

## 第24讲 | 比特币专题（一）历史与货币

2018-05-18 陈浩

深入浅出区块链

[进入课程 >](#)



讲述：黄洲君

时长 10:40 大小 6.12M



我们终于到了“信仰”篇。“信仰”这个词是我经常在公司调侃新员工，问他们有没有为“信仰”充值，这里的信仰指代的就是比特币。

比特币相关的技术前面一个专题已经介绍过了，再深入挖掘就是隔离见证和扩容之争了，我们今天重点介绍比特币本身的来龙去脉，感受一下这个世界的变化之大。

### 比特币的逆袭史

俗话说读史明智，我们就从比特币的历史开始聊起。比特币的历史总结起来大约有四个时期：创立前期、创立期、成长和稳定期。

#### 创立前期

在比特币创立之前，世界上已有多种类似技术产品，最早的是 Ecash 协议，接着 Ecash 又有多种数字货币产品出现，其中以亚当·贝克的“Hashcash”和戴维 (Wei Dai) 的“B-money”、尼克·萨博的“Bit-gold”，以及哈尔·芬尼在“Hashcash”技术上发展出来的“RPOW”等技术产品。

## 创立期

2008 年 11 月，中本聪发表了比特币的白皮书《比特币：一种点对点的电子现金系统》，接下来的时间中本聪实现了他所描述的比特币系统。


2009 年 1 月 3 日，比特币网络正式开始运行。中本聪在创始区块中写道“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”。这句话有两层意义，第一层意思是表示了中本聪没有预先挖矿，毕竟这是当天泰晤士报的新闻，中本聪显然不可能预先获知泰晤士报将要报道些什么。通常对这句话第二层意思的解读是：认为中本聪嘲讽了当下的中心化银行体系。

2009 年 1 月 9 日，Bitcoin v0.1 版本发布，12 日中本聪进行了第一次交易，这一次交易中，中本聪给海尔发送了 10 个比特币。

2009 年秋天，一个叫“新自由标准”的用户通过 Paypal 支付了 5.02 美元，购买了 5050 个比特币，折合 0.000994 美元一个比特币，这是比特币和法币的第一次兑换。

□2009 年到 2010 年初，已经有一些其他的开发者被逐渐吸引过来，大家一起开发、维护、挖矿，那时候普通电脑还可以挖到比特币。

2010 年 4 月，一个叫拉斯诺的人发现可以使用 GPU 来挖比特币，5 月 22 日，他用挖到的比特币购买了两个比萨，共花费 10000BTC，这是比特币第一次被用于实物支付，也就是著名的比特币披萨事件。


 Author

Topic: Pizza for bitcoins? (Read 776199 times)

laszlo


Full Member

Activity: 199  
Merit: 242



**Pizza for bitcoins?**

May 18, 2010, 12:35:20 AM

 Merited by Seccour (50), alani123 (12), Ognasty (10), the\_poet (10), mnightwaffle (10), arthurbonora (10), d5000 (5), Betwrong (5), malevolent (1), EFS (1), vapourminer (1), iluvbitcoins (1), HI-TEC99 (1), jacktheking (1), LoyceV (1), bitart (1), Astargath (1), coolcoinz (1), apoorvathey (1), Kda2018 (1), Financisto (1), TheQuin (1), Toxic2040 (1), amishmanish (1), Toughit (1), nullius (1), alia (1), inkling (1)

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,  
Laszlo

BC: 157fRrqAKrDyGHR1Bx3yDxeMv8Rh45aUet

2010 年 7 月，世界上第一家比特币交易所在日本东京成立，名叫 Mt.Gox，中文“门头沟”。



## 成长期和稳定期

2014 年 2 月，发生“门头沟事件”，门头沟交易所被黑一事震惊全球，比特币价格应声跳水；

2014 年 6 月，以太坊开始了为期 42 天的 ICO，众筹使用的是 BTC；

2017 年 11 月 28 日，比特币价格超过一万美元。

最后附一份由维基百科归纳的比特币价格变化以及对应的事件。

比特币兑美元价格历史		
日期	BTC: USD	备注
2010年	初始 400 : 1	在比特币论坛“bitcointalk”上，用户群自发交易中，产生了第一个比特币公允汇率。该交易是一名用户发送10,000比特币，购买了一块价值25美元的披萨饼。 <sup>[27][28]</sup> 比特币公开交易开始时，其汇率主要参考Mtgox交易所内比特币与美元的成交汇率。 <sup>[29]</sup>
2011年	最低 100 : 1	为了打破全球权威集团的金融封锁， <a href="#">维基解密</a> 刚宣布接受比特币捐助，全球最大的交易网站Mt. Gox就被黑客攻击，当时比特币价格迅速降到0.01\$/BTC。 <sup>[30]</sup>
2012年	最高 1 : 33	2012年11月以前，比特币的最高汇率为33美元。在2012年8月，比特币的汇率为10美元左右。11月底，比特币的汇率为12.5美元左右。
2013年	最高 1 : 1200	3月30日，全部发行比特币按市价换算为美元后，总值突破为10亿美元。 <sup>[31][32][33]</sup> 对美元的初始汇率2月开始，比特币的汇率由2月的20美元急升至4月的180美元，据此按照已经产生的比特币总数来计算，比特币的总市值约为20亿美元。 <sup>[34]</sup> 5月30日，Facebook前高管Chamath Palihapitiya在彭博社发表文章预期，比特币将在10年内升值3,000倍。 <sup>[35]</sup> 11月28日，比特币成交价首次突破1000美元。 <sup>[36]</sup> 12月1日，比特币涨521%，价格首次超越1盎司黄金价格。 <sup>[37]</sup>
2014年	1 : 750-1000	2014年中旬，比特币汇率又一次因为比特币交易所Mt. Gox遭到黑客袭击急剧波动。原因是他们忽略了2013年2月19日更安全可靠的比特币0.8.0系统发行，没有及时更新自己的2011年操作系统，为黑客带来可乘之机。 <sup>[38]</sup>
2017年	最高约1 : 20000	2017年5月4日，比特币价值首次突破1500美元，市值达250亿美元以上，近期成交量大增，日本 bitFlyer 比特币交易所的成交量比例为52.35%。11~12月初更大幅度上涨至近两万美金

从上图可以看出，比特币的成长史就是对美元的逆袭史，比特币的发展经历了很多争议和阻碍，但是依然不妨碍它成为一种世界级现象，甚至是很多人的信仰，那么比特币的意义到哪在那里呢？

## 比特币的意义

这个话题可能会引起一些争论，我姑且将本节的内容限定为“我”所理解的比特币，仅供你参考。

首先比特币没有通常意义上的实用价值，不单单是比特币，所有的信用货币，包括黄金白银在内都不具备实用价值。

这里的实用价值是指解决人的低层次需求，如果按照马斯洛需求层次理论来分，是指衣食住行等生存需求。

换句话说，比特币也好，黄金也好，在生活面前都是废物，而无法直接利用，毕竟黄金吃下去也不能饱还有生命危险，比特币的私钥即使看得见却也摸不到。

但是用货币就是能买东西，买来的东西可以帮你解决□生存需求，说白了吃饱了才能干其他事情。“买”这个动作就是比特币所要解决的，当然信用货币也能解决，也就是我们所说的支付功能。

所以作为信用货币的比较，比特币到底有什么不同？它的意义超过信用货币吗？我个人认为是超过的。老生常谈的去中心化、防篡改我这里就不谈了，我们接下来换几个角度来聊聊它。

## 1. 无国界的共识

它打破了一般信用货币的局限性，我称作无国界的共识。

比较常见的论调，比特币你信它就有价值，不信就什么用途也没有。这里隐含的语义是“承认过程”。

例如你在美国吃顿饭，使用人民币支付，美国人一定不是特别同意，毕竟在美国就必须使用美元支付。换句话说，“承认过程”很大程度上是身不由己，你所处的国家决定了必须承认某种信用货币。

比特币奇怪就奇怪在，没有人会强迫你使用比特币，你的一念之间就可以决定比特币对于你的价值。

如果类比到黄金，比如你长这么大，□一直都是别人告诉你黄金非常值钱，所以你也觉得黄金值钱，这其实就是共识灌输的过程，当然你也可以公开表示“我觉得黄金不值钱”，这当然也没什么问题。

想象一下，如果全世界都能达成比特币都可以用于支付的共识，比特币和黄金在共识的效果上也没什么不同了，那么声称“我觉得黄金不值钱”就变成了“我觉得比特币不值钱”，这里的逻辑是一样的。

## 2. 记账是本职

比特币的本职是记账，不要想得太复杂，它就是来帮你记账的。例如你在宜家买了一套家具，比特币可以帮你记下来，当然不是说这个事件，而是帮你记录价值转移，你动用了你曾经创造的价值多少（BTC）来购买这套家具。

这个记账过程防篡改能力非常强，几乎没人能操控，也没有国界之分，只要你的交易方承认比特币，这笔买卖就可以达成。

### 3. 高效的资源调度

比特币使用的是 PoW 算法，这个需要消耗大量能源进行挖矿的算法一直被人诟病；但是结合上述记账本职，我们也换个角度来看这件事。

目前全国的电力分配不均，中国的内蒙东北有着丰富的风力电，可惜这些富余的电力难以调度，超高压输电线路造价高昂，甚至超出了电厂本身。

而比特币挖矿恰好需要极大地耗费能源，如果在偏远的资源丰富地区进行挖矿，相当于将架设超高压输电线路蜕化为网络通信设施，地方政府可以把庞大的风电资源转化成比特币，最多只需要十分钟，就可以在资本市场变现。所以每个人每次使用比特币的过程，相当于让偏远地区获得了平等参与社会运作的过程。

### 4. 三权分立的社区自治形态

这里讨论的三权分立的形态，并不是指政府组织结构的形式，而是指矿工、开发者、投资者三者组成了相互制衡的数字货币的治理形态。

比特币并没有真正意义上完全地去中心化，在记账权上，它目前被 5 大矿池所把持。当人们抨击 EOS 的 21 个节点有中心化的嫌疑时，BM 总是拿出比特币矿池的例子来反击。

实际上这里偷换了概念，比特币中矿工的权力其实是有限的。

技术限制：由于 PoW 的特性，矿工无法进行长程攻击（Long Range Attack），篡改和分叉的边际成本随着篡改的区块数量线性攀升，所以看似矿工的 51% 攻击，也就改一两个块而已。

开发者制衡：扩容之争是很好的例子，我们下一篇会详细介绍，矿工是逐利的，而开发者决定了比特币的长期发展，所以从某种意义上来说，作弊不如和开发者合作。

投资者制衡：矿工是比特币的直接利益相关者，无论是社区分歧还是主链分叉，矿工首先确保的是收益稳定，黑天鹅事件造成的巨大价格波动是不利于收益预期的。

总结起来就是，虽然比特币在记账权上没有彻底去中心化，但是目前的情况也可以接受，至少矿工还受两方制约，矿工看收益，收益的价格看投资者，投资者看比特币长期发展，比特

币长期发展看开发者，开发者受制于矿工，三者相互制衡。

## BIP 及其发展

比特币 BIP (Bitcoin Improvement Proposals) 是一种设计文档，用来描述比特币新特性的提案，第一个比特币 BIP 是 2011 年 8 月 19 号一个名为 Amir Taaki 的人提交的，编号 bip001，它描述了 BIP 本身是什么。

随后几年直到现在，比特币的 BIP 编号将近 200 个，它展示了比特币强大的社区协作能力。

很多人认为某个区块链项目一旦上线这个链就稳了，实际上，做公链好比一场没有尽头的马拉松长跑，主网上线表示长跑开始，接下来才是真正拼实力的时候。

具体怎么拼？则要看 IP (Improvement Proposal)。可以说 IP 代表了一个区块链项目的生命力。□例如 HD 账户是 bip32 和 bip39 提出的，最开始的比特币是没有这个功能的，隔离见证也是由一系列 bip 组成的。

我们再比如说，就算是你想修改比特币的 2100 万上限也是可以的，只要你提的 BIP 详细论证了改上限的必要性以及充分验证了达成条件，如果最终社区同意了你的提案，2100 万上限改成 3000 万个也不是梦，一切都是可以操作的。

这就回到了社区自治的特性上了，你承认并持有比特币，那么你就可以参与决策比特币的发展。

## 总结

好了，今天我们简要回顾了比特币的历史和货币形态，最后还介绍了 BIP，为下一篇介绍扩容之争做准备。

其实比特币作为整个数字货币的标杆和领头，对区块链生态和未来有不可忽视的力量。虽然现在号称区块链 2.0、区块链 3.0 的项目很多，但是真正意义上达到了工业级水准的，还是只有比特币。

无独有偶，我有一次在外面帮投资机构评估一个区块链项目，我也提到了信仰，□项目方不约而同地表示持有，不过，他们的信仰是以太坊，所以今天的问题是，你觉得以太坊以后会

取代比特币的地位吗？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。

参考链接：

1. <https://zh.wikipedia.org/wiki/%E6%AF%94%E7%89%B9%E5%B9%A3%E6%AD%B7%E5%8F%B2>
2. <http://www.btcshuo.com/portal.php?mod=view&aid=339>
3. <https://bitcointalk.org/index.php?topic=137.0>

 极客时间

# 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23讲 | 联盟链和它的困境

下一篇 第25讲 | 比特币专题（二）：扩容之争、IFO与链上治理

精选留言 (9)

 写留言



ytl  
2018-05-18



风力发电和光伏发电等新能源发电，波动性较大，对电网冲击高，输电成本高。如果在分布式发电地把电力用于挖矿，价值瞬间转移出去。



夏天的雨云

2018-10-31



关于比特币的价值问题，我依然有些不太理解，有些人比较早参与挖矿或者直接购买，那时的成本几乎可以忽略不计，到了这两年，比特币的价值上天了，早期的人因此获得巨大的收益，但这也不见得就一定是合理的吧？似乎并没有创造什么价值或者对社会有什么贡献？可能我的理解太肤浅，见笑了。😄



zjhiphop

2018-05-19



比特币和以太坊本身定位不一样，比特币是更多是作为货币的形式存在的，以太坊是为了解决交易和价值转移而实现的。

本身没有超越之说，但是我更看好EOS的未来，如果说以太坊是价值转移的CPU，那么EOS则是价值转移的操作系统

展开 ∨

作者回复: EOS的中心化问题为人们所诟病，具体运营情况我们还需拭目以待。



夏天的雨云

2018-10-31



请教一个问题，比特币主网上线之初，中本聪本人是否为自己预留了一定数量的比特币？看你的文章介绍应该没有，但之前听说他为自己预留了很多，误传？

展开 ∨



Rain

2018-07-12



文章举了一个「修改 2100万上限，需要社区同意」的例子，具体「社区同意」是怎么执行的？谁来做决定？毕竟社区也是由人组成的，这里不太明白。





李锦

2018-05-21



以太坊的价值以及能力很可能超越比特，目前 eos 以及 neo 都无法与以太竞争。

就以太而已言，苹果创始人沃兹对以太的评价已经值了。



lily

2018-05-19



数字货币是历史发展的必然趋势！但虚拟资产则寿命有限，流通产生价值，分配需要共识！



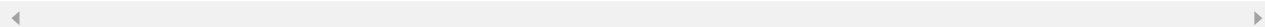
有风的林子

2018-05-19



一个定位电子现金，一个是智能合约平台。各有擅长侧重，可能不存在替代的关系吧

作者回复: 两者方向有融合的趋势哦。至少比特币和以太币都是硬通货



ytl

2018-05-18



以太坊不可能取代比特币，但青出于蓝胜于蓝，以太坊对智能合约贡献巨大。但性能问题让以太坊很难再突破，江山代有才人出。

人们认识区块链基本从比特币开始，比特币有教科书意义，积累了最多人的信心，目前最成熟的工业级区块链应用，在未来可能成为数字黄金。以太坊取代不了这样的历史地位。

展开 ∨