Market Talks

教育中心

区块链 · 初级 · 第1课，共13课

信任问题

为什么每一笔数字支付都需要中间人，以及区块链为何被发明出来改变这一点

阅读约7分钟　　6道测验题，附答案

区块链 · 初级 · 第1课，共13课

信任问题

一句话概括

如今，每一笔数字支付都依赖一个受信任的中间人来记账。区块链则尝试建立一个无需信任任何人的共享账本。

钱是一条记录，而不是一件实物

您拥有的大部分钱并不是抽屉里的现金，而是银行数据库中的一个数字。当您从账户向别人付款时，没有任何实物被转移。您的银行在记录中减少一条数字，收款人的银行则增加另一条。

所以，您真正持有的是一个*承诺*：银行承诺其记录准确无误，并会在您需要时兑现。银行卡余额、支付应用以及存放在交易所的资金也是如此。从本质上说，数字货币就是由某一方保管的一条记录。

我们为什么依赖中间人

想象一下，您要向世界另一端一位素未谋面的卖家付款。您无法查看对方的记录，对方也无法查看您的记录，你们都没有理由信任彼此。中间人通过同时承担三项职能来解决这个问题：

- **保管官方记录**，记录谁拥有什么。
- **核查每一笔付款**，例如确认您确实拥有要汇出的资金。
- **处理争议**，包括撤销错误和欺诈交易。

银行、银行卡网络、支付应用和交易所都扮演着这一角色。在大多数情况下，这种安排运作良好，这也正是它主导金融世界的原因。

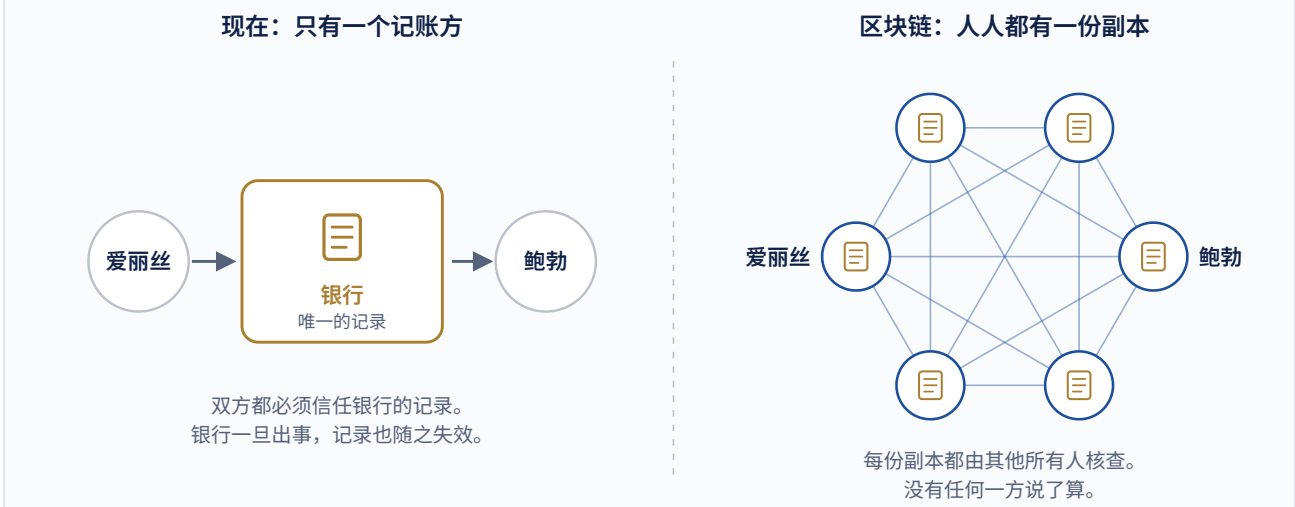


图1。有中间人时，只有一方持有唯一的记录。在区块链中，每个参与者都持有并核查一份完全相同的副本。

信任他人的隐性成本

依赖中间人很方便，但从来都不是免费的。其成本体现在四个方面：

- **费用和延迟。**一笔国际汇款可能要经过一连串银行，每家都会增加时间和费用。据世界银行统计，2025年初向海外汇款200美元的平均成本为6.49%，是3%全球目标的两倍多。
- **准入限制。**中间人可以冻结、关闭或拒绝开设账户。据世界银行统计，全球仍有超过10亿成年人完全没有银行账户。
- **单点故障。**一旦中间人遭到黑客攻击、服务中断或倒闭，所有依赖它的人都会同时受到影响。
- **无法核查的记录。**您只能看到中间人选择向您展示的余额，无法亲自审计它的账目。

这并不意味着银行不好，而是说明信任是有代价的，无论您是否意识到，都在为此付费。

真实案例

2022年11月，加密货币交易所FTX崩溃并申请破产。原以为自己在平台上持有比特币和美元的客户发现，他们实际上只持有对一家濒临破产公司的债权。在破产程序进行期间，他们的资金被冻结了数年。

为什么不直接创造数字货币？双重支付问题

数字内容可以被完美复制。当您通过电子邮件把一张照片发给朋友时，您并不会失去这张照片，现在你们俩都有了。对照片来说这没什么问题，但对钱来说却是灾难。如果钱只是一个文件，您就可以把同一个文件发给一百个人，用它向所有人付款。

一枚实体硬币不可能同时出现在两个口袋里，但数字货币可以，除非有某种机制阻止它。这就是**双重支付问题**，它是数字货币面临的核心挑战。

在2008年之前，唯一可靠的解决办法是由一个中央记账方来判断哪笔付款在先，并拒绝副本。因此，每一次创造数字现金的尝试仍然需要中间人，而当这个中间人失败或被关闭时，这种货币也随之消失。我们将在第3课介绍这些早期尝试。

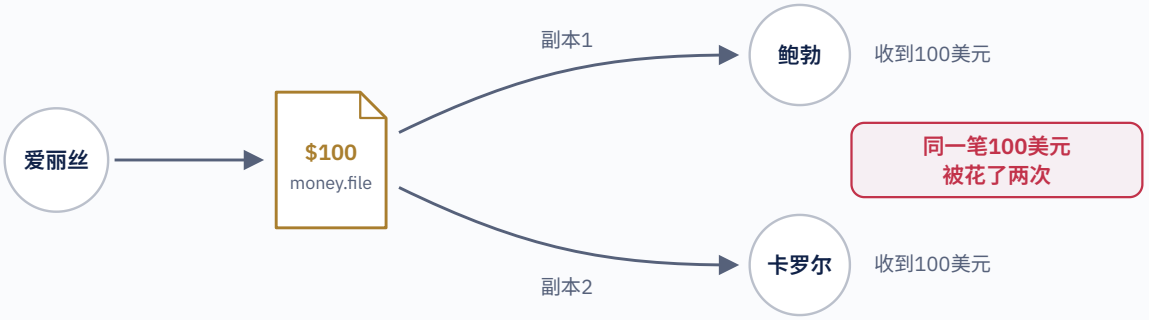


图2。数字文件可以被复制，因此如果没有防护措施，同一笔钱可能同时被发给两个人。

区块链要回答的问题

把以上内容综合起来，我们会得出一个问题：

> 一群互不信任的陌生人，能否在没有任何人负责的情况下，共同维护一份所有人都认可的记录？

这正是区块链要解决的问题。2008年，一篇署名中本聪的论文提出了解决方案，几个月后比特币正式上线。我们将在第4课讲述这段历史。

简而言之，核心思路是：

- 不再由一个保管方持有唯一的记录，而是由任何愿意的人持有**许多完全相同的副本**。
- 每一条新记录都**由所有人**按照同一套公开规则**进行核查**。
- 修改过去的记录**代价极其高昂**，因此历史记录值得信赖。

信任从机构转移到规则、数学和公开验证上。加密社区用一句话来概括：*不要信任，去验证。*

类比：共享表格

想象一个由某家公司托管的在线表格。这家公司可以把您挡在门外、修改其中的行，或者弄丢文件。再想象另一个表格：每个人都有一份完整的副本，只有当整个群体确认新的一行符合规则时，它才会被加入，旧的行都被封存，无法再修改。它不属于任何人，任何人都可以核查。第二个表格就是区块链的基本思路。

区块链无法消除的东西

从一开始就坦诚说明其局限性很重要。区块链消除了对*单一记账方*的信任需求，但并没有完全消除信任。您仍然要依赖软件的正确性、您自己保护密钥的谨慎程度，而且往往还要依赖交易所和钱包应用等新的中间人。

它还去掉了安全网。通常没有客服可以为您撤销一笔误发的付款。在本课程的后续课程中，您将详细了解这些权衡的两个方面。

这对交易者为何重要

- **交易对手风险无处不在。**当您的资金存放在交易所或经纪商那里时，您持有的是这家公司的承诺，而不是资产本身。FTX的崩溃说明了这种差别在现实中意味着什么。
- **结算方式不同。**美国股票交易在成交后一个工作日结算（T+1，自2024年5月起），而且只在工作日进行。比特币转账则按照网络自身的规则全天候结算，周末也不例外。
- **信任塑造市场叙事。**比特币诞生于2008年银行业危机之后。2023年3月，美国多家地区性银行倒闭，此后数周比特币大幅上涨，许多市场评论人士将这一走势与人们对银行重新产生的疑虑联系起来。理解信任问题，有助于您理解这类叙事为何会推动价格。

关键术语

中间人	在双方之间保管记录并处理付款的第三方，例如银行或交易所。
账本	记录交易和余额的簿册。区块链是一种特殊的账本。
交易对手风险	约定中的另一方未能履行其义务的风险。
双重支付	同一笔数字货币被花费不止一次。防止双重支付是数字现金的核心挑战。
结算	付款或交易完成、所有权变更成为最终状态的时刻。

去信任（Trustless）	一种无需信任任何单一方的系统，因为任何人都可以核查规则。这并不意味着完全不需要信任。

要点总结

1. 数字货币是一条记录，如今由中间人替我们保管这条记录。
2. 中间人带来便利，但也带来费用、延迟、准入限制和单点故障。
3. 由于数字文件可以被完美复制，数字货币面临双重支付问题。
4. 在2008年之前，只有中央记账方才能防止双重支付。
5. 区块链让许多独立的参与者共同维护一份任何人都可以核查的共享记录，而无需任何人负责。

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. 当您从银行账户向别人付款时，实际上发生了什么？

- A 现金在银行金库之间被运送
- B 银行更新其记录中的条目
- C 一个数字硬币文件被发送给收款人
- D 中央银行为收款人印发新钞

2. 什么是双重支付问题？

- A 一笔交易支付两次手续费
- B 被错误地扣款两次
- C 由于数字文件可以复制，同一笔数字货币被花费不止一次
- D 同时把钱汇给两家银行

3. 在2008年之前，数字支付系统通常如何防止双重支付？

A 依靠一个保管官方记录的中央机构
B 把付款限制在小额范围内
C 同时使用实体硬币和数字货币
D 根本无法防止

4. 以下哪一项不是依赖中间人的成本？

A 费用和延迟
B 账户被冻结的风险
C 单点故障
D 付款永远无法撤销

5. 如果您把资金存放在交易所，您实际持有的是什么？

A 以您的名义记录在区块链上的资产本身
B 对交易所的债权，其价值取决于交易所能否保持偿付能力
C 保证全额偿还的保险
D 交易所私钥的副本

6. 在区块链中，「去信任」（Trustless）是什么意思？

A 谁也不信任谁，所以什么都无法运作
B 完全不需要任何信任
C 您无需信任任何单一方，因为任何人都可以核查规则和记录
D 只有受信任的成员才能加入网络

答案与解释

1 B

银行更新其记录中的条目

没有任何实物被转移。银行在记录中减少您的余额，并增加收款人的余额。您的钱实际上就是银行的记录，以及银行兑现它的承诺。

2 C

由于数字文件可以复制，同一笔数字货币被花费不止一次

数字文件可以被完美复制，因此如果没有防护措施，同一笔数字货币可能被发给许多人。防止这种情况是数字现金的核心挑战。

3 A

依靠一个保管官方记录的中央机构

由中央记账方判断哪笔付款在先，并拒绝副本。这种方法行之有效，但意味着每个系统都依赖中间人。

4 D

付款永远无法撤销

中间人通常可以撤销错误和欺诈交易。不可撤销的付款是区块链的特点，同时也是它的风险，而不是传统中间人的特点。

5 B

对交易所的债权，其价值取决于交易所能否保持偿付能力

您持有的是交易所的承诺。如果交易所像2022年的FTX那样倒闭，这一承诺可能被冻结或化为乌有。这就是交易对手风险。

6 C

您无需信任任何单一方，因为任何人都可以核查规则和记录

去信任意味着您不必依赖某一家机构的一面之词。某些信任依然存在，例如对软件的信任，以及对您自己保管密钥方式的信任。

资料来源

- 世界银行，Remittance Prices Worldwide，2025年第一季度报告: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q125_1_0.pdf

Market Talks

继续学习

下一课：第2课
中心化、分布式与去中心化

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。