

大家好，今天小编来为大家解答比特币争论这个问题，比特币争议很多人还不知道，现在让我们一起来看看吧！

本文目录

- [1. 如果靠卖比特币赚了十亿，那这笔钱我可以顺利提现到个人账户吗？](#)
- [2. 比特币、数字虚拟货币究竟创造了什么价值，疯狂背后是是什么？](#)
- [3. 比特币谁发明的？](#)
- [4. 如何看待比特币Segwit2x硬分叉？](#)

如果靠卖比特币赚了十亿，那这笔钱我可以顺利提现到个人账户吗？

交易所卖掉换usdt、usdc、pax稳定币倒是简单，挂币安估计一两个小时肯定卖掉了，难点在于USDT等换成人民币，主要是套现这么多，一定会触发银行风控，然后就会打麻烦，一旦银行为了保险起见严格执行五部委文件，你就得把钱提走换个银行，就算这样可以，一次500万500万卖，也要卖好久。

而且卖的时候币价还会跌。

另外一种方法是场外交易，专业的场外交易团队，千八百个比特币出掉是不难的，毕竟现在圈子也大了，同行都有联系，大单子吃不下大家分一分就行了。

但是资金汇聚到银行卡上，还是会触发银行风控，法律方面没风险，就是打麻烦，银行会追问你的资金来源，需要提供材料，然后还是有可能触发执行五部委文件精神。

要我说，你还是留着一半卖一半，卖出来的换成usdc（合规稳定币），需要钱的时候就场外交易卖点出来，隔几个月卖三五十万百八十万，那问题就不大了，至于美元贬值就贬值吧，怕贬值BTC就别卖，零利率总比负利率强。

比特币、数字虚拟货币究竟创造了什么价值，疯狂背后是是什么？

银行记账方法存在巨大的不合理性

最常见的模型：贷款修路，收费还款（示意图如下）。

假设政府贷款1万亿建设高速公路，公众（修路企业和员工）合计获得1万亿收入

。

建成后（收费还款），政府分20年连本带息付给银行，每年要收取约1000+亿过路费。10年时间，公众赚取的劳动收入全部被银行收回，但政府（公众代表）依然欠银行5000多亿贷款。公众要继续还款只能贷款还贷款。当然很多人说实际市场很复杂，但当你就揪住一点，你会发现这个账早晚会严重不平衡。即除了银行之外，所有市场参与单元（政府、企业、个人）都欠一屁股债。要让账目保持平衡唯有订单增速始终保持在5%（比银行贷款利息增速快）以上，但实际订单增速不可能永远保持5%以上的增速。

比特币等于给我们提供了一个全新的记账思路。

公众打1万亿数字白条（编码），给政府纳税。政府直接以公众的白条支付高速公路建设款。按照这种方式，高速公路建成，并不会形成1万亿负债（本息合计要还2万亿），没有负债，自然就不需要收费还款。不需要收费还款，公众因为修路获得的劳动收入就不会被债务吞噬掉。同理，高铁、电力、石油、煤炭.....都是这种逻辑。公众以白条直接授信政府，在以劳动赚回自己发行的白条，建成无需要收费还贷的基础设施。对政府和公众都是重大利好。而对银行而言则是被去掉（传统中介）。

数据，所有市场参与单元负债，我们到底欠谁钱？中央政府：财政部数据显示，截至三季度末中央政府债务余额报12.8932万亿元人民币。地方政府：截至2017年12月末，全国地方政府债务余额164706亿元，控制在全国人大批准的限额之内。其中，一般债务103322亿元，专项债务61384亿元；政府债券147448亿元，非政府债券形式存量政府债务17258亿元[③]。中国制造/国企：财政部12月22日发布的最新数据：截止11月末，国有企业负债总额首次突破百万亿关口，达到100.08万亿元。而2016年全年的负债总额为870377.3亿元。地产商：中国前首富王健林负债4000+亿，并疯狂甩卖资产还债事件，已经清晰表明地产商光鲜资产背后是巨额负债。居民：然而截至2017年5月，央行公布的境内居民住户存款总额为62.6万亿。境内居民人民币贷款已经从2010年的8.8万亿飙升到现在的36.4万亿元。把境内居民的人民币存款减去住户的贷款后发现，中国人手里已经没有大量存款了，全国居民净存款仅剩26万亿！人均不足2万。

看似很合理的资产负债平衡表记账方式。当它把所有市场参与单元变成了债务人（穷鬼）。他的合理性真的还那么充分吗？实际美国这个问题更加严重（感兴趣自己查，美国人、美国政府理论上已经破产），因为美国市场经济存续时间比我们更长。一个把世界上具有最强创新能力，最强军事能力，最好教育体系，最佳民主体系的世界一哥搞成破产国家的记账方式，它的合理性还那么充分吗？

引发大家从仰视到平视，再到鄙视银行系统，就是比特币的价值所在。至于比特币和其他数字货币被传统诋毁，被各国政府如过街老鼠般碾压，只能说传统思维还十

分彪悍，就如同文艺复兴之中的宗教势力，吓得哥白尼快死了，才敢拿出《日心说》，委托朋友发表！如果你打算拍砖，请先回答上面的问题，都是债务人，到底我们欠谁钱？

比特币谁发明的？

比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

比特币可以用来兑现，可以兑换成大多数国家的货币。使用者可以用比特币购买一些虚拟物品，比如网络游戏当中的衣服、帽子、装备等，只要有人接受，也可以使用比特币购买现实生活当中的物品。[1][2]

西维吉尼亚州民主党参议员乔·曼钦（JoeManchin）2014年2月26日向美国联邦政府多个监管部门发出公开信，希望有关机构能够就比特币鼓励非法活动和扰乱金融秩序的现状予以重视，并要求能尽快采取行动，以全面封杀该电子货币。[3]

2017年1月24日中午12：00起，中国三大比特币平台正式开始收取交易费。[4]

中文名

比特币

外文名

Bitcoin

种类

电子货币

流通平台

网络

概念创始人

中本聪

发展历程听语音

2008年爆发全球金融危机，当时有人用“中本聪”的化名发表了一篇论文，描述了比特币的模式。

共2张

比特币

和法定货币相比，比特币没有一个集中的发行方，而是由网络节点的计算生成，谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。[2]2009年，不受央行和任何金融机构控制的比特币诞生。[2]比特币是一种“电子货币”，由计算机生成的一串串复杂代码组成，新比特币通过预设的程序制造，随着比特币总量的增加，新币制造的速度减慢，直到2014年达到2100万个的总量上限，被挖出的比特币总量已经超过1200万个。[2]

每当比特币进入主流媒体的视野时，主流媒体总会请一些主流经济学家分析一下比特币。早先，这些分析总是集中在比特币是不是骗局。而现如今的分析总是集中在比特币能否成为未来的主流货币。而这其中争论的焦点又往往集中在比特币的通缩特性上。[5]

不少比特币玩家是被比特币的不能随意增发所吸引的。和比特币玩家的态度截然相反，经济学家们对比特币2100万固定总量的态度两极分化。[6]

凯恩斯学派的经济学家们认为政府应该积极调控货币总量，用货币政策的松紧来为经济适时的加油或者刹车。因此，他们认为比特币固定总量货币牺牲了可调控性，而且更糟糕的是将不可避免地导致通货紧缩，进而伤害整体经济。奥地利学派经济

学家们的观点却截然相反，他们认为政府对货币的干预越少越好，货币总量的固定导致的通缩并没什么大不了的，甚至是社会进步的标志。

比特币网络通过“挖矿”来生成新的比特币。所谓“挖矿”实质上是用计算机解决一项复杂的数学问题，来保证比特币网络分布式记账系统的一致性。比特币网络会自动调整数学问题的难度，让整个网络约每10分钟得到一个合格答案。随后比特币网络会新生成一定量的比特币作为赏金，奖励获得答案的人。

2009年比特币诞生的时候，每笔赏金是50个比特币。诞生10分钟后，第一批50个比特币生成了，而此时的货币总量就是50。随后比特币就以约每10分钟50个的速度增长。当总量达到1050万时(2100万的50%)，赏金减半为25个。当总量达到1575万(新产出525万，即1050的50%)时，赏金再减半为12.5个。[7]

首先，根据其设计原理，比特币的总量会持续增长，直至100多年后达到2100万的那一天。但比特币货币总量后期增长的速度会非常缓慢。事实上，87.5%的比特币都将在头12年内被“挖”出来。所以从货币总量上看，比特币并不会达到固定量，其货币总量实质上是会不断膨胀的，尽管速度越来越慢。因此看起来比特币似乎是通胀货币才对。

然而判断处于通货紧缩还是膨胀，并不依据货币总量是减少还是增多，而是看整体物价水平是下跌还是上涨。整体物价上升即为通货膨胀，反之则为通货紧缩。长期看来，比特币的发行机制决定了它的货币总量增长速度将远低于社会财富的增长速度。

凯恩斯学派的经济学家们认为，物价持续下跌会让人们倾向于推迟消费，因为同样一块钱明天就能买到更多的东西。消费意愿的降低又进一步导致了需求萎缩、商品滞销，使物价变得更低，步入“通缩螺旋”的恶性循环。同样，通缩货币哪怕不存入银行本身也能升值（购买力越来越强），人们的投资意愿也会升高，社会生产也会陷入低迷。[5]因此比特币是一种具备通缩倾向的货币。比特币经济体中，以比特币定价的商品价格将会持续下跌。[1]

比特币是一种网络虚拟货币，数量有限，但是可以用来套现：可以兑换成大多数国家的货币。你可以使用比特币购买一些虚拟的物品，比如网络游戏当中的衣服、帽子、装备等，只要有人接受，你也可以使用比特币购买现实生活当中的物品。[1][1]

2014年9月9日，美国电商巨头eBay宣布，该公司旗下支付处理子公司Braintree将开始接受比特币支付。该公司已与比特币交易平台Coinbase达成合作，开始接受这种相对较新的支付手段。

虽然eBay市场交易平台和PayPal业务还不接受比特币支付，但旅行房屋租赁社区Airbnb和租车服务Uber等Braintree客户将可开始接受这种虚拟货币。Braintree的主要业务是面向企业提供支付处理软件，该公司在去年被eBay以大约8亿美元的价格收购。

2017年1月22日晚间，火币网、比特币中国与OKCoin币行相继在各自官网发布公告称，为进一步抑制投机，防止价格剧烈波动，各平台将于2017年1月24日中午12:00起开始收取交易服务费，服务费按成交金额的0.2%固定费率收取，且主动成交和被动成交费率一致。[4]5月5日，OKCoin币行网的最新数据显示，比特币的价格刚刚再度刷新历史，截止发稿前最高触及9222点高位。[8]

创始人物听语音

2008年11月1日，一个自称中本聪(Satoshi Nakamoto)的人在一个隐秘的密码学评论组上贴出了一篇研讨陈述，陈述了他对电子货币的新设想——比特币就此面世，比特币的首笔交易完成。比特币用揭露散布总账摆脱了第三方机构的制约，中本聪称之为“区域链”。用户乐于奉献出CPU的运算能力，运转一个特别的软件来做一名“挖矿工”，这会构成一个网络共同来保持“区域链”。这个过程中，他们也会生成新货币。买卖也在这个网络上延伸，运转这个软件的电脑真相破解不可逆暗码难题，这些难题包含好几个买卖数据。第一个处理难题的“矿工”会得到50比特币奖赏，相关买卖区域加入链条。跟着“矿工”数量的添加，每个谜题的艰难程度也随之进步，这使每个买卖区的比特币生产率保持约在10分钟一枚。

京都大学数学教授望月新一

2009年，中本聪设计出了一种数字货币，即比特币，风风火火的比特币市场起了又落，而其创始人“中本聪”的身份一直都是个谜，关于“比特币之父”的传闻牵涉到从美国国家安全局到金融专家，也给比特币罩上了神秘光环。

据外媒报道称，计算机科学家Ted Nelson周日在网络上发布视频称，他已经确定出，比特币的创始人是京都大学数学教授望月新一(Shinichi Mochizuki)。比特币的创始人一直以来使用的都是中本聪(Satoshi Nakamoto)的假名，互联网领域也对其真实身份展开了大量推测。纳尔逊发布视频称，他已确定望月新一就是比特币的真正创始人。[9]

望月新一2013年因为证明ABC猜想而名声大噪。他高中时就读于菲利普埃克塞特学院，后者是美国最具声望的高中之一，仅仅两年后就毕业。望月新一16岁进入美国普林斯顿大学，22岁时以博士身份离校，33岁就成为正教授，这么年轻就获得正教授职称在学术界极为罕见。这个数学界的巨星可能已经攻破了该领域最为重要的

难题之一。

中本聪本人在互联网上留下的个人资料很少，尤其是近几年几乎完全销声匿迹，因此其身世也变成了一个迷。2014年3月7日，当比特币创始人多利安·P·中本聪被找到的新闻传出后，迅速成为互联网上最吸引人的消息。

与外界揣测其可能是个虚构的名字不同，“中本聪”是个真实的名字，他是一名64岁的日裔美国人，他喜欢收集火车模型，曾供职大企业和美国军方，从事机密工作。在过去的40年中，中本聪从不在生活中用他的真名。根据美国洛杉矶地方法院1973年的档案，在他23岁从加州州立理工大学毕业时，将自己的名字改为了多利安·普伦蒂斯·中本聪（Dorian Prentice Satoshi Nakamoto）。从那时起，他不再使用“聪”这个名字，而用多利安·中本S（Dorian S. Nakamoto）作为签名。[9]

产生原理听语音

从比特币的本质说起，比特币的本质其实就是一堆复杂算法所生成的特解。特解是指方程组所能得到无限个（其实比特币是有限个）解中的一组。而每一个特解都能解开方程并且是唯一的。[10]以人民币来比喻的话，比特币就是人民币的序列号，你知道了某张钞票上的序列号，你就拥有了这张钞票。而挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组的特解，这个方程组被设计成了只有2100万个特解，所以比特币的上限就是2100万。[10]

疯狂涨势

要挖掘比特币可以下载专用的比特币运算工具，然后注册各种合作网站，把注册来的用户名和密码填入计算程序中，再点击运算就正式开始。[11]完成Bitcoin客户端安装后，可以直接获得一个Bitcoin地址，当别人付钱的时候，只需要自己把地址贴给别人，就能通过同样的客户端进行付款。在安装好比特币客户端后，它将会分配一个私有密钥和一个公开密钥。需要备份你包含私有密钥的钱包数据，才能保证财产不丢失。如果不幸完全格式化硬盘，个人的比特币将会完全丢失。

货币特征听语音

去中心化：比特币是第一种分布式的虚拟货币，整个网络由用户构成，没有中央银行。去中心化是比特币安全与自由的保证。

全世界流通：比特币可以在任意一台接入互联网的电脑上管理。不管身处何方，任何人都可以挖掘、购买、出售或收取比特币。

专属所有权：操控比特币需要私钥，它可以被隔离保存在任何存储介质。除了用户自己之外无人可以获取。

低交易费用：可以免费汇出比特币，但最终对每笔交易将收取约1比特的交易费以确保交易更快执行。

无隐藏成本：作为由A到B的支付手段，比特币没有繁琐的额度与手续限制。知道对方比特币地址就可以进行支付。

跨平台挖掘：用户可以在众多平台上发掘不同硬件的计算能力。

优点

完全去中心化，没有发行机构，也就不可能操纵发行数量。其发行与流通，是通过开源的p2p算法实现。

匿名、免税、免监管。

健壮性。比特币完全依赖p2p网络，无发行中心，所以外部无法关闭它。比特币价格可能波动、崩盘，多国政府可能宣布它非法，但比特币和比特币庞大的p2p网络不会消失。

无国界、跨境。跨国汇款，会经过层层外汇管制机构，而且交易记录会被多方记录在案。但如果用比特币交易，直接输入数字地址，点一下鼠标，等待p2p网络确认交易后，大量资金就过去了。不经过任何管控机构，也不会留下任何跨境交易记录。

山寨者难于生存。由于比特币算法是完全开源的，谁都可以下载到源码，修改些参数，重新编译下，就能创造一种新的p2p货币。但这些山寨货币很脆弱，极易遭到51%攻击。任何个人或组织，只要控制一种p2p货币网络51%的运算能力，就可以随意操纵交易、币值，这会对p2p货币构成毁灭性打击。很多山寨币，就是死在了这一环节上。而比特币网络已经足够健壮，想要控制比特币网络51%的运算力，所需要的cpu/gpu数量将是一个天文数字。

缺点

交易平台的脆弱性。比特币网络很健壮，但比特币交易平台很脆弱。交易平台通常是一个网站，而网站会遭到黑客攻击，或者遭到主管部门的关闭。

交易确认时间长。比特币钱包初次安装时，会消耗大量时间下载历史交易数据块。而比特币交易时，为了确认数据准确性，会消耗一些时间，与p2p网络进行交互，得到全网确认后，交易才算完成。

价格波动极大。由于大量炒家介入，导致比特币兑换现金的价格如过山车一般起伏。使得比特币更适合投机，而不是匿名交易。

大众对原理不理解，以及传统金融从业人员的抵制。活跃网民了解p2p网络的原理，知道比特币无法人为操纵和控制。但大众并不理解，很多人甚至无法分清比特币和Q币的区别。“没有发行者”是比特币的优点，但在传统金融从业人员看来，“没有发行者”的货币毫无价值。[12]

货币交易听语音

购买方法

用户可以买到比特币，同时还可以使用计算机依照算法进行大量的运算来“开采”比特币。在用户“开采”比特币时，需要用电脑搜寻64位的数字就行，然后通过反复解谜密与其他淘金者相互竞争，为比特币网络提供所需的数字，如果用户的电脑成功地创造出一组数字，那么就将会获得25个比特币。

由于比特币系统采用了分散化编程，所以在每10分钟内只能获得25个比特币，而到2140年，流通的比特币上限将会达到2100万。换句话说，比特币系统是能够实现自给自足的，通过编码来抵御通胀，并防止他人对这些代码进行破坏。

交易方式

比特币是类似电子邮件的电子现金，交易双方需要类似电子邮箱的“比特币钱包”和类似电邮地址的“比特币地址”。和收发电子邮件一样，汇款方通过电脑或智能手机，按收款方地址将比特币直接付给对方。下列表格，列出了免费下载比特币钱包和地址的部分网站。

比特币地址是大约33位长的、由字母和数字构成的一串字符，总是由1或者3开头，例如"1DwunA9otZZQyhkVvkLJ8DV1tuSwMF7r3v"。比特币软件可以自动生成地址，生成地址时也不需要联网交换信息，可以离线进行[2]。可用的比特币地址超过2个。形象地说，全世界约有2粒沙，如果每一粒沙中有一个地球，那么比特币地址总数远远超过所有这些“地球”上的所有的沙子的数量。

比特币地址和私钥是成对出现的，他们的关系就像银行卡号和密码。比特币地址就

像银行卡号一样用来记录你在该地址上存有多少比特币。你可以随意的生成比特币地址来存放比特币。每个比特币地址在生成时，都会有一个相对应的该地址的私钥被生成出来。这个私钥可以证明你对该地址上的比特币具有所有权。我们可以简单的把比特币地址理解成为银行卡号，该地址的私钥理解成为所对应银行卡号的密码。只有你在知道银行密码的情况下才能使用银行卡号上的钱。所以，在使用比特币钱包时请保存好你的地址和私钥。

比特币的交易数据被打包到一个“数据块”或“区块”(block)中后，交易就算初步确认了。当区块链接到前一个区块之后，交易会得到进一步的确认。在连续得到6个区块确认之后，这笔交易基本上就不可逆转地得到确认了。比特币对等网络将所有的交易历史都储存在“区块链”(blockchain)中。区块链在持续延长，而且新区块一旦加入到区块链中，就不会再被移走。区块链实际上是一群分散的用户端节点，并由所有参与者组成的分布式数据库，是对所有比特币交易历史的记录。中本聪预计，当数据量增大之后，用户端希望这些数据并不全部储存自己的节点中。为了实现这一目标，他采用引入散列函数机制。这样用户端将能够自动剔除掉那些自己永远用不到的部分，比方说极为早期的一些比特币交易记录。

消费方式

许多面向科技玩家的网站，已经开始接受比特币交易。包括Mtgox, BTCChina之类的网站，以及淘宝某些商店，甚至能接受比特币兑换美元、欧元等服务。毫无疑问，比特币已经成为真正的流通货币，而非腾讯Q币那样的虚拟货币。国外已经有专门的比特币第三方支付公司，类似国内的支付宝，可以提供API接口服务。

可以用钱来买比特币，也可以当采矿者，“开采”它们用电脑搜寻64位的数字就行。通过用电脑反复解密，与其他的淘金者竞争，为比特币网络提供所需的数字。如果电脑能够成功地创造出一组数字，就会获得25个比特币。比特币是分散化的，需要在每个单位计算时间内创造固定数量比特币是每10分钟内可获得25个比特币。到2140年，流通的比特币上限将达到2100万。换句话说，比特币体制是可以自给自足的，译成编码可抵御通胀，防止他人搞破坏。

支付案例

在被投资者疯狂追逐的同时，比特币已经在现实中被个别商家接受。北京一家餐馆开启了比特币支付。这家位于朝阳大悦城的餐馆称，该店从2013年11月底开始接受比特币支付。消费者在用餐结束时，把一定数量的比特币转账到该店账户，即可完成支付，整个过程类似于银行转账。该餐馆曾以0.13个比特币结算了一笔650元的餐费。[13]

2014年1月，Overstock开始接受比特币，成为首家接受比特币的大型网络零售商。^[14]

如何看待比特币Segwit2x硬分叉？

对于这个问题，每日经济新闻编辑张杨运认为：

11月9日早间，据财经杂志最新消息，比特币本月中硬分叉项目紧急中止。有关比特币硬分叉的争论旷日持久。比特币硬分叉是一个关乎比特币生死的问题，比特币的运营者和每一个矿工都负有责任，所以硬分叉考虑需要慎之又慎。

为什么比特币Segwit2x要硬分叉？比特币的区块链一开始被设定为只能承载1MB大小的信息量，能够容纳的交易总数量是有限制的。这会导致很多问题，比如成交缓慢、转账到别人的比特币账户耗时过长等问题。打个简单的比喻，这就像没有电脑时代的证券交易所，需要人工来进行手动交易，交易量如果暴涨还需要排队，所以随着比特币交易量的增加，速度变得越来越慢，扩容问题成了摆在当前的一个首要问题。所以比特币的矿工和开发团队做出了让步，决定使用Segwit2x方案进行扩容。

Segwit2x方案内容分为两条：

1. 隔离见证的区块会将交易资料、金额等信息分开处理。
2. 将区块扩容至2MB。

所以比特币Segwit2x要硬分叉的原因显而易见，交易速度要加速。

那为什么11月9日比特币硬分叉方案会再次搁浅？硬分叉的原理是不向前兼容，旧版本不会接受新版本创建的合法区块，那么肯定有些矿池运营者没有更新版本，或是不相信这个新方案，没有足够的支持者，方案自然就无法通过。当然比特币的开发者是在积极推动方案的施行。但想想就知道，这样一项事关比特币未来的大事，全球那么多的比特币矿工就根本不会完全同意，要所有人都同意，这几乎是一个无法完成的任务。要么牺牲少部分人的利益成全大多数，当少部分人的比例占比过大，比特币的吸引力也会下降，而这，也成了一个哲学问题。

此外，与硬分叉相对的是软分叉，软分叉之所以连考虑都不考虑，原因也很简单，虽然软分叉旧版区块链可以验证新版区块链，但毕竟是不同的区块链，一旦产生不能验证的区块，又将出现硬分叉，产生独立的区块链，更为复杂。

好了，文章到此结束，希望可以帮助到大家。