# BiTCOin Legend 比特币传奇

荆涛◎著

回归交易的本质，造就另外一个传奇。
比特币，拉开了数字经济时代的大幕。

煤炭工业出版社

# BiTCoin Legend 比特币传奇

荆涛◎著

煤炭工业出版社
·北　京·

**图书在版编目（CIP）数据**

比特币传奇／荆涛著．--北京：煤炭工业出版社，2019

ISBN 978-7-5020-7119-6

Ⅰ.①比… Ⅱ.①荆… Ⅲ.①电子货币—研究 Ⅳ.①F830.46

中国版本图书馆 CIP 数据核字（2018）第 291483 号

**比特币传奇**

**著　　者**　荆　涛
**责任编辑**　高红勤
**封面设计**　胡椒书衣

**出版发行**　煤炭工业出版社（北京市朝阳区芍药居 35 号　100029）
**电　　话**　010-84657898（总编室）　010-84657880（读者服务部）
**网　　址**　www.cciph.com.cn
**印　　刷**　华睿林（天津）印刷有限公司
**经　　销**　全国新华书店

**开　　本**　710mm×1000mm 1/16　**印张**　16　**字数**　210 千字
**版　　次**　2019 年 3 月第 1 版　2019 年 3 月第 1 次印刷
**社内编号**　20181753　　**定价**　48.00 元

# 前 言

比特币，目前火得发烫的一个“名词”，它从一文不值到身价过万用了不到十年的时间。有人把比特币比喻成“变态”币，一路带着节奏、高歌猛进的比特币确实像一个处于“野蛮成长期”的年轻人那样，充满着无限活力。甚至有人畅想：有朝一日，比特币将取代美元，成为一种世界性的法定货币。俗话说：“一千个人的眼里就有一千个哈姆雷特。”事实上，比特币从诞生之日起，就成了热议焦点屡登头条，这也让那些苦苦想要上头条博眼球的人“羡慕嫉妒恨”！

比特币为何这么受关注？真的是因为它奇货可居吗？一位比特币的投资者是这么认为的：“全世界只有2100万枚，难道这还不算稀缺资产吗？如果比特币数量可以无限复制，那一定是不值钱的！”我们知道这样一个价值定律：稀缺数量决定价值大小。黄金、白银等贵金属之所以值钱，就是因为其资源有限。历史上出现的“金本位”体系就是以黄金为本位的经济体系，为此地球上还爆发过大面积的“黄金争夺战”！如果以数量进行衡量，比特币似乎比黄金还要贵重。

有人说比特币是一种宝贵资源，甚至是一种不可再生的资源；也有人说比特币完全是炒作出来的产物，是一个惊天骗局。举个例子：按照一定的计算方式，通过消耗“算力”，我们就可以得到比特币；如果按照其他计算方式并消耗算力，我们也可以得到其他类别的数字货币，比如莱特币、狗狗币、龙币等，以此类推，比特币似乎是完全不值钱的！比特币的“价值属性”，似乎又完全符合庞氏诈骗逻辑。比特币是人还是鬼，到现在为止还没有一个正确结论。

不管如何，比特币是一个新事物。面对一个新事物，我们似乎不应该用一种过于严厉的态度去对待它，许多人更喜欢用一种发展的眼光去对待它。比特币从出生到现在也仅仅只有十年时间，十年对于人类历史而言仅仅只是一个“标点”符号而已。或者说，比特币是一种“价值思考方式”，获取它的目的并不是让它变得“值钱”，而是为了审视、衡量人们的价值观、世界观。

货币，不仅仅只是一种等价符号，它还要承担起更多的社会责任。如果有人愿意接受比特币作为“货币”进行商业交易行为，为何我们还要制止呢？还有一些人开始呼吁：“我们需要‘去中心化’的货币，但是不需要比特币。”这样的呼吁，是一种对政府的喊话。众所周知，比特币是一款“区块链产品”。区块链技术是一项非常先进的技术，甚至具有颠覆性意义。如果政府依靠区块链技术开发具备法币效力的数字货币，是否会带来划时代的意义呢？

圣雄甘地有一句话：“一开始他们忽略你，然后他们嘲笑你，接着他们攻击你，最后你获胜。”如今，比特币还不能用“夹缝中求生存”来形容，至少它的身后还有一群狂热的粉丝为它摇旗呐喊！因此，也请广大读者或者对比特币感兴趣的朋友跟着我一起走进《比特币传奇》。

荆涛

2018 年 9 月

# 目 录

# 第一章

# 数字货币的起源

## 1. 从原始货币到数字货币

人类文明的标志，大概就是从原始社会的“原始交易”开始的。原始社会，什么东西都是原始的，风餐露宿、茹毛饮血，生产工具也是非常简单。真是应了相声段子里的一句话：“用我手里的蒜换你手里的葱，用我手上的布换你手里的肉。”原始社会是以物易物的社会，根本没有货币这种东西。

后来原始人认为“以物易物”太麻烦了，如果用一头牛肉换一把菜刀，不仅牛的个头太大，难以挪动，而且还存在一定的风险。因此，一种贝壳类的原始货币出现了。《尚书·盘庚中》记载：“贝者，水虫，古人取其甲以

为货，如今之用钱然。”贝壳币，就是一种原始货币，我们也可以把它称为“自然货币”。这种货币五贝为一串，两串为一朋。由于贝壳币产自海洋，在当时的社会数量甚为稀少，因此贝壳币非常值钱。由于贝壳币的数量实在是太少了，后来一些“代贝壳币”也纷纷出现，比如骨币、石币等。

随着社会的发展以及人类文明的进步，另外一种货币出现了，这种货币叫“金属货币”！如今，金属货币依旧存在，比如人们使用的“钢镚儿”就是一种金属货币。奴隶社会时期，人们就已经掌握了“冶金术”，同时也把金属当成一种非常宝贵的资源。

人们都知道，在信用货币出现之前，货币就是“钱”，是一种价值衡量单位，它本身也要具备一定的价值。金属作为一种“稀缺品”，自然也就成为铸币的最佳原材料。金属化学性能稳定、易于分割和保存，用金属铸造的货币一经上市就引起了强烈的社会反响。司马迁在《史记·平淮书》中写道：“农工商交易之路通，而龟贝金钱刀布之币兴焉。所从来久远……虞夏之币，金为三品，或黄或白或赤或钱或布或刀或龟贝。”这段话的意思说，虞舜王朝和夏朝的时候，自然货币和金属货币已经同时存在了。但是随着时间的推移和冶金术的提升，金属货币逐渐代替了原始货币，人类也由此进入了金属货币时代。

古往今来，金属货币通常有四种材质：金、银、铜、铁。其中金和银为贵金属，铜和铁为贱金属。我们最为熟知的“铜钱”，就是一种币值较低的金属货币，比“铜钱”值钱的还有银锭和金元宝。封建社会时期，穷人家庭主要用铜钱，银锭、金元宝则属于上流社会。因此有人说：“金属货币带有一种阶级属性。”虽然金属货币凭借其良好的物理特性和“手感”主导货币史几千年，但是另外一种货币也开始跃跃欲试了，这种货币就是“纸币”！

北宋时期，一种名为“交子”的东西出现了。其实“交子”就是一种纸币，这种纸币最早出现在四川，是一些不便携带巨款的商人为了交易之便而印制的一种“价值凭据”。商人们用“交子”进行交易，等同于背着一麻袋铜钱进行交易。商人们用铜钱换取“交子”的柜房被称为“交子铺”，“交子铺”也就是我们现在所说的银行。由于历史原因，“交子”并未得到大范围的推广，“交子”不稳定的化学属性决定其无法撼动金属货币的地位。

1661年，欧洲大陆也开始出现纸币。瑞典银行最初发行的纸币并无“价值”，因为发行数量巨大，这种纸币并不能兑换相应价值的金属货币或者购买相同价值的物资。换句话说，这种纸币更像是一种花纸头。直到1694年，英格兰银行发行的“银单”才具有实际意义上的货币价值。后来纸币不再手写，而改成印版印刷，逐渐有了现代纸币的影子。如今世界上有200多种纸币，流通于190多个国家和地区。

有人说：“时代是不断进步的，任何一种事物都有可能卷进历史的洪流，被另外一种事物所代替。”随着互联网时代的到来，货币又有了新的变化。

首先，电子货币出现了。什么是电子货币呢？严格来讲，电子货币并不是一种货币，它只是一种技术，或者是一种电子化的转账工具。人们通过扫二维码，可以将自己银行卡里的现金转移到商家的银行卡或者现金账户上。这种货币是无形的，它只是以一种符号的形式存在。与这种“电子货币”不同的是，游戏币也是一种电子货币，比如Q币。人们可以用现金账户购买价值相同的Q币，实现腾讯公司所属业务或服务的购买需求。从某个角度上讲，Q币也具备价值交换功能，只不过Q币的流通范围仅限于腾讯公司相关的业务。

随后，数字货币也出现了。数字货币与电子货币完全不同，它是借助特定的算法，通过算力获得的。这种货币不依赖于政府信用体系，完全是一种

基于互联网P2P技术的去中心化的货币。这种货币，人人都可以挖掘，人人皆可创造。著名的比特币就是一种数字货币，它已经成为当今最吸引眼球的一种货币符号。

数字货币不仅仅只是一种概念，而是被人们手把手地创造出来的新型货币形式。也许，数字货币还暂时无法取代其他法定货币，但是它的出现已经潜移默化地改变了人们的思维，进一步推动了数字货币的发展。或许未来有一天，数字货币也会成为一种广泛流通的法定货币。

## 2. 数字货币的原理

我们常常思考：一只鸡是如何诞生的？是先有的鸡蛋，还是先有的鸡？世界上的人也因此分成了两派，并为此争论不休。货币又是怎么诞生的？当我们思考这个问题时，自然会联想到人类的文明社会。这个问题是有根可循的，它完全不同于“先有鸡蛋还是先有鸡”这种需要诡辩的问题。货币的发展，是人类文明史的发展。比如，金属货币标志着人们对金属冶炼技术的掌握和铸币技术的发展，金属货币越来越“精美”，以至于它变成了一件“艺术品”。依赖于铸造技术和人类文明的发展，更加先进、安全的货币也会登

上人类世界的舞台。数字货币，就像一个戴着神秘面纱的“乘客”，它出现在人类世界，引发人们对它的好奇。事实上，数字货币与鸡蛋和鸡一样，它并不是凭空产生的，它是伟大的人类基于互联网技术和区块链应用而设计出来的。数字货币是一件应景之作，它依旧延续了货币在人类社会中的存在价值。

数字货币代表着一种技术，它有着神秘的制作原理。众所周知，数字货币不同于任何一种货币，它没有重量，没有体积，没有质地，甚至完全是“虚无”的，肉眼看不到的。它仅仅存在于虚拟空间里，是一种没有“货币”自然属性的“货币符号”。而它的的确确是一个符号，由一堆代码组成，看上去就像某种“电脑纹身”……数字货币的原理到底是什么呢？

首先，我们不得不提“P2P”这个概念。什么是P2P呢？P2P即“Person-to-person或“peer-to-peer”，是一种对等计算机网络。在P2P中，共享性、对定性、无中介性似乎成为它的最大特点。人们对P2P的具体定义是这样的：“人们在网上共享他们的一部分硬件资源，这些资源可以通过互联网提供有价值的信息，这些信息都可以被另外一个对应节点上的用户直接访问并使用，且不需要‘中间商’提供访问服务。”我们可以把P2P看成一个没有支点的天平，天平两端的节点是平等的，没有主次之分，也无阶级之别。因此P2P中的任何一个节点，既是资源的参与者和分享者，又是资源、内容的获取者。任何一个节点都具有功能、职责的“交互性”和“对等性”，因此P2P技术让交易变得更加简单、直接，完全消除了“中间商赚差价”这一现象，并且把权利交还给了用户。

数字货币是一种P2P形式的货币，它不依赖于“铸币机构”，甚至不需要信用价值机构赋予“法定”价值，它是依照某种“算法”而产生的，是一种“去中心化”的货币形式。当然，许多人并不承认数字货币是一种“货

币”，它更像是一种“等价交易”形式，但是这种“等价交易”形式不也是法定货币的属性吗？只不过它并未被广泛认知，而“技术”等方面的限制令数字货币的发展仍旧处于一种被观望的阶段。

其次，我们还要提到“Ledger”这个词。“Ledger”是账本的意思，也就是数字货币的钱包。只不过这个钱包与装现金的钱包不同，它是虚拟的。数字货币的总账本被托管在分散在世界各个角落、并运行着数字货币软件的服务器里。这些分散在世界各地的服务器可以看作一个“节点”，无数个“节点”就会形成一张数字货币网。因此，数字货币的“Ledger”是广泛分布于世界里的，就像繁星之于宇宙般神奇！而这些数字货币服务器同步和验证总账的机制，我们称为“共识”。举个例子，一个人想要发起一笔交易，将一笔钱转给另外一个节点上的朋友。在发起“交易”的同时，一组被信任的服务器对该“交易行为”进行核实，并确定该交易是否有效。在另外一端，也就是收款一方，则需要准备具有相同价值的物品，即等价物。当这个“等价物”也被核实有效后，这笔交易才能被通过，并最终实现交易。或许有人抱着脑袋纠结：“这么麻烦的交易过程，岂能比得上一手交钱一手交货？”这样的纠结完全是没有必要的，因为基于P2P技术的数字货币在交易过程中可以瞬间完成，尤其在两个节点“跨距”非常大的情况下，即使一个北京人向太平洋对面的洛杉矶人发起交易，也会瞬间完成。数字货币技术是非常先进的，甚至可以用“颠覆”二字来形容。

数字货币的技术原理说简单也简单，说复杂也十分复杂，它的出现是令世人值得庆祝的。未来数字货币或许存有很多不确定的“可能”，这些“可能”也是我们保持关注的重要原因。