我们在区块链白皮书里经常会看到这么一个词：“Oracle”。这个Oracle到底是什么东西？和硅谷的甲骨文公司到底有什么关系？今天，小编为你一一解答！ 

不知道大家发现没有，现在的区块链白皮书中会经常出现一个词组：预言机
oracle甚至有时只使用单词 oracle。这些白皮书通常强调 oracle 非常重要，却基本没有对其含义准确的说明。一般读者如果不懂技术自己查询往往也会陷入迷茫：因为这个词的常见翻译 “先知”、“预言”
等都有很大的迷惑性。这些神叨叨的意思，和区块链到底有什么关系？这个 oracle 跟甲骨文公司 Oracle、或者甲骨文公司的 oracle 数据库有什么关系吗？其实，还真有一毛钱的关系！1、预言机的用武之地：智能合约要想理解预言机
oracle，就需要知道它的背景，也就是白皮书频频提到的“价值”，那就是 oracle 是智能合约的重要基础。而智能合约是以以太坊为代表的区块链 2.0 的标志性技术，是区块链技术走向商业化的一块重要基石。智能合约，简单地说，就是一段满足一定条件就可以自动执行的程序。智能合约其实没你想得那么“高大上”，我们现在的生活里也有智能合约的雏形，比如 “信用卡自动还款”，其实就可以视为一个低级版的智能合约：信用卡一般和另外一张银行借记卡绑定，到了还款日，如果银行卡中有足够的余额，则信用卡会自动扣钱还款。怎么样，目前为止的内容都还能看懂吧！那咱再举一个更复杂也更具有商业化前景的案例，你也一定能看懂：2018 世界杯即将开赛，球迷可用智能合约来实现对赌，比如有球迷 A
预测巴西队会夺冠，另有球迷 B
预测德国队夺冠。这就可以开设一个赌局：巴西队夺冠，则 B 的赌注判给 A，反之亦然，如果两队都没有夺冠，则赌约自动解除。赌约的规则很简单，但在区块链去中心化体系下存在一个关键问题是，如何将比赛结果放进这个赌约当中去？也就是说如何扣动扳机，让这个智能合约运转起来？这对传统博彩业来说极其简单。球迷竞猜其实是和博彩公司对赌，博彩公司其实暗中承担了赌约的信息输入和胜负判决的责任，既当拳击手，又当裁判员。也就是说，博彩公司承担了赌局的组织和信用职责，这也是博彩公司肥利的基础。但在去中心化的区块链体系中，赌局双方是意见不同的球迷，没有了第三方中介机构，也就取消了裁判，由此产生了谁来宣布赌局胜负的问题。这就需要第三方信息的介入，这个功能就是预言机 oracle 发挥作用的地方。这是一个表面简单，但实际比较复杂的问题。智能合约还有更广泛的应用，比如金融领域的股票、保险、期货、期权交易，供应链中的物流、信息流、资金流的合一，智能制造中的定制化生产等等，都可以使用智能合约来提升效率。而在这些复杂应用场景中，如何确保第三方输入信息的准确性是智能合约发挥威力的关键。2、链上链下的隔离区块链系统从功能角度讲，是一个价值交换网络。目前，BTC、ETH 等虚拟币是具有货币属性的资产。未来，人类拥有的实物资产、股票、各类卡券，甚至学历、著作权等资质证明，都可以定义为 token（代币）在这个网络中流通。这也是区块链的独特优势。区块链上的信息都是有序的、标准化的、

可信的，但是现实世界却是无序的、复杂的、可信度难以判断的。瞄准现实世界的智能合约才有广泛性和商业价值，但区块链和现实世界的隔离是制约智能合约发展的一大障碍。举一个简单的例子，现在有一个赌局：看美国总统川普是能强力控局，干满四年任期，还是在此之前就被建制派弹劾下台？这可不是无聊的政治八卦——大国的政治走向会深刻影响社会。基于这样的赌局，可以做很多金融交易决策，类似的案例还有英国脱欧等。这些事件在现实社会一旦发生，其重要性不言而喻。但是，区块链系统中却无从判断外面现实世界发生的事件，这就需要我们引入一种机制将现实社会的事件输入区块链之中。不过，因为区块链“去中心化”的特点，没有一个节点可以对输入信息的真伪做出裁决，如果这种机制设计得不够周密，那么参与智能合约赌局的一方就很有可能为了利益而否认事实。其实某些有大量“客观数据”产生的应用中，仍然存在输入信息是否可信的问题。我们拿橡胶期货交易作为的例子：橡胶是热带作物，受日照、气温等自然因素很大，橡胶的交易又受汽车、合成橡胶、外汇等多种市场因素影响。基于天气数据和各类市场交易数据可以构建一个基于智能交易合约的交易模型。从表面看，这些数据都可以从气象站、公司网站、交易所直接导入，但实际上一旦涉及利益，就无法完全保障提供这些数据的机构不作恶。这就是为什么我们非要引入一种机制，以保障输入智能合约的数据都是可信的，这就是 oracle。Oracle
是连接现实世界和区块链系统的桥梁。3、oracle 是一种机制有文章把 oracle 说成是为区块链提供外部数据的信息平台或技术，这么理解当然没有错，但可能没有完全揭露实质。比如共识机制解决了区块链各节点信息统一的问题，不完全靠的是技术，它也同样依靠利益平衡机制：在 POW
机制中，作恶的节点记账结果会遭到拒绝承认而白白浪费电力；在 POS
机制中，虽然存在“富者恒富”的弊端，但至少富者和全网络的利益是一体的，所以他们有动力维护系统的稳定；在 DPOS 机制中，认真负责的节点会被赋予记账权并获得激励，反之则被撤销记账权。为确保链外数据的可靠性，也需要引入各种机制“惩恶扬善”。目前，常见的机制包括“多数据源互相认证，通过投票和惩罚的机制来减弱撒谎的动机，通过事前投资获得验证权的方式减少‘僵尸粉（Sybil Attack）’的影响”等等。听起来似乎我们已经把所有能想到的问题都解决了？其实，尽管已经有很多尝试，但目前 oracle 设计仍有两大障碍：一是 oracle 的安全性不够，被骗的可能比在现实世界中被骗的可能仍然大很多；二是成本高，智能合约使用 oracle 的花费的时间和投入，比在现实世界中获取信息要高得多。其中第一个障碍涉及到尚没有得到完全解决的博弈论问题：在一个系统之中，如果一半以上的成员都是坏人的情况下（好人占多数的情况下，好人的收益是有限制的），是否有一种机制限制坏人作恶，并保证这个系统产生的数据是真实可信的？所以，基于以上原因，笔者认为，在可以不经允许即可加入网络的公有链上运行智能合约还会遇到较大困难。较为实用的智能合约可能会在相对去中心化的联盟链、私有链中首先落地，因为参与联盟链、私有链的节点已经有一定程度的信任基础，他们对进入区块链的外部数据的可信度也更容易达成共识。为什么叫
oracle？由上已经可以得知，oracle 就是为区块链智能合约提供可信链外数据以触

发智能合约顺利执行的数据源。那么问题来了，为什么叫
oracle？如果直接百度搜索
oracle，你多半会查到甲骨文公司，或者是甲骨文公司的 oracle
数据库技术和产品。查专业词典就可以发现这个词的多种含义：Oracle 一词最初是来源于古希腊宗教，意为“神谕、神使、先知、预言”，很多提到区块链 oracle 的文章就直接取了 oracle 的本意。这个词还有一些宗教色彩更淡的词义，如“圣贤、哲人、睿智的回答”等；再经过演化，oracle 就产生了“指示物，可靠的指导（如钟表等）”等含义，已经完全失去了宗教和神秘色彩，纯粹指可以信赖的人或物。比如我们可以说 “ my sister is the oracle on beauty
matters——我妹妹是美容方面的大行家”。所以，笔者认为，区块链的 oracle 应该理解为“区块链可信数据源”。那么，我们在讨论区块链时提到的
oracle，和甲骨文公司的 oracle 有没有关系呢？甲骨文创始人 Ellison 和 Miner 给新公司起名确实是取的“神谕、先知”等宗教、神秘含义，装个X嘛，可以理解。这就是区块链 oracle 与甲骨文公司的一毛钱关系。至于为啥美国的 oracle 公司到中国就注册成了“甲骨文”公司，那是因为中国殷商时代的“甲骨文”
被翻译为 oracle bone
inscriptions。有中国独有文化特征的甲骨文又为啥被翻译成有希腊宗教色彩的 oracle 呢？因为“甲骨”也是占卜用的，和 oracle 的“神谕”含义接近。当然也有人认为这样的翻译并不妥当，那就是与本文更远的糊涂账了。