比特币

自我保管钱包的内核和体验

曾汨 BTCStudy.org 贡献者

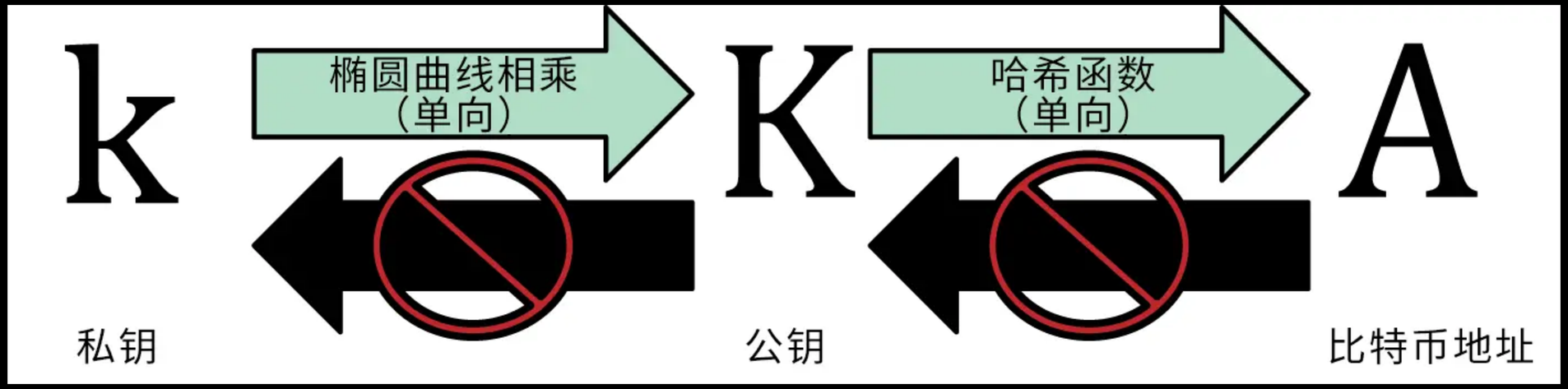
大纲

钱包基础入门

自我保管实践

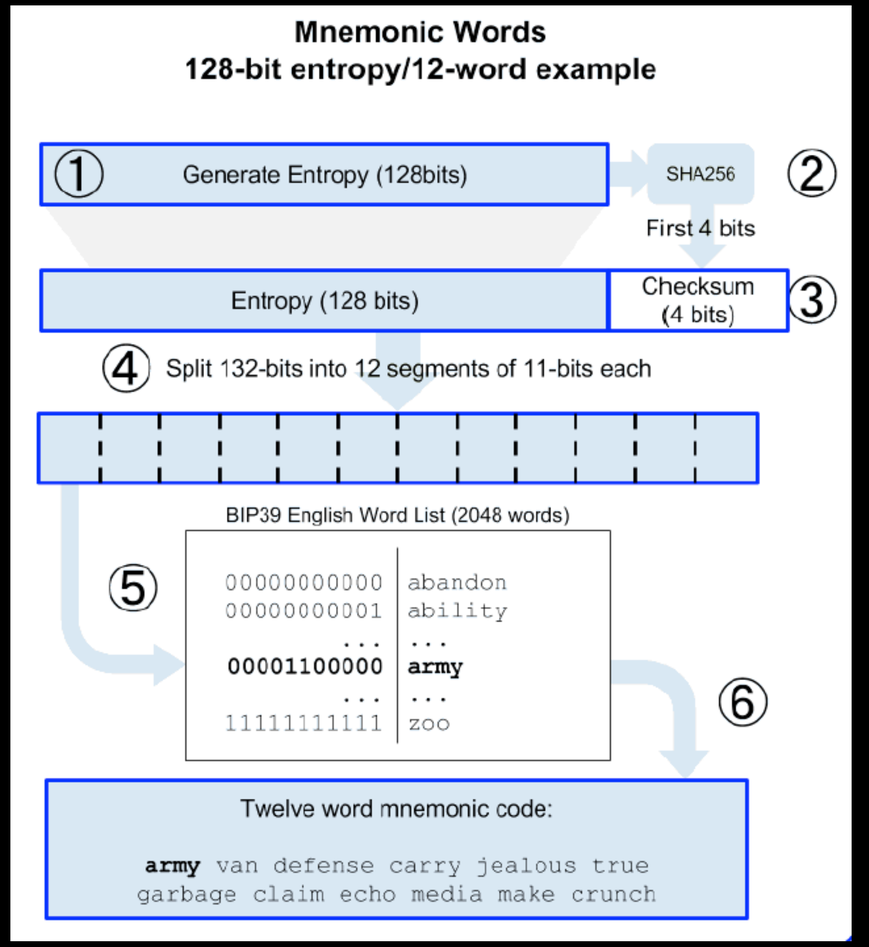
解锁未来可能

钱包基础

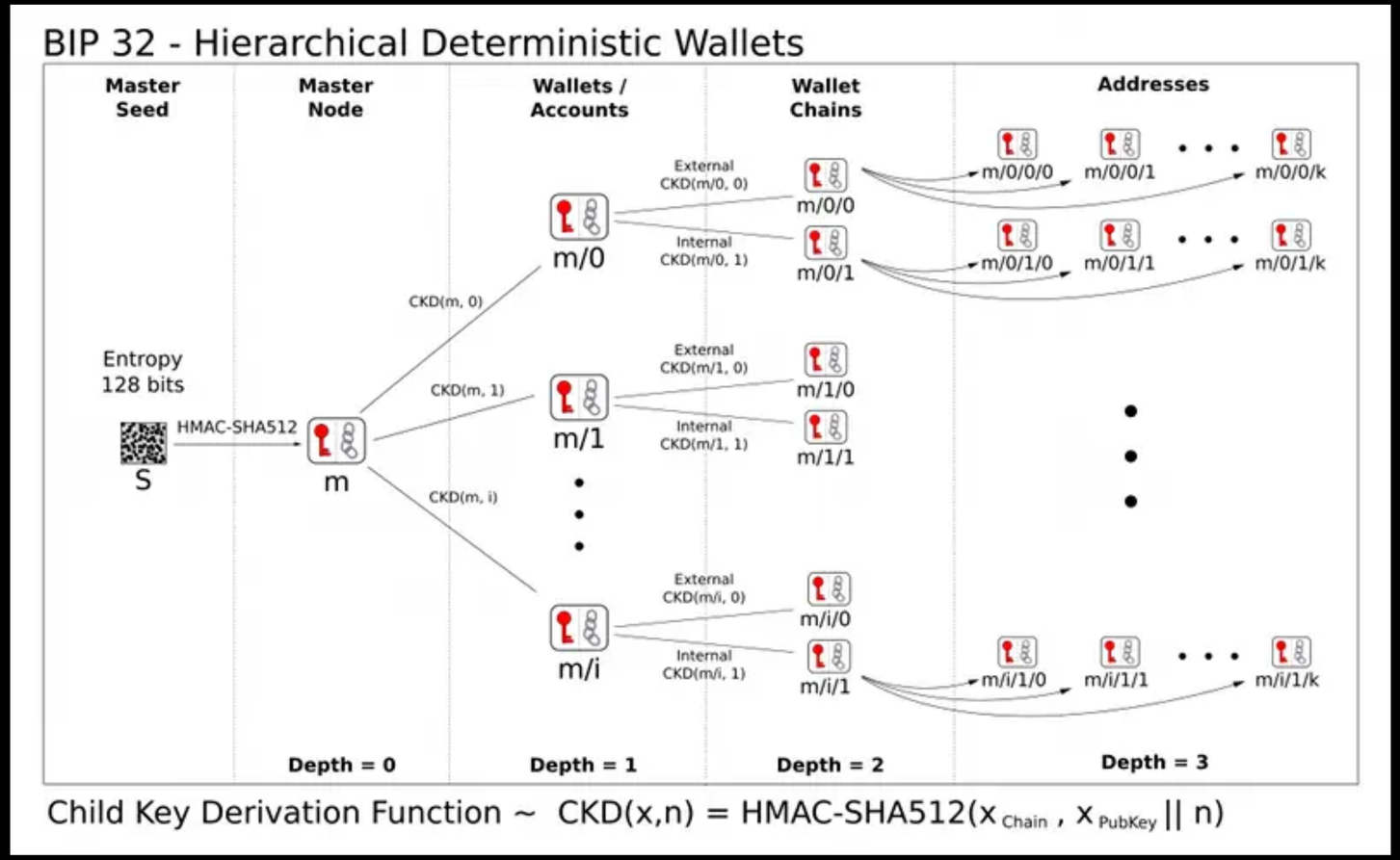


https://learnmeabitcoin.com/technical/keys/

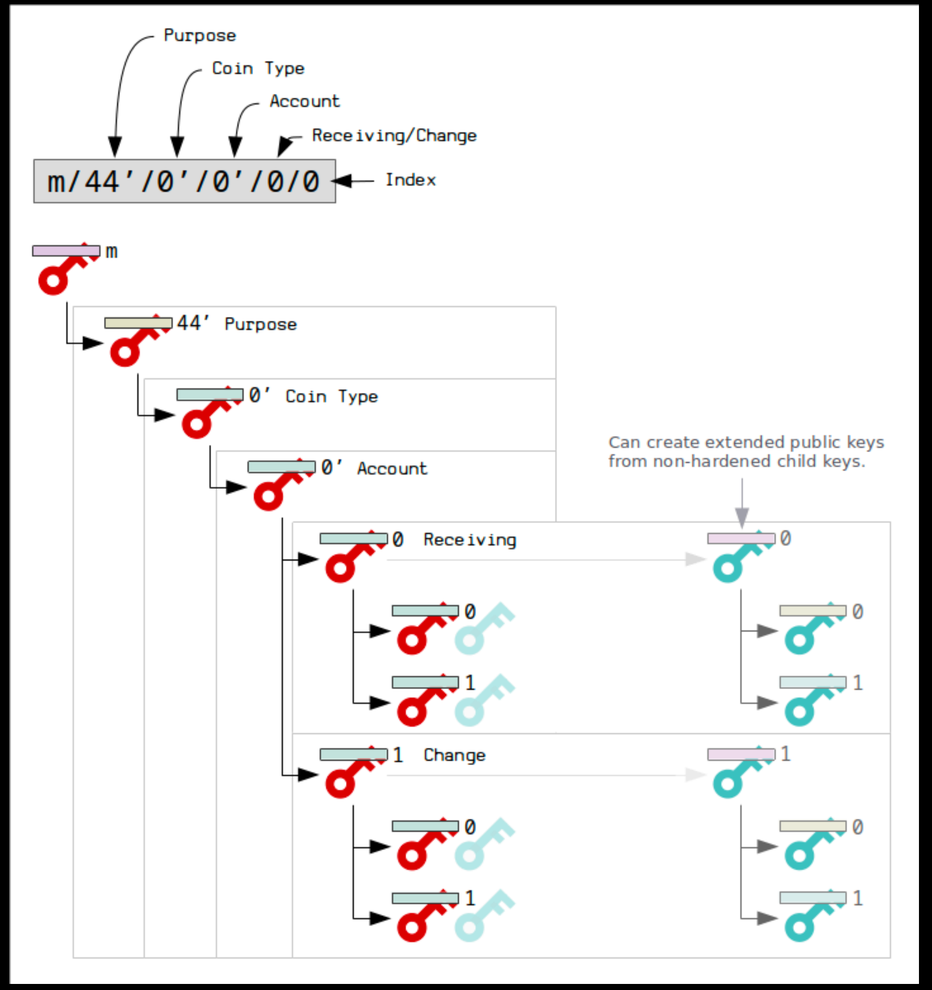
BIP39：助记词


Mnemonic Words
128-bit entropy/12-word example
① Generate Entropy (128bits)
SHA256
②
First 4 bits
Entropy (128 bits)
Checksum (4 bits)
③
④ Split 132-bits into 12 segments of 11-bits each
BIP39 English Word List (2048 words)
⑤
00000000000 abandon
00000000001 ability
... ...
00001100000 army
... ...
11111111111 zoo
⑥
Twelve word mnemonic code:
army van defense carry jealous true
garbage claim echo media make crunch

BIP32：确定性密钥派生



BIP44：派生路径


Purpose
Coin Type
Account
Receiving/Change
m/44'/0'/0'/0/0
Index
m
44' Purpose
0' Coin Type
0' Account
0 Receiving
1 Change
Can create extended public keys
from non-hardened child keys.

什么是比特币钱包?

比特币钱包并不保存比特币！

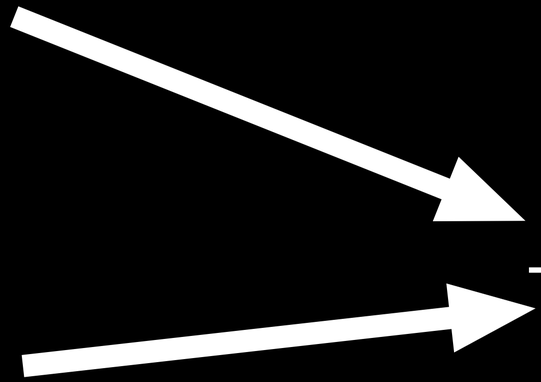
什么是比特币钱包?

存储和管理私钥

构造交易

生成数字签名

与比特币网络通信



解析交易

~~硬件钱包~~

硬件签名器

软件钱包

观察钱包

一个典型的比特币钱包

https://sparrowwallet.com/

如何选择比特币钱包?

BTC-Only

开源可验证。Don’t trust, verify!

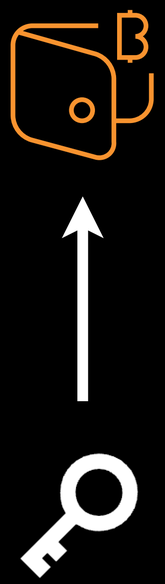
基于标准

地址复用 ❎

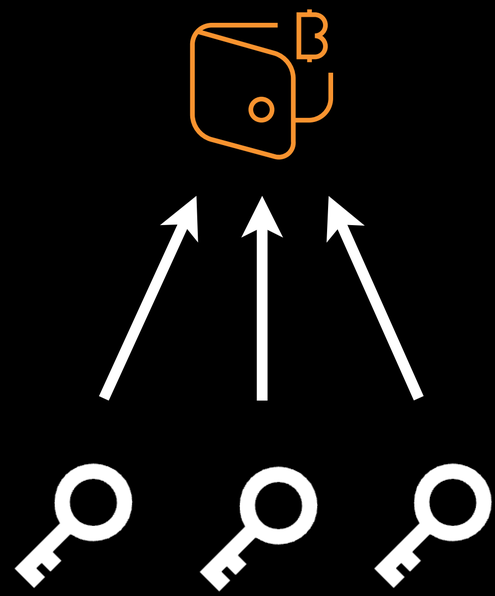
连接自己的节点

自我保管钱包的类型

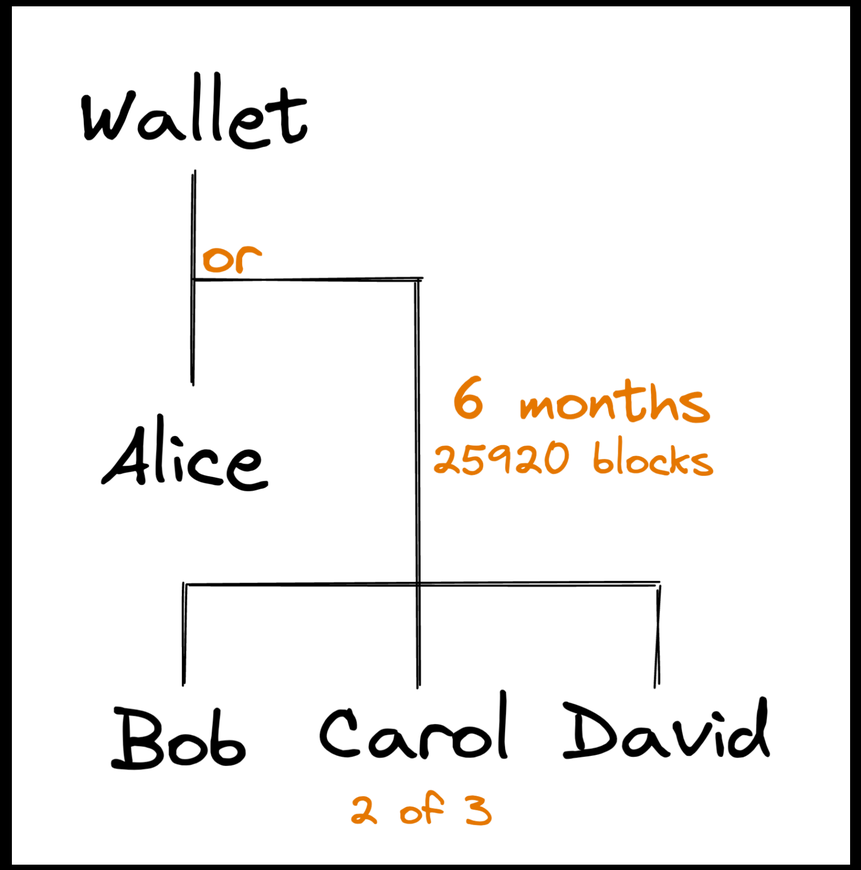
单签名钱包



多签名钱包



Timelocks 时间锁



基于时间锁和多签名的社交恢复钱包

困境

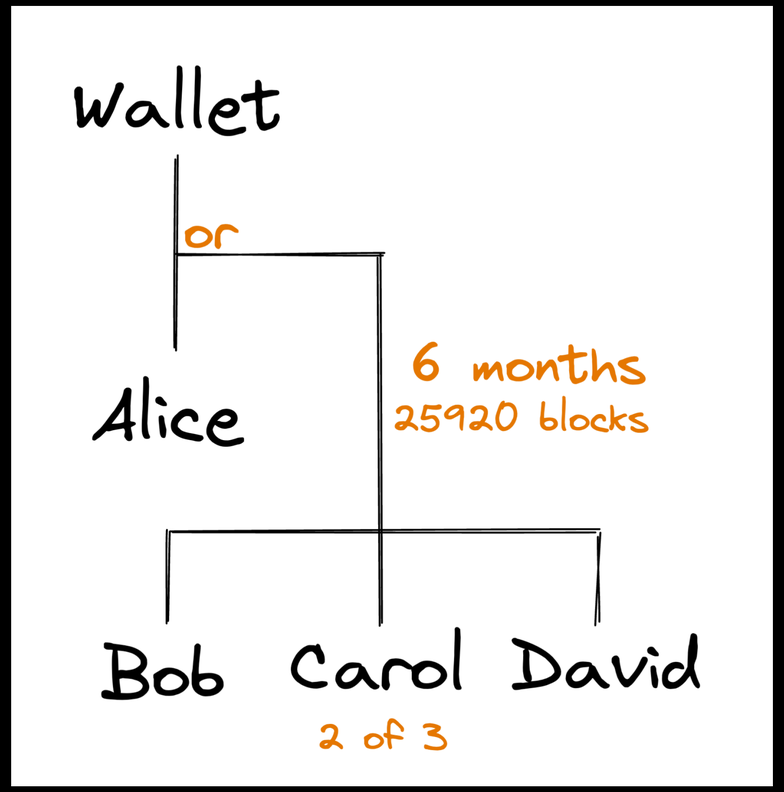
困境 1

难以编程花费策略（spending policies）

困境 2

钱包间缺乏可组合性

Bitcoin Script



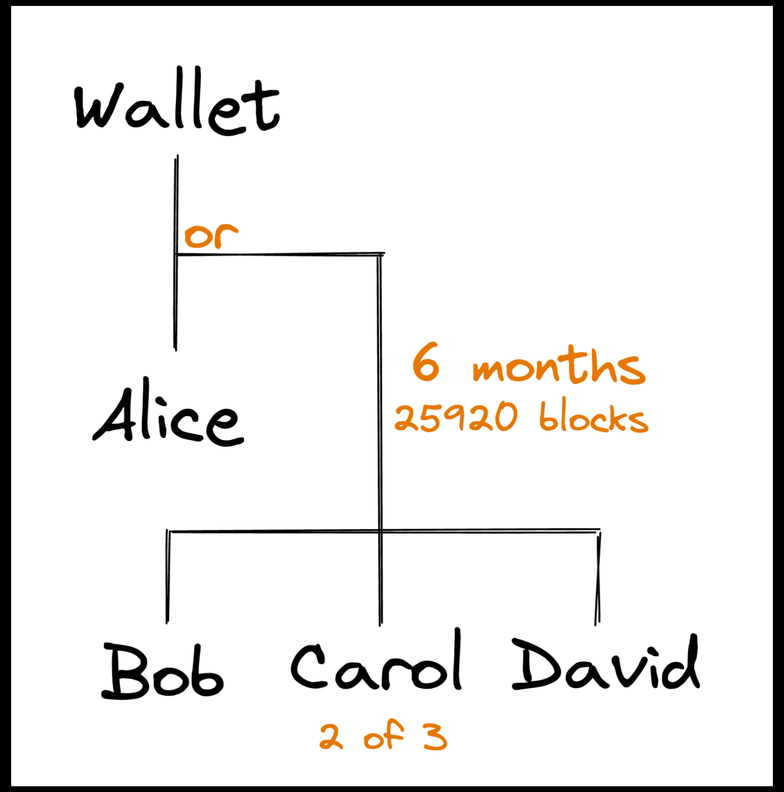
<A> OP_CHECKSIG

OP_IFDUP OP_NOTIF

2 <B> <C> <D> 3 OP_CHECKMULTISIGVERIFY <4065> OP_CHECKSEQUENCEVERIFY

OP_ENDIF

Bitcoin Script



<A> OP_CHECKSIG

OP_IFDUP OP_NOTIF

2 <B> <C> <D> 3 OP_CHECKMULTISIGVERIFY <4065> OP_CHECKSEQUENCEVERIFY

OP_ENDIF

Bitcoin Script

Script 的问题

- 难以编程
- 难以分析
- 难以预估开销
- 难以组合

```
<A> OP_CHECKSIG
OP_IFDUP OP_NOTIF
  2 <B> <C> <D> 3 OP_CHECKMULTISIGVERIFY <4065> OP_CHECKSEQUENCEVERIFY
OP_ENDIF
```

Miniscript 迷你脚本

描述资产要满足的花费条件，而非要机器要执行的操作指令。

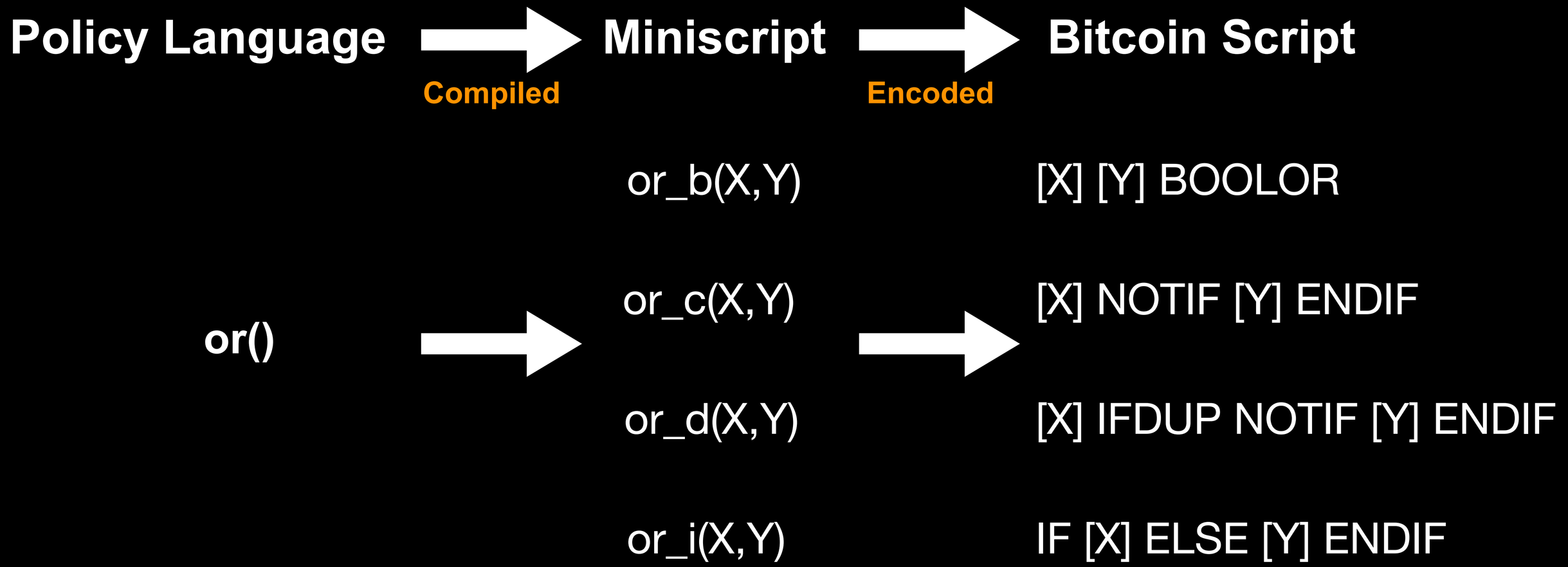
- 为常用的 Script 创建模版：timelocks、signature checks、hashlocks
  - pk(A) ➡️ <A> CHECKSIG
  - after(NUM)、older(NUM) ➡️ CLTV、CSV
  - multi(2,B,C,D) ➡️ 2 <B> <C> <D> 3 CHECKMULTISIG
- 为可组合的逻辑创建模板： AND、OR、thresholds
  - and(A,B) 、or(A,B)、thresh(2,A,B,C)

Miniscript

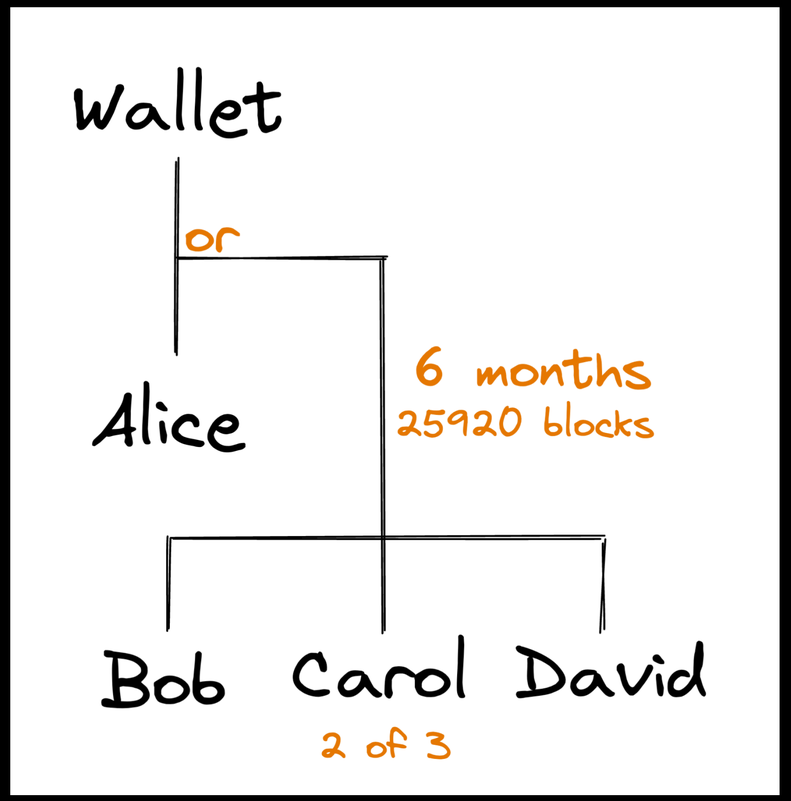
Policy Language → (Compiled) **Miniscript** → (Encoded) **Bitcoin Script**

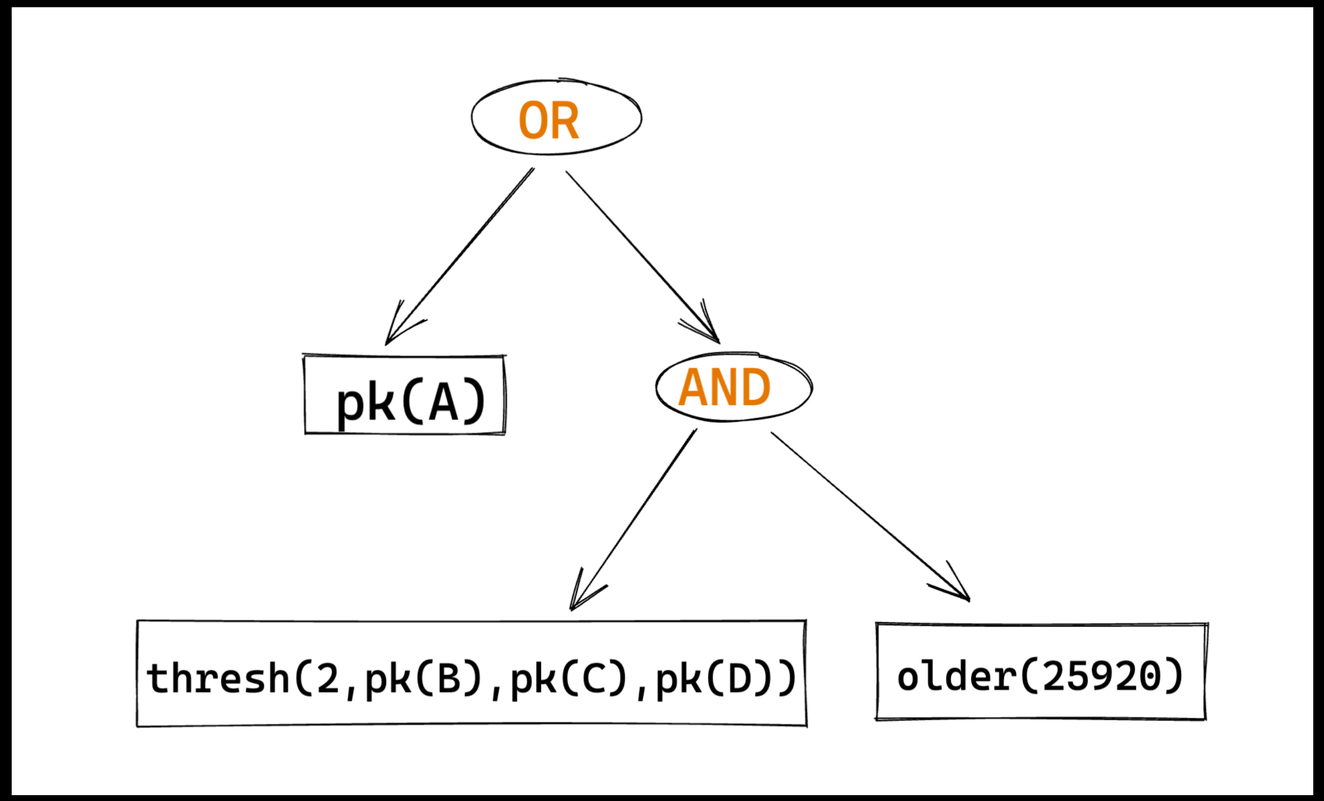
- pk()
- older()
- after()
- and()
- or()
- thresh()
- sha256()
- hash256()
- hash160()
- ripemd160()

Miniscript

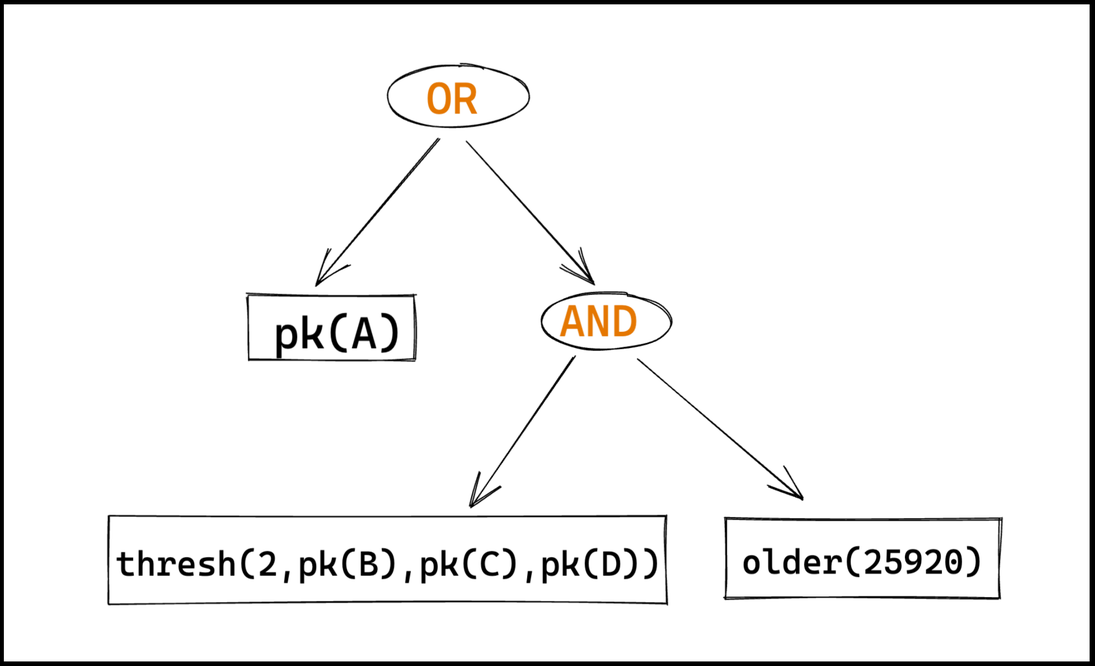

Policy Language
Compiled
Miniscript
Encoded
Bitcoin Script
or_b(X,Y)
[X] [Y] BOOLOR
or()
or_c(X,Y)
[X] NOTIF [Y] ENDIF
or_d(X,Y)
[X] IFDUP NOTIF [Y] ENDIF
or_i(X,Y)
IF [X] ELSE [Y] ENDIF

Miniscript


Wallet
or
Alice
6 months
25920 blocks
Bob
Carol
David
2 of 3


OR
pk(A)
AND
thresh(2,pk(B),pk(C),pk(D))
older(25920)

Miniscript



Policy Language or(pk(A), and(older(25920), thresh(2, pk(B), pk(C), pk(D))))

Miniscript

Policy Language

or(pk(A), and(older(25920), thresh(2, pk(B), pk(C), pk(D))))

Compiled

Miniscript

or_d(pk(A),and_v(v:multi(2,B,C,D),older(25920)))

Encoded

Bitcoin Script

<A> OP_CHECKSIG
OP_IFDUP OP_NOTIF
2 <B> <C> <D> 3 OP_CHECKMULTISIGVERIFY <4065>
OP_CHECKSEQUENCEVERIFY
OP_ENDIF

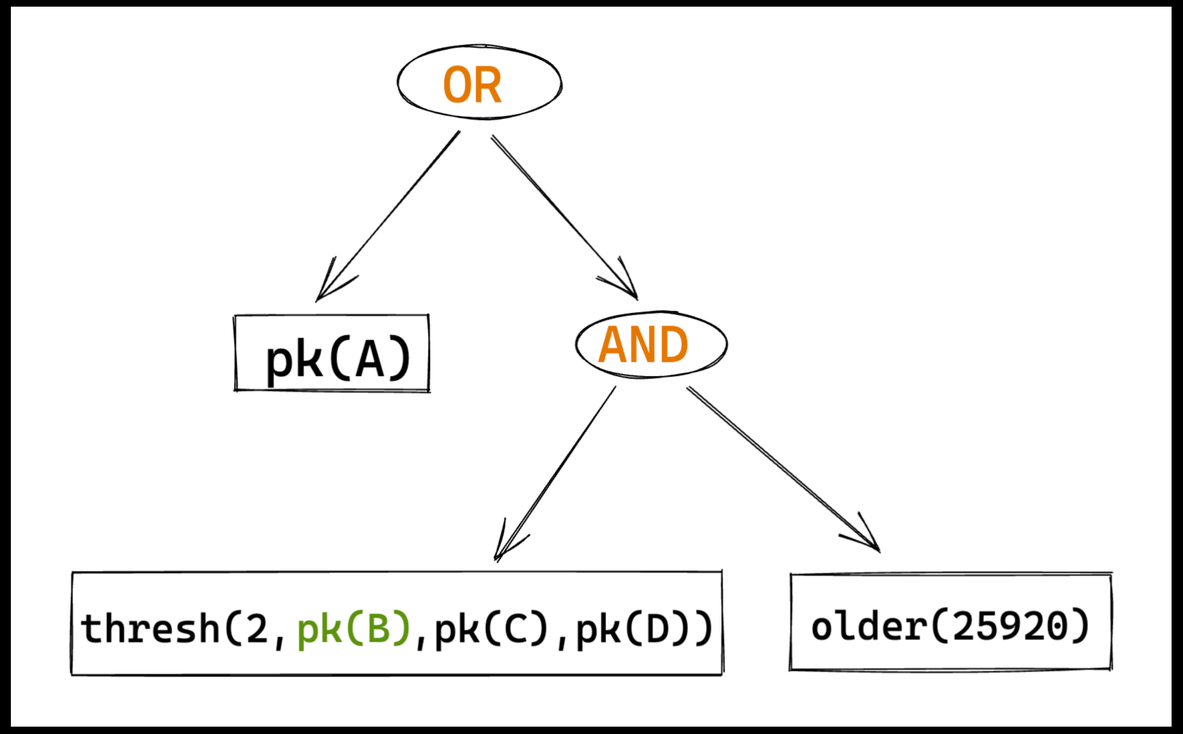
Miniscript

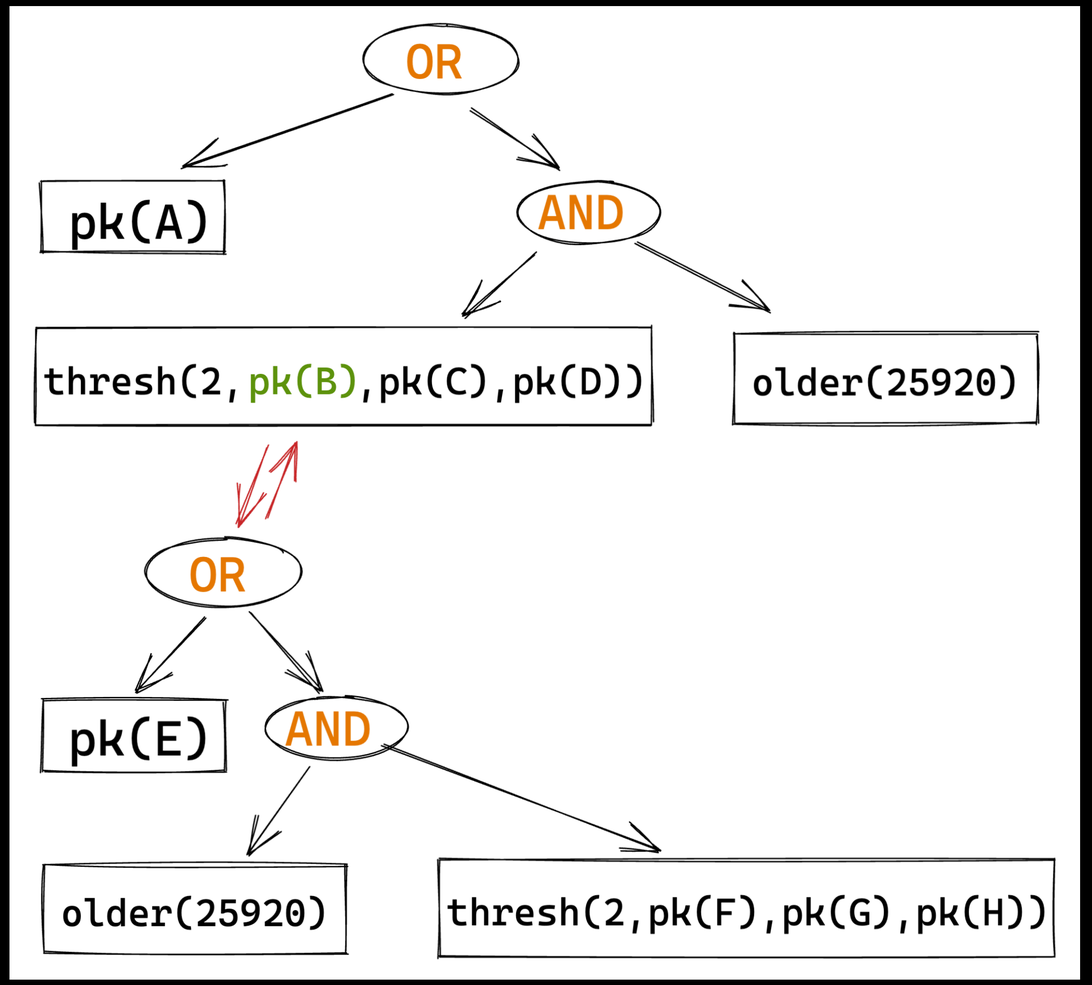
可分析　　可计算　　可组合

https://bitcoin.sipa.be/miniscript/

or(pk(A), and(older(25920), thresh(2, pk(B), pk(C), pk(D))))

可组合　　轻松将某个 key 替换成另一个完整的花费策略





如何解决钱包间的可组合性困境?

Output Descriptors 输出描述符

告诉钱包如何找到和花费你的比特币

Descriptors： address type(spending policy)#checksum

```
wsh(sortedmulti(2,[73f11d36/48h/0h/0h/2h]xpub6E9PLd6JNV5FJq35D
D2MXLaPvKkz7BLVjsiVPWRwL4hmv4oaPCUqUC6mrmABrcuExx2b55YN94Gw5Hs
rbC8P3w7ScxtJ37ytKarKNyrsNw7/<0;1>/*,[3047ea38/48h/0h/0h/2h]xp
ub6Eyn1SSBYndAMB9j7h3tyShcxqjU8YC5hNqnnBBsPdYdK2Bxt2Tk3QtCdP7A
K8RNE2vDoLFWM3UTZaqXKoGJ6a7TQn1e1vnCiGzSKt3U9vw/<0;1>/*,[cf586
77d/48h/0h/0h/2h]xpub6EJQe5cWV2KzhSikSEqPTD8WKfZqBw7NrP15Yp7d2
XFcuTpDZrMfPJmNvbeYBTrPs6d9srCSQ7pWFaT9xu3sPFzNPLwkBdMu9d1vnJn
871t/<0;1>/*))#9t03rtqn
```

-Example-

案例

社交恢复 & 继承

无需备份主要路径的 “单” 签名钱包

专为 HODLer 打造的强制储蓄钱包

……

Supported Wallets

Software

Liana

MyCitadel

Hardware

LEDGER

BitBox02

COLDCARD

Specter DIY

相关链接

Learn Me A Bitcoin

Sparrow Wallet

播客：挑选比特币钱包的自我修养

利用树莓派运行比特币全节点

比特币多签指南

Miniscript 编译器

Q&A