关于比特币（BTC）

原文:
https://www.btcc.com/zh-CN/markets/Bitcoin/chat

比特币是世界上第一个被广泛采用的加密货币，作为一种数字现金形式，它无需银行或政府等中央机构。相反，比特币使用点对点互联网网络直接在用户之间确认购买。

由神秘的开发者中本聪于 2009 年推出，比特币 (BTC) 是被称为加密货币的新兴资产类别中的第一个，也是最有价值的进入者。

目前，它已经成为全球市值最大且最知名的加密货币。它的流行激发了许多其他加密货币的发展。这些竞争对手要么试图将其替换为支付系统，要么在其他区块链和新兴金融技术中用作实用程式或证券代币。

比特币的发展

数位加密货币的概念最先于1998年由Wei Dai在线上论坛Cypherpunks的电邮通讯中所提出，他相信使用密码学原理的应用将可以促成社会变革并且提高信息时代的隐私水平。然而比特币从理念发展到成型却是经历了十年时间。

一位名为中本聪的人在2008年发表了一篇名为《比特币：一种点对点的电子现金系统》论文，这篇论文也被称为「比特币白皮书」，其中描述了比特币运作原理。

2009年1月，中本聪发布了第一个开源的比特币软体客户端，安装该客户端的人都可以开始使用比特币。

最初，比特币的支持者大体上为主张使用强大密码学和隐私增强技术来推动社会和政治变革的人士。但在接下来的十年里，比特币的用户数量不断增长，使用比特币的人群也不在局限于最初的「密码朋克」中了。

随着主要经济体的监管机构明确了比特币的合法性，大量的比特币交易所建立了与银行的关联，使得当地货币与比特币之间可以轻松兑换。随着越来越多的知名投资者表现出对比特币的兴趣，其他的一些企业也建立了强大的托管服务，使机构投资者更容易接触到这种资产。

比特币的工作原理

当你想要用比特币买东西时，你就需要打开你的比特币钱包，然后将约定数量的比特币发送给商家。比特币交易会透过「私钥」来确认钱包之间的比特币交换，这样有助于提高安全性。

交易完成后，矿工们会将这些交易打包成一个「区块」，然后利用哈希函数进行运算并加密生成独一无二的签名。哈希运算是比特币运作方式的一个非常重要的环节，简单点讲就是将一个特定区块中的所有交易数据压缩成能够被读懂且易于区分的代码，这串代码就叫哈希值。

最后，包含哈希值的区块会被广播到网络中进行验证，如果验证为有效，该区块就会被添加到「区块链」

当中供网络上的其他人查看。

比特币挖矿

要进行比特币挖矿，您就需要运作一个收集比特币交易记录并将其打包成区块的挖矿节点，该节点还需要拥有足够的计算能力才能够让您有机会成为第一个算出符合要求哈希值的矿工。正因为如此，挖矿节点的运行成本很高，它需要一台功能强大的电脑和大量电力来维持。

为了抵消这些成本并增加成功的机会，矿工可以将他们的资源组合成一个「矿池」，即将个人的小量算力和资源合并起来进行挖矿，这样做可以最大限度地提高他们率先打包出新区块并获得比特币奖励的能力。

比特币分叉

如果要正确理解比特币分叉，我们还需要从区分软体分叉的「软分叉」和「硬分叉」开始。

软分叉

在软分叉当中，新系统仍然与旧系统「向后兼容」。这里向后兼容的意思是指经过升级过后的新区块链将负责验证区块的交易，并且旧的区块链也仍然能够识别和记录这些交易。然而，新的区块链不会识别现有区块链上以旧程序挖出来的区块。

硬分叉

相比之下，硬分叉进一步引进了与旧网络不相容的新软件。这意味着所有交易都必须在新的区块链上进行处理，并且使用旧软件的矿工都必须进行升级。

如果用户没有通过达成共识解决硬分叉，那么一个新的数位加密货币将被创建，相关的例子比如就有比特币现金（bitcoin cash）和比特币黄金。

比特币安全

自 2010 年以来，已经发生了近十次加密货币交易所的黑客攻击。损失范围达数亿（美元）。然而，相对而言，传统银行和金融机构在同一时间段内已经为网络犯罪分子损失了数十亿美元。程序员和加密货币社区正在努力识别和修复其区块链网络中的漏洞。

在个人层面上，任何投资比特币的人在访问金融信息和进行交易之前都应该有适当的互联网安全措施。

白皮书　　官网