**初始预言机（Oracel）**

**——203 王玥**

* 官方定义:区块链外信息写入区块链内的机制
* 功能：将外界信息写入到区块链内，完成区块链与现实的数据互通；使确定的智能合约对不确定的外部世界进行数据交互的唯一途径，也是区块链与现实世界之间实现数据互通的工具。
* 产生原因：区块链是一个确定的、封闭性的环境，它只能获取到链内的数据，与链外世界是割裂的；而智能合约不允许不确定的事情或因素，所以VM不让智能合约进行I/O操作、对外请求、网络调用等，当触发条件是链外信息时，就需要预言机来提供服务
* 解决方法：用户的智能合约将请求发送给链上Oracle合约，通过链下的API接口获得外部数据，然后Oracle合约再把数据给用户的智能合约
* 应用场景：一切需要与链下进行数据交互的DApp

eg：DeFi、博彩游戏、借贷平台、快速追踪/IOF等

* DeFi：对于稳定币系统，需要获取ETH的的实时价格来判断货币是否达到平仓价格进而触发平仓，否则由于ETH价格实时变化、网络原因等，每个节点获取到的E价格可能不同，会导致节点间无法达成共识
* 博彩游戏：其核心是不可预测、可验证的随机数；但在链上是不能生成随机数的（即使可以生成，也是伪随机数，其随机数是可以被预测和破解的）这时候就需要预言机从外部给智能合约安全的、不可预测的随机数。

我是参考一个博主的文章写的

他在评论区也解决了我原本也存在的一个疑问

Q：有人觉得预言机是一个伪概念吗？因为所谓的外界信息也是非常中心化的，预言机只是把输入答案这个事情自动化一点，可是如果输错了也是错了，并不能保证传递的链外信息的真实性

A：首先离开具体场景谈中心化、去中心化和信任就容易得出错误的结论。“飞机晚点了没” - 正常是不是去查一下飞常准或者google flights? “现在几度” - 一般是不是用气象软件或雅虎天气搜一下？“现在BTC/USD什么价格” - 是不是看一下CoinMarketCap或者某个常用交易所的数据？可见的信息的正确与否、是否有价值是对特定使用者和使用场景而言的，而且追根到底信任总是有一个载体，不会凭空产生。智能合约要想有大规模应用场景必然离不开它特定应用场景下的链外数据，这是能通过预言机来提供的的；至于某个具体的合约需要什么样的数据源，这是需要合约来指定的而且这些数据源对预言机来说都是无差的。一个做crypto借贷的合约如果需要知道币安BTC/USD的价格流那应该显明的指出这个数据源，那么意味着在这个场景下合约默认信任了币安的数据 (不然整个应用场景都不成立)，那么预言机在证明自己没有作恶篡改输入的情况下就可以给合约提供来自币安的authenticated data feed。如果合约不信任币安的数据，那么要么不使用币安的数据，要么告诉预言机除了币安之外还需要Bitfinex和Coinbase的数据然后在合约内用三个数据源做交叉验证 - 这是应用层的需要做的，但不是预言机在协议层(或者说infra层)必须做的。协议需要保证的是预言机对每个请求怎么自证清白没有篡改结果，如果有篡改怎么监测出来并且惩罚恶意提交者。这是应用层和协议层的典型区别。如果预言机网络连接了足够多的数据源并且有足够多的需求方时，也许可以通过一个marketplace来提供聚合了几个典型数据源的数据来让合约更简单的获取常用的数据 - 比如币价，但这不是必须的，在一开始不会提供。

## Chainlink

是一个去中心的预言机项目，以最安全的方式向区块链提供现实世界中的数据，在基于预言机原理的实现方式上，围绕 LINK token 通过经济激励建立了一个良性循环的生态系统。Chainlink 预言机需要通过 LINK token 的转账来实现触发。

下面链接是一个简单的获取ETH价格的代码例子，讲解Chainlink预言机的基本过程：https://learnblockchain.cn/article/587