去判断区块链的应用场景，不少人往往都会感到无从下手。本篇章就以此出发，为大家提供思路和方法帮助你建立分析区块链应用场景的能力。

众所周知，区块链本质上就是一个去中心化的数据库，使用数据库的各方都可以存储交易数据。需要注意的是，这里的交易指的是广义的交易，并不限于货币和金融的交易，一切会产生数据状态变化的事务都称之为交易，例如，创建账户，修改密码等等。

这里有一个需要讨论的问题是，是否所有的交易数据都需要存储在区块链上？答案当时是不一定，那么什么样的数据不适合上链以及什么样的数据适合上链？

首先来看看什么样的数据不适合上链。从业务角度看，不需要共享的数据不适合上链。 例如，用户账户密码，这本身就是高度隐私化的数据，相信没有人希望自己的密码被其他人知晓。尽管区块链加密技术可以保证数据的隐私性，但是也有泄露的可能性，因此没有必要上链。从性能角度讲，过于庞大的数据和更新过于频繁的数据也不适合上链。例如，时钟信息，假使它以秒为单位更新时间，那么区块链上最终会记录所有的时刻信息，相信没过多久，区块链的存储空间会变得非常大，这会严重的影响到同步性能。

那么什么样的数据适合上链呢？简单来说就是需要共享的、需要具备可信度、不能被篡改并且需要可追溯的数据。例如保险行业的保单信息，用户签署了什么样的保险协议，需要被妥善保存。将来一旦出险，存储在区块链上的信息将会作为索赔的依据。因为不可篡改，保险公司也无法抵赖。也因为可以共享和追溯，一旦产生纠纷，监管部门、法院也可以追溯取证。

前面提到了区块链可以简单理解为一个分布式的账本，那么相比于传统的中心化数据库，两者有什么区别呢？

<https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database>

1. 区块链的历史数据永久保留

任意一个写操作不会覆盖区块链账本的原始记录，只会将写操作的内容打包进新的区块链接到最后一个区块上，不过写操作会更新世界状态中的值。引入世界状态（world state）的概念就是方便获取账本的当前状态值。你不需要遍历整个区块链去计算账本当前的状态的值(余额)，可以直接从世界状态获取。假如说，原本你的钱包有100元，世界状态里钱包的余额同样也是100元。当你消费花了10元，钱包在世界状态里的余额就成了90元，不过区块链账本中100元的记录依旧存在，同时会记录一条花费10元的记录。我们可以看到区块链数据库会保存所有的记录，而传统数据库大多都是升级到最终的数据状态，当然历史数据表除外。

1. 数据的完整性

虽然传统的数据库安全性也是有保障的，但是不排除有黑客的攻击或者使用者的误操作导致数据的丢失，篡改。区块链的数据完整性是有完整的机制保证，节点都存在区块链账本的备份。及时某一个节点账本出现不同步的情况，该节点也会很快通过gossip协议确保数据的完整性。这是传统数据库无法保证的。

虽然有性质上的不同，不少人还是觉得区块链本质上还是一个数据库。虽然区块链使用场景只是数据库使用场景中的一部分，但是当我们探讨区块链的使用场景时，首先我们得确保交易数据是可以获取同时可以量化存储到数据库中。

1. 是否可以将内容数字化存储到数据库中

假设有个非常有意义的基于区块链的气候保护条约。区块链节点遍布全球主要国家，每个节点追踪、测量自己国家的C02排放量，然后基于区块链的同步机制，大家共享所有的信息。不过，该方案不具备可行性。为什么呢？因为目前为止，没有一种有效的方式能够准确测量出每个国家的C02释放量，也就是说无法找到一种方式关联感兴趣的实物和未来存储在区块链上的数字信息。这违背了讨论区块链应用的前提条件，是否可以将内容数字化存储到数据库中。那么如果满足了该前提条件，就一定要使用区块链吗？答案是不一定。如果有些问题可以用传统的数据库解决，比如学校需要存储过往考试试卷内容，传统数据库本身就可以很好的解决该问题。需要明确的是，区块链不是万能的，不是所有问题的最优解。如果现有的技术已经可以完美解决问题，就完全没有必要非要使用区块链。区块链网络的搭建维护，本身也消耗很多的资源。接下来，我们会探讨在哪些场景下，我们需要使用区块链而传统的数据库是没法实现的。

在分析很多允许的区块链网络使用场景之后，我们总结了最佳使用场景的4个因素。前三个是必须的，最后一个因素虽然不一定需要满足，但是满足它能够说明该使用场景更加适合许可链。许可链（Permissioned Blockchain）是指参与到区块链系统中的每个节点都是经过许可的，未经许可的节点是不可以接入到系统中。前面介绍的私有链和联盟链都都属于许可链， 只是私有的程度不同。

多方写入

许可链允许不同的参与方在一定的规则下访问、修改一个共享的数据库。也就是说多方写入才会发挥区块链的潜力。比如比特币网络，每一个参与者都有自己的钱包，他们可以在任意时间发起转账付款交易参与到比特币网络。相反的，假使一个线上的自行车销售商户考虑将所有客户采购订单信息迁移到区块链上以保证数据的完整性。当客户订购一款自行车之后，店家首先需要确认店内是否有这款自行车以及验证客户付款方式的有效性。可以看到人工的参与不会因为区块链的使用就能被取代。如果一切确认无误，店家将订单添加到区块链中。在这个例子中，只有店家才有权限访问修改用于自行车订单的信息，而客户是无法访问的。这种情况下，使用区块链存储客户订单是没有意义的，因为所有的交易都是由一方也就是店家完成的。设想个稍微不同的场景，淘宝电商平台。淘宝上的所有店家在准入之后，可以自行销售自己的商品，这种场景下多方写入的条件就很好的满足了。那么淘宝网需要搭建个区块链网络记录所有的交易信息嘛？+++

信任缺失

区块链的引入就是解决不同参与方某种程度上信任缺失的问题。如果组织本身或者个体之间在某件事上不存在信任的问题，区块链在这样的情景下反而有些多此一举。比如一个研发团队通过git 仓库管理代码提交，每个人不会恶意去篡改共享空间的内容。