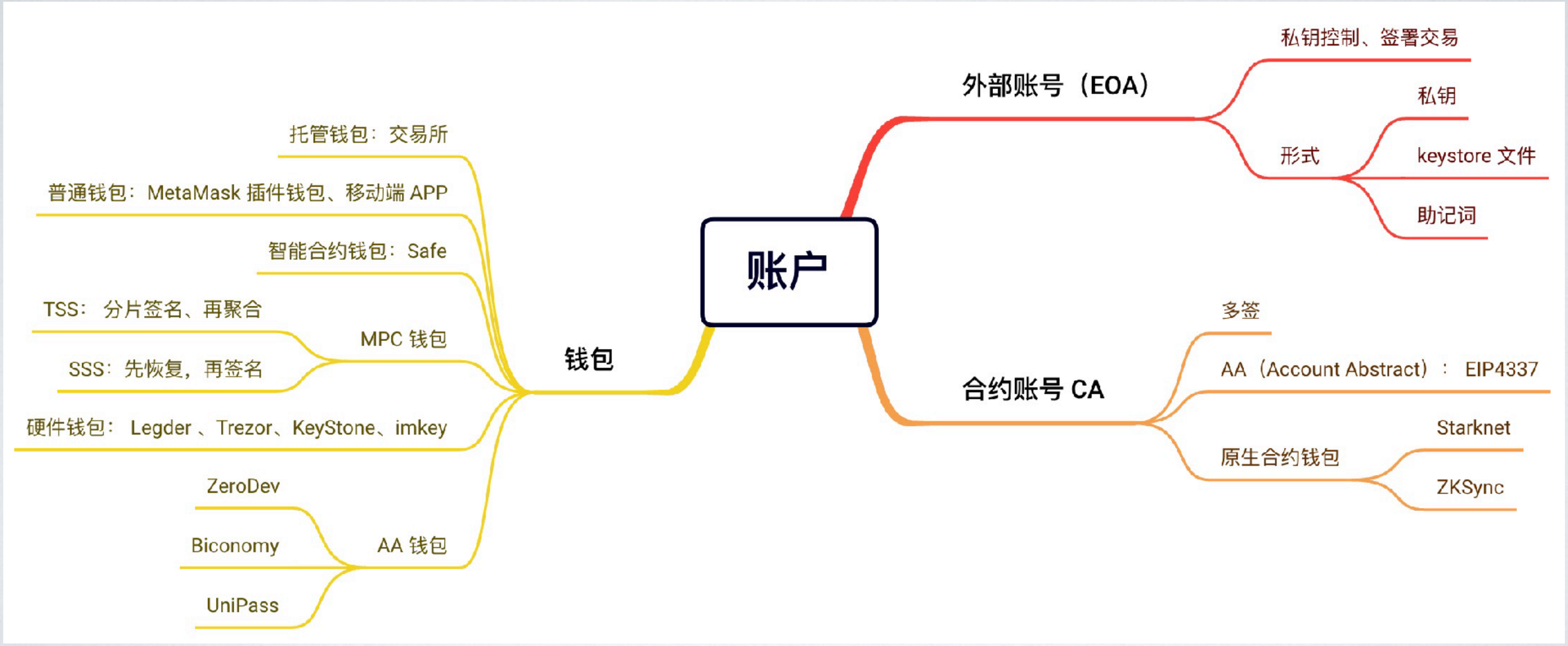
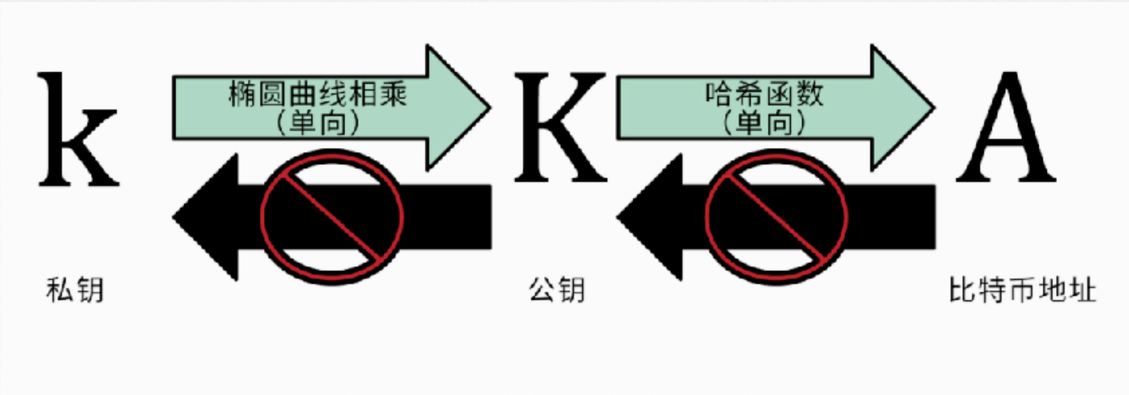
账号 / 钱包



硬件钱包： https://www.bilibili.com/video/BV1sM4m1R72B/?spm_id_from=333.999.0.0

EOA 账号

- 本质是一个 32 字节的私钥（随机数）



Demo: OpenSpace100/account_demo/create_by_raw.js

创建 EOA 账号

- 找到一个安全的熵源（不可预测、不可重复），如掷硬币256次。
- 使用 secp256k1椭圆曲线算法计算出公钥
- 对公钥进行keccak256 hash运算再取后40位得到

Demo: OpenSpace100/account_demo/create_by_raw.js

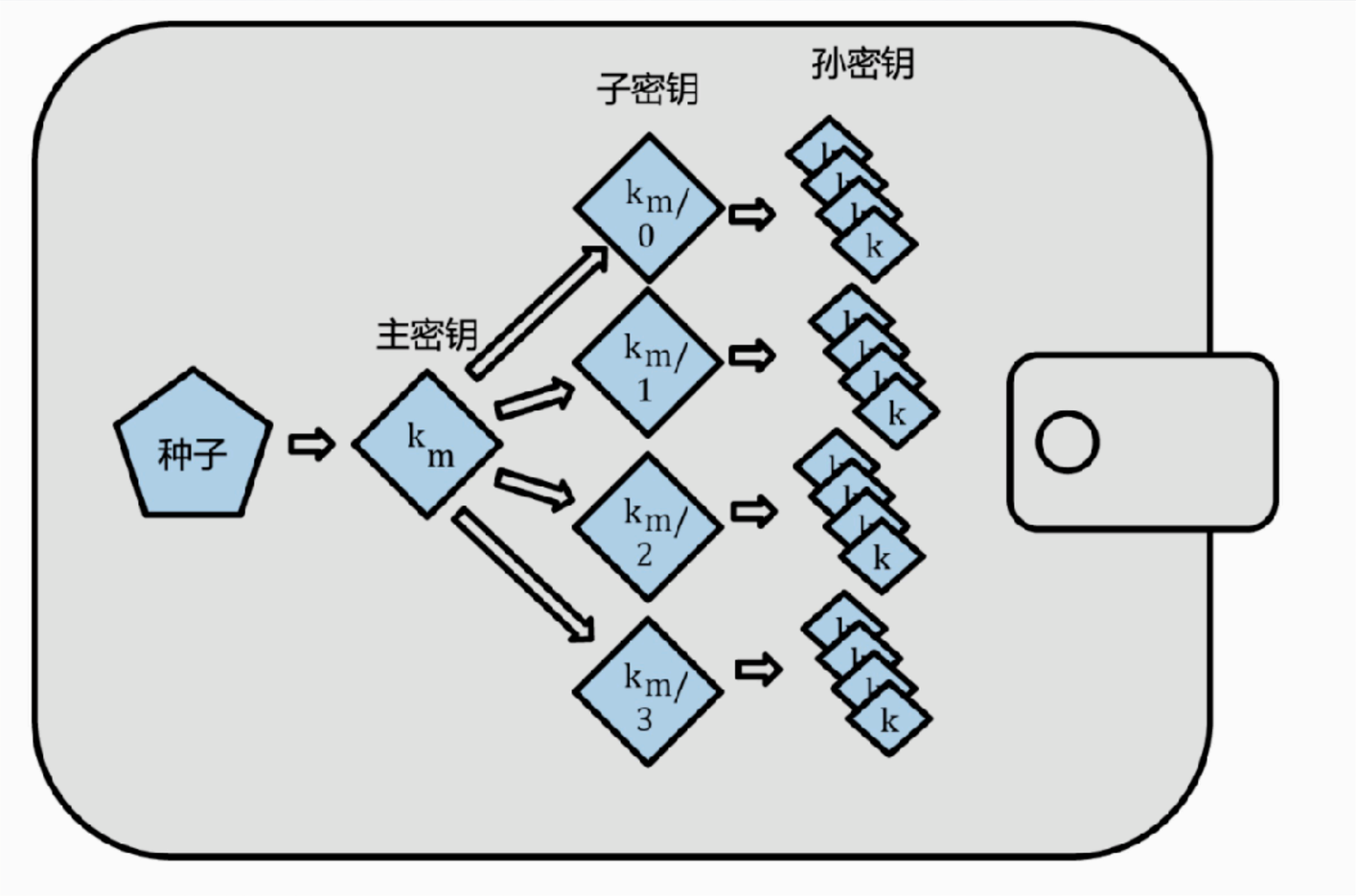
分层确定性推倒

- 随机生成的私钥，备份麻烦，不易管理
- BIP32 提案（HD钱包）：由同一个种子，就可以生成无数个私钥和地址
- BIP44 提案： 给给bip32的路径赋予意义来支持做多币种、多地址
- BIP39: 使用助记词的方式，生成种子

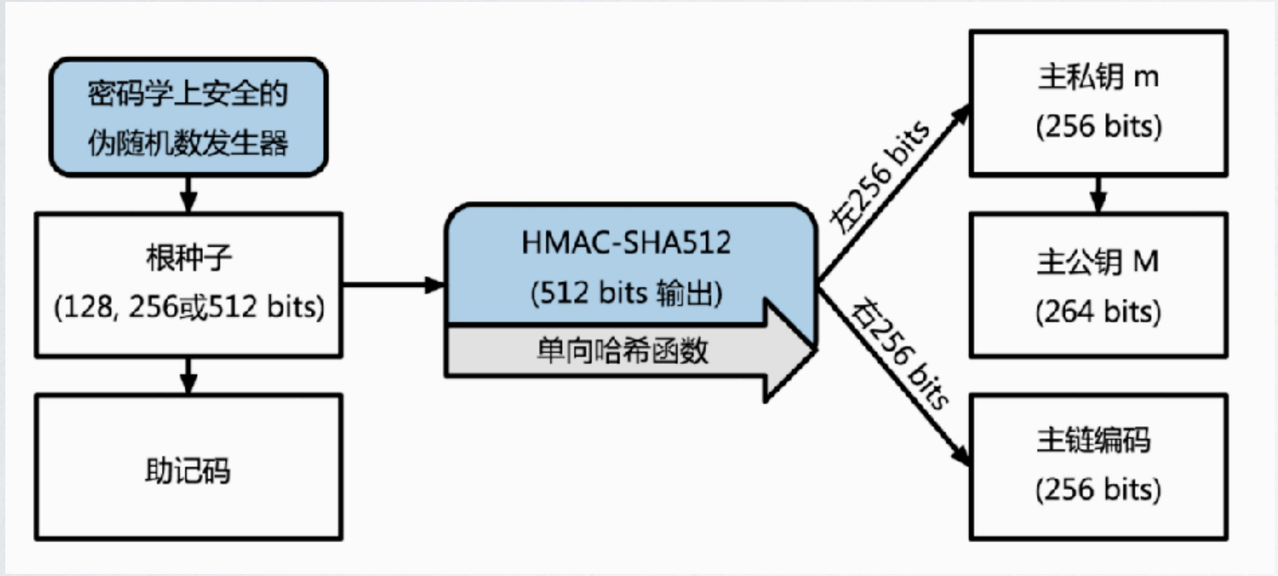
BIP32

种子推倒生成私钥

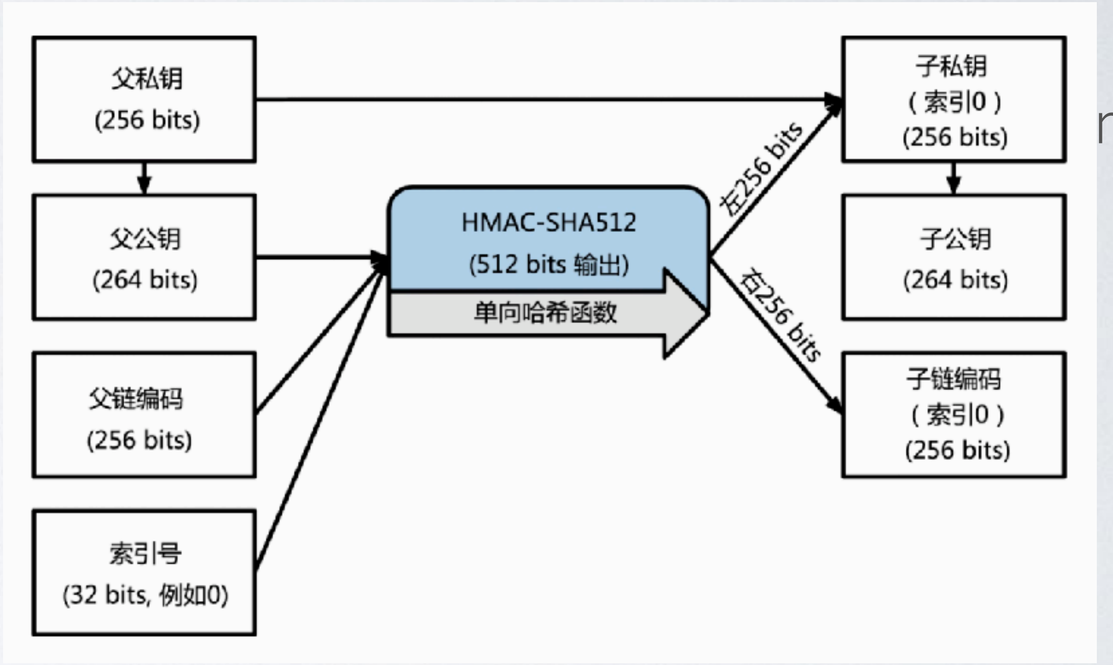
https://learnblockchain.cn/2018/09/28/hdwallet/



BIP32 / BIP44



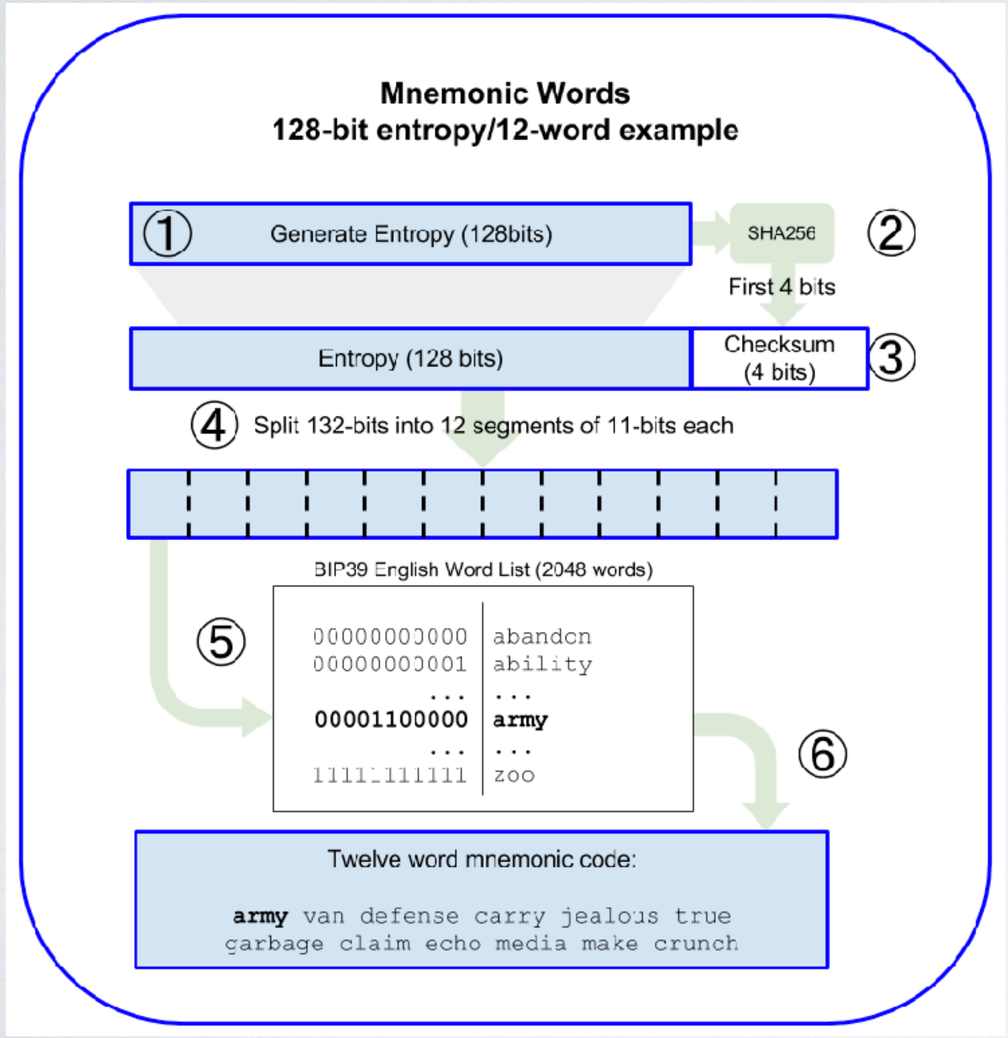
m/0/0

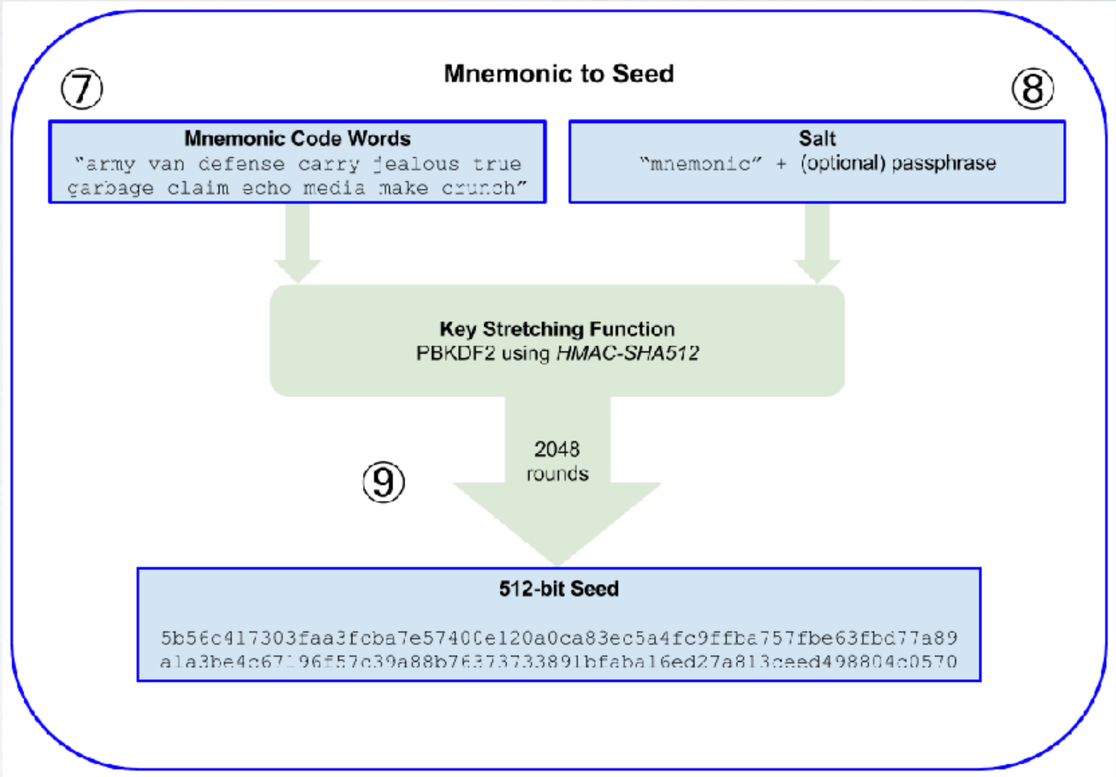


m/0

BIP44: m / purpose' / coin' / account' / change / address_index

BIP39





Demo: OpenSpace100/account_demo/create_by_mnemonic.js

合约账户 -> 智能合约钱包

- 外部账户（EOA）与 合约账户在 EVM 层面是等效的，都是有：nonce（交易序号）、balance（余额）、storageRoot（状态）、codeHash（代码）
- 如果该合约可以持有资金、调用任意合约方法，就是一个智能合约钱包账户
- 智能合约钱包：支持多签、multicall、密钥替换、找回
- ERC4337： 抽象掉 EOA 与 智能合约钱包的区别

https://learnblockchain.cn/article/5426

智能合约钱包

Demo： OpenSpace100/blockchain-tasks/solidity_sample_code/ContractWallet.sol

多签钱包SAFE

https://safe.global/wallet

作业

- 实现一个简单的多签钱包， 功能：
  - 多签持有人可提交交易
  - 其他多签人确认交易（使用交易的方式确认即可）
  - 达到多签门槛、任何人都可以执行交易

https://decert.me/quests/f832d7a2-2806-4ad9-8560-a27ad8570c6f