如何让区块链连接外面的世界

文丨高志豪

“世界那么大，我想去看看”——2015年4月14日早晨，一封辞职信引发热评。同一年，Reality Keys和Oraclize相继推出Oracle（这里是指预言机，而不是指甲骨文数据库）解决方案，带着区块链区看外面真实的世界。

高志豪（Elwin）

资深互联网技术专家，拥有超过十多年多的企业大型IT系统、互联网产品、移动应用、区块链等产品设计及多终端跨平台架构和系统开发经验，目前是广州两家软件公司及互联网公司的技术总监。

为什么要带着区块链看外面的世界？

首先，我们以一个实际场景来了解为什么要带着区块链看外面的世界。从一个基于区块链的数字货币交易平台来看，这个系统需要定时获取指定数字货币的最新价格，在传统的互联网系统中这个是最简单不过的，定期输入价格数据或通过第三方接口来获取数据即可，但就基于区块链的系统来说，情况会变得不一样。

在区块链体系中，第三方的外部数据来源（Data Feed）会发送给你的区块链和智能合约指定的信息数据，但由于数据传送者是一个中心化的参与者，因此不能想当然地认为智能合约可以自己去直接获取相关外部数据。比如你想从某些互联网交易中获取ETH/USD的最新成交价格，数据传送者会从这些交易数据中返回折中计算的成交价格。这个数据传送者也会整合不同的数据来源并达成共识获取平衡的交易价格。但是，你怎么能确保这个数据传送者不会在过程中修改数据？在接收外部数据的节点是单个节点又还是所有节点都接收呢？这些外部数据的又如何在区块链中达成共识呢？区块链本身是一个世界——去中心化的系统的世界，区块链对外界信息不了解，而币价是在区块链外部的信息，外面的信息如何输入到区块链里，众多区块链节点是如何接入外部信息，会否变成中心化方案，这个都会有很多变数。

那么，目前有什么方案可以解决区块链连接外面的世界的这些问题呢？就Elwin所了解的目前主要有Reality Keys和Oraclize两个比较成熟的方案。Reality Keys提供一个可以自动检查和加密预言提交的预言机方案，而Oraclize也提供一个类似的解决方案和并为以太坊的应用而度身定制。

Reality Keys：

Reality Keys是关于事实预测的加密证明，它的服务是提供自动化和人工验证的数据，将有希望提供新一代的自动化、无条件信任的信息服务。Reality Keys监测一系列的数据来源包括汇率、加密货币交易、个人训练目标（可以在Reality Keys网站建立)或在维基的数百万主题，所有这些都是基于公共提供的API接口。 除了公开的API外，任何人都可以往Reality Keys体检事实和检查存在事实的状态。Reality Keys的这个服务是完全免费的，只是另外提供人工二次确认的收费服务，来避免数据的自动化检查之外的疏漏或变更。

Elwin在此简单介绍一下Reality Keys的工作原理。针对每个事实（证明），在系统中设有两个ECDSA（椭圆曲线签名算法）类型的Reality Keys，一个是Yes，一个是No。我们自己持有私钥和对外发布公钥，这样你可以创建加密信息或比特币合约。对于以太坊的用户和其他高级的智能合约平台，系统会提供一个来验证结果的哈希和我们用来签名的地址。

当你创建一个事实时，系统会一直等待直到指定时间。系统此时会对正确API执行自动检查并发布结果。当出现任何人质

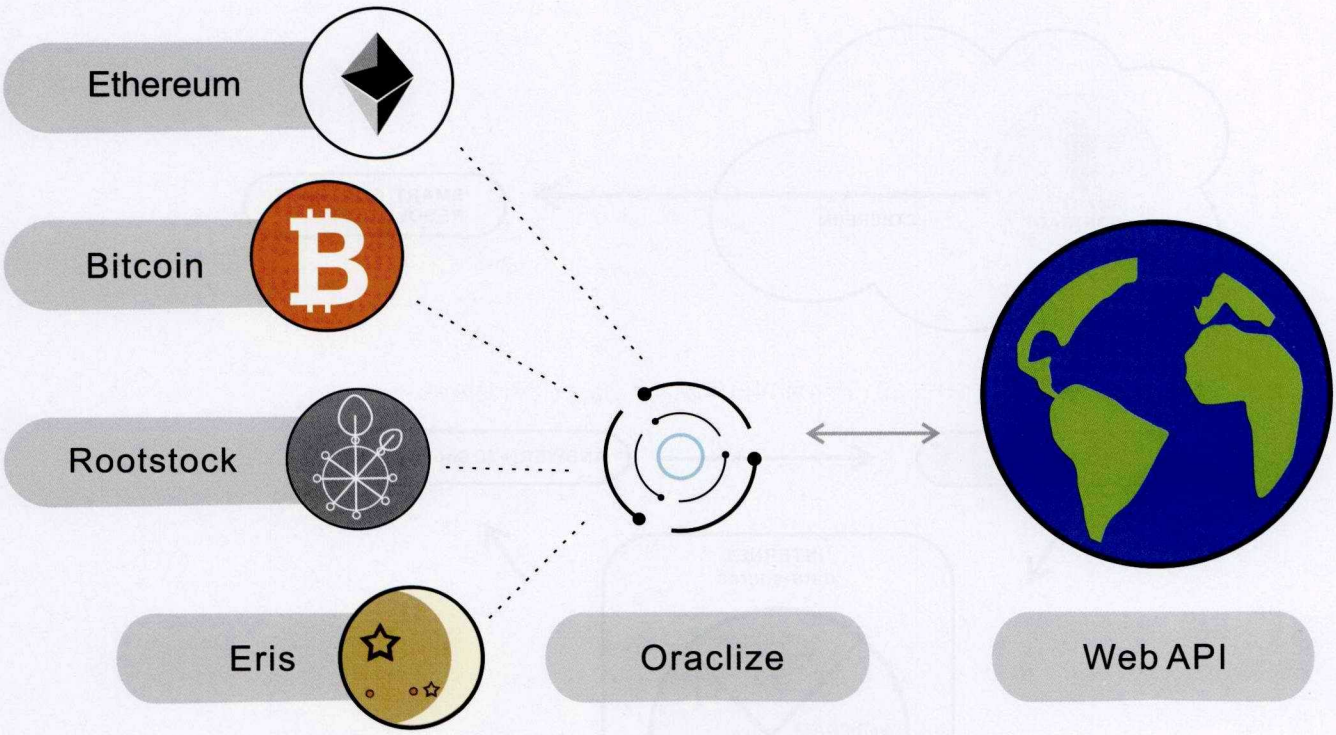

图1 各种区块链通过Oraclize连接互联网的示意图

疑通过API查询结果有误的情况，他们可以支付费用进行人工二次确认。否则会维持原来API返回的结果。当某个事实登记的时候，为每个可能的结果输出的公钥就会发布。而当结果被确认后，对应正确结果的私钥会发布。对应结果的私钥如果不存在则永远不会发布。对于被选中的结果，我们通过对应结果的私钥去解密信息或者完成比特币合约。如果私钥丢失，结果则永远不会被释放。我们也可以通过以太坊地址对返回值进行签名，以便支持以太坊智能合约。

在财务交易中，Reality Keys提供的数据可以被第三方托管系统进行验证。比特币和类似的去中心化虚拟货币允许你在网络直接执行担保交易，而不需要信任其他第三方。Reality Keys和比特币网络兼容，可以用来创建只针对某个支出来进行支付的交易。

Etheropt是一个完全去中心化的平台,目的是进行多种数字货币的期权交易。其中以太币的价格来源很多，包括主要的以太币交易所Poloniex，然后Reality Keys会对这些消息进行验证。平台无运营方，所有以太币交易、存储、提取、由以太坊智能合约自动执行。Reality Keys解决了外部价格信息获取的可靠性和真实性问题，使得这个去中心化自主交易能够得以顺利实现。

Reality Keys的开源代码地址：

https://github.com/realitykeys

Oraclize:

Oraclize定位为去中心化应用的数据搬运工，他作为Web APIs和DApp的可靠链接。有了Oraclize，就不需要建立额额外的信任链，因为我们的行为已经被强制加密验证。Oraclize是一个可证明的诚实的预言机服务，可以让智能合约访问互联网。Oraclize是平台关的，为所有主流的智能合约能力平台提供一种虚拟的接口。可以想象，通过这个投入成千上万的有意义的数据到区块链中，可以使得智能合约产业更繁荣和更多有价值的应用呈现更大的生命力。（**图1**）

尽管Oraclize是一个中心化服务，但他正在分享去中心化网络的远景，提供一个可证明的诚实服务。通过Oraclize,目前可以支持太坊、比特币币、RootStock、Eris(厄里斯区块链，一种联盟链）连接外面的互联网世界，获取有价值的信息。DApps通过使用Oraclize的服务做为额外一层用来作安全数据获取，确保DApps的系统足够健壮和可信，通过他们的oracle机制确保不易轻易被攻击。

用以太坊为例子，以太坊智能合约目前只

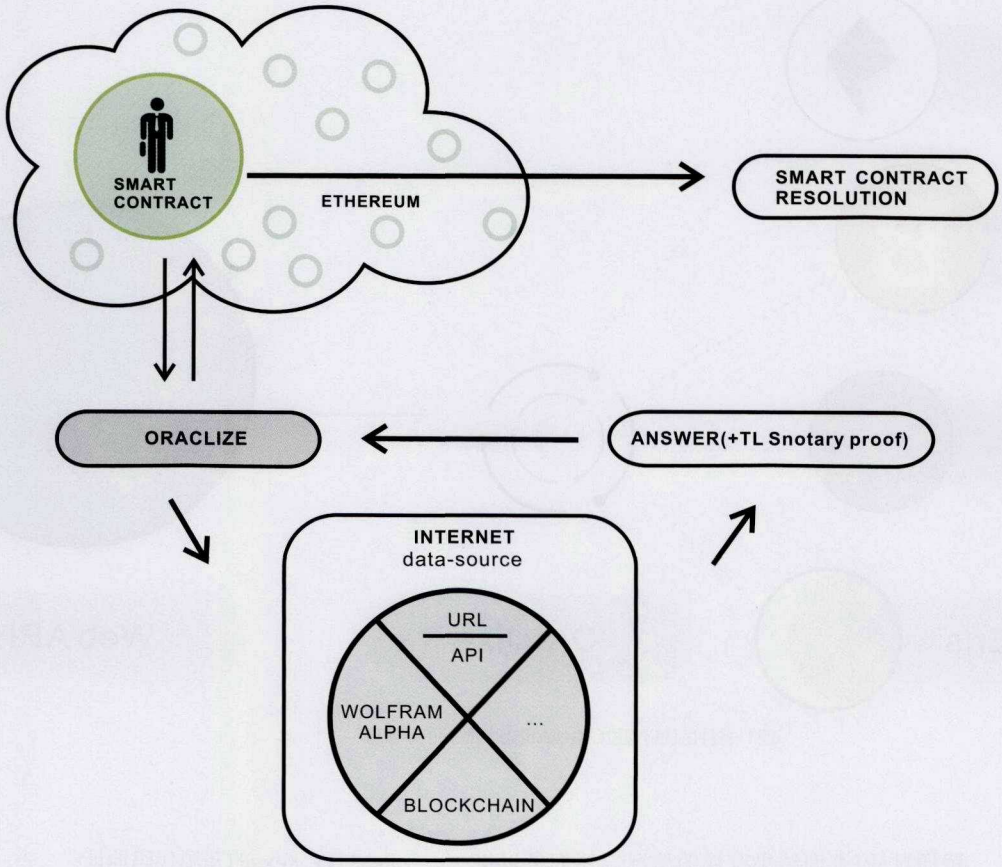

图2 以太坊智能合约通过Oraclize连接互联网数据的示意图

能存取访问链上的信息，它们自身无法取得外部信息和数据，而Oraclize作为一个数据传送者，可以在以太坊的DApps与Web APIs之间提供可靠连接，让基于智能合约的Dapp应用无需信任地取得外部信息和数据。在以太坊公链上使用Oraclize服务很简单，只需要在你的智能合约代码引用usingOraclize的合约，然后根据API文档进行相关方法调用就可以了。如果是私链则会麻烦一些，需要自己另外部署Oraclize服务。（图2）

Oraclize之所以可以提供一个可证明的诚实从互联网页面安全获取信息的能力，是依赖于TLS公证（TLSnotary）。TLS公证是一个服务，它允许一个审计师来验证是否一个特定的Web页面被准确地获取。

作为数据传送者第三方，必须保持数据以防止数据源操纵他们的数据，使得你获取的数据实际上是不真实的。换句话说，需要避免类似由互联网人们说出的类似“我从来没有说过!”的谎言。TLS 公证就是这个第三方，它实际上是安全的，因为它就像当你浏览到HTTPS安全的网站,你可以看到证实他们是X公司(如果您检查证书）。TLS公证本质上是以这样一种方式能够记录这些数据字节，你可以稍后再使用，这样你就可以再次验证这些数据字节。

Oraclize的开源代码地址：

https://github.com/oraclize

结语

预言机Oraclize有不少应用场景，用基于区块链的自动执行智能合约代替人力，包括去中心化交易市场系统、用于航班晚点的赔偿即时计算和支付的应用、链上身份认证系统、基于在线系统（如Twitter或微博）的声望系统、去中心化的博彩系统、各种预测系统（如体育运动比赛结果或竞选活动）、自动货到付款系统、自动托管内部发布和赞助商系统等等。连接了互联网，打开了外面的真实世界，区块链和智能合约将会变得有更多活力和可能性。

（作者微博：weibo.com/elwingao）

如对本文观点有任何讨论和补充，请发信至：qkbj@ste.gd.cn。