Market Talks
教育中心

区块链 · 初级 · 第3课，共13课

比特币之前：数字现金的种种实验

二十五年的尝试、险些成功与失败，以及每一次留给比特币的那块拼图

阅读约8分钟　6道测验题，附答案

区块链 · 初级 · 第3课，共13课

比特币之前：数字现金的种种实验

一句话概括

比特币并非凭空出现。它融合了早期数字现金项目的想法，并且在设计上避开了让其中大多数项目失败的那个共同弱点。

比网页浏览器还早的梦想

在第1课和第2课中，我们认识了两个问题：数字货币可以被复制，而由单一方运营的系统可能被冻结、关闭或腐化。早在比特币出现之前，密码学家和创业者就已经在尝试同时解决这两个问题。

他们的项目从20世纪80年代初一直延续到21世纪头十年中期。有些成了拥有真实客户的真实企业，有些始终停留在纸面上。没有一个完全成功，但几乎每一个都贡献了比特币后来用到的东西。追溯它们的故事，是理解比特币为何如此构建的最好方法。



图1. 在比特币之前，已有超过25年的数字现金实验。每一次都为最终设计留下了一块拼图。

DigiCash：隐私有了，却由一家公司掌控

1982年，密码学家大卫·乔姆（David Chaum）提出了一种名为**盲签名**的技术。它让银行可以为一枚数字硬币签名、确认其有效，却看不到自己签的是哪一枚。结果就是一种可以像现金一样私密花费的数字货币，因为银行无法把一笔付款与取出这枚硬币的人联系起来。

乔姆于1989年创立DigiCash，把这一想法变成产品；1995年，圣路易斯的马克·吐温银行开始向客户提供它的eCash。技术是可行的，生意却不行：加入的银行和商家太少，DigiCash于1998年申请破产。

更深层的弱点在于结构本身。每一枚硬币仍然必须由一家中央银行或公司发行，而检查双重支付的也是这同一个中心方。公司倒下时，钱也随之消失。

e-gold：真实背书，单点故障

1996年推出的e-gold走了另一条路。每一个单位都由存放在金库中的实物黄金背书，用户可以在几秒钟内把以黄金为支撑的余额发送到世界各地。它增长迅速：到2006年，每年处理的支付超过20亿美元。

但e-gold是一家公司，这也让它成了一个靶子。缺乏身份核查使它吸引了犯罪分子，美国当局于2007年起诉了该公司及其董事。2008年，他们承认共谋洗钱以及经营无牌汇款业务的罪名；2009年，转账被暂停。账户持有人等了好几年，才等到追回资金的程序。

第2课的道理在现实中上演：单一控制点同时也是单点故障，不论原因是黑客、破产还是法院命令。

Hashcash：故意让事情变得昂贵

1997年，密码学家亚当·贝克（Adam Back）提出了**Hashcash**，用来防御垃圾邮件。发送邮件之前，发件人的电脑必须解一道小谜题，花费片刻的计算工作。对一封邮件来说，这个成本几乎察觉不到；但对要发送数百万封邮件的垃圾邮件发送者来说，成本会迅速累积。

巧妙之处在于不对称：谜题解起来慢，验证起来却是瞬间的。任何收到邮件的人都能确认工作已经完成，而无需重做一遍。这一思想被称为**工作量证明**（proof of work），比特币白皮书明确将Hashcash列为直接影响来源。

> **类比：数独测试**
>
> 一道难的数独可能要花一小时才能解出，但检查一张填好的格子只需一分钟。如果有人递给你一道已完成的数独，你就知道他下了功夫，即使你从没看到他是怎么做的。工作量证明把这个想法变成了一枚数字化的“努力印章”，任何电脑都能验证。

b-money、Bit Gold 与 RPOW：蓝图

1998年，有两个方案在纸面上与比特币惊人地接近。计算机工程师戴伟（Wei Dai）描述了**b-money**：每个参与者都保存一份“谁拥有什么”的记录副本，新钱通过解决计算问题来创造。差不多同一时期，法律学者兼计算机科学家尼克·萨博（Nick Szabo）提出了**Bit Gold**，它把工作量证明的解与时间戳串联起来，创造出一种稀缺且生产成本高的东西，一种数字黄金。

两者都从未真正上线。它们都留下了一个重要问题：如果许多互相独立的人都在保存记录，在没有人主管的情况下，他们如何就哪份记录正确达成一致？

2004年，密码学家哈尔·芬尼（Hal Finney）构建了**RPOW**（可重复使用的工作量证明），让工作量证明代币可以在人与人之间传递。它确实运行起来了，但为了防止双重支付，它依赖一台运行在特殊安全硬件上的可信服务器。中心仍然站着一个可信方。五年后，芬尼收到了历史上第一笔由一个人发给另一个人的比特币。

时间戳之链

还有一块拼图来自货币世界之外。1991年，研究人员斯图尔特·哈伯（Stuart Haber）和W.斯科特·斯托内塔（W. Scott Stornetta）思考的问题是：如何证明一份数字文档是何时创建的，并且此后没有被改动过。

他们的答案是把记录连成一条链。每条新记录都带着前一条记录的数字指纹，因此改动任何一条旧记录，都会破坏其后的每一个环节。历史由此变得**篡改可见**：你仍然可以尝试改写它，但所有人都会看到你这么做了。比特币白皮书三次引用了他们的工作，而以这种方式连接记录的想法，成了区块链中的“链”（chain）。第6课会详细解释这些指纹是如何运作的。

真实案例

为了让自己的链无法被悄悄改写，哈伯和斯托内塔的公司从1995年开始，把最新记录的指纹刊登在《纽约时报》的分类广告栏里。任何人都可以拿印刷的报纸与链进行比对，而没有人能在事后修改成千上万份已印刷的报纸。

缺失的那一块

到21世纪头十年中期，几乎所有部件都已存在。仍然缺少的，是最难的那一块：

项目	它带来了什么	还缺什么
DigiCash（1989）	私密的数字支付	依赖一个中央发行方
时间戳链（1991）	记录相互链接，历史无法被悄悄改动	并非为货币而设计
e-gold（1996）	大规模的全球转账	一家可以被关停的公司
Hashcash（1997）	工作量证明：创建昂贵，验证便宜	不是货币，只是一枚印章
b-money、Bit Gold（1998）	共享记录，以及通过工作创造的货币	没有领导者就无法达成一致；从未上线
RPOW（2004）	可以转手的工作量证明代币	依赖一台可信服务器

每一次尝试，要么依赖一个主管方，要么从未解决陌生人如何在没有主管方的情况下就同一份历史达成一致。2008年，一位匿名作者把这些拼图拼到一起，并补上了缺失的那一块。这就是第4课的故事。

这对交易者为何重要

- **中心化发行方的失败方式似曾相识。**DigiCash破产，e-gold被检方关闭。2013年同样的模式再次出现：美国当局关闭了另一种中心化运营的数字货币Liberty Reserve。任何依赖单一发行方的资产，都背负着该发行方的经营风险和法律风险。
- **今天的稳定币与e-gold相似。**以美元为支撑的稳定币遵循类似的模式：一家公司持有储备，并据此发行代币。因此，在依赖某个稳定币之前，值得先了解其发行方的储备、牌照和法律地位。
- **“数字黄金”的叙事源远流长。**Bit Gold关于“因为创造成本高所以稀缺”的想法，至今仍影响着许多投资者如何把比特币与黄金相比较。了解一个叙事从何而来，有助于你在它推动市场时判断它值得多大的分量。

关键术语

盲签名	银行或发行方批准一枚数字硬币、却看不到自己批准的是哪一枚的方法，使支付得以保持私密。
工作量证明	证明一台电脑为解一道谜题付出了真实努力。生成很慢，验证瞬间完成。
资产背书	价值由发行方持有的真实资产（如黄金或美元）支撑的货币或代币。
时间戳	证明一条数字记录何时创建，并且此后没有被改动。
篡改可见	一种设计，使对过往记录的任何改动都对所有人可见，即使在物理上无法阻止改动。
数字稀缺性	某种数字事物的有限供应，无法被简单复制或免费创造。

要点总结

1. 数字现金实验始于20世纪80年代初，比比特币早了25年以上。
2. DigiCash带来了隐私，e-gold带来了全球规模，但两者都依赖一家公司，也随公司一同倒下。

3. Hashcash引入了工作量证明：生成缓慢、验证瞬间的努力。
4. b-money、Bit Gold和RPOW勾勒出共享记录和基于工作的货币，但都没有解决陌生人如何在没有可信方的情况下达成一致。
5. 相互链接的时间戳展示了如何让历史篡改可见。比特币把这些拼图组合起来，并补上了缺失的那一块。

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. DigiCash背后的关键创新是什么?

A 存放在金库里的黄金
B 让数字支付保持私密的盲签名
C 用来阻止垃圾邮件的工作量证明
D 每个用户都保存一份副本的账本

2. e-gold为什么走向终结?

A 针对运营它的那一家公司的法律行动
B 它的黄金储备被盗
C 一个漏洞让用户可以复制硬币
D 它的用户转投了比特币

3. Hashcash最初是为了做什么而设计的?

A 让网上支付保持私密
B 保存以黄金为支撑的余额
C 让发送垃圾邮件变得昂贵
D 为法律文件加时间戳

4. 哪一个特性让工作量证明有用?

A 任何人都能瞬间生成
B 只有中央服务器才能检查
C 很容易复制
D 生成缓慢，但验证瞬间完成

5. 哈伯和斯托内塔1991年的工作贡献了什么?

A 以黄金为支撑的数字货币
B 把记录连成一条链，使改动历史变得可见
C 匿名电子邮件
D 第一家加密货币交易所

6. 2008年之前，还缺哪一块拼图?

A 更快的网络连接
B 让支付保持私密的方法
C 让陌生人在无人主管的情况下就同一份共享历史达成一致的方法
D 足以进行工作量证明的强大电脑

答案与解释

1 B

让数字支付保持私密的盲签名

大卫·乔姆的盲签名让银行可以批准一枚硬币而看不到是哪一枚，因此支付可以像现金一样保持私密。

2 A

针对运营它的那一家公司的法律行动

e-gold由一家公司运营。检方起诉后，该公司及其董事于2008年认罪，转账于2009年暂停。一家公司就意味着一个单点故障。

3 C

让发送垃圾邮件变得昂贵

亚当·贝克提出Hashcash是为了对抗垃圾邮件。每封邮件需要一点计算工作：对一封邮件微不足道，对数百万封邮件则非常昂贵。

4 D

生成缓慢，但验证瞬间完成

就像一道已完成的数独，工作量证明创建时需要付出努力，检查却只需片刻。这让任何人都能确认工作已完成，而无需重做。

5 B

把记录连成一条链，使改动历史变得可见

每条记录都带有前一条记录的指纹，所以改动一条旧记录会破坏其后的每一个环节。这个想法成了区块链中的“链”。

6 C

让陌生人在无人主管的情况下就同一份共享历史达成一致的方法

早期系统要么依赖可信方，要么从未解决许多独立参与者如何就同一份记录达成一致。比特币补上了这缺失的一块，第4课会详细讲解。

资料来源

- 美国司法部，e-gold认罪（2008年7月）: https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
- 维基百科，DigiCash: https://en.wikipedia.org/wiki/DigiCash
- 维基百科，e-gold: https://en.wikipedia.org/wiki/E-gold
- Satoshi Nakamoto Institute，哈尔·芬尼：RPOW: https://nakamotoinstitute.org/finney/rpow/
- Cointelegraph，区块链共同发明人谈他为何不是中本聪: https://cointelegraph.com/news/co-inventor-of-blockchain-on-why-he-is-not-satoshi-nakamoto

Market Talks

继续学习

下一课：第4课
2008年与比特币的诞生

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。