

## 第7讲 | 区块链的常见误区

2018-04-09 陈浩

深入浅出区块链

[进入课程 >](#)



讲述：黄洲君

时长 10:51 大小 4.97M



经过了我前面几篇文章的铺垫讲解，你应该已经对区块链的知识体系已经有了一个基本的了解，但是，区块链是一项新兴的事物，大多数人依然处于知识的迷雾区，对区块链的理解并不是十分透彻。

我在很多场合都做过区块链领域的分享，有趣的是，无论是线上还是线下，大家都会问我一些相似的问题，今天，我就跟你一起聊聊几类理解区块链的常见误区。观点仅代表我个人的看法，也希望你可以提出不同的见解。

### 1. 数字货币没有背书，我为什么要用呢？

在各种场合聊起数字货币时，我都会被问到这个问题。

其实，这个问题不是单纯一个数字货币的问题，而是货币发展的问题。

因为我们从小就被灌输了“钱可以买到东西”，所以信用货币的概念已经成了一种本能反应，这种本能反应会让我们觉得信用货币的存在是那样的理所应当，同时也自然而然地会把信用货币的概念代入到数字货币当中。

所以，这个时候，我们首先要跳出自己的视野局限。

如果你穿越成唐代人，忽然讨论起人民币这种特殊的纸可以买米买粮，其他唐代人肯定不买账。因为大家只认金子和银子。同理，当我们在讨论数字货币的时候，你完全套用信用货币的概念势必难以兼容，这与唐代人处境是不是相似呢？

并且，信用货币的体系并不是完美无缺的，首先是它在刚出现的时候不是特别的稳定，发展过程一波三折。一战和二战期间的经济问题，或多或少都与当时的货币设计缺陷有关，现代信用货币的设计都是建立在这些血的教训上的。

其次是信用货币是与国家利益息息相关的。比如国家之间的贸易战，通常会在本国货币政策上所有体现。

所以当我们在讨论数字货币的时候，先要想清楚我们到底在讨论什么，因为我们没有讨论任何基于国家的信用货币体系，我们在讨论的是一个完全崭新的虚拟货币体系。

很多人理解信用货币的方法很简单，比如我经常遇见的观点有：我相信法币是因为有政府背书。

但如果我们换个角度想，选择相信其实是个人行为。如果某种资产具有非常高度流动性，比方说美元，在东南亚或者中东地区，如果你不接受美元支付，美国政府也不会拿你怎么样，这桩生意你不做总有人做。

所以你通常会换个思路，我先接受，待会换成人民币不就好了，数字货币也是同理，充足的流动性本身就可以为资产提供良好的背书。

如果硬要说一说数字货币的背书，我认为，社区本身就是一种背书。

社区由用户、开发者、矿工三者组成的。

他们之间的利益相互绑定，用户使用数字货币决定了市场价格，开发者为数字货币开发了更多的功能来提升生产效率，矿工是系统的维护者，三者包含了数量巨大的个体，每个个体都相当于为数字货币作了背书。

## 2. 数字货币是不是投机炒币？

另外还有一种误解来自于行业之外的人，认为数字货币就是投机、就是炒币。其实不是这样的，数字货币出现的初衷并不是为了投机炒币，而是希望构造一个点对点的去信任系统，只是在发展过程中被投机主义者大肆利用了。

确切的说法应该是数字货币的特性刚好满足投机者的需求，即使没有数字货币，投机主义也会存在并且长期存在，而且投机在金融领域并不是一个贬义词，它也是中性词汇。

投机者为整个交易市场提供了充足的流动性，商品价格波动风险被所有投机者所稀释，这是一个健康的交易场所必备的。所以数字货币是中立性的工具，我们应当理性看待。

## 3. 区块链是不是万能的？

很多人接触了区块链以后，觉得看什么都想拿区块链来做。但是，你忽略了一点，区块链本身也属于分布式系统，分布式系统有哪些局限、哪些约束，区块链一样也有。

需要指出的是，区块链领域有个说法叫做“不可能三角”，意思是说区块链的“去中心化”“安全”“环保”三个要素不可能同时全部满足。

这个说法我没有仔细论证，个人感觉这三个指标并不好量化，所以未必成立。本着学术严谨的原则，我不作过多的评价。

反而在分布式领域，有个著名的 CAP 定理。

在 CAP 中，Consistency 是一致性，表示同样数据在分布式系统中所有地方都是被复制成相同；Availability 是可用性，表示所有在分布式系统活跃的节点都能够处理操作且能响应查询；Partition tolerance 是分区容忍性，表示不同节点之间数据同步有意外情况产生时，能够容错。

一般情况下，CAP 理论认为你不能同时拥有上述三种，只能同时选择两种。所以，当我们应用到区块链上时，可以明显地发现区块链其实是一个 AP 系统，尤其在 A 这个指标上，

也就是可用性做得非常好，所以相应地，C 就会降低，反映到具体系统中的交易吞吐量上，自然会也会降低。

当我们在分区容忍性和一致性中做取舍的时候，如果强调“不可篡改”“去中心化”这两个特性，就会明显感觉到区块链跟不上大吞吐量的业务。

所以理解了以上内容，我们在做技术选型时，如果去中心化不是强需求，还是建议你使用中心化的解决方案。

## 4. 去中心化是不是区块链唯一的评价标准？

既然谈到了中心化，我们就来看看“你是否应该去中心化”的话题，自区块链发展至今，“中心化”和“去中心化”的争论就一直存在。

支持去中心化的观点认为：区块链的初衷就是去中心化，所以也衍生出一条准则：“凡是没做好去中心化指标的系统都不是区块链”。

持有这样观点的人通常都跟我一样是技术出身，或多或少都有些理想主义的极客情怀，这一点本来是无可厚非的，但市场是逐利的，情怀其实常常并没有办法变现。

所以，这导致的最直接结果就是：秉持这种去中心化原则会让区块链的落地过程异常缓慢。

持有“去中心化是唯一准则”这样的观点，往往也会误导刚刚入门的业务和产品相关的人员，误以为去中心化是区块链产品的一条评价标准。

其实并不是这样，去中心化只是一个公有区块链应当具备的基本特性，但是我们衍生到区块链应用层面的时候，其实去中心化往往并不能契合到一个公司的业务上，所以我在这里提倡：当我们在思考区块链的解决方案时，还是应当以需求为第一导向。

事实上，我们在讨论去中心化的时候，更多是夹杂了对强势的不满，这其实可以转化成“对服务者进行监督”的思路，一味地强调去中心化可能会陷入舍本逐末的尴尬境地，我们一定要看需求是什么，再去选择要不要。

换句话说，任何情况下，人与人之间必然存在信息不对称和认知不对称的问题，任何应用都会存在信息提供者和信息消费者这两种角色。

这是由人类社会结构决定的，妄图消除这两种角色之间的差异是非常难的。所以应用的“去中心化”要问运营者和消费者，而不是空喊口号。

有个常提及的词叫做“赋能”，被赋予能力的角色始终处于被动地位的，我们可以把区块链看做新型的赋能工具，至于是不是去中心化，设计过程中要看具体的应用场景，实施过程最终取决于消费者。

## 5. 联盟链为什么没有公有链普及？

我相信很多人入门区块链以后都会有个疑问，区块链这么火热，怎么都是公有链热度高，联盟链反而声响不大。

所谓联盟链，就是这个区块链具有准入许可，不像公链，任何人都可以随时进入，准入许可意味着候选节点进入区块链时，需要得到已经在网络中的节点的许可，所以联盟链也叫做许可链。联盟链的节点数通常不多，维护成本相比公链要低。

造成联盟链不普及的原因，有以下三种。

第一是观察者偏差，因为 To B 的业务往往是商务合作的形式，并不直接进入大家的视野，实际上有很多大型机构已经尝试，或者已经部分落地了的联盟链业务。

第二是联盟链往往会遇到政策和监管要求，与公链相比，实施起来条条框框太多了，发挥的空间有限。

第三是联盟链表面上是一个技术问题，本质上是一个博弈问题，这是我 2016 年在文章《论联盟链的局限性与公有链》表达过的一个观点。

你往往需要设计一个业务模型，使得所有的博弈趋于均衡稳定，但是这又非常困难，我们无法一概而论。

总不能每做一块业务还要搞个形式化验证吧，并且联盟链无论是应用生态还是技术迭代都会比公链缓慢。

所以整体上看，联盟链的应用范围仍然不及公链广泛。

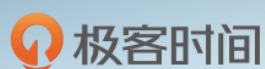
## 6. 区块链是否会颠覆当下互联网？

很多早期的区块链文章经常说：区块链会颠覆当下的互联网什么的，关于这一点，我其实持保留意见。区块链如何打通与现有互联网的界限还是一个未知数，最大的可能性仍然是区块链成为互联网的一部分，作为底层设施改进了原来互联网的架构。

## 总结

今天，我带着你从不同的角度聊了理解区块链的常见误区，我们从谁在为区块链背书谈起，提到了区块链是否是万能的，去中心化是不是区块链的唯一标准，联盟链为什么没有公有链普及，以及区块链是否颠覆了当下的互联网。希望能唤起你对区块链的独立思考。

最后和你分享一个问题，区块链会改变微信和支付宝的地位吗？你可以给我留言，我们一起讨论，感谢你的收听，我们下期再见。



# 深入浅出区块链

你的区块链入门第一课

陈浩 元界 CTO



新版升级：点击「 请朋友读」，10位好友免费读，邀请订阅更有**现金**奖励。

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 第6讲 | 理解区块链之前，先上手体验一把数字货币

下一篇 第8讲 | 最主流区块链项目有哪些？





unite

2018-04-09

15

针对微信的聊天社交功能，我觉得完全可以用区块链技术进行代替。原因如下：

1.朋友之间的对话有加密需求。大多数人都不会让别人知道自己和朋友聊了什么，对话内容需要加密，且聊天软件存储的数据尽可能存在数量很多的服务器上，一来减少自己存储数据所需的服务器成本，二来所有数据加密且去中心化提高系统安全性。

2.个人隐私的保护。最近facebook的由于个人隐私的泄露被搞的焦头烂额，如果把每个...  
展开



阿痕

2018-04-21

8

区块链会改变微信和支付宝的地位吗？这个问题的本质是去中心化的应用DAPP会取代中心化应用吗？这个取决于整个社会对安全和效率之间的平衡。在当前中国，大部分人会优先选择效率，从而出让个人隐私。但随着时间的推移，当越来越多的facebook事件出现后，整个社会会越来越向安全这边倾斜，不过个人认为这是个漫长的过程。

展开



duer

2018-04-09

4

应该很难，从“货币”的角度，我的理由是会得到央行的监管产生的“保护”。目前支付宝和微信的主要功能还是承载法币电子化的应用功能，比如支付、流通、储蓄等。比如最近余额宝等货币基金逐步被取消“支付功能”而回归基金本身来看，金融创新的边界是不能影响国家对于法币的监督和管控，也就是利用货币进行经济调控的能力。所以央行会继续出一系列的政策来制止数字货币的流通。

展开

作者回复: 不同意，rmb本身的问题是经济和货币问题，数字货币的出现是一个机会，非常可惜，我们失去了一个很好的机会。制止数字货币其实。。。哎，经济调控看美元，不是看自己。



龐校長

2018-05-19

3

微信和支付宝，对于人们来说是一个什么角色呢？

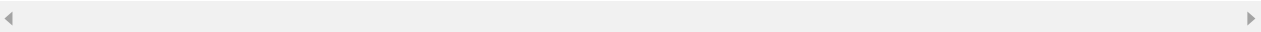
微信，是一个中心化的社交平台。

支付宝，是一个中心化的支付平台。

社交是否有信任危机，需要区块链去解决信任问题？...

展开 ∨

作者回复: 有道理~



咏哥

2018-04-11

👍 2

rmb本身的问题是经济和货币问题，数字货币的出现是一个机会，非常可惜，我们失去了一个很好的机会。制止数字货币其实。。。哎，经济调控看美元，不是看自己。

2018-04-09完全同感！

展开 ∨



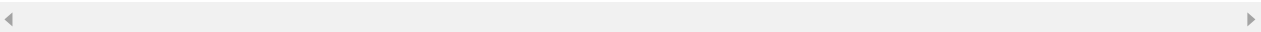
YYifan

2018-06-16

👍 1

不能寄望区块链保护隐私，我们被每个app侵犯隐私前都点过同意。你能不用微信吗？即使放在区块链上你还是得乖乖点同意交出隐私

作者回复: 同意，区块链隐私有两面性。审查也是必要的。



chengzise

2018-04-26

👍 1

区块链的技术在公益上可以推广，人人可以参与整个过程的监督

展开 ∨



酱了个油

2018-04-10

👍 1

今天的问题也是我很困惑的问题，希望老师可以解答，就是“区块链如何处理高频交易”，拿比特币来说，每个区块的认可要60分钟，我们买瓶可乐，商家需要等60分钟肯定是不可行的，但是我不知道有没有办法解决这个问题。

展开 ∨

作者回复: 目前有闪电网络等类似小额支付通道的方案，后续会有讲解。





良辰美景

2018-04-10



个人感觉不会，不是一个东西，区块链属于技术，支付宝属于应用。如果问题是数字货币会挑战法币么，个人认为还有个稀缺性的问题，每个社区都可以发布自己的数字货币。目前来看就有上千种数字货币。比特币目前每秒最多只能交易七笔。而对于扩容社区出现了巨大的不同意见。分布式和中心话在发展效率上是否有巨大的不同

展开 ∨



泽star

2018-04-09



微信服务是提供信息交流平台，但是个人产生的数据并不是自己的。而区块链既能解决信息传递，更能解决信息回归用户，这点区块链取胜。支付宝，微信支付解决信任问题，而区块链本身就是为解决信任问题而来，只是区块链现在因为法规，无落地项目，大众不知，没有广大用户，监管不严等现实问题，暂时无法取代微信与支付宝，但是从解决问题，提供更好服务，区块链未来是有机会颠覆的。

展开 ∨



Michael

2019-04-01



区块链和微信是不同的应用场景。以当前的技术发展，区块链不能取代微信。微信的服务器需要承载大量的服务器，对于用户来说，很重要的一点是速度问题，当前区块链的技术没办法实现。

展开 ∨



Kira

2018-10-30



对降低c导致系统吞吐量下降的解释有点疑惑，请老师解答下。系统为了可用性降低对一致性的要求，会大大提升交易并发量和系统吞吐量。最终一致性时间拖长了导致系统吞吐量下降，说明系统还是要求保证一致性啊，按这个解释不应该更像是个cp系统吗。



tmy13

2018-06-19



不是很明白没有去中心化的区块链是个什么东西，有没有现成的例子或者应用？

作者回复: 有的，比特币等一大堆数字货币



**YYifan**

2018-06-16



如果央行做出数字货币，更需要无政府的数字货币应对，央行的数字货币一定是中心化（银行和云计算商组成的私链）、身份透明、毫无隐私的

作者回复: 去的是自己的技术中心，提高效率为主，主权仍然是中央的



**robbin**

2018-06-04



我觉得以前是公有链，现在慢慢都会转向私有链，在以后会转向联盟链，那时公有链可能会淘汰掉很多，而且被边缘化

作者回复: 你好，我们观点不同哦，我认为恰恰相反，也会共存。



**Clancey**

2018-05-14



中国央行现在做的数字货币基本目的是要取代现金，如果央行做的数字货币推广应用的话，相信会对支付宝、微信产生巨大的冲击。

作者回复: 其实支付宝和微信也可以转型的，参考bitpay。毕竟用户流量是优势基础呢



**中华老朱**

2018-05-12



我觉得区块链不会改变支付宝和微信的地位，但会促进支付宝和微信进行底层架构的改变，来适应时代的发展趋势！



明月

2018-04-19



它该怎么取代支付宝和微信的地位呢？

展开 ∨



ytl

2018-04-17



支付宝主打电子移动支付，和区块链很相近，很可能被取代。不可篡改，数据透明，无人运维，全球货币流通的优势是支付宝不具备的。

微信主打社交，但数据的隐私保护，数据的取证，免审查是区块链的优势，微信不具备这些优势，可能也会被取代。

展开 ∨



Gavin

2018-04-10



我认为可以，但变革可能来自其外部，也可能来自其内部。目前的互联网应用，基本都是信息流应用，只完成了建立数字化时代的一小部分，我认为，真正的数字化时代需要包括价值信任甚至道德艺术的全数字化，届时目前的互联网应用都将变革，这也是区块链受热捧的一个原因吧，它带来了希望。