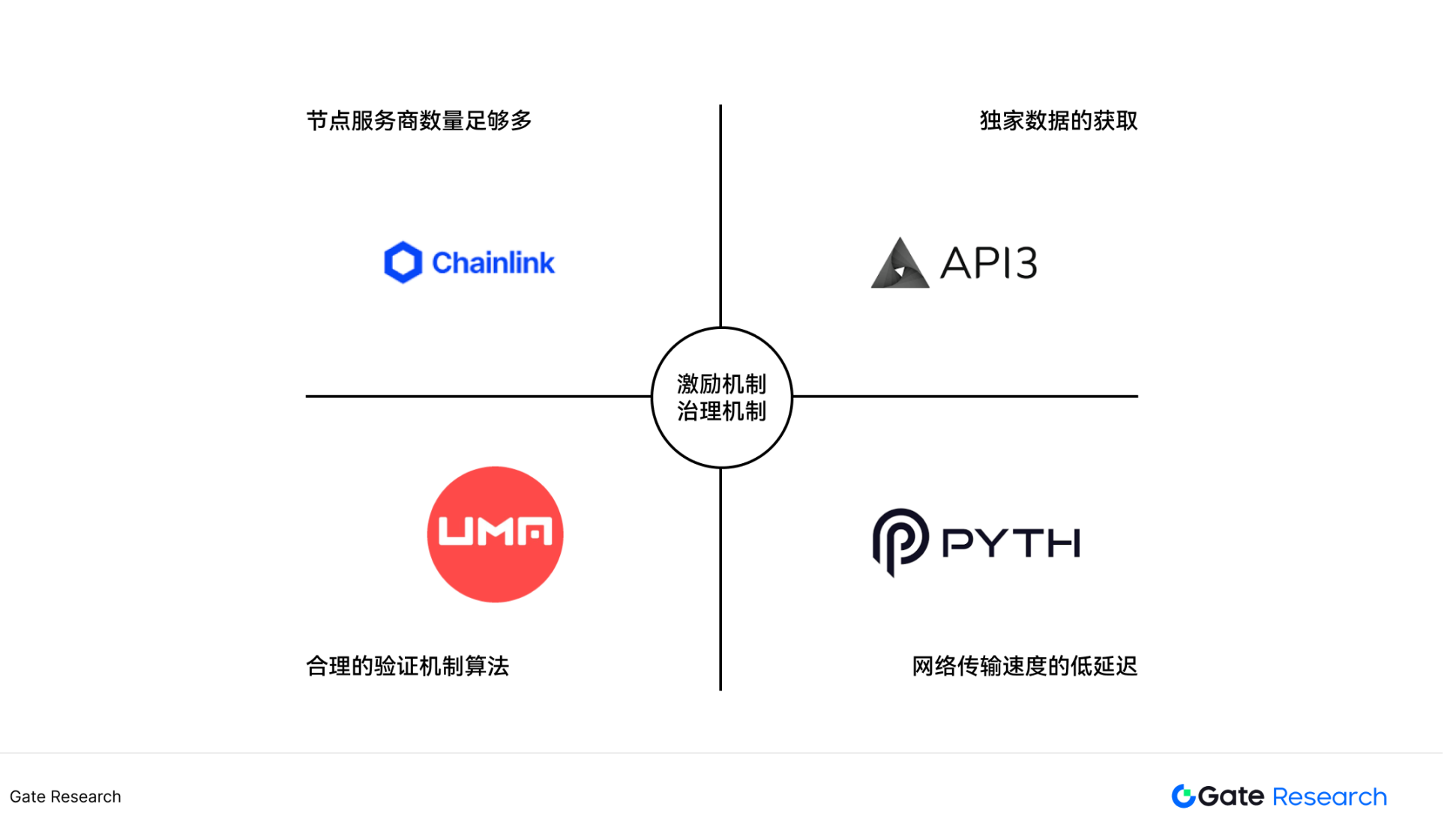
**市场现状**

[数据来源](https://defillama.com/oracles)



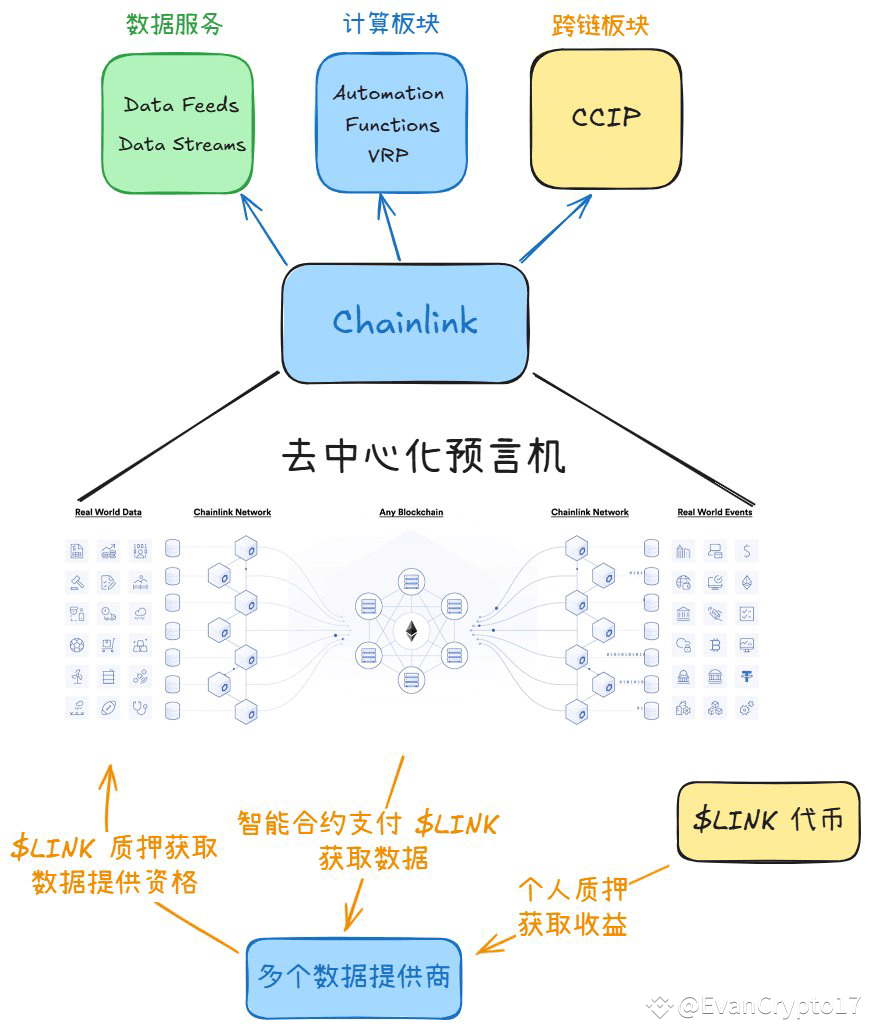


**竞争模型**



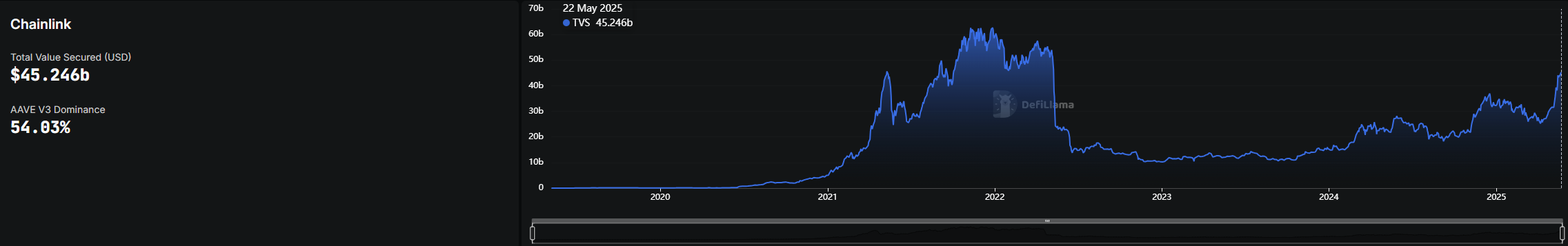
**Chainlink**

[Chainlink](https://chain.link/) 是一个去中心化的预言机网络，旨在将区块链智能合约安全可靠地连接至链下系统。Chainlink采用了与区块链相同的模式，建立了去中心化的独立预言机网络，网络中的预言机从多个数据源共同获取数据，将数据聚合，并将经过验证的聚合数据传输至智能合约，触发合约执行，在整个过程中规避了所有中心化风险。



* **开源**——Chainlink是开源技术，整个区块链社区可以独立验证Chainlink源代码和功能的安全性和可靠性，并不断进行完善。
* **外部适配器**——节点可以安全地储存API秘钥并管理账户登录信息，这使智能合约能够从任何链下系统和API获取数据，包括受密码保护的认证API。
* **去中心化**——在节点和数据源层面都实现去中心化，避免出现节点或数据源的单点失效，为用户保障数据传输的及时性和完整性。
* **数据签名**——节点需要对发送至智能合约的数据进行加密签名，因此用户可以查看哪个节点发送了哪些数据，并查看节点的历史服务记录以了解其服务水平。
* **服务协议**——请求数据的智能合约与预言机运营商需要在链上签署具有约束力的服务协议，约定预言机服务条款以及奖惩制度，为用户保障链下数据的质量。
* **声誉系统**——将经过签名的链上数据传输至声誉系统，让用户可以做出理性选择，基于完成任务数量、服务客户数量和平均响应时间等各种指标判断节点的优劣。
* **认证服务**——为节点提供KYC、节点地理位置以及基础架构安全评估等认证，提升节点的安全性和可靠性。
* **高级加密技术和硬件保护**——零知识证明等高级加密技术以及可信执行环境等硬件保护可以为预言机带来额外的安全保障，比如向智能合约证明数据来源（注：证明数据来自某一服务器），向预言机隐藏数据内容，以及执行链下计算等。

**TVS**



[市场数据来源](https://defillama.com/protocol/chainlink)

**白皮书**

**1.0**

* **核心功能：**

**链下数据喂价 (Data Feeds)，**1.0 版本的主要功能是安全地将外部数据（主要是金融市场的价格数据）传输到区块链上的智能合约。

* **架构：**
* **独立请求模型：** 智能合约向单个 Chainlink 节点发起数据请求，节点从外部 API 获取数据并返回。
* **去中心化数据模型：** 为了提高可靠性，引入了从多个独立 Chainlink 节点聚合数据的模型，这些节点将数据提交到链上，通过链上聚合合约进行汇总。
* **Off-chain Reporting (OCR)：** 这是 Chainlink 1.0 后期引入的一项关键改进，它允许节点在链下进行数据聚合和共识，然后只将一个签名过的聚合结果提交到链上，极大地降低了 gas 成本并提高了效率。
* **主要服务：** 价格喂价 (Price Feeds)、可验证随机函数 (VRF) v1。
* **侧重：** 解决智能合约的“预言机问题”，即让智能合约安全地访问现实世界数据。

**2.0**

主要改进和新功能包括：

* **从“数据传递”到“链下计算”**
* **DONs 作为计算层**

Chainlink 2.0 将 DONs 视为一个能够执行各种链下计算的去中心化元层，而不仅仅是数据传输。这意味着 DONs 可以处理复杂的逻辑，而这些逻辑在链上执行成本过高或无法实现。

* **混合智能合约**

智能合约将成为“混合”的，结合了链上代码的确定性和安全性，以及链下 DONs 提供的连接性、可扩展性、保密性和计算能力。

* **更强大的安全模型**
* **超线性质押 (Super-linear Staking)**

Chainlink 2.0 引入了更先进的质押机制，旨在通过经济激励，以远超节点总质押金额的成本，来阻止恶意行为。攻击者需要投入的资源是所有 DON 节点抵押的总和的平方级别。

* **两层仲裁系统**

引入了更强大的安全保障，包括一个两层仲裁系统，以解决数据争议和确保报告的准确性。

* **去中心化警报系统、**

允许 DON 独立识别和报告潜在的恶意行为或数据异常。

* **扩展的服务范围**
* **Chainlink Automation (原 Keepers)**

提供去中心化的智能合约自动化服务。例如，自动触发清算、定期执行合约功能等，而无需依赖中心化服务器。

* **Chainlink VRF v2.0+**

改进后的可验证随机函数，提供更低的 Gas 成本、更灵活的订阅管理和更高的安全性，广泛应用于 GameFi、NFT 和其他需要可验证随机数的场景。

* **跨链互操作协议 (CCIP - Cross-Chain Interoperability Protocol)**

这是 2.0 愿景中最宏伟的部分之一。CCIP 旨在提供安全、可靠且去中心化的跨链消息传递和价值转移功能，允许任何区块链上的应用与任何其他区块链上的应用通信，是实现真正的 Web3 互联互通的关键基础设施。

* **可信执行环境 (TEE) / 零知识证明 (ZKP) 整合**

探索使用更高级的隐私保护和数据完整性技术，例如在 TEE 内执行链下计算，或使用 ZKP 证明计算的正确性而无需透露原始数据。

* **公平排序服务 (Fair Sequencing Services, FSS)**

旨在解决 MEV (最大可提取价值) 问题，通过去中心化的方式确保交易的公平排序。

**应用场景**

* **Defi**

为 Aave、Compound 等提供价格数据，支持借贷和衍生品。

* **保险**

如 Arbol 的农业保险，利用 Chainlink 获取天气数据。

* **游戏**

通过 VRF 提供随机性，如 Axie Infinity 的游戏机制。

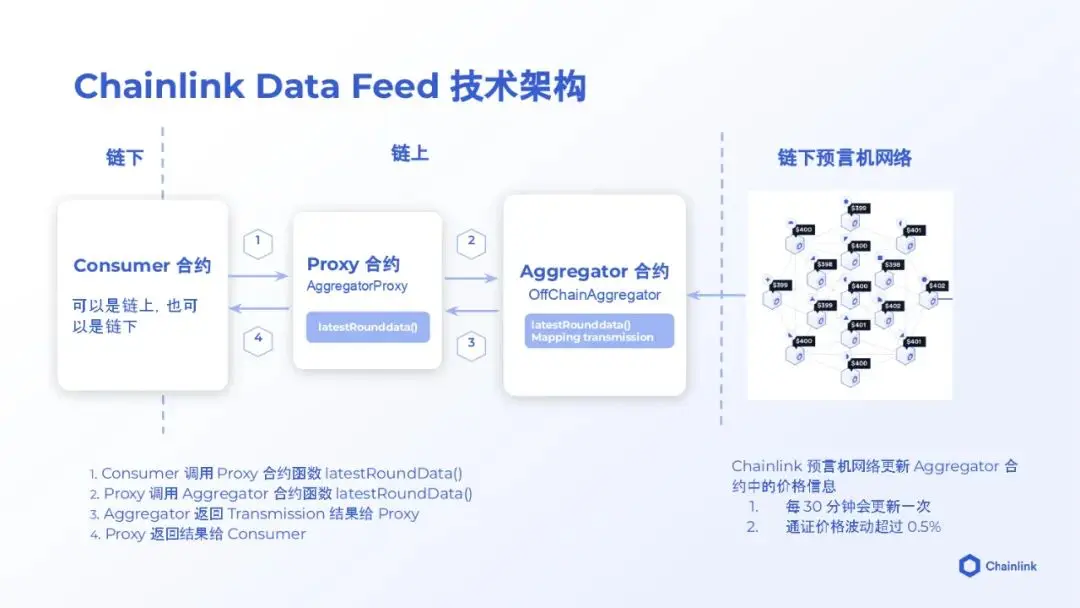
* **跨链生态**

通过 CCIP 支持 Polygon、Avalanche 等链的互操作。

**核心产品**

* 数据类
* **Market and Data Feeds**

[Chainlink Data Feeds](https://data.chain.link/) 主要包含了三个合约，第一个是 Consumer 合约 ( 用户合约 )，第二个是 Proxy 合约 ( 代理合约 )，第三个就是刚才提到的 [Aggregator 合约](https://github.com/smartcontractkit/libocr/blob/master/contract/AccessControlledOffchainAggregator.sol) ( 聚合合约 )。Proxy 合约作为接口连接 Consumer 合约和 Aggregator 合约，屏蔽了 Aggregator 的复杂性，对外向用户提供一个统一的接口（latestRounddata），返回预言机网络最近一次的价格数据。



* 案例场景

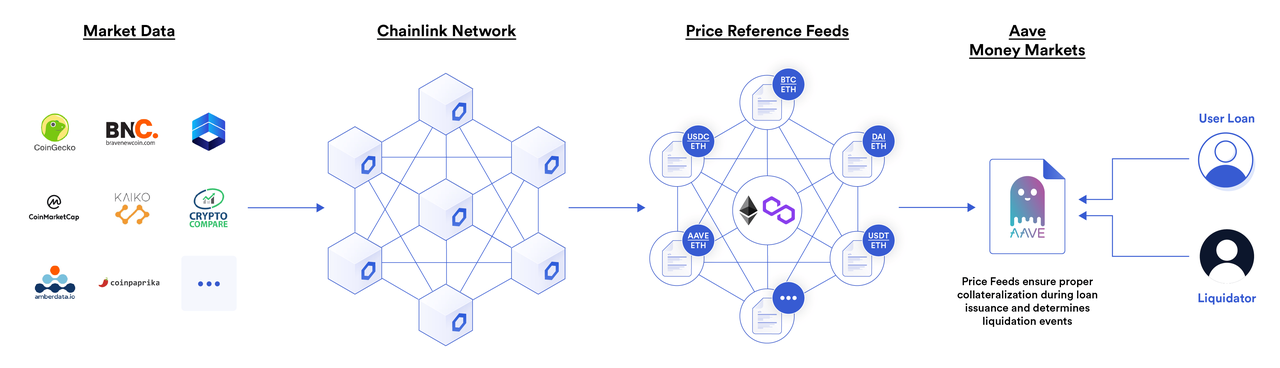
Data feeds 应用场景非常广泛，很多主流 DeFi 项目都集成了 Data Feeds。

最常见的一个应用场景是借贷协议，比如 Ethereum 上的 AAVE，Compound ， BNB 上的 Venus。当用户在 AAVE 上存入一个 BTC 然后贷出来 USD 时， AAVE 需要知道 BTC 和 DAI 的兑换比例，才能决定给用户贷多少 USD。

第二个应用场景是合成资产，比如Synthetix（SNX），它可以让用户去交易一些主流资产，比如美股股票。用户合成资产时，协议肯定需要知道资产价格，这个价格就是通过 Data Feeds 获取的。

第三个应用场景是抵押型 Stablecoin 。抵押型 Stablecoin 要发行的话，需要抵押相应的资产。Stablecoin 的协议需要通过 Data Feeds 获取资产的价格后，才可以计算得出抵押资产的总价值，根据总价值决定 Stablecoin 的发行数量。

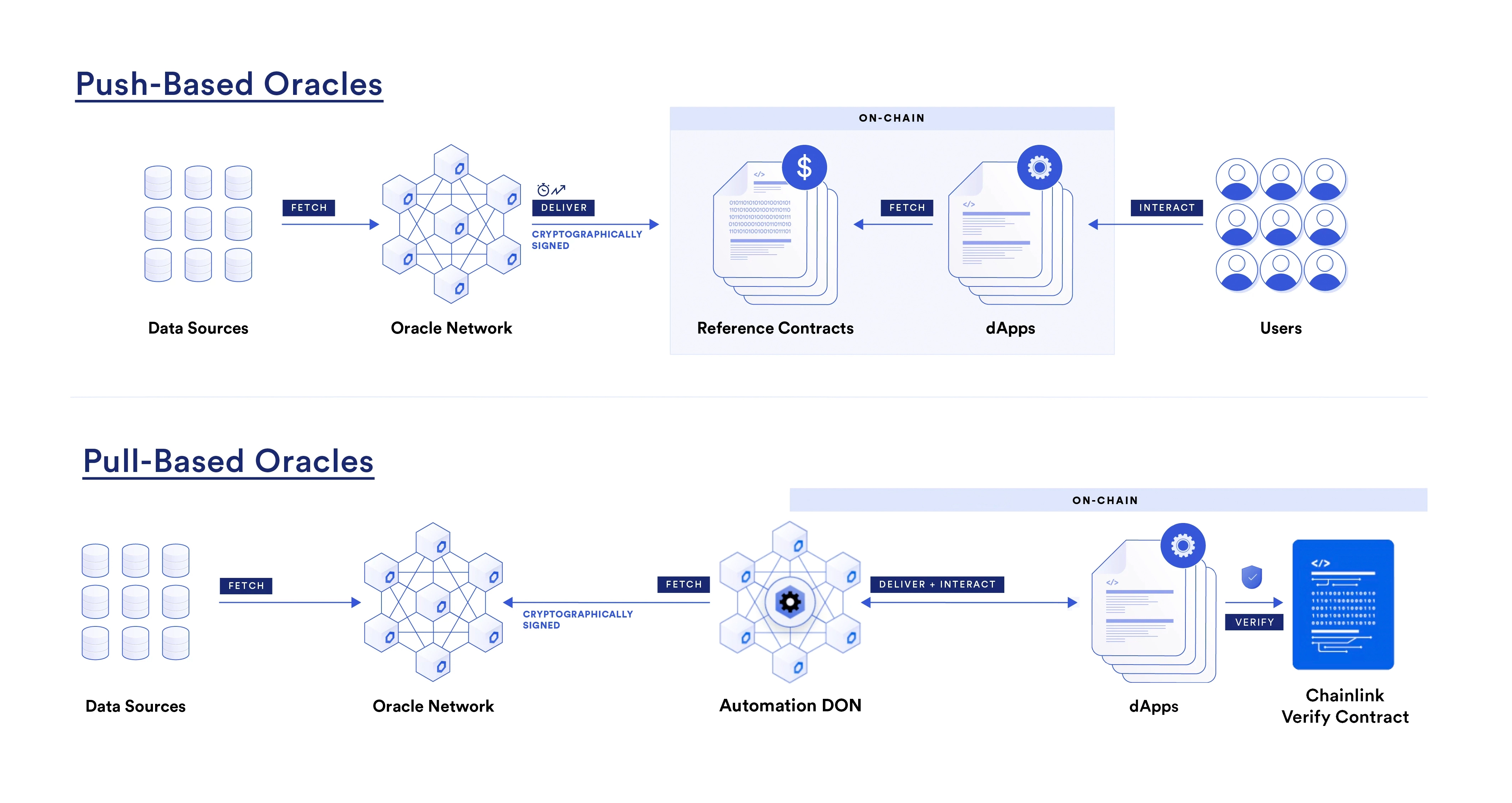
第四个是资产管理和衍生品的交易平台。像期权、期货交易平台，它们对价格都很敏感，需要提供稳定、准确的价格数据， Data Feeds 提供的数据完美的满足了它们的业务需求。



* **Data Stream**

[Chainlink Data Streams](https://data.chain.link/streams) 采用拉取式设计，允许您随时检索报告并在链上进行验证。验证过程确认去中心化预言机网络 (DON) 已同意并签署了数据。有些应用只需要固定间隔的链上数据，这很适合推送式预言机。然而，有些应用需要更高频率的更新和更低的延迟。拉取式预言机可以满足这些需求，同时仍然提供数据准确性的加密保证。

是 Chainlink 预言机网络提供的一项高级服务，旨在为去中心化金融（DeFi）应用提供**低延迟、高吞吐量**的市场数据。它与 Chainlink 传统的“推送式”（Push-based）数据源（Data Feeds）有所不同，采用了\*\*“拉取式”（Pull-based）模型\*\*，更适合需要\*\*亚秒级（sub-second）\*\*数据更新的应用场景，例如永续合约、期权交易和高频交易。



主要功能包括：

* **链下数据持续可用**
* Chainlink DON 节点不断从数据源获取价格，并将其签名后的报告发送到链下的 **Data Streams 聚合网络**。
* 这个聚合网络保证数据报告的亚秒级更新和高可用性，并提供 WebSocket 接口供应用监听。
* **链上智能合约逻辑**
* DeFi 协议（例如永续合约交易所）的智能合约中包含需要实时价格的逻辑（如清算、计算资金费率、执行限价单等）。
* 这些操作通常由外部触发（用户交易、清算机器人、自动化任务）
* **Chainlink Automation (Keepers)**
* **作为“执行者”**

智能合约会与 Chainlink Automation 集成。当满足特定条件（例如，需要执行一笔清算、用户提交了一笔交易需要价格）时，自动化机器人会被触发。

* **原子化执行**

这个自动化机器人会执行以下操作：

* 从链下 Data Streams 聚合网络“拉取”最新、由 DON 节点签名的价格报告。
* 将这个签名报告作为 calldata 或交易参数，与需要执行的交易（例如 liquidate() 函数调用）一起， 在一个单笔原子化交易中提交到链上。
* **链上验证与执行**
* 当这笔交易到达 Layer-1（或 Layer-2 Rollup）时，智能合约首先会调用 Chainlink Data Streams 的**链上验证器。**
* 验证器会检查提交的签名报告
* 验证这些签名是否有效（由 Chainlink DON 节点正确签名）。
* 验证报告是否是最新的（在合理的时间窗口内）。
* 验证报告中的数据是否与共识值一致（通常要求多数节点签名）
* 只有当签名报告通过验证后，智能合约才会使用报告中的价格数据来执行其核心业务逻辑（如清算）

|  |  |  |
| --- | --- | --- |
| **特性** | **传统 Chainlink Data Feeds（推送式）** | **Chainlink Data Streams（拉取式）** |
| **数据上链方式** | DON 节点主动将价格更新推送（写入）到链上 | 签名数据在链下持续更新。仅在需要时，由 Automation 或用户将签名报告作为交易的一部分拉到链上并验证 |
| **链上价格更新** | 持续发生（例如，每小时，或价格波动超过 0.5%） | 不发生持续的价格更新。链上价格数据仅在交易发生时被验证和使用 |
| **延迟** | 通常为几秒到几十秒（取决于更新频率和链确认时间） | 亚秒级链下延迟，链上延迟仅为单次交易的确认时间 |
| **Gas 成本** | 节点推送数据到链上需要支付 Gas 费 | 主要 Gas 成本发生在使用数据进行交易时，显著降低非必要的 Gas 消耗 |
| **MEV 风险** | 数据在链上更新时可能存在 MEV 风险（如抢跑清算） | 通过原子化执行和提交-揭示模型，有效缓解 MEV 风险 |
| **适用场景** | 借贷协议、稳定币抵押、资产定价等对实时性要求不那么极致的场景 | 永续合约、期权、高频交易、动态清算等对延迟极度敏感的场景 |

* **POR（Proof of Reserve）**

Chainlink Proof of Reserve（PoR）是 Chainlink 去中心化预言机网络的一项服务，旨在为区块链上的资产提供透明、实时的储备验证，确保链上代币（如稳定币、包装代币、代币化现实世界资产等）与链下或跨链储备资产的1:1锚定。

* **CCIP**

这是 Chainlink 2.0 愿景中的核心组件之一，旨在提供安全、可靠且去中心化的跨链消息传递和价值转移服务。它允许任何区块链上的应用与任何其他区块链上的应用进行通信和资产转移。

* 任意消息

能够将任意数据（编码为字节）发送到不同区块链上的接收智能合约。开发人员可以自由地对想要发送的任何数据进行编码。

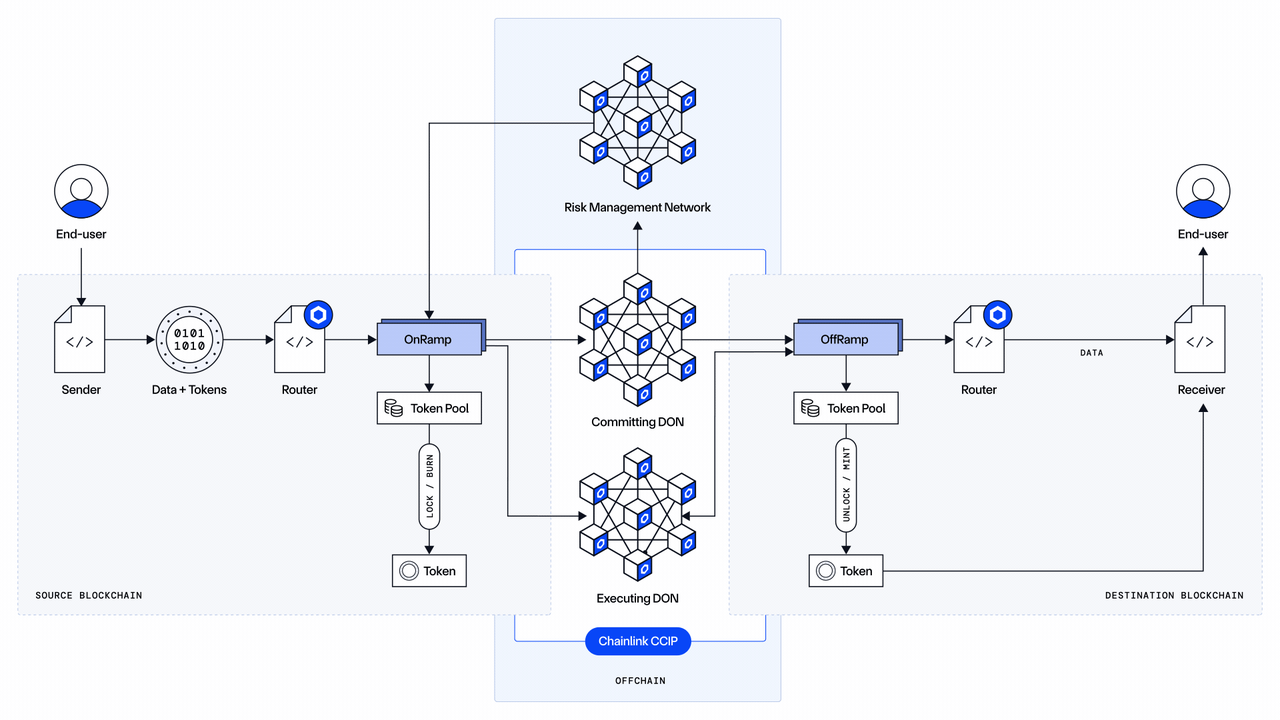
通常，开发者使用任意消息来触发接收智能合约的合理操作，例如重新平衡指数、铸造特定的 NFT，或使用发送的数据作为自定义参数调用任意函数。开发者可以在一条消息中编码多条指令，从而能够协调复杂、多步骤、多链的任务。

* 代币转移

将代币转移到不同区块链账户的能力。此功能可实现跨链资产的无缝转移。

* 可编程代币转移

能够在单笔交易中同时传输代币和任意数据（以字节为单位）。此机制允许用户传输代币并发送如何处理这些代币的指令。例如，用户可以将代币转移到借贷协议，并按照指令利用这些代币作为贷款的抵押品，借入另一项资产并将其返还给用户。



* 计算类
* **Function**

支持开发者调用任意链下 API，扩展了数据源范围（如 Google Maps、航班状态）。

* **Automation**

从轮询模型升级为共识机制，增强了自动化任务的可靠性和安全性，降低了链上计算成本。

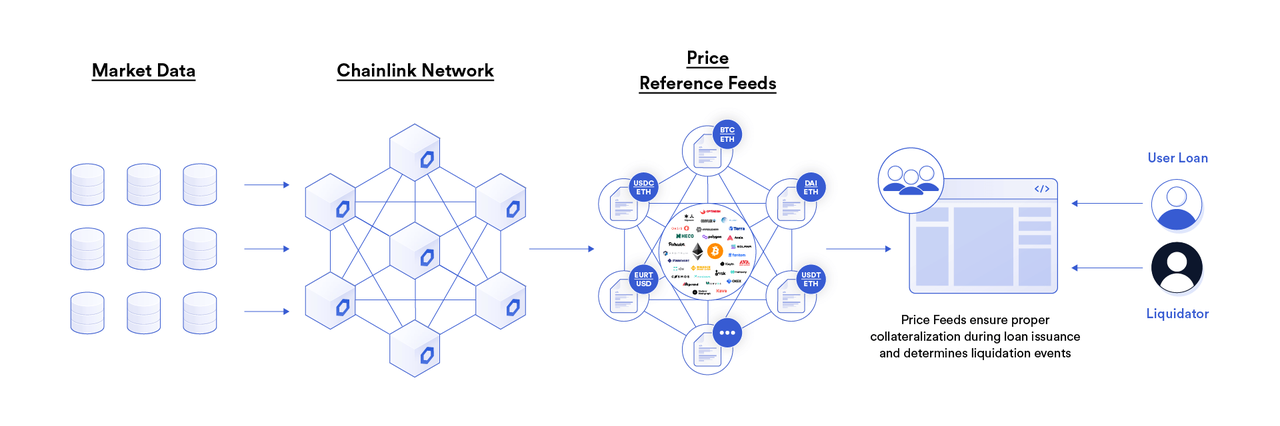
* **Vrf**

为游戏、NFT 等提供安全的链下随机数生成。

* **FSS**

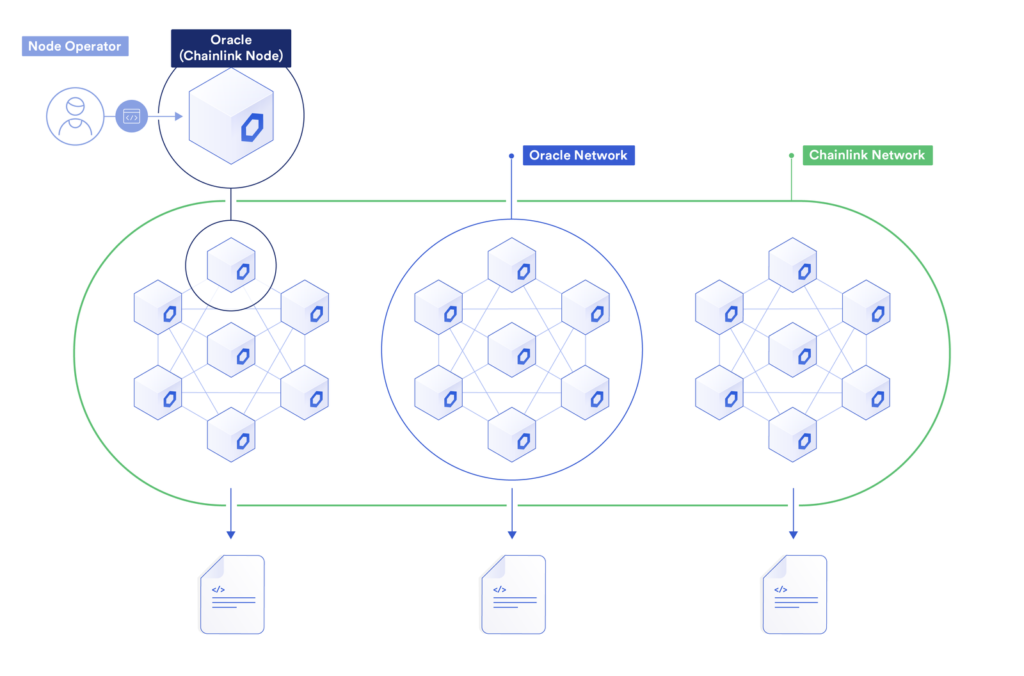
解决MEV问题

**网络结构**



**Chainlink网络**

Chainlink 是构建在现有区块链之上的。这意味着 Chainlink 本身依赖于其所运行的**底层区块链的共识机制**来保证其链上操作（如智能合约的执行、数据提交的最终性、交易的防篡改性）的安全性。例如，如果 Chainlink 运行在以太坊上，它就受益于以太坊的 PoS 共识。



**链上层**

链上组件是部署在区块链（如以太坊、Solana 等）上的智能合约，负责与链下组件交互、处理用户请求和存储结果。

* **请求合约 / 消费者合约 (Requesting/Consumer Contracts)**

这是由 DApp 开发者编写并部署在区块链上的智能合约。当它们需要链下数据或触发链下计算时，它们会向 Chainlink 的链上合约发起请求。

* **Chainlink 协调器 / 路由合约 (Coordinator/Router Contracts)**

这些是 Chainlink 官方部署在各条区块链上的核心智能合约。它们充当请求合约的网关，接收请求，管理订阅，并将请求路由到链下的 Chainlink 去中心化预言机网络 (DONs)。对于 CCIP 这样的服务，还有专门的路由合约负责跨链消息的传递。

* **聚合器合约 (Aggregator Contracts)**

主要用于 Chainlink Data Feeds。当多个 Chainlink 节点提交数据时，聚合器合约负责收集这些数据，并根据预设的算法（如中位数）进行聚合，生成一个被大多数节点认可的单一、权威的链上数据点。

* **声誉合约 (Reputation Contracts)**

跟踪和记录 Chainlink 节点运营商的历史性能、响应时间、数据准确性等指标。这些信息可以帮助请求合约选择表现良好的节点。

* **质押合约 (Staking Contracts)**

负责管理节点运营商质押的 LINK 代币。这些质押是节点服务可靠性的经济担保，如果节点行为不当，其质押可能会被罚没。

* **跨链互操作协议（CCIP Contracts）**  
  支持跨链通信，允许不同区块链之间传输数据和资产。

**链下层**

* **Node**
* **Job Spec**

Job Spec 就像是给 Chainlink 节点下达的“工作指令”或“操作手册”。它详细定义了节点需要执行的一系列任务，以完成一个特定的数据请求。对于获取链下数据而言，Job Spec 中就包含了明确的数据源信息和解析规则。Job Spec 通常由 Chainlink 节点运营商在配置其节点时创建和部署，或者由智能合约通过 Chainlink Functions/Any API 等方式直接指定。

在 Job Spec 中会包含以下核心信息：

* **数据源 URL (Endpoint URL)：** 明确指定了 Data Provider 提供数据的 API 端点。
* 例如：https://api.enterpriseA.com/soybean\_price
* **HTTP 请求方法：** 指明节点应该使用哪种 HTTP 方法来请求数据（通常是 GET 或 POST）。
* **JSONPath 表达式 (或解析逻辑)：** 这是指导节点如何从 API 响应中提取所需数据的关键。
* 如果企业 A 的 API 返回 JSON 格式的数据，Job Spec 会包含一个 JSONPath 表达式（例如 $.price），告诉节点从 JSON 响应的根目录下的 "price" 字段中获取数值。
* 如果数据格式更复杂，或者需要进行额外的计算/转换，Job Spec 可能会引用一个 **外部适配器 (External Adapter)**。
* **Data Provider 与 Node 接入方式**
* 与现有 Chainlink 节点运营商合作
* 自己运营 Chainlink 节点
* **Node 获取 Data 流程**

1. 节点配置

Chainlink 节点运营商在设置其节点时，会向节点加载一系列的 Job Spec 。这些 Job Specs 包含了节点能够提供哪些服务的详细指令。其中一个 Job Spec 可能就是专门用于获取价格数据的。

1. 服务提供者注册

在 Chainlink Data Feeds 的场景中，节点运营商会使其节点成为一个特定 Data Feed（如BTCUSDT价格喂价）的参与者。这意味着该节点声明自己能够提供这个数据。

1. 智能合约请求
2. 当企业 A 在以太坊上的智能合约需要大豆价格时，它会向 Chainlink 的**聚合器合约**发起请求（或者直接调用）。
3. 聚合器合约（或 Chainlink 协调器）会选择一组合格的 Chainlink 节点来满足这个请求。
4. Job Spec 触发与执行

* 被选中的 Chainlink 节点收到链上的数据请求事件。
* 节点会查看其内部存储的 Job Specs，找到与该请求对应的 Job Spec（例如，根据 jobId 匹配）。
* 根据 Job Spec 的指示，节点执行一系列“任务 (Tasks)”，例如：
* HTTP GET/POST Task

节点会根据 Job Spec 中指定的 URL（即企业 A 的 API 端点 https://api.enterpriseA.com/soybean\_price）发送 HTTP 请求。

* JSON Parse Task

|  |
| --- |
| JSON {  "symbol": "SOYBEAN\_USD",  "price": 1250.75,  "timestamp": 1716307200,  "unit": "USD\_PER\_BUSHEL" } |

* 其他 Tasks

可能还有如 multiply（进行单位转换）、ethabiencode（将数据编码成区块链可识别的格式）、ethtx（将最终数据提交到链上）等任务。

* 外部适配器

如果涉及到外部适配器，Job Spec 会有一个 bridge 类型的任务，告诉节点去调用这个外部适配器，而外部适配器则负责与企业 A 的 API 交互并返回处理后的结果。

1. 数据聚合与链上提交

多个参与的节点会执行上述步骤，然后在链下通过 OCR 协议进行数据聚合。最终，一个聚合后的价格会被提交到链上，供企业 A 的合约使用。

* 潜在收益
* 提供专有、高质量或有价值的数据，Data Provider 可以向 Chainlink 节点运营商收费，以提供 Api 访问。
* 消费者 在使用以太坊网络上的智能合约数据时，那么该智能合约需要向 Chainlink 节点运营商支付费用。
* 支付 LINK 代币

智能合约使用 Chainlink 服务（无论是 Data Feeds、VRF、Automation 还是 Functions）都需要支付 Chainlink 的原生代币 LINK 作为服务费。这些费用直接支付给提供服务的 Chainlink 节点运营商。

* 费用构成

费用通常包括：

* Gas 成本: 节点将数据提交到链上所需的以太坊 Gas 费用。
* 服务溢价: 支付给节点运营商，作为他们运行基础设施、维护服务质量和承担风险的报酬。
* 灵活的支付方式

尽管最终支付是 LINK，但 Chainlink 提供了“支付抽象 (Payment Abstraction)”等机制，允许智能合约开发者用其他加密资产（如 ETH、稳定币）来支付，然后由 Chainlink 的自动化服务在后台将其转换为 LINK。

* **External Adapter**
* **处理复杂逻辑**

如果仅仅通过 JSONPath 无法满足数据解析或预处理的需求（例如，数据需要多步转换，或者从多个 API 获取后进行初步合并，或者需要特殊认证），节点运营商会开发或使用一个 **External Adapter**。

* **独立服务**

External Adapter 也是一个独立运行的服务（通常是一个小型 Web 服务器），它与 Chainlink 节点通过本地网络通信。Job Spec 会告诉节点去调用这个 External Adapter。

* **API 凭证管理**

如果企业 A 的 API 需要认证（如 API Key），External Adapter 也可以安全地存储和管理这些敏感凭证，避免直接在 Job Spec 中暴露。

* **Dons**
* **多节点协作**

一个 DON 由多个独立的 Chainlink 节点组成。当智能合约请求数据时，这些节点会并行地从多个链下数据源获取数据。

* **链下聚合与共识**

节点不会将各自获取的原始数据全部提交到链上。相反，它们在链下使用 OCR 协议进行高效的通信、数据共享和加密验证。它们会根据预设的聚合算法（例如，取所有节点报告数据中的位数）共同计算出一个**聚合结果**。

* **阈值签名**

DON 中的大多数节点必须对这个聚合结果达成一致，并使用各自的私钥对结果进行签名。只有当达到预设的**阈值数量**的节点签名（例如，如果一个 DON 有 21 个节点，可能需要 15 个节点签名）时，这个聚合结果才被认为是有效的。

* **单一链上报告**

最终，由 DON 中的一个节点（通常是轮流选出的领导者）将这个经多方签名的聚合结果一次性提交到链上。这大大降低了 Gas 成本，并提高了数据更新的频率。

* **OCR**（**Off-Chain Reporting**）

Chainlink 2.0 引入的链下共识机制，节点在链下完成数据验证和聚合，仅将最终结果上链。这降低了 Gas 费用，提高了性能和可扩展性。

**Pyth**

|  |  |  |
| --- | --- | --- |
| **特征** | **Chainlink** | **Pyth Network** |
| **数据来源** | 第三方数据聚合商、API，通过节点运营商传输 | 第一方金融机构、交易所、做市商直接提供 |
| **更新模型** | 推模型 (Push Model)，基于阈值/心跳更新 | 拉模型 (Pull Model)，高频实时数据，按需拉取 |
| **延迟** | 相对较高（几秒到几分钟） | 极低延迟（亚秒级） |
| **跨链** | 多链原生部署，通过 CCIP 实现通用跨链通信 | Pythnet 聚合，通过 Wormhole 等协议分发至多条链 |
| **数据范围** | 广泛（金融、物联网、体育、天气等） | 专注于机构级金融市场数据 |
| **主要目标** | Web3 通用预言机基础设施，提供多样化数据和计算服务 | 为高频、低延迟的 DeFi 金融应用提供实时市场数据 |
| **信任模型** | 去中心化节点网络、声誉、经济激励、数据聚合 | 第一方数据提供商的经济动机、信心区间、Pythnet 聚合 |