Market Talks
教育中心

区块链 · 初级 · 第5课，共13课

区块链到底是什么

一个清晰的定义、每条区块链都具备的三个部分，以及那些并不属实的流行说法

阅读约7分钟　　6道测验题，附答案

区块链 · 初级 · 第5课，共13课

区块链到底是什么

一句话概括

区块链是由许多独立电脑共同维护的一份交易记录。新条目以相互链接的批次加入，旧条目无法被悄悄改动，而决定什么能被加入的是共同的规则，而不是某家公司。

一个真正好用的定义

在前四课中，我们追随一个问题，以及寻找答案的漫长过程。现在可以给这个答案一个准确的名字了。去掉炒作，区块链就是：

一份由许多独立电脑共同维护的交易记录：新条目以相互链接的批次加入，旧条目无法被悄悄改动，由共同的规则决定什么可以被加入。

这句话的每一部分都很重要。“许多独立电脑”去掉了第1课中的中间人。“相互链接的批次”是从第3课时间戳研究中发展出来的区块链条。“共同的规则”是第4课的达成一致的方法。去掉其中任何一个，你拥有的就不再是比特币所开创的那种区块链。

这类记录被称为**账本**：一份记载谁在什么时候把什么发给了谁的清单。区块链是记账的一种特定方式，专为参与者彼此并不完全信任的情况而设计。

协同运作的三个部分

可以把每一条公链想象成叠在一起的三层：

- **记录。**交易被打包成区块，每个区块都指向前一个区块，一直追溯到第一个区块。第6课会具体展示这种链接是如何形成的。
- **网络。**成千上万台被称为**节点**的电脑各自保存一份完整的记录，并相互传递新的交易和区块。第7课会详细介绍它们。
- **规则。**每个节点在接受新区块之前，都会用同一套规则检查它。违反规则的区块会被拒绝，无论是谁发送的。选择由谁添加下一个区块的方法叫作**共识**，比特币采用的就是你在第4课认识的工作量证明。

这些部分单独看都不新鲜。数据库、网络和规则检查早在2008年之前就已存在。区块链的不同之处在于把它们组合在一起，并且没有任何一方能控制这三者中的任何一个。

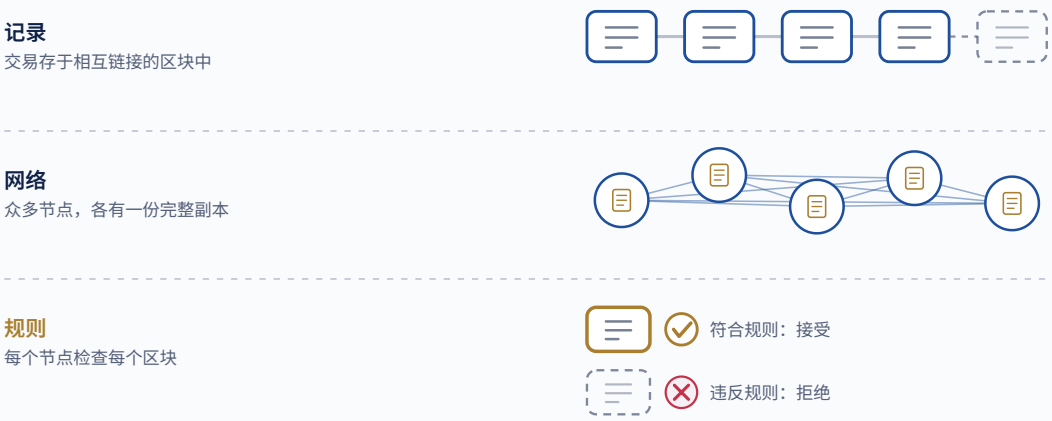


图1. 区块链结合了三个部分：由相互链接的区块组成的记录、由独立副本组成的网络，以及每个节点用来接受或拒绝新区块的共同规则。

里面到底装着什么

常见的想象是一个装满硬币的巨大金库。实际上它更像一份非常长的转账清单。一个比特币区块主要包含交易，每笔交易实质上都在说“这些币从这里转到那里”，外加一个把它与前一个区块相连的小区块头。

任何地方都没有一行写着“爱丽丝拥有2个比特币”。你的钱包通过查看与你的地址相关的所有历史交易来计算余额。你的余额是历史的结果，而不是某人单独保存、可以随意修改的一个数字。

名字也不会被保存。交易指向的是**地址**，即一长串字母和数字。这让比特币成为**假名**的，而不是匿名的：任何人都能看到每个地址做过什么，只是无法自动知道背后是谁。第8课会解释地址从何而来。

亲自查一查

第一笔人与人之间的支付，也就是中本聪在2009年1月发给哈尔·芬尼的10个比特币，就在第170号区块里。打开任意一个免费的区块浏览器网站，搜索区块170，你就能找到它，17年多过去了依然原封未动。世界上每一个全节点仍然保存着这同一笔交易。

四个重要特性

像比特币这样的公链具有四个普通系统通常不具备的特性：

- **只增不改。**新条目可以添加到末尾，旧条目永远不会被编辑或删除。出错时用一笔新交易来纠正，而不是抹掉旧的。

- **多副本。**同一份完整记录存在于许多国家的成千上万台机器上。失去其中一部分不会改变任何事情。
- **透明。**任何人都可以下载这份记录，阅读有史以来的每一笔交易，无需任何人许可。
- **无需许可。**任何人都可以发送交易或运行节点，不需要注册或审批。第12课会介绍私有链，那里情况并非如此。

类比：没人能编辑的群聊

想象一个群聊：每位成员的手机都保存完整的聊天记录，消息永远不能编辑或撤回，而一条新消息只有在大多数手机确认它符合群规之后才会出现。你可以从自己的手机上删除这个应用，但对话会在其他所有地方继续。想要改动去年说过的话，你就得同时在成千上万部手机上改动它。

区块链不是什么

区块链总是伴随着各种夸大的说法。有几条值得尽早纠正：

- **它不是更快或更便宜的数据库。**让成千上万个副本保持一致本来就是刻意设计得又慢又贵的。对于大多数日常软件来说，普通数据库是更好的选择。
- **它并非无法被黑。**比特币的记录本身已被证明极难攻击，但围绕区块链构建的交易所、钱包和应用却经常遭到黑客攻击。大多数损失发生在那里，而不是链上。
- **它不是真相机器。**区块链能证明某个条目被记录过且未被改动，却无法证明这个条目一开始就是真的。如果输入的是虚假信息，链会忠实地保存一份虚假记录。

	普通数据库	公链
谁可以添加记录	所有者及其批准的人	任何遵守规则的人
修改旧记录	可以，而且往往不为人知	不可能在所有人都看不到的情况下修改
谁保存副本	所有者	成千上万个独立节点
谁可以读取	所有者允许的人	任何人
速度与成本	快且便宜	较慢且较贵
如果运营者消失	系统停止运行	网络继续运行

这对交易者为何重要

- **交易所余额不在区块链上。**当你在交易所买入比特币时，这笔交易记录在交易所自己的数据库里。区块链只能看到充值和提现。2022年11月FTX倒闭时，客户屏幕上显示的余额是公司无力兑付的。第10课会讲如何看待这种风险。
- **公开数据就是交易数据。**由于记录是透明的，任何人都能关注大额转账、币流入或流出交易所，以及沉睡多年的钱包。许多交易者会使用这些链上数据，高级阶段还有一整课专门讲解。
- **这个词本身就能撬动市场。**2017年12月，Long Island Iced Tea公司更名为Long Blockchain，股价在几个小时内翻了几倍，而背后并没有任何真正的区块链业务。后来美国证交会撤销了该股票的注册，并以内幕交易罪起诉了三个人。理解区块链是什么，能帮助你一眼识破炒作。

关键术语

账本	记载谁在什么时候把什么发给了谁的记录。区块链是记账的一种方式。
节点	保存一份区块链副本、按规则检查新区块并与其他节点共享的电脑。
共识	区块链网络就下一个添加哪个区块达成一致的方法。比特币使用工作量证明。
只增不改	可以添加新条目，但旧条目永远不能被编辑或删除的记录。
假名	与地址而非真实姓名相关联。活动是公开的，但背后的人不会被自动识别。
无需许可	对所有人开放，发送交易或运行节点都无需注册或审批。

要点总结

1. 区块链是由许多独立电脑共同维护的交易记录，以相互链接的批次加入，并受共同规则约束。
2. 每条公链都有三个部分：记录、节点网络，以及决定什么可以被加入的规则。
3. 区块里装的是交易，而不是余额或姓名。你的余额是根据你的地址的完整历史计算出来的。
4. 公链具有只增不改、多副本、透明和无需许可的特性。

5. 区块链不是更快的数据库，并非无法被黑，也不是真相机器。它证明条目未被改动，而不证明条目为真。

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. 以下哪种对区块链的描述最准确？

A 一个存放数字硬币的安全金库
B 一份由许多独立电脑按照共同规则共同维护的交易记录
C 一种由科技公司运营的更快的数据库
D 一个人们买卖加密货币的网站

2. 每条公链结合了哪三个部分？

A 硬币、钱包和交易所
B 矿工、银行和监管机构
C 记录、节点网络和规则
D 密码、服务器和备份

3. 你的钱包如何知道你的比特币余额？

A 把与你的地址相关的所有历史交易加总
B 读取每个区块中保存的余额行
C 询问运营比特币的公司
D 在区块链里查找你的名字

4. “只增不改”是什么意思？

A 只有经过批准的用户才能添加记录
B 记录在一段时间后会被删除
C 只能读取最新的区块
D 可以添加新条目，但旧条目永远不会被编辑或删除

5. 为什么说比特币是假名的而不是匿名的?

A 因为交易对公众隐藏

B 因为活动是公开的并与地址相关联，但不会自动与真实姓名关联

C 因为用户必须用真实姓名注册

D 因为只有矿工能看到交易

6. 关于区块链，哪种说法是正确的?

A 区块链能证明其中的信息是真的

B 区块链比普通数据库更快更便宜

C 区块链能证明条目未被改动，但不能证明它在录入时是真的

D 围绕区块链构建的任何东西都不会被黑

答案与解释

1 B

一份由许多独立电脑按照共同规则共同维护的交易记录

区块链是一份共享账本。许多独立电脑保存副本，新条目以相互链接的区块加入，由共同规则决定什么可以进入。

2 C

记录、节点网络和规则

记录保存相互链接的区块，节点网络保存并共享副本，规则决定哪些区块被接受。

3 A

把与你的地址相关的所有历史交易加总

区块保存的是转账，而不是余额。你的余额是根据所有转入和转出你的地址的交易历史计算出来的。

4 D

可以添加新条目，但旧条目永远不会被编辑或删除

在只增不改的记录中，历史只会增长。出错时用一笔新交易纠正，而不是修改旧交易。

5 B

因为活动是公开的并与地址相关联，但不会自动与真实姓名关联

任何人都能看到一个地址的每一笔交易。无法自动知道的，是这个地址背后的真实的人。

6 C

区块链能证明条目未被改动，但不能证明它在录入时是真的

区块链保护记录不被改动。如果录入的是虚假信息，它同样会忠实地保存这份虚假记录。

资料来源

- 中本聪，Bitcoin: A Peer-to-Peer Electronic Cash System（2008）: https://bitcoin.org/bitcoin.pdf
- 吉尼斯世界纪录，第一笔比特币交易: https://guinnessworldrecords.com/world-records/696243-first-bitcoin-transaction
- Fortune，美国证交会就Long Blockchain更名事件提起内幕交易指控（2021年7月）: https://fortune.com/2021/07/09/sec-insider-trading-long-blockchain
- CoinDesk，美国证交会将Long Blockchain公司股票摘牌: https://www.coindesk.com/long-blockchain-corporation-shares-delisted-sec

Market Talks

继续学习

下一课：第6课
通俗讲解区块与哈希

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。