Market Talks
教育中心

区块链 · 初级 · 第8课，共13课

私钥、地址与钱包

什么才真正证明一枚比特币属于你，你分享什么来收款，以及钱包里到底装着什么

阅读约6分钟　　6道测验题，附答案

区块链 · 初级 · 第8课，共13课

私钥、地址与钱包

一句话概括

拥有比特币，意味着持有一把私钥，也就是一个让你能为支付签名的秘密数字。由它可以得到一把公钥和一个可以公开分享的地址。钱包根本不装币：它装的是密钥，并用密钥来签名。

一个秘密，两样可以分享的东西

在第5课中我们看到，区块链上没有姓名，只有地址。那么网络怎么知道一枚币是你的？答案是三样相互关联的东西：

- **私钥。**一个从极其庞大的范围中随机选出的秘密数字，这个范围有78位数，与第6课中哈希的规模相同。谁知道它，谁就能花掉与之关联的币。
- **公钥。**用一种特殊的数学方法从私钥计算出来的数字，可以给任何人看。
- **地址。**对公钥进行哈希得到的更短的代码，内置一道校验，可以发现输入错误。这就是你给别人、让他们向你付款的东西。

每一步都只能单向进行。把私钥变成公钥、再把公钥变成地址，电脑只需不到一秒。反向推算则几乎不可能。正因如此，你可以把地址公布在任何地方，而不会让你的币面临风险。



每个箭头只需不到一秒；反方向推算则几乎不可能。

图1. 私钥生成公钥，公钥生成地址。每一步都只能单向进行，所以分享地址永远不会泄露你的私钥。

花钱就是签名

要花比特币，你的钱包会构建一笔交易，并附上一个用你的私钥生成的**数字签名**。任何节点都可以用你的公钥检查这个签名，确认它是由对应的私钥生成的，而全程看不到私钥本身。

签名还与这一笔交易的具体细节绑定在一起。只要有人把金额或收款方改动哪怕一个字符，签名就对不上了，所有节点都会拒绝它。所以没有人能在你的支付经过网络时半路截下并改道。

这正是与银行的根本区别。银行通过核实你的身份来决定你能否花钱；比特币只检查签名是否有效。没有姓名，没有重置密码，没有客服，只有数学。

类比：带投信口的信箱

把地址想象成一个前面有投信口的信箱。任何知道它在哪儿的人都能投进一封信，整条街都看得到来了多少封信。但只有拿着钥匙的人才能打开信箱取出信件。钥匙丢了，信就永远锁在里面；钥匙被人复制，别人就能把信箱清空。

比特币地址长什么样

比特币的地址格式改过几次。所有格式至今都还能用，可以通过开头的字符来区分：

开头字符	类型	推出年份
1	Legacy，最初的格式	2009
3	脚本地址，常用于共享或多重签名钱包	2012
bc1q	原生SegWit，交易更小、手续费更低	2017
bc1p	Taproot，最新格式，隐私性和灵活性更强	2021

其他区块链有自己的格式。例如以太坊地址以*0x*开头，后面跟着40个字符。比特币地址不能拿以太坊地址来代替，即使同一个应用里两者都显示。

好的钱包每次在你要收款时都会生成一个新地址。这些地址都属于同一个钱包，旧地址也照样可用。使用新地址能让陌生人更难把你的所有支付串联起来。

钱包里到底装着什么

尽管叫钱包，它从来不装币。币只以区块链上的记录形式存在。**钱包**是一个工具：保存你的密钥，读取区块链来显示余额，创建交易并为其签名。

钱包大致分为两类：

- **热钱包**把密钥保存在联网的设备上，比如手机应用或电脑程序。日常使用很方便，但密钥暴露在任何可能攻击该设备的威胁之下。

- **冷钱包**把密钥离线保存。**硬件钱包**是一个小设备，把密钥存放在内部，签名时从不把密钥暴露给你的电脑。用起来慢一些，但被黑客攻破的难度要大得多。

如果你的币放在交易所，那么掌握密钥的是交易所，而不是你。第10课会比较这两种选择，第9课会讲解能一次性保护你全部密钥的备份方法。

真实案例：垃圾填埋场里的硬盘

2013年，威尔士的电脑工程师詹姆斯·豪威尔斯不小心扔掉了一块旧硬盘，里面存着他多年前挖到的8,000枚比特币的私钥。硬盘最终进了城市的垃圾填埋场。十多年来他一直请求允许挖掘。2025年1月，英国法院驳回了他的诉讼，同年3月他的上诉也被驳回。这些币至今仍在区块链上，人人都看得见，却没有人能花。

这对交易者为何重要

- **每次都核对完整地址。**在地址投毒骗局中，攻击者从一个与你常用地址几乎一模一样的地址向你发送一笔极小的交易，指望你下次从交易记录里复制它。2024年5月，一位交易者向这样的地址转了1,155枚封装比特币（WBTC），价值约6,800万美元。攻击者后来在谈判后归还了大部分资金，这种结局极为罕见。
- **核对网络，而不只是地址。**交易所常常在多个网络上支持同一种币。如果用接收方不支持的网络发送，资金可能很难甚至无法找回。确认前请检查网络以及任何必填的备注或标签。
- **先发一笔小额测试。**对于大额或首次转账，一笔小额测试只需花一点手续费，却可能保住全部金额。许多交易者还会在交易所账户中启用提币地址白名单。

关键术语

私钥	一个随机的秘密数字，持有者可以用它签署交易并花掉与之关联的币。
公钥	由私钥计算出来、可以公开分享、用于验证签名的数字。
地址	由公钥生成的更短的代码，你把它分享出去，让别人向你转币。
数字签名	用私钥生成、批准某一笔具体交易的证明，任何人都可以用公钥验证。
钱包	保存你的密钥、根据区块链显示余额、并创建和签署交易的工具。
硬件钱包	把私钥离线保存、签署交易时不向电脑暴露密钥的小设备。

要点总结

1. 拥有比特币就是掌控一把私钥。谁拥有私钥，谁就能花掉这些币。
2. 公钥和地址都由私钥计算而来，而且都无法反推回私钥。
3. 花钱需要一个与具体交易绑定的数字签名，任何节点都能在看不到私钥的情况下验证它。
4. 比特币地址按类型以1、3、bc1q或bc1p开头，钱包可以为每笔支付生成新地址。
5. 钱包装的是密钥而不是币。热钱包方便，冷钱包则把密钥离线保存，安全得多。

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. 什么让一个人有能力花掉比特币？

A 知道地址
B 持有私钥
C 在交易所有账户
D 知道交易ID

2. 为什么公开分享你的地址是安全的？

A 因为地址用一次就会失效
B 因为网络会对他人隐藏地址
C 因为没有人能从地址反推出私钥
D 因为地址是加密的

3. 如果有人修改了一笔已签名交易的金额，会怎样？

A 签名对不上，节点拒绝这笔交易
B 交易按新金额完成
C 签名会自动更新
D 由矿工决定用哪个金额

4. 加密货币钱包实际上保存的是什么?

A 你的币
B 整条区块链的副本
C 你的银行信息
D 你的密钥

5. 一个比特币地址以bc1q开头，它是什么类型?

A Legacy
B 原生SegWit
C 以太坊
D Taproot

6. 硬件钱包的主要优势是什么?

A 让交易更快
B 免除所有手续费
C 把私钥离线保存，签名时不暴露私钥
D 可以追回转错地址的币

答案与解释

1 B

持有私钥

签署支付的是私钥。谁拥有它，谁就能花掉这些币，所以它必须保密。

2 C

因为没有人能从地址反推出私钥

从私钥到公钥再到地址，每一步都是单向的。别人可以向你的地址转账，却无法用它找到你的私钥。

3 A

签名对不上，节点拒绝这笔交易

签名与一笔交易的具体细节绑定。任何改动，哪怕一个字符，都会让签名失效。

4 D

你的密钥

币只存在于区块链上。钱包保存你的密钥，从链上读取余额，并为你的交易签名。

5 B

原生SegWit

以bc1q开头的地址是原生SegWit地址，于2017年推出。Taproot地址以bc1p开头，Legacy地址以1开头。

6 C

把私钥离线保存，签名时不暴露私钥

硬件钱包把密钥保存在设备内部，只输出已签名的交易，因此你电脑上的恶意软件无法读取密钥。

资料来源

- 中本聪，Bitcoin: A Peer-to-Peer Electronic Cash System（2008）: https://bitcoin.org/bitcoin.pdf
- 维基百科，埋在纽波特垃圾填埋场的比特币: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph，交易者在地址投毒骗局中损失6,800万美元（2024年5月）: https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph，攻击者谈判后归还资金: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

继续学习

下一课：第9课
助记词与备份

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。