

中本聪

比特币之父，名字叫中本聪。受2008年金融危机影响，中本聪提出了一种虚拟货币，通过技术手段真正保证了私有化财富的不可侵犯性。也就是说，除了你自己，没人能拿走你的比特币。没人知道你有多少比特币。

但这种货币不在任何国家发行，只卡在电脑上。中本聪是加密算法的天才。如果一个群体想要获取比特币，就必须有特定的软件来利用计算能力获取。，即比特币网络处置能力的计量单位，解决一些数学问题，比特币作为破解奖励。这个奖池一共2100万个比特币，也就是说比特币的数量是一定的。挖掘出来的比特币占奖池比特币的50%后，奖励会减半。最后的奖励是每次50个比特币，以此类推，也就是说2100万个比特币永远挖不出来。

未来比特币很可能会成为一个革命性的东西，比如世界货币。大约在未来的某一天，它会变得毫无意义，毫无价值！但是比特币的发明者中本聪将被载入史册。

比特币的概念最终于2009年由中本聪提出。根据中本聪的思想，想象一下已经发布的开源软件和建立在其上的P2P网络。比特币是一种P2P数字货币。点对点传输意味着一个分散的支付系统。

与大多数货币不同，比特币不是由特定的货币机构发行的。比特币经济根据特定的算法，经过少量的计算，利用整个P2P网络中众多节点形成的分布式数据库，确认和记录所有的交易行为，并利用密码学的想象力，保证币滞所有环节的安全。。P2P的去中心化特性和算法本身可以保证货币不能被人操纵，制造少量的比特币。基于密码学的想象可以让比特币只被真正的拥有者转移或支付。这保证了货币所有权的匿名性和交易的停滞。。比特币与其他虚拟货币最大的区别在于其总量非常有限，极其稀缺。货币制度只需要在四年内不超过1050万，总数将永远限制在2100万。

比特币可以用来套现。可以兑换成大多数国家的货币。用户可以使用比特币购买一些虚拟物品，比如衣服、帽子、装备等。在网络游戏中。只要有人接受，也可以用比特币购买理想生活中的物品。[1][2]

2014年2月26日，西弗吉尼亚州威权党派参议员乔曼钦(JoeManchin)收回了一封致美国联邦政府多个监管部门的公开信，希望相关机构能够关注比特币鼓励合法活动、扰乱金融从属地位的现状。并恳求尽快采取措施，单方面封杀电子货币。[3]

2017年1月24日中午12:00起，国内三大比特币平台正式收取交易费用。 [4]

中文名

比特币

mbth

比特币

类别

电子货币

停滞平台

网络[

开始倾听声音的过程

2008年，全球金融危机期间，有人在generate上以“中本聪”并描述了比特币的方式。

有两个

比特币

与法定货币相比，比特币没有集体发行者，而是由网络节点计算产生。任何人都可以参与制造比特币，它可以在全球范围内一蹴不振，可以在任何一台联网的电脑上买卖，无论他们身在何处。，任何人都可以开采、购买、出售或收集比特币，其他人也可以“识别用户”；买卖过程中的身份音频。 [2]2009年，不受央行或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乱码组成，新的比特币是由预设的第二时间制造的。随着比特币总量的增加，制造新币的速度变慢，直到2014年达到2100万的下限，挖出的比特币总量一度超过1200万。 [2]

每当比特币进入主流媒体“；”的视野，主流媒体总是请一些支流经济学家来分析比特币。此前，这些分析总是聚焦于比特币是否是骗局。通常的分析总是聚焦于比特币未来能否成为朝贡货币。。而狡猾的焦点往往收敛于比特币的通缩特性。 [5]

很多比特币玩家被比特币接受；公司不能随意增发股票。与比特币玩家的态度相反，经济学家对比特币2100万的总活跃度持两极分化的态度。 [6]

凯恩斯主义经济学家认为，政府应该自动控制货币总量，利用货币政策的松紧适时给经济加油。所以他们认为比特币的活跃总量牺牲了可控性。更糟糕的是，这将不可避免地导致通货紧缩，从而损害当地经济。奥地利经济学家也有同样的想法。他们认为政府对货币的干预越少越好。货币总量流动导致的通货紧缩不是什么大事，甚至是社会进步的标志。

比特币网络是“开采”来产生新的比特币。所谓的“采矿”本质上是用计算机处理一个复杂的数学效果来保证比特币网络中分布式记账的一致性。比特币网络会自动调整数学效果的难度。让全网大概每10分钟得到一个合格的答案。然后比特币网络会再生成一定数量的比特币作为奖励，奖励得到答案的人。

2009年比特币诞生的时候，每份赏金是50个比特币。出生后十分钟第一批50个比特币产生，此时的货币总量为50。然后比特币以每10分钟50个左右的速度递增。当总额达到1050万(2100万的50%)时，奖励减半至25。当总量达到1575万时(新增产量525万)，也就是1050的50%)，奖励减半到12.5。 [7]

首先，根据其假想原理，比特币的总量会不断增加，直到100多年后达到2100万。但是，比特币的货币总量在前期会增长非常缓慢。。在梦里，87.5%的比特币将“挖”在最初的12年。所以从货币总量来看，比特币不会达到流动性，它的货币总量其实会时不时的缩水，虽然速度越来越慢。所以看起来比特币是一种通货膨胀的货币。

但通缩和收缩的区别不是基于货币总量是否在增加，而是基于当地物价水平是否在下降。当地价格下降就是通货膨胀，反之亦然。就目前而言，比特币的发行机制决定了其货币总量的增减速度会远低于社会财富的增减速度。

凯恩斯主义经济学家认为，物价的持续下跌会使人们倾向于延迟消费，因为一美元明天可以买到更多的东西。。自愿消费的减少进一步导致需求萎缩和商品滞销，使价格走低，陷入“通货紧缩螺旋”。矛盾的是，通缩货币即使不拿出银行本身也能升值(购买力越来越强)，人；美国的投资意愿也会降低。社会消费也会陷入低迷。 [5]因此，比特币是一种具有通货紧缩倾向的货币。在比特币经济中，用比特币定价的商品价格会继续下跌。 [1]

比特币是一种网络虚拟货币，数量有限。但是它可以用来兑换现金：它可以兑换成大多数国家的货币。可以用比特币购买一些虚拟物品，比如网游中的衣服帽子装备等。只要有人接受，你也可以用比特币购买幻想生活中的物品。 [1][1]

2014年9月9日，美国电商巨头易贝宣布，该公司旗下的Braintree将在年底接受比特币。该公司已与比特币交易平台比特币基地达成合作。最后，承担这种相对较新的支付手段。

虽然易贝市场交易平台和PayPal业务不接受比特币支付。然而，旅游租赁社区Airbnb和汽车租赁机构优步等布伦特里的客户最终将能够接受这种虚拟货币。布伦特里的主要业务是为企业支付处理软件。该公司去年被易贝以大约8亿美元的价格收购。

2017年1月22日晚间，Huobi.com、btc中国、OKCoin相继在各自官网发布公告称，为进一步抑制投机行为，防止价格剧烈坚挺，各平台将于2017年1月24日中午12:00开始收取交易生效费，生效费按交易金额0.2%的浮动费率收取，主动交易费率与主动交易费率相同。[4]5月5日，OKCoin币网最新数据出现。比特币的价格刚刚刷新纪录，在截稿前触及9222点的高点。[8]

创造人们听语音

2008年11月1日一个自称中本聪的人在一个隐藏的密码学评论小组里发表了一个讨论。陈说，陈说了他的电子货币的新想法，——一个比特币出来了，比特币的第一笔交易完成了。。比特币通过公开中本聪称之为“区域链”。用户愿意贡献CPU的计算能力，运行一个特殊的软件成为一个“挖掘者”，这将形成一个网络来坚持“区域链”一个人。在这个过程中，他们也将产生新的钱。交易也在这个网络上延伸，运行这个软件的计算机真正解决了不可逆的暗码问题，其中包含了几个交易数据。第一个“矿工”解决问题将获得50个比特币的奖励，相关交易区域将参与链中。。随着“数量的增加矿工”，每个谜题的难度等级也有所提高，使得每个交易区的比特币消耗速度都坚持在10分钟左右。

京都大学数学教授ShinichiMochizuki[XY002][XY001]2009年，中本聪设计了一种数字货币。也就是比特币，蓬勃发展的比特币市场跌宕起伏，其创始人中本聪的身份一直是个谜。关于“比特币之父”涉及从美国国安局到金融专家的人士，也给比特币蒙上了一层微妙的光环。

据国外媒体报道，计算机迷信者TedNelson周日在网上发布了一段视频，称他确定比特币的创始人是京都大学数学教授ShinichiMochizuki。。比特币的创始人一直用的是SatoshiNakamoto这个笔名，网上对其真实身份也有一点猜测。尼尔森发布视频称，他确定望月新一是比特币的真正创始人。[9]

望月新一2013年因证明ABC猜想而成名。高中时，他就读于美国最负盛名的高中之一菲利普埃克塞特学院，两年后才毕业。望月新一16岁进入普林斯顿大学，22岁离

开学校成为一名医生。他在33岁时成为正教授。如此年轻就获得正教授头衔，在学术界极为罕见。这位数学界的超级明星可能已经突破了这个世界最重要的问题之一。中本聪本人在网上几乎没有留下任何群组信息。尤其是近几年彻底消亡，所以它的身世成了一个谜。2014年3月7日，比特币创始人多里安·中本聪被找到的旧闻一出，迅速成为网络上收到最多的消息。

与可能是虚拟名称的推测相反，“中本聪”是真名。他是一名64岁的日裔美国人。他喜欢收集火车模型。他曾为大型企业和美国军方工作，从事秘密义务。在过去的40年里，中本聪在生活中从不使用真名。根据1973年洛杉矶地方法院的档案，当他23岁从加州州立理工大学毕业时，改名为Dorian Prentice Satoshi Nakamoto。从那以后，他不再使用“中本聪”，并与多里安·中本聪(Dorian Nakamoto)为署名。[9]

发生原理

从比特币的本质来看，比特币的本质其实是一堆冗杂算法生成的特殊解。特解是指一组有限的(其实比特币是有限的)解，可以通过方程丢失。而且每个特解都能解方程，是唯一的。[10]就大众货币而言，比特币是大众货币的序列号。你知道钞票上的序列号。你有这张账单。挖掘的过程就是通过庞大的计算，时不时的求这个方程组的特解。这个方程组被设计成只需要2100万个特解，所以比特币的下限是2100万。[10]

猖狂崛起

挖矿比特币，可以下载公共比特币计算工具，然后注册各种合作网站，在计算顺序中填写注册用户名和密码，然后点击操作正式开始。[11]完成比特币客户端设备后可以直接得到一个比特币地址。别人付款的时候，你只需要把地址公布给别人，就可以通过不同的客户端支付。安装比特币客户端后，它会分配一个私钥和一个公钥。您需要备份您的钱包数据，包括您的私钥，以确保您的财富不会丢失。假设完全格式化的硬盘被反转，则组的比特币会原封不动的丢失。

货币特征

去中心化：比特币是第一种分布式虚拟货币。整个网络由没有中央银行的用户组成。去中心化是比特币的保障；安全和自由。

整个世界都不景气：比特币可以在任何能上网的电脑上进行管理。无论你在哪里，任何人都可以挖掘、购买、出售或收集比特币。

独占所有权：操纵比特币需要一个私钥，这个私钥可以被隔离并保存在任何存储介质中。除了用户自己，没有人能得到。

交易成本低：比特币可以免费汇出。但最终每笔交易会收取1bit左右的交易费，以保证交易更快的实现。

无隐性利益：比特币作为从A到B的支付手段，没有复杂的限额和手续。了解对方就可以止付；的比特币地址。

跨平台挖掘：用户可以挖掘许多平台上不同硬件的计算能力。

优点

完全分散，没有发行人，就无法安排发行数量。它的释放和迟缓是通过开源的p2p算法来完成的。

匿名、免税、免监管。

鲁棒性。比特币完全依赖p2p网络，没有集散中心，无法对外封锁。比特币价格可以坚挺，也可以崩盘，很多政府可以合法发布。但是比特币和比特币；庞大的p2p网络不会消失。

无边框和跨界。跨境汇款会经过层层外汇管制机构，交易记录会被多方记录。但是假设你用比特币交易，直接输入数字地址，点击鼠标。等待p2p网络确认交易后，会有少量资金通过。不经过任何监管机构，不会留下任何跨境交易的记录。

山寨的人很难活。因为比特币算法是完全开源的，任何人都可以下载源代码，修改一些参数，重新编译。你可以创建一个新的p2p货币。然而，这些假币很弱，容易受到51%的攻击。任何团体或组织，只要掌握了一个p2p货币网络51%的计算能力，就可以任意安排交易和货币价值，这将对p2p货币构成毁灭性的打击。很多仿冒品，是死在这个环节上的。比特币网络足够强大。要掌握比特币网络51%的计算能力，需要的cpu/gpu数量将是天文数字。

缺陷

交易平台的弱点。比特币网络非常健壮。但是比特币交易平台很弱。交易平台一般是网站，网站会被黑客攻击，被主管部门屏蔽。

交易确认时间长。比特币钱包第一次安装时，下载历史交易数据块会消耗少量时间

。。交易比特币时，为了确认数据的准确性，需要一段时间停止与p2p网络的交互，失去全网确认后交易才算完成。价格波动很大。由于少数投机者的介入，比特币兑换现金的价格犹如过山车。。让比特币更适合投机而不是匿名交易。

大众不了解原理，以及激进金融从业者的抵触情绪。生动的网友了解p2p网络的原理，知道比特币是无法人为安排和控制的。但是公众不知道。我不明白很多人可以“我甚至分不清比特币和q币的区别。”没有发行者“是比特币的优势，但在激进的金融从业者看来，没有发行方的货币一文不值。[12]

听货币交易之声

购买方法

用户可以购买比特币，同时可以使用计算机根据算法停止大量操作，以“我的比特币。当用户“我的比特币，他们需要用电搜索64位数字，然后通过反复解谜与其他淘金者合作。为比特币网络提供所需的号码，假设用户“的计算机成功创建了一组数字，那么将获得25个比特币。

由于比特币是通过聚合逐段编程的，每10分钟只能获得25个比特币，到2140年，不景气的比特币下限将达到2100万。换句话说，比特币系统可以实现自力更生，通过编码抵御通货膨胀，并阻止他人停止破坏这些代码。

交易方式

比特币是类似电子邮件的电子现金。双方都需要一个“比特币钱包”有相似的电子邮件地址和一个“比特币地址”有着相似的电子邮件地址。就像收发邮件一样，发件人根据收件人间接支付比特币给对方“；你可以通过电脑或智能手机找到他的地址。下表，上面列出了一些付费下载比特币钱包和地址的网站。

比特币地址是一串大约33位长的字母和数字，总是以1或3结尾。例如，“1dwuna9otzzqyhkvklj8dv1tuswmf7r3v”；比特币软件可以主动生成地址，生成地址时不需要在线交换音频，可以离线停止[2]。可用的比特币地址超过2个。一般而言世界上大约有2粒沙子。假设每一粒沙子里都有一个地球，比特币地址的总数远远超过所有这些沙子的总数“地球”。

比特币地址和私钥是成对出现的，它们的联系就像银行卡号和密码。。比特币地址就像一个银行卡号，记录你在那个地址有多少比特币。可以随意生成一个比特币地址来注册比特币。每生成一个比特币地址，都会生成该地址对应的私钥。。这个私

钥可以证明你拥有这个地址的比特币的所有权。我们可以冗杂地把比特币地址理解为银行卡号，地址的私钥理解为对应银行卡号的密码。知道银行密码才能用银行卡号上的钱。因此使用比特币钱包时请保管好自己的地址和私钥。

比特币的交易数据打包成一个“数据块”或者一个“阻止”，交易被初步确认。当一个块链接到前一个块时，事务将失去进一步的确认。。连续被六块确认后，交易基本确认不可逆。比特币点对点网络将所有交易历史存储在一个“区块链”。区块链继续延伸，一旦新的区块加入区块链，，它将不会被再次删除。区块链实际上是一组聚集的客户端节点，是一个由所有参与者组成的分布式数据库，是所有比特币交易历史的记录。中本聪估计，当数据量增加时，客户端希望这些数据不会存储在本地自己的节点中。。为了完成这一点，他采用了引入哈希函数的机制。通过这种方式，客户端将能够主动消除那些他们永远不会使用的部分，例如一些非常早期的比特币交易记录。

消费模式

很多技术玩家的网站，已经开始接受比特币交易。包括Mtgox、BTCChina等网站，以及淘宝的一些店铺，甚至可以接受比特币兑换美元、欧元等服务。毫无疑问，比特币已经成为流通中的真实货币，而不是腾讯q币那样的虚拟货币。。国外有专门的第三方支付公司，类似支付宝，可以提供API接口服务。

你可以用钱买比特币，也可以当矿工“我的通过用计算机搜索64位数字。通过用计算机反复解密与其他淘金者合作，为比特币网络提供所需数字。假设计算机能成功创建一组数字，将获得25个比特币。比特币是集中式的，它需要在每单位计算时间内创建一个移动号码。比特币每10分钟可以获得25个比特币。。到2140年，流通中的比特币下限将达到2100万。换句话说，比特币系统可以自力更生，翻译成代码可以抵御通货膨胀，防止别人破坏。

支付案例

在被投资人疯狂追逐的同时，比特币已经被幻想中的普通商家所接受。北京一家餐厅屏蔽了比特币支付。襄阳大悦城的餐厅表示，2013年11月底开始接受比特币支付。用餐结束时，消费者将一定数量的比特币转入商店账户，，就可以完成支付，整个过程和银行转账差不多。餐厅曾经用0.13比特币结算了一顿饭650元。[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批发商。。[14]

比特币是中本聪创造的，这(几乎可以肯定)是一个化名。到目前为止，还没有人能

真正把比特币和一个真实的人或者一群人联系起来。中本聪于2011年从互联网上消失了。几乎没有任何线索表明他们可能是谁。这些年来，很多人都公开声称自己是聪，但他们并没有用无可争辩的幻想来支持这种说法。

在一个早期的比特币论坛。Satoshi说，他们从2007年开始讨论比特币，比第一个区块开采早两年。2009年1月3日，比特币区块链的第一个区块——创世纪——区块被开采。中本聪是创世纪区块的矿工，获得了首批投入流通的50枚比特币。但是第一个盒子的奖励是无法支付的，因为代码中创世纪盒子的表述有点奇怪。BitMEX发布了对比特币后期剥削的分析。得出的结论是“有人”挖掘了70万个比特币。虽然很多人认为这是Satoshi，但是官方并没有证明。人们只能想象如果他们的身份被暴露，中本聪会得到什么样的名声。更不用说他们将收集的巨额财富(虽然佐藤没有；似乎没有花掉任何他们应该开采的硬币)。久而久之，很多人都自称是聪，也有人是被迫的。虚假索赔自称为智的最著名的例子之一是澳大利亚学者中本聪。早在2015年，莱特就多次试图向公众展示他是比特币创造者的无可辩驳的证据，但直到明天也没有胜诉。空想地他的“证据”证明是假的。

为什么Satoshi要匿名

中本聪，世界；美国第一个集合货币的创造者，可以说是坚持匿名，因为他们创造的性质。在创建了一个没有失败中心的协议后，中本聪可能已经意识到，坚持匿名可能会消除比特币可能存在的最后一个失败中心：创建它的人。去掉很多可能与比特币的出现有关的身份。它删除了任何可能影响比特币社区政治、规则或决策的众多面孔。

不管Satoshi是谁，他们无疑是我们这个时代的人才。比特币协议在所有适当的中心提供经济鼓励。为拜占庭将军的效果提供了特殊的处置方案。中本聪利用密码学、数学、博弈论和经济学的概念，创造了一个精心设计的——数字稀缺资产——比特币。

比特币的创造者是日本人，名叫中本聪，2009年1月3日，世界；s第一批比特币诞生，数字货币正式诞生。数字货币的价格直到2013年底才迅速下降。过去从10美元左右涨到900多美元。2016年，比特币热真的起来了。价格暴涨，被称为“数字黄金”。比特币为什么这么值钱？

1. 采矿很难。比特币挖矿需要具体操作，对操作时间的兴趣很高，前期实物投入也很大。
2. 比特币具有货币属性，被市场怀疑。比特币的加密算法很难破解，保证了它的

唯一性。

3. 比特币交易市场透明度高，市场价格都是公开透明的。虚拟数字商品的流动和交易方便快捷。

4. 随着一些国家的认可，相对于特种货币，数字货币出台的一些政策无疑会缓解比特币的价格下跌。

物以稀为贵，比特币相对来说比较少见。目前要挖掘出可比较的钱币非常困难，供求关系的影响，市场上供不应求的情况等。无疑对价格下跌起到了很大的作用。在交易平台购买比特币赚取差价需要谨慎。

比特币是一种P2P数字货币。点对点传输意味着一个分散的支付系统。2009年，日本人中本聪提出了比特币的概念。自诞生以来，比特币的价格高得难以想象。比特币为什么这么值钱？

Let's；让我们杂乱无章地谈论它。

比特币挖矿者的操作有一个特殊的顺序。操作后可以获得类似股权奖励的比特币。以前比特币的产量很低，每天大约生产3600枚新币，数量有限。比特币挖矿价格高。自比特币大热以来，专业矿机的价格一直在万元左右，平时的价格已经超过30万元。前期设备投入需要大量财力；采矿需要很长时间。比特币挖矿是特定的复杂操作，消耗时间很长；比特币挖矿机耗电量很大，除了自己的消耗。比特币挖矿机日耗电量可达1.88亿千瓦时。，相当于中国的百分之一's；的日发电量。比特币的数量还在时不时的增加，没有机构评价。2019年比特币挖矿耗电量将超过美国。

比特币的价格一直与媒体比较有关。在这里，我提醒自己。比特币价格涨的快，跌的也会快，风险大。想亏本买比特币的朋友一定要慎重参与。

沉寂多日的比特币，利用'勒索'病毒又堵住了熟悉的逃跑途径。这种虚拟货币叫做'数字黄金'8年暴涨300万倍，连中国大妈都入市了。有人认为这是一个传递包裹式的游戏。有人坚信比特币会成为稀缺资产。还有人说，它会是历史长河中闪闪发光的一个节点，大多数人会把它生吞活剥。，只是惊讶于另一轮财富在生成。

艾比投认为比特币到底是谁创造的？关于比特币的发明者一直没有定论，普遍的说法是日本人'中本聪'。2009年1月3日世界's；美国第一批比特币被挖出，这种数字货币由一个代号为'中本聪'正式诞生了。从那以后，有15个组织被怀疑是'中本聪'。2014年，美国权威媒体披露，这位日

裔美国物理学家的真名是“中本聪”，就是传说中的“比特币之父”，但老教授坚定地承认了。图为难得一见的中本聪被媒体围攻，不时挡住镜头，坦白与比特币有任何联系。

2016年5月澳大利亚工程师兼企业家克雷格赖特公开宣称自己是比特币——中本聪的创造者。但仅仅几天后，怀特本人“叛逃”并宣布他已经“未能出示关键证据”为了证明自己。。尽管中本聪被提名为2016年诺贝尔经济学奖候选人，但他的真实身份还没有完全揭开。图片：BBC(来自：腾讯图片)

克雷格怀特(Craig White)在与比特币挂钩后，被警方盯上。。图为澳大利亚联邦警察和税务官员搜寻怀特；他们的比特币相关业务具有税收效应。据媒体报道，这个微妙的数字“中本聪”持有100多万比特币，按照现在的15000元公币计算。他的身价超过150亿公共硬币。根据最终的苛刻设计，比特币总数限制在2100万枚，目前已经开采了约1400万枚。图片：路透社

中本聪，我不；我不知道他的真实身体。

到目前为止，中本聪还不确定是谁。应该不是一个团体，而是一个机构

。是比特币的创始人(发明者)

，符合监管。

中本聪(中本聪)是最初的比特币客户端的创始人。

2019年8月16日匿名十余年后，比特币之父Satoshi Nakamoto将于美国东部时间8月18日周日下午4点在相关网站上发布我的启示，以表明自己的真实身份。