Market Talks
教育中心

区块链 · 初级 · 第4课，共13课

2008年与比特币的诞生

一篇九页的论文，一条藏在第一个区块里的报纸头条，以及一位悄然离开的创造者

阅读约8分钟　　6道测验题，附答案

区块链 · 初级 · 第4课，共13课

2008年与比特币的诞生

一句话概括

2008年，一位名叫中本聪的匿名作者把早期实验留下的拼图组合起来，解决了它们都没能解决的那个问题：如何让互不相识的人在没有任何主管方的情况下，就同一份历史达成一致。

危机之中的九页纸

2008年9月，投资银行雷曼兄弟倒闭，世界各国政府纷纷动用公共资金救助本国银行。人们对金融体系的信任跌到了谷底。

六周后，2008年10月31日，一封邮件出现在一个由密码学家阅读的邮件列表中。署名**中本聪**（Satoshi Nakamoto）的作者宣布了一种新型电子现金：它在用户之间直接运作，无需任何可信第三方。邮件附上了一篇短论文的链接：*Bitcoin: A Peer-to-Peer Electronic Cash System*（《比特币：一种点对点的电子现金系统》）。全文只有九页。

这篇论文并不掩饰自己的来源。它引用了b-money、Hashcash，以及你在第3课认识的时间戳研究。它新增的，是一种让这些部件协同运作的方法，中心不需要公司、银行或可信服务器。列表上的许多读者心存怀疑：有人认为它永远处理不了足够多的支付，也有人干脆置之不理。

补上缺失的那一块

第3课留下了一个悬而未决的问题：如果成千上万台独立的电脑各自保存一份记录，在没有人主管的情况下，它们如何就哪个版本正确达成一致？比特币的答案分为三部分。

第一，支付被打包成一批批的**区块**，每个区块都与前一个区块相连，就像第3课中的时间戳链。第二，添加下一个区块的权利通过**工作量证明**来赢得，这正是Hashcash最早使用的思路。被称为**矿工**的电脑竞相解一道谜题，获胜者的区块会先经所有人检查，然后大家再在它之后继续构建。第三，如果历史出现两个相互竞争的版本，每台电脑都会跟随背后工作量最多的那条链。

这些规则结合在一起，让作弊的代价变得极其高昂。要改写一笔已经埋在链中的支付，攻击者必须重做那个区块以及之后每一个区块的工作，而且速度要比全网其余部分加起来还快。获胜的矿工还会得到新创造的比特币作为奖励，因此保护记录的同一份工作也同时发行了货币。这两件事都不需要任何公司。



图1. 有时两位矿工几乎同时找到一个区块。网络会在工作量最多的链上继续构建，竞争区块则被舍弃。

类比：昂贵的抽奖

想象一本大家共用的笔记本，每次只能由一个人来写。为了决定谁写下一页，所有人都去买抽奖券，而每张券都要花费真实的电费。大约每十分钟抽出一位赢家。想伪造旧页的人必须一次又一次中奖，也就是要买下比其他所有人加起来还多的券。诚实的书写者会一直中奖，因为他们的人数多得多。

2009年1月3日：第一个区块

2009年1月3日，中本聪创建了比特币链上的第一个区块，即**创世区块**。它的奖励是50个比特币，而由于代码中的一个特殊之处，这些币永远无法花费。六天后，软件发布，任何人都可以下载运行。

2009年1月12日，中本聪向哈尔·芬尼发送了10个比特币，他正是第3课中RPOW的作者。这是网络上第一笔人与人之间的支付。此后的好几个月里，用户只是一小群在家用电脑上运行程序的爱好者。

藏在第一个区块里的信息

中本聪在创世区块中写入了一行文字：*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*（《泰晤士报》2009年1月3日：财政大臣即将对银行实施第二轮救助）。这是那家英国报纸当天的头版标题。就像第3课中刊登在报纸上的指纹一样，它证明这个区块不可能早于那一天被创建。许多人也把它看作对比特币诞生原因的一种注解。

从第一天就写定的规则

与DigiCash或e-gold不同，比特币没有决定发行多少货币的发行方。供应遵循从一开始就内置在软件中的规则：

- **大约每10分钟一个新区块。**每2,016个区块，也就是大约每两周，谜题会自动变难或变易，以维持这一节奏，无论矿工增加还是减少机器。

- **不断减少的奖励。**每个区块的奖励最初是50个比特币，每210,000个区块减半一次，大约每四年一次。这一事件被称为**减半**。2024年4月减半之后，奖励为3.125个比特币。
- **固定的上限。**由于奖励不断减半，总供应量永远不会超过2,100万个比特币。最后的零头预计将在2140年前后被挖出。

改变这些规则不是某一个人能做到的。网络中的每台电脑都会按照自己运行的规则检查每一个区块，违反规则的区块会直接被拒绝。第7课会更详细地介绍这些电脑。

从爱好到第一个价格

2009年的大部分时间里，比特币根本没有价格。2009年10月，一位自称New Liberty Standard的用户公布了第一个美元汇率：1美元兑1,309.03个比特币。他是通过计算自己的电脑挖矿所耗的电费得出这个数字的。

2010年5月22日，佛罗里达州的程序员拉斯洛·汉耶茨（Laszlo Hanyecz）用10,000个比特币买了两个披萨，这是用这种货币购买实物商品的最早案例之一。2010年间，第一批交易所陆续出现，比特币开始拥有每天变动的市场价格。一个交易市场就此诞生。

悄然离开的创造者

中本聪从未透露真实姓名、长相或所在地，只通过论坛帖子和电子邮件交流。2010年间，中本聪逐步把代码的控制权交给其他志愿开发者。最后一条得到确认的消息，是一封日期为2011年4月23日的邮件，信中说中本聪已经“转向其他事情”。这个名字背后的身份至今仍是谜。

研究最早期区块的人估计，有一位矿工在第一年里收集了约110万个比特币，许多人认为他就是中本聪。这些证据只是间接的，而这些币从未被移动过。

这次消失后来被证明意义重大。DigiCash和e-gold都有创始人和公司，可能破产、被起诉或受到施压。比特币两者都没有：没有可以关闭的总部，也没有一个所有人都必须服从其决定的领导者。

早期的弱点	比特币的答案
数字货币可以被复制	每笔支付都要对照同一份共享历史进行检查
由一家公司决定有多少货币	新币只按软件中的固定规则产生
靠一台可信服务器阻止双重支付	成千上万台独立电脑检查每一个区块
没有领导者就无法达成一致	工作量证明决定谁添加下一个区块，工作量最多的链胜出
创始人可能被起诉或受到施压	一位已经离开的匿名创造者

这对交易者为何重要

- **危机是故事的一部分。**比特币诞生于一场银行危机之中，第一个区块里就写着银行救助的头条。每当银行承压，这个故事就会重新浮现。2023年3月，美国多家银行倒闭，比特币大幅上涨，因为部分投资者在寻找银行体系之外的资产。这类叙事能够推动价格，即使影响并不持久。
- **供应时间表是公开的。**每次减半的日期都可以提前多年估算，许多交易者会跟踪围绕减半的大约四年周期。请记住，已知的事件可能早已被计入价格，过去的周期也不能保证下一个周期。
- **早期的币受到密切关注。**最早几年的币只要一移动就会成为新闻。2026年9月，600个挖于2010年的比特币在沉寂16年后被转移，分析人士很快发现它们与中本聪没有明确关联。在对头条做出反应之前先查看链上证据，可以帮你避免根据传闻交易。

关键术语

白皮书	一份简短的文件，说明一个新系统或项目打算如何运作。比特币白皮书只有九页。
创世区块	一条区块链的第一个区块。比特币的创世区块创建于2009年1月3日。
矿工	通过工作量证明竞争添加下一个区块、以换取奖励的电脑或其运营者。
区块奖励	获胜矿工因添加一个区块而获得的新比特币。所有新比特币都是这样产生的。
减半	每210,000个区块，即大约每四年，区块奖励减少一半。
最大工作量链	当历史的不同版本相互竞争时，网络跟随背后工作量证明最多的那个版本的规则。

要点总结

1. 中本聪于2008年10月31日、银行危机最严重之时，发布了九页的比特币白皮书。
2. 比特币结合了连成链的区块、工作量证明和最大工作量规则，让互不相识的人在无人主管的情况下就同一份历史达成一致。
3. 2009年1月3日的创世区块载有一条关于银行救助的报纸头条，证明了它的创建日期。
4. 新比特币只来自区块奖励，奖励大约每四年减半一次，总量永远不会超过2,100万。

5. 中本聪于2011年离开，从未透露身份，没有留下任何可以被关闭的创始人或公司。

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. 比特币白皮书是什么时候发布的?

A 2009年1月
B 2008年10月31日
C 2010年5月
D 2011年4月

2. 如果区块链的两个版本相互竞争，网络会跟随哪一个?

A 由最老的电脑创建的那个
B 由交易所投票选出的那个
C 背后工作量证明最多的那个
D 包含支付最多的那个

3. 创世区块中的报纸头条证明了什么?

A 这个区块不可能早于2009年1月3日被创建
B 有一家银行批准了比特币
C 中本聪住在英国
D 最早的比特币以英镑为支撑

4. 新比特币是如何产生的?

A 由中央银行按需印发
B 由中本聪每年发放
C 需求上升时由交易所创造
D 矿工添加区块时作为奖励获得

5. 减半时会发生什么?

A 比特币价格减半

B 添加一个区块的奖励减半

C 所有比特币中的一半被销毁

D 区块添加速度加快一倍

6. 为什么中本聪的消失对比特币有帮助?

A 它让挖比特币变得更便宜

B 它取消了系统中的所有规则

C 它没有留下任何可以被关闭或施压的创始人或公司

D 它让中本聪可以秘密卖币

答案与解释

1 B

2008年10月31日

中本聪于2008年10月31日在一个密码学邮件列表中分享了这篇九页的论文，大约在雷曼兄弟倒闭六周之后。

2 C

背后工作量证明最多的那个

每台电脑都跟随背后工作量最多的链。要取代它，攻击者需要的算力必须超过全网其余部分的总和。

3 A

这个区块不可能早于2009年1月3日被创建

这条头条刊登于2009年1月3日，所以区块不可能比这一天更早。中本聪是谁、住在哪里，至今仍不得而知。

4 D

矿工添加区块时作为奖励获得

区块奖励是新比特币产生的唯一途径。它遵循软件中的固定规则，因此没有人能决定多发行。

5 B

添加一个区块的奖励减半

每210,000个区块，即大约每四年，区块奖励减半一次。这就是总供应量永远不会超过2,100万的原因。

6 C

它没有留下任何可以被关闭或施压的创始人或公司

DigiCash和e-gold都随着各自的公司一起倒下。没有已知的领导者，比特币就没有可以关闭的总部，也没有一个所有人都必须服从的人。

资料来源

- 中本聪，Bitcoin: A Peer-to-Peer Electronic Cash System（2008）: https://bitcoin.org/bitcoin.pdf
- 密码学邮件列表，Bitcoin P2P e-cash paper（2008年10月31日）: https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
- Cointelegraph，创世区块周年：比特币十岁了: https://cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block
- Bitcoin Magazine，比特币自首次以美元定价以来上涨65亿个百分点: https://bitcoinmagazine.com/culture/bitcoin-is-up-6-5-billion-percent-since-it-was-first-priced-in-usd
- The Defiant，中本聪于2011年4月23日发给迈克·赫恩的最后一封邮件: https://thedefiant.io/news/people/bitcoin-creator-satoshi-nakamoto-sent-final-email-to-mike-hearn-on-april-23-2011-6735013c
- Cointelegraph，中本聪真的拥有100万个比特币吗？: https://cointelegraph.com/news/big-questions-does-satoshi-actually-own-1-million-bitcoin

Market Talks

继续学习

下一课：第5课
区块链到底是什么

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。