**一文读懂预言机**

目录

[1.背景 1](#_Toc69219276)

[2.chainlink 2](#_Toc69219277)

[2.1.解决的痛点 2](#_Toc69219278)

[2.2.中心化预言机单点故障的问题 3](#_Toc69219279)

[2.3.oracle网络 4](#_Toc69219280)

[2.3.1.已经存在的oracle网络 4](#_Toc69219281)

[2.3.2.需要自己构建的oracle网络和外部适配器 5](#_Toc69219282)

[2.4.去中心化特性 6](#_Toc69219283)

[2.5.可连接的数据源 6](#_Toc69219284)

[2.6.智能合约的进化 7](#_Toc69219285)

[2.7.激励机制 7](#_Toc69219286)

[2.8.消费真实世界的REST API 8](#_Toc69219287)

[3.预言机和TEE的结合 8](#_Toc69219288)

[3.1.TEE的特性 8](#_Toc69219289)

[3.2.预言机和TEE的结合点 8](#_Toc69219290)

[3.3.基于TEE的预言机的主流方案---Town Crier 9](#_Toc69219291)

[3.3.1.oracle完整性 10](#_Toc69219292)

[3.3.2.基于TEE的oracle机密性 10](#_Toc69219293)

[4.国内大厂的预言机布局 12](#_Toc69219294)

[5.参考资料 13](#_Toc69219295)

# 1.背景

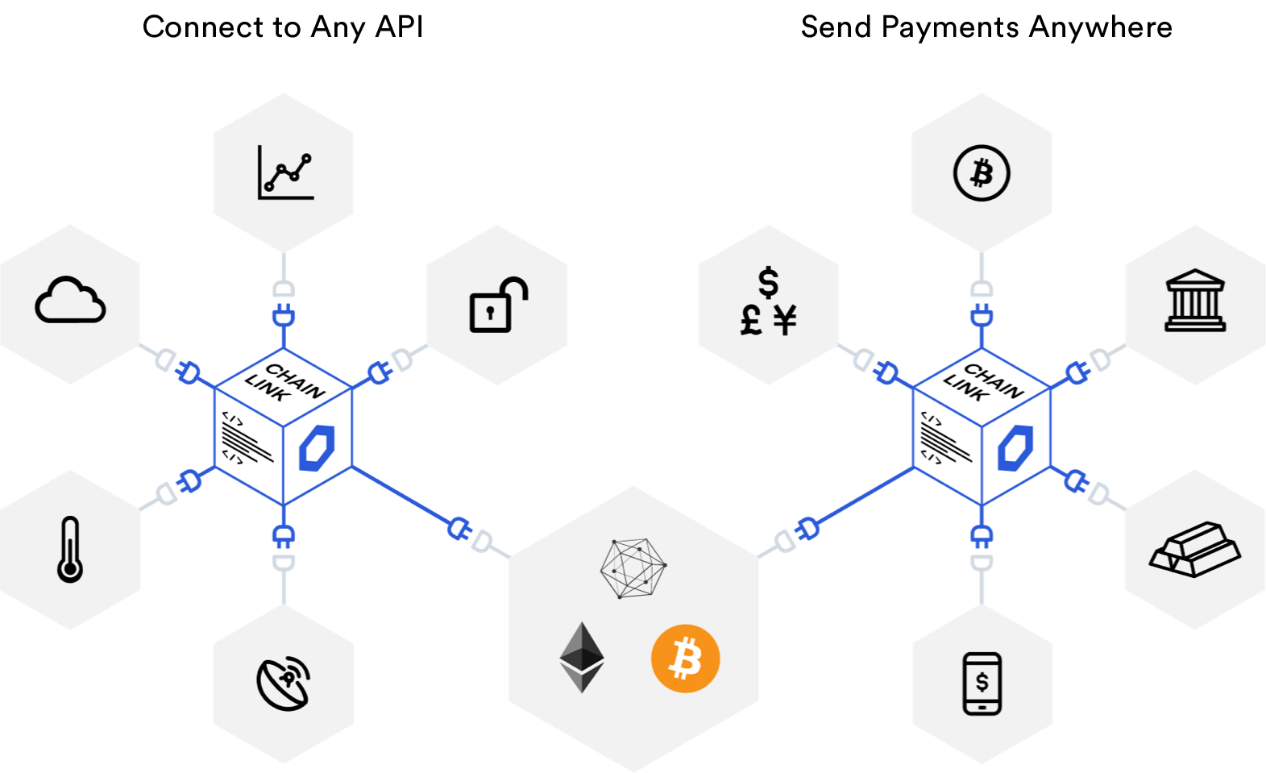
区块链是一个确定性的、封闭的系统环境，目前区块链只能获取到链内的数据，而不能获取到链外真实世界的数据，区块链与现实世界是割裂的。传统的智能合约本身不能连接真实世界，只能处理链上的数据，比如token的转账或者内置代币的转账，但不能处理链下真实世界的数据，即不能接收链下的数据、事件（接收input），也不能对链下的数据产生影响（产生output），也就是说智能合约和真实世界是隔离的、没有交互，这样就严重地局限了智能合约的使用场景，除了围绕token的场景外，几乎没有用武之地，所以智能合约并没有真正对经济和社会产生重大影响。业界有专家认为，智能合约80%的使用场景需要和真实世界发生交互，所以需要找到一种能够把智能合约和真实世界连接起来并发生交互的方法，这样才能够大大地释放智能合约的潜力，使智能合约为经济和社会的运转发挥更大的作用。

预言机的出现就是为了解决智能合约和真实世界的连接和交互问题，即从真实世界接收数据以及改变真实世界的数据。目前预言机领域的绝对领先者是chainlink，它的市值远远高于其他预言机，并且使用最广泛，有良好的生态圈，且被中国国家区块链服务网络BSN认可和整合，所以chainlink是预言机领域事实上的第一，chainlink在预言机领域的地位基本上等同于以太坊在区块链领域的地位或者IPFS在去中心化存储领域的地位，本次预言机的调研也是基于chainlink。

chainlink是基于以太坊的预言机，chainlink有自己的token:LINK，遵循以太坊ERC677规范，此规范继承了ERC20，并且允许token transfer包含data payload。

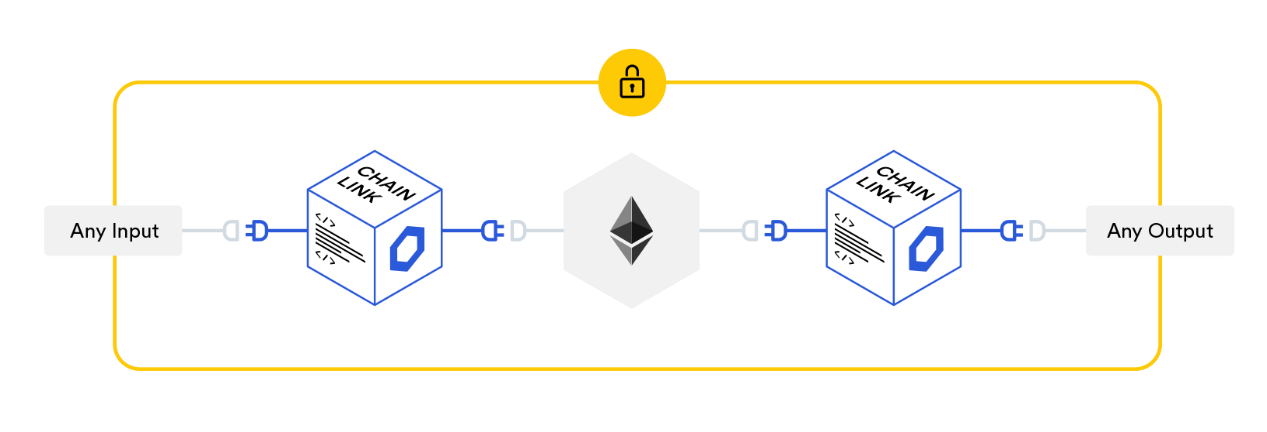
# 2.chainlink

chainlink是一个通用的框架，用于构建**去中心化的oracle网络**，为智能合约提供安全可靠的数据输入和输出的访问。它能够让智能合约连接到真实世界的数据和事件，并让智能合约对真实世界施加影响，比如通过智能合约发起一笔真实世界的支付（例如：银行卡支付、微信支付等等）。chainlink相当于是智能合约连接真实世界的一个中介。

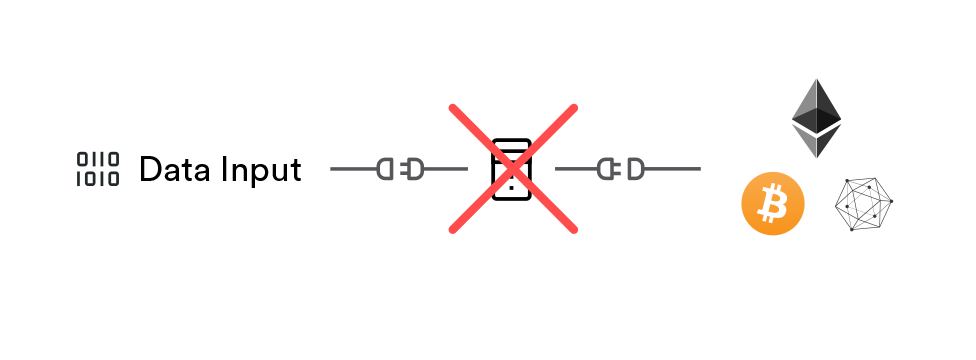


## 2.1.解决的痛点

**智能合约需要端到端的可靠性**：智能合约提供执行防篡改的数字契约的能力，这被认为是高度安全和高度可靠的。为了保持合约的整体可靠性，合约所依赖的输入和输出也需要是安全的。chainlink提供了到外部数据的可靠连接，是端到端安全的。

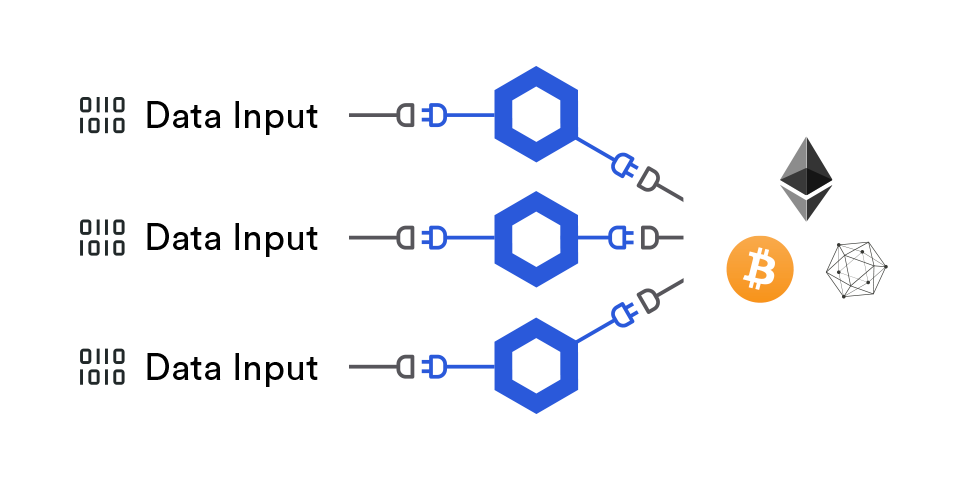


## 2.2.中心化预言机单点故障的问题



如果通过单个oracle节点来为智能合约提供链下输入数据，那么一旦这个oracle节点遇到故障或者提供虚假的数据，就会造成单点故障的问题，那么就会导致智能合约的可靠性大打折扣。智能合约本身的初衷之一就是避免单点故障，做到去中心化或者弱中心化，如果oracle节点也是中心化的，就会违背这一初衷。

**解决oracle单点故障的方案：高度可靠的去中心化oracle网络**



**去中心化是chainlink预言机的主要特征**。chainlink的中心化oracle网络提供了和智能合约同等级别的安全性保障，通过多个chainlink oracle节点提供相同的数据，就可以消除单点故障，并且保证数据的真实性和准确性，达到的效果是让连接预言机的智能合约高度安全、可靠、可信。

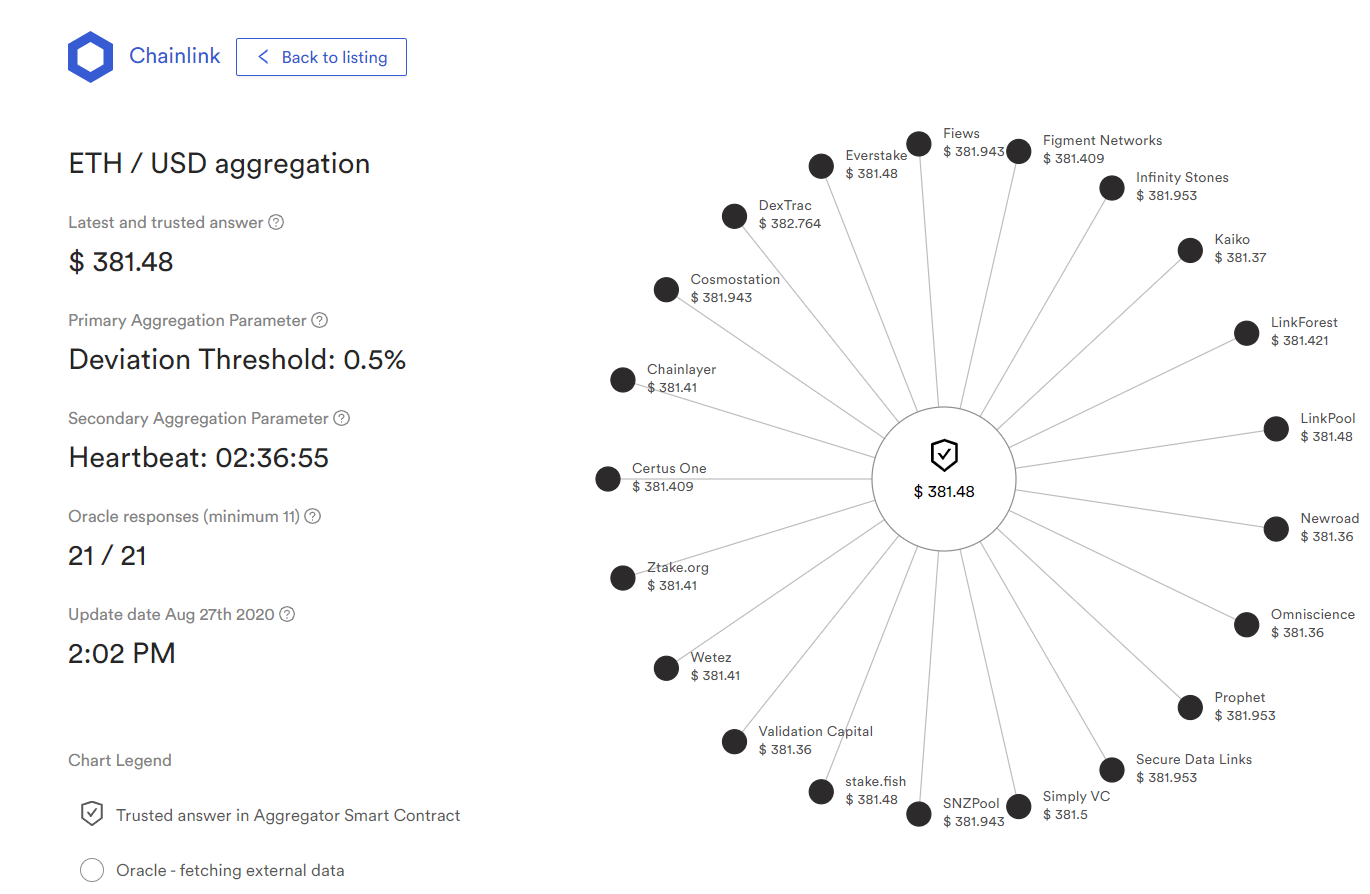
## 2.3.oracle网络

根据智能合约请求的数据和类型的不同，对应不同的oracle网络。每个oracle网络包含：

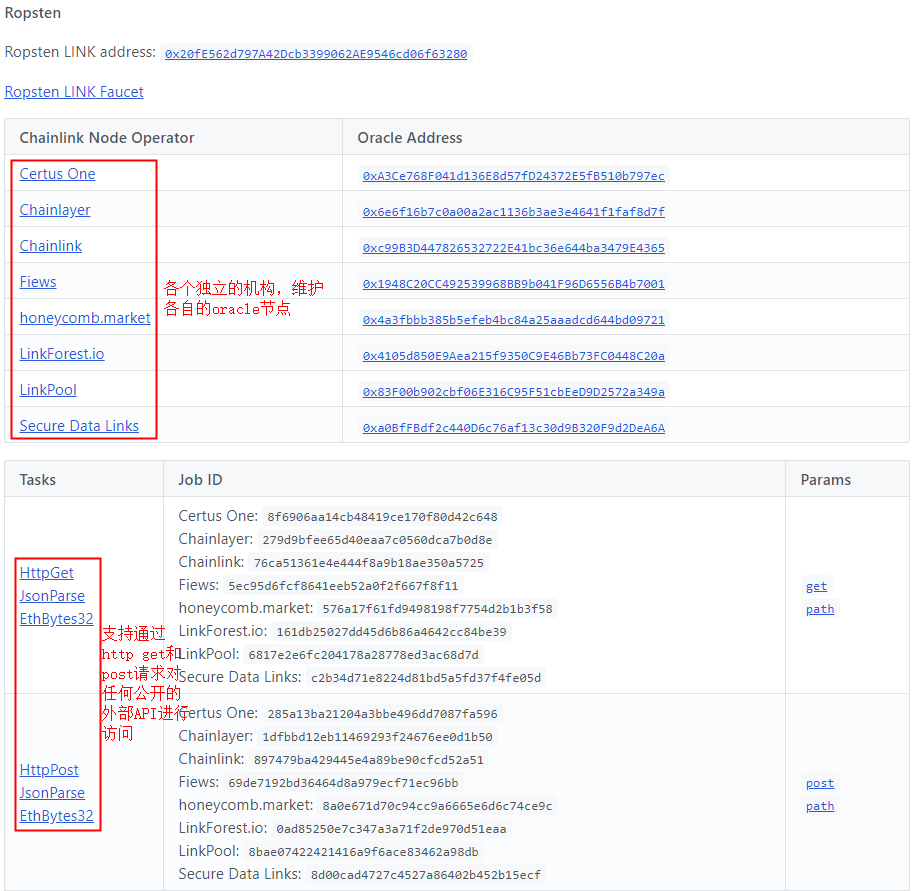
* 多个独立的oracle节点
* 一个聚合数据的方法
* external adaptor（外部适配器）：作为中间件，可访问任何API，利用数据和外部服务

### 2.3.1.已经存在的oracle网络

有一些被广泛需要的数据，比如数字货币的价格、安全的随机数生成器，对于这类数据，oracle网络是已经存在的，其oracle节点由区块链领域的多个独立机构/组织部署和运行，提供独立的数据输入，保证了去中心化。比如对于ETH的价格，通过一个聚合智能合约从很多个独立的oracle节点获取ETH的价格，在定义好的偏差阈值0.5%之内，计算出的ETH价格$381.48即被认为是当前可信的价格。



除了支持具体的数据需求的oracle网络外，还有一种支持更加通用的http get和post接口的oracle网络，可以用于访问任何外部的公开的API，这种oracle网络也由多个独立的机构运行的oracle节点组成，支持同样的tasks，例如：



如果我们的业务需求需要访问真实世界的http API，可以直接使用现有的oracle节点，不需要自己搭建oracle节点，这是最简便的一种方式。

### 2.3.2.需要自己构建的oracle网络和外部适配器

如果有特殊的需求，比如通过gRPC接口而非REST接口访问外部API，如果没有现有的支持gRPC的oracle节点，那么就需要我们自己：

* 部署自己的oracle节点，如果能同时让其他组织也部署同样的oracle节点就更好，这样就不会有单点故障问题，并且尽量实现去中心化或者弱中心化
* 开发自己的外部适配器，被oracle节点用于通过gRPC接口访问外部API

由于目前大部分的API都是REST API，所以大部分的应用场景不需要我们自己构建oracle网络和开发外部适配器，直接利用现有的oracle网络就可以了。

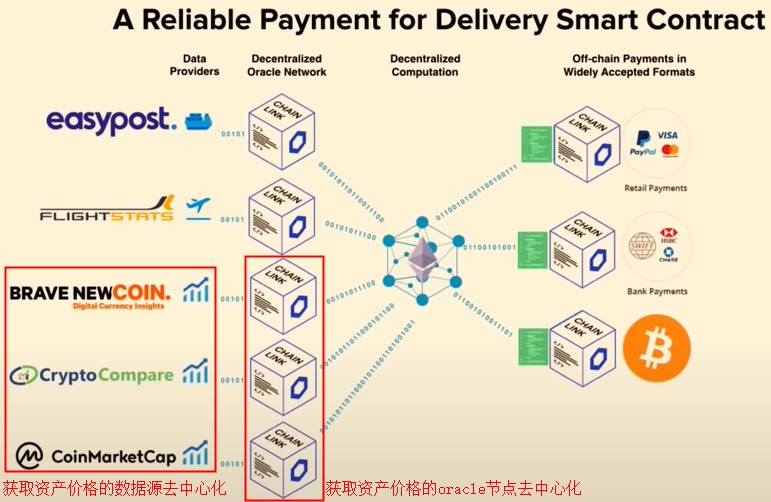
Chainlink的去中心化oracle网络为智能合约提供了push和pull数据的能力，促进了链上和链下应用程序之间的互操作性。

## 2.4.去中心化特性

chainlink的去中心化特性包含两个层面：

* **oracle节点的去中心化**：通过使用多个独立的chainlink节点，用户可以防止一个oracle成为单点故障。
* **数据源的去中心化**：以ETH价格为例，不同的oracle节点可以使用不同的数据源来获取ETH的市场价格，即使用多个数据源来确定市场价格，可以避免一个数据源成为单一的真相来源。

下图展示了两个层面的去中心化：oracle节点去中心化和数据去中心化

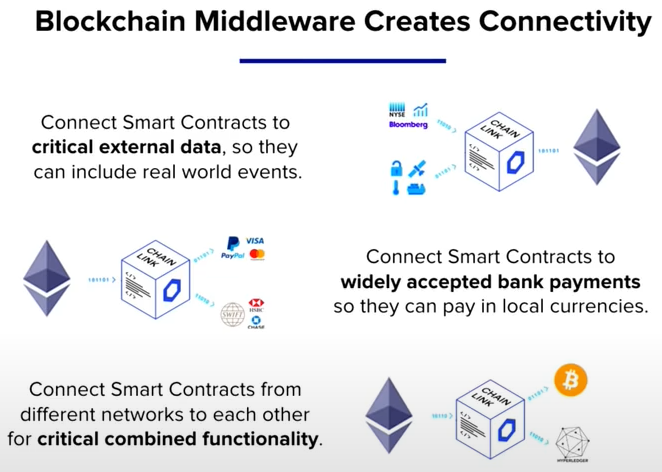


有了这两个层面的去中心化，就可以确保触发智能合约的oracle机制与底层区块链一样安全可靠。

## 2.5.可连接的数据源

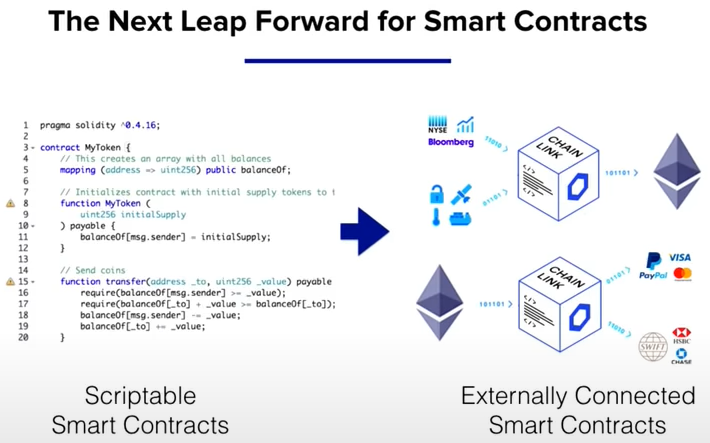
现实世界中有多种数据源可供连接，比如web APIs、企业系统、云服务商、IoT设备、支付系统，甚至其他区块链（跨链场景的另一种思路）。

下面展示了chainlink能够在获取外部数据、进行支付和跨链中发挥的作用。



## 2.6.智能合约的进化

有了预言机，智能合约就能发生质的进化，从传统的链上智能合约进化为**链上链下相结合**的智能合约，这样就能充分释放和发挥智能合约的潜能。



## 2.7.激励机制

智能合约通过去中心化的方式调用多个机构运营的oracle节点获取真实世界的数据，并不是免费的，天下没有免费的午餐，因为oracle节点的运营机构也是有成本的，并且也需要赚钱，所以在以太坊主网上，每个oracle每提供一次真实世界数据的查询，都可以得到0.1 LINK（LINK是chainlink的token），在ropsten测试网上，可以得到1 LINK。这些LINK来自于向oracle节点发送请求的智能合约，所以，在使用去中心化oracle服务之前，需要先向智能合约充LINK token，保证智能合约有足够的LINK token用于获取真实世界的数据。在主网上，需要通过ETH购买LINK，然后给智能合约充值；在ropsten测试网上，可以直接通过chainlink faucet获取免费的LINK。

正是因为有激励机制，oracle节点的提供者才有动力持续地维护oracle节点。

## 2.8.消费真实世界的REST API

oracle中的角色有两种：

* **oracle节点的提供者**（上一节已经提到）
* **oracle节点的消费者**

作为oracle节点的消费者，可以通过调用提供了http get/post job的oracle节点来访问真实世界的REST API以获取任何外部的数据源，比如体育赛事结果、最新的天气信息、航班信息等等，具体就是通过在智能合约中引入chainlink的library，并且配置好需要连接的oracle节点的地址、job id、手续费（LINK）等信息，就可以调用oracle节点，更细节的步骤不在此处赘述，可以查看官方文档。

**值得注意的是一个最佳实践：在智能合约中最好使用多个oracle节点，保证更高的可靠性。**

# 3.预言机和TEE的结合

## 3.1.TEE的特性

TEE主要保证了：

* **完整性**：对代码和数据实行硬件防护，攻击者甚至TEE所在的操作系统本身都无法篡改TEE中的代码和数据，这是物理层面的防篡改保护。
* **机密性**：攻击者、TEE的拥有者和运维人员都不能访问TEE中的内容（代码和数据），可以保证数据的隐私

## 3.2.预言机和TEE的结合点

结合点主要在于把预言机oracle节点运行在TEE中，提供更高层级的安全防护，基于TEE的特性，还是两个层面：

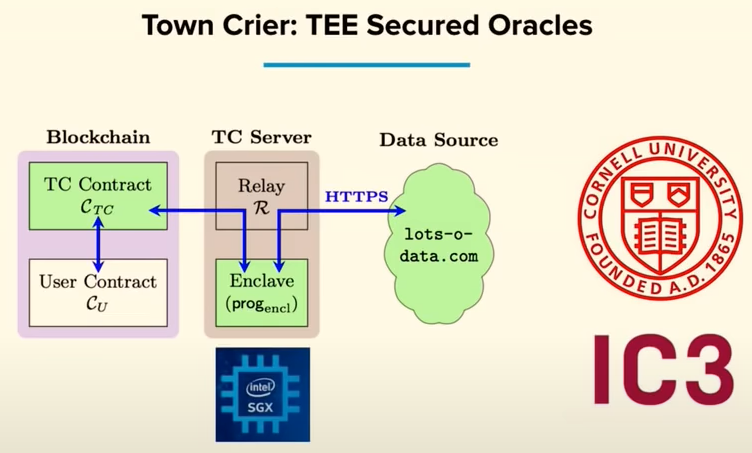
* **完整性**：由于攻击者无法篡改TEE中的代码，可以确保oracle节点是一个诚实的oracle节点，提供给智能合约的数据不会被篡改。
* **机密性**：由于攻击者无法获取TEE中的内容，利用此特性可以安全地处理敏感数据，比如密码、私钥、个人身份信息。

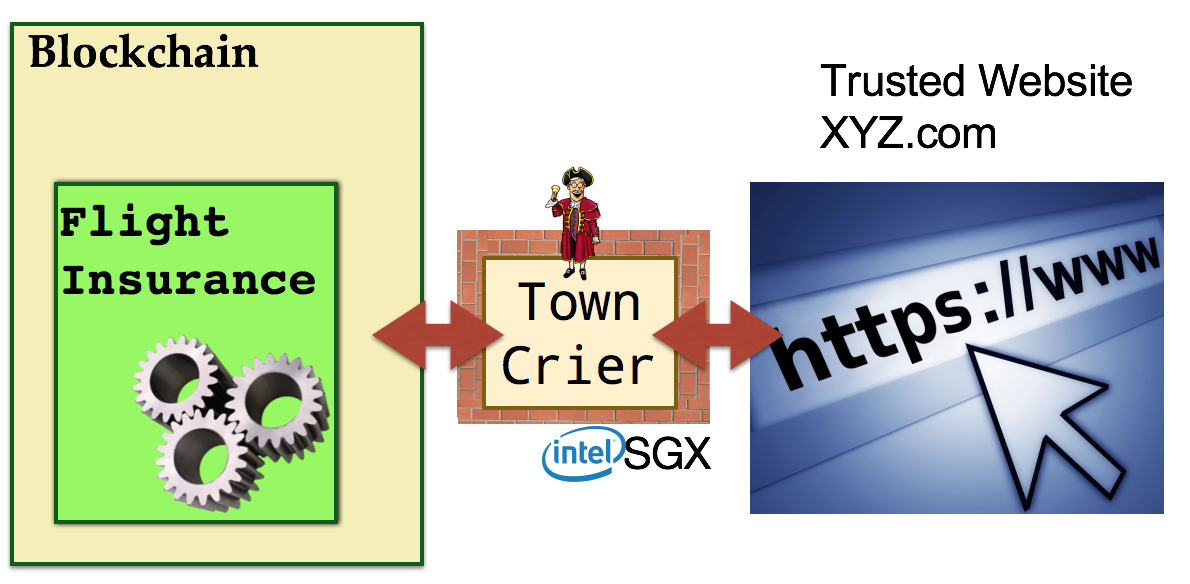
## 3.3.基于TEE的预言机的主流方案---Town Crier

目前业界的主流方案是依然是基于chainlink的方案---Town Crier。Town Crier是一个单独的产品，同时也是chainlink生态圈的一部分，其主要的技术人员是顶级学府康奈尔大学的教师和学生（很大一部分是华裔），有些成员还是chainlink的技术顾问。康奈尔大学在区块链领域的研究是比较领先的，并且提供了很多的区块链课程，所以康奈尔大学的技术实力基本没有什么问题。

Town Crier提供了部署在TEE中的oracle节点，能够很好地保证代码和数据的完整性和机密性。可以将TEE看作一个黑盒，一种可在其中安全运行程序的加固的不透明环境，可以将TC（Town Crier的简称）看作运行在这样一个黑盒中的oracle。

TC采用的TEE是Intel的SGX（Intel Software Guard eXtensions），它被植入到了Intel的CPU中，其不仅提供了完整性和机密性，还提供了attestation：一种特定程序正在enclave中运行的远程证明。





### 3.3.1.oracle完整性

chainlink的去中心化特性确保了oracle的完整性，基于TEE的oracle节点又从硬件防护的层面提供了新的一层oracle完整性，所以基于去中心化和TEE，oracle完整性有三种方案：

* **去中心化方案**：从多个oracle节点以及数据源头获取数据
* **TEE方案**：只从一个部署在TEE中的oracle节点获取数据，攻击者无法篡改数据，但数据来源还是单一的，无法解决单点故障问题
* **去中心化+TEE方案**：前两种方案的结合，从两个维度保证了oracle的完整性，这是最安全的一种方案

### 3.3.2.基于TEE的oracle机密性

如前所述，攻击者、TEE的拥有者和运维人员都不能访问TEE中的内容（代码和数据），可以保证数据的隐私，基于TEE的oracle节点可以安全地处理敏感数据，比如密码、私钥、个人身份信息。

接下来用几个典型应用场景来阐述基于TEE的oracle机密性

#### 场景1：链上链下资产交换

Alice和Bob约定好，Alice用50个腾讯Q币换取Bob的50个ether。大致逻辑是：Alice通过腾讯的Q币平台发送50个Q币给Bob🡪智能合约查询Alice的确已经发送了50个Q币给Bob🡪智能合约转Bob的50个ether给Alice。

然而，智能合约发送50个ether给Alice很容易，但合约很难验证Alice的确已经发送了50个Q币给Bob，因为没有一个公开的API来查询，必须要通过Alice通过账号和密码登录进Q币平台查询自己的转账记录才行，或者说通过一个API来查询，但是需要用Alice的密码作为参数。

**解决方案**：Alice可以把密码发送给TC oracle，用这个密码登录，然后验证她的确发送了Q币给Bob，验证结果只需要返回是或否即可。因为TC oracle部署在TEE中，能够保证密码不被泄露。如果oracle不是部署在TEE中，则不能保证Alice密码的安全，所以涉及到隐私信息的场景，就适合用TEE来解决。

#### 场景2：智能合约管理飞机延误险

某人乘坐某一趟航班，买了一份延误险，智能合约通过oracle判断该飞机是否晚点，如果晚点，就自动通过oracle调用链下支付进行赔付

这里有两个需求：

* **需求1**：某人坐的航班号不应该在区块链上可见，因为这属于隐私，不应该被公众看到

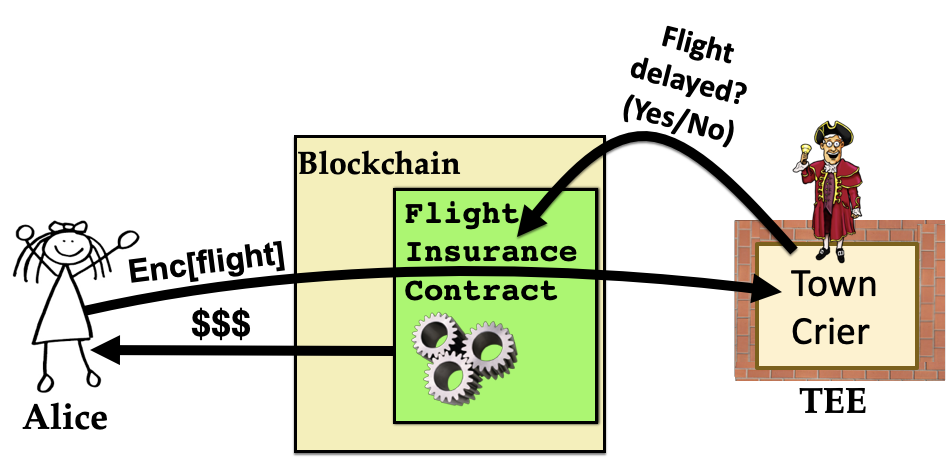
正常思维：智能合约需要从oracle节点获取某趟航班是否延误的信息🡪意味着智能合约需要知道某人乘坐的航班号🡪航班号就被记录在了区块链上，然而航班号是个人隐私信息，不应该公开在链上被所有人都能够访问

**解决方案**：智能合约使用oracle节点账号的公钥对航班进行加密🡪由于最终是oracle节点需要航班号来判断航班是否延误，所以oracle节点通过其私钥对航班号进行解密

然而，这个方案依然有瑕疵：如果oracle节点不是运行在TEE中，那么oracle节点的拥有者或运维人员可以获取解密后的航班号，导致航班号泄露，造成隐私泄露

* **需求2**：某人坐的航班号不应该在oracle节点被泄露

**解决方案**：通过TC，把oracle节点运行在TEE中，这样oracle节点的拥有者或运维人员就不能获取解密后的航班号，保证了航班号没有泄露，达到了“可用而不可见”的效果，智能合约调用oracle的接口查询航班是否延误，oracle节点只需要返回是或否即可。这就解决了需求1方案中的缺陷。



总结来说，通过TEE oracle就能很好地解决隐私安全问题。

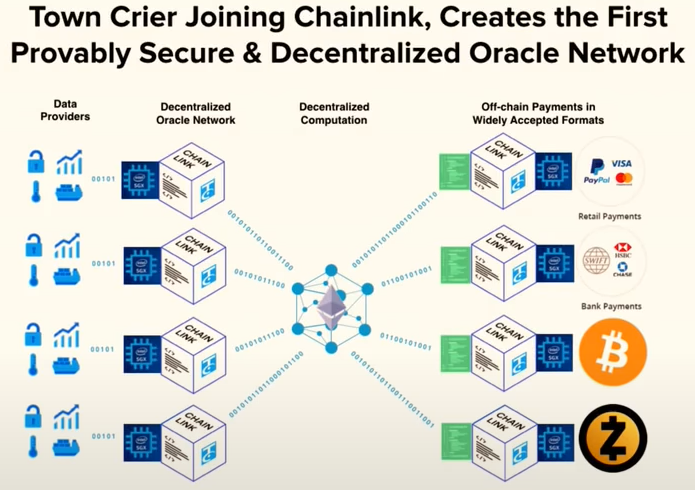
#### 场景3：贷款智能合约的隐私计算

假设有一个贷款智能合约，它需要根据合约创建者专有的特殊公式F来确定一个人是否有信用，例如，F可能会结合一个人的银行账户余额，在社交媒体上的朋友网络的质量，以及在主要机构（如支付宝）的信用评分来决定是否准予发放贷款。

在整个过程中涉及三种类型的机密性

* 某人登录网站（比如支付宝芝麻信用）获取信用评分时使用的凭证(如密码)
* 信用评分数据本身
* 公式F本身，合约创建者可能希望保密

**解决方案**：和场景2类似，同样可以把需要保密的数据通过oracle节点的公钥加密后发送给oracle节点进行处理，oracle节点的返回结果仅仅是某人是否有信用，true或false，然后智能合约调用链下支付接口发放贷款。这就是Town Crier结合chainlink体现出来的价值，完全可以解决真实世界中的很多问题。



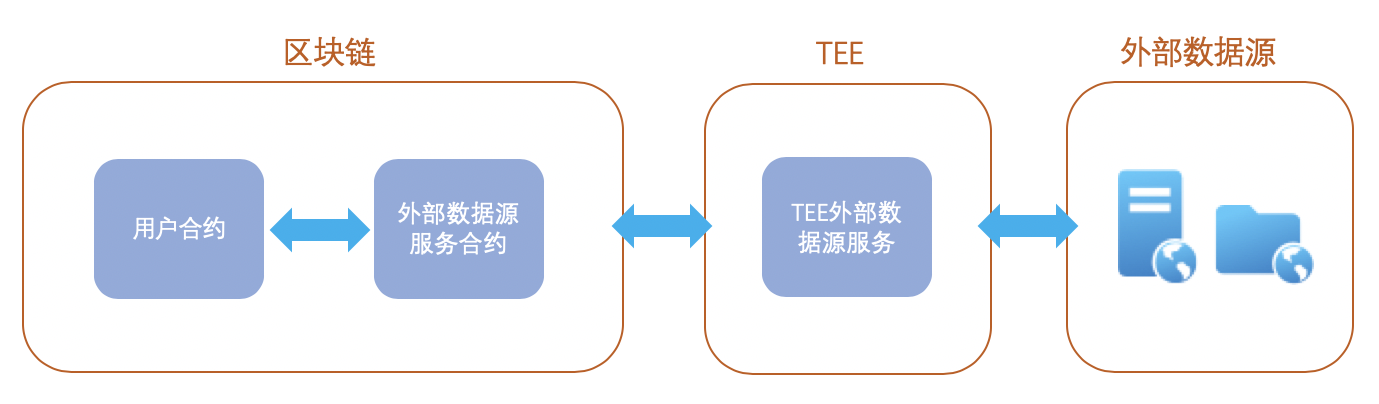
#### 场景4：IoT设备的监控和控制

可以使用GPS或北斗全球定位系统跟踪食品的运输，监测和分析温度传感器数据，以确保冷链的完整性，并在付款后和其他条件满足时解锁集装箱。贸易的支付取决于IoT传感器确认货物的安全到达🡪货物到达后智能合约自动发起支付🡪真正做到不可抵赖的货到付款，一手交钱一手交货。

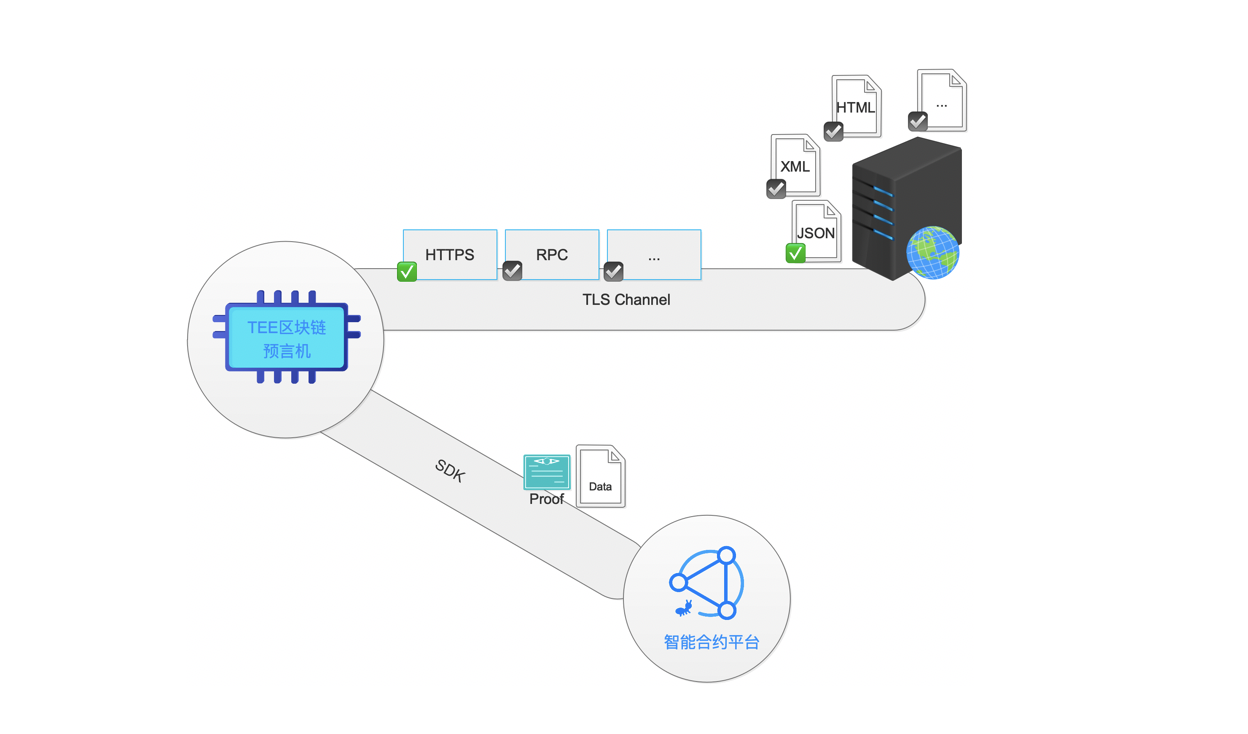
# 4.国内大厂的预言机布局

从网上可以获取的资料来看，腾讯、京东、百度、华为在预言机领域都没有布局，搜不到资料。

只有蚂蚁链在预言机领域是有明确布局的，蚂蚁链的BaaS平台推出了基于TEE的oracle服务，其基本理念和逻辑和chainlink+Town Crier基本一致，外部数据源服务会在智能合约平台部署一个外部数据源服务合约，用户合约通过调用该服务合约发送外部数据源请求，链下的 TEE 外部数据源服务对接该服务合约，监听用户的请求，然后去对应的外部数据源取数据，最后将结果返回给用户合约。



外部数据源服务使用 TEE 技术实现，对于每笔外部数据请求都将在可信硬件环境中执行。可信硬件环境会验证外部数据源的 TLS 通讯证书以确认数据源的身份，通过 TLS 协议确保拿到的数据没有被第三方篡改。可信硬件环境得到数据后，会使用硬件私钥对数据进行签名，并返回给智能合约，智能合约将自动验证可信硬件的签名，确保数据是可信硬件执行结果，没有被第三方篡改，从而安全可靠地获取来自指定外部数据源的数据。



蚂蚁链推出的基于TEE的oracle服务和chainlink结合Town Crier的方案有如下的不同：

* 蚂蚁的oracle服务是基于蚂蚁链这个联盟链的，不是基于公链的。虽然是集群服务，但是oracle节点是蚂蚁链这一家公司部署的，是中心化的，虽然说TEE能够很大程度上保证数据的完整性和机密性，但始终存在单点故障，也不能完全排除单个公司篡改数据的可能。chainlink结合Town Crier除了同样是基于TEE的，也是基于公链的，去中心化的方案，任何人都可以部署自己的oracle节点，为其他人提供服务，保证了数据来源的多样性。从去中心化这个角度讲，chainlink结合Town Crier的方案优于蚂蚁链的方案。
* 蚂蚁链的方案是基于蚂蚁自己的联盟链的，可以直接和蚂蚁链上的智能合约交互，但不能和其他联盟链比如FISCO,Fabric等交互。而chainlink结合Town Crier的方案是基于以太坊的，仅能和以太坊上的智能合约交互，所以，要和联盟链如FISCO,Fabric等交互，比如通过上层应用作为中介来实现。
* 蚂蚁链的方案基于联盟链，所以没有类似于chainlink的token激励机制。蚂蚁链的oracle节点的利润来源于使用蚂蚁链BaaS整体解决方案的客户，chainlink oracle节点的利润来源于提供预言机服务所获得的LINK token。
* 蚂蚁链是没有开源的，无法基于其做二次开发或部署。chainlink是开源的，可以做二次开发以及部署自己的节点（基于国产TEE）。

# 5.参考资料

chainlink官方文档

https://chain.link/

Town Crier官方文档

https://www.town-crier.org/

chainlink白皮书

https://link.smartcontract.com/whitepaper

Town Crier白皮书:An Authenticated Data Feed for Smart Contracts

https://eprint.iacr.org/2016/168.pdf

Decentralized Oracles: Reliably Triggering Smart Contracts using Decentralized Computation and TEEs

https://www.youtube.com/watch?v=yHh-j\_NdRZw

Town Crier and Chainlink: Enriching and Extending the Possibilities of Oracles

https://blog.chain.link/town-crier-and-chainlink/

Developing with Chainlink Decentralized Oracles: Unitize2020 Hackathon Presentation

https://www.youtube.com/watch?v=wmALQok\_WFg

ETH/USD feed

https://market.link/feeds/6dd8e645-0b17-4f7b-b169-bbec8abe9e29

What Is Chainlink? Introduction to LINK Token

https://cryptobriefing.com/what-is-chainlink-link-token/

BSN成功引入IRITA跨链和Chainlink预言机服务

https://www.sohu.com/a/404453963\_100217347?\_trans\_=000014\_bdss\_dkmwzacjP3p:CP=

大国重器 即将发布的国家区块链平台BSN是什么

http://blockchain.hexun.com/2020-04-24/201131617.html

Trust No Dapp: Chainlink Launches Oracle for Provable Randomness

https://www.coindesk.com/trust-no-dapp-chainlink-launches-oracle-for-provable-randomness

Solidity Development: Setting up environment

https://medium.com/coinmonks/solidity-development-setting-up-environment-611c4bc2530b

PRICE REFERENCE DATA

https://feeds.chain.link/

Omniscience node

https://market.link/nodes/62bb8c36-220e-4645-8bd9-4d7400e3cc17/jobs

Chainlink Library

https://docs.chain.link/docs/chainlink-framework

Chainlink Market

https://market.link/

Driving Demand for Enterprise Smart Contracts Using the Trusted Computation Framework and Attested Oracles via Chainlink

https://blog.chain.link/driving-demand-for-enterprise-smart-contracts-using-the-trusted-computation-framework-and-attested-oracles-via-chainlink/

Decentralised Oracles: a comprehensive overview

<https://medium.com/fabric-ventures/decentralised-oracles-a-comprehensive-overview-d3168b9a8841>

蚂蚁链外部数据源服务概述

<https://antchain.antgroup.com/docs/11/108575>

蚂蚁区块链项城：TEE+预言机，蚂蚁为大规模、金融级场景提供隐私保护“大杀器”

https://www.8btc.com/article/404602

蚂蚁区块链第18课 区块链预言机(ORACLE)的定义及在蚂蚁BAAS中的使用

https://blog.csdn.net/wangdenghui2005/article/details/89187097