Market Talks
教育中心

区块链 · 初级 · 第10课，共13课

托管：交易所账户还是自己的钱包

谁才真正持有你的币，历史对两种选择说明了什么，以及大多数交易者如何折中

阅读约5分钟　　6道测验题，附答案

区块链 · 初级 · 第10课，共13课

托管：交易所账户还是自己的钱包

一句话概括

把加密货币放在交易所，意味着交易所持有密钥，你持有的只是一个承诺。放在自己的钱包里，意味着你持有密钥，也承担全部责任。两种选择防范的是不同的风险。

持有同一枚比特币的两种方式

托管（custody）简单来说就是：私钥在谁手里。基本有两种模式：

- **托管式。**由交易所或其他公司持有密钥。你用密码登录，你的余额是公司自己数据库里的一个数字，正如我们在第5课看到的。你提币时，由公司替你签署交易。
- **自我托管。**密钥在你自己手里，通常存放在用第9课的助记词备份的钱包中。没有人能动你的币，也没有人能阻止你动它们，但如果你弄丢了密钥，也没有人能救你。

在区块链上，并不存在你在交易所的“账户”。交易所的地址把所有人的币放在一起，它的数据库记录着这堆币里每位客户各占多少。

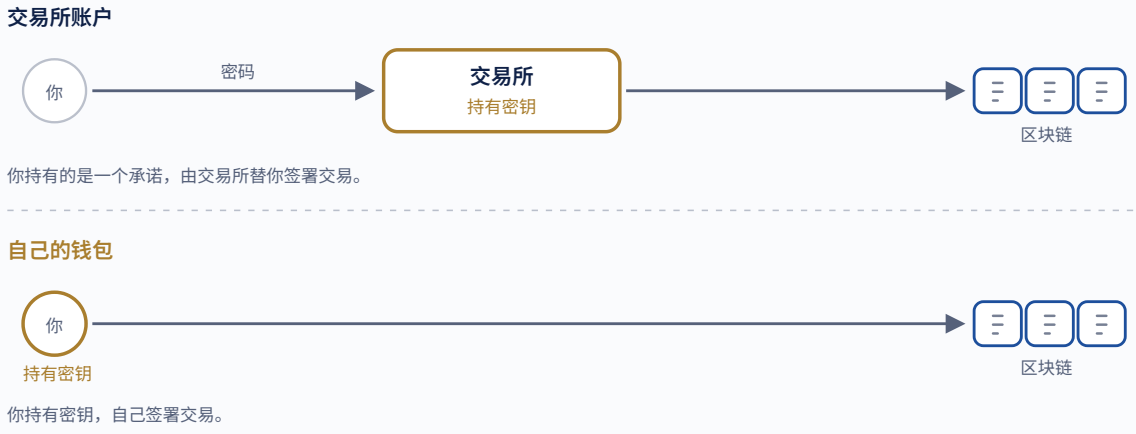


图1. 使用交易所账户时，公司持有密钥，你通过它接触区块链。使用自己的钱包时，你持有密钥，直接与区块链打交道。

类比：衣帽寄存处

在人多的活动上，你把外套交给衣帽寄存处，换来一张号码牌。这很方便，外套通常也能拿回来。但这一晚你手里拿的是号码牌，不是外套。如果寄存处被盗、提前关门，或者悄悄把外套借给了别人，你的号码牌就只值柜台后面那些人的信用。穿着外套不太舒服，但除了你没人能把它弄丢。

历史对交易所说明了什么

大多数交易所从未倒闭。但大型交易所一旦倒下，客户往往要等上好几年，而且常常损失大部分资金：

交易所	发生了什么	客户的遭遇
Mt. Gox（2014）	当时最大的比特币交易所因被盗和管理不善损失约850,000枚比特币	剩余资产直到2024年7月才开始偿还，整整晚了十年
QuadrigaCX（2019）	创始人去世，而只有他一人掌控的冷钱包几乎是空的	约76,000名用户被拖欠约2.15亿加元
FTX（2022）	客户资金被一家关联交易公司挪用，提币在几天之内停止	数十亿美元客户资金不翼而飞，创始人后来被判欺诈罪成立

在每一起事件中，屏幕上的余额直到最后都显示正常。交易所里的余额是你对这家公司的债权，而不是币确实还在的证明。

自己保管的风险

自我托管把公司从等式中去掉了，但把所有工作都交给了你。人们自己弄丢币最常见的方式有：

- **备份丢失。**助记词丢了，设备又坏了，币就被永远锁住了。Chainalysis的研究人员在2017年估计，约有280万到380万枚比特币已经以这种方式丢失，大约占当时已挖出全部币的五分之一。
- **备份泄露。**把助记词输入假网站或假应用，就等于把一切交给了小偷，正如第9课所讲。
- **发送出错。**地址或网络填错无法撤回，正如第8课所讲。

没有客服，也没有重置密码。这就是不依赖一家可能倒闭或冻结你资金的公司所要付出的代价。

大多数人如何分配

对很多人来说，答案并不是二选一。一种常见的做法是：把交易所当作口袋里的钱包，把自我托管当作家里的保险箱：

	交易所账户	自己的钱包
谁持有密钥	交易所	你
忘记密码时	客服通常可以帮你恢复访问	只有助记词能帮你
公司倒闭时	你的币可能被冻结或损失	没有任何变化
最适合	活跃交易和即将要用的资金	长期持有和储蓄
主要风险	公司：黑客攻击、欺诈、冻结、倒闭	你自己：备份丢失、诈骗、操作失误

如果你确实要在交易所存放资金，请优先选择历史悠久、受监管的大型平台，开启它们提供的所有安全功能，并查看它们是否定期公布储备证明（proof of reserves）。请记住，储备证明展示的是交易所在某一时刻持有的资产，但并不总能反映它所欠的全部负债。

这对交易者为何重要

- **期货和杠杆需要托管。**要交易永续合约，你的保证金必须放在交易所。只放仓位所需的金额，而不是全部身家，并定期把交易用不到的利润转到自己的钱包。
- **留意预警信号。**提币变慢或暂停、提币限额突然调整，以及链上出现大量币流出某交易所，往往是出事的前兆。2022年11月初，FTX的提币先是变慢，几天之内就完全停止。在最早的迹象出现时行动，比在最后关头行动容易得多。
- **自我托管要付出速度的代价。**把币从钱包转到交易所需要时间和网络手续费，而在快速行情中，每一分钟都很重要。要在波动到来之前，而不是之中，规划好两边各放多少。

关键术语

托管	对私钥的控制，也就是对这些私钥所能解锁的币的控制。
托管式	由公司替你持有密钥的方式，比如交易所账户。
自我托管	在自己掌控的钱包中持有自己的密钥，通常用助记词备份。
交易对手风险	替你保管资产的公司倒闭、冻结资产或不予归还的风险。
储备证明	公开发布的核查，展示交易所在某一时刻持有的资产，但可能无法反映它所欠的全部负债。

Not your keys, not your coins	一句常见说法：“不是你的私钥，就不是你的币。”如果密钥在别人手里，你拥有的只是对方归还币的承诺。

要点总结

1. 托管指的是密钥在谁手里。在交易所由公司持有，自我托管则由你持有。
2. 交易所余额是公司数据库里的一个数字，是你对该公司的债权，而不是你掌控的币。
3. Mt. Gox、QuadrigaCX和FTX表明，交易所倒闭可能让客户资金冻结数年，甚至血本无归。
4. 自我托管消除了公司风险，但增加了个人风险：备份丢失、助记词泄露以及发送出错。
5. 许多人把交易资金放在可信的交易所，把长期持有的资产放在自己的钱包里。

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. 在加密货币中，托管（custody）是什么意思？

- A 私钥在谁手里
- B 哪家交易所手续费最低
- C 你打算持有一种币多久
- D 哪个国家监管某种币

2. 你的交易所账户里有1枚BTC。你实际上拥有的是什么？

- A 一把以你的名字保存的私钥
- B 记录在交易所数据库里、对交易所的一项债权
- C 只有你能控制的个人地址里的币
- D 由交易所代为保管的硬件钱包

3. QuadrigaCX的客户无法拿回资金，一个关键原因是什么？

A 比特币网络停止运行
B 客户弄丢了助记词
C 只有创始人掌控钱包，而他去世时钱包几乎是空的
D 政府没收了加拿大所有交易所

4. 自我托管消除了哪种风险？

A 弄丢助记词的风险
B 转错地址的风险
C 钓鱼诈骗的风险
D 交易所冻结或弄丢你的币的风险

5. 在两种模式之间分配资金，常见的做法是什么？

A 为了方便全部放在交易所
B 交易资金放在可信的交易所，长期储蓄放在自己的钱包
C 全部自我托管，包括期货保证金
D 尽可能平均分散到更多交易所

6. 储备证明可能无法展示什么？

A 交易所持有哪些币
B 交易所的钱包地址
C 交易所欠客户和贷款方的全部负债
D 核查的日期

答案与解释

1 A

私钥在谁手里

谁持有私钥，谁就控制这些币。托管问的就是这个人是谁。

2 B

记录在交易所数据库里、对交易所的一项债权

交易所持有共用地址的密钥。你的余额是它记录的、欠你多少的账目。

3 C

只有创始人掌控钱包，而他去世时钱包几乎是空的

由一个人掌控密钥，加上资金被挪用，在他去世后，大部分资金已无法追回。

4 D

交易所冻结或弄丢你的币的风险

密钥在自己手里，任何公司都无法冻结、出借或弄丢你的币。剩下的风险是你自己的失误和诈骗。

5 B

交易资金放在可信的交易所，长期储蓄放在自己的钱包

交易需要资金放在交易所，而储蓄放在自己的钱包里能更好地规避公司风险。两边各司其职。

6 C

交易所欠客户和贷款方的全部负债

储备证明展示的是某一时刻的资产。如果没有负债的全貌，就无法证明交易所能偿还所有人。

资料来源

- The Block，Mt. Gox自2024年7月起开始以比特币偿还: https://www.theblock.co/post/301448/mt-gox-to-distribute-9-billion-of-bitcoin-bitcoin-cash-repayments-from-beginning-of-july
- Crowdfund Insider，QuadrigaCX托管人报告：76,000名用户损失2.15亿美元: https://www.crowdfundinsider.com/2019/05/147401-quadrigacx-trustees-final-report-finds-not-much-left-for-76-000-exchange-users-who-lost-215-million/
- 维基百科，FTX破产: https://en.wikipedia.org/wiki/Bankruptcy_of_FTX
- Cointelegraph，多达四百万枚比特币可能已永久丢失（Chainalysis估计）: https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

继续学习

下一课：第11课
一笔交易的旅程

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。