什么是预言机（Oracle）

原文作者：DOS Network Team

原文来源：_DOS Network

智能合约存在外部数据的交互需求。比如，一些像是股票或者币价的实时价格数据，天气预报，市场预测等其他数据。

那么，这里就引出了预言机（oracle）这样一个概念。

什么是预言机?

预言机就是一种单向的数字代理，可以查找和验证真实世界的数据，并以加密的方式将信息提交给智能合约。预言机就好比区块链世界中的一个第三方数据代理商。

举例来说，假设现实世界中的「数据源」和区块链中的「数据接口」，是两个使用不同语言的国家，预言机就是中间的翻译官。通过预言机智能合约就可以和链外数据进行无障碍交流。

在实际使用智能合约中，需要预言机对数据进行验证。因为区块链也是基于共识的系统，所运行的智能合约也要求一定要是确定性的程序。预言机对数据验证这一步骤是为了契合共识机制，使最后反馈给智能合约的数据也是「确定性」的。

预言机的运行原理：当区块链上的某个智能合约有数据交互需求时，预言机在接收到需求后，帮助智能合约在链外收集外界数据，验证后再将获取的数据反馈回链上的智能合约。

区块链为什么需要预言机?

因为区块链上的智能合约和去中心化应用（DAPP）对外界数据拥有交互需求。

区块链是一个封闭的环境，链上是无法主动获取链外真实世界的数据。主要是因为区块链无法主动发起 Network call （网络调用）而链上智能合约是被动接收数据的。其次，智能合约其实并不「智能」，它只是在满足相应条件下，才达到触发状态的程序。同时，智能合约最终的执行需要合约参与方的私钥签署，智能合约本身没有办法自动执行。

当智能合约的触发条件取决于区块链外信息时，这些信息需先写入区块链内记录。此时需要通过预言机来提供这些区块链外的信息。

先举一个通俗易懂的例子，假设现在我被关进了一个小黑屋里，我对外面的世界发生了什么几乎一无所知，不知道外面是否有人，即使呼叫也没有人回应，只有外面的人在门口告诉我，我才可以得知外面的改变。

智能合约就像这个例子中的「我」一样，它无论何时何地，都无法主动向外寻求信息，只能外部把消息或数据给到里面。而预言机就是这个在门口收到我的请求后，从外面输送消息和数据的人。

或许你又会提出疑问为什么链上无法直接导入和接收数据？主要是因为区块链的共识机制。

区块链是基于共识的网络，所运行的智能合约也要求一定要是确定性的程序，每笔交易和区块处理过后，每个节点必须要达到相同的状态。但是数据本身具有复杂性和多样性，这也是为什么预言机为了契合区块链的共识机制，除了搜集数据还有一步数据验证的步骤才将最后的「确定性」信息反馈给智能合约。

预言机应用场景有哪些?

目前预言机在区块链里涉及的应用领域有菠菜、稳定币、借贷、金融衍生品、保险以及预测市场。目前，比较热门的应用场景是菠菜、稳定币和借贷。

1、菠菜（Bócǎi）

区块链内菠菜 Dapp 或者菠菜类游戏都涉及到随机数。菠菜类应用的核心是不可预测、可验证的随机数，随机数决定赌注的最终结果，但是在封闭状态的链上无法产生安全的随机数。

现在的大多数菠菜游戏都是在链上生产随机数，所以很容易被预测和破解导致资产被盗。之前一些菠菜类应用因为随机数问题而遭受黑客攻击，比如 EOS 上面的掷色子游戏或者以太坊上的 FOMO3D。因为他们没有满足智能合约 /Dapp 场景下对安全伪随机数的要求：随机，不可预测。他们用到链上公开，被其他合约所调用，可以被预测的信息所生成的种子（seed）从而导致他们的随机数可以被预测。菠菜类游戏，要想得到安全的随机数，只有通过预言机从链外获取。

2、稳定币

目前预言机主要服务于加密资产类稳定币。

加密资产类稳定币是由加密货币抵押为基础。加密资产类稳定币不是保持一对一的比率，而是试图通过维持更高的抵押品与稳定币比来将其价格与法定货币挂钩。例如 DAI 和 bitUSD。DAI 通过超额抵押资产发行，其抵押物为以太坊等链上资产。

加密资产类稳定币有链外信息交互需求，需要预言机实时的去获取外部世界稳定货币本身和锚定资产的兑换率等数据。

3、借贷

NEST、抵押借DAI、 ETHlend 等去中心化 P2P 借贷平台允许匿名的用户用区块链上的加密资产抵押，来借贷出法币或者加密资产。

这类应用需要使用预言机在贷款生成时提供价格数据， 并且能监控加密抵押物的保证金比率，在保证金不足的时候发出警告并触发清算程序。同时，借贷平台也能用 Oracle 来导入借款人的社交和信用和身份信息来确定不同的贷款利率。

哪些团队正在开发预言机?

1、Oraclize：

Oraclize 是一个为以太坊提供中心化数据传输预言机服务的项目，其依托亚马逊 AWS 服务和 TLSNotary 证明技术，提供预言机的服务。在区块链环境下，Oraclize 把获取的信息返回链上且保证保证数据与数据源相同，用户可以自行抓取数据。Oraclize 不干涉信息源的选取和信息源本身的准确度。

2、Augur：

不同于 Oracle 的中心化，Augur 是一个去中心化的预测市场平台。Augu 的核心是预测市场，主要是通过利益驱动的投票机制来确定结果。用户可以用数字货币进行预测和下注，依靠群体智慧来预判事件的发展结果。用户可以选择围绕任何未来事件创建预测市场，参与者可以押注该事件的结果。参与者根据创建的未来事件的实际结果赢钱或者输钱。平台本身无法验证事件的真实结果是什么，因此 Augur 依靠用户和复杂的结果报告系统来鼓励诚实的结果报告行为。本身也可以作为其他应用的输入源，但是它们的输出结果需要很长时间的延迟和大量用户的参与。

3、Chainlink：

Chainlink 是第一个去中心化的预言机。比起 Oraclize 的中心化，Chainlink 更符合区块链去中心化的准则。Chainlink 主要提供用于帮助智能合约访问关键链外资源、网站 API 和传统银行账户支付的预言机服务。链下节点来提供数据，chainlink 的链上部分会收集数据请求的需求，然后收集合适的节点的回答，在加权得到结论后反馈给信息请求方。chainlink 也拥有一个对节点的信誉评价体系，信息需求方可以选择特定信誉级别的节点，每次信息反馈之后也会更新每个节点的信誉评分。

4、DOS Network

DOS Network 是一个提供去中心化的预言机服务的网络。它可以连接智能合约和链外互联网世界，同时也为区块链提供无限的且可验证的计算力。Dos Network 在链上监测用户数据请求，链下监控和接收数据请求，再通过链下随机选一组节点来提供数据，一旦收集来的数据通过组内 51% 节点共识被视为「正确答案」，最后链下再将获取的答案反馈给链上信息请求方。DOS 设立一个对于诚实节点的奖励机制：除了给节点的数据处理费，30% 总供应量的虚拟采矿奖励，持续十年。