智能合约中存在的3种最常见的误解

作者：Gideon Greenspan 原文：http://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/#userconsent#

译者：nous 译文：http://www.8btc.com/beware-the-impossible-smart-contract

# 世俗的智能合约

作为一名受欢迎的区块链平台的开发者，我们有时被问到类似以太坊的智能合约是否走多链路线。我总是回答说：没有，至少目前还没有。

但智能合约在区块链充满炒作的世界里都可以风靡一时，为什么以前不行呢？那么问题是，尽管我们现在了解了关于比特币区块链的三大强势用例（出处，公司之间记录和轻量级的融资），但我们尚未找到以太坊智能合约的等价物。

这并不是说人们缺乏想要利用智能合约的想法。相反，这些想法很多是根本不可能实现的。你看，当精明的人听到“智能合约”这个词，他们的想象力往往就会天马行空。他们联想到自动化智能软件，去融入这个世界，利用其数据凑凑热闹。

不幸的是智能合约的现实远远比这些更世俗：智能合约其实是一段被存储在一个区块链上的代码，由区块链交易触发。它读取并且在区块链数据库写入数据，这就是智能合约。真的，智能合约仅仅是一串在区块链上运行的有着奇特名字的代码，并与区块链状态模式相互影响。什么是代码？代码可以是帕斯卡，是Python，是PHP。它是Java，是Fortran语言，是C++。如果我们谈论的是数据库，它就是写在扩展SQL的存储过程。所有这些语言基本上是等价的，解决了同一种类同样类型问题的解决方法。当然，每一种语言都有其长处和短处 —— 你一定是疯了才会用C语言去建立网站或用Ruby压缩高清视频。但是至少在原则上，你可以，只要你想。你只是在便利性和性能方面付出了沉重的代价。

智能合约的问题并不仅仅是人们的期望被夸大了。而是那些期望导致许多人在不可能实现的想法上耗费时间与资金。看来大公司得有充足的资源去经历一个漫长的路程 ——当高级管理人员遇到了一种新的技术并真正理解它的优点和局限性的那一刻起。也许我们自己的经验能够帮助缩短这个时间。

在过去的九个月中，我们已经投了不少智能合约的用例，并且已经找到了我们自己的响应，一次又一次地，那是他们根本无法做到的。最终，我们已经鉴别了三种智能合约最常见的误解。这些想法都没有错，因为技术不成熟，或者工具尚不可用。相反，他们误解的只是在一个数据库中以分散方式运行代码的基本性质。

## 1.1 联系外部服务

通常情况下，第一个用例提出的智能合约是**改变其行为以响应一些外部事件**。例如，在一个给定的月份里，根据降雨的数量来支付的农业保险政策。想象中的过程大概是这样：智能合约等到预定的时间，会从外部服务检索天气预报，并根据收到的数据进行适当的行为。

这一切听起来很简单，但同时也是不可能的。 为什么呢？**由于区块链是基于共识的系统，这意味着只有在处理完一笔交易后的每一个节点达到相同的状态，它才会起作用。**这一切都只能存在于区块链必须是完全确定，没有任何可能发生差异的情况下。当有两个诚实的节点不同意这条链状态的那一刻，整个系统将变得一文不值。

现在回想一下，**智能合约是由链上的每个节点独立地执行的。因此，如果智能合约从外部源检索获取一些信息，那么会重复再检索并分别由每个节点执行。但是，由于信息源是区块链以外的，不能保证每个节点都会接收相同的答案。**也许信息源将改变它在不同节点之间请求的响应时间，或者它会成为暂时不可用的状态。无论哪种方式，一旦共识被打破，整个区块链系统都会瘫痪。

那么，有什么**解决办法**吗？其实，这很简单。替代智能合约发起启动外部数据检索，在一个或多个信任方（“数据库”）的检索创建中嵌入交易链中的数据。每个节点都会有一个数据完全相同的副本，因此它可以安全的在一个智能计算合同中使用。换句话说，由数据库推送数据到区块链要比智能合约拖出数据要好得多。

当智能合约涉及到引发导致外界事件，会出现类似的问题。例如，很多人喜欢智能合约中一个调用银行API以完成转账的想法。如果每个节点都是独立地执行链中的代码，谁负责调用这个程序接口？如果回答是某一个节点，如果那个特定的节点出现故障会发生什么，你还能从容不迫吗？如果回答是每一个节点，我们可以信任每个节点与该接口的密码吗？难道我们真的希望这个程序接口被调用数百次吗？更糟糕的是，如果智能合约需要知道接口调用是否成功，我们就又回到了依赖于外部数据的问题上。

和原来一样，有一个简单的解决方法。取而代之的是智能合约调用外部的API，我们**使用一个可信赖的服务器监测区块链的状态和执行某些操作的响应**。例如，银行可能前瞻性地观看区块链，并实施资金转移以及反映上链交易。这对于区块链的共识并没有任何风险，因为链扮演着一个完全被动的角色。

看着这两种解决方法，我们可以提出一些意见。首先，它们都需要一个可靠的实体来应对区块链和外界之间的相互作用。尽管这在技术上是可能的，但它破坏了一个分散系统的目标。其次，这些解决方法中使用读取和写入数据库的机制就是直截了当的的例子。它提供外部信息的数据库只是简单地将这些信息写人链中。这反映了区块链的状态在现实世界中要做的无非是从链读取数据。换言之，一个区块链和外界之间的任何相互作用仅限于常规数据库操作。我们稍后再就这一点做详细讨论。

## 1.2 强制执行链上付款

我们往往会听到很多关于另一个建议：使用一个智能合同来自动化支付的优惠券，即所谓的“智能债券”。这个想法是**在适当的时间，自动启动智能合约的付款代码，既避免了手动过程，同时又保障了发行者无法违约。**

当然，为了这项工作，用来偿还的资金必须在区块链内部流通为好，否则智能合约无法保障付款。现在回想一下，区块链就是一个数据库，这种情况下，财务总账包含发放的债券以及一部分现金。因此，当我们谈论优惠券付款时，实际上是在讨论约定的时间内自动发生的数据库操作。

虽然这种自动化在技术上具有可行性，但它始终被财政困难所困扰。如果用于支付债券的资金是由债券的智能合约控制，那么这些付款的确能得到保障。但这也意味着这些资金不能由债券发行方作为他用。如果这些资金不在智能合约的控制下，那么就没有办法保证付款可以得到保障。

换句话说，智能债券要么是毫无意义的发行人，要么是毫无意义的投资者。如果你仔细想想，这完全是一种显而易见的结果。从投资者的角度来看，债券的重点就是其具有吸引力的回报率，但有一定的违约风险成本。而对于发行人来说，债券的目的是用类似筹集资金用于生产，但也有些活动有风险，例如建立新厂。所以是没有办法让债券发行人能够募集到资金的同时保证投资者可以得到偿还。这并没有什么好意外的，原本风险和回报之间的关系就不是区块链能解决的问题。

## 1.3 隐藏机密数据

正如我之前已经写过的，**有效利用区块链最大的挑战就是它提供过于彻底的透明度**。例如，如果十家银行在一起建立一个区块链，有两家进行了一项双向交易，这项交易将立即对其他八家可见。虽然也有缓解这个问题的各种策略，但还没有一个可以击败简单有效的中央数据库，除非能有一个可靠的管理员已经完全控制谁可以看到什么。

有些人认为智能合约可以解决这个问题。他们提出每个智能合约都包含了自己的微型数据库这一论据，认为它具有完全控制的能力。由于该数据库中所有的读写操作是由合约代码所介导的，所以合约无法直接读取其他数据。 （数据和代码之间的这种紧密耦合称为埋离子，并且是流行的面向对象编程范例的基础。）

所以，如果一个智能合约不能访问其他的数据，我们能否解决区块链保密性的问题？讨论在智能合约中隐藏信息是否有意义？不幸的是，答案是否定的。因为即使一个智能合约无法读取其他的数据，该数据仍然存储在链中的每一个节点上。对于每个区块链的参与者来说，完全可以控制一个系统的存储器或者磁盘。如果当他们想要从自己的系统中阅读信息，有什么能阻止他们呢？

在智能合约隐藏网页数据就像把它隐藏在HTML代码里一样安全。当然，一般的网路用户不会看到它，因为它并未显示在他们的浏览器窗口中。但是，所有这一切需要一个网页浏览器添加“查看源文件”功能（因为它们都有），并且隐藏的信息变得普遍可见。同样，对于隐藏在智能合约的数据，所需要的只是有人修改其区块链软件显示合约的全部状态，就可以看到隐秘的假象。只要一个差不多的程序员花一个小时左右就可以做到。

# 什么是智能合约？

有了这么多智能合约不能做到的事情，有人可能会问它们实际上到底是什么。但要回答这个问题，我们需要回到自己区块链的基础。扼要重述一下，区块链使数据库可以被彼此互不信任的实体直接和安全地共享，而无需中央管理。 区块链实现了数据中介化，并显著减少了复杂性以及大量成本。

所有数据库都是通过“交易数据”来进行更改，其中包含一组对该数据库的更改，但它必须作为一个整体进行更改，不论成功或失败。例如，在财务分类账里，Alice向Bob进行付款，那么这笔交易就表现为：（a）检查Alice是否有足够的资金；（b）从Alice的帐户扣除一定和交易款项相等的金额；（c）在Bob的账户上增加相等的金额。

在常规的集中的数据库，这些交易是由一个单一可信权威管理机构创建的。相比之下，由区块链驱动的共享数据库，交易可以由任何一个区块链的用户创建。而且，由于这些用户不完全信任对方，数据库必须含有限制进行交易的规则。例如，在一个对等网络的财务分类账，每一笔交易必须保持资金的总量不变，否则，用户可以随意给自己取尽可能多的钱，因为他们都很喜欢。

可以想象表示这些规则的各种方式，但现在有两种主导模式，分别用比特币和以太坊启动。

我们可以称比特币的方法为“交易限制”，是在几方面评估每一笔交易：（a）删除该交易的数据库条目，和（b）区块创建。在一个财务分类账中，该规则规定已删除条目的资金总数量必须与所创建的总数量匹配。 （我们认为现有条目的修改相当于删除该条目并在其位置上创建一个新的。）

第二种模式来源于以太坊，即智能合约。这表明所有修改合约数据的操作必须通过执行代码实现。 （在传统的数据库的背景下，我们可以认为这是一个**强制存储过程**。）要修改合约数据，区块链用户会发送请求到代码，代码决定是否满足以及如何满足这些请求。而在这个例子中，作为一个财务分类账的智能合约中心数据库的管理员，同样需要执行的三个步骤：检查是否有足够的资金，从一个帐户扣除资金，并添加到另一个账户。

这两种模式都是有效的，而且每一种都有其优点和缺点，正如我在前面深入讨论的那样。总而言之，比特币形式的交易限制提供了优越的性能和并发性，而以太坊式智能合约则提供了更大的灵活性。因此，回到智能合约是什么的问题就是：**智能合约适用于不能通过交易限制来实现的区块链用例。**

给予了智能合约这一标准，我还没有看到它变成符合区块链拥有权限的强大用例。我所知道的有说服力的区块链应用程序都使用比特币交易的方式，它可以处理管理权限和一般的数据存储，以及资产的创建、转移、托管、交易和消除。尽管如此，新的用例仍然在出现。就算有的用例的确需要智能合约，我也不会惊讶。或者说，至少是比特币模式的延伸。

不管答案是什么，关键要记住的是，智能合同只是一种限制在数据库中进行的交易的方法。这无疑是一个有用的东西，而且是使该数据库安全共享的关键。但智能合约不能做任何事情，它们当然也无法逃脱他们所在数据库的边界。