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.quora.com/Whats-the-difference-between-blockchain-and-a-database>

<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准确度量，并且数字化存储到数据库中。

1. 是否可以将交易信息准确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，大家共享全球的信息。不过，该方案可行性有待商榷。因为目前为止，没有一种有效的方式能够精确测量每个国家的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存储在区块链上的交易信息。这违背了讨论区块链应用的前提条件，是否可以将交易信息数字化存储到数据库中。

如果满足了该条件，就一定要使用区块链吗？如果有些问题可以用传统的数据库解决，比如学校存储期末考试试卷，传统数据库本身就可以很好的解决，这样就没有必要一定要使用区块链上。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，就完全没有必要刻意使用区块链。区块链网络的搭建维护，本身也消耗很多的资源。接下来，我们会一起探讨在哪些场景下，我们有可能需要使用区块链而传统的数据库是没法实现的。

是否存储状态只是判断标准的第一不，还需要其他依据帮助分析区块链应用场景。本书总结了区块链最佳应用场景的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。~~

b. 是否多方协同写入

有人曾经说，区块链颠覆的核心就在于去中心话，也就是说多方协同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交易。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。这里可以看到，人工的参与不会因为区块链的使用就会被取代。如果一切确认无误，店家将新的订单添加到区块链中。在这个例子中，只有店家才有权访问、修改自行车订单的信息，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就变得没有那么适合，因为所有的交易都是由店家一方完成的，多方协同写入准则是没有满足的。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？这又牵扯到前面提到的什么样的数据不适合上链。

因此，如果一个区块链网络只有一个写入者，那么无论拥有多少共识节点都是没有意义的， 因为写入者可以随意写入、变更数据，本质上又变成了一个集中式的系统。一个合理的区块链应用是要求参与的各方都可以具备预先设定好的写入权限，从而真正意义上达到去中心话的目的。

c. 是否存在信任缺失

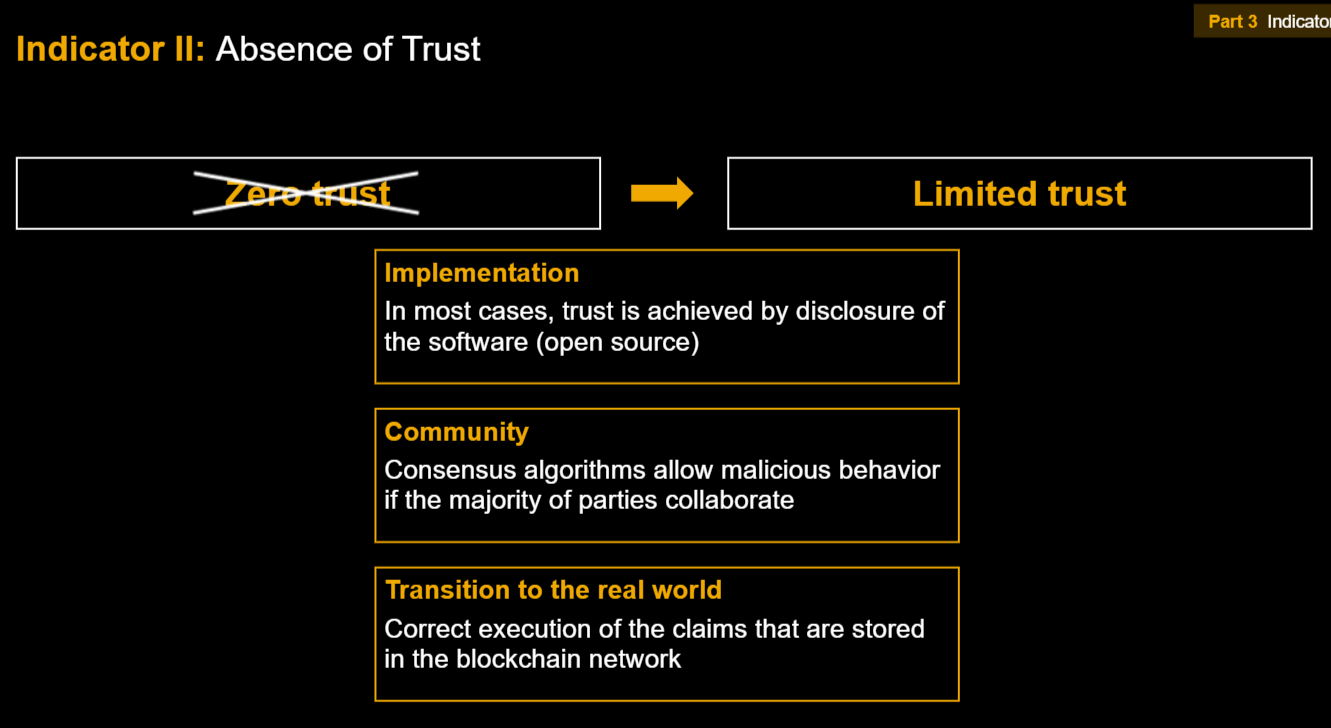
区块链的意义在于使得互不信任的各方可以通过区块链传递和获取信任，并且这种信任建立的成本是很低的而且性价比极高，基于区块链本身的特点。如果参与方本身不存在信任的问题，这种场景下区块链的信任传递特性反而有些多此一举。~~举例来说，一个研发团队通过git管理产品代码，每个人都是贡献者，信任缺失的问题一定程度上是不存在的，贡献者没有理由恶意篡改代码内容， 而且git本身也有权限管理的设计。因此区块链在此场景的适用性就值得再考虑了。~~

尽管上述例子中团队信任是存在的，然而并不能完全保证永远不会有人蓄意销毁代码库。换句话说，完全信任存在但是比例非常有限的。这里需要指出区块链技术很重要的一点：区块链的参与方可以不完全信任彼此，但是需要建立一定程度上的信任才能受益于区块链网络。

这种最低程度的信任可以分解成以下三个要素。

第一点，参与方需要信任区块链网络，比如分布式账本的实施。多数情况下，该信任是通过开源区块链网络代码来建立的。例如超级账本，多链以及其他公开的区块链网络实现方式。第二点，参与方需要信任有所有参与方组成的整个社区。这就牵扯到区块链网络的共识算法， 公链比特币的POW算法依赖于超过50%的网络节点是可信的，这是非常重要的假设条件。如果该条件不能满足，区块链能够带来的信任是完全无法保证的。虽然允许区块链基于其他的共识算法，真个系统网络的信任度还是依赖一些参与方的真实性。

第三点，参与方需要信任数据库数据到真实场景的过渡。区块链可以很好的确保数据的真实性，这些真实的数据接下来的使用、实现参与方也需要建立一定的信任。



前面提到区块链颠覆的核心在于去中心化，那么区块链与生俱来具备的互信特性就是去中心化的基础。没有最基本的信任，去中心化等所有特性都会变得毫无意义。

d. 是否需要取代第三方

比特币区块链网络的引入，使得数字交易不需要第三方金融机构的参与，点对点可以高效安全的完成。回想传统的跨境交易需要经由各个国家金融机构的审批，整个过程不仅会产生手续费，也会产生时间成本。可以说去除中间商，一直也是区块链相比传统行业很大的优势。

可以看到一定情况下取代中间商会带来时间，成本上的节约。不过不是所有的场景，中间商都需要被取代或者能被取代。如果可信任的第三方已经存在而且能够解决问题， 那么可能就没有必要上区块链。切记，区块链不是万能钥匙，本身也捆绑很多资源成本。

Airbnb, 是一家联系旅游人士和家有空房出租的房主的服务型网站，它可以为用户提供多样的住宿信息。可以看到，Airbnb并不仅仅只是一个房屋信息提供平台，同时需要做很多的沟通工作，协调房主以及旅客。而这些内容是不能被区块链的实施就能取代的。因此，我们在判断应用是否适合使用区块链的时候，不能简单认为有中间商的应用场景都适用区块链。

需要注意的是，本书中提到的判断标准是作为判断区块链应用的充分不必要条件，也就是说，如果满足四大判断准则就基本可以肯定为区块链应用，但没有全部满足的应用也很可能是区块链应用。