Market Talks
教育中心

加密货币 · 初级 · 第15课，共15课

真正的入门：交易所、KYC与钱包

最初几个实际步骤是什么样子：选择交易所、通过KYC、保护账户安全、完成第一笔购买、设置自托管钱包，以及把资金转入其中

阅读约12分钟　　8道测验题，附答案

加密货币 · 初级 · 第15课，共15课

真正的入门：交易所、KYC与钱包

一句话概括

大多数人从中心化交易所开始接触加密货币，之后再添加一个由自己掌控的钱包。本课逐一讲解每个步骤：它包含什么，以及常见的错误出在哪里。

持有加密货币的两种方式

在开设任何账户之前，先了解持有加密货币的两种基本方式会很有帮助：

- **放在交易所（托管）：**你在Binance或Coinbase这样的公司开设账户。私钥由交易所掌握，你的余额只是它数据库里的一个数字，就像银行账户里的钱。这种方式很简单，如果忘记密码，交易所可以帮你重新登录。
- **放在自己的钱包（自托管）：**你安装MetaMask这样的钱包，或使用Ledger这样的硬件设备。你通过助记词掌握私钥。没有人能替你冻结或弄丢你的币，但也没有人能替你找回它们。

一句流行的说法概括了两者的区别：**“不是你的私钥，就不是你的币”**（not your keys, not your coins）。许多人两种方式都用：用交易所买卖，用钱包持有加密货币并在区块链上使用（第9课和第12课，以及区块链课程第9课）。



图1. 在交易所，私钥由公司掌握；在自托管钱包中，私钥由你掌握。

例子：当交易所出事时

2022年11月，交易所FTX倒闭，客户在很长一段时间内无法提取资金。2025年2月，被FBI认定与朝鲜有关的黑客从Bybit盗走了价值约**15亿美元**的以太币。Bybit保持提现正常开放，并表示会承担客户的损失，但这两起事件说明了同一个道理：放在交易所里的币，取决于这家公司的安全性和诚信。

选择交易所

中心化交易所（第9课）是常见的入金渠道，也就是把普通货币换成加密货币的地方。人们通常会比较以下几点：

- **可用性与牌照：**这家交易所是否获准为你所在国家的用户提供服务，以及由哪家监管机构监管。
- **入金方式：**银行转账、银行卡或本地支付方式，以及支持哪些法币。
- **币种与网络：**上架了哪些币，充值和提现支持哪些网络（第5课）。
- **费用：**交易手续费、银行卡手续费、“快捷买币”中的价差，以及提现手续费。
- **过往记录：**是否有过被黑或冻结提现的历史，以及是否公布储备证明。

交易所	特点
Binance	按交易量计全球最大的交易所，上架币种非常多
Coinbase	美国上市公司，应用简单，在美国和欧洲实力较强
OKX	全球性交易所，内置自托管钱包
Bybit	全球性交易所，以衍生品交易著称
Kraken	历史最悠久的交易所之一，在美国和欧洲实力较强
Upbit	韩国最大的交易所，以韩元交易

这些名称只是广泛使用的服务的例子，**并非推荐**。服务和规则会变化，也并非每家交易所都在每个国家可用。在一些国家，例如韩国，本地交易所还要求用户在合作银行开设实名银行账户。

注册与KYC

受监管的交易所必须核实客户的身份。这叫做**KYC**，是“了解你的客户”（know your customer）的缩写，在大多数国家属于反洗钱（AML）法律的一部分。典型的注册流程如下：

1. **账户：**邮箱或手机号，以及密码。

2. **个人信息：**全名、出生日期、地址和国籍。
3. **身份证件：**护照、身份证或驾照的照片。
4. **自拍或视频验证：**应用会检查面部是否与证件相符，以及是否有真人在场。
5. **审核通过：**通常几分钟内完成，有时需要几天。有些交易所之后会要求提供地址证明或资金来源证明，以获得更高的额度。

根据一项相关规定，即**旅行规则**（Travel Rule），许多国家的交易所在彼此之间进行较大额转账时，还会共享发送方和接收方的信息，并可能询问你要提现到的钱包归谁所有。

KYC意味着交易所保存着敏感的个人数据。这也是确认网站真实可靠很重要的原因之一：虚假交易所网站同样会收集证件照片（第14课）。



图2. 开设交易所账户时常见的KYC步骤。

保护账户安全

交易所账户是攻击目标，所以交易所提供了好几层保护。以下是最常被首先开启的几项：

- **双重验证（2FA）：**登录和提现时需要的第二个验证码。Google Authenticator等身份验证器应用，以及通行密钥或安全密钥，比短信验证码更难被盗；短信验证码可能通过SIM卡调换被人拿走。
- **防钓鱼码：**你自己设定的一个词，交易所会把它放进发出的每一封真实邮件里。没有这个词的邮件就不是交易所发来的。
- **提现白名单：**只允许向你事先保存的地址提现，新地址通常还有一段等待期。
- **设备与登录提醒：**有人从新设备或新地点登录时会收到通知。
- **一个独特的强密码**，不在任何其他地方使用。



图3. 交易所提供多层账户保护。

完成第一笔购买

账户通过验证后，就可以充值并把钱换成加密货币：

- **充值：**银行转账通常是最便宜的方式。银行卡更快，但往往要多花几个百分点。有些交易所还提供P2P市场，用户可以通过交易所彼此直接交易。
- **“买入”或“闪兑”按钮：**最简单的方式。你输入金额，得到一个报价。费用往往隐藏在更宽的买卖价格里（价差）。
- **现货市场：**带有订单簿的交易界面（第9课）。市价单以当时最优的价格买入；限价单等待你设定的价格。这里的手续费通常更低。

购买之后，币就放在你的交易所账户里。它们可以留在那里、被卖出，或被提现到钱包。



图4. 充值之后在交易所购买的两种方式。

例子：两种购买方式

Sophie通过银行转账充值了500美元。她用简单的“买入”按钮买了250美元的比特币，收到的比预期少一点，因为报价里包含了约1%的价差。另外250美元，她在现货市场下了一笔市价单，支付了0.1%的交易手续费，约25美分。两种都是正常的购买方式，区别主要在于成本，以及她愿意和交易界面打多少交道。

钱包：热钱包、冷钱包与常见名称

自托管钱包是一个存储你的私钥并签署交易的应用或设备（区块链课程第9课）。主要类型有：

- **热钱包**连接着互联网：手机应用和浏览器插件。它们免费，日常使用和连接DeFi应用都很方便。
- **冷钱包**把私钥离线保存，通常是在一个小型硬件设备上。交易需要按下设备上的按钮来批准，因此电脑上的恶意软件无法自行签名。

钱包	类型	主要网络
MetaMask	浏览器插件和手机应用	Ethereum及其他EVM网络，例如BNB Chain、Base和Arbitrum，现在也支持Solana和Bitcoin
Trust Wallet	手机应用和插件	许多网络，包括BNB Chain、Ethereum和Bitcoin
Phantom	手机应用和插件	以Solana为主，也支持Ethereum、Base和Bitcoin
Ledger	硬件钱包	许多网络，配合自家的Ledger Live应用或其他钱包使用
Trezor	硬件钱包	许多网络，配合自家的Trezor Suite应用或其他钱包使用

同样，这些只是常见的例子，并非推荐。钱包应用是仿冒者最喜欢的目标，所以人们通常只通过官方网站或官网上的链接下载。硬件钱包通常直接从制造商处购买，因为二手或被动过手脚的设备可能并不安全。



图5. 热钱包在线且方便；冷钱包把私钥离线保存。名称仅为例子，并非推荐。

设置钱包与助记词

创建新钱包时，它会显示一组由12或24个单词组成的**助记词**（也称恢复短语）。这些单词可以在任何兼容的应用或设备上重建钱包里的每一把私钥。这意味着：

- 任何看到助记词的人都能拿走钱包里的一切。
- 如果手机丢了，助记词也丢了，资金就永远没了。钱包公司没有副本，也无法重置。

常见的做法是把这些单词写在纸上或刻在金属上，仔细核对，然后离线存放在安全的地方，有时分放两处。截图、照片、云笔记、邮件以及在线同步的密码管理器，是助记词被盗的常见途径。真正的客服人员、应用或网站都不会需要它（第14课）。



图6. 助记词掌控着钱包。它的保存方式决定了谁能拿走资金。

把资金转入钱包并完成第一次兑换

从交易所提现到你自己的钱包，会用到第10课的全部内容：

1. 从钱包中复制对应网络的**收款地址**。
2. 在交易所选择**“提现”**，粘贴地址，并选择**相同的网络**。只有在收款方需要时才填写备注标签。

3. 核对地址开头和结尾的几个字符。
4. 许多人会先发送一笔**小额测试转账**，到账后再发送其余部分。

要在该网络上使用钱包，还需要少量该网络的**原生币来支付Gas费**，例如Ethereum上的ETH、BNB Chain上的BNB或Solana上的SOL（第5课）。

接下来，在去中心化交易所（第9课）上的第一次兑换是这样进行的：打开官方DEX网站，**连接**钱包，选择两种代币，查看价格影响和滑点，如有提示则**授权**该代币（第14课解释了授权为何重要），然后在钱包中**确认**兑换并支付Gas费。

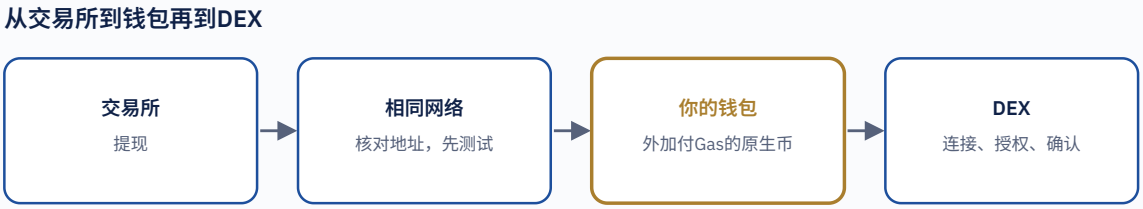


图7. 把资金从交易所转入自托管钱包，然后在DEX上完成第一次兑换。

一图看懂全过程

把本课内容合在一起，典型的首次设置分为八个阶段。并非每个人都会全部做完：许多人只使用交易所，也有人在一段时间后转向自托管。

本课是加密货币初级课程的最后一课。现在你已经了解了加密货币是什么，币、代币和网络有何不同，它们在哪里交易，价格如何变动，主要风险有哪些，以及最初的实际步骤如何进行。面向会员的加密货币中级和高级课程会更深入地讲解交易、链上数据和DeFi。



图8. 典型的首次设置，从交易所账户到第一次DEX兑换。

这对交易者为何重要

- **交易所的选择会影响成本。**交易手续费、价差、资金费率和提现手续费，会在多次交易中不断累积。手续费等级通常取决于交易量。
- **交易对手风险真实存在。**为交易而放在交易所的资金取决于这家交易所。许多交易者只在那里放交易所需的资金，其余的存放在别处。
- **安全设置保护交易账户。**双重验证、防钓鱼码和提现白名单，能让被盗的密码对攻击者的用处大大降低。
- **在交易所和钱包之间转移资金是日常操作。**选择正确的网络和核对地址，会成为活跃交易者的日常习惯。

关键术语

托管（custodial）	由交易所等公司代你掌握私钥的方式。
自托管（self-custody）	在你自己掌控的钱包中持有私钥，没有任何公司能冻结或找回这些资金。
KYC	了解你的客户（know your customer）：受监管的交易所在为客户提供服务之前或期间必须进行的身份核验。
旅行规则（Travel Rule）	要求交易所在某些转账中共享发送方和接收方信息的规定。
双重验证（2FA）	除密码之外的第二重身份证明，例如身份验证器应用生成的验证码。
防钓鱼码	交易所放进其真实邮件中的个人专属词语，方便用户识别虚假邮件。
提现白名单	一份已保存地址的列表，只有列表中的地址才能接收该账户的提现。
热钱包	私钥存放在联网设备上的钱包，例如手机应用或浏览器插件。
冷钱包	把私钥离线保存的钱包，通常是硬件设备。
助记词	由12或24个单词组成的列表，可以重建一个钱包的全部私钥。
EVM网络	运行以太坊虚拟机（EVM）的区块链，因此可以使用与Ethereum相同的钱包、地址和应用。BNB Chain、Base、Arbitrum和Polygon都是例子。

要点总结

1. 加密货币可以放在交易所（托管），也可以放在自己的钱包（自托管）。许多人两种都用。
2. 各家交易所在可用性、入金方式、币种、网络、费用和过往记录上各不相同。本课提到的名称只是例子，并非推荐。
3. KYC是指反洗钱法律要求的证件和自拍验证。
4. 使用身份验证器应用或通行密钥的双重验证、防钓鱼码和提现白名单，是主要的账户保护措施。
5. 热钱包方便；冷钱包把私钥离线保存。助记词掌控一切，而且无法重置。
6. 提现到钱包需要正确的地址、相同的网络，以及少量用于支付Gas费的原生币。在DEX上兑换意味着连接、授权和确认。

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. “不是你的私钥，就不是你的币”是什么意思？

A 放在交易所的币总是会丢失
B 如果私钥由别人掌握，你的币就取决于他们
C 只有比特币才需要私钥
D 你必须拥有硬件钱包才能购买加密货币

2. 为什么受监管的交易所要求提供证件和自拍？

A 为了设定你的交易手续费
B 因为KYC和反洗钱法律
C 为了选择你的网络
D 为了生成你的助记词

3. 什么是防钓鱼码?

A 提现用的密码
B 交易所放进其真实邮件里的一个词
C 一个阻止所有登录的代码
D 一种硬件钱包

4. 哪种双重验证最容易被盗?

A 身份验证器应用
B 硬件安全密钥
C 短信验证码
D 通行密钥

5. 热钱包和冷钱包的主要区别是什么?

A 热钱包只能存放比特币
B 冷钱包把私钥离线保存
C 热钱包没有助记词
D 冷钱包无法发送交易

6. Anna弄丢了手机，而且从没抄下她的助记词。她的自托管钱包会怎样?

A 钱包公司会重置它
B 她的交易所可以恢复它
C 资金再也无法访问
D 区块链会把币退回

7. Lucas要把USDT从交易所提现到他在BNB Chain上的钱包。他在交易所应该选择哪个网络?

A 任何网络都行，它们都一样
B Ethereum，因为它最大
C BNB Chain，与他的钱包地址相同的网络
D Bitcoin

8. Lucas的USDT到账了，但兑换失败，因为他付不了手续费。缺少的是什么?

A 助记词

B 少量用于支付Gas费的BNB

C KYC审核通过

D 防钓鱼码

答案与解释

1 B

如果私钥由别人掌握，你的币就取决于他们

在交易所，私钥由公司掌握，所以你的余额取决于它的安全性和诚信。

2 B

因为KYC和反洗钱法律

在大多数国家，KYC核验是受监管交易所的法定要求。

3 B

交易所放进其真实邮件里的一个词

如果一封自称来自交易所的邮件没有显示你的防钓鱼码，它就不是真的。

4 C

短信验证码

短信验证码可能通过SIM卡调换被盗：攻击者把你的手机号转移到他们的SIM卡上。

5 B

冷钱包把私钥离线保存

热钱包把私钥放在联网设备上；冷钱包把私钥离线保存，并在设备上批准交易。

6 C

资金再也无法访问

只有助记词能重建私钥。没有它，谁也无法找回资金。

7 C

BNB Chain，与他的钱包地址相同的网络

发送和接收的网络必须一致，否则资金可能丢失或很难找回（第10课）。

8 B

少量用于支付Gas费的BNB

网络上的每笔交易都要用该网络的原生币支付，这里就是BNB Chain上的BNB。

资料来源

- TRM Labs，Bybit 被盗事件：追踪朝鲜规模最大的一次攻击: https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit
- TechTarget，FBI：Lazarus Group 是 15 亿美元 Bybit 盗窃案的幕后黑手: https://www.techtarget.com/cybersecurity/news/366619872/FBI-Lazarus-Group-behind-15-billion-Bybit-heist
- The Block，MetaMask 走向多链：一个账户支持 EVM、Solana，并即将支持 Bitcoin: https://theblock.co/post/376450/metamask-multichain-account
- Cointelegraph，MetaMask 新增 Bitcoin 支持: https://cointelegraph.com/news/metamask-adds-bitcoin-support-after-teasing-february
- Tiger Research，2026 年韩国加密货币市场: https://reports.tiger-research.com/p/2026-korea-cryptocurrency-market-eng

Market Talks

继续学习

本课属于 MARKET TALKS 教育中心的加密货币课程。初级课程免费，每课都配有测验和可下载的PDF。中级和高级课程面向会员开放。

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。