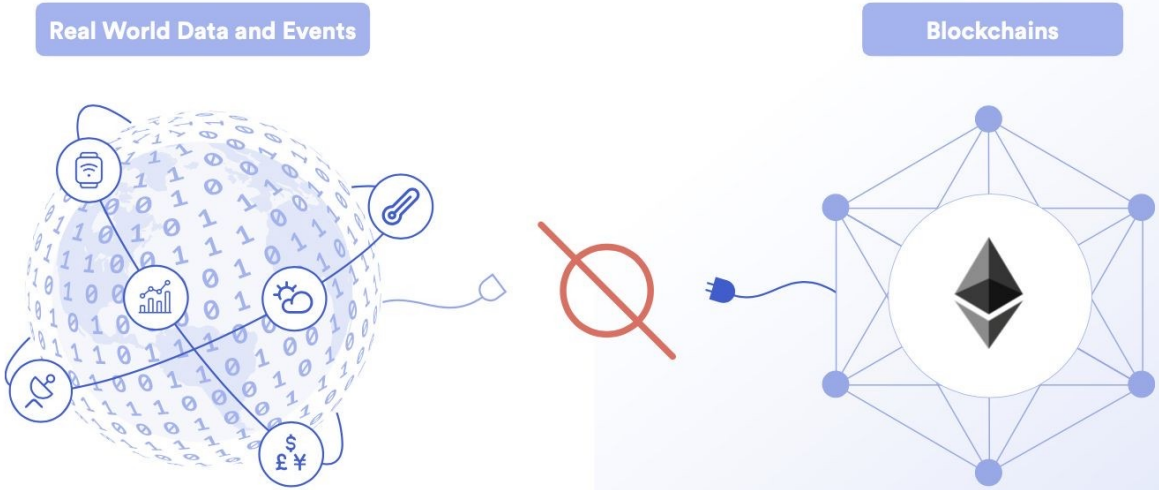
Chainlink

Chainlink 原理

预言机问题

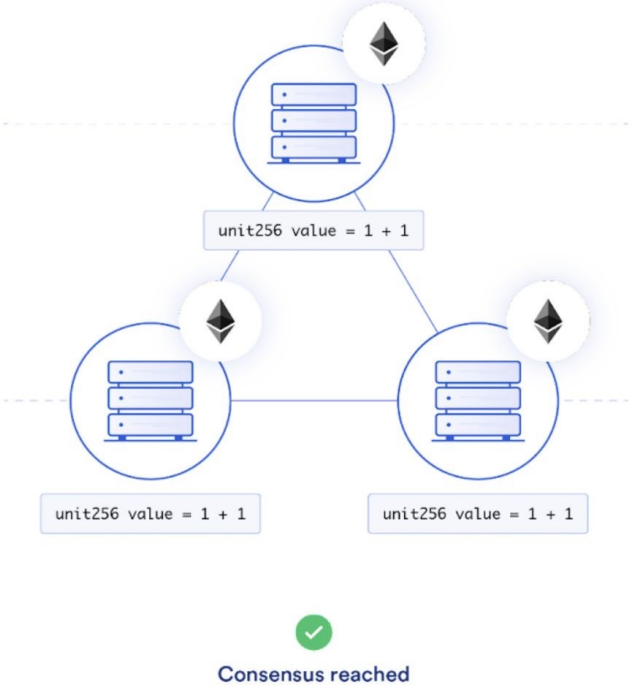
智能合约无法获取区块链以外的数据， 外部 API 提供的数据和任何其他链下资源都无法获取。



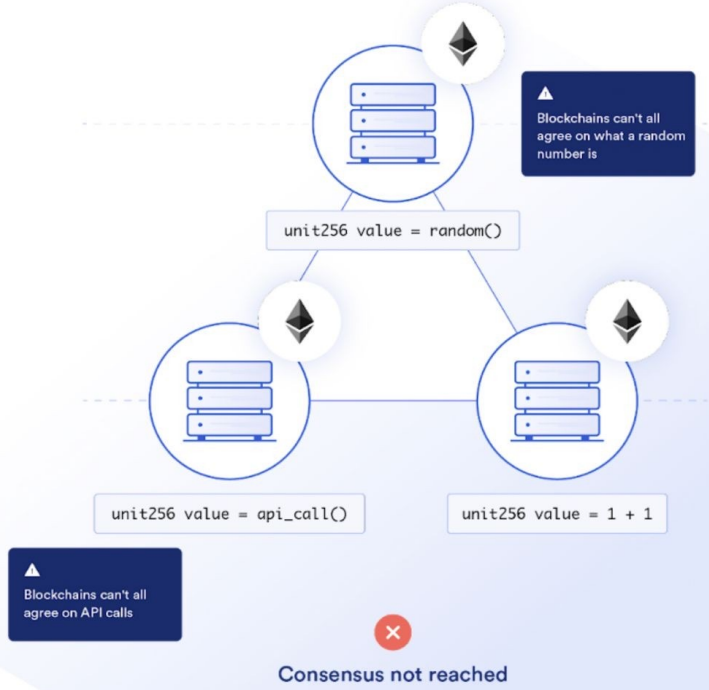
Chainlink

非确定性操作

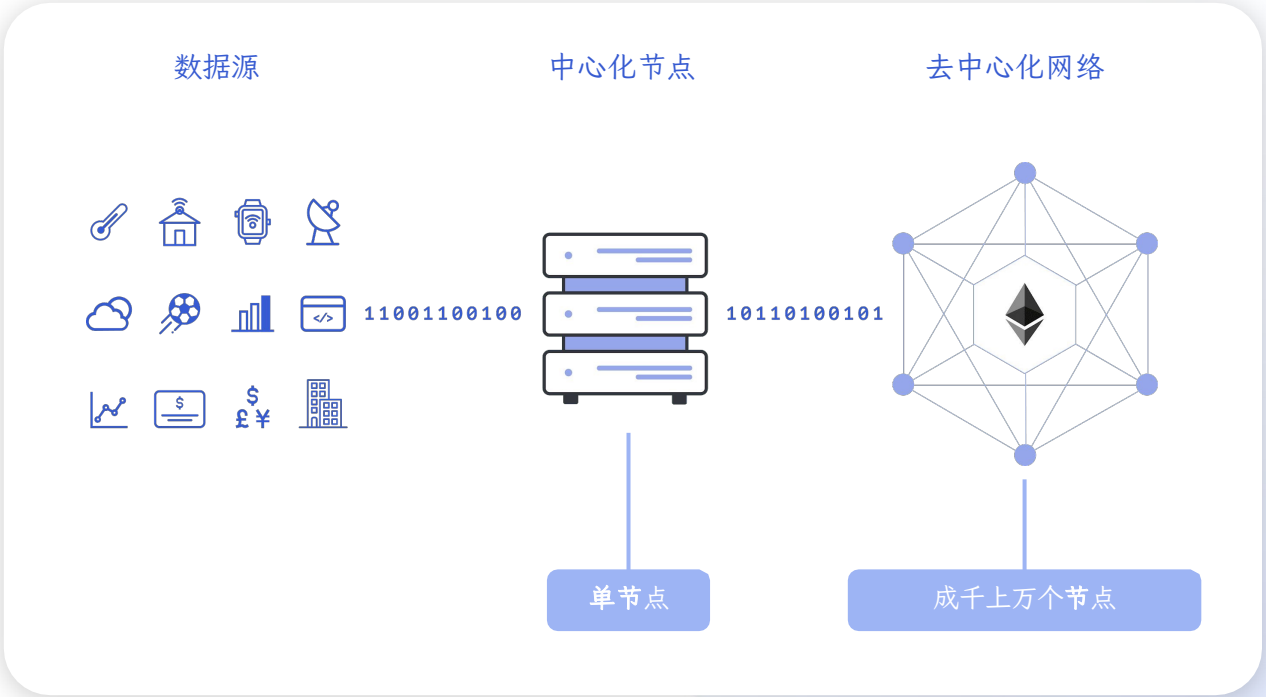
确定性操作



非确定性操作

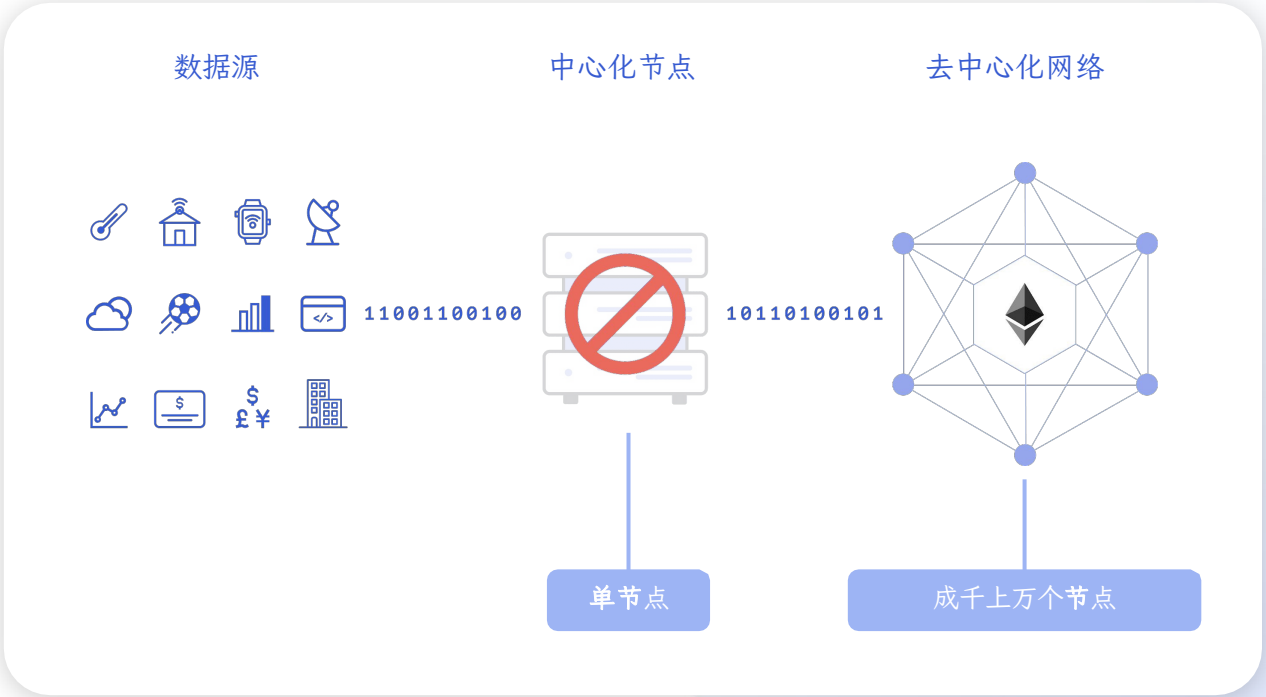


中心化预言机工作流程



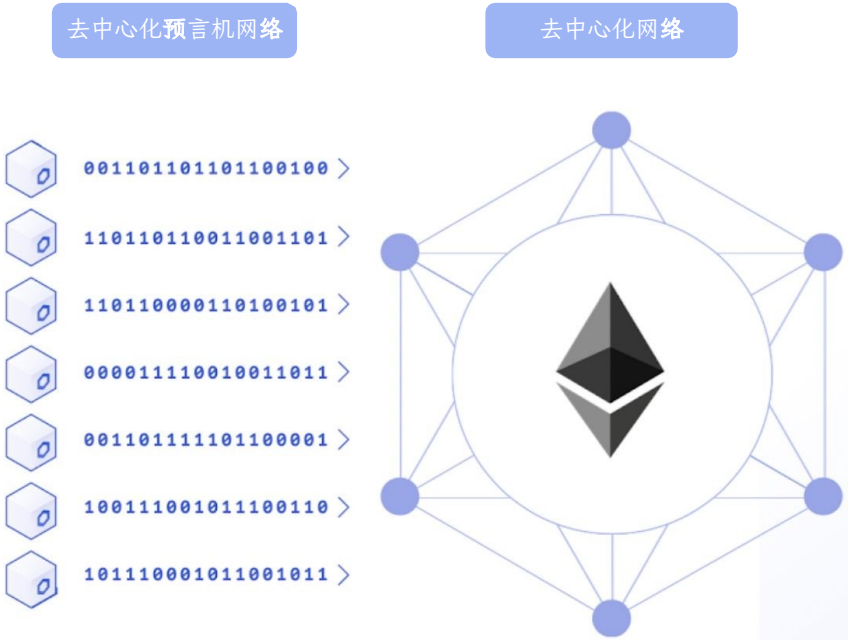
Chainlink

中心化预言机单点失败风险



Chainlink

去中心化预言机网络



去中心化预言机网络

多个数据节点形成去中心预言机网络，每个节点都会收集数据，达成共识后输入到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，通过网络对多个数据源进行验证

Chainlink

Chainlink

Chainlink Data Feed

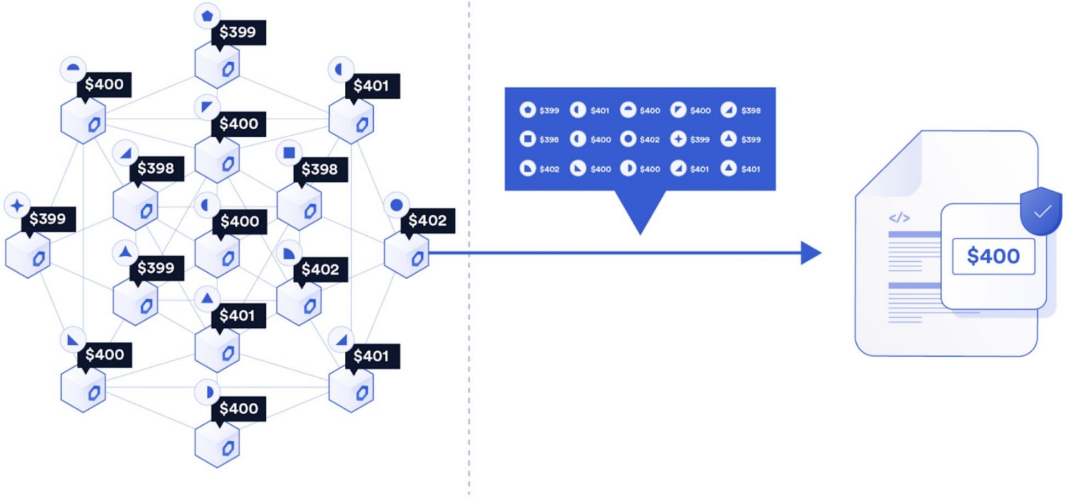
Chainlink Data Feed

去中心化预言机网络

Chainlink 预言机节点

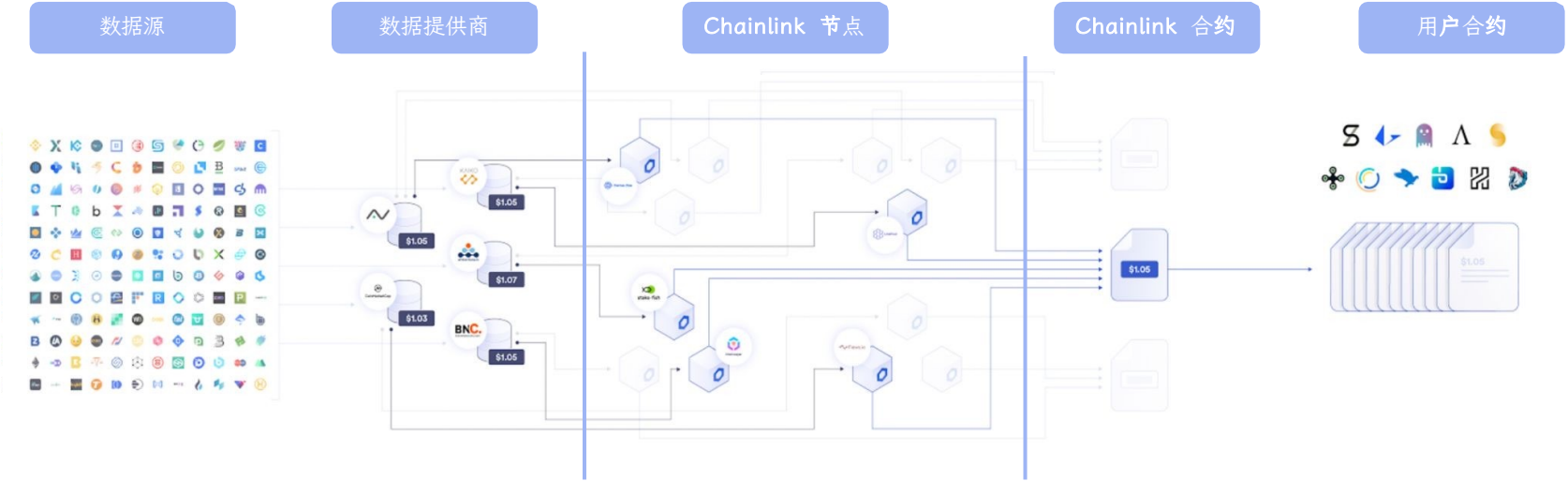
区块链网络

智能合约



Chainlink

Chainlink Data Feed 业务流程



Chainlink Data Feed 技术架构

链下

链上

链下预言机网络

Consumer 合约

可以是链上，也
可以是链下

1

4

Proxy 合约

AggregatorProxy

latestRounddata()

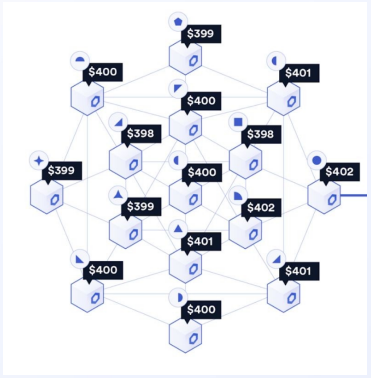
2

3

Aggregator 合约

OffChainAggregator

latestRounddata()
Mapping transmission



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 Aggregator 合约中的价格信息

1. 每 30 分钟会更新一次
2. 通证价格波动超过 0.5%

Chainlink Data Feed 用户案例

Chainlink

Lending and borrowing

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

AAVE · Compound · venus

Mirrored assets

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

Stablecoins

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

Liquity · Fei Protocol · Ampleforth

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

Options and futures

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

dYdX · Lyra · THALES

Chainlink

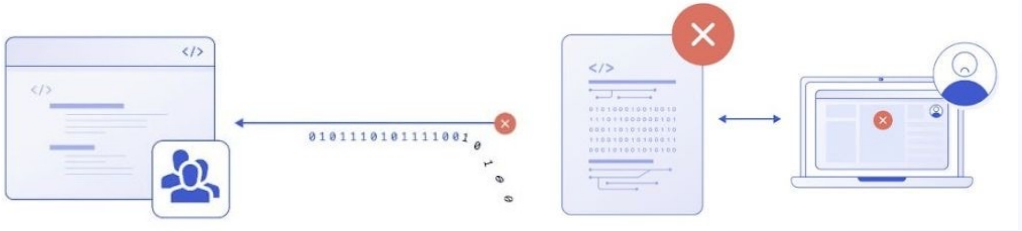
Chainlink Keepers

合约自动化执行

Chainlink

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。

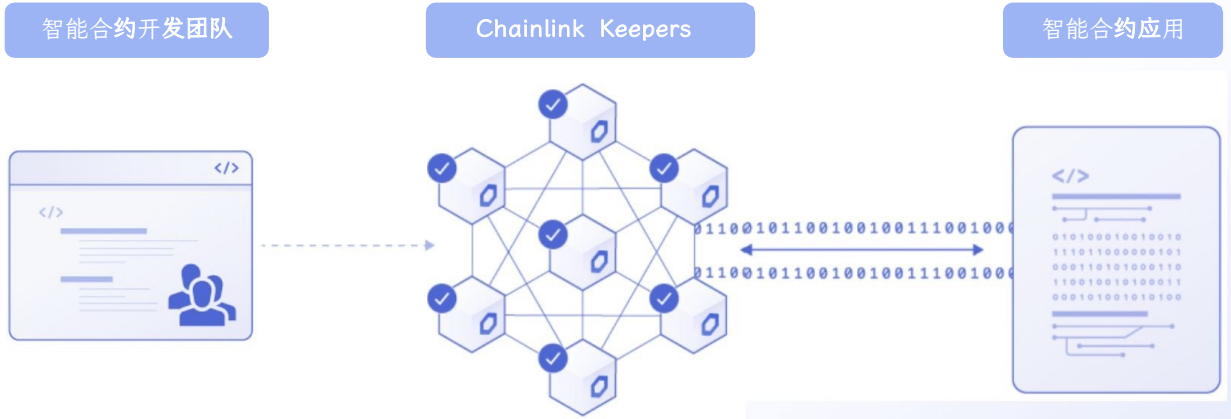
- 单点失败风险
- 占用团队时间和资源

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。

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

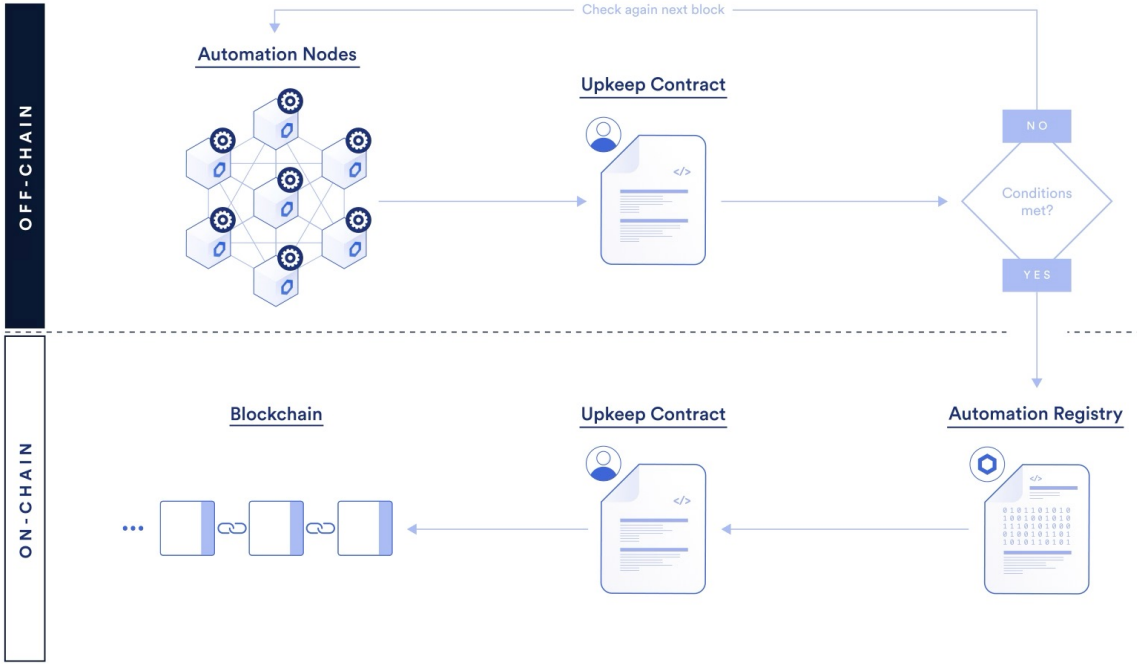
Chainlink Keepers（合约自动化执行工具）



1 智能合约开发团队，创建一个 upKeep

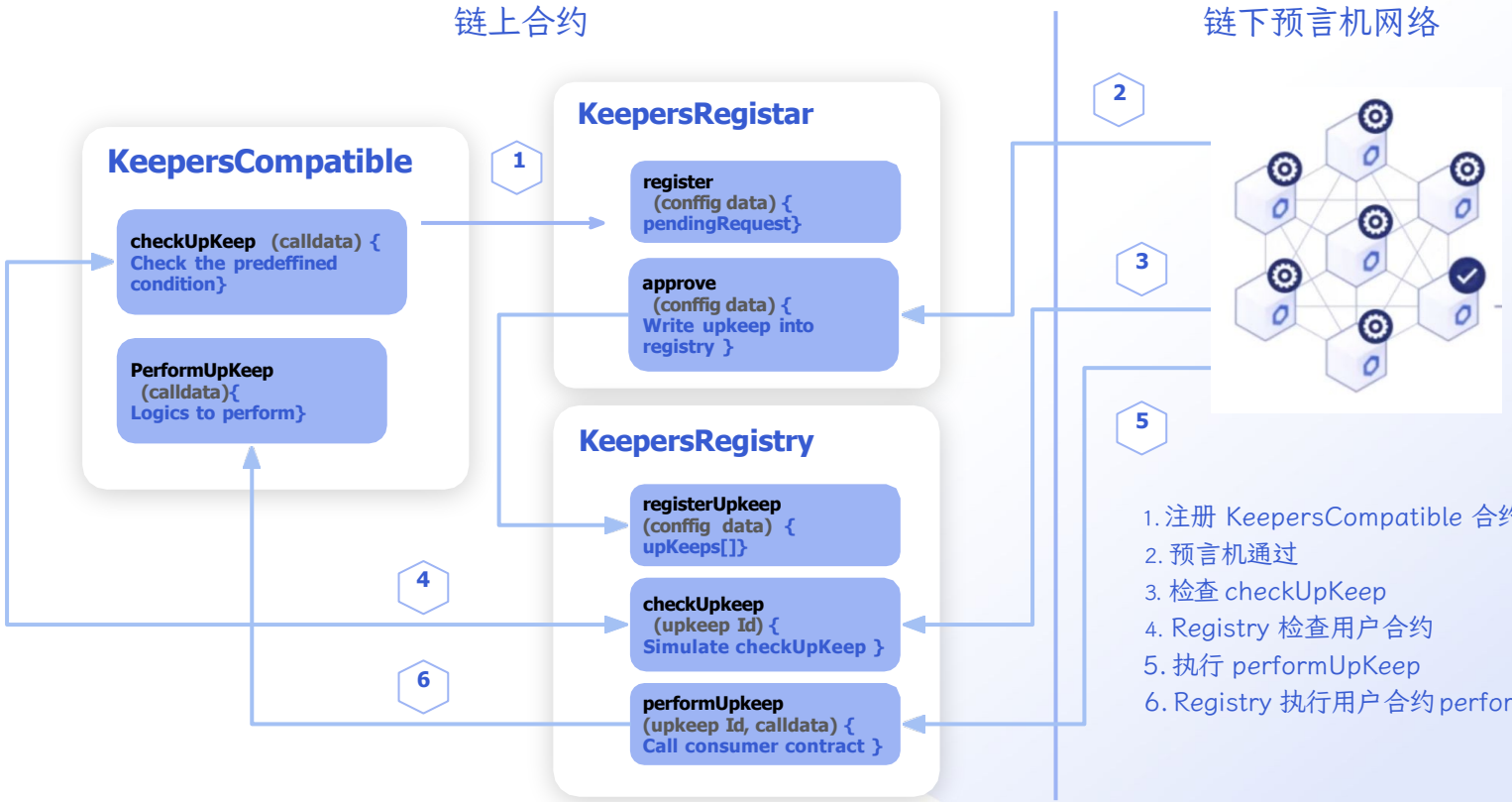
2 Keepers 在不需要输入的条件下，不断检测预设合约设定的预设条件，满足即会执行。

Chainlink Keepers 业务流程



1. eth_call，判断是否满足条件
2. 下个区块继续检查
3. 调用 keepers 注册合约
4. Keepers 注册合约调用用户合约

Chainlink Keepers 技术架构



Chainlink

Chainlink Keepers 使用场景

自动复利 & yield （Yield Harvesting and Compounding）

流动性管理（Liquidity management）

借贷平台清算（Liquidation）

跨链 NFT 铸造（cross-chain minting）

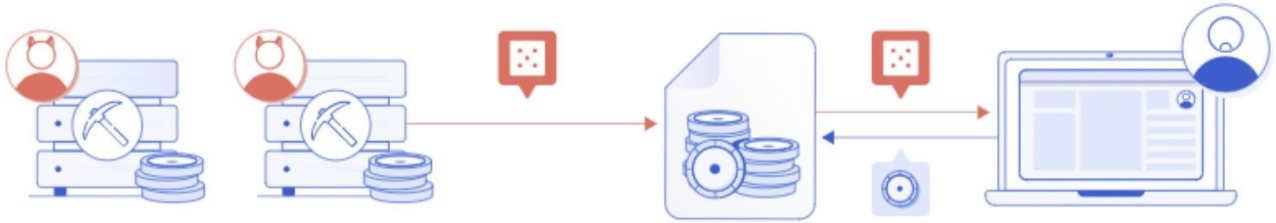
DEX 限价单（DEX limit orders）

动态 NFT （Dynamic NFT）

Chainlink

Chainlink VRF

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

随机数生成器（RNG）- 预言机方案

1. 用户合约给预言机发送随机数请求
2. 预言机获取种子，生成随机数以及相关的Proof
3. VRF 合约验证随机数是否由预言机按照约定算法生成
4. 用户合约接受已验证的随机数

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 是由 **3** 个函数组成：

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

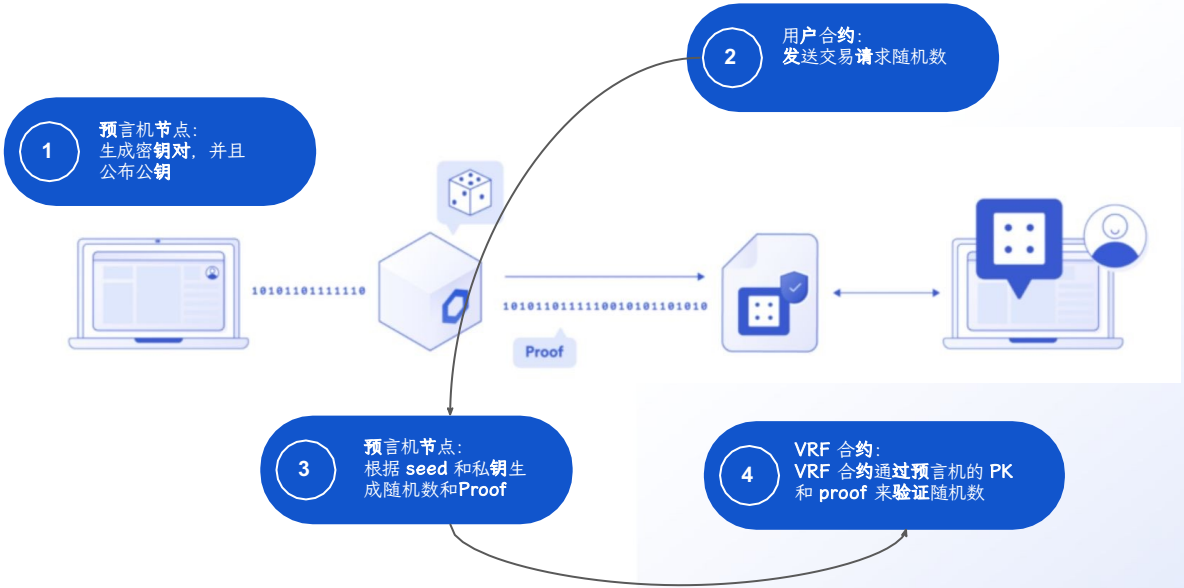
3. 验证函数（**Verify**）

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

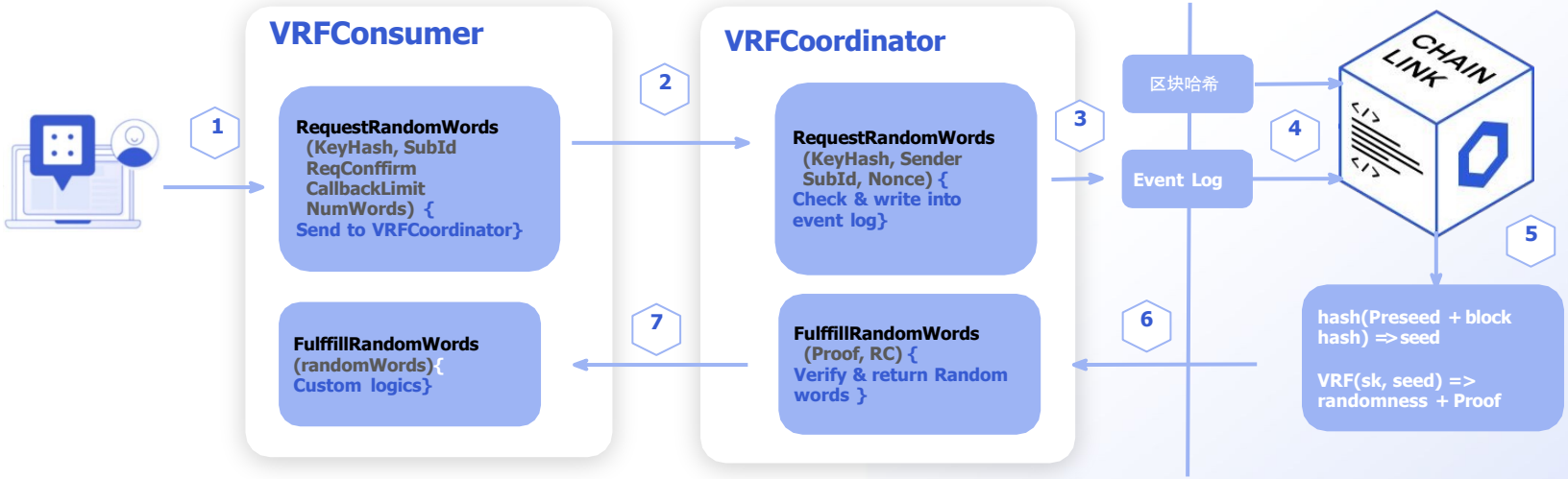
   true：验证成功

   false：验证失败

Chainlink VRF 业务流程



Chainlink 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 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

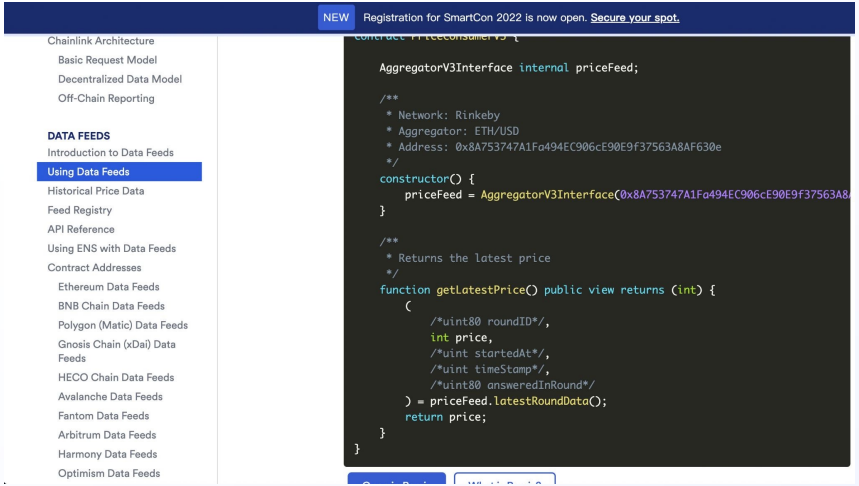
查看 35 个应用场景

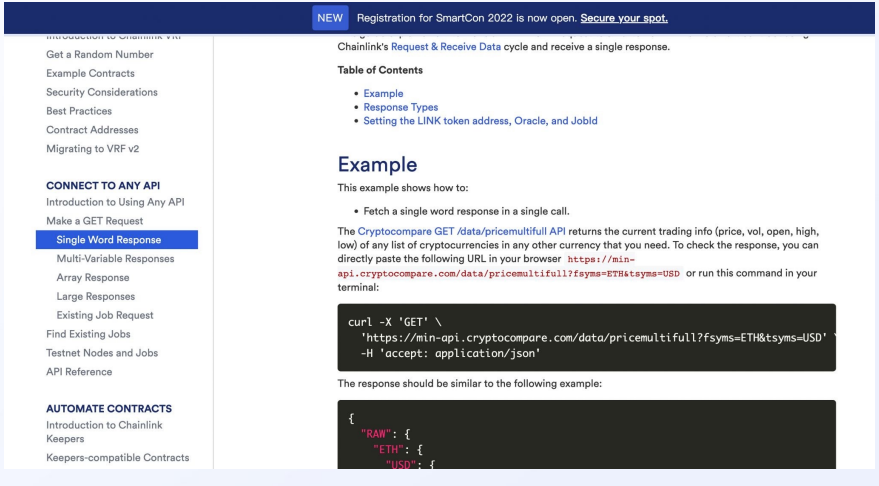
https://blog.chain.link/blockchain-rng-use-cases-enabled-by-chainlink-vrf/

Chainlink

Chainlink 学习资料

学习资料





https://docs.chain.link/

Chainlink

学习资料

登链社区

https://learnblockchain.cn/people/398

Chainlink