Chainlink

Chainlink 预言机简介

Building Web3 Together

Frank
开发者关系工程师
Chainlink Labs

Web3 - 数据所有权

Web 1.0

READ ONLY

静态，只读

Web 2.0

READ-WRITE

中心化，可参与

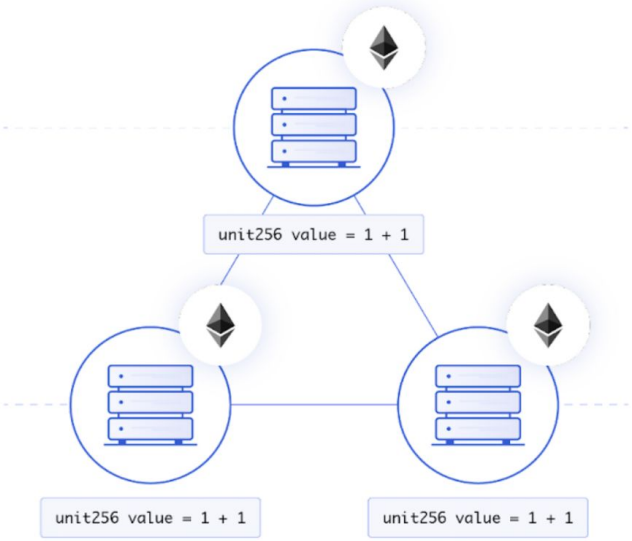
Web 3.0

READ-WRITE-OWN

数据可拥有

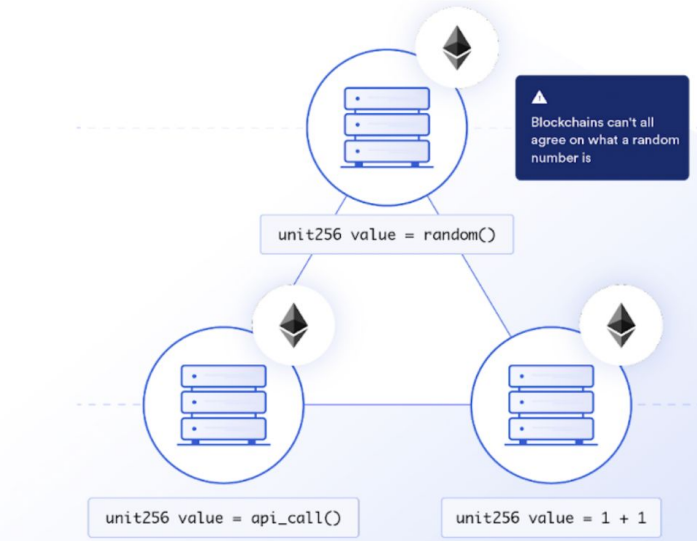
确定性系统的缺陷

确定性操作



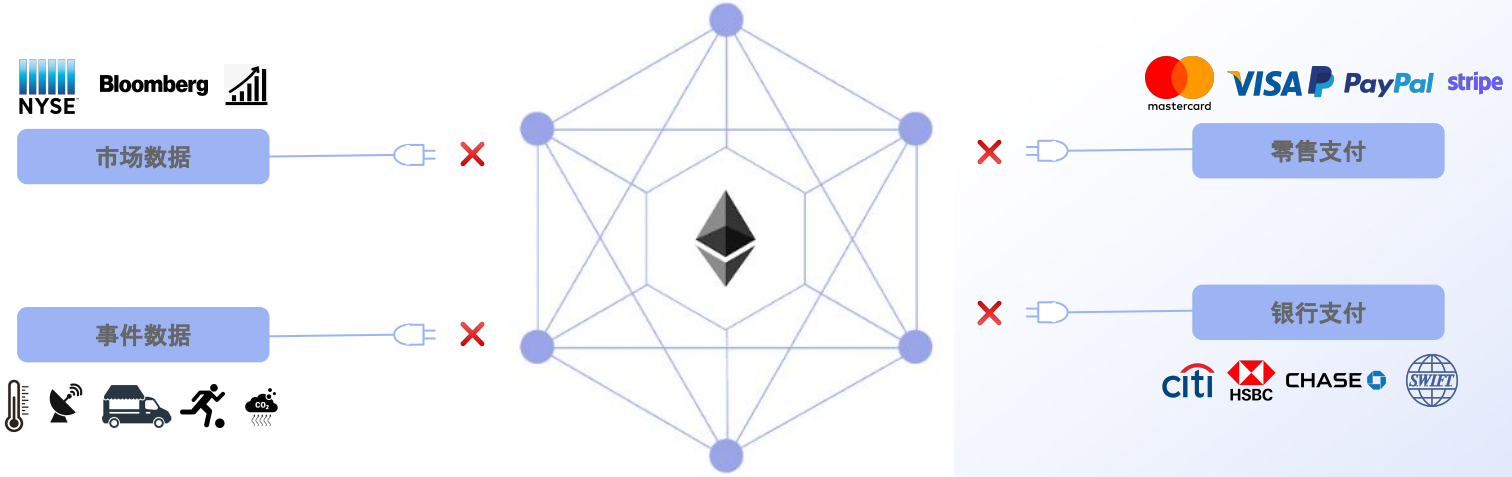
Consensus reached

非确定性操作

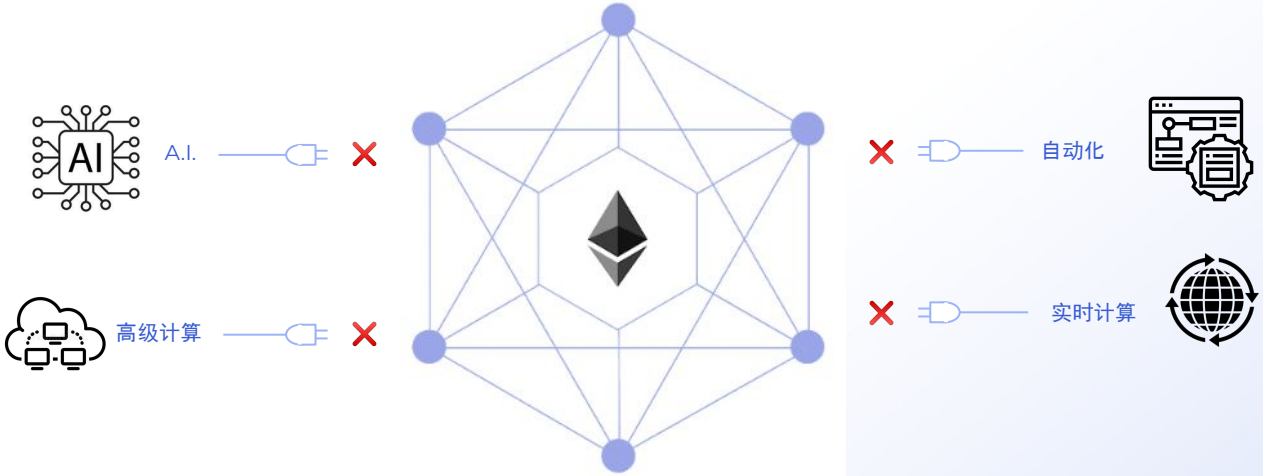


Consensus not reached

#1 区块链无法连接 Web2 的数据



#2 区块链无法承载多种类型的计算



dApp 需要涉及到链下数据与计算

DeFi

资产(on L1)

智能合约逻辑 (on L2)

市场数据

Gaming

高级计算

智能合约

支付数据

保险

自动化服务

事件数据

保险智能合约

Web2 接口 (网站&SMS)

资产通证化

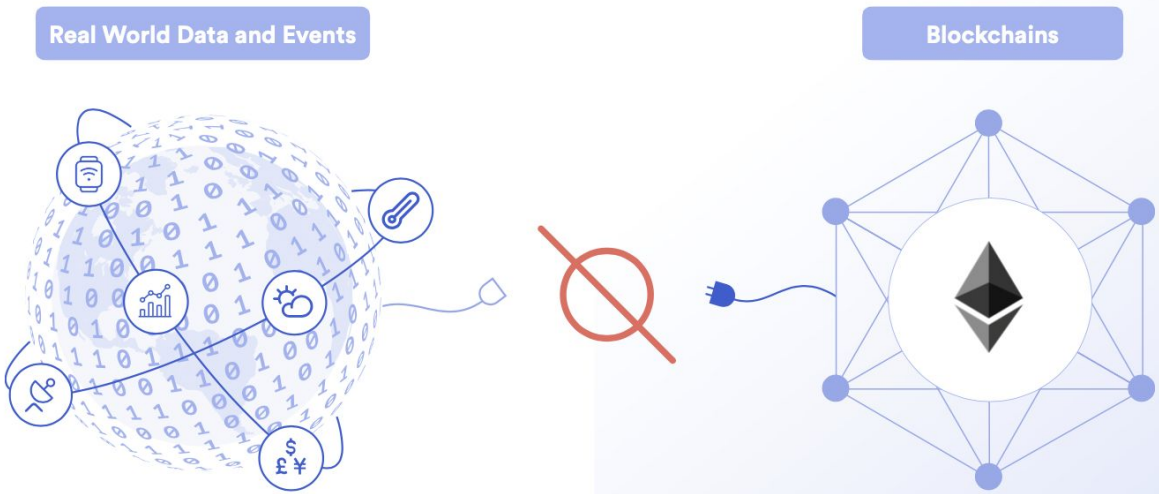
支付数据

智能合约逻辑 (on L1)

智能合约逻辑 (on L1)

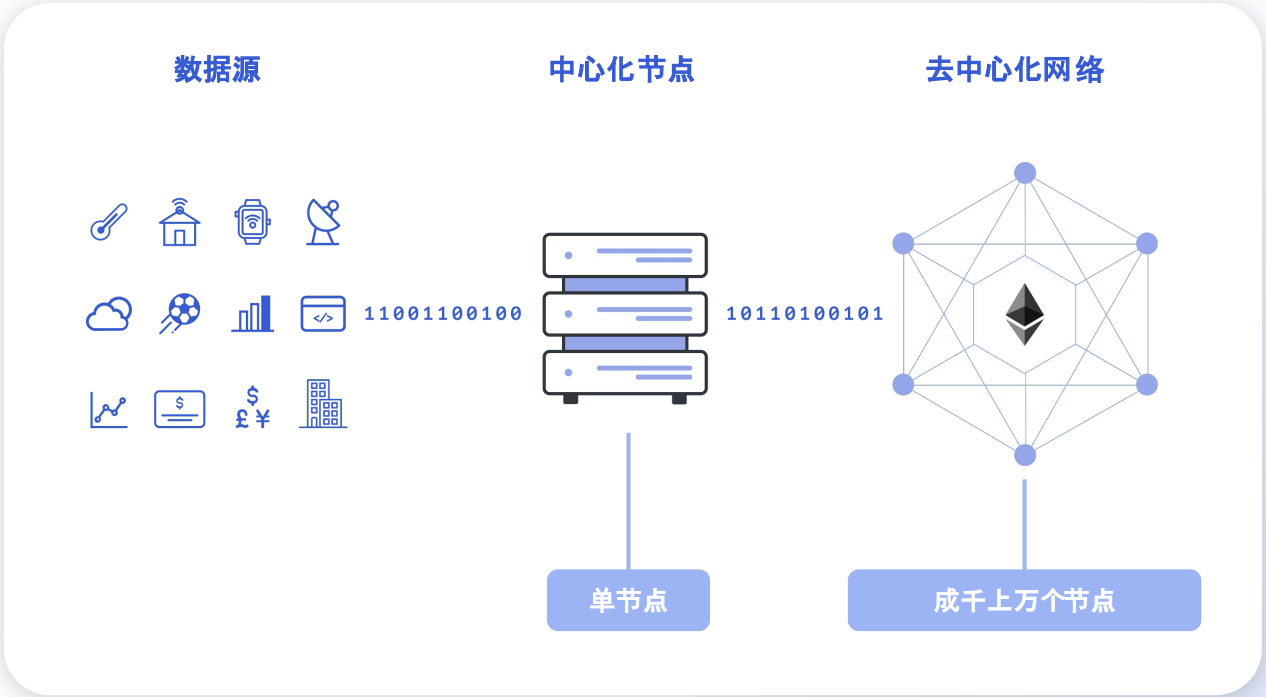
预言机问题

区块链是一个**孤立的，确定性**系统。无法**主动**从链下**获取数据**



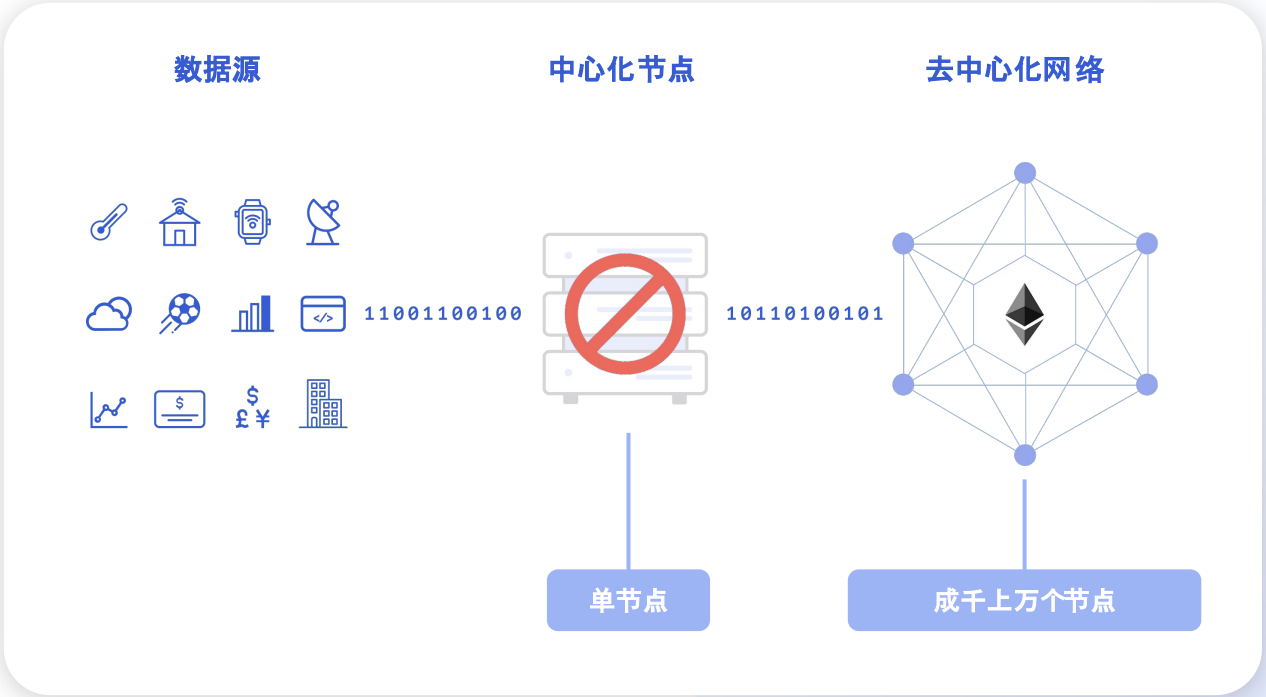
Chainlink

中心化预言机



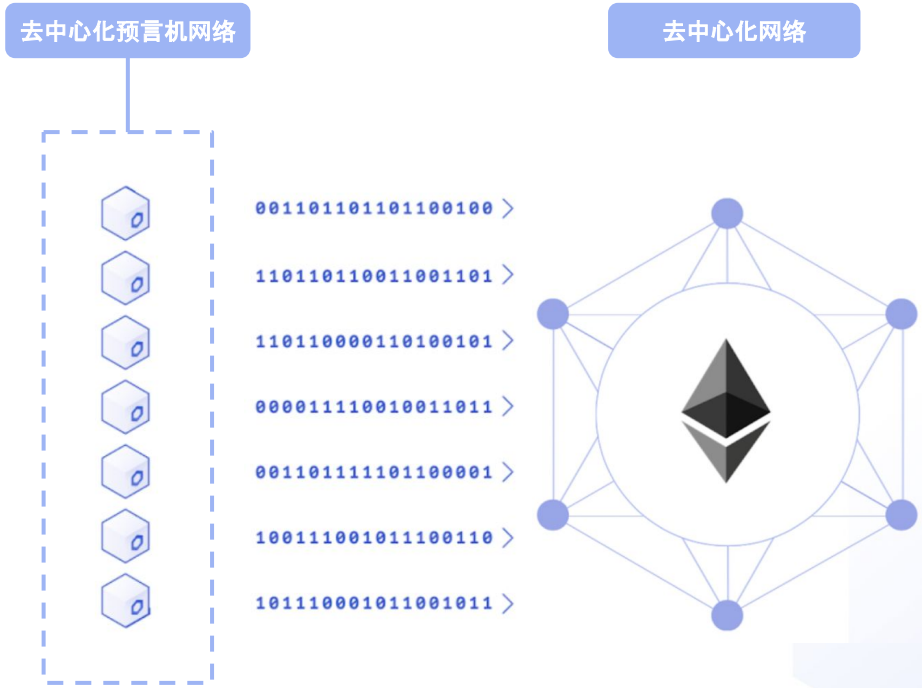
Chainlink

单点失败风险



Chainlink

去中心化预言机网络(Decentralized Oracle Network)



去中心化预言机网络(DON)

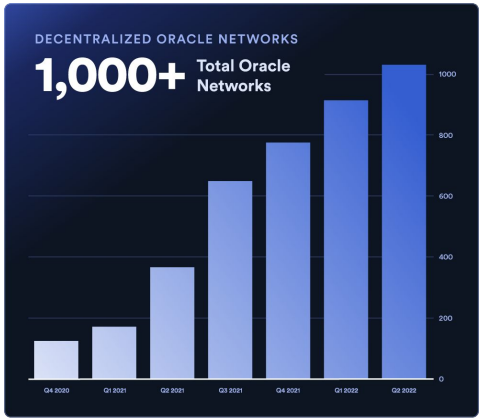
每个预言机节点通过自身的数据源收集数据，共识后提交给区块链上的智能合约：

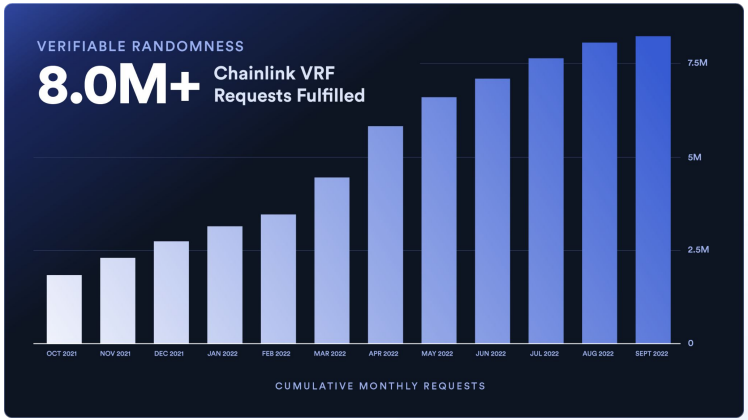
1. 技术上，避免了单点失败风险
2. 数据上，避免数据被单个参与方控制

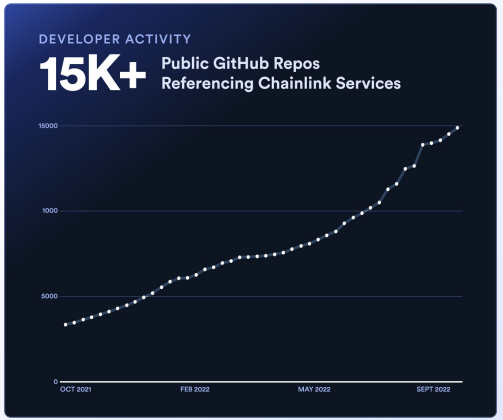
Chainlink


Web3 应用开发者
需要用到多链，合约，资产和其他 Web2 资源
Chainlink Web3 服务
数据
计算
跨链
去中心化预言机网络（Decentralized Oracle Network）
区块链（L1/L2）
合约 & 资产
Web 2
数据，应用 & 企业已有系统

预言机使用趋势







Chainlink


Web3 应用开发者
需要用到多链，合约，资产和其他 Web2 资源
Chainlink Web3 服务
数据
Feed | Any API | Proof of Reserve | DECO
计算
VRF | Automation | FSS
跨链
CCIP | Token Bridge
去中心化预言机网络（Decentralized Oracle Network）
区块链（L1/L2）
合约 & 资产
Web 2
数据，应用 & 企业已有系统

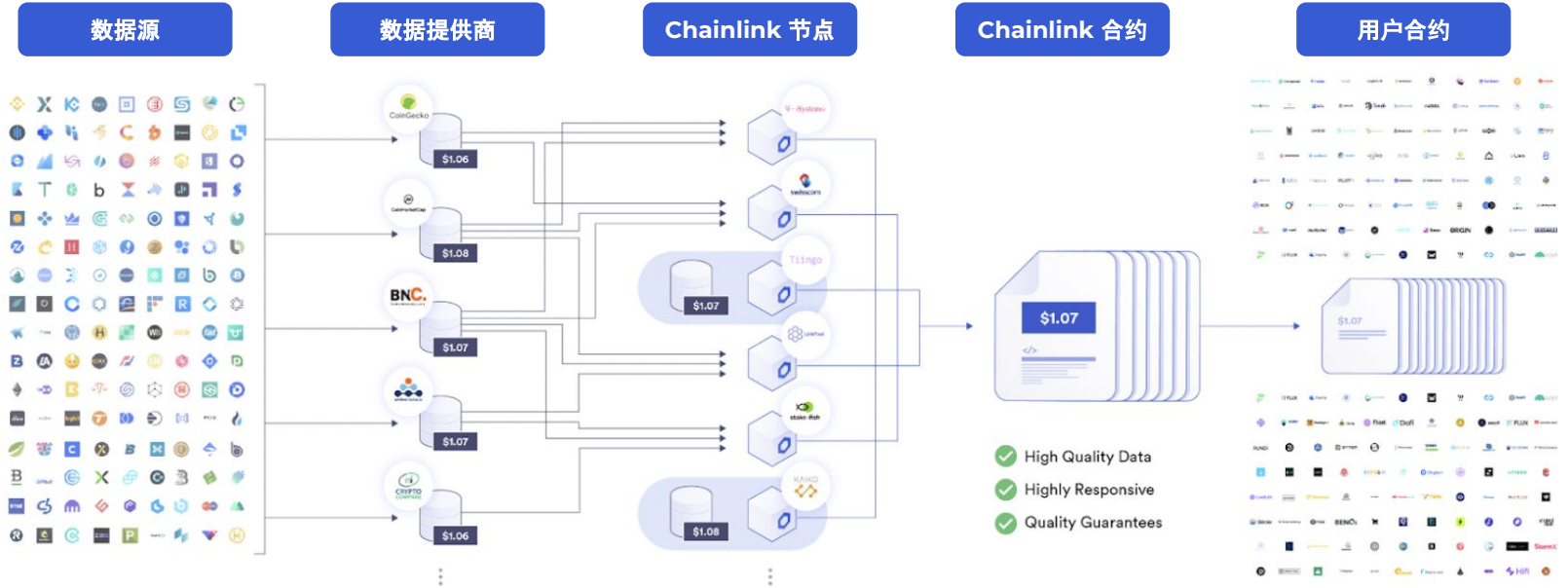
Chainlink

Chainlink 预言机数据服务

Data Feed - 喂价

Chainlink

Data Feed 业务流程



Chainlink

Data Feed 用户案例

借贷 (Lending & borrowing)

Issue and settle loans, liquidate undercollateralized positions, trigger collateral swaps, and help protect against insolvency.

AAVE · Compound · venus

合成资产 (Mirror Asset)

Generate mirrored versions of real-world and on-chain assets using on-chain collateral and Price Feeds as the reference point for minting and redemption.

SYNTHETIX · opium · ALCHEMIX

Stable Coin

Use financial market data to determine the collateralization of stablecoins, automate mint/burn operations, and trigger rebasing functions.

Liquity · Fei Protocol · Ampleforth

资产管理 (Asset management)

Enable the automated management of capital pools and the marking of funds to market by referring to Price Feeds for rebalances.

Set · Nexus Mutual · VISOR

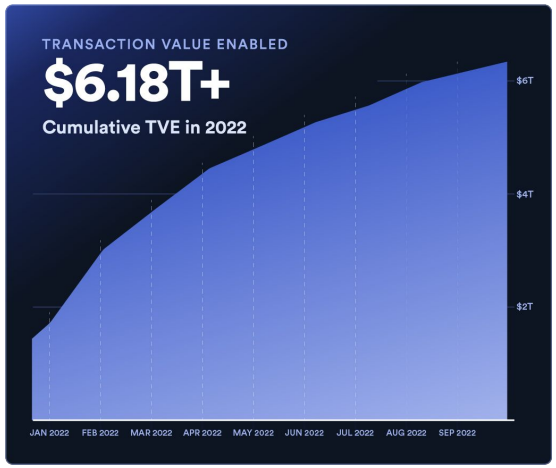
衍生品交易 (Option and Future)

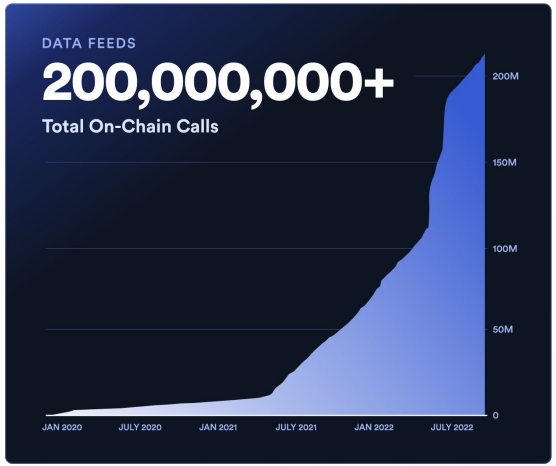
Power advanced financial instruments and ensure platform solvency by dynamically setting the funding rate and settling agreements.

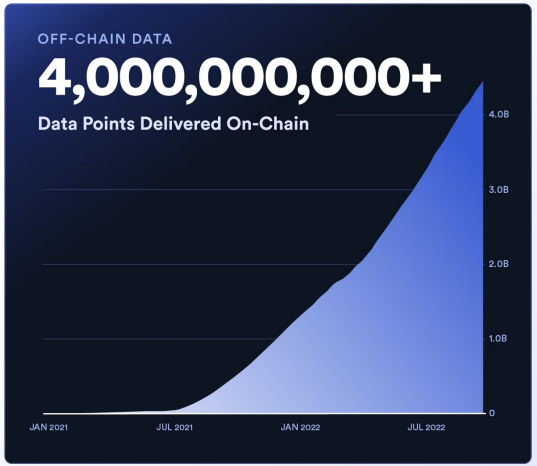
dYdX · Lyra · THALES

Chainlink

Data Feed 使用趋势

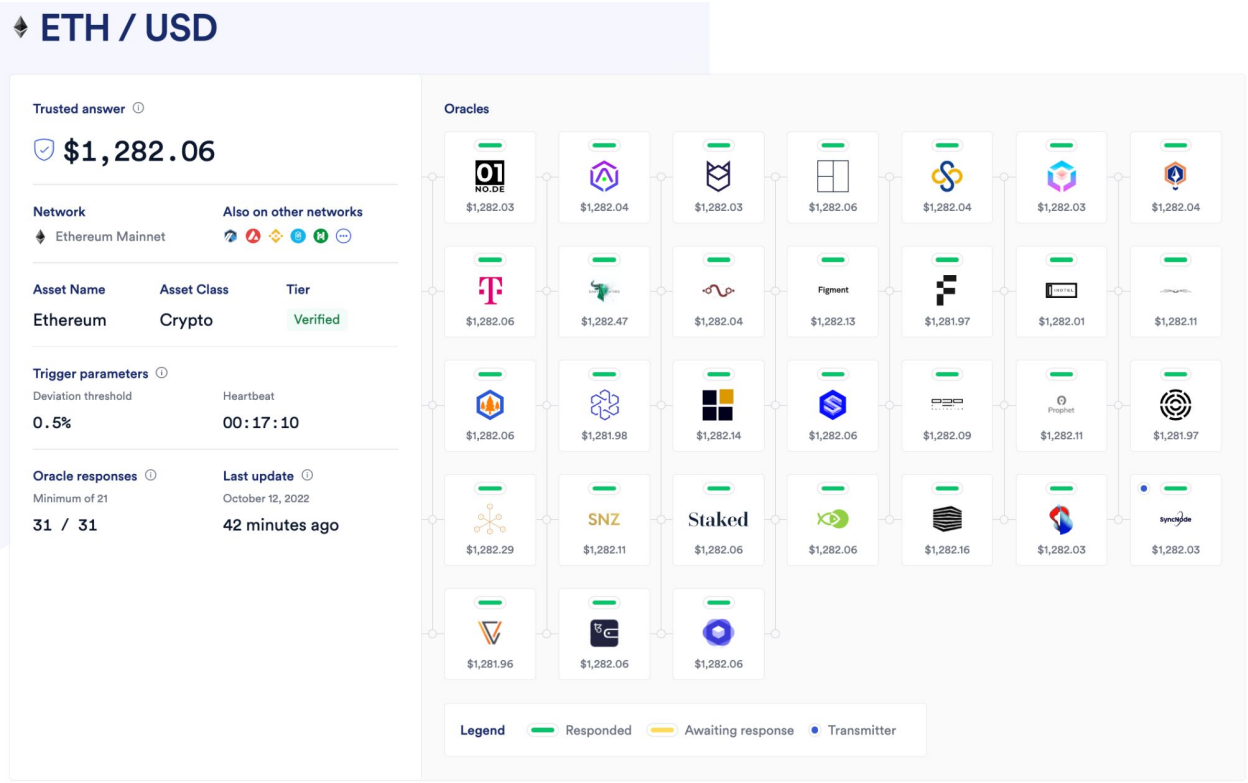






Chainlink

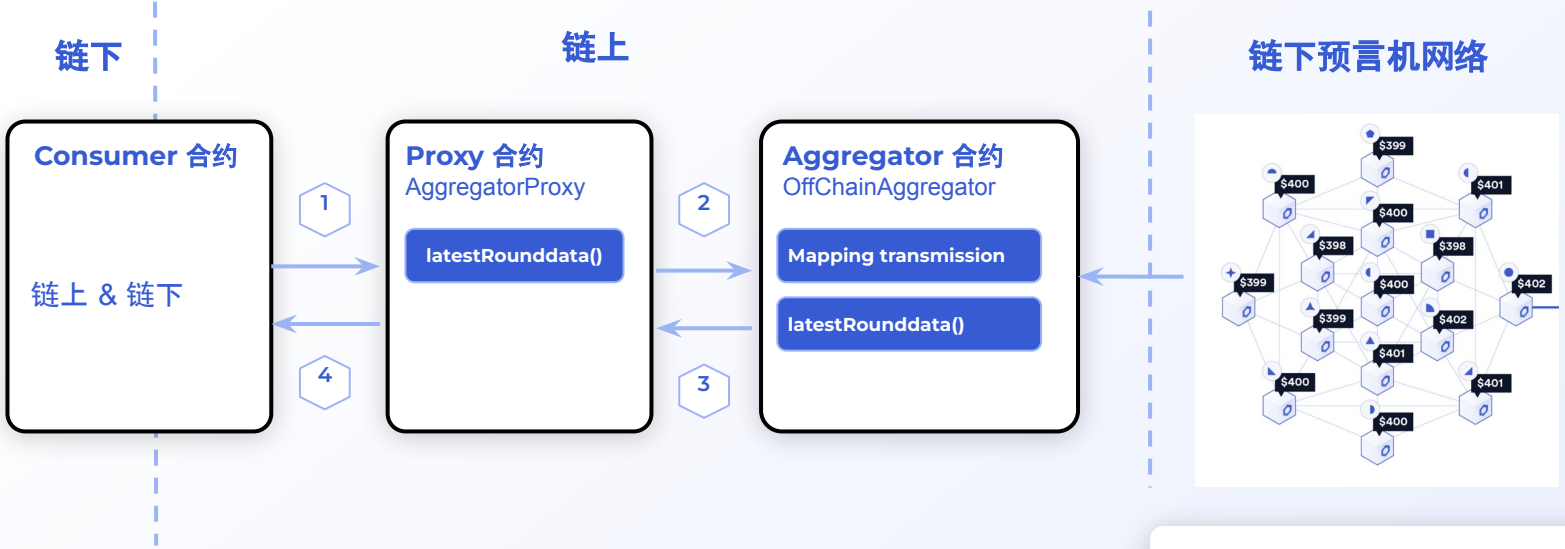
Data Feed - ETH/USD



Data Feed 应用页面：
https://data.chain.link/

查看多条链上多个交易对的价格以及节点的具体信息

Data Feed 技术架构



1. **Consumer** 调用 **Proxy** 合约函数 *latestRoundData()*
2. **Proxy** 调用 Aggregator 合约函数 *latestRoundData()*
3. **Aggregator** 返回 *Transmission* 结果给 Proxy
4. **Proxy** 返回结果给 **Consumer**

Chainlink 预言机网络更新触发条件

1. 每 30 分钟会更新一次
2. 通证价格波动超过 0.5%

Chainlink

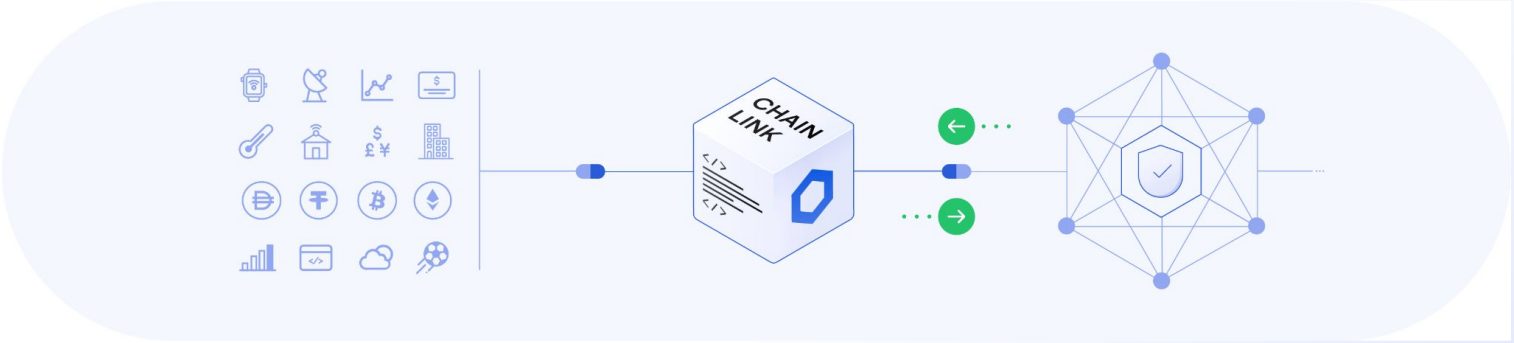
Chainlink

Chainlink 预言机数据服务

Any API - 获取任意 API 数据

Any API 业务流程

开发可以把所有 Web2 的数据，引入到 Web3 dApp 中，并且只需要几行代码就可以实现。

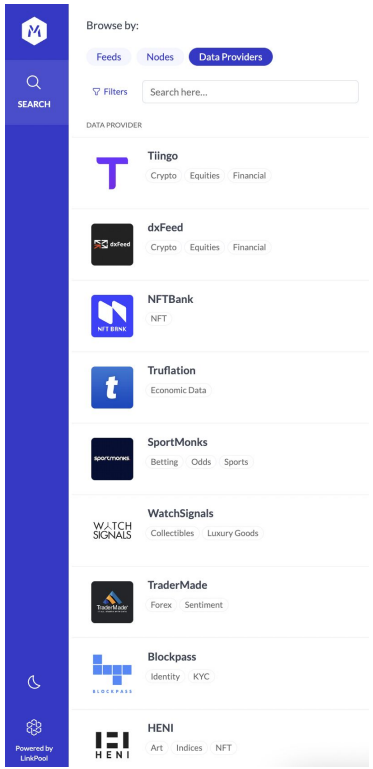


自定义数据源：市场，事件，金融以及支付数据的 API

Chainlink 节点

dApp 请求

Any API - 数据市场



United States of America	United Kingdom
Truflation CPI US Index	Truflation CPI UK Index
Truflation CPI US Food Category Index	Truflation CPI UK Food Category Index
Truflation CPI US Food @ Home Sub Category Index	Truflation CPI UK Housing Category Index
Truflation CPI US Food Away from Home Sub Category Index	Truflation CPI UK Transportation Category Index
Truflation CPI US Housing Category Index	Truflation CPI UK Utilities Category Index
Truflation CPI US Rented Housing Sub Category Index	Truflation CPI UK Health Category Index
Truflation CPI US Transportation Vehicle Purchase Sub Category Index	Truflation CPI UK Alcohol & Tobacco Category Index
Truflation CPI US Transportation Used Vehicle Purchase Sub Category Index	Truflation CPI UK Clothing Category Index
Truflation CPI US Transportation Gasoline Sub Category Index	Truflation CPI UK Communications Category Index
Truflation CPI US Utilities Category Index	Truflation CPI UK Education Category Index
Truflation CPI US Health Category Index	Truflation CPI UK Recreation & Culture Category Index
Truflation CPI US Household Durables Category Index	Truflation CPI UK Misc Category Index
Truflation CPI US Alcohol & Tobacco Category Index	
Truflation CPI US Clothing Category Index	
Truflation CPI US Communications Category Index	
Truflation CPI US Education Category Index	
Truflation CPI US Recreation & Culture Category Index	
Truflation CPI US Misc Category Index	

Any API 应用页面：
https://market.link/

查看不同的数据提供商所提供的关于股票数据，事件型数据，宏观经济数据，身份数据等等。

Chainlink

Any API 使用场景

Any API 可以增加你的应用可能性

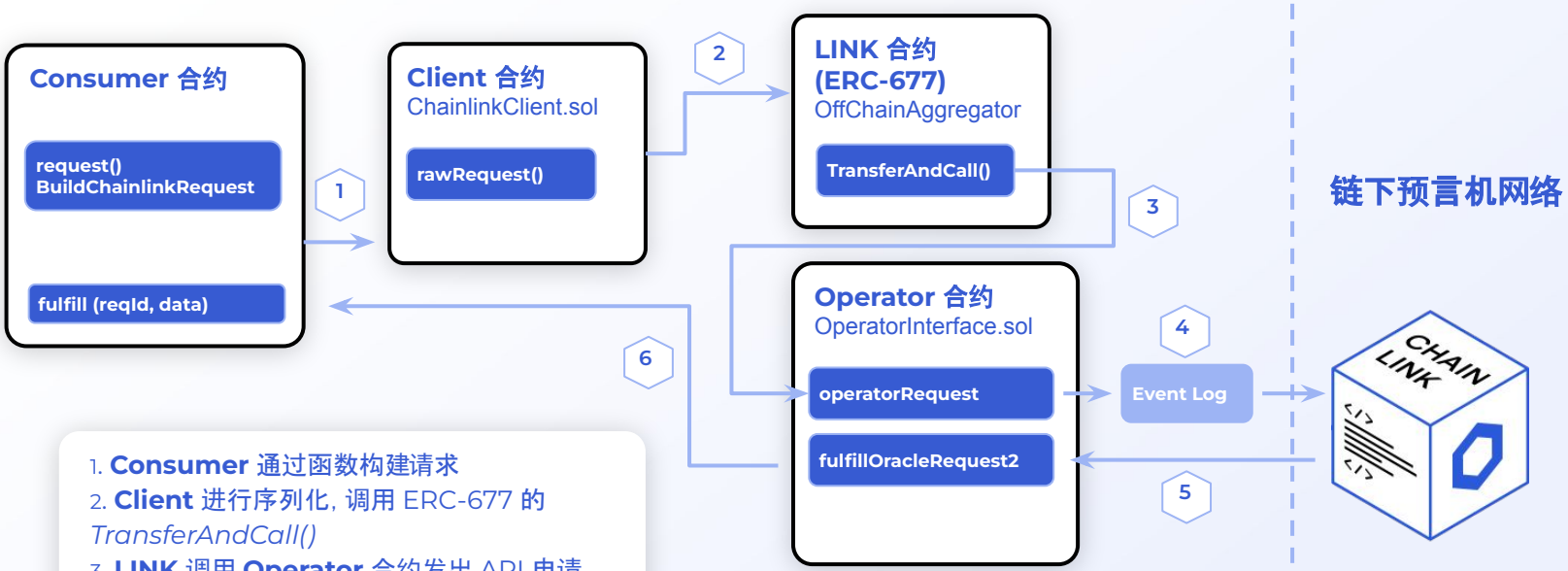
天气以及航班延误数据：为保险应用提供必要的数据参数

温室气体排放数据：提供碳资产市场所需要的数据

选举以及体育比赛数据：预测市场以及动态 NFT

资产以及宏观经济数据：为资产提供更多的流动性

Any API 技术架构



1. **Consumer** 通过函数构建请求
2. **Client** 进行序列化，调用 ERC-677 的 *TransferAndCall()*
3. **LINK** 调用 **Operator** 合约发出 API 申请
4. **Operator** 将请求写入 EventLog
5-6. **预言机节点**获得请求并且将数据写回到 Consumer

Chainlink


Web3 应用开发者
需要用到多链，合约，资产和其他 Web2 资源
Chainlink Web3 服务
数据
Feed | Any API | Proof of Reserve | DECO
计算
VRF | Automation | FSS
跨链
CCIP | Token Bridge
去中心化预言机网络（Decentralized Oracle Network）
区块链（L1/L2）
合约 & 资产
Web 2
数据，应用 & 企业已有系统

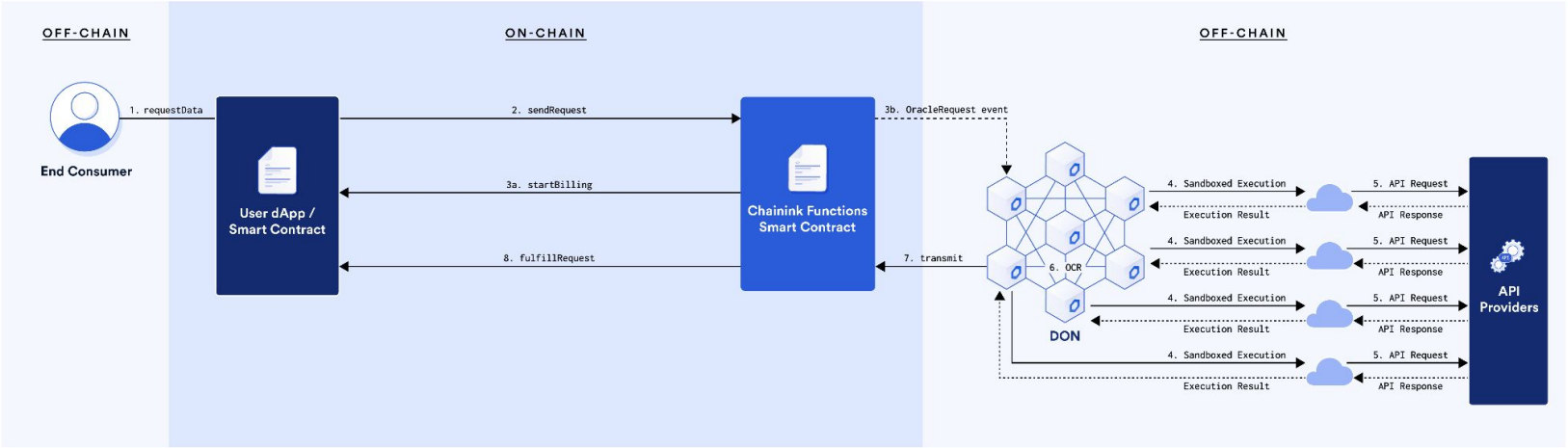
Chainlink

Chainlink 预言机网络

Functions

Chainlink

Chainlink Functions 业务流程



1. An end user initiates the Chainlink Function embedded within the dApp.

2. The dApp makes an request to the Chainlink Functions smart contract. This request consists of the API endpoint, any transformations to the data, and encrypted credentials (if any).

3. A decentralized oracle network (DON) continuously listens to the Chainlink Functions smart contract. When it picks up the request, each node independently triggers their runtime environment to fetch external data, performs any computations on it, and returns the result.

4. The nodes reach a consensus on the final answer using OCR 2.0. One node is then picked to transmit the result back on-chain. In the unlikely event that the node fails to publish the data, another node is chosen to transmit it on-chain. The end result is high reliability and trust-minimized security.

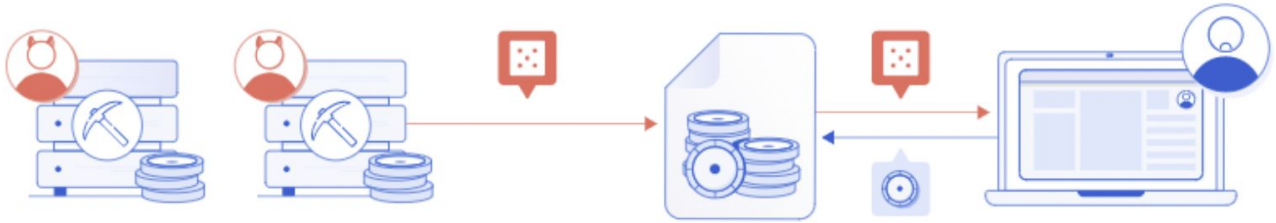
Chainlink

Chainlink 预言机计算服务

VRF - 可验证随机数

Chainlink

随机数生成器(RNG)- 链上方案



1 恶意矿工选择性打包交易

随机数函数的方案，所以依 赖的随机数，比如说区块哈希有可能被 矿工操纵

2 合约中的随机数生成被所操纵区块影响

被操纵的随机数会影响到智能合 约输入，进而又可能导致用户资产的损失

Chainlink

可验证随机数函数（VRF）

可验证随机数（VRF）定义：

In cryptography, a verifiable random function (VRF) is a public-key pseudorandom function that provides proofs that its outputs were calculated correctly.

1. **可证明性（Provability）**
2. **独特性（Uniqueness）**
3. **伪随机性（Pseudorandomness）**

VRF 的 3 个函数：

1. **密钥生成函数（Key Gen）**

   G(r) => (PK, SK)

   PK：public key，公钥

   SK：secret key，密钥

2. **随机数生成函数（Evaluate）**

   E(SK, seed) => (Randomness, Proof)

   seed：RNG的种子

   Randomness：随机数

   Proof：证明

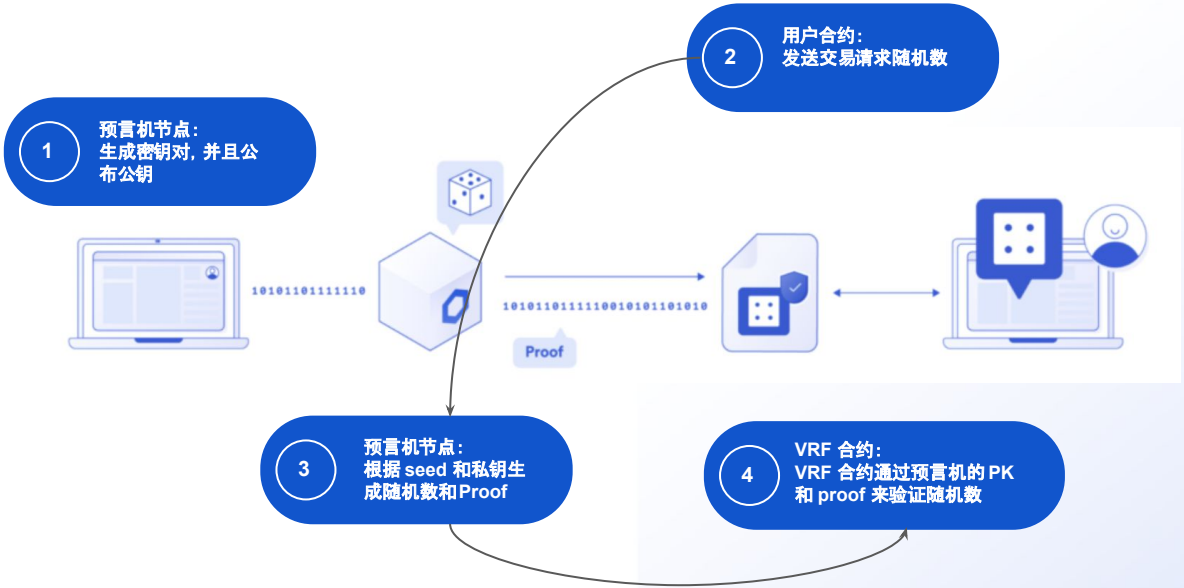
3. **验证函数（Verify）**

   V(PK, seed, Randomness, Proof) => (true or false)

   true：验证成功

   false：验证失败

Chainlink VRF 业务流程



Chainlink

Chainlink VRF 使用场景

NFT 创建和分发（NFT Creation & Distribution）

- 通过 VRF 给要生成的 NFT 分配随机属性
- 给 NFT collection 参与者随机分配稀有NFT

公平抽奖（Fair selecting）

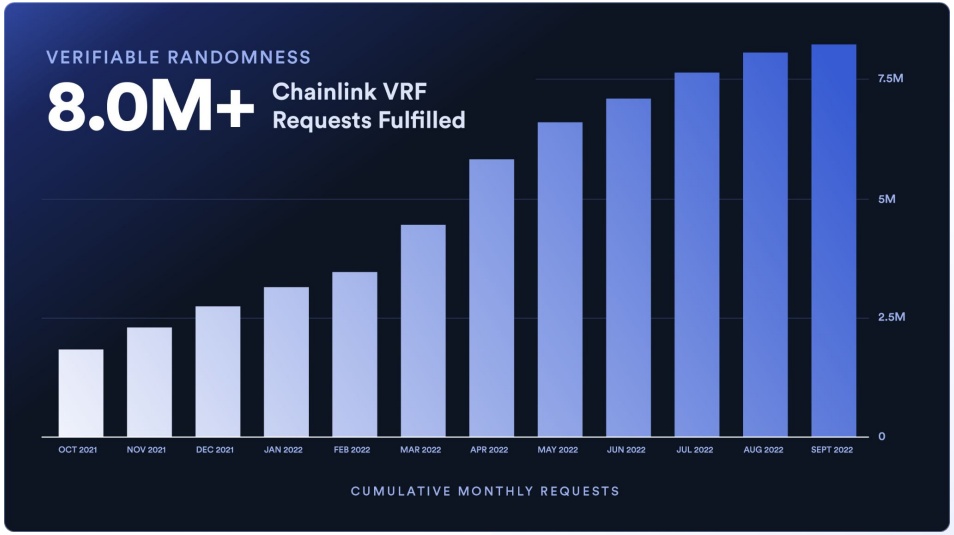
- 给孵化项目的参与者发放白名单

查看 35 个应用场景

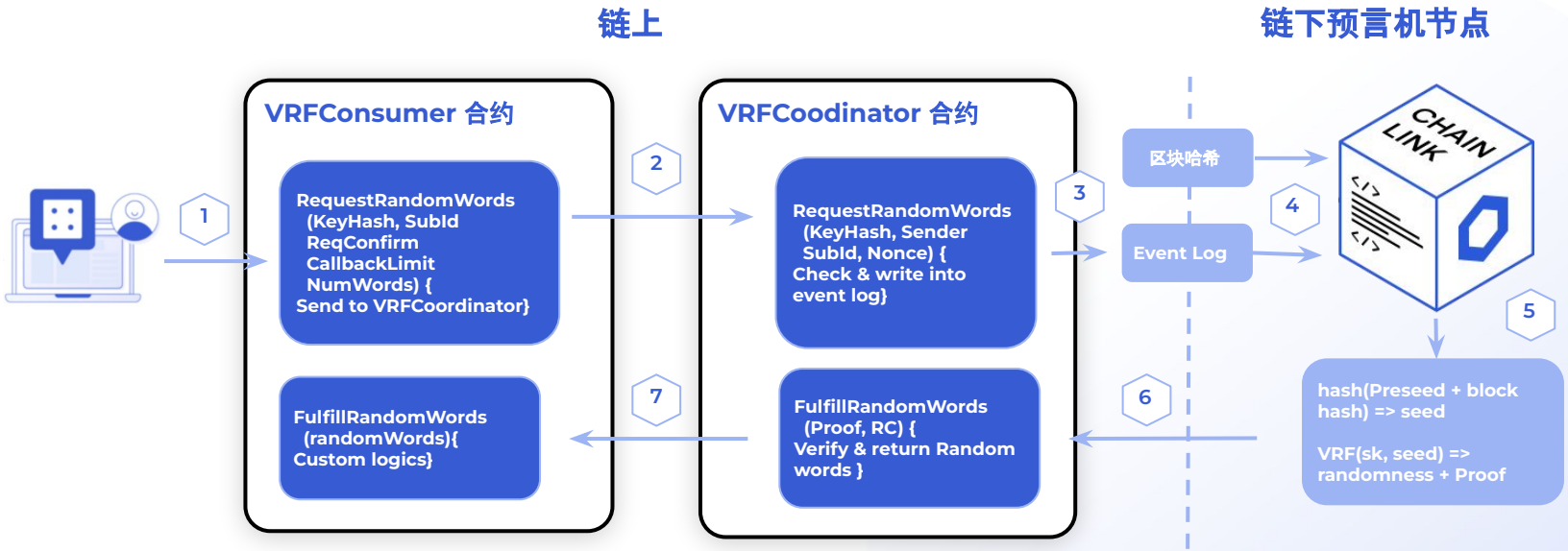
https://blog.chain.link/blockchain-rng-use-cases-enabled-by-chainlink-vrf/

Chainlink

在过去的 12 个月增长了 440%



Chainlink VRF 技术架构



1. 调用 Consumer 合约的函数请求随机数
2. 用户合约调用 Coordinator 合约的函数请求随机数
3. 将 PreSeed 写入 Event log
4. 预言机读取 Event log 中的 PreSeed 和 blockhash
5. 预言机通过 VRF 生成随机数和 Proof
6. 预言机将 rc 和 proof 写入 Coordinator
7. Coordinator 进行验证 & 将随机数写入 Consumer 合约

Chainlink

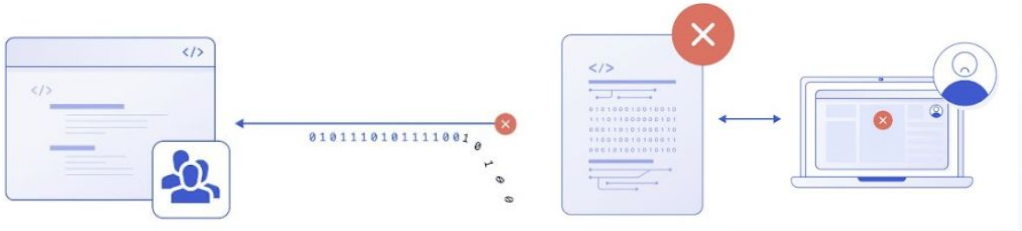
Chainlink 预言机计算服务

Automation - 智能合约自动化

合约自动化执行(Smart Contract Execution Automation)

智能合约开发团队

智能合约应用



1 手动 DevOp & 中心化服务器

开发者人员通过一个中心化服 务器去执行 Solidity 的 Cron job，监控合约状态，并且发送交易给链上合约。

- 占用团队时间和资源
- 单点失败风险

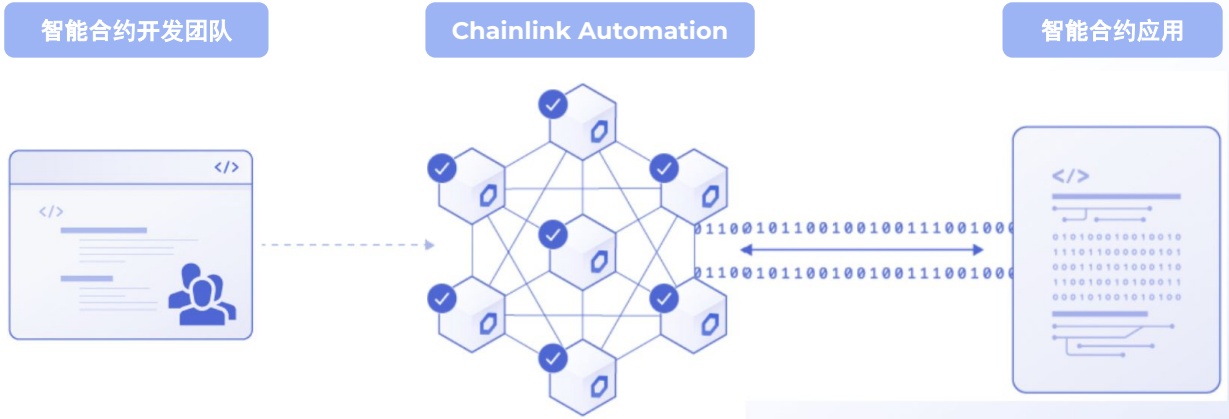
2 Bounty 模式(ETH Alarm clock)

给交易触发的个人账户提供赏金，交易执行成功即可获得经济激励。

- 没有 direct commitment
- winner-takes-all reward
- 增加链的拥挤程度

Chainlink

Chainlink Automation 保证执行的稳定性

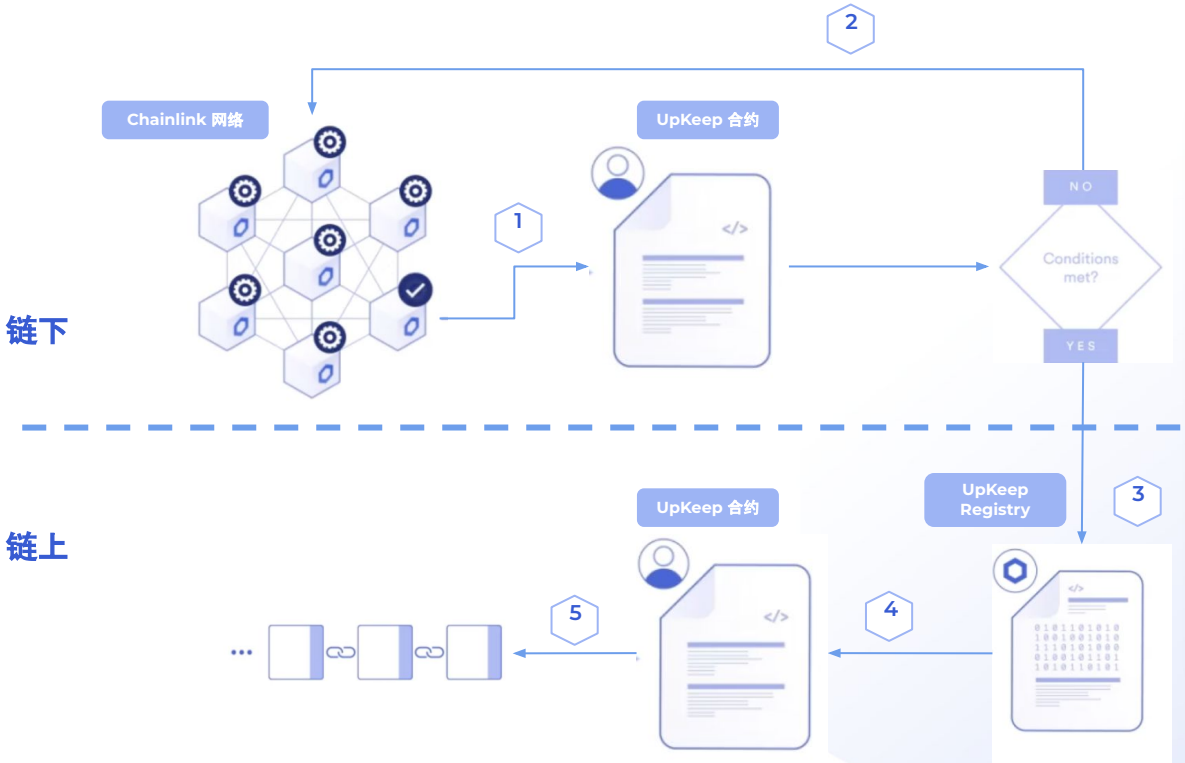


1 智能合约开发团队，创建一个 upKeep

2 Automation 不需要输入，即可循环检测预设条件，满足即会触发执行。

Chainlink

合约自动化执行(Smart Contract Execution Automation)



1. **Oracle 检查 CheckUpkeep**，判断是否满足条件

2. 如果 CheckUpkeep 条件不满足，则下个区块继续检查

3. 如果 CheckUpkeep 条件满足，**oracle 调用 keepers 注册合约**

4. Keepers 注册合约调用 **consumer 合约 performUpkeep 函数**

Chainlink

Chainlink Automation 使用场景

自动复利 & yield（Yield Harvesting and Compounding）

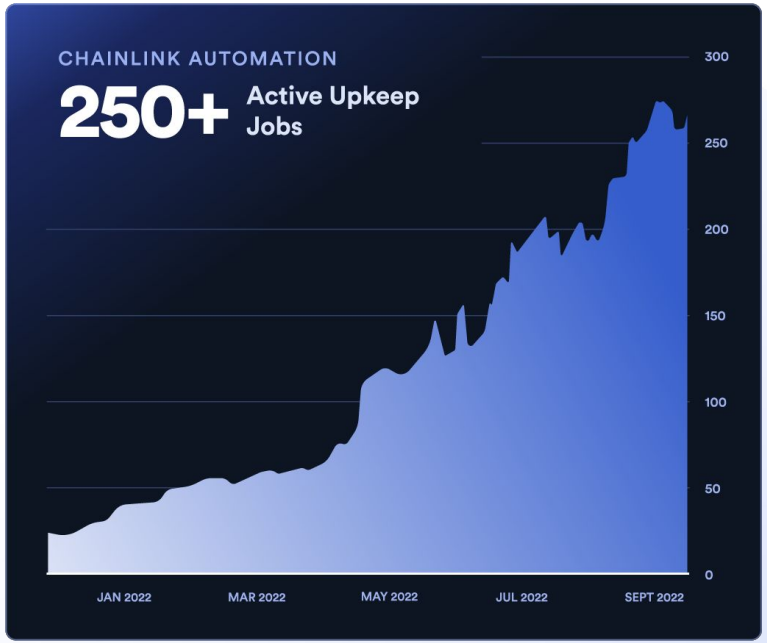
DEX 限价单（DEX limit orders）

借贷平台清算（Liquidation）

动态 NFT（Dynamic NFT）

Chainlink Automation 使用趋势

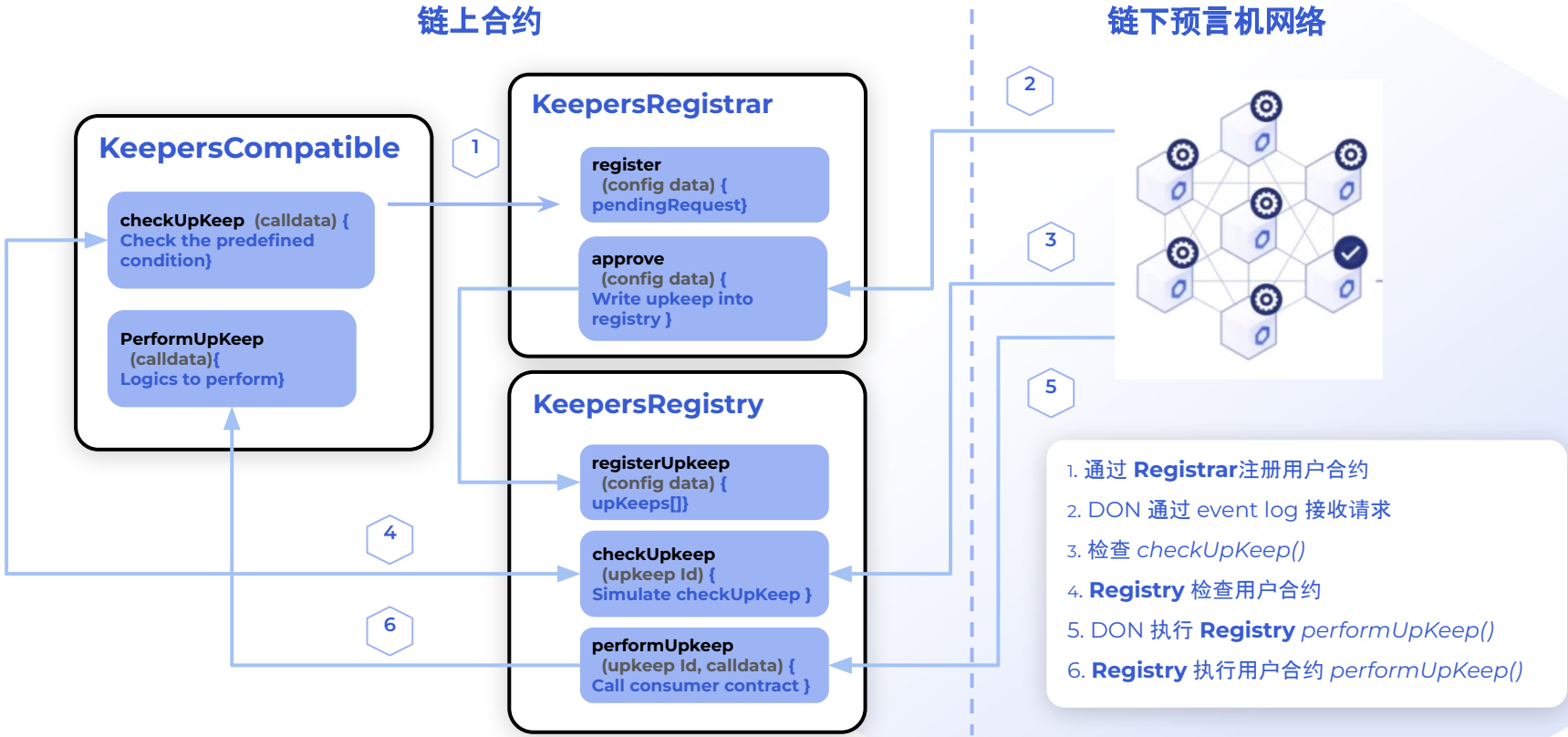
Chainlink Automation 在 Web3 自动化服务上覆盖了 130 个项目，自动化作业 250+



"We needed a reliable automation service in order for our prediction market to run exactly on-time every 5 minutes. Chainlink Automation provided us with a highly reliable solution we can depend on."

- Chef Snowball, the Head Chef at PancakeSwap

Chainlink Automation 技术架构

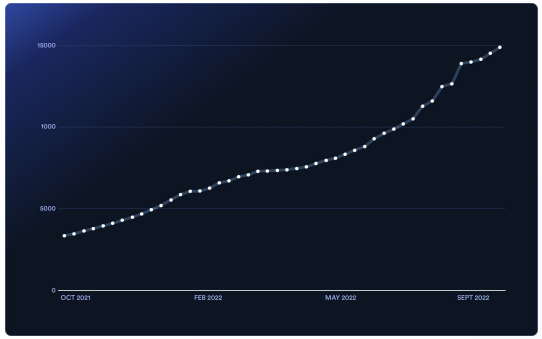


Chainlink

Chainlink 预言机网络

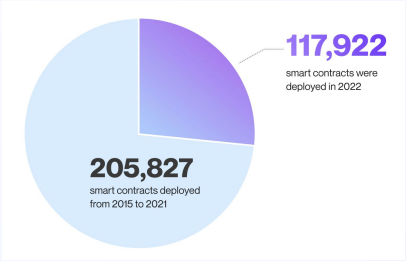
开发者社区

开发者增长趋势



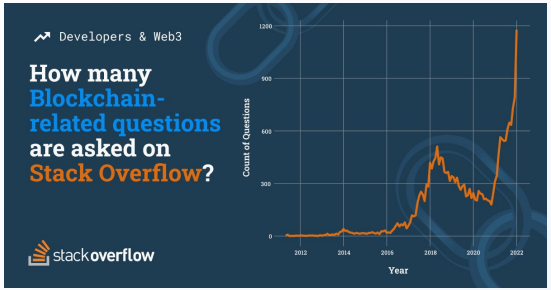
Chainlink 数据

使用到 Chainlink 的 GitHub repos 数量



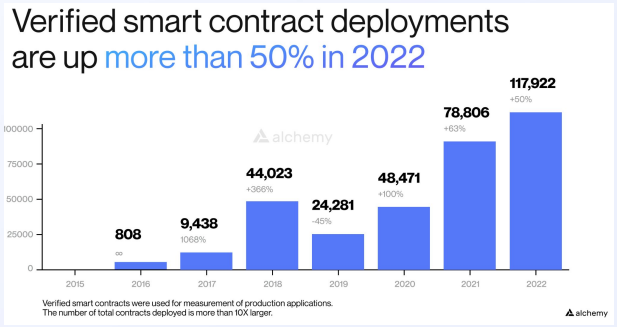
Alchmey 数据

智能合约的部署数量



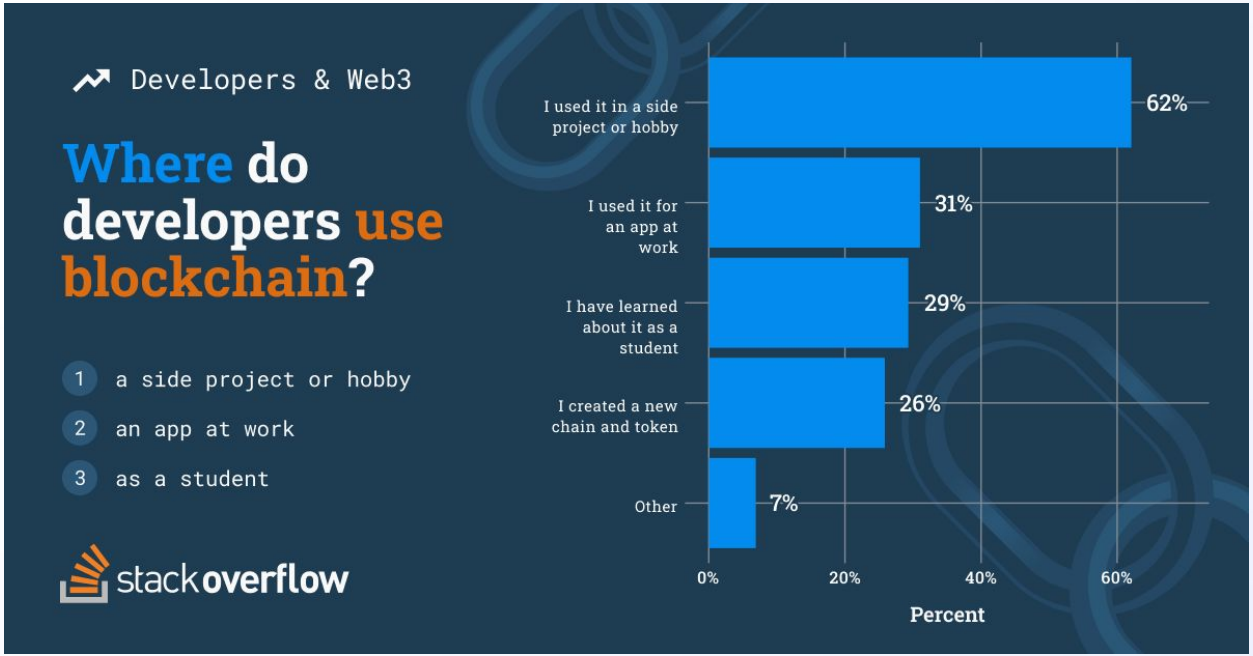
Stackoverflow

关于区块链的问题数量



Chainlink

开发者类型


Developers & Web3
Where do developers use blockchain?
1 a side project or hobby
2 an app at work
3 as a student
stackoverflow
I used it in a side project or hobby
62%
I used it for an app at work
31%
I have learned about it as a student
29%
I created a new chain and token
26%
Other
7%
0%
20%
40%
60%
Percent

参与方式 - 2022 秋黑客松

秋季黑客松:10.14 - 11.18 线上举行
https://chain.link/hackathon

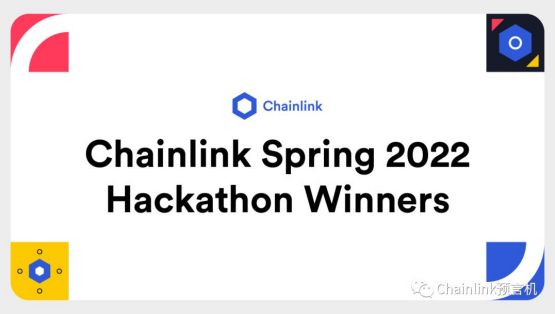
总奖金 - $475,000

- Chainlink Grand Prize - $25,000
- Chainlink NFT & Gaming - $15,000
- Chainlink DeFi Prize - $15,000
- Chainlink DAO Prize - $10,000
- Chainlink Social Impact Prize - $10,000
- Chainlink Women in Tech Prize - $10,000
- Chainlink Services - First Place - $7,000
- Chainlink Services - Second Place - $4,000
- Chainlink Services - Third Place - $2,000
- Chainlink Top Quality Projects - $20,000 (40)

- Filecoin - *General* StorageWizard - $22,500(3)
- Filecoin - *Bonus* Web3Fy - $7,500
- Filecoin - *Bonus* Social Good Warrior - $7,500
- Filecoin - *Bonus* On the Tools - $7,500
- Filecoin - *Bonus* Gaming, Metaverse, Daos & NFTs (Oh My!) - $7,500
- Filecoin - *Bonus* Computer Over Data - $7,500
- Filecoin *Bonus* DeFi Magician - $2,500
- Filecoin - Runners up - $12,500 (20)
- Truflation - $10,000 - 3 total winners (3)
- Solana Foundation - $10,000
- QuickNode - $5,000

Chainlink

2022 春黑客松



[2022 春季黑客松获奖项目清单]
[2022 春季黑客松获奖项目清单(英文)]

Grand Prize

- **Chainlink Verifiable Merkle Tree**
- https://devpost.com/software/chainlink-vmt
- https://github.com/vmtree/hackathon

NFT & Metaverse

- **NUSIC: Layer 1 for Music**
- https://devpost.com/software/nusic-layer-1-for-music
- https://github.com/nusic-fm
- https://nusic.fm/

DeFi

- **DeFi for People**
- https://chainlinkspring2022.devpost.com/submissions/329669-defi-for-people
- https://github.com/defiforpeople

Chainlink

Grant

[点击产看 Grant 具体介绍]

[点击查看以往的 Grant 案例]

Grant Program 是为了鼓励能够增加 Chainlink 功能，提升工具易用性的项目，目的是能够让 Chainlink 被广泛使用，以更好地服务Web3 生态系统。

Grants

HackBG Receives Chainlink Grant to Develop Gas-Efficient, Open-Source NFT Reveal Templates Using Chainlink Keepers and VRF

July 1, 2022 • Chainlink

HackBG has been awarded a Chainlink Community Grant to build open-source templates that help reduce gas costs for NFT mints.

Grants

Floodlight Receives Chainlink Grant To Build Global Greenhouse Gas Emissions Data Feed

June 3, 2022 • Chainlink

Floodlight has been awarded a Chainlink Community Grant to fund the development of a data feed that makes geospatial climate data accessible on-chain.

Grants

ChainSafe Receives Chainlink Community Grant to Natively Integrate Chainlink Into web3.js

March 25, 2022 • Chainlink

ChainSafe, a leading blockchain R&D firm, has been awarded a Chainlink Grant to natively integrate Chainlink into the web3.js library.

Chainlink

Startup with Chainlink

点击产看 Startup with Chainlink 申请表格

- **Startup with Chainlink 想做什么？**
  - 推动区块链产业进步，帮助年轻创业者成功
- **谁有申请资格？**
  - All levels of maturity
  - 你已经有一个团队，并且正在做开创性工作
  - 聚焦在种子轮的团队
- **通过 Startup with Chainlink 你将会得到什么？**
  - 商业模型设计
  - 接触导师以及服务提供商
  - 风投基金融资机会

Chainlink

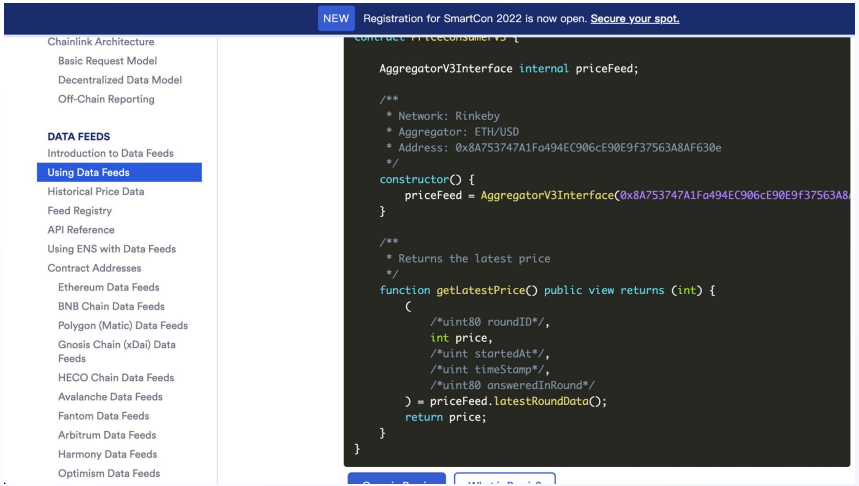
Chainlink

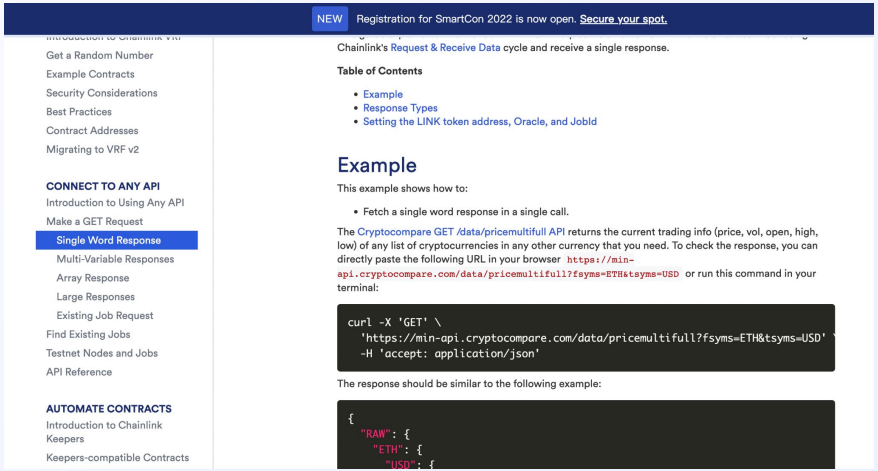
Chainlink 预言机网络

文档 & 教程

官方文档

https://docs.chain.link/





Chainlink

视频教程（中文）

2021秋季黑客松workshop 34

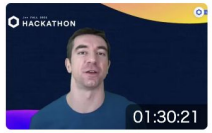
播放全部 更多

Chainlink 2021秋季黑客松——闭幕式

58 2021-12-17

【Chainlink 2021秋季黑客松】NFT前端——龙与地下城

176 2021-12-9

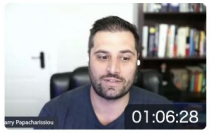


【Chainlink 2021秋季黑客松】基于Moralis的全栈开发

180 2021-12-9

【Chainlink 2021秋季黑客松】治理和DAO

114 2021-12-9



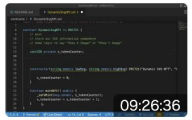
【Chainlink 2021秋季黑客松】创建并使用外部适配器开

57 2021-12-9

开发者大使课程 2

（32 小时最全课程）区块链，智能合约 & 全栈 Web3

1970 7-11



（32 小时最全课程第二部分）区块链，智能合约 & 全

395 昨天

Chainlink开发教程【中文字幕】 9

Solidity中的事件和日志

192 2-10

如何使用Chainlink Keepers自动化Solidity智能合约

120 1-20

7-Chainlink Price Feed 喂价-Chainlink开发教程

258 2020-9-27

https://space.bilibili.com/482973600

Chainlink

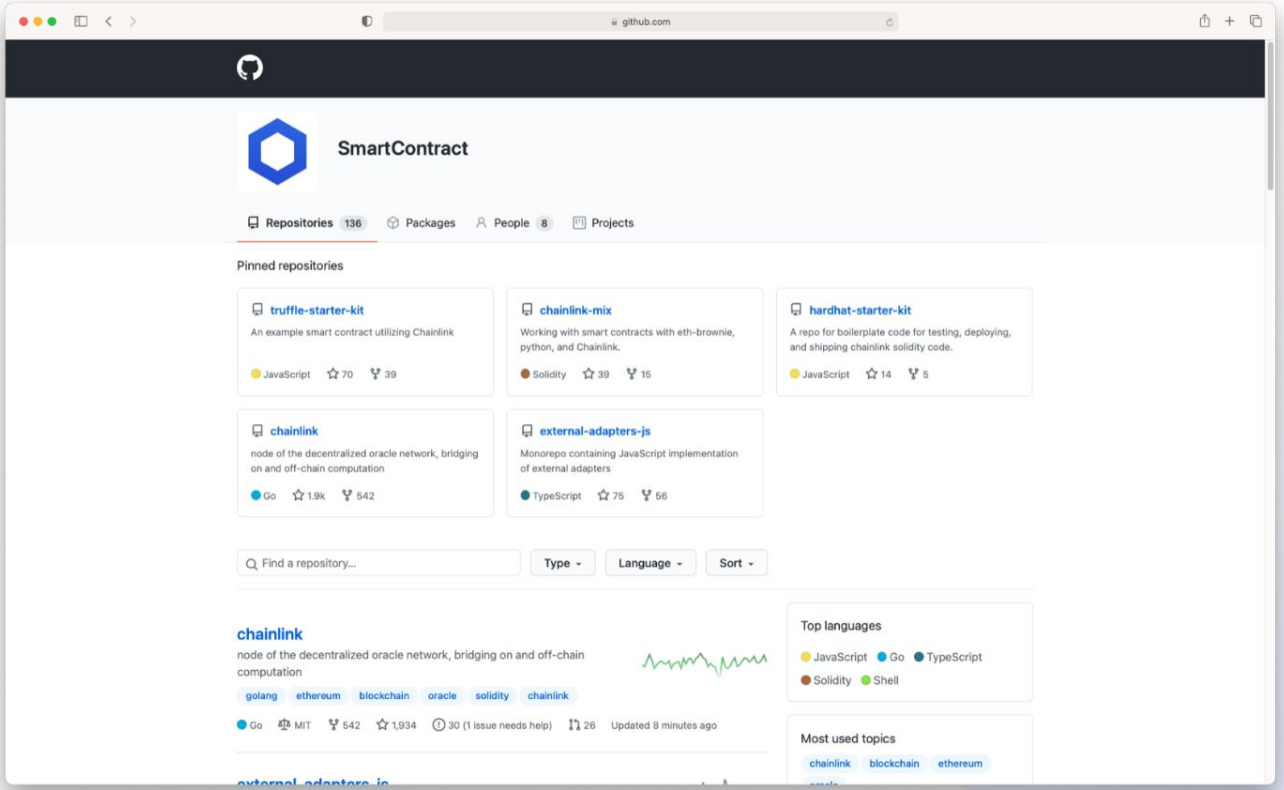
QA & 技术文章

登链社区

https://learnblockchain.cn/people/398

Chainlink

Solidity and Smart Contract Starter Kits!



Chainlink

谢谢

Chainlink