# 对区块链的理性认识

2019-11-05

曾以为区块链是革命性的、颠覆性的技术，毕竟区块链和人工智能、大数据并列互联网前沿技术。但是，人工智能达到真正的智能暂时还是梦，大数据也实现不了像《复联》里一样的精准分析。前几天国家领导人对区块链的讲话振奋人心，可过去几年的物联网、互联网+，不也都无疾而终了吗。

## 公有链无法脱离货币

有的观点认为，核反应最初的目的是建造核弹，而核反应现在也作为电能的来源服务于人民，区块链最初的目的是支持比特币的运作，现在我们想要区块链应用于其他方向。也就是说，观点认为核反应的位置和区块链是对等的。

```
核反应 -> 核弹
区块链 -> 比特币
```

可是仔细想想，到底该如何对比这几乎完全不一样的两种事物。如果你看过几本区块链相关的书，会发现讲的东西并不会特别新鲜，观点也完全够不上所谓革命、创新。比特币诞生至今不过10年左右，并没有克服技术上的难题，只是不同机制的组合，它应该和P2P或者某种电子游戏处在同一地位。比特币的价值在于进行电子交易，而不是货币本身。

```
核反应 -> 核能量 -> 大爆炸
区块链 -> 比特币 -> 电子交易
```

因为核反应，才能产出核能量，有了核能量，才能够产生大爆炸。因为区块链，才有了比特币，有了比特币，才能够进行电子交易。所以这样来看，核能量是离不开核反应的，比特币是离不开区块链的。

那么，区块链能够离开比特币单独应用于场景吗？或者说，其实区块链和比特币是一体的，就像核反应产生出的核能量，有价值的是能量而不是反应，区块链产出比特币，运作于区块链上的比特币才有所谓匿名、不可篡改、可溯源等特性，有价值的是比特币而不是区块链。

几天前广州市政府发布补贴区块链企业的细则（实施细则），明确要求“无币”公有链项目。这项政策，一方面是国家不允许发币，另一方面，公有链无币其实是区块链最理想的情况，一般来说，理想是难以实现的。

比特币解决的是交易中的信任问题，解决方式归根结底是数据存在哪儿。两个人进行交易，如果由交易发起方记账，或者交易接受方记账，或者两个人都记账，无论谁记，只要有一方说谎，甚至不说谎，他就是记错了，都会产生争执，不认账怎么办！这时就需要第三方机构介入，通过银行记账，通过律所解决纠纷。要是连银行、政府、法律都不相信，就不用活了。

如果真的不信任中心化的机构，比特币提出的办法是，让全世界的人都为你记账，全世界的人都会记住两个人的交易记录，谁给谁转账多少，这样无论如何都不再会有差错，除非全世界一半以上的人都犯了同样的错误。所以问题在于，凭什么让全世界的人为两个人的个人交易记账？人家为什么要记？于是将比特币作为奖励，谁记账了，并且被系统认为记的账是有效的，谁就可以得到奖金。

没有奖励，世界上的人不会主动为你记账，分布式账本还怎么维持运行？

## 比特币并非去中心化

有人认为分布式记账、分布式数据库就已经是去中心化了，但这一定不是去中心化的最终形态。比如，比特币程序的开发、维护和升级？数据确实天下共享，但程序还是要有人制定规则，有人开发，有人发布，出bug了要有人修复，有更好的点子了要迭代升级，分布式的数据全部经由中心化的程序发布中心发布的程序处理。目前解决程序上信任的方式是将程序开源……这一点暂且

可行，但是程序升级带来的困难就要大多了，要么确保向下兼容，要么确保所有人更新程序。

另外，比特币的数据冗余是个极大的问题，每个节点都需要备份全量数据，而且大多数是不相关的历史数据。如果单个节点不保留全部数据，就无法保证分布式数据的可靠性，但如果保留全部数据，又是对资源很大的浪费。中心化系统一份数据就可以解决的问题，为了能够相互信任，就多出来几十亿份数据？就好比我不相信银行，就自己造一个银行，自己管自己？

可以畅想一下，在牺牲去中心化概念的情况下，能够有哪些可能。

一、全球共用一个数据库，数据库只承担储存数据的任务，分布式程序只解决共识问题。数据库非常安全，数据容量非常大，但是写入规则严格，需要全球一半以上的人认可，或者通过其他的共识机制准入。任何人可以随意查询，可溯源，历史数据不能修改。共识程序是必要的，决定了哪些数据可以写入，比如判断余额是否足够，而且是全世界的人一起判断，如果有坏人想要写入非法数据，需要买通全球一半以上的人……这样数据冗余最少。

二、每个节点只保留一半数据，数据拆分为历史的一半和当前的一半。一个人储存最新的一半数据，另一个人储存旧的一半数据，旧数据只需要负责储存，当新数据过多时同步到旧数据这里。新数据负责接收广播、写入数据，功能等同于现在的节点，如果遇到需要查询历史数据的情况，就从旧数据的一半查。相当于两人合作完成一个节点，新旧节点随时随机搭配，节点的新旧由系统平均分配。至于安全性，因为全网的节点随机配对，应该不会低于比特币，最坏的情况是一半的节点全部挂掉。同理，可将两份数据扩展到多份数据的情况。

三、每个节点只保留一半数据或者更多份，数据对半拆分。就是同一条数据，按照一定规则拆分为多个数据包，分别储存在不同的节点，参考HDFS的储存方式，存在一定冗余，但又节省了不少空间。再激进一点，数据可以实现自验证，网络中的每个节点储存的数据大小是随机的，当用户查询某一条数据时，从全网的节点中搜寻可以组成所需数据的节点，然后从中取出数据。也就是说整个节点网络的数据都混杂在一起，难点变成了如何给数据包设计自验证机制。

## 数字货币和区块链没有关系

有的人谈到区块链的应用，会把央行关于数字货币的研究给扯上，甚至某交易所知名总监，以区块链为主题的演讲，却把比特币和Libra的趣闻轶事说了一遍。很多人都在忽略概念上的区别，这无关紧要，也至关重要。央行说有发行数字货币的计划，也说过区块链可以作为技术选择之一，但区块链从不是必须的技术。区块链对于国家的意义，是“以去中心化之名，行中心化之实”，意在一统国内互联网，方便监管。即使没有区块链，国家也有能力实现各种应用，只是借势上了区块链的船而已。

过去的区块链指支撑比特币运行的技术体系，未来的区块链将几乎约等于联盟链。

华为区块链白皮书中的观点很客观，区块链是互联网的补充，它不会脱离传统数据库，离不开TCP，只是在特定场合下发挥独特的作用。对于国家来说，链上的数据清晰可见，没有人能暗箱操作；对于企业来说，可以方便的实现制衡，几家企业合作共享一组数据，区块链则是打开大门的钥匙。如果没有区块链，可能说不上来数据共享是个什么样子，区块链诞生了，并且比特币在世界范围稳定运行了十多年，所以这是可信的、有前途的技术方向，大家都争先恐后创新、落地。

可以预见，未来区块链的开发会分为两类，一类底层开发，一类应用层开发。底层开发的技术要求更高，开发者素质更高，应用层开发则类似于现在的Web开发。会先后出现一些区块链应用提供商，也会相应的出现一些SDK，开发者调用区块链储存数据、进行交易，类似于现在调用数据库提供的API、请求支付机构的接口。

## 所以

区块链会被广泛应用到我们的网络中，但不足以改变世界。（不要笑）

## 更新

无意间发现了分布式网络 ZeroNet，是一个早在2015年就发布的项目，它几乎满足了所有我对区块链储存系统的想象，而且功能完备，可以基于这个网络搭建博客、论坛、邮箱、共享文件等。当然，我曾想到的、应该存在的问题，ZeroNet也一个都没有解决，算是对我的一些想法的验证，惟一不同的是我希望将分布式网络对接到公网，但ZeroNet的做法是建立了一套自治的网络系统，包括.bit域名也只能作为URI的后缀，这无疑限制了该网络无法被更加广泛传播使用。另外，由于点对点文件系统难以监管，GWF将ZeroNet列入名单，这虽然是特殊现象，但ZeroNet和IPFS等网络似乎可以说明，区块链最适合也只能应用于金融领域或者受限制的互联网中。