什么是加密货币？它们和比特币一样吗？

一言以蔽之：是的。

比特币是第一个加密货币，目前也是规模最大的加密货币，但是自它诞生近8年来，一直有其它加密货币要夺取王位。

所有加密货币都有一个共同特点：都使用了区块链技术。区块链分享公开交易记录，创造并追踪新型数字令牌：无论做什么事，只有网络达成一致，才能创造并分享。以此作为基础，生态系统孕育出大量的变种。

一些加密货币的职能和比特币相似，比如莱特卡和狗狗币，只是在细节方面稍作修改，比如交易速度更快、确保通胀达到一个基本水平。还有一些货币原则一样，但是目的比较特殊，比如以太坊和Bat，前一个面向云计算，后一个面向数字广告。

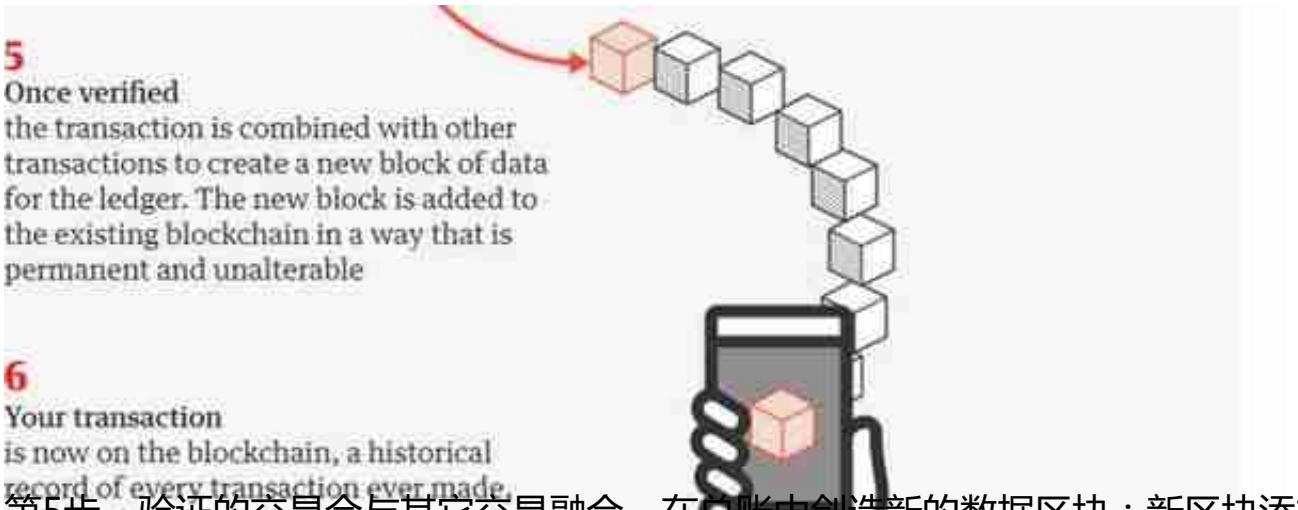
什么是比特币？我能拥有一个吗？

比特币并不以物理形式存在，甚至都不是数字形式。如果我的数字钱包里有0.5个比特币，并不意味着还有半个存在于其它地方。

当你拥有一枚比特币，实际上拥有一份集体协议，这份协议存在于比特币网络的其它计算机上，你的比特币就是由一名比特币矿工合法创造的，然后以合法交易的形式转给你。如果你想拥有一些比特币，有两种办法：成为矿工，不过要投入一些钱购买计算机，交电费，花的钱可能比赚的钱还要多，除非你非常聪明；或者用传统货币从其它人手中购买比特币，一般通过比特币交易所进行，比如Coinbase、Bitfinex。

货币有许多怪异之处，主要归结于集体协议，它规定什么才是合法的。例如，第一枚比特币是2009年创造出来的，到了今天，总数量的增长很缓慢，增速正在下滑，确保到了大约2140年时，总数量会达到2100万枚，再也不会有新比特币产生。

如果你不认同这种集体协议，可以与更广泛的网络分道扬镳，创造自己的“比特币”。这就是所谓的“分叉”（Fork），在过去一段时间，这种事实发生过好多次。因为分叉，才出现了竞争对手莱特币、狗狗币。难点在于你要说服其它人追随你。如果一种货币只被一个人使用，就不能称为货币。



第5步，验证的交易会与其它交易融合，在总账中创造新的数据区块；新区块添加到现有区块链，其加入是永恒性的，不可修改。

第6步，现在交易已经存储在区块链上，每一次交易的历史都存在那里，一直可以追溯到第一枚比特币诞生。

我能用加密货币做什么？

从理论上讲，所有可以用计算云做的事情，都可以用加密货币平台做，做的方式不一样。我们可以建一种加密货币，将全球计算机网络变成分散平台，存储数据，处理数据，相当于庞大的“群蜂式”PC。听起来和货币没有什么关系，正因如此，才会有人提议用“分散App”（decentralised apps）来描述。

我们已经看到，有人提议用加密货币搭建YouTube克隆体、集换式卡牌游戏(Collectible card games,CCGs)和数字广告交易平台。现在创业公司喜欢说自己“x but on the blockchain”公司，不再说自己是“Uber for X”公司或者“x but on the iPhone”公司。

尽管如此，实用性仍然有限。比特币可以用作支付系统，但是只能完成少量的交易，在真实世界中能够完成的交易更少，至于其它加密货币，那就更加稚嫩了。为什么大家对这个领域如此兴奋？主要是因为它的潜力巨大，并不是因为它现在有多好。

为什么分散如此重要？

从本质上讲，加密货币就是一个数据库。例如，比特币是一个庞大的数据库，记录着谁拥有什么比特币，所有者之间发生了怎样的交易。

这套系统与传统银行基本一样，银行也是一个庞大的数据库，记录着谁拥有英磅，

所有者之间发生了怎样的交易。

区别在于，比特币不需要中央机构来运营数据库。银行可以单方面修改数据库，改变你所拥有的钱数，银行经常这样干。有时银行的做法对你有利，比如如果信用卡被偷了，被使用了，银行会补偿你；有时不利，比如银行如果认为你洗钱，可能会冻结你的帐户，摧毁你的业务。

如果使用比特币，没有人能这样做。在比特币网络上，只有一个”权威“，也就是获得大多数比特币用户的同意，而获得大多数人的同意正是网络运行的基本规则。

与犯罪有关吗？

与犯罪有很大的关系。因为加密货币的数据库是分散的，对于大多数人来说，在大多数时间里，它弥补了集中数据库的缺点。如果你信任某个存储资金的金融系统，或者信任存储文件的Dropbox，或者是存储视频的YouTube，那就没有必要使用这些服务的分散版本，因为效率更低。

如果你准备实施金融犯罪，存储非法下载的东西，或者存储盗版视频，使用分散版服务就会变得很有吸引力。正因如此，网络毒贩会使用比特币，窃取数据勒索赎金的黑客会使用比特币。

”犯罪“是一个很宽泛的术语，在许多国家，持有不同政见被认为是犯罪。如果加密货币能够让人越过障碍，从技术角度看它的确在助长犯罪，但是其方式并不是加密货币批评者所说的那样。

你老是说“区块链”，它到底是什么？

区块链是加密货币的核心。它相当于资产所有权变动的分散记录，从简单的层面上讲，就是花了一个比特币，或者在某种二代加密货币上执行复杂的“智能合约”，比如以太坊。

当加密货币交易出现，花钱的一方会将交易的细节广播到整个网络，确保每一个人都能拿到所有权的最新信息。每隔一段时间，所有最新记录都会捆绑，放进“区块”，加入到历史记录。区块链（之前区块连成的链条）就成为了完整完全的记录，告诉你谁在网络拥有什么。

矿工做什么？

矿工建设区块链。具体做什么会因为加密货币不同而不同，比特币算是一个比较好

的例子：大约每隔10分钟，就会有一名矿工以半随机的形式选中，他对听到的交易进行处理，宣布已经确认交易，然后将交易打包，捆绑到一个交易区块，加入到链条。为了报答他的工作，获胜的矿工获得许可，可以“印刷”一些新比特币，支付给自己作为回报，当然，获得的是比特币，目前价值约为14万美元。

任何人都可以成为矿工，只需要用挖矿模式运行比特币软件就行了。难点在于如何成为赚钱的矿工。将交易捆绑的工作实际上还是很容易的，真正的成本来自于赢家选取方式。我们可以用彩票来类比，只是买票时你要用自己的计算机解决一个非常复杂、无休无止的算法问题。如果你想提高获奖的机率（14万美元），要以每秒几百次甚至几百万次的速度解答问题，然后才能提高胜率，夺得尽可能多的彩票，所以你要搭建专用计算机，降低电费，或者入侵无辜者，使用他们的计算机挖矿，不用付出任何代价。

为什么有人赚这么多钱？

这个问题很大。已经发行的比特币价值高达1900亿美元。简单来回答，就是低价买入、高价卖出。8年前，比特币几乎一文不值，8个月前涨到1200美元，12月涨到2万美元，现在约为1.1万美元。如果早期拥有足够多的比特币，现在都很富有了，至少从纸面上看很富有。

为什么一枚比特币值1.1万美元？为什么以太坊值1040美元？为什么Cryptokitty值10万美元？这可能才是真问题。答案如下：所有加密货币都是稀有资产，数量有限。如果货币被人们接受并广泛使用，人们就要购买这些稀有资产，那么它的价值就会涨得比今天还要高。当前的价格反应了某种加密货币的潜力，它未来可能会被人们广泛使用。

前面会出现麻烦吗？

因为“集体贪婪”的存在，市场已经出现泡沫，最终会破灭。大家听到许多故事，说某人从加密货币中赚了大钱，他们自己出价自己购买，哄抬价格，于是又冒出更多的暴富故事，吸引更多的投资。如此循环，最终导致资产的价格脱离现实。泡沫最终会破灭，会有许多人亏损。

接下来？

腾飞
：加密货币也许会实现自己的抱负，在日常生活中被人们广泛使用。最终会有少数人暴富，并不比当年早早向基础技术（比如计算、互联网）投资的人多。

硬着陆
：我们认为的“泡沫“可能会破灭，让大家对整个行业失去信心，投资者逃离，矿工破产，因为他们向专用硬件投入了巨额资金，只有比特币价格高升，他们才能赚到钱，最终加密货币作为一门技术被打入冷宫。

巡航高度（Cruising
altitude）
：也许形势会像过去5年一样发展。加密货币的实际使用保持稳定，大部分使用是非法的，在地下进行，它们的价格与市场价格分离，被金融投机者炒得大起大落。最终，不稳定变成一种奇怪的稳定，成为一种可预测的状态。

编译组出品

编辑：郝鹏程、王雅琪