

今天我将从原理、应用及投资的角度和大家谈一谈区块链。



## 区块链的原理

首先，区块链是什么？

区块链是一种去信任中介的、可靠的分布式账本技术，它有以下三个特质：

- 区块链是一种以密码学方式保证的、不可篡改和不可伪造的分布式账本技术；
- 以严谨的数学解决方案构建起了与“中心化”机制相媲美的“去中心化”信任机制；
- 区块链技术将重构人类经济活动的基础架构，催生出全新的分布式商业形态。

关于它的定义，我比较认可的是“区块链是在没有信任基础的主体间构筑合作的一种技术手段”。最典型的例子就是比特币。相隔万里的参与者可以共同参与比特币网络的维护，在没有信任基础的主体间构筑或大或小规模的协作，这是区块链技术最核心的东西。这个核心特质与分布式商业非常吻合，即通过技术手段保证合作各方相互之间的对等。

那么，什么是分布式商业形态？

分布式商业是基于区块链技术和思维的新型商业形态，其最重要的特质就是使对等合作成为可能。如果用一句话概括，就是以对等合作为基础的商业形态或者商业模式。比特币网络就是对等网络，这个网络里的每个节点，都是对等的，不存在中心化的节点。

## 区块链的应用

分布式资本从2015年开始做区块链领域的投资，是中国区块链行业最早的机构投资者之一。至今三年多的时间内，共投资超过一百五十个项目，其中70%左右是境外项目。通过这几年的投资，我们接触了整个市场上相当大部分的项目。目前来看，区块链在以下领域已经有了一定程度的落地应用。

### 金融领域

区块链最早被应用的领域是金融行业。在金融行业里又可以进一步细分为三个子领域。

一是清结算。2015-2016年的时候，第一批对区块链感兴趣的机构就是金融体系里的清结算机构，比如DTCC、欧交所、中证登、中债登等。在区块链的世界里，支付即结算，比特币不需要任何第三方中介机构记账，支付后就可以直接在钱包里看到。现行的所有金融交易都包括交易环节和清结算环节。为了金融体系运转，清结算环节耗费了大量的经济资源。如果我们用区块链技术构建一个金融交易系统，则会比传统的交易和清结算系统效率更高，成本也更低。这方面很多机构都在做尝试，例如澳大利亚证券交易所就正在着手构建基于区块链技术的交易系统。

二是支付。不仅仅是比特币，还包括现实生活中真正的支付。现在跨国间的支付效率不高，花费时间较长，而且成本相当高。这是跨国支付的痛点，用现有的技术手段、组织架构、思路不能解决，于是有人就想到用区块链技术的特点来解决这些痛点。abra就提出了一个理念，在跨国支付领域里面基于区块链技术，人人都是一个支付节点，不需要任何现有的金融基础设施。用abra开发的系统思路，完全不需要用现在的银行，他用比特币系统做一个桥接，比特币系统是一个全球性的网络，在主要经济体里面都形成了效率很高的比特币和本国法币之间的交易系统，可以很方便地把所持有的法币换成比特币或者反过来。这个商业模式给我们一个启示，基于区块链的商业模式未必是完全去中心化的。

第三个是保险。最开始，保险不是现在的商业保险形式，而是互助保险。即有共同利益的群体在一起，相互提供支撑，这是互助保险的概念。互助保险能够使得某个

群体抗风险能力增强，但也有一个致命弱点，那就是构筑互助保险的群体很难找到有共同需求的人。于是商业保险出现了，商业保险虽然使得生活受到了保障，但需要支付很高的保费。因此，当区块链技术出现之后，很多人就开始研究区块链与保险结合的可能性。因为区块链的本质是在没有信任基础的主体之间构筑大规模协作，保险的本质是互助，区块链的技术手段和思维模式，可以使得保险回归“互助”本质。

以太坊区块链的出现使得智能合约的概念诞生。智能合约能把以前通过个体与个体之间基于社会法律保障体系和制度缔约形成的合约，变成无需外部制度来确保执行的某种合约或某种约定，通过代码自动执行。

现在已经有人开始尝试开发相应的智能合约，来自动化执行保险合同。当然，现在还做不到像传统商业保险机构所提供的那样复杂的保险合同，但一步步小的尝试，其实也能带来大量的创新，解决很多问题。



## 供应链管理

除了金融行业之外，区块链技术落地的另外一个领域是供应链管理。国内就有很多结合区块链技术做供应链管理的项目，涉及家电、汽车等行业。供应链涉及到大规模协作，因此它很适合应用区块链技术。

## 媒体领域

第三个是媒体。区块链上记录的数据可追踪，因此在媒体领域可以用于数字版权的记录和追踪。当然，并不是简单的追踪就可以了，现有的管理体制要求要有权威机构认定，因此区块链技术在这一领域的普遍应用还需要相应的社会管理体制的适度调整。

## 防伪溯源

第四个就是防伪溯源，利用的是区块链可追溯、不可篡改的特点。但并不是基于区块链技术就能彻底解决防伪溯源的所有问题，区块链技术能保证链上的记录是不可篡改的，但是不能保证上链之前的东西一定是真的，所以要彻底解决防伪溯源问题需要结合其它的技术。

## 医疗领域

第五大领域是医疗。现在医疗机构获得的医疗数据呈爆炸式增长，这些数据存在哪里？存在医院里、研究机构里、大型医疗设备商手上，很容易造成数据泄露，有可能导致致命的后果。

基于区块链系统保存的数据，可以做到“谁的数据谁作主”。数据安全性得到保障后，会延伸出很多新的商业模式。每个人可以掌握自己的数据主权，有权决定自己的数据用到哪里，同时如果对方要用自己的数据，需要支付一定的报酬。这就是一种新的分布式商业生态，每个人对等的合作，我该有的权利我掌控，贡献能贡献的东西、得到能得到的东西。

## 身份验证领域

身份验证领域也能用到区块链技术。传统互联网缺乏一个身份层，每个人的身份是依托中心化机构认定的。中心化的认证机构会导致整个互联网的效率都很低，反复认证的成本也很高。区块链技术能为所有网络参与者构造出一个分布式的身份体系，这会极大地提高互联网的运行效率。有很多项目都在做身份验证，但还只是开始，需要找到一系列具体的方法来构建基于区块链的分布式身份认证体系。

## 公共管理领域

接下来的领域是公共管理，最典型的的就是投票。比如，美国总统大选的时候，大家都排着队投票，效率低，又容易出错。如果基于区块链技术构建一个投票体系，再结合前面所讲的身份体系，那选民在互联网上就有一个唯一的身份，这样政务管理

系统就能改善很多。

## 物联网领域

其它可能会深度应用区块链的领域包括AI、大数据、物联网、人工智能等，这些领域将来都少不了区块链。物联网出现很多年了，但到现在还没出现大规模的商用。一方面可能是因为硬件跟不上，缺乏高可用、高灵敏度的传感器。另一方面可能是底层技术的问题，物联网时代万物互联，人机之间、机机之间数据交互，不同的设备不需要人的指令，只需要获得其它设备数据就能有所动作，这是物联网未来所应该达到的目标。基于此，数据的安全性就变得至关重要，需要有一套机制或者一种技术让人相信这个数据，以及数据传输是万无一失的。如果这两者的安全性不达标，那基于数据的这些领域的发展都是空谈。现在来看，比较现实可用的底层技术可能就是区块链，如果这些领域的数据是构筑在基于区块链的数据交互系统上，那么它上层的应用才可能让大家放心。

## 区块链监管

最后我们来看看监管方面的情况，全球范围内的区块链监管大体上分为三类一类是经济体量不大且相对落后的国家把区块链看作一个发展机会，在监管上比较开放；另一类是监管框架清晰并且相对宽松的发达经济体，如新加坡、瑞士等，目前大部分区块链项目都注册在这些国家；第三类是以美国为代表的大型重要经济体，这些经济体的监管机构一直都在比较积极地跟踪、研究区块链的发展，再加上来自区块链业内的一些力量自下而上的推动，我们预期不用太久，其监管框架就会变得逐步明晰。