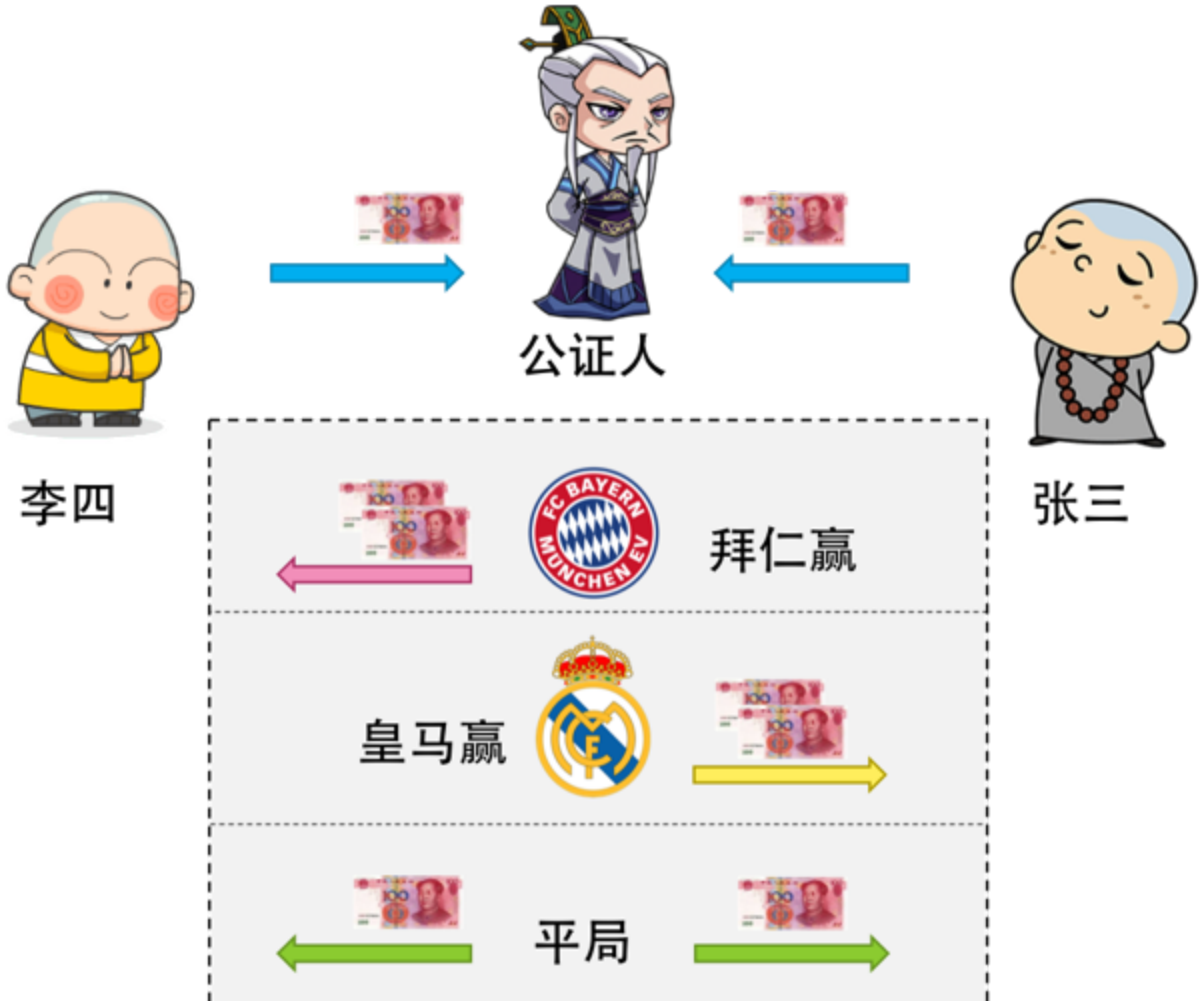
67 | 区块链技术细节：智能合约

2018-5-22 陈皓

要讲清楚智能合约，我先给你看几个案例。第一个案例是打赌。比如，张三和李四打赌，周末拜仁和皇马的足球比赛谁会赢。如果拜仁赢了，张三给李四100元；如果反过来，李四给张三100元；如果打成平局，则不赢不输。

张三和李四都怕对方不认账，所以，他们需要找一个他们都信得过的人来做公证，两人都把100元钱给这个公证人。然后，如果拜仁赢了，公证人把全部200元给李四；如果皇马赢了，则全部给张三；如果是平局，则分别退还100元。



上面这个模型什么都好，就是有一个问题，这个“公证人”跑路了怎么办？因为他们只赌100元，公证人犯不着为了200元跑路。但是，如果有一万人把赌金交给公证人呢？如果张三李四赌金是100万呢？公证人的人性会受到极大的挑战，他还有那么可信吗？

银行的资金托管业务

也就是说，当业务大到一定程度的时候，个人的信用是不足以来当中间公证人这个角色了。这时，你要找更为靠谱的机构，这个机构叫银行，银行的信用等级至少在这几方面上要比个人高。

银行是机构，所以受政府监管，受法律约束；

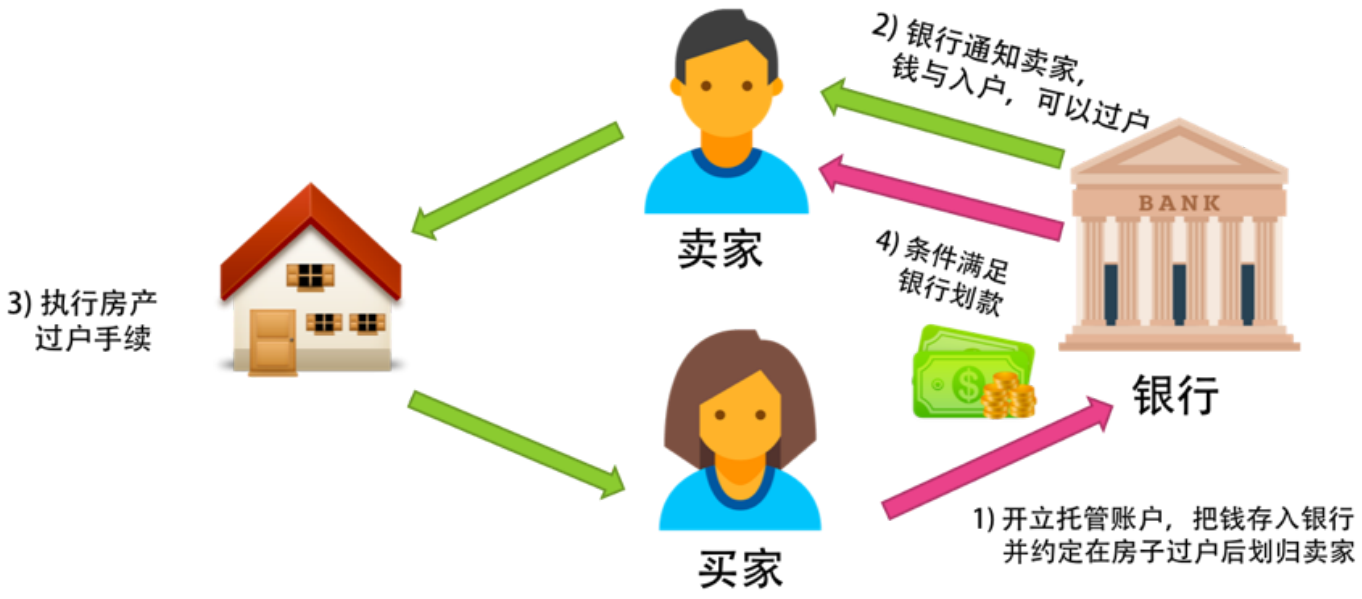
银行的钱很多，就算是里面有员工作案，银行也赔得起；

银行里有比较安全的资金管理流程和措施；

因此，银行的受信程度很高，可以来做担保。

下面，我们来看一个示例，银行在二手房交易中的“资金托管”业务。因为房屋交易时涉及到的资金数目太大，买家怕交了钱后，卖家不过户，卖家也怕过了户后，买家不给钱。而一般像“链家”或是“我爱我家”这样的房屋中介是没有能力来做大额交易的担保的（政府也不会让它们来做）。

于是银行就出来了。买家先到银行开个户，把购房款全额存进去。这个账户和一般的账户不一样，这叫资金托管账户，钱一旦进入后，你就取不出来了，除非满足了某个条件。在开户时，房屋的买卖方和银行三方约定，一旦房产证从卖家过户到买家30天后没有纠纷，钱就划给卖家了。



这其实跟在淘宝上买东西差不多，买家把钱转给支付宝，然后买家确认收到货后，在支付宝上点确认，钱就划给商家了。唯一不一样的是，支付宝没有资格担保像房屋交易这么大的交易金额。这是国家为了防范相关的金融风险所采取的措施。

以太坊的智能合约

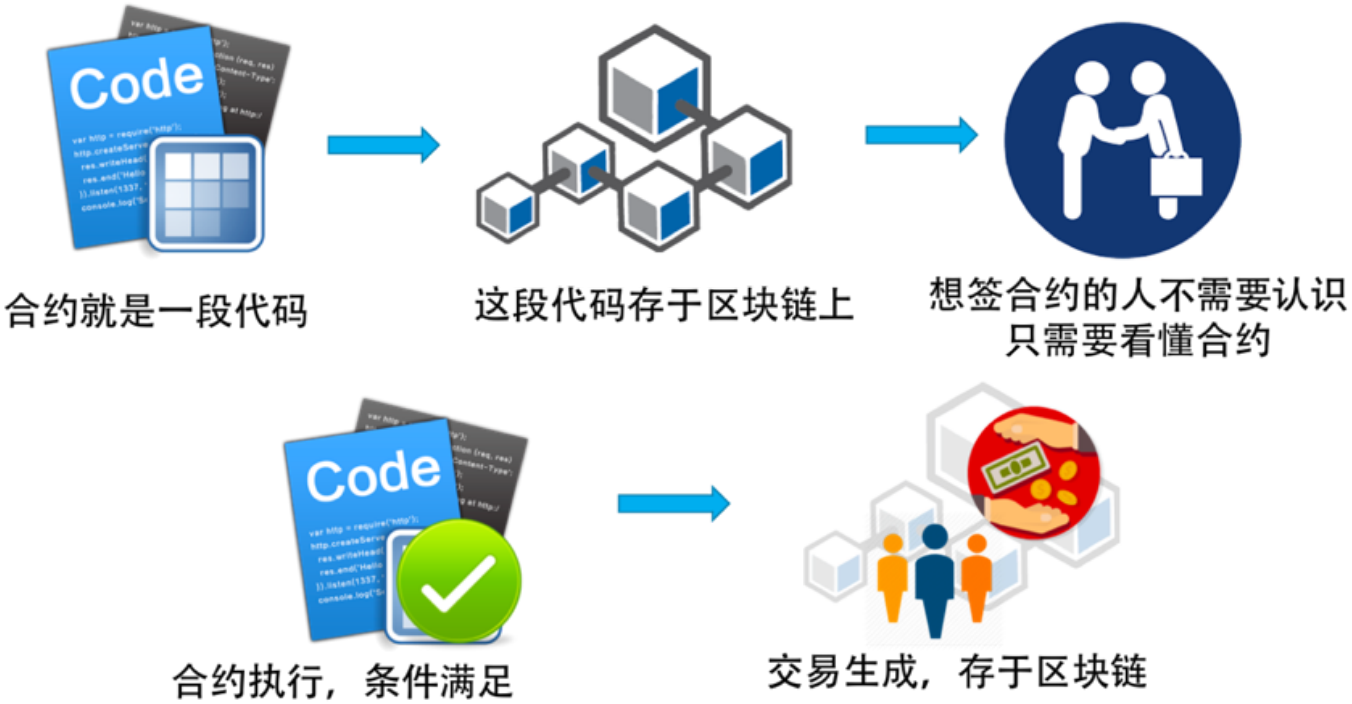
对于以太坊来说，智能合约其实就是一段可执行的程序片段，由发布人使用一种类似于JavaScript或是Python的编程语言来编写。就像最开始那个民间担保的案例一样，合同的发布可以写成如下形式：

```
Contract MyContract{
    function transferFrom(  address _from, address _to, uint256 _value) {
        if ( isBayernWin ) {
            blanceOf[_from] +=  _value
            blanceOf[_to] -= value
        }else if ( isRealMadridWin ) {
            blanceOf[_from] -= _value
            blanceOf[_to] += value
        }
    }
}
```

嗯，合同都要用代码来写了。看来，我们程序员离统治世界又近了一步。

我们把合约代码在本地编译成功后发布到区块链上，可以理解为一个特殊的交易（包括可执行代码），然后会被矿工打包记录在某一个区块中。当需要调用这个智能合约的方法时，只需要向这个智能合约的地址发送一笔交易即可。

每个节点的电脑都需要安装以太坊客户端，客户端自带了一个和JVM类似的一个EVM。通过交易触发智能合约后，智能合约的代码就会在EVM中执行了。这种方式相当于把程序部署到了非常非常多的电脑上，随时都可以通过交易来触发这些智能合约的执行，也从而完成了分布式程序的部署和调用。



这感觉就是Funciton-as-a-Service的一种实现啊。

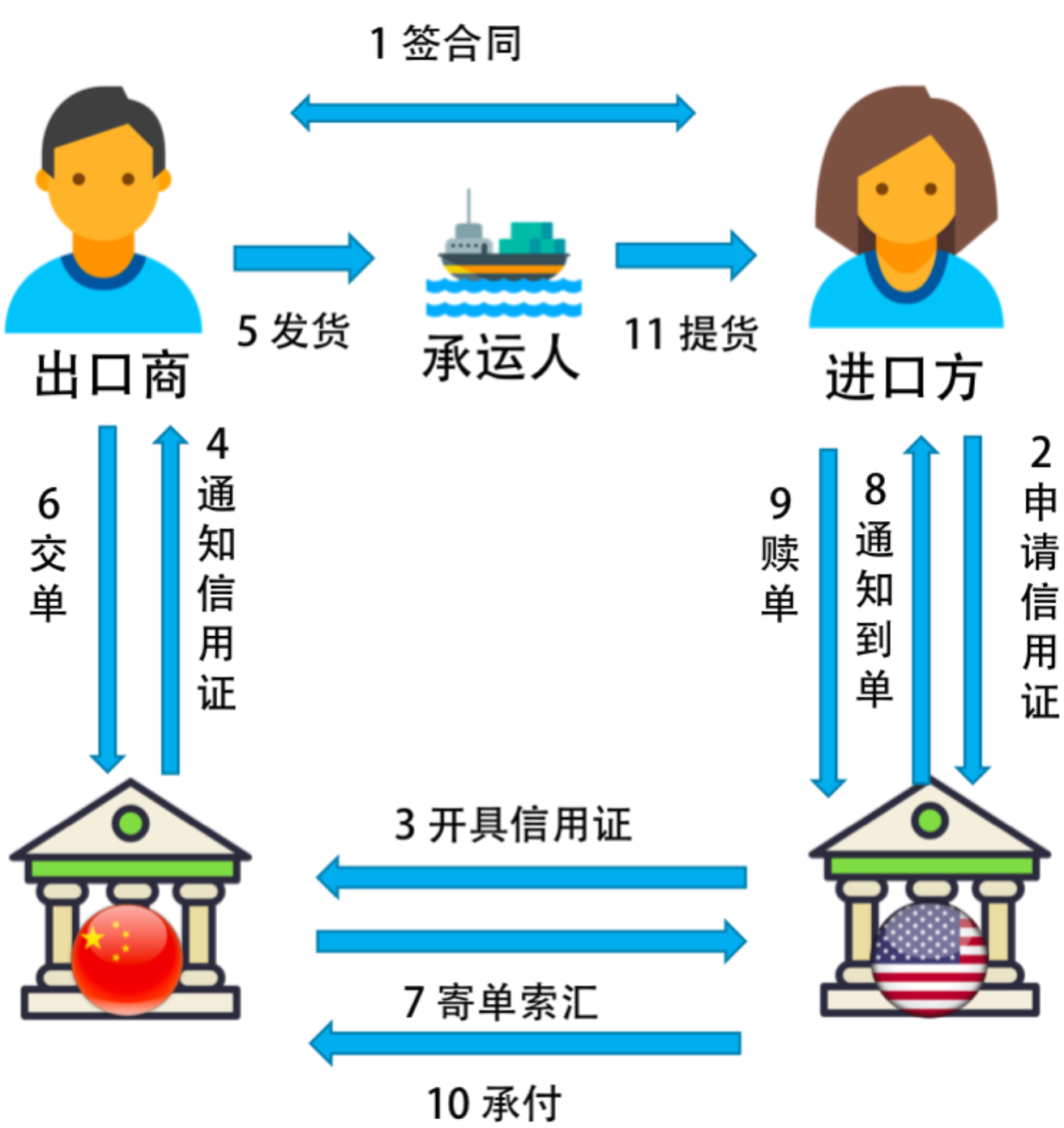
如果人与人之间的交易条件（合约）就像代码一样被严格地执行，你觉得这个世界会变成什么样呢？是不是会少一些无赖，少一些扯皮，多了很多效率，多了很多确定性呢？

有银行担保的国际业务

我们再来看一个国际贸易的流程。

假如中国某出口商和美国一个进口方做生意，会遇到货币不一样的问题。如果没有货币兑换，那就只有通过大家都认可的黄金交易了。你给我发一船货，我给你发一船黄金，风险也高，交易的效率非常低下。

如果有银行在中间协调，比如中国的某个银行和美国的某个银行签了互信协议，那么国际贸易的银行担保流程如下。下面是描述这一过程的图片。



1. 首先，出口商和进口商签订买卖合同。
2. 然后，美国的进口方到美国银行那边申请信用证（信用证需要用钱来开的，也是有价格属性的，比如200万美金的信用证，就需要用200万美金来申请）。
3. 美国的银行向中国银行开具信用证，中国银行根本不关心进口方有没有把钱给了美国银行，反正你开了200万美金面额的信用证，我以后要问你要钱的。
4. 中国银行收到信用证后，给出口商发出通知信用证，告之可以发货。
5. 出口商发货，由相关承运人从中国把货运到美国。
6. 然后，中国出口商把提货单交给中国的银行。
7. 中国的银行向美国银行发出“寄单索汇”业务。
8. 美国银行收到提货单后，通知进口方到单。

9. 进口方把货款的钱补完，比如补300万美金“赎回”提货单。
10. 然后美国银行向中国银行付款。
11. 美国进口方到承运人提货。

看看，这个过程如此复杂，而且很机械，感觉完全可以用程序来实现。如果用以太坊的智能合约来写一下，这段代码会写成什么样呢？

好像可以写得很简单。

1. 进口方把钱垫到区块链上。
2. 出口方发货方发货。
3. 进口方验货后，钱就到了出口方。

当然，这其上有一些事也需要写在程序中。

1. 一个是进口方的钱垫到区块链上，就需要被冻结掉。
2. 另外还需要物流信息，不然，进口方说没有收到，不好验证。但物流信息要是造假怎么办？
3. 另一个是需要把进口方验货的标准给写进来。代码不知道条件怎么满足，也许需要进口方那边点个确认。如果不点确认，则有个过期时间，时间一到就自动确认。
4. 另外，如果进口方觉得有问题，需要退货，或是需要重新议价，那么需要相关的关联合同。

其中，比较难办的是第2步，需要其他方也进入区块链。如果不进来，这事就不好玩了。但是，物流信息怎么才能做到真实可靠的呢？这需要双方选择一个都相信的中心化的物流公司，还是我们搞一个去中心化的物流公司？去中心化的物流公司是个什么形态，你能想像得出来吗？我想象不出来。

合同的Bug

另外，我们要小心智能合同。有程序的地方就会有Bug，现实生活中会有Bug，合同也会有Bug。出现了Bug后，大家可以相互协商，给合同打补丁（附加条款，或是重新签合同）。然而，代码合同则不一样，Bug也会被残酷无情地执行，一旦执行就很难补救了。

最著名的例子就是以太坊一个叫The DAO的应用，它是一个去中心化的风险投资基金，以智能合约的形式运行在以太坊区块链上。它也是一个盈利性的去中心化自治组织，它将利用自

己掌控的以太币资金通过投资以太坊上的应用为其成员创造价值。在The DAO创建期，任何人都可以向它的众筹合约发送以太币，获得DAO代币。

因为 The DAO这个程序写得不好，黑客在其智能合约里找到Bug，把所有的钱给调走了，大约7000多万美刀。这成为有史以来最大宗的数字劫案，而且FBI也找不到人。这个项目因为钱被偷走而倒闭以后，引起了以太坊的强行分叉，变成ETH和ETC。关于技术细节可参见其 漏洞分析文章，整个事件的始末可以参见《彭博社深度还原：The DAO 大劫案始末》。

还有一个案例，是2017年发生的智能钱包（多签名钱包）Parity被盗事件。它号称自己的智能合约被很多很厉害的安全人员都审查过，都认为没问题。但最后还是被黑客利用了一个叫做initwallet的函数，反复调用它，转走了3000万美金。

老实说，我觉得任何合同都是会有Bug的，无论是在现实生活中，还是在代码中。唯一的不同是，现实生活中的合同出现Bug，可以自行协商解决，也可以通过法律或仲裁的方式解决。然而，在数字社会中，代码无论好坏都会被计算机残酷无情地严格执行。

有时候，当你是利益方时，你会觉得是好事。但有时候，你是受害方时，你还是会想有挽回的余地。现实生活中可以做到，但我不知道代码世界中的合同如何解决这些Bug，所以还是不要叫"智能合约"，至少现在还不是。

文末给出了《区块链技术》系列文章的目录，希望你能在这个列表里找到自己感兴趣的内容。

精选留言 10

李博越
1523689716

作为整个分布式系统的半壁江山，啥时候开专题讲下数据库领域方面的知识？急需一张认知地图带我打开视野

阿舍利手斧
1523605557

人工智能里面的智能该怎么理解，智能手机的智能该怎么理解

neohope
1529665023

智能合约本身说白了，只不过是在矿工端执行函数调用API而已，但国内很多教程都是hello world水平，想写好智能合约还是要啃API和看开源的合约的。

就本文而言，如果能讲解一下两个点，一个是矿工如何执行合约的，一个是合约的中间状态是如何保存的，应该就更棒了！如果能深入讲解一下EVM虚拟机，那就物超所值了。

不想打酱油
1526433872

楼上说打水漂的那个哥们是不是想要看：如何开发自己的智能合约。

edisonhuang
1564708601

智能合约类似于现实交易中银行担保人的意义，让我们把合同作为一段代码随着区块一起发布出去，在每一台电脑上执行。但是该合约的问题在于没法解决bug，当代码出现bug时合约一样会被严格执行，这时造成的损失是巨大的。与此相反，现实世界的合约有bug则可以双方协商，或是通过法律途径沟通解决。

格瑞图
1542847287

这感觉就是 Funciton-as-a-Service 的一种实现啊。function

登高
1524971768

去中心化完美解决oracle问题，智能合约就完全独立了

刘海（steven）
1523691989

没写出实质东西

kursk.ye
1523580986

想象一下，如果区块链真的大规模普及成功了。所有的经济活动都在上面实现，每个人都可以看到每笔钱是怎么花掉的，每个人都掌握了所有的经济信息，区块链成了地球上最中立的“组织”，那不是银行没用了，而是政府没有用处了，因为政府的最大作用就是其中立性和掌握全面信息，做出最有中立和远见的判断，仔细想想，真是极思恐怖

菡萏如佳人

1523544877

目前所谓的智能合约其实一点也不智能哈，更像是一种规约脚本。真正实现智能合约的那天，是不是就是程序员猿统治世界的时候了