

# 区块链入门

## —— 最最基础概念


### 助记词


助记词 = 你的钱包超级密码!!


不仅仅是密码，更是你的账户身份  
它由 12 至 24 个单词组成，是找回钱包的唯一凭证


同一组助记词可通用于多个区块链和钱包

有了助记词，无论换钱包还是设备，都能随时找回资产！

 最重要的事

 手写备份，妥善保管！

 千万不要截图、存手机或云端！

 助记词一旦泄露，资产将不再属于你！

# PIN码

PIN码 = 解锁钱包的密码

PIN码是你的钱包安全锁，但它不是助记词！

主要作用是防止他人未经授权访问你的钱包并转移资金。

如果钱包丢失，PIN码可以保护你的资产不被盗取

忘记 PIN 码可能会导致无法解锁钱包，但只要妥善保管助记词，就能恢复钱包！

# 区块链

区块链 = 透明记账本

区块链是一个公开的账本，所有人都可以查看其中的转账记录，但任何人都无法修改已写入的数据。在

传统银行体系中，银行可以冻结你的账户、更改你的余额，但在区块链世界，只有拥有助记词的你才能控制自己的资产，完全无需中介机构。


我们常说的 以太坊Ethereum、Polygon、Solana、Cardano 等，都是不同的区块链（简称“链”）。每条链相当于一个独立的账本。


在区块链的世界，每条链就像一个独立的国度，而这个国度有它的法定货币——原生币（Native Token）。想要在某个“国度”内交易，必须使用该国度的**原生币**支付手续费。不同的链之间也存在交易

需求，这就像跨国贸易，需要通过跨链桥（Bridge）进行转换。如果你建造了这样的桥，就可以赚取手续费（类似过路费）。

你可能会看到许多相同名字的币，例如 ETH，但它可能分布在不同的链上，比如 Ethereum、Polygon、BNB Chain、Base 等。这时，你必须确认它属于哪个“国度”（哪条链），否则即便你持有它，也无法直接使用。

### 交易小贴士

 确认币所在的链，避免转错无法找回！

 跨链桥交易需谨慎，选择官方或知名的桥，防止资产丢失！

✅ 交易手续费绝大多数链都是用原生币

## 数字钱包


数字钱包 = 手机银行


像支付宝、微信钱包，但更自由。功能相同都是以转账消费为主，但本质不同。


支付宝、微信钱包的余额是直接关联银行账户的，受银行和平台监管。


数字钱包直接与区块链交互，不依赖银行，你可以自由收款、转账、查看余额（别人有你的地址也可以查看你的转账记录和余额）


你的收钱、转账、查看余额都是由数字钱包和区块链的交互来完成。


 钱包丢了，钱还在吗？

 你的数字货币不在钱包里，而是存储在区块链上！

 只要有助记词，就能随时找回资产，换钱包、换设备都不怕。

 任何支持你的助记词的数字钱包，都可以用来恢复你的资产。

 丢了钱包  $\neq$  丢了钱，但丢了助记词 = 彻底丢失资产！

 数字钱包只是访问区块链的工具，保护助记词才是最重要的！

## 钱包地址

钱包地址=你的银行卡号

数字钱包用助记词自动生成不同的钱包地址

一组助记词可以在很多不同的区块

链上使用

同时每个区块链上都可以生成很多不同的钱包地址



### 关键点

转账时，一定要复制粘贴，不要手写，一个字母错了，钱就可能打丢了！

钱包地址本身是匿名的，别人可以知道你的地址，但不会知道你是谁。

用助记词可以找回所有钱包地址  
相同助记词在不同区块链上通常拥有不同地址（子链和主链地址通常一样）

# 私钥签名

私钥签名=你的签字或公章

用来证明这笔交易是你自己批准的，别人不能伪造！



关键点

私钥太长不需要记，有助记词同样可以恢复

私钥同样不能泄露！签名是私钥生成的，如果私钥泄露，别人就能用你的私钥随便签名，转走你的钱！

# Gas费

Gas费 = 交易手续费

Gas源于汽油，为了让区块链上的交易和智能合约跑起来，就要付油钱，这些费用主要用于奖励矿工或验证节点，主流的区块链都要收手



续费，几乎没有免费转账这回事

（目前没有哪个公链能做到免费转账，羊毛出在羊生上，这个费用一定要有，否则这个链就没人来维护，更没人来保证其去中心化）

Gas费通常是由发起交易者支付，你转账给他人你支付，你购买NFT你支付，接收者、售卖者则无需支付。

## 智能合约

智能合约 = 代码化的合同

区块链是一个透明的账本，交易记录是数据，代码程序也是数据。有人想到，把代码程序放进区块链，这样它就能自动执行预设的规则

传统合同：纸质协议，签署后需双方履行，若违约需借助法律解决  
智能合约：合同条款写成代码，满足条件即自动执行，无需第三方

## DApp

DApp = 区块链应用

D代表去中心化，严格说就是区块链应用。

区块链上可以转账，还有智能合约也就是以二进制的形式存储在区块链上的代码。做为用户是很难直接调用这些代码去干一些复杂的事情。而DApp就把这些代码封装起来方便我们使用。要使用DApp都需要让它与我们的数字钱包相连才能工作。

# 代币

代币 = 现金等价物

代币Token是相对原生币Coin而言，在每条区块链上，通常都有一种核心货币，称为原生币，它是该链的基础资产，主要用于：

- 支付手续费Gas，确保区块链正常运行
- 激励节点维护者，维持去中心化网络
- 执行智能合约，让链上的应用程序得以运作

之前将区块链比作一个“国度”：

- 原生币 = 这个国度的法定货币
- 代币 = Q币、代金券、信用卡积分、股票、债券等

代币是在某条区块链上发行的其他资产，它可能具有经济价值，但本身不承担链的运行成本。

例如，USDT（泰达币）是以太坊上的一种代币，它本质上是基于以太坊网络的“电子美元”，但转账USDT时，仍然需要以太坊的原生币ETH支付手续费。