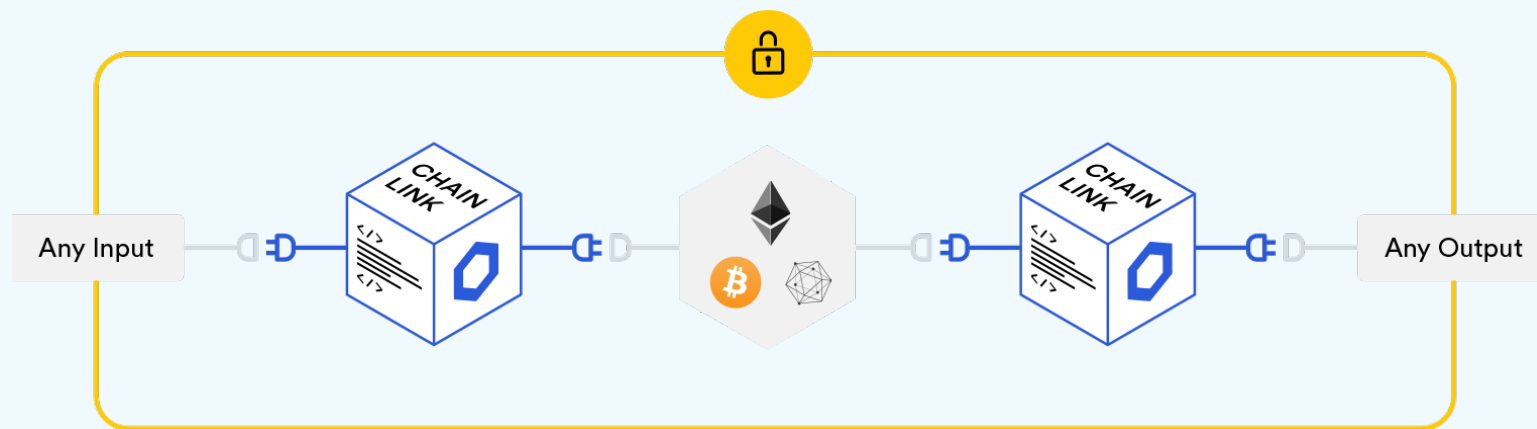


智能合约与现实世界

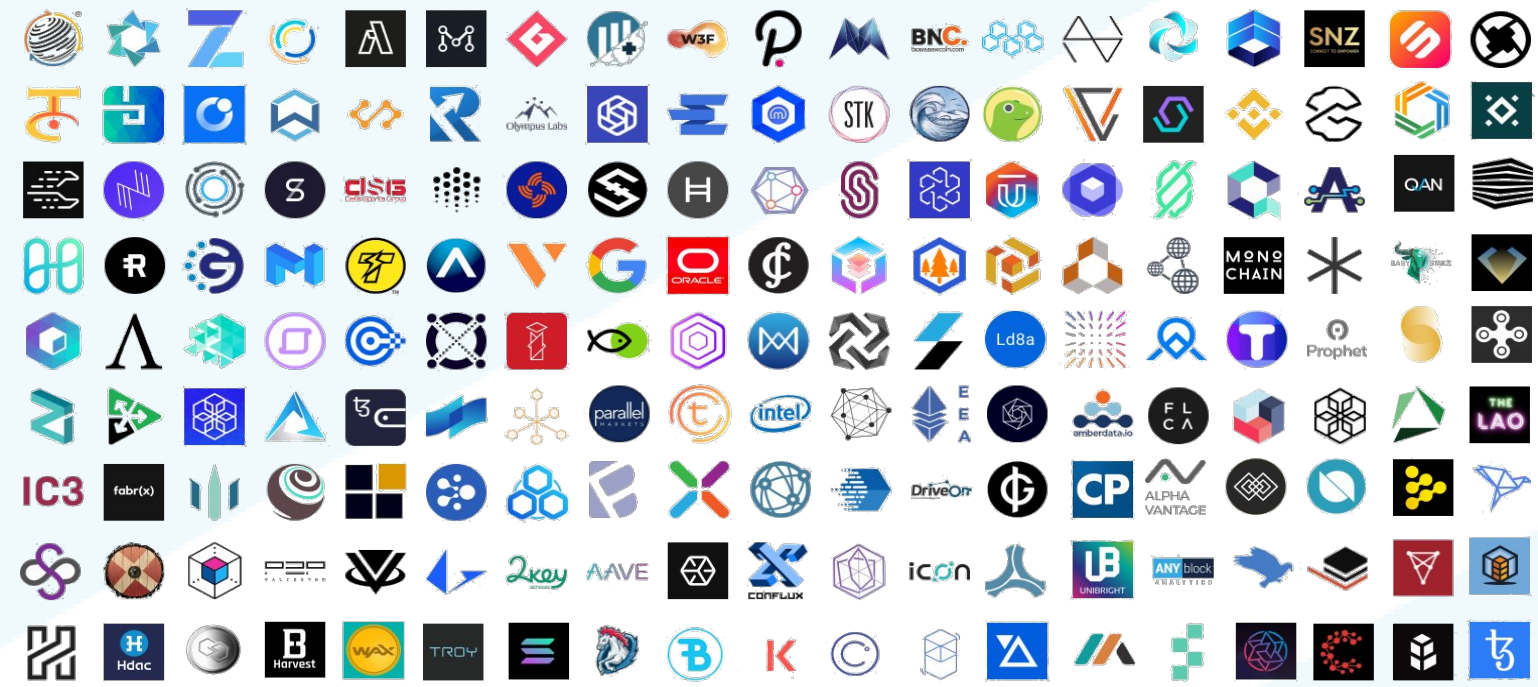
使智能合约能够用上保险安全的I / O*, 并且启动区块链之间的互通性

智能合约提供了为具有高度安全和高度可靠特质的防篡改性数字协议/合同能够被有效执行的能力。 为了维护这些数字协议/合同的整体可靠性，它们所依赖的输入和输出数据也必须是安全可靠的。Chainlink为采集外部数据提供了可靠和安全的端到端连接。



合作伙伴和客户

- 以太坊主网上的30多个价格反馈用在了14个DeFi项目上
- 100多个集成，包括 [Polkadot](#)³, [Tezos](#)⁴, [Synthetix](#)⁵, [Aave](#)⁶, [Openlaw](#)⁷, [Web3](#)⁸ 等等。
- 与 [Google](#)⁹, [Oracle](#)¹⁰, [SWIFT](#)¹¹ 等大型企业合作。
- 在许多开发框架中都可使用，特别是到目前为止最受欢迎的Truffle。
- Chainlink与 [Intel](#), [Microsoft](#), [IBM](#)¹² 和其他公司一起正在开发“Hyperledger Avalon”，以允许使用TEE（如Intel SGX）进行安全的链外计算。



平台，集成，框架，客户和合作伙伴的完整列表 <https://chainlinkcosystem.com>¹³

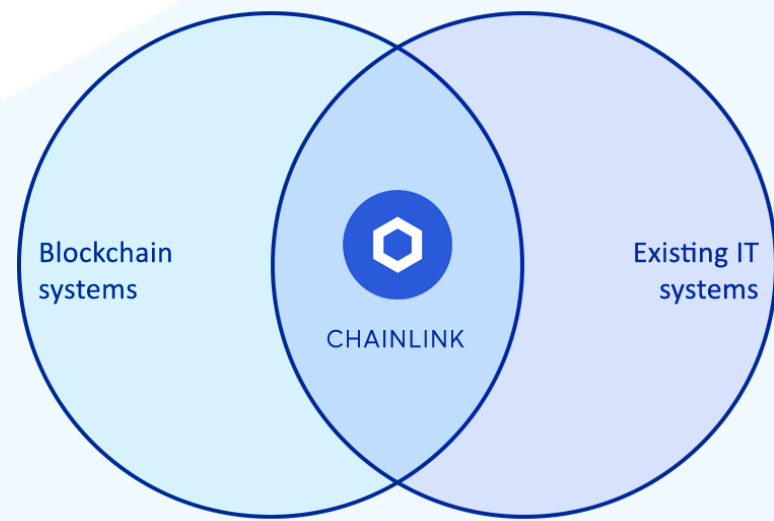
用例

能够对外部数据进行自由的采集为智能合约开启了一系列的全新功能。 互联网智能合约具有无限潜力，涉及广泛的行业：

- 货币与金融
- 付款方式
- 保险
- 供应链
- 政府
- 企业系统
- 授权和身份
- 公用事业
- 赌博

本质上，人们对以太坊充满热情时想到的几乎所有有远见的用例都取决于区块链无法获得的数据。 仅举几例：智能合约上的现实世界商品的衍生产品（[Google](#)¹⁴ 样机），基于传统交易指标（例如RSI和EMA）的自动重新平衡投资组合，市场情绪，甚至比特币的网络难度，当一个航班晚点到达时的自动保险支付，触发基于智能合约结果的通用银行转账，没有中间商的不同类型的贷款产品，将云基础设施连接到智能合约，等等。

强烈建议阅读的使用案例: [改善智能合约的44种方法](#)¹⁵



向分散的区块链馈送集中式数据是毫无意义的

Chainlink在任何区块链上提供分散，可靠和防篡改的I/Oblockchain

实现分散化

在信息源不能被完全信任的世界中，真的有可能保证真实性吗？ Chainlink通过Oracle网络实现这个目的。通过Chainlink所请求的数据是由多个独立的节点操作员使用多个数据源API传递的，它们通过激励提供正确的数据。

通过选择几个节点和数据源，可以极大的增加真实性的几率。 使用阈值签名，节点将在链外汇总其回应，以便在将最终数据点发送到链上智能合约之前达成协议。 此外，节点选择将根据于本节点的信誉和先前的工作表现。 因此，智能合约安全性的保证不仅来自于选择大量节点，而且还来自于要选择信誉良好的节点来馈送数据。 您可以在第3页中看到有关Chainlink工作原理的分步示例

LINK代币效用

LINK代币用于作为支付品和抵押品，以维护整个网络的网络安全性和激励措施。 该代币将用于：

1. 付费于节点运营商，用于向智能合约交付链下数据费用。
2. 节点操作员将用LINK代币用作抵押品以满足合同创建者的要求，去确保其节点工作正确。 恶意或无响应的节点将被削减其抵押物并降低声誉，以作为惩罚。

LINK代币是具有ERC677标准的ERC20代币。 ERC677是专门为Chainlink开发的，并集成到以太坊。 它增加了TransferAndCall功能，可在单次交易中进行付款和数据检索。

LINK是一个以太坊代币，但在最坏的情况下，它可以转移到任何区块链平台上。 Chainlink代币不仅限于以太坊。

Chainlink代币分配

固定数量的LINK代币：10亿

- 在代币初筹中售出了3亿5千万代币。
- 3亿5千万代币用于通过补贴激励节点运营商（解决了引导新网络的先有鸡还是先有蛋的问题）。
- 3亿代币转让给SmartContract Chainlink Ltd（用于持续开发，这样一来他们无需付费）。

为什么不使用以太坊而是LINK？

使用LINK而不是以太坊有几个原因：

- 将节点运营商的激励与整个Chainlink网络的良好联系在一起。
- 将安全性和带宽的经济性（抵押品为LINK）与Chainlink抵押者无法控制的外部因素隔离。
- 如果发生了重大的网络攻击，则LINK抵押品将毫无价值，直接的伤害攻击者。 但是如果用了无关资产（比如以太坊）则这个不成立。
- 稳定币将无法满足要求，因为它们要么受到法令的限制并因此而受到审查，要么依靠Oracle发挥作用。
- 对LINK代币的需求不断增长，加上供应减少（由于抵押），形成了一个积极的反馈环，在这种情况下，采用率的提高会提高LINK代币的价格，从而增加经济带宽并支持更多的采用率。
- Chainlink与区块链无关，并且需要代币才能轻松在区块链之间进行桥接。

如果LINK是ERC代币，那么它仅适用于以太坊吗？

不，任何区块链都可以轻松编写一个外部适配器来调用Chainlink。 请参阅下一节。

不可知的区块链

Chainlink支持任何区块链。 LINK是作为以以太坊代币创建的，但是Chainlink网络可以将数据提供给任何平台。

集成Chainlink的方法有两种：

1. 任何开发人员都可以创建一个简单的外部适配器，使任何区块链都可以从Chainlink节点请求和接收外部数据。 通过这种方式，LINK付款和抵押仍然在以太坊上执行
2. 通过LockDeposit合同可以将LINK代币桥接到另一个区块链，从而实现本机LINK支付，并在任何区块链上获得支持，从而使以太坊外部的应用程序可以请求数据，而无需通过以太坊。

在新的区块链中部署Chainlink合同并链接代币是一个复杂的过程，需要跨链交易支持，因此，为简便起见，一些简单的数据请求可能仍会通过以太坊进行传输。

Chainlink支持的区块链：

- 以太坊
- Tezos
- 波卡
- Hedera Hashgraph
- 任何支持EVM的区块链
- Zilliqa
- Kava/Cosmos
- 比特币
- 还有很多

自定义数据 and 安全性

Chainlink的灵活性很大程度上来自“服务协议”（SA）模型：任何开发人员都可以连接或构建满足其确切需求的Oracle网络。

定制各种参数

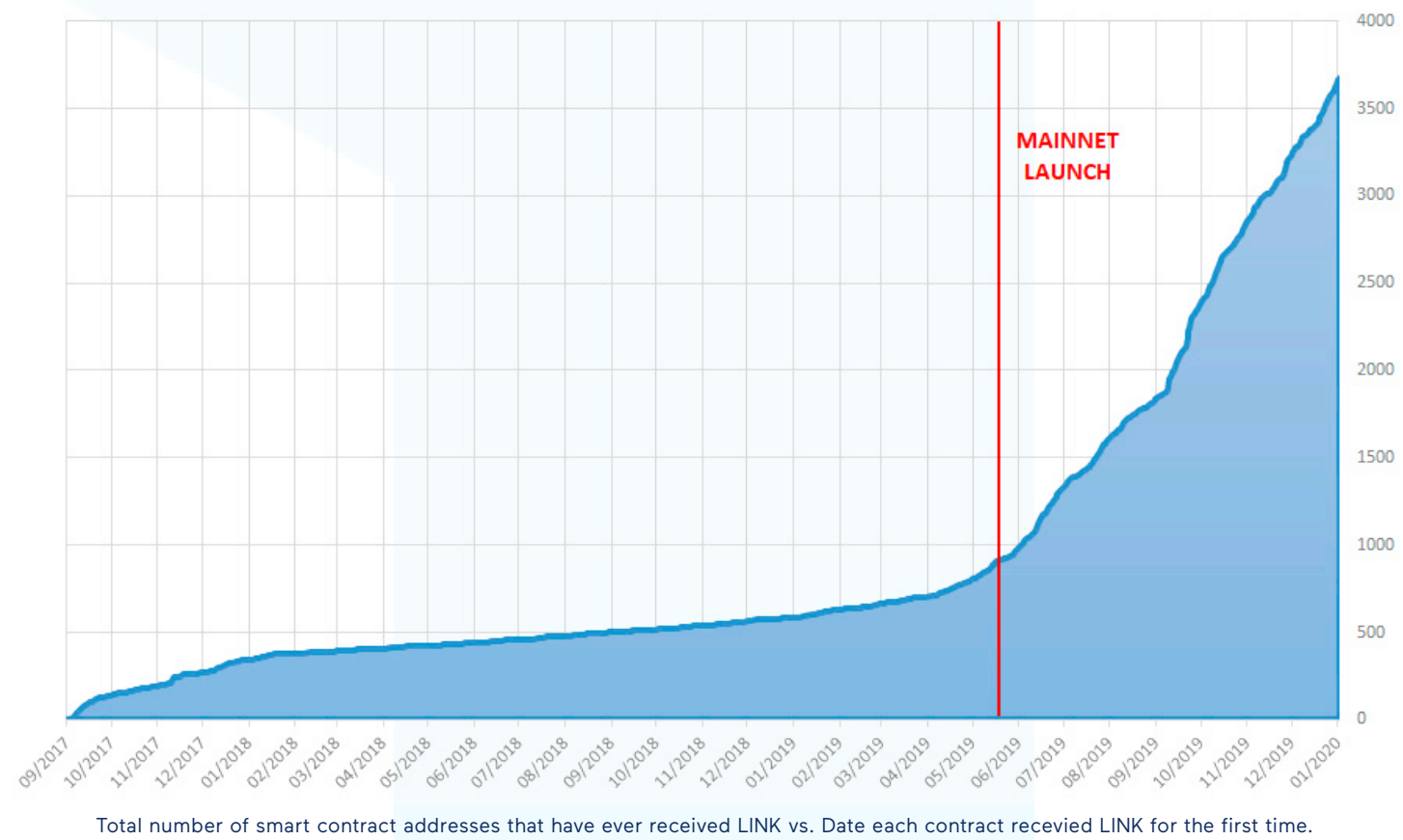
- 节点选择和节点数
- 数据源的选择和数量
- LINK节点付款金额
- LINK代币抵押要求
- 最低声誉要求*
- 削减条件
- 节点认证
- 阈值签名
- 下面有解释TEE是什么
- 混合物

节点信誉/排名*： Chainlink节点具有“声誉”因素。 Chainlink客户端将能够要求所有节点的信誉级别达到最低。 节点信誉取决于以下因素：

- 节点可用性（正常运行时间）
- 回应的正确性
- 平均回应时间
- 被分配的请求总数
- 已完成的请求总数
- 接受的请求总数
- 罚款金额
- 持有的LINK代币数量（抵押）

网络使用

Chainlink相关智能合约的增长表明网络实用程序和开发人员的兴趣增强。



* I/O代表输入/输出。 在区块链环境中，I/O代表即将输入智能合约的输入以及这些输入触发的智能合约的执行结果。

* 一个API允许程序与另一个进行沟通。 TradingView使用Binance API来获取价格/交易量数据，以将其显示在自己的网站上。 Uber构建于使用付款，GPS，SMS和KYC API。

允许或不允许，公共或私有，所有区块链和DLT都需要一个值得信赖的oracle 或预言机才能真正有用

先发优势

- 第一个分散的oracle框架。
- 与行业领导者 ([Swift](#)¹⁷, [Google](#)¹⁸, 和 [Oracle](#)¹⁹), 技术领先的研究顾问 ([Gartner](#)²⁰ 和 [Capgemini](#)²¹) 以及企业联盟 ([IC3](#)²², [EEA](#)²³, [Baseline protocol](#)²⁴ 协议和 [Hyperledger](#)²⁵) 建立了长期联系。
- 网络效应: Chainlink的大量客户端, 节点和数据源吸引了使用。

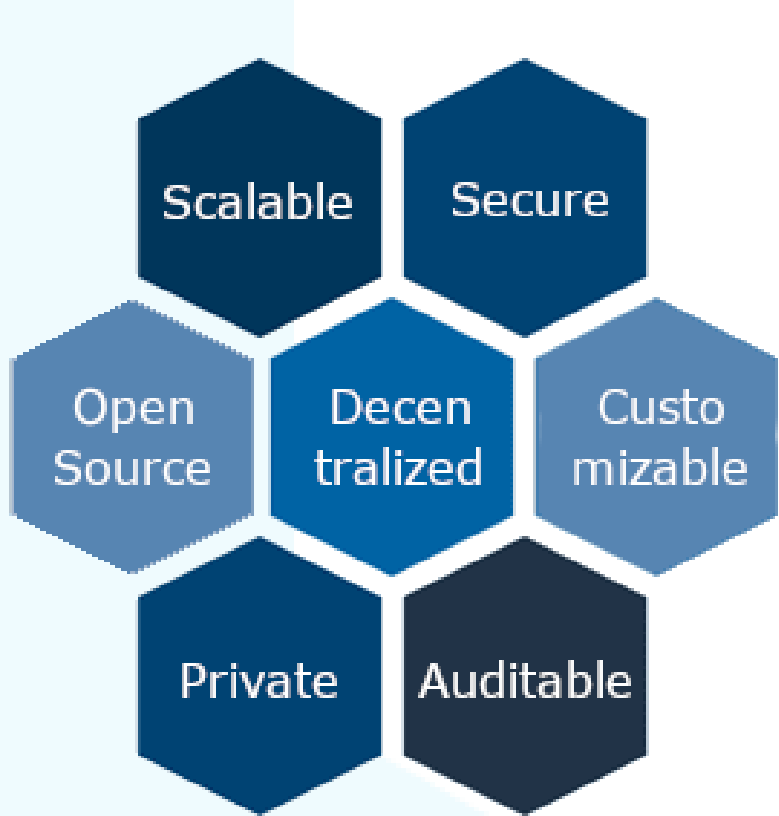
竞争者

- **直接的竞争者:** 直接的竞争者: 其它的分散性oracle只有很少使用或没有使用, 可定制性僵化, 尚未达到临界质量, 或者是自制的专用Oracle解决方案。其中包括 [Tellor](#)²⁶, [Witnet](#)²⁷, [Compound's OOS](#)²⁸, [Maker's OSM](#)²⁹, [Doracle](#)³⁰ f 其中包括 iExec的Doracle (与Chainlink集成) 和 Band.

- **间接的竞争者:** 集中式的Oracle例如 [Provable](#)³¹ 与Chainlink合作) 和 [Rhombus](#)³².

新的竞争者为争夺市场份额而挣扎, 因为他们缺乏节点和数据源的大量选择, 缺少补贴, 缺少经过时间考验的安全性, 缺少了先发优势和网络效应。

*关于竞争对手和 [‘Coinbase_oracle’](#) 的注意事项: 尽管Coinbase在这个领域是一个重要的知名参与者, 但他们提供的服务只是价格馈送 (而不是一般的oracle), 而且结果并未写在链上。因此, 不能将其视为Oracle领域的区块链Oracle或竞争对手。



开源和审核

- 代码是开源的 ([此处](#)³³).
- 可公开追踪的开发 ([此处](#)³⁴).
- 错误赏金计划 ([此处](#)^{34B})
- 4次独立审核:
 - 3在主要合同上 ([此处](#)³⁵).
 - 1在聚合器合同上 ([此处](#)³⁶).
 - 1个在Mixicles上 (进行中).

强大的社区

- Chainlink社区是加密货币空间中规模最大, 教育程度最高, 最具创造力的社区之一, 以其搞笑图和成员之间的友谊而著称。
- 通过官方 [discord](#)³⁷ 和 [gitter](#)³⁸ 直接联系到团队。
- 一个正式的Chainlink社区倡导者计划已经在全世界多个城市和大洲存在。[城市清单在此](#)。³⁹.

团队

- [团队已有25人以上](#)⁴⁰
- 6位顾问, 其中:
 - T. Gonser (DocuSign创始人)
 - [Article](#)⁴¹
 - Ari Juels ([正式化](#)⁴² Proof of Work; RSA [首席科学家](#)⁴³; IC3 [联合创始人](#)⁴⁴)
 - Evan Cheng ([Facebook](#)⁴⁵ 研发总监和 LLVM, 苹果公司作者)
 - Hudson Jameson ([以太坊基金会](#)⁴⁶)
 - Andrew Miller ([Consensus](#)研究员⁴⁷)

- [目前, 有11个职位空缺](#)⁴⁸
- 团队没有炒作, 只有专业精神。

Chainlink不会与任何区块链平台竞争, 它会改善它们

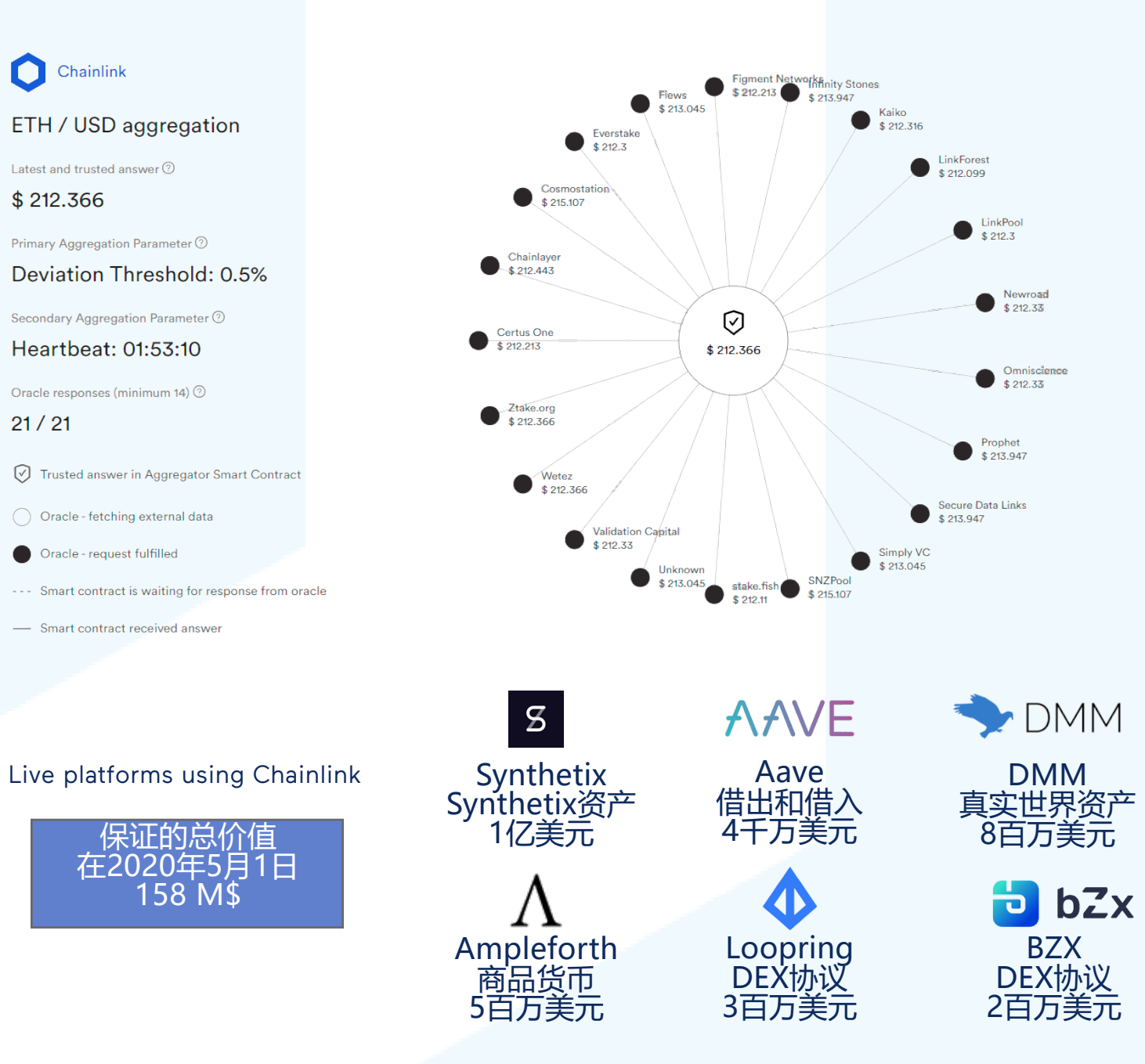
去中心化金融和Chainlink

DeFi (去中心化金融) 目前是去中心化生态系统中增长最快的板块之一。DeFi不仅包括去中心化交易所, 还包括以完全去中心化和不用委托的方式运行的借贷平台和衍生产品。

开放财务并不是要从头开始创建新系统, 而是要使现有系统民主化, 并使用开放协议和透明数据使其更加公平。传统的金融系统有一些缺点, 例如跨境汇款速度慢, 手续费高, 审查制度/歧视性 (“除非拥有100万美元, 否则您就无法投资”), 银行可以冻结资金, 甚至像在金融危机中银行可能就崩溃了。

DeFi板块的业务模型要求所有资产能够拥有100%安全, 准确的价格信息 (超过90%的DeFi需要oracles或预言机)。在DeFi中, 就像在一般情况下的金融系统, 安全性, 可靠性和信誉度对于获利同样重要。[请参阅团队强烈推荐的有关DeFi的文章](#)。⁵⁵

Chainlink当前正在提供36种资产或货币对的参考数据, 例如EUR / USD。这些价格供稿已被 [Synthetix](#)⁵⁶ (排名第二的锁定美元价值), [Aave](#)⁵⁷ (排名第五的锁定), [Ampleforth](#)⁵⁸ 和 [dy/dx](#)⁵⁹ (排名第七的) 正在使用。数据来自: [defipulse.com](#)⁶⁰, [exploring.link](#)⁶¹, 参考 [ETH/USD](#)⁶², 提供的[所有供稿列表](#)⁶³



一览Chainlink背后的技术

这些创新技术共同提供了迄今为止最先进的oracle解决方案

1. 隐私和可审核性: 混音

Mixicles本质上是一个混合器, 它使用外部Oracles或预言机为公共区块链智能合约启用了链上隐私。合同分为两个部分, 敏感数据和业务逻辑保持脱链状态, 而私人结算在链上。混合启用了:

- 加密合同业务逻辑和外部Oracle数据, 以及最终收款人结果。
- **金融合同对公众是保密的, 但可以由监管机构审核。**
- 区块链不可知论者&也可以在企业区块链中使用。
- 新一代的隐私保护和可扩展DeFi工具。

目前正在审核中。[强烈推荐这里的文章](#)。⁴⁹.

2. 低成本且可扩展: 阈值签名

阈值签名 (TS) 正在Chainlink中实现, 这使节点可以在链外批量处理其回应, 从而在最大程度降低区块链网络拥塞影响的同时降低交易成本 (gas)。

如何做到这一点? 阈值为解决Oracle难题铺平了道路: 人们希望上百, 上千, 甚至成千上万的证人就数据点达成共识, 但由于所需的交易量不断增加, 因此成本很高。

TS使oracle可以在链下彼此对话, 在某个观察上达成一致, 聚集单个签名以来证明组观察, 然后仅使用单个链上交易来响应原始数据请求。

4. 抵押品 (直接参与于游戏中)

简而言之, 放样是指在数据传输到智能合约的节点时抵押预定量的LINK代币作为抵押。

- 如果节点无法交付可靠的数据点, 比如不能及时的提供数据点或根本不交付数据, 则可以通过大幅削减其LINK抵押物来惩罚节点, 从而对节点造成经济损失。

- 当节点能够提供可靠, 及时的oracle的数据点时, 本节点可以收取LINK代币作为报酬。他们可以提取费用而保留其抵押品, 或者也可以部分/全部提取抵押品。恶意或无响应节点将被削减其抵押品, 其声誉也将因此而受到惩罚。[Article](#)⁵³.

这就是Chainlink网络激励诚实行为并惩罚节点恶意行为的方式。

Chainlink和标准化过程

Chainlink参与了多项计划, 以协调和标准化区块链技术

1. 企业以太坊联盟和Chainlink

[企业以太坊联盟 \(EEA\)](#)⁶⁴ 是一个成员驱动的标准组织, 其章程旨在制定开放的区块链规范, 以推动全球企业和消费者的协调与互操作性。自2017年以来, Chainlink与知名企业一起进入欧洲经济区。· [2020年1月, EEA成立了由Chainlink等领导的集成主网 “EMINENT”任务组](#)。⁶⁵ 该工作组的重点是为以太坊主网与企业“记录系统”集成构建开放源代码可用的参考实现和指南。换句话说, 目标是实现一个允许将业务后端 (CRM和ERP) 连接到以太坊主网的标准。



2. 准协议和Chainlink

由四大安永会计师事务所 (Ernst & Young) 与微软, Consensusys, AMD, Chainlink和其他公司合作于2020年3月提出的基准协议是一项开源计划, 结合了密码学, 区块链和开放标准方面的先进技术, 通过以太坊公共主网以低成本提供了安全的私有业务流程。该协议将为企业提供一个通用框架, 使企业之间能够进行机密而复杂的协作, 而无需在链上保留任何敏感数据。[请参阅此处的新闻稿](#)。⁶⁶.

3. Hyperledger Avalon和Chainlink

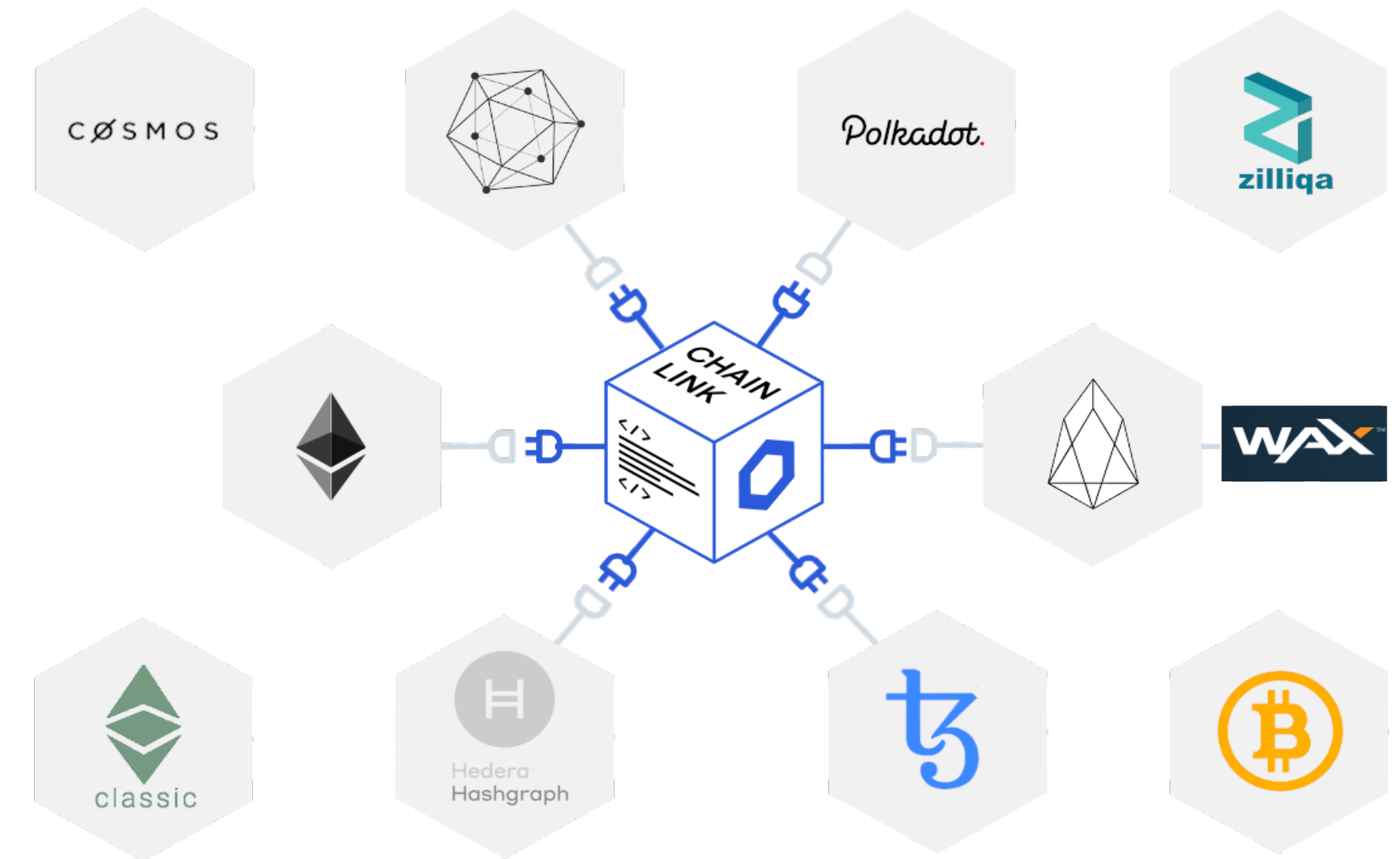
在2019年10月, Hyperledger推出了Hyperledger Avalon。它是独立账本在可信计算框架上的实现。它旨在以安全的方式将链上处理转移到链外 (云)。Avalon旨在缓解链上计算的缺点 (可伸缩性和置信度)。它减轻了链的负担, 提高了性能, 同时仍保持完整性和认证。Chainlink与其他合作伙伴 (例如IBM, Oracle, Microsoft等) 正在制定Avalon规范。英特尔新闻稿 [Intel Press Release](#)⁶⁷



一些有趣的亮点

- 根据甲骨文公司在Openworld 2020年大会上的报道，甲骨文公司将在2020年第三季度整合Chainlink。[在这里滑动。](#)⁶⁸.
- Chainlink was selected by the World Economic Forum's [Tipping point report](#)⁶⁹ as the "Shift in action" for smart contracts.
- Chainlink长期以来一直是 IC3⁷⁰ 的成员，IC3是DLT的领先学术研究计划，由Ari Juels共同创立。与Chainlink并存的IC3成员是摩根大通，微软，思科，西门子，英特尔。
- 关于ISDA（国际掉期和衍生产品协会）：2020年1月，BAPI⁷¹正式诞生了，这是一个使用标准ISDA模板，以太坊，OpenLaw，Chainlink和Kaleido等技术的双边智能衍生品平台。它是由桑坦德投资银行执行董事Carlos Matilla共同开发的。
- Chainlink目前正在与银行间消息传递的全球标准 [SWIFT](#)⁷² SWIFT在200多个国家和地区的11,000多家金融机构中得到使用，每天有超过3200万条消息移动数万亿美元。
- 2017年1月，世界经济论坛创始人兼主席克劳斯·施瓦布（Klaus Schwab）教授写了一本书，名为《第四次工业革命》。在本书中，施瓦布将SmartContract.com描述为“比特币和区块链”下“行动的转变”的转折点。[\(看这里⁷⁴\)](#).
- There are 3 types of APIs: Private, partner or public. Two require passwords. Chainlink provides data from all three. Neither the direct competitors Teller or Band can access data from private or partner APIs.
- Chainlink在美国上市的受监管交易所Coinbase，Gemini和Kraken进行交易，它们为纽约投资者提供LINK代币交易。而纽约市的金融安全法是世界上严格的法律。
- Chainlink收购了IC3的“Town Crier” oracle，目的是在本地TEE支持下扩展其去中心化oracle网络的可能性。（[《福布斯》文章⁷⁵](#) | [更多信息⁷⁶](#) | *什么是TEE?）
- Chainlink有两个主要市场：
 - 1.由LinkPool创建的[market.link](#)⁷⁷，是一个市场，这个市场让任何人都可以列出其节点，适配器及其可提供的服务。任何人都可以看到此节点列表，并可以按不同条件进行过滤。
 - 2.由CLCG创建的[honeycomb.market](#)⁷⁸，允许开发人员使用来自Certus.One，LinkForest和Cosmostation等运营商的多个高质量经过审查的Chainlink节点，将其智能合约和去中心化应用程序连接到各种高质量的付费API。免费提供Testnet API。
- 甚至像“Provable”这样的集中式Oracle也可以通过创建外部适配器并将数据作为Chainlink网络中的另一个可用来源进行数据销售，从而保持其照常销售数据的业务。因此，他们俩都通过常规的集中式方式以及通过分散的Chainlink网络销售数据来赚钱。
- 这是关于Chainlink作为一项投资的唯一说明：Chainlink在过去2.5年中一直是表现最好的加密货币。它的投资回报率比平均表现好的山寨币高1,700%，比比特币高900%。[\(看这里⁷⁹\)](#).

Chainlink已经支持的区块链



任何输入。任何输出。任何区块链



Connect to any source of data feed / API

Public/private blockchains can support Chainlink

Send payments anywhere Connect to backend systems

通过示例和常见问题解答演示Chainlink

Chainlink工作原理的一个示例 (有抵押)

1. 鲍勃（Bob）需要提供非信托化的数据给他的智能合约，因此他查询Chainlink。
2. 然后，Bob使用合同指定一定数量的Chainlink节点，该合同规定它们必须满足至少一定数量的先前交易，准确性的百分比，并要求每个单独的节点将一定数量的LINK代币作为罚金来放样。确保他们将履行合同的期限
3. Bob还设置了他愿意支付多少LINK代币作为数据检索费用
4. 现在，所有符合Bob规格的Chainlink节点都将成为其合同的oracle或预言机。然后，Bob将选择要求最低LINK代币金额作为交易费用的oracle或预言机。
5. Bob的选定节点提供了他们的数据，并且答案由Bob选定的汇总合同汇总。现在，Bob的智能合约会获取此数据，并向每个节点支付LINK代币，并且会向所有数据与共识不一致的节点收取罚款。
6. 诚实正确的节点现在拥有更多的LINK代币，它们现在可以保留这些LINK代币以用于将来的罚款支付，也可以在市场上出售。

两个重要注意事项:

- 一旦Mixicles生效（目前正在审核），合同业务逻辑，外部oracle数据和最终收款人结果都将会被保密，但同时仍可供监管机构审核。
- 阈值签名生效后，无需每个节点在链上写入响应（高成本，网络阻塞），它们将达成链下共识，并仅在一项交易中写入结果。

常见问题/答案

- 1. 节点排名和抵押是否相同？**
不，每个节点都有一个根据其过去表现确定的排名（声誉）。抵押是此之上的附加度量标准，用户在选择要请求的节点时会考虑到该度量标准。拥有更多可用于抵押的LINK代币可以增加节点正确性的可能性，但是节点的排名也是其中一个因素。
- 2. 持有大量LINK代币不会自动将您的节点排在首位吗？**
不，节点排名考虑了声誉的多个因素（请参阅# 3），LINK代币抵押数量是与其他因素一起考虑的参数之一。
- 3. 节点排名考虑哪些因素？**
这取决于多种因素：正常运行时间，响应的正确性/准确性，已分配/已接受/已完成/已拒绝请求的总数，平均响应时间，大幅削减历史记录和抵押的LINK代币数量。ed.
- 4. LINK代币抵押已经实现了吗？**
还没有，它可能会在其他主要功能（例如mixicles和阈值签名）之后出现。如今的网络受到节点信誉和因为恶意而引起未来收入损失的机会成本的保护。Chainlink核心团队还通过代币销售筹集的资金对oracle网络进行补贴，以确保节点的正确响应，并确保在网络的早期运行节点在经济上是可行的。
- 5. 抵押有什么回报？**
根据节点的等级（请参阅第3点），信誉，抵押的LINK代币数量以及收到的服务要求数量，会影响到节点之间的差异。节点响应越可靠，准确性和敏捷性越高，工作量会越大，可收取的费用会越高，它们更有可能在所抵押的LINK代币上产生更高的回报。
- 6. 是否会有只需要零抵押的合同？**
有的，合同可以要求放任何数量的LINK代币（包括零）（请参阅第1页的“自定义数据和安全性”一节）。抵押金额只是请求者在其服务协议中可能需要的一个因素。由请求者决定要为一个服务作业放样多少LINK代币，并且由节点决定他们愿意接受哪些服务作业。