**四个真正的区块链使用案例**

原文（英）：<https://www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/>

译文：<http://www.sohu.com/a/225385829_100122322>

在第一次发布MutiChain之后的大约一年时间里，我们已经学到了一大堆关于区块链如何在私有和非加密货币意义上可以或不能应用于现实世界的问题。请允许我分享我们迄今为止所了解的内容。

首先，我们（和许多其他人）开始的第一个想法似乎是错误的。这种直接受比特币启发的想法是，**私人区块链（或“共享分类账”）可用于直接结算金融领域的大部分支付和交易，使用链上代币代表现金，股票，债券和更多。**

这在技术层面上是完全可行的，那么问题是什么？**保密。**如果多个机构使用共享分类帐，则每个机构都会看到该分类账上的每笔交易，即使他们没有立即知道所涉各方的真实身份。无论是在监管方面，还是在银行间竞争的商业现实方面，这都是一个巨大的问题。虽然有各种策略可用于或正在开发中以缓解此问题，但没有任何策略能够与由可信中介管理的集中式数据库的简单性和高效性相匹配，从而可以完全控制谁可以查看内容。至少现在看来，大型金融机构似乎更倾向于将大部分交易隐藏在这些中间数据库中，尽管涉及成本。

我的结论不仅取决于我们自己的经验，还取决于一些初创目标是为银行开发共享分类账的初创公司的方向。例如，R3CEV和Digital Asset现在分别在corda和Delan上开发“合同描述语言” （早期的例子包括MuFI和Ricardian合约）。这些语言可以使复杂的金融合同条件正式、明确地以计算机可读格式表示，同时避免太坊式通用计算的缺点。相反，区块链只起到支持作用，以加密形式存储或公证合同，并执行一些基本的重复检测。实际的合同执行不会发生在区块链上 - 而只能由合同的交易对手执行，并且可能会增加审计师和监管机构。

在短期内，这可能是最好的做法，但是选择放弃更大的野心去做受许可区块链这条路要走向何方？是否还有其他应用可以构成这个难题更重要的部分？

这个问题可以从理论和经验两方面进行探讨。理论上，通过关注区块链和传统数据库之间的关键区别，以及它们如何告知可能的用例集。在我们的案例中，通过对现在建立在MultiChain上的真实世界的解决方案进行分类，从经验的角度来看。毫不奇怪，无论我们是专注于理论还是实践，都会出现相同类别的用例：

* **轻量级财务系统。**
* **来源追踪。**
* **组织间记录保存。**
* **多方聚合。**

在详细解释这些之前，让我们回顾一下这个理论。正如我之前讨论的，区块链和集中式数据库之间的两个最重要的区别可以表征如下：

1. 去中介。区块链支持多个彼此不完全相互信任的团体安全地直接共享单个数据库，而不需要可信中介。

2. 保密性：区块链中的所有参与者都可以看到发生的所有交易。（即使我们使用假名地址和高级密码术来隐藏这些交易的某些方面，区块链总是会泄漏比集中数据库更多的信息。）

换句话说，区块链是共享数据库的理想选择，其中每个用户都可以读取所有内容，但没有可以编写内容的单个用户控件。相比之下，在传统数据库中，单个实体对所有读写操作施加控制权，而其他用户则完全服从该实体的异想天开。总结一句话：

**区块链代表了以保密为代价取得非中介化的权衡。**

在研究以下四种用例时，我们会多次回顾这一核心权衡，解释为什么在每种情况下，非中介化的好处都超过了降低机密性的成本。

## **轻量级财务系统**

让我们从最熟悉的一组区块链应用开始，其中一组实体希望建立一个金融系统。在这个系统内，一个或多个稀缺资产在这些实体之间进行交易和交换。

为了让任何资产保持稀缺，必须解决两个相关的问题。首先，我们必须确保不会将同一单位的资产发送到多个地方（“双重花费”）。其次，任何人都不可能随心所欲地创建资产的新单位（“伪造”）。任何可以做这些事情的实体都可以从系统中窃取无限价值。

这些问题的常见解决方案是物理令牌，例如金属硬币或安全打印的纸张。这些令牌平凡地解决了双重支出的问题，因为物理规则（字面上）阻止一个令牌同时在两个地方。通过使令牌非常难以制造来解决伪造问题。尽管如此，物理令牌有几个缺点，可能会导致它们不切实际：

* 作为纯粹的持有者资产，物理令牌可以被窃取而无痕迹或追索权。
* 它们运行速度慢且成本高，无法大量运输或长途运输。
* 创建不可伪造的物理令牌是棘手和昂贵的。

通过留下物理令牌可以避免这些缺陷，并且可以通过由可信中介管理的分类帐重新定义资产所有权。过去，这些分类帐基于纸质记录，现在它们倾向于在常规数据库上运行。无论哪种方式，中介通过修改分类帐的内容来实现所有权的转移，以响应已认证的请求。与使用物理令牌进行结算不同，有问题的交易可以快速轻松地撤消。

那么分类帐有什么问题？简而言之，就是控制权的集中。通过在一个地方投入如此多的力量，我们从技术和人力两个方面创造了重大的安全挑战。如果外部的人可以入侵数据库，他们可以随意更改账本，窃取他人的资金或完全摧毁其内容。更糟的是，内部有人可能会破坏分类账，这种攻击难以发现或证明。因此，无论我们拥有集中式分类帐，我们都必须投入大量时间和金钱来维护分类账的完整性。而且在很多情况下，我们需要使用中央分类账与每个交易各方之间的基于批次的调节进行持续核实。

输入区块链（或“共享分类帐”）。这提供了分类帐的好处，而不会产生集中问题。相反，每个实体运行一个持有分类帐副本的“节点”，并对其自己的资产进行完全控制，这些资产受私钥保护。事务以点对点的方式在节点之间传播，区块链确保维护共识。这种架构没有留下黑客或内部人员可能破坏账簿内容的中央攻击点。因此，数字金融系统可以更快速，更便宜地部署，并且可以实时自动实现对账。

那么缺点是什么？如前所述，共享分类帐中的所有参与者都会查看所有发生的交易，使其在需要保密的情况下无法使用。相反，区块链适用于我称之为轻量级金融系统的领域，即**经济利益或参与者数量相对较低的区块链**。在这些情况下，机密性往往不是一个问题 - 即使参与者密切关注彼此的行为，他们也不会学到很多价值。正因为风险很低，我们宁愿避免设立中间人的麻烦和成本。

轻量级金融体系的一些明显例子包括：**众筹，礼品卡，信用积分和当地货币** - 尤其是在资产可以在多个地方赎回的情况下。但是我们也看到了主流金融部门的用例，比如**不直接竞争的资产管理者之间的点对点交易**。区块链甚至在内部会计系统中进行测试，在大型组织中，每个部门或地点都必须保持对其资金的控制。在所有这些情况下，区块链的低成本和冲突提供了直接的好处，而保密性的丧失并不是问题。

## **来源追踪**

以下是我们多次听到MultiChain用户使用的第二类用例：追踪整个供应链中高价值产品的起源和移动，例如奢侈品，药品，化妆品和电子产品。同样重要的文件，如提单或信用证。在跨越时间和距离的供应链中，所有这些物品都遭受假冒和盗窃。

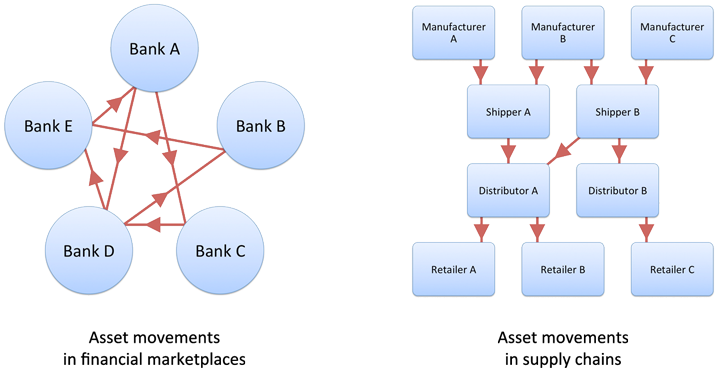
该问题可以通过以下方式使用区块链解决：当创建高价值物品时，相应的数字令牌由可信实体发布，该可信实体用于验证其原点。然后，每当物理项目转手时，数字令牌就会并行移动，以便真实世界的监管链由区块链上的一系列交易精确地反映出来。

如果你喜欢，这个令牌就是一个虚拟的“真实性证书”，它比一张纸更难以窃取或伪造。收到数字令牌后，无论是银行，分销商，零售商还是客户，实体商品的最终收款人都可以验证监管链，一直返回原点。事实上，在提单等文件的情况下，我们可以完全废除物理项目。

虽然所有这些都是有道理的，但精明的读者会注意到由一个物品制造商管理（例如）的常规数据库可以完成相同的任务。该数据库将存储每个项目当前所有者的记录，接受代表每次所有权变更的已签名交易，并响应有关当前状态的传入请求。

那么为什么要使用区块链呢？答案是，对于这种类型的应用程序来说，分布式信任是有好处的。无论集中的数据库在哪里举行，那里都会有人有能力（并且可能会受到贿赂）腐蚀其内容，将伪造或被盗物品标记为合法。相比之下，如果在源于集体供应链参与者的区块链上追踪出处，则没有任何单个实体或小组实体可以破坏监管链，并且最终用户可以对他们收到的答案有更多的信心。作为奖励，可以安全地直接交换不同的令牌（比如某些货物和相应的提单），并在最低区块链级别保证双向交换。

那么保密问题呢？区块链对供应链起源的适用性是该应用程序简单交易模式的一个令人满意的结果。与金融市场形成对比的是，大多数代币都是从原点到终点的单一方向移动，而不会在区块链参与者之间反复交易。如果竞争对手很少与对方进行交易（例如玩具制造商对玩具制造商或零售商或零售商），他们就无法相互学习彼此的区块链“地址”并将其与真实世界的身份相联系。此外，活动可以很容易地划分为多个分类账，每个分类账代表不同的订单或类型。



## **组织间记录保存**

以前的两种用例均基于标记化资产，即参与者之间转移的价值项目的链式表示。然而，第二组区块链使用案例与资产无关。相反，该链作为集体记录和公证任何类型数据的机制，其意义可以是财务或其他方式。

其中一个例子就是两个或更多组织之间的关键沟通的审计追踪，例如医疗保健或法律部门。组织内的任何组织都不能信任维护这些记录档案，因为伪造或删除的信息会严重损害其他组织。尽管如此，为了防止争端，所有人都必须就档案的内容达成一致。

为了解决这个问题，我们需要一个共享数据库，所有的记录都被写入其中，每条记录都附有时间戳和原始证据。标准解决方案是创建一个可信中介，其作用是集中收集和存储记录。但区块链提供了一种不同的方法，为组织提供了共同管理这个档案的方法，同时防止个别参与者（或其小团体）破坏它。

其中最有启发性的谈话我已经在过去两年中与Michael Mainelli的Z/Yen集团。20年来，他的公司一直在建立多个实体共同管理共享数字审计线索的系统，使用时间戳，数字签名和循环法共识方案。当他解释这些系统的技术细节时，很明显他们在各方面都是经过许可的区块链。换句话说，使用区块链进行组织间记录并不是什么新鲜事 - 只是世界终于意识到了这种可能性。

就存储在区块链中的实际数据而言，有三种常用选项：

* **未加密的数据**。这可以被区块链上的每个参与者读取，提供全面的集体透明度和立即解决在发生争议的情况下。
* **加密的数据**。这只能由具有对应解密密钥的参与者读取。在发生争议时，任何人都可以揭示这一关键，值得信赖的权威机构，如法院，并使用blockchain证明原始数据进行一定一方在某一时间点添加。
* **散列数据**。“ 散列”充当紧凑型数字指纹，代表对特定数据的承诺，同时保持数据隐藏。给定一些数据，任何一方都可以很容易地确认它是否与给定散列相匹配，但是从散列推断数据在计算上是不可能的。只有哈希被放置在区块链上，原始数据由相关方存储在链下，可以在发生争议时将其揭示出来。

如前所述，R3CEV的Corda产品采用了第三种方法，在区块链中储存哈希值以公证对手方之间的合同，但不公开其内容。此方法既可用于计算机可读的合同描述，也可用于包含纸质文档的PDF文件。

当然，保密性对于组织间记录保存来说不是问题，因为整个目的是创建一个所有参与者都可以看到的共享档案（即使某些数据被加密或散列）。的确，在某些情况下，区块链可以通过提供数字签名访问请求的不可变记录来帮助管理访问机密的脱链数据。无论哪种方式，非中介的直接好处是不必创建额外的实体并且信任它来维护此记录。

## **多方聚合**

从技术上讲，这个最终用例与前一类似，因为多方正在将数据写入集体管理的记录。然而，在这种情况下，动机是不同的 - **克服来自大量单独来源的信息的基础结构困难。**

想象两家银行拥有内部客户身份验证数据库。在某个时候，他们注意到他们分享了很多客户，因此他们进入了互惠分享安排，他们交换验证数据以避免重复工作。从技术上讲，协议是通过使用标准的主从数据复制来实现的，其中每个银行都维护另一个数据库的实时只读副本，并且针对自己的数据库和副本并行运行查询。到现在为止还挺好。

现在想象这两家银行邀请另外三家银行参与这个分享圈子。5个银行中的每一个都运行其自己的主数据库，以及其他4个只读副本。有5个主数据库和20个副本数据库，我们共有25个数据库实例。虽然可行，但这会消耗每家银行IT部门的显着时间和资源。

快进到20家银行以这种方式共享信息的时候，我们总共查看了400个数据库实例。对于100家银行，我们达到10000个实例。一般来说，如果每个参与方都彼此共享信息，则数据库实例的总数会随参与者数量的平方增长。在这个过程中的某个时刻，系统必然会崩溃。

那么解决方案是什么？一个显而易见的选择是所有银行都将其数据提交给可信中介，该中间人的任务是将这些数据汇总到一个主数据库中。然后，每家银行可以远程查询此数据库，或者在其四面墙内运行本地只读副本。虽然这种方法没有问题，但区块链提供了一种更便宜的选择，其中共享数据库由使用它的银行直接运行。区块链还为整个系统带来了冗余和故障转移的额外好处。

区分链不像Cassandra或RethinkDB这样的分布式数据库，必须澄清一点。与这些系统不同，每个区块链节点都实施一组规则，以防止一个参与者修改或删除另一个参与者添加的数据。事实上，这似乎仍然存在一些混淆 - 最近发布的区块链平台可能会被一个单一的不当行为节点破坏。无论如何，一个好的平台还可以让管理数千个节点的网络变得轻松，如果授予适当的权限，则可以随意加入和离开。

虽然我对区块链和物联网之间的经常引用的关联有点怀疑，但我认为这可能是强大的协同作用所在。当然，每个“东西”都太小，无法在本地存储完整的区块链副本。相反，它会将数据承载事务传输到分布式链接节点的分布式网络，并将它们整理在一起以供进一步检索和分析。

**结论：金融区块链**

我以质疑金融领域区块链的初始使用案例，即支付和交换交易的批量结算，开始撰写本文。尽管我相信这个结论已经成为普遍的看法（有一个明显的例外），但这并不意味着区块链在这个行业中没有其他应用。事实上，对于上述四类用例中的每一类，我们都看到了银行和其他金融机构的明确申请。它们分别是：**小型贸易圈，贸易融资来源，双边合同公证和反洗钱/ KYC数据汇总**。

需要理解的关键是，从架构上来说，我们的四类用例并非针对财务，与保险，医疗保健，分销，制造和IT等其他部门同等相关。实际上，对于两个或两个以上组织需要共同观察现实情况的任何情况，都应该考虑使用私人区块链，并且这种观点不是来源于单一来源。在这些情况下，区块链可以替代对可信中介的需求，从而显着节省麻烦和成本。