Market Talks
教育中心

区块链 · 初级 · 第13课，共13课

误解与真相

人们对区块链常有的六个误解，有高估也有低估，以及证据实际显示了什么

阅读约5分钟　　6道测验题，附答案

区块链 · 初级 · 第13课，共13课

误解与真相

一句话概括

区块链既不是魔法，也不是骗局。它在少数几件具体的事情上非常擅长，比如无需中间人就能完成价值结算、保存一份难以篡改的共享记录，而在其他方面则较弱。分清哪些是哪些，能让你既不被炒作冲昏头脑，也不会一概否定。

误解1：“比特币是匿名的”

真相：它是假名的，正如第5课所解释的。地址上没有姓名，但地址之间的每一笔付款都会永远公开。一旦某个地址与某个人对应起来，比如通过一家核实过其身份的交易所，这个人的大部分历史记录就都能被追踪。

2021年6月就有一个清楚的例子。勒索软件攻击Colonial Pipeline，导致美国东海岸燃油供应中断，之后美国司法部在区块链上追踪赎金，追回了所支付75枚比特币中的63.7枚。公开账本原来是个很糟糕的藏身之处。



图1. 区块链在少数几项具体工作上很强，在其他方面较弱。大多数误解都源于忘记了天平的某一边。

类比：玻璃房里的笔名

想象你每封信都用笔名署名，但所有信都钉在一栋临街玻璃大楼的墙上。一开始没人知道你的真名。可一旦有人看到你贴上其中一封信，他就能读到所有署同一个笔名的信。

误解2：“加密货币主要被用于犯罪”

真相：犯罪确实存在，但只占活动的一小部分。分析公司Chainalysis估计，2025年非法地址至少收到了1540亿美元，这个数字非常大，但仍不到其追踪的全部加密货币交易量的1%。其中很大一部分来

自规避制裁以及由国家支持的团伙实施的盗窃。

两方面都很重要。占比很小，但金额大到让监管机构、交易所和银行都严肃对待加密犯罪，这也是交易所要求身份验证的原因。

误解3：“区块链不可能被黑”

真相：比特币账本本身从未被改写过，但它周围的几乎一切都可能遭到攻击。最大的损失来自边缘地带：交易所、钱包、智能合约，以及在链与链之间转移代币的**跨链桥**。2022年3月，攻击者控制了负责批准提款的大部分密钥，从游戏Axie Infinity使用的Ronin跨链桥上盗走约6.25亿美元。美国财政部后来将这起盗窃与朝鲜的Lazarus组织联系起来。

小型链是第二个薄弱环节。如果一个网络背后的算力或质押很少，改写最近的区块就可能代价不高，这就是所谓的51%攻击。安全性取决于作弊需要付出多大代价，而这个代价在不同链之间差别很大。

误解4：“上了区块链就是真的”

真相：区块链能证明一条记录自写入以来没有被改动过，但不能证明这条记录一开始就是正确的。如果供应商在一箱普通蔬菜旁边写上“有机”，链就会忠实地永远保存这个虚假的说法。

这有时被称为**预言机问题**：每当价格、交货或所有权等现实世界的事实进入区块链时，都得有人来报告，而这个人必须被信任。当资产完全存在于链上时，比如比特币本身，链的作用才最强。

误解5和6：“比特币浪费能源”与“区块链又快又免费”

能源方面的真相：比特币挖矿确实耗电很多，根据剑桥大学2025年的一项研究，每年约138太瓦时，大约占全球用电量的0.5%。同一研究发现，其中52.4%来自可持续能源，主要是水电、风电和核电。以太坊这类权益证明网络的耗电量只有其中极小的一部分。这些能源是否值得，仍是一个真正存在争议的问题。

速度方面的真相：公有链在设计上就很慢，因为成千上万台计算机必须达成一致。比特币主链每秒只能处理少量交易，需求激增时手续费就会上涨，正如第11课所示。人们正在其上构建更快的系统，但每一种都要有所取舍。

区块链擅长的	区块链薄弱的
无需中间人转移价值	大规模下的速度和成本
极难篡改的记录	核实现实世界数据是否真实
对任何人开放，难以审查	错误和盗窃无法撤回
人人都能核验规则	隐私，因为一切都是公开的

这对交易者为何重要

- **误解会推动价格。**2021年5月12日，特斯拉以挖矿耗能为由，停止接受用比特币买车，比特币当天下跌约12%。关于能源、犯罪和黑客攻击的报道会一再出现，市场往往在核实事实之前就已作出反应。
- **黑客攻击打击的是代币，不一定是链本身。**当一个跨链桥或交易所被掏空时，相关代币可能暴跌，而底层网络照常运行。在判断这对你持有的币意味着什么之前，先弄清楚到底是什么遭到了攻击。
- **炒作是双向的。**“区块链能解决一切”和“区块链毫无用处”都是很容易写的标题。真正有用的问题总是更具体：这个项目是否需要一份开放的共享记录，它是否真的在使用？

关键术语

假名性	用地址代替姓名。活动是公开的，身份只在地址与某个人对应起来之前保持隐藏。
跨链桥	在两条区块链之间转移代币的服务，常在一处存放大量资金，因此经常成为攻击目标。
51%攻击	某人控制了一条链的大部分算力或质押，并利用它改写最近区块的攻击。
预言机问题	把现实世界的信息放上区块链时，难以避免必须信任报告者的问题。
非法交易量	与诈骗、盗窃、勒索软件和规避制裁等犯罪相关的地址所收到的加密货币价值。
权益证明	通过锁定币而不是挖矿来保护区块链的方式，所需电力少得多。

要点总结

1. 比特币是假名的，而不是匿名的，付款可以被追踪，Colonial Pipeline赎金的追回就说明了这一点。
2. 非法活动以美元计规模很大，但一直低于所追踪加密货币交易量的1%。
3. 比特币账本从未被改写过，但交易所、跨链桥、智能合约和小型链经常遭到攻击。
4. 区块链能让记录保持不变，却无法核实现实世界的数据在写入时是否真实。
5. 比特币耗能很大，公有链在设计上就很慢。了解真正的优势和局限，能让你免受两个方向的炒作影响。

自我测验

请为每道题圈出一个答案。答案及解释在下一页。您也可以在 markettalks.info 在线完成此测验，并立即查看得分。

1. 为什么说比特币是假名的而不是匿名的?

A 交易对矿工以外的所有人都是隐藏的
B 地址上没有姓名，但每笔交易都是公开的，可以被追踪
C 只有交易所能看到区块链
D 用户必须在区块链上登记姓名

2. Chainalysis对2025年非法加密活动有什么发现?

A 它占了全部加密交易量的大部分
B 新规出台后它降到了零
C 至少有1540亿美元，但仍不到所追踪交易量的1%
D 只在比特币上发现

3. 在2022年3月的Ronin黑客事件中，遭到攻击的是什么?

A 比特币区块链本身
B 一个跨链桥，攻击者控制了负责批准提款的大部分密钥
C 所有以太坊钱包同时被攻击
D 一位矿工的硬件

4. 一家供应商把虚假信息记录到区块链上。区块链能保证什么？

A 信息会被自动更正

B 信息是真的，因为它在区块链上

C 这条记录以后不会被改动，尽管它是假的

D 矿工会拒绝虚假数据

5. 根据剑桥大学2025年的研究，比特币挖矿大约占全球用电量的多少？

A 约0.5%

B 约5%

C 约25%

D 超过一半

6. 一个存放热门代币的跨链桥被黑了。对交易者来说，最明智的第一个问题是什么？

A 整条区块链是不是停止运行了？

B 我是不是应该立刻卖掉手里所有的币？

C 是不是所有区块链现在都不安全了？

D 到底是什么遭到了攻击，影响了哪些代币？

答案与解释

1 B

地址上没有姓名，但每笔交易都是公开的，可以被追踪

账本完全公开。一旦某个地址与某个人对应起来，他过去的付款就能被追踪，调查人员追查Colonial Pipeline赎金时正是这样做的。

2 C

至少有1540亿美元，但仍不到所追踪交易量的1%

以美元计金额很大，但与所追踪的全部活动相比，占比仍低于1%。

3 B

一个跨链桥，攻击者控制了负责批准提款的大部分密钥

攻击者夺取了批准跨链桥提款的密钥。底层区块链照常运行。

4 C

这条记录以后不会被改动，尽管它是假的

区块链保护记录不被事后修改，却无法知道一个关于现实世界的说法在写入时是否真实。这就是预言机问题。

5 A

约0.5%

该研究估计每年约138太瓦时，大约占全球用电量的0.5%，其中略多于一半来自可持续能源。

6 D

到底是什么遭到了攻击，影响了哪些代币？

大多数黑客攻击针对的是围绕链构建的服务，而不是链本身。弄清楚被攻击的是什么，才能知道哪些资产真正面临风险。

资料来源

- NPR，美国追回支付给Colonial Pipeline黑客的数百万美元赎金（2021年6月）: https://www.kunc.org/npr-news/2021-06-07/u-s-has-recovered-some-of-the-millions-paid-in-ransom-to-colonial-pipeline-hackers
- The Block，2025年加密犯罪超过1500亿美元（Chainalysis）: https://www.theblock.co/post/384753/crypto-crime-150-billion-usd-2025-state-actors-scale-onchain-chainalysis
- TechCrunch，美国官员将朝鲜Lazarus黑客与Ronin 6.25亿美元盗窃案联系起来: https://techcrunch.com/2022/04/15/us-officials-link-north-korean-lazarus-hackers-to-625m-axie-infinity-crypto-theft
- 剑桥大学贾奇商学院，比特币挖矿中可持续能源占比上升（2025年4月）: https://jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/
- SiliconANGLE，特斯拉停止接受比特币支付后比特币价格暴跌（2021年5月）: https://siliconangle.com/2021/05/12/bitcoin-price-plunges-elon-musk-pulls-support-citing-environmental-concerns/

Market Talks

继续学习

本课属于 MARKET TALKS 教育中心免费的区块链课程，涵盖初级、中级和高级课程，每课都配有测验和可下载的PDF。

教育中心
从基本原理到高级主题的课程

市场分析
主要市场的技术面与基本面分析

报告
比特币、黄金、白银、SPX等

markettalks.info

Telegram @MARKET_TALKS

仅供教育用途。本文件的任何内容均不构成投资建议。© 2026 MARKET TALKS。欢迎在不作修改的前提下分享本PDF。