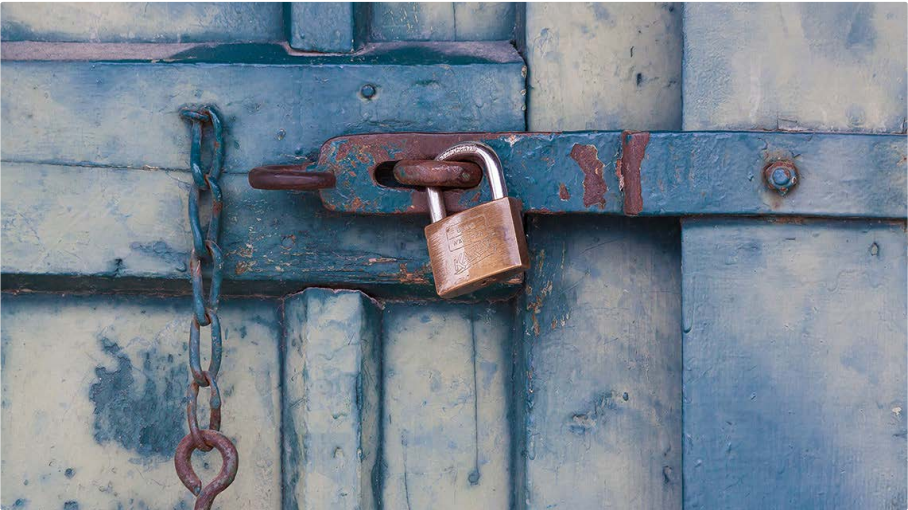


区块链技术（6）-传统金融和虚拟货币

2018-04-17 陈皓





区块链技术（6）-传统金融和虚拟货币

陈皓

- 00:00 / 20:34

前面我们讲了银行的资金托管业务以及国际贸易业务。我讲这些东西，主要想讲什么呢？

金融的本质

我想讲金融的本质。我个人认为金融行业最大的本质就是——促进交易完成，实现价值提升！也就是说，如果整个社会的交易能够更快更高效更安全地完成，那么我们这个社会就会有更好的运作效率，更低的成本，更多的价值。这对于促进整个社会的经济发展是相当关键的。

所以，为了保证交易完成，金融行业需要解决下面几个问题。

- 1. 交易中的信用问题。所以，银行会来作中间人来担保。
- 2. 交易中的资金不足的问题。通过借贷来让交易完成。
- 3. 交易中的大额的问题。把一个大额的金融事件以股份的方式拆碎进行大众投资。

总之，金融行业就是要促进社会的交易，使得这个社会的交易越来越活跃，从而可以产生更多的价值。那么，这个社会的经济就会越来越健康。

下图给出了金融业的四个重要属性。



**效率**

- 加快货币流通
- 快速促成交易



**价值**

- 实际价值的体现
- 让价值得以提升



**激励**

- 实体经济的催化剂
- 激励社会创造价值



**信用**

- 建立信用社会
- 评估信用等级

- 效率提升：加快货币、股票、债券的流通性，快速地促成交易。
- 价值提升：通过金融产品的流通性，让实际价值得到充分地体现，并升值。
- 激励机制：为实体经济添砖加瓦，并激励社会持续付出和成长。
- 信用评级：建立信用社会、评估信用等级，从而改善社会。

是不是有银行做担保，有这些金融机构我们就可以高枕无忧了？不是的，我在前面说过，主要是钱不够多，只要钱多到一定数量的时候，什么事都可能发生。因为逐利是人性中非常疯狂的一个特征。只要有利益，人们就会想要更多的利益。这有时候并不是一件好事。

经济运作的原理

说到这里，我想先说一下经济是什么。对于经济来说，说白了就是整个社会的交易。每个交易中，对于买方，其需要付出的是货币和信用，对于卖方，其需要支付的是商品、服务或金融资产。而支出方是整个经济的驱动力。也就是说，一个社会的最基本的经济活动是交易，而经济状况好的好坏是受支出方影响的。

所以，一个市场的好坏，和支出方有很大关系。在整个社会运作的过程中，需要有一个“贷款机构”，这些机构把钱贷给想要花钱且有偿还能能力的人，然后这会增加整个社会的支出。于是，你的支出成为了别人的收入，别人的收入多了，也会增加他的支出，而如果支出越来越多，某些人的收入就越来越多。

于是这些人的钱花不完，他们就会开始想用钱来生钱。于是就有更多的人借钱给别人。也就是我们所说的投资，而这又增加了更我的支出。于是，整个人社会就运作起来了。所以说，支出是经济的原动力。

我们知道，经济的价值是可能通过提高“生产率”来提高的。然而，生产率并不是很容易能提高的，这是一个长期的过程。而通过“借贷”我们可以短期的提高经济价值，在借贷发生时，消费超过产出，在还贷时，消费低于产出。

所以，整个人类世界的影响经济波动的东西就是“借贷”，也就是为了购买现在买不起的东西，向未来的自己去借钱，或是由未来的自己去还债。这种未来消费的方式并不一定是坏事。如果能还了，就是良性，如果还不了了，那就成了恶性的。

另外，还有一个问题，如果整个社会的支出变多，于是就会出现一片繁荣的情况。大多数人都是目光短浅的，所以，大多数人都觉得经济形势很好，于是就出现更多的借贷。人们觉得挣钱好容易，于是就借钱来买其他金融产品，导致金融产品上涨，于是导致大家觉得应该花更多的钱来投资，那样就会借更多的钱……这样一来，就会出现巨大的泡沫……

关于这个，你可以看一下网易公开课的《[经济机器是怎样运行的](#)》。

## 2008年的次贷危机

2008年暴发的全球金融次贷危机算是一个银行玩出来的事儿。自2003年来，美国人的房价就在不停地上涨，而买房贷款的那些人基本上来说都有比较稳定的工作来每个月偿还房贷。于是，这些人的信用记录，导致房贷成为了比较好的金融产品。

美国房地产贷款系统里面分为三类：优质贷款市场、次优级贷款市场、次级贷款市场。美国把消费者的信用等级分为优级、次优级和次级。

那些能够按时付款的消费者的信用等级被定为优级，那些不能按时付款的消费者的信用等级被定为次级。次级贷款市场就是面向那些收入信誉程度不高的客户，其贷款利率通常比一般抵押贷款高出2%～3%。尽管美国次级贷款市场所占美国整体房贷市场比重并不大，大约占7%～8%，但其利润最高，风险最大。

想一想，如果供房人能还款，那是优质贷款，如果不能还了，把房子收回来，也可以卖个高价。毕竟房价一直在涨呢。

贪婪的资本家们觉得，既然房贷的回报如此优秀，为什么不把这些当成债权出售。嗯，债权转让虽然可以让资金快速回来，但是挣得不够多。于是，贪婪的银行家们决定，把这些房贷打包，形成一个优质的金融产品，然后，在二级市场上发行IPO，让更多的人来投资和炒作，这样就可以挣到一大笔钱。

的确，只要供房人按时供房，这个金融产品就没有问题，所以，房贷打包的二级市场也非常不错。于是，再继续衍生更多的金融产品，各种“杠杆”，然后再加上保险公司为其保险。全世界都疯了。

银行开始乱放贷款，把贷款发给好多根本没有能力还款的人，且在相信房价将继续升值的前提下，鼓励了许多次级贷款借款人去取得浮动利率抵押贷款。这些抵押贷款以在预先确定的期限内低于市场利率引诱借款人，期限过后剩下的则是以市场利率计算。

而美国最权威的评级机构也还错误地把风险比较高的金融产品评成最优质的级别。这样在二级甚至三级市场上套更多的人进入。

最终，最底层的越来越多的人不还贷款了，越来越多的房子被拍卖。一方面导致房价下跌，另一方面，导致银行坏账，最终，像多米诺骨牌一样倒了一片……

然而，因为这事玩得太大了，于是美国政府拿出了7000亿美金来救那些贪婪的银行，而一些投资机构就此破产，还对国内的经济造成了巨大的打击……

## 金融的监督

上面，我们可以看到金融行业非常积极的本质和作用，也能看到其带来的副作用。金融行业发展成百上千年了，今天，我们还是可以看到其存在很多问题。就像上面说的2008年金融危机一样，银行业过于快速地促成交易，加快货币、股票、债券的流通性，导致了各种“杠杆”以及“多杠杆”的出现。

当整个社会为之疯狂的时候，信用评级、风险控制都被抛到脑后了，最终出现投资大大超过和实际价值完全不等价的局面。实际价值无法支撑投资时，风险发生时，整个世界就会出现连锁反应，一发不可收拾。

对于经济活动，这两个事需要平衡，一个是“资”，一个是“债”。如果不平衡了，风险就出现了。无论是对于我们个人，还是对于企业，或是银行，都是一样的。但总是会有人冲昏头脑的，尤其是有“财务窟窿”或者“巨大利诱”的时候，所以，才会有监管机构来审查这些金融机构的“资”和“债”的风险，并制定相关的政策和条例。

而有时候，监管机构又管得过死，导致经济不能充分发展。于是造成了我们经常听到的“不管就乱，一管就死”的局面。所以，很多时候，政府或央行会通过调节货币利率，以及发行更多货币等手段来引导或调整市场，控制风险。

于是，出现了各种经济学，比如，主张政府强干预的凯恩斯经济学，以及马克思主义的政治经济学均表示出了对市场经济没有信心，需要用政治干预手段。还有亚当·斯密的以市场为主导的经济学等。

可能这个问题怎么讨论也讨论不清楚。我个人比较认可的是，经济还是需要自由的，而政府应该控制的是风险和保证经济实体的产权。只有自由的市场经济才会回归金融的本质，促进交易提升，激励大众而提升价值。而政府的风控措施可以对整体金融风险进行调节，这是市场经济不能完成的。政府还要保护私人产权，这对于经济活动是非常重要的，产权保护是经济活动的根本基础。

## 虚拟货币

首先，如果虚拟货币想要有货币的特征，那么就需要何持其稳定。这个稳定不仅仅只是不增发（在你看过上述的经济活动的原理，你知道增发货币并不一定是个坏事），其价值最好是稳定的，因为其要代表某种经济体的稳定性。这就好像黄金、欧元、英镑，要比非洲某些国家的货币更硬一些。然而，目前的虚拟货币没有一个经济体以后面为其背书，所以其远远达不到货币的功能。

于是，虚拟货币开始变成股票一样的，股票是需要后面实体的公司经营情况来背书的，所以流通性比较好的股票，一般来说需要透明公开公司的经营情况，并会受到行情和政策的影响。然而虚拟货币的交易所市场完全在售卖概念，到目前为止还没有一个真正成功的，能够有颠覆性的项目。然而，其靠发布白皮书就可以变成一个几十亿规模的公司。

当然，现在区块链里的经济，是靠二级市场撑着。所以，就像前面说的那个经济规律一样，只要有不停的支出，就会造就一种繁荣的景象。这种繁荣的景象，对于绝大多数不明真相的人来说是很容易让他们心动的，因为人性是想不劳而获且趋利避害的。于是就会引发更多的人进入，于是形成更大的繁荣。

但是，这种后台没有价值体现的玩法，总有一天会达到瓶颈的——就是“支出”不再能够维持下去的时候。也就是没有新入场的时候，老人因为钱投进去了，也不会有更多的钱投入的时候。那个时候就是泡沫破灭的时候。

我在这里讲了这些东西，我想说，就算是虚拟货币，数字货币，其本质也是一样的。如果不能提高效率，降低成本，没有风控和评级，这样完全自由地发展，我认为风险是非常大的。说白了，这就是一个高级赌场罢了，人类历史上已经有过无数这样的案例了……

## 虚拟货币其他的一些问题

### 比特币的几个问题

我们先来看几个比特币的问题，了解了这些问题后，我们才能独立思考后面的几个逻辑问题。

1. 交易成本上升。由于工作量证明需要消耗大量的算力，同时比特币大约 10分钟才会产生一个区块，区块的大小只有 1MB，仅仅能够包含三四千笔交易，平均下来每秒只能够处理 5～7（个位数）笔交易，所以比特币网络的拥堵状况非常严重。有时候，一笔交易确认的小费已经很高了（并不见得比银行便宜），另一方面，确认时间很长，在拥堵的时候需要好几天。
2. 个人无法参与。一条链已经非常长了，所以个人电脑已经跑不动了。也就是说，如果你想玩比特币，你电脑的算力都很难校验账本了。另外，记账的人也越来越趋于巨大的大公司。本来是一个全民参与的去中心化的事儿，而现在成了大众无法参与的事了。那么，这还是去中心化吗？
3. 社区的利益纷争。上述两个比特币的技术问题必需亟待解决，比特币才能玩下去，不然，也就是这一两年比特币也就快玩完了。所以，社区内也很迫切地想解决这两个技术问题。

然而，自从中本聪把所有的工作交给比特币的核心团队（core team）并消失之后，比特币社区中就这些技术问题如何解决，核心团队和矿工的谈判就没有谈好过。你可以看到，其中的利益纷争和中心化的组织结构没什么两样。（具体你可以参看这篇文章《[金融史上的神奇怪胎：比特币扩容大战的前世今生](#)》。）

作为标杆数字货币，比特币姑且这样，何况其他数据货币呢？但是你要解决这个问题，就会像前面那样所说的那样，你就需要适当地去“去中心化”了。

几个功能的问题

我认为，下面这几个问题如果不解决好，同样虚拟货币也是有很大风险的。

- 交易时的身份验证。银行对于网上交易的验权是相当复杂的，不同的金额会有不同的验证。而虚拟代币只关心私钥，而不关心是不是这个人。
- 资金归属权保护。对于银行，如果我的卡丢了，密码丢了，U盾丢了，我可以申请冻结账户，并能通过到银行柜面把我的财产声明回来。虚拟代币如果你的密码和私钥丢了，那就真的丢了。
- 损失赔偿问题。我有个表妹在英国生活，有次在ATM机上取款时，突然接了一个公司打来的电话，说有急事需要处理，于是，忘了取卡就走了。被后面的人取了2000英镑。后面发现了，报了警，银行方面向警方确认后把失窃的钱全部赔给了我的表妹。

也许，第一个问题还好解决，第二个问题，我觉得在区块链上是没有解的，而想解决第三个问题，我认为需要一整套的社会运行机制，区块链这个技术更显得无能为力。

几个逻辑问题

最后，我们再来思考几个逻辑问题。

- 技术驾驭能力问题。这种去中心化的技术难题并不是什么人都能Hold得住的。一方面是结点是不可信任的假设，另一方面，其中有太多的政治上的博弈问题不是技术能解的。所以，那些说用区块链来解决各种业务问题并颠覆现有大公司的人或公司，我觉得他们无论是在业务上还是技术上的水份都很大，更别说颠覆了。思考问题：这是不是一个概念炒作远远大于实际能力的乌托邦？
- 比特币颠覆了什么？有人说：“比特币本来应该要证明一个真正的自由市场力量，结果却充满了诈骗者、投机者和小偷，而且对真实世界的交易没有帮助，还消耗了这么多的社会资源”。本来，中本聪想通过比特币来建立一个可以避免政府、银行家和企业的支付系统，从而避免通货膨胀或金融腐败。但相反的是，比特币现在是一堆快速膨胀的投机泡沫，其创造了另一个和传统世界一样的金融体系。思考问题：数字货币是在颠覆现有的传统金融体系，还是建立另外一个一模一样，但充满更多泡沫和投机的体系？
- 是否消除了中间商？如今比特币已有各种不同类型的中间商，像是能帮用户把零碎比特币存储成账户的钱包服务等。这些中间商的存在却也破坏了比特币的隐私特性，像 Coinbase 这种中间商就会搜集跟用户有关的大量信息。这并不能怪罪中间商的贪婪，而是因为比特币本身的设计让交易变得非常复杂。对非技术背景的使用者来说，如果没有中间商或应用程序简化，使用比特币还是不太便利。思考问题：比特币的原意是建立一种无需银行和中间商，不会有交易费用的交易系统，但现在比特币的进展却反过来复制了原本想破坏的体系。
- 大公司参与的区块链？看到像投资银行高盛或是中介机构蚂蚁金融这样的公司参与到区块链这个事来？你有没有觉得，有点奇怪？我还看到有些人评论到：“区块链就是需要大公司来参与”。看到这，我不知道中本聪会怎么想？反正我感觉有很强烈的喜感。思考问题：区块链本质上是要颠覆这些银行和中间商的，代表了先进的生产关系，而这些传统的落后的生产力来玩这个事，是不是有点像，我造了一列火车，而要用这些马车来拉……
- 投资人投资去中心化的公司？我有点不明白，为什么投资人或是投资公司会关注这个事？如果投资人看到了去中心化这个事可以颠覆现有大公司，所以看好这个事。于是把钱投给了去颠覆中心化的大公司的这些公司，而这些公司又会成为中心化的大公司。这看起来好奇怪啊。因为真正的去中心化是完全找不到主体的。思考问题：去中心化需要有公司吗？有公司的话，还能叫是去中心化吗？投资人并不傻，那么，他们想来这里面干点什么呢？是投机吗？
- 有挣大钱的机会，你会共享出来？传销组织的三个阶段：第一，让你觉得你很穷困，告诉你致富的捷径。第二，模糊掉具体细节，用各种高大上的类比和比喻来取得你的信任。第三，通过发展下线来制造虚假繁荣，让你信以为真。所以，虚拟货币中绝大多数都是这样的特征。他们和骗子们所有的技巧如出一辙——“我有一个挣大钱的机会，但是我想和你共享出来，只需要你对我投资一点钱，未来你可以得到百倍的分红”。我靠，可能挣大钱的事，你愿意分享给这么多人？思考问题：在区块链中你有没有发现这样的身影？为什么他们要把这样超级革命性的可以挣大钱的项目在这么早的时候就分享给这么多人？

最后一个哲学问题

当一个社会出现问题的时候，在民众开始抱怨和发泄不满的时候，需要一个目标。这是一件很自然的事。于是有人就满足大众，告诉大家，你们今天之所以穷，之所以苦，之所以不公，是因为那些中间商玩弄了你们，是因为政府不可信，是因为有坏人……因为这是最好被民众所理解的，因为有明确的目标，简单粗暴。这也是人们容易被煽动的原因。

然而，整个社会的运作其实是一种协同，由多方带着不同的利益或诉求而形成的。也就是说，问题的出现是多方造成的，或是社会协同出了问题造成的，是机制造成的。并不是其中的某个实体造成的。

而且，无论你制定出什么样的机制或是规则，都会有好的一面和不好的一面，这一面有多好另一面就有多不好。所以，如果一件事完全只有好的，而没有不好的，那么，你有绝大可能是在被人忽悠中。

去中心化就是好吗？我们不需要权威机构了吗？技术可以解决信任问题吗？

我是要继续改善我们现在这个社会，还是直接毁了再建一个？是“破坏性的建设（Disruptive Construction）”，还是“建设性的破坏（Constructive Disruption）”？

我不知道你喜欢哪个，而我喜欢后者。

文末给出了《区块链技术》系列文章的目录，希望你能在这个列表里找到自己感兴趣的内容。

- [区块链技术（1）-区块链的革命性及技术愿景](#)
- [区块链技术（2）-区块链技术细节：哈希算法](#)
- [区块链技术（3）-区块链技术细节：加密和挖矿](#)
- [区块链技术（4）-去中心化的共识机制](#)
- [区块链技术（5）-智能合约](#)
- [区块链技术（6）-传统金融和虚拟货币](#)



宇宙全栈	2018-04-18
这篇文章太赞了，建议加到免费试读中，让更多的人看到	
JasonHu	2018-04-19
说实话随着我在跟深入的研究也发现你说的问题，只是没有你怎么清晰，佩服耗子哥的能马上看到事物本质的能力	
neohope	2018-06-22
试着回答一下最后几个问题：	
1、很多币都是在炒概念，发空气币，泡沫挺大的，有能力驾驭的团队少之又少。但一些运营较好的团队由于盈利很多，所以也能开始雇到一些有水平的人。	
2、现在好多人都用社会学心理学去研究比特币了。比特币本身没有做太多的颠覆，但它选了一个最容易成功的点进行实验并取得了一定成功，并且其带来了区块链2.0，区块链3.0的繁荣。我感觉颠覆在2.0之后。	
3、从来没有消除中间商。比如交易所，比如矿工，只是形式变了而已。但匿名性好了一些。但数据隐私性下降了。	
4、大公司做链，其实一般不发币，主要用于结算或交易确认。而他们用的都是联盟链，不是公链，就是你进来要我给你发牌照噢，所以反而不造成威胁，同样是中心化的。	
5、VC在市圈不太吃的开，一般是基金会，而大家说白了都是在走快速套现的套路，就是为了赚钱噢。国内好项目被BAT干掉了一大半，没有好项目投，又不能投地严，咋办？总要有个出口。和某些共享单车公司一样，把量做上来，转手一卖赚一笔，思路没什么区别。	
6、这个就和黄金一样，大家承认他的稀缺性，就有价值。如果只有一个人认为黄金有价值，那金山都没用。所以，一定要大家都进来，才会升值噢。	
咋说呢，我也是个旁观者，有些观点不太一致的地方，按我理解链圈和市圈还是有些差别的。另外，比特币和政府发行的电子货币，赌球和足彩；非法集资和股市；区别在哪里？背书的人不一样噢。	
作者回复	2018-06-26
◆◆	
露了个油	2018-04-17
耗子叔，以太坊的智能合约是否有它的价值呀？我觉得这个场景还挺有意思的	
50in5days	2018-04-17
请教个问题区块链校验不是只和上个区块有关 为什么链长会影响效率？	
光光	2018-07-13
我理解区块链要全民都能参与才有前途，我们是不是能通过某种方式限制大机构的参与，来保证都是个人用户参与到区块链中呀？	
SoWhat	2018-06-27
这篇文章真的太好了，值	
吴常亮	2018-06-20
这篇文章写的思考太好了，比单纯从技术角度看区块链更引发思考	
王宏华	2018-06-13
mises.org上有一个比特币的经济学基础课程，耗子哥欢迎看看，主讲博士之一是遗忘私钥丢了十几个币.只说关于自由市场,您这篇文章的理解是错误的.自由市场不是说没有犯罪.而是保护自己的方式全靠你自己或者你选择的机构，而不是一个强制性的组织。	
Watts	2018-06-02
钢不是纯铁，区块链项目就要绝对去中心化吗？但不是绝对的铁也不能叫铁。	
奔跑的蜗牛	2018-05-11
文章犀利透彻，佩服佩服	
Juguya	2018-04-19

耗子叔知识面好广	
极客时间测试账号	2018-04-18
学习了	
DaiNiu	
不能成为货币，依靠稀缺性是否能成为数字黄金成为避险资产呢？反正大家都认就行，我觉得这也是一种隐蔽的行贿受贿手段！	2018-04-17



