Market Talks
教育中心

区块链 · 初级 · 第11课，共13课

一笔交易的旅程

从按下“发送”到币到账之间发生了什么，以及为什么有时比你预想的更久

阅读约6分钟　　6道测验题，附答案

区块链 · 初级 · 第11课，共13课

一笔交易的旅程

一句话概括

一笔加密货币交易先在你的钱包里构建并签名，然后在节点之间传递，在一个等待区排队，被矿工或验证者打包进区块，之后再被新的区块一层层压在下面。你支付的手续费决定了它多快离开队列。

第1步：钱包构建并签名

当你按下“发送”时，还没有任何东西到达区块链。钱包首先会拼出一条简短的消息，里面写明三件事：花的是哪些币、发给谁，以及你愿意付多少手续费。

在比特币里，你的余额并不是一个数字，而是一组你之前收到的、彼此独立的币块，叫作**未花费输出**。要从一块价值0.5 BTC的币中发出0.3 BTC，钱包会把整块花掉：0.3给收款人，一小部分作为手续费，剩下的作为**找零**回到你自己的地址。以太坊更像银行余额，但签名的原理是一样的。

最后，钱包用你的私钥给这条消息签名，就像第8课讲过的那样。签名证明所有者批准了这笔特定的付款。事后哪怕改动一个数字，签名就对不上了。

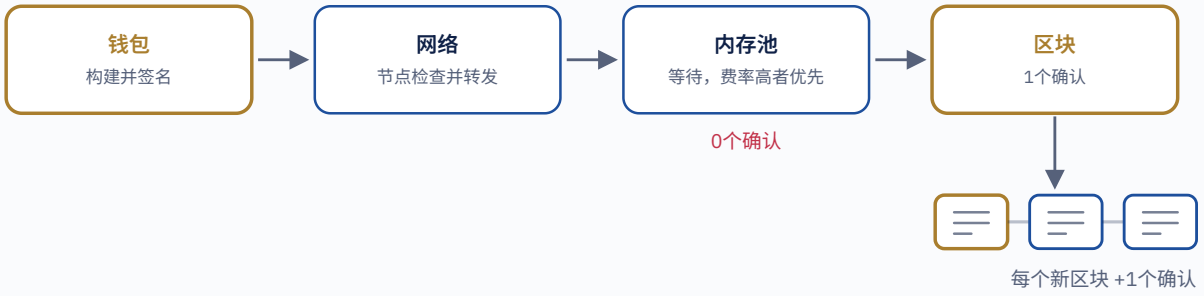


图1. 交易在钱包中签名，由节点检查并转发，在内存池中等待，被矿工打包进区块后获得第一个确认。之后每个区块再增加一个确认。

例子：0.5 BTC去了哪里

你持有一块价值0.5 BTC的币，想给朋友发0.3 BTC。钱包会写出一笔有两个输出的交易：0.3 BTC给朋友，0.1999 BTC回到你自己的找零地址。少掉的0.0001 BTC并没有作为输出写在任何地方。剩下的部分就是手续费，由打包这笔交易的矿工收取。

第2步：广播与候车室

签好名的交易会交给一个节点，节点会检查它：签名是否有效？这些币是否存在？是否已经花过了？如果全部通过，节点就把它转发给自己的对等节点，几秒钟之内就传遍整个网络，正如第7课所示。

每个节点都会把它收到的有效交易放在一个等待区里，这个等待区叫作**内存池**（mempool，memory pool的简称）。并不存在一个统一的内存池。每个节点都有自己的内存池，所以内容会略有不同。交易待在那里时，它有**零个确认**：网络已经知道它，但它还没有上链，在少数情况下仍可能被替换。

第3步：手续费决定谁先走

比特币大约每十分钟出一个区块，空间有限。当等待的交易多于一个区块能容纳的数量时，矿工会优先放入为所占空间付费最多的交易。因此比特币手续费是以费率报价的，单位是**聪/虚拟字节**（sat/vB），而不是金额的百分比。只要交易大小相同，转10美元和转1000万美元的成本一样。

网络状况	通常会发生什么
内存池空闲	即使手续费很低，也能进入下一个或下下个区块
内存池拥堵	低手续费的交易要等待，有时长达数小时或数天
突然涌入	手续费可能在一小时内翻好几倍

涌入有时会非常极端。2024年4月20日，把比特币挖矿奖励减半的那个区块，也就是第840,000个区块，收取了超过37 BTC的手续费，按当时价格约合240万美元，因为大量用户争相挤进这个具有历史意义的区块。

类比：晚上的最后一班渡轮

一艘小渡轮每十分钟开一班，座位数固定。平静的夜晚，每个人都能上船。到了节假日周末，队伍很长，船员会让每个座位出价最高的人先上。如果你只出了最低价，下一班船来了你还在排队，再下一班也一样。

第4步：确认与结算

当矿工把你的交易放进一个被网络接受的区块时，它就有了**一个确认**。之后每叠加一个区块，就再多一个确认。每多一个区块，撤销这笔付款就更难，因为攻击者必须重做所有这些区块，正如第6课所解释的。

确认数（比特币）	通常的含义
0	网络已看到，但还不在区块里
1	已进入区块，对日常小额付款来说足够
数个	交易所在为存款入账前通常等待的数量，因平台而异
6	针对大额的长期经验法则，大约一小时

其他网络有各自的节奏。以太坊每12秒出一个区块，大约13分钟后把区块视为最终确定，此时若要撤销，就必须销毁大量质押的ETH。

交易卡住时

如果在繁忙时段把手续费设得太低，你的交易可能会在内存池里等很久。不会有任何损失：币并没有离开。很旧的交易最终会被大多数内存池丢弃，币就留在原处。常见的解决办法有两种：

- **手续费替换（Replace-by-fee，RBF）。**钱包发送同一笔付款的新版本，手续费更高，用它替换旧的那笔。
- **子交易为父交易付费（Child pays for parent，CPFP）。**收款人，或者你通过找零，在一笔高手续费的新交易中花掉卡住的币，这样矿工就有理由把两笔交易一起打包。

无论用哪种办法，你都可以自己追踪整个旅程。每笔交易都有一个编号，叫**txid**，把它粘贴到区块浏览器里，就能看到它是在等待、已确认，以及被压在多深的位置。

这对交易者为何重要

- **存款不是即时到账的。**交易所只有在达到它要求的确认数之后，才会把你的比特币入账。如果你打算在一波快速行情中交易，币需要在行情出现之前就已经在交易所里，而不是还在路上。
- **行情波动时手续费会上涨。**剧烈的价格波动会让很多人同时涌向区块链，手续费也随之飙升。发送前先查看当前费率，在时间要紧时避免选择最低档。
- **保存好txid。**如果存款或提现似乎迟迟未到，txid能准确告诉你它在哪里。这也是交易所客服首先会问你要的东西。

关键术语

内存池	每个节点存放有效交易的等待区，这些交易正在等待被打包进区块。
交易手续费	发送方为让交易被打包而支付的费用。在比特币中，它就是输入减去输出后剩下的部分。
sat/vB	聪/虚拟字节，用来比较比特币手续费的费率单位。一聪等于一亿分之一个比特币。
确认	链上包含你的交易或排在它之后的一个区块。确认越多，付款就越难被撤销。
找零输出	被花掉的币中，由钱包退回到发送方自己地址的那一部分。
交易编号（txid）	标识一笔交易的唯一代码，可以用它在区块浏览器中查询这笔交易。

要点总结

1. 交易在发送到网络之前，就已经在你的钱包里构建好并完成签名。
2. 节点检查交易、继续转发，并把它放在各自的内存池里，此时它的确认数为零。
3. 区块空间有限，所以矿工挑选的是手续费率最高的交易，而不是金额最大的交易。
4. 你的区块之后每增加一个区块，就多一个确认，交易所会等到规定的确认数才给你入账。
5. 卡住的交易可以用手续费替换或子交易为父交易付费来加速，并可通过txid追踪。

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. 交易是在哪里签名的?

- A 由第一个收到它的节点签名
- B 在发送方的钱包里，发送之前
- C 由把它打包进区块的矿工签名
- D 到达时由收款人的钱包签名

2. 你花掉一块0.5 BTC的币来发送0.3 BTC。剩下的部分会怎样?

A 永远丢失
B 被锁定到下一次减半
C 大部分作为找零回到你手里，剩下的一小部分就是手续费
D 收款人把它当作小费留下

3. 什么是内存池?

A 每个节点存放等待进入区块的有效交易的等待区
B 由比特币开发者运营的一台全球服务器
C 为交易所存放币的钱包
D 区块中记录手续费的部分

4. 两笔比特币交易大小相同，一笔转10美元，另一笔转1000万美元。哪一笔需要更高的手续费才能快速被打包?

A 1000万美元那笔，因为手续费是按百分比收取的
B 都不需要，它们需要相同的手续费率
C 10美元那笔，因为小额付款会被延迟
D 手续费由交易所决定，而不是网络

5. 你的交易已经进入一个区块，之后又增加了两个区块。它有几个确认?

A 一个
B 两个
C 三个
D 六个

6. 在繁忙时段，你的低手续费交易已经等了好几个小时。标准的解决办法是什么?

A 把同样的币再发一次到新地址
B 联系矿工请他们打包
C 用助记词恢复钱包
D 用手续费替换发送一个手续费更高的新版本

答案与解释

1 B

在发送方的钱包里，发送之前

钱包在广播之前用私钥签名。节点和矿工只检查签名，无法生成签名。

2 C

大部分作为找零回到你手里，剩下的一小部分就是手续费

比特币是整块花币的。钱包把差额发回你自己的找零地址，并留下一小部分不分配，作为手续费。

3 A

每个节点存放等待进入区块的有效交易的等待区

每个节点都有自己的内存池，所以不存在统一的内存池。它存放的是有效但尚未进入区块的交易。

4 B

都不需要，它们需要相同的手续费率

矿工比较的是每虚拟字节空间的手续费。转账金额无关紧要，只看交易的大小。

5 C

三个

包含它的区块算作第一个确认，之后每个区块再加一个，所以一加二等于三。

6 D

用手续费替换发送一个手续费更高的新版本

手续费替换会用一个手续费更高的版本换掉正在等待的交易。另一个常见的选择是子交易为父交易付费。

资料来源

- Bitcoin Developer Guide，交易: https://developer.bitcoin.org/devguide/transactions.html
- Cointelegraph，比特币用户在减半区块上花费创纪录的240万美元手续费: https://cointelegraph.com/news/bitcoin-halving-users-spend-record-millions-block-space-runes-rare-satoshis
- ethereum.org，权益证明与最终性: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Bitcoin Optech，Replace-by-fee: https://bitcoinops.org/en/topics/replace-by-fee/

Market Talks

继续学习

下一课：第12课
公有链、私有链与联盟链

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。