人饼合一·高级脑完全手册

面向主权个体与进阶持有者的自主密钥工程指南（第二版·2026 年修订）



价值观决定认知

认知决定判断力

判断力决定选择

选择决定结果

I COME, I SEE, I HODL.

作者：达哥（@BTCDAGE）

本书中的演示口令及公开示例仅用于学习，请勿用于存放真实资产。

序言：从一把钥匙说起

想象一下，你出门旅行，随身带着一把重要的钥匙。钥匙可能丢在路上，保险箱可能损坏，写在纸上的秘密也可能被人看见。有没有可能把找回钥匙的方法，留在自己的记忆和一套确定的规则里？这就是本书想和你一起探讨的问题。即使你从未接触过比特币，也可以从第一章开始，逐步理解钱包、私钥和高级脑的基本思想。

很多人谈到比特币安全，首先想到加密算法、随机数和密钥长度。这些当然重要，但安全从来不只发生在算法里面。私钥从哪里来，规则由谁掌握，材料怎样组织，工具怎样执行，秘密经过哪些设备，使用者能否记住并在多年后重新生成，家人能否在意外发生后恢复——这些事情连在一起，才是现实中的安全。密码学提供坚实的数学工具，工程学把这些工具、人的记忆、设备和生活安排成一套真正能使用、能维护的体系。高级脑就是从这条路出发。

本书强调“确定性不等于可预测性”。同样的材料，按照同样的规则，必然得到同样的结果；但这不代表旁人知道材料和规则。高级脑把个人信息指针与秘密算法 F 放在生成过程的中心：信息指针来自个人经历，F 由使用者自主设计并掌握。SHA-256 是公开的散列工具，公开工具并不意味着个人的材料和规则也必须公开。

“高级脑消除随机性”有明确范围：当初始材料和完整规则事先确定后，生成阶段不再临时抽取随机数，同样的材料经过同样的步骤，必然得到同样的结果。初始材料可以来自可靠的随机来源，也可以来自个人事先确定的信息。高级脑要解决的是如何由本人掌握材料、规则和复现过程，而不是把“确定性”误解成“任何人都能预测”。

我希望用生活化的比喻讲清楚技术。你会看到：密码像钥匙，生成规则像配钥匙的方法，备份像为家人留下一张可靠的路线图。我们也会讨论 SHA-256、BIP39、离线工具、恢复与继承。每个概念都尽量先用故事说明，再用更准确的术语解释。理论可以不断进步，但资产安全的代价不容轻率。

本书讨论高级脑的思想与实践方法，也提醒读者认识自定义密钥方案的风险。书中的理念不能代替独立审查和实际测试。涉及真实资产时，必须先验证工具与规则，完成备份、恢复和签名演练，再决定是否采用。

——达哥（@BTCDAGE）

2026 年 11 月

https://btcdage2011.github.io

https://btcdage.rf.gd

Nostr：npub17ahz4xa3hvkvvhh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

阅读指南：先学会提问，再理解技术

全书共 14 章。前四章从零讲起，介绍比特币与钱包；第五至七章讲高级脑的思想、确定性计算与秘密规则；后面依次进入生成、验证、备份、地址、风险及实战。你无需具备编程或密码学基础，也无需查阅任何旧版本。先读生活中的比喻，再看技术解释和练习题。下面先约定几个讨论边界。

公约一丨固定输入、固定规则、固定结果。以 K=F(x)概括高级脑的确定性生成过程；使用者掌握完整 F 和 x 时，可以准确复现 K。生成阶段不需要临时抽取随机数。

公约二丨以 SHA-256 作为最终散列的基础标准。F 由使用者自主设计，可以包括信息指针、秘密材料、编码、拼接、迭代、序号和其他确定性步骤。中间步骤允许采用 SHA-256、SHA-512 或多个散列结果组合，但不建议用低于 SHA-256 强度的散列算法削弱处理链；无论中间如何组合，最终输出仍按既定的 256 位结果生成。

公约三丨为讨论短输入经散列后的表示形式，部分章节会举 UTF-8 编码不足 32 字节的例子。这只是教学场景，不是安全分界线。完整安全性要看个人信息指针、秘密规则 F、初始脑口令和整个生成过程，不能只看某一段输入的长度。

公约四丨把数学性质放在正确的位置。SHA-256 提供固定的 256 位散列结果及成熟的抗碰撞、抗原像能力。高级脑不以随机性或香农熵作为设计目标；它关注个人信息指针、秘密规则 F 和确定性生成过程如何共同构成安全体系。讨论时应说明算法性质，也要把完整生成规则放在眼前。

公约五丨把安全放在完整生命周期中考虑。从初始脑口令、信息指针和 F 的设计，到工具运行、私钥生成、地址使用、备份、恢复和继承，每一步都要安排清楚。任何一环出错，都可能影响最终安全。

公约六丨高级脑有明确的主张，但不靠口号代替设计。我们主张由使用者掌握自己的秘密规则和生成过程，尽可能减少对黑盒设备、厂商和外部服务的依赖。要让这套方法真正可靠，规则必须经得起复现，工具必须经过检查，备份必须经过恢复测试。

寓教于乐的小练习：同样使用公开的 SHA-256，甲知道输入和规则，乙只知道输入可能来自一组常见材料，丙既不知道个人信息指针的具体取法，也不知道完整的秘密规则 F。三人面对的条件是否相同？答案将在第六章展开。

我们根本不是密码学演进，而是私钥管理安全的演进。高级脑不重新发明 SHA-256，也不改变比特币的密码学规则；它重新思考的是个人如何生成、掌握、备份和恢复自己的私钥。

目录

序言：从一把钥匙说起 2

阅读指南：先学会提问，再理解技术 3

第一章：认识比特币——数字黄金，自由之钥 10

1.1 前言：打破束缚，财富的新篇章 10

1.2 什么是比特币？——一个全球共享的电子账本 11

1.3 比特币的特点——去中心化、假名性、稀缺性、全球流通 11

1.4 比特币的发行和总量限制：——“挖矿”与减半机制 11

1.5 为什么比特币有价值？——三重价值的体现 12

1.6 小结：比特币——自由、透明的未来 12

延伸阅读丨把“控制权”与“风险”一起讲明白 13

第二章：比特币钱包——你的数字金库，私钥的守护者 14

2.1 比特币钱包：并非“装币”的钱包 14

2.2 私钥：通往财富大门的钥匙 14

2.3 公钥：可以公开的“银行账号” 15

2.4 地址：接收比特币的“收件箱” 15

2.5 私钥、公钥和地址的关系：一把钥匙、一把锁、一个邮箱 15

2.6 重点强调：私钥、公钥、地址与比特币网络的独立性 16

2.7 钱包的功能：私钥的管理专家 16

2.8 小结：私钥是比特币安全的基石 17

延伸阅读丨“钥匙—门锁”比喻的边界 17

第三章：钱包的种类——百花齐放，各有所长 18

3.1 钱包的分类：连接网络与否 18

3.2 常见的钱包类型：各有侧重，各有优缺 19

3.3 深入了解：BIP39 助记词——从随机熵到确定性派生 20

3.4 对比总结：选择适合自己的钱包 20

3.5 小结：了解钱包，才能更好地保护你的资产 21

延伸阅读 | 随机源风险是故障模式，不是所有随机方案的定论 21

第四章：初识脑钱包——把私钥藏在你的大脑里 22

4.1 脑钱包：私钥的“终极”存储方式 22

4.2 脑口令：开启财富之门的“咒语” 22

4.3 脑钱包的工作原理：将记忆转化为私钥 23

4.4 脑钱包的优点：无需设备，私密安全 23

4.5 “一维脑钱包”的风险：口令至关重要，记忆不可靠 23

4.6 为什么我们不建议直接使用“一维脑钱包”？ 24

4.7 小结：脑钱包的理念，高级脑钱包的基础 24

延伸阅读 | 记忆不是万能保险箱 25

第五章：为什么我们需要高级脑钱包？ 26

先把本书的立场说清楚。普通人谈比特币安全，往往只想到加密算法、随机数和密钥长度，仿佛只要选对算法，安全就自然有了。可现实不是这样。算法要由人设计、由工具执行、由人保存和恢复。设备可能被篡改，供应链可能出问题，随机数路径可能实现错误，备份也可能遗失。只研究加密学，不研究整个系统怎样运行，就看不见许多真正的风险。高级脑强调工程学，就是要把这些环节放在一起考虑。 26

高级脑首先相信一个朴素的事实：每个人的生命经验都不一样。你忘不了的事，别人可能从未听说；别人珍藏的记忆，对你也可能毫无意义。信息指针正是从这里来。它不是统一发给所有人的标准口令，而是每个人从自己的经历中找到的线索。 26

5.1 普通脑钱包的局限性：看似安全，实则危机四伏 26

5.2 高级脑钱包：从“一维”到“多维”的飞跃 27

5.3 高级脑钱包的核心思想：确定性不等于可预测性 27

5.4 高级脑的特点：自主设计与整体安排 28

5.5 高级脑钱包的必要性：避免“一维脑”的风险 28

5.6 小结：高级脑钱包——安全与便捷的完美结合 29

延伸阅读 | 规则设计要落到现实生活 29

第六章：高级脑的工程安全基础——从算法走向完整系统 30

本章会讲必要的密码学知识，但全书的视角是工程学。我们要看算法怎样进入人的生活：秘密从哪里来，规则由谁掌握，设备是否可信，结果能否复现，发生意外后能否恢复。只知道加密学，却不理解工程过程，就容易把某个算法或设备当成全部安全。 30

6.1 为什么我们要了解安全性基础？——磨刀不误砍柴工 30

6.2 哈希算法：神奇的“信息指纹” 31

6.3 抗碰撞性：避免“撞衫”的秘密 31

6.4 散列性：让输入经过充分扩散 32

6.5 从一个字母到 64 个十六进制字符：先问清楚“复杂”是什么 32

6.5.1 表示空间容量 RSC——一个教学指标 32

6.5.2 信息论概念与高级脑的设计目标 32

6.5.3 从数学性质回到现实使用 33

6.6 SHA-256 与个人秘密规则 F 33

6.6.1 三个一眼就懂的实验 33

6.6.2 把私钥管理看成一项完整工程 33

6.7 如何利用这些知识，设计更安全、更易继承的高级脑钱包？—— “信息的指针记忆法” 34

6.8 小结：利用安全性基础，构建你的安全堡垒 36

延伸阅读｜研究公约与三个容易混淆的数字 37

第七章：设计你的高级脑钱包算法——打造独一无二的“秘籍” 39

7.1 设计原则：灵活、安全、易记 39

7.2 设计步骤：从种子到私钥的奇妙旅程 40

7.3 设计高级脑钱包算法 41

延伸阅读｜一份可复现的算法说明至少包含什么 44

第八章：使用工具生成地址——验证你的规则与生成结果 45

8.1 为什么需要工具？——专业的事情交给专业的工具 45

8.2 选择合适的工具：开源、安全、离线 45

8.3 离线操作的重要性：保护私钥的生命线 46

8.4 使用达哥的 Python 工具生成地址：按步骤操作 46

8.5 验证地址：确保地址的正确性 47

8.6 小结：安全生成你的“加密秘钥” 48

延伸阅读 | 离线不等于可信 49

第九章：安全存储与备份——你的“加密秘籍”的守护之道 50

9.1 为什么需要安全存储和备份？——未雨绸缪，防患未然 50

9.2 “关键脑口令”的特殊性：只记在脑中，不落于纸笔 51

9.3 算法规则的备份策略：打印多份，分散存储 51

9.4 其他脑口令和盐值的备份：灵活选择，多重保障 51

9.5 可继承性：为未来做好准备 52

9.6 小结：妥善保管你的“加密秘籍” 52

延伸阅读 | 备份方案与继承演练是两套测试 53

第十章：HD 钱包、派生路径、多重地址 54

10.1 HD 钱包：一颗种子，无限可能 54

10.2 派生路径：生成密钥的“路线图” 55

10.3 多重地址：管理资产的“分身术” 55

10.4 高级脑钱包与 HD 钱包的思路差异：手动生成 vs 自动派生 55

10.5 高级脑的地址管理理念：自主、隐私与可恢复 56

10.6 小结：高级脑钱包的独特性 56

延伸阅读 | 多地址不等于天然的隐私 58

第十一章：高级脑的工程安全观 59

前面谈过私钥、哈希、规则和地址。本章把视角再拉远一些：安全不是某个算法或某台设备单独提供的属性，而是整套安排共同产生的结果。算法可以正确，设备也可以可靠，但只要使用者记错一个步骤，或者多年后无人知道怎样恢复，资产仍可能失去控制。工程学关心的，就是这些环节如何衔接。 59

11.1 安全不是绝对的：风险无处不在 59

11.2 安全习惯：每天进步一点点 60

11.3 安全是自我责任：没有人可以完全依赖 60

11.4 高级脑钱包工具：只是工具，安全取决于你 60

11.5 高级脑钱包 vs 硬件钱包：优势对比 61

11.6 现实案例：随机数失效与硬件植入——当保险箱在别处出了问题 62
案例一：COLDCARD 随机数路径错误（2026 年 7 月披露） 62
案例二：Ledger 经销渠道的恶意硬件植入（2026 年 10 月披露） 62
从这两起事件理解高级脑的系统安全哲学 63
资料与事件时间线（截至 2026 年 11 月 1 日） 63
11.7 高级脑与多签钱包：精简、自主与冗余的取舍 63
11.8 小结：安全之路，永无止境，不同托管方式的安全取舍 64
延伸阅读丨高级脑的自主安全主张 66
第十二章：比特币安全的未来 67
12.1 量子计算的威胁：未来的隐形敌人 67
12.2 技术发展带来的影响：挑战与机遇并存 68
12.3 高级脑钱包的注意事项：认识局限，不断进步 68
12.4 小结：安全之路，永无止境，共同应对未来挑战 68
延伸阅读丨量子风险不能用“地址未花费”一概化解 70
第十三章：自由之钥，安全同行 71
13.1 回顾：我们走过的旅程 71
13.2 高级脑的精髓：掌握核心，融会贯通 72
13.3 “人饼合一”的真谛：将财富融入生命 72
13.4 展望未来：拥抱变化，探索无限可能 73
延伸阅读丨自由与责任并行 74
第十四章：高级脑钱包实战教程 75
14.1 实战 75
14.2 准备工作 75
14.3 设计高级脑钱包算法 76
14.4 使用工具生成地址 76
14.5 验证地址的正确性 77
14.6 安全存储和备份 78

14.8 常见问题解答 81

14.9 小结 82

延伸阅读｜实战发布安全闸门（务必先读） 83

结语：人饼合一，安全同行，未来由你定义 84

附录 A｜安全术语速查 85

附录 B｜真实资产使用前的十二项核验 86

附录 C｜参考标准与阅读索引 87

第一章：认识比特币——数字黄金，自由之钥



生活中的例子 | 想象一个没有总行长的公共账本：全班同学各自保存一本相同的账本。谁想偷偷改掉一笔旧账，不仅要涂改自己的本子，还得让其他人接受他的版本。比特币的运行机制当然复杂得多，但“许多人独立核对同一套规则”就是理解它的第一步。

1.1 前言：打破束缚，财富的新篇章

你有没有想过，你存在银行里的钱，真的完全属于你吗？或许你会觉得这是理所当然的，但其实，你的钱一直都掌握在银行或者其他金融机构的手中。它们就像是看管你财产的“管家”，虽然大部分时候很尽责，但你依然需要依赖它们。

比特币的出现，就像一股清新的风，吹开了传统金融的限制。它是一种全新的数字货币，一种完全去中心化的财富形式，它第一次让我们有机会真正拥有和掌控自己的资产，不再需要依赖任何第三方机构。就像你的手机，你的钱包一样，你的比特币也应该由你自己掌控，而不是由任何银行或机构来代为保管。

那么，什么是比特币？它又有什么特别之处呢？在这一章中，我们将一起揭开比特币神秘的面纱，带你了解这个正在改变世界的数字奇迹。

1.2 什么是比特币？——一个全球共享的电子账本

想象一下，你现在想给朋友转账。在过去，你可能需要通过银行或者支付宝，对吧？这些机构就像是中间人，它们会记录你的转账信息，并且负责控制资金的流动。

而比特币，却完全不同。它就像一个全球共享的电子账本，记录着每一笔比特币的交易。这个账本不是由任何一家公司或者机构来维护，而是由全球成千上万的电脑共同维护的。这就意味着，没有任何人能够随意篡改或者删除比特币的交易记录，它就像一个公开透明的“大账本”，记录着每笔交易的来龙去脉。

更重要的是，这个账本是完全去中心化的。没有哪一个人或者机构可以控制它，这也意味着，我们不再需要依赖银行或者支付机构，就能自由的进行交易。

1.3 比特币的特点——去中心化、假名性、稀缺性、全球流通

比特币之所以如此特别，是因为它具有以下四个重要的特点：

- 去中心化（Decentralization）： 比特币不是由任何一家公司或者政府来控制的，而是由全球成千上万的计算机共同维护的，就像一个社区，公共事务不是由某个领导说了算，而是由大家共同商议决定的。这意味着，没有哪一个人或者机构能够随意修改比特币的规则。
- 假名性（Pseudonymity）： 比特币的地址就像一串神秘的代码，它并不直接对应你的真实身份。就像你在网上购物，商家只知道你的收货地址，并不知道你的具体身份。这在一定程度上保护了你的隐私。当然，这并不意味着比特币具有完全匿名性，但它确实比传统的金融系统更保护用户的隐私。
- 稀缺性（Scarcity）： 比特币现行共识规则将最终发行总量限制在约 2100 万个。如同稀有的黄金，因为它数量有限，所以价格昂贵，比特币也因为其有限的总量而具有一定的保值作用。
- 全球流通（Global Circulation）： 你可以在全球任何地方使用比特币进行交易，不受国界和汇率的限制。就像你在网上购物，可以从全球任何一个地方购买商品，而不用担心支付问题，比特币的流通也是如此。

1.4 比特币的发行和总量限制：——“挖矿”与减半机制

- 比特币的发行机制： 比特币的发行并非由任何中心机构控制，而是通过一种称为“挖矿”的方式完成。其本质是分布式网络中的节点通过算力竞争，来记录交易并获得新发行的比特币。这个过程依赖于“工作量证明”（Proof of Work, PoW）机制，即矿工需要通过计算机进行大量的复杂运算，竞争记账权，成功后才能将新的交易记录添加至新的区块中。PoW 机制保证了比特币网络的安全性和去中心化特性，因为攻击者需要投入巨大的算力成本才能篡改交易记录。

- 区块奖励： 为了鼓励“矿工”们维护比特币网络的安全，比特币系统会给予成功挖出新区块的矿工一定的比特币奖励。这类似于你帮助朋友整理账目，朋友会给予你报酬。最初，每当矿工成功挖出一个新的区块，就会获得 50 个比特币的奖励。
- “减半”机制： 为了控制比特币的发行速度，比特币系统设定了“减半”机制。每产生 21 万个区块（大约每四年左右），比特币的区块奖励就会减半。这意味着，比特币的发行速度会随着时间的推移越来越慢，最终趋近于零。
  - 最初，每挖出一个区块，奖励 50 个比特币。
  - 21 万个区块后，奖励变为 25 个比特币。
  - 再过 21 万个区块，奖励变为 12.5 个比特币。
  - 以此类推，不断减半。
- 总量的限制： 由于“减半”机制的存在，比特币现行共识规则将最终发行总量限制在约 2100 万个。这与黄金的总量有限相似，使其具有稀缺性和保值潜力。
- 比特币交易的确认： 当一笔比特币交易发生后，需要被矿工打包进新的区块中。为了确保交易的不可逆转，该交易需要在区块链上经过若干个区块的确认。通常，6 个区块确认（大约 1 小时）被认为是比较安全的确认数。这意味着这笔交易被记录在区块链上，并且难以被篡改。

1.5 为什么比特币有价值？——三重价值的体现

比特币的价值，可以从以下三个方面来理解：

- 价值存储（Store of Value）：比特币的稀缺性和不可篡改性，使它可以作为一种价值储存的工具，由于美联储和各国央行一直致力于持续印钞，造成的通胀让你的钱随着时间的推移越来越贬值。而比特币正是对抗印钞机的工具，他给人们一个选择，让通胀无法收割自己的财富。
- 交易媒介（Medium of Exchange）： 在一些地方，你已经可以使用比特币购买商品或者服务，如同你用支付宝或者微信支付一样，你也可以用比特币在商店里购买东西。随着比特币的普及，未来会有越来越多的商家接受比特币支付。
- 投资标的（Investment Asset）： 有越来越多的人开始将比特币作为一种投资资产。就像你买股票或者基金一样，你也可以把比特币作为一种投资，期待它能为你带来收益。他们相信比特币的价值会随着时间的推移而增长，因此长期持有。

1.6 小结：比特币——自由、透明的未来

比特币是一种去中心化的数字货币，具有假名性、稀缺性和全球流通等特点。它不仅是一种支付工具，也可以作为价值储存和交易媒介。它代表着一种不同于传统金融体系的价值转移方式。

但要真正理解比特币，并掌控自己的比特币资产，我们还需要进一步了解比特币钱包，以及如何安全地管理私钥。在接下来的章节中，我们将深入探讨这些问题。

本章小测验：

1. 比特币的总量是多少？
2. 什么是“挖矿”？
3. 比特币的“减半”机制是什么？

延伸阅读丨把“控制权”与“风险”一起讲明白

比特币赋予个人直接持有密钥、独立验证交易的能力，但私钥自托管也意味着本人需要承担操作、备份与继承责任。公开链记录具有可追踪性，“假名”不等于不可识别。对于新手，先用小额练习接收、找零与恢复，比立即追求复杂技术更重要。

想一想：一个完全拥有私钥的人，如果从未验证过恢复流程，是否已经具备完整的资产控制能力？

第二章：比特币钱包——你的数字金库，私钥的守护者



生活中的例子 | 你家的现金不会真的存在手机银行 App 的图标里。同样，比特币也不是一个个小金币装在钱包软件内。钱包更像管理钥匙的工具箱：钥匙决定你能否授权使用相应的资产，工具箱则负责让钥匙更方便、更安全地使用。

2.1 比特币钱包：并非“装币”的钱包

我们常说的“比特币钱包”，其实跟我们平时用的钱包不太一样。你平常的钱包，是用来放现金的，而比特币钱包，并不是真的用来装比特币的。比特币本身，是记录在区块链上的，你可以把它想象成存在于互联网上的数字信息，而非具体的实物。它就像存在于一个透明的大账本里，谁也拿不走，也无法修改，除非拥有这个比特币的私钥。

那么，比特币钱包到底是什么呢？

你可以把它想象成一个管理你比特币的“工具箱”。它主要用来帮你保管和使用你的比特币“钥匙”，也就是私钥。有了私钥，你才能真正控制你的比特币。就好比你家的门锁，只有你有钥匙才能开门，比特币也一样，只有你拥有私钥，你才能动用你的比特币。

2.2 私钥：通往财富大门的钥匙

- 私钥的本质：私钥是一串由随机字符组成的神秘代码，就像你银行卡密码一样，只有你知道，绝对不能泄露给任何人。它就像打开你比特币账户的重要的控制凭据。

- 私钥的重要性：谁拥有私钥，谁就拥有了这笔比特币的支配权。一旦私钥丢失或者被盗，你的比特币也就岌岌可危了。
- 私钥的独一无二：常见单签地址与相应密钥材料存在可验证的对应关系，但不同脚本类型和多签结构并非一地址对应一把私钥，就如同每把锁都有其对应的唯一钥匙。

2.3 公钥：可以公开的“银行账号”

- 公钥的由来：公钥是通过私钥经过复杂的数学运算得出的，你可以把它想象成你比特币的“银行账号”，你可以公开给别人，让他们往你的地址转账。
- 公钥的用途：就像你把银行账号告诉别人，他们就能往你的银行卡里转账，同样，你把公钥告诉别人，他们就能往你的比特币地址转账。因为比特币地址就是用公钥经过公开算法生成的。
- 公钥的公开性：公钥是可以公开的，就像你的银行账号，不考虑量子霸权的情况下，别人知道了不会对你的资产造成威胁，但你必须保管好你的私钥，才能保证你的资产安全。
- 公钥无法反推私钥：不考虑量子霸权的情况下，即使别人知道了你的公钥，也无法反推出你的私钥。这就像你知道了银行账号，你也无法反推出银行卡密码。关于量子霸权，将会在第 11 章和第 12 章介绍。

2.4 地址：接收比特币的“收件箱”

- 地址的由来：地址也是通过公钥经过复杂的数学运算得出的，它就像你比特币的“收件箱”，用来接收别人转给你的比特币。
- 地址的用途：就像你的邮箱地址，别人需要通过它才能给你发邮件，同样，别人需要通过你的比特币地址才能给你转账。
- 地址的公开性：地址是可以公开的，你可以把地址告诉别人，让他们往你的地址转账，不用担心自己的私钥会泄露。
- 多个地址：你可以创建多个比特币地址，就像你有多个邮箱一样，你可以用不同的地址来接收来自不同来源的比特币。

2.5 私钥、公钥和地址的关系：一把钥匙、一把锁、一个邮箱

为了更好的理解它们之间的关系，我们不妨这样来比喻：

- 私钥 就像你家的门钥匙，只有你能打开你家的门。
- 公钥 就像你家的门锁，只有对应的私钥才能打开它。
- 地址 就像你家的门牌号，别人可以通过门牌号找到你，把信件投递到你家的邮箱里。

别人可以通过你的地址给你转账，就如同别人知道你家的门牌号可以把信件投递到你家。只有拥有你私钥的人，才能解锁这笔比特币，就像只有你拥有钥匙才能打开你家的门。

2.6 重点强调：私钥、公钥、地址与比特币网络的独立性

现在，我们来强调一个非常重要的概念：私钥、公钥和地址的生成，与比特币网络区块链本身并没有直接的关系！

你可以把比特币网络区块链想象成一个巨大的、公开透明的账本，记录着每一笔比特币的交易。这个账本就像一个公开的邮局，所有人都可以在这里看到每笔交易的记录，但是只有拥有私钥的人，才能对属于自己的比特币进行支配。

而我们的私钥、公钥和地址，就好像钥匙、锁和家庭地址，它们都独立存在，并不依赖于任何特定的“快递公司”或者“邮局”。

- 独立性比喻： 就像你家的大门钥匙、门锁和家庭住址，它们并不依赖于顺丰快递、或者邮政快递，无论有没有快递公司，你的钥匙、锁和家庭住址，它们的功能都是不变的。同样的道理，无论有没有比特币的钱包软件或者硬件，你的私钥、公钥和地址都是独立存在的。更重要的是，这些密钥对的生成过程完全在你本地完成，是一个本地行为，不依赖于任何网络连接或比特币区块链。私钥是通过随机数生成算法产生的，公钥是由私钥通过特定的单向函数推导得出，而比特币地址又是通过对公钥进行哈希运算产生的。这一系列的生成过程都在本地完成，与比特币网络无关。 它们是你在比特币世界里拥有的身份证明。
- 钱包的作用： 钱包只是一个工具，用来帮助你生成和管理私钥、公钥和地址。你可以使用各种不同的工具来生成这些密钥对，比如纸和笔，或者计算机程序。但无论你使用什么工具，它们都只是工具，并不会改变你私钥、公钥和地址本身。钱包的作用是帮你安全存储私钥，并方便你进行交易，而不是生成密钥对本身。
- 常见误解： 很多初学者会误以为一定要购买硬件钱包或者软件钱包才能拥有比特币地址，这其实是错误的。地址和密钥对本身是独立存在的，你可以用各种工具创建它们，而钱包只是用来方便你管理这些密钥对的工具。密钥的生成是完全本地化的过程，即使断开网络连接，你仍然可以生成密钥对。

总结： 我们的私钥、公钥和地址就像一把独立的钥匙、一个独立的锁和一个独立的家庭地址，不依赖于任何的工具，也不依赖于任何的机构，更不依赖于比特币网络本身。 它们独立存在，且其生成过程是完全本地化的，如果不考虑转出币，仅仅用来生成存储比特币地址和对应的私钥，你只需要本地进行一些数学和字符运算即可，不需要任何交易型的钱包软硬件。需要转出币时再使用钱包软硬件导入私钥即可管理你的资产。

2.7 钱包的功能：私钥的管理专家

现在我们知道，钱包本身不存储比特币，它主要功能是管理私钥，包括：

- 生成和存储私钥：钱包会帮你生成私钥，并安全地保存起来。
- 生成和管理地址：钱包会帮你生成地址，并管理你的比特币地址，方便你接收和发送比特币。
- 交易签名：当你要进行比特币转账时，钱包会使用你的私钥对交易进行签名，证明这笔交易是你发起的。

2.8 小结：私钥是比特币安全的基石

比特币钱包的核心在于对私钥的管理。私钥就像你进入比特币世界的大门钥匙，掌握好私钥，你就拥有了比特币。务必妥善保管你的私钥，不要把它泄露给任何人，否则你的比特币将面临巨大的风险。

同时也要明确：私钥，公钥和地址都是独立的，不依赖于任何的工具。钱包只是帮助你生成和管理私钥的工具。

上一章小测验答案：

1. 比特币的总量是多少？

答：比特币的总量是约等于 2100 万个。

2. 什么是“挖矿”？

答：“挖矿”是通过计算机进行复杂的运算，来验证和记录新的交易，并将这些交易信息添加到新的区块中。

3. 比特币的“减半”机制是什么？

答：“减半”机制是指，每当区块链中产生 21 万个区块（大约每四年左右），比特币的区块奖励就会减半。

本章小测验：

1. 私钥有什么作用？它为什么如此重要？
2. 公钥和地址可以公开吗？
3. 私钥、公钥和地址是否依赖于比特币网络区块链？

延伸阅读｜“钥匙—门锁”比喻的边界

私钥可在离线环境中生成，但交易、UTXO 和脚本状态存在于比特币网络；单个私钥也可能参与不同脚本和地址的控制。某些输出由多签、时间锁或其他脚本条件约束，无法简化为“一个地址等于一把钥匙”。因此记录恢复方案时，应保留密钥之外必要的脚本、派生路径与网络信息。

第三章：钱包的种类——百花齐放，各有所长



生活中的例子 | 把日常零钱想成口袋里的钱包，把长期储蓄想成家里的保险柜：使用频率不同，适合的防护方法自然不同。热钱包和冷钱包也是如此。重要的不是争论哪一类永远最好，而是弄清自己的使用场景、风险承受能力与备份能力。

3.1 钱包的分类：连接网络与否

上一章我们了解了比特币钱包的本质，知道它其实是管理私钥的工具。那么，市面上那么多类型的钱包，它们之间又有什么区别呢？我们可以根据钱包是否连接互联网，将它们分为两大类：热钱包和冷钱包。

- 热钱包（Hot Wallet）： 就像一个常用的钱包，经常带着现金，随时可以拿出来用。热钱包是连接互联网的，比如你手机上的 APP 钱包、电脑上的软件钱包、交易所里的钱包，这些都属于热钱包。
  - 优点： 使用方便快捷，可以随时进行交易。
  - 缺点： 由于一直连接着互联网，容易受到黑客攻击，存在一定的安全风险。
- 冷钱包（Cold Wallet）： 就像一个保险箱，把钱存进去之后就锁起来，一般不轻易动用。冷钱包是不连接互联网的，比如硬件钱包、纸钱包、脑钱包，这些都属于冷钱包。
  - 优点： 由于不连接互联网，可以减少联网环境带来的部分远程攻击面，但离线设备和备份仍需防范恶意程序、篡改和物理泄露。
  - 缺点： 使用起来相对麻烦一些，不如热钱包方便。

小结：长期保存比特币，应优先考虑离线、自主、可验证的保管方式。高级脑强调由本人掌握生成规则，减少对专用黑盒设备的依赖；无论采用哪种方式，都必须完成备份和恢复演练。

3.2 常见的钱包类型：各有侧重，各有优缺

了解了热钱包和冷钱包的基本概念，接下来我们来详细了解一些常见的钱包类型，以及它们的优缺点。

- 软件钱包（Software Wallet）： 软件钱包是一种安装在手机或电脑上的应用程序，比如 imToken、Trust Wallet、Electrum 等。
  - 优点： 使用方便，随时随地都可以使用，而且通常是免费的。
  - 缺点： 由于依赖于手机或电脑的环境，容易受到病毒或恶意软件的攻击，安全性和隐私性相对较低。
  - 适用人群： 适合存储少量比特币，经常进行交易的用户。
- 交易所钱包（Exchange Wallet）： 交易所钱包是指将比特币存放在中心化交易所的账户中。
  - 优点： 方便交易，可以直接在交易所里进行买卖。
  - 缺点： 最大的风险在于交易所本身。如果交易所被黑客攻击、倒闭、跑路，或者被监管部门冻结，你的比特币将会面临巨大的损失。
  - 适用人群： 适合在交易所进行交易的用户，但不适合长期存储大量比特币。
- 硬件钱包（Hardware Wallet）： 硬件钱包是一种专门用于存储私钥的硬件设备，比如 Ledger、Trezor 等。
  - 优点： 安全性较高，私钥存储在硬件设备中，不容易被网络攻击。
  - 缺点： 需要额外购买硬件设备，价格较贵，操作相对复杂一些，并且依赖于生产商，存在着厂商倒闭、后门等风险。
  - 适用人群： 适合还没有学习高级脑，对存储比特币的隐私性不在意的用户。
- 纸钱包（Paper Wallet）： 纸钱包是将私钥和地址打印在纸上，然后离线存储。
  - 优点： 安全性较高，私钥不接触网络，不容易被黑客攻击。
  - 缺点： 容易丢失、损坏、被复制，使用和备份不方便，不适合频繁交易。
  - 适用人群： 适合还没有学习高级脑，对物理存储条件绝对自信的用户。
- 脑钱包（Brain Wallet）： 脑钱包是将私钥存储在大脑中，通过记住一段复杂的口令或者一段记忆来生成私钥。
  - 优点： 私密性极高，无需携带任何设备，不依赖单一实体载体（仍应制定恢复方案），理论上最方便快捷。

- 缺点： 口令太复杂则容易忘记口令，口令太简单容易被破解，因此脑钱包不宜直接使用。
- 适用人群： 适合有一定经验的用户，并且需要有足够复杂的脑口令。

3.3 深入了解：BIP39 助记词——从随机熵到确定性派生

BIP39 标准支持 12、15、18、21 和 24 个助记词；具体采用哪一种，取决于生成时使用的熵长度及校验位。

BIP39 是广泛使用的助记词标准。它首先获取随机产生的熵，追加校验位，再按 11 位一组映射到 2048 词的词表，形成助记词；之后以 PBKDF2-HMAC-SHA512（2048 次迭代）把助记词和可选口令转换为 512 位种子，供后续确定性密钥派生使用。这里要分清："随机生成初始熵"与"由既定助记词确定性恢复种子"是两个阶段。

- 初始随机源：合格随机源对 BIP39 初始秘密的不可预测性非常重要。随机源故障、供应链风险和实现问题值得评估，但这并不等于所有硬件钱包或 BIP39 实现都不可靠。
- 确定性恢复：只要助记词、可选口令、规范化及派生参数相同，恢复的种子与后续密钥可以一致。BIP39 并非每次打开钱包都重新抽取随机数。
- 可选口令：BIP39 passphrase 不是普通的软件解锁密码；不同口令会生成不同的钱包。遗忘口令意味着恢复失败。
- 地址派生：BIP32/BIP44/BIP49/BIP84/BIP86 等规范涉及钱包派生与脚本类型。助记词本身并不直接决定单一地址。
- 实用建议：用于真实资产时，应优先选择可验证、可恢复且经过广泛审查的实现，并完成备份与恢复演练。

与高级脑比较时，本书讨论的重点是：BIP39 标准初始秘密通常来自随机熵；本书所研究的高级脑方案则允许用户预先决定秘密输入和生成规则，在每次生成时无须调用随机数发生器。两者后续都可以使用确定性计算。

3.4 对比总结：选择适合自己的钱包

每种类型的钱包都有自己的优缺点，没有绝对安全或者绝对完美的钱包，我们需要根据自己的实际情况，选择适合自己的钱包。

- 热钱包： 适合存储少量比特币，经常交易的用户，但要注意安全，不要存储大量的资产。
- 冷钱包： 适合存储大量比特币，注重安全性的用户，但使用起来不如热钱包方便。
- 硬件钱包： 安全性较高，适合长期存储，但成本较高，操作复杂，并存在一定的厂商风险。 适用人群： 适合还没有学习高级脑，对存储比特币的隐私性不在意的用户。

- 纸钱包： 适合存储少量比特币，长期不交易的用户，但要注意纸张的保存。 适用人群： 适合还没有学习高级脑，对物理存储条件绝对自信的用户。
- 脑钱包： 私密性极高，但风险也极高，适合有一定经验的用户，并且需要有足够复杂的脑口令。缺点： 口令太复杂则容易忘记口令，口令太简单容易被破解，因此脑钱包不宜直接使用。
- BIP39： 方便易用，但是仍然存在依赖第三方，以及存储风险，而且不够灵活，记忆难度仍然偏高。

3.5 小结：了解钱包，才能更好地保护你的资产

了解不同类型的钱包，才能更好地保护你的比特币资产。我们既要选择合适的工具，又要掌握安全使用的技巧，才能在比特币世界里自由穿梭。

上一章小测验答案：

1. 私钥有什么作用？它为什么如此重要？

答：私钥是用来控制比特币的重要的控制凭据，拥有私钥就拥有了对比特币的支配权，因此非常重要。

2. 公钥和地址可以公开吗？

答：地址通常可用于收币；公钥可以公开用于验证，但地址与公钥并非完全相同，公开地址可能影响交易隐私。

3. 私钥、公钥和地址是否依赖于比特币网络区块链？

答：私钥、公钥和地址是不依赖于比特币网络区块链的，它们是独立存在的。

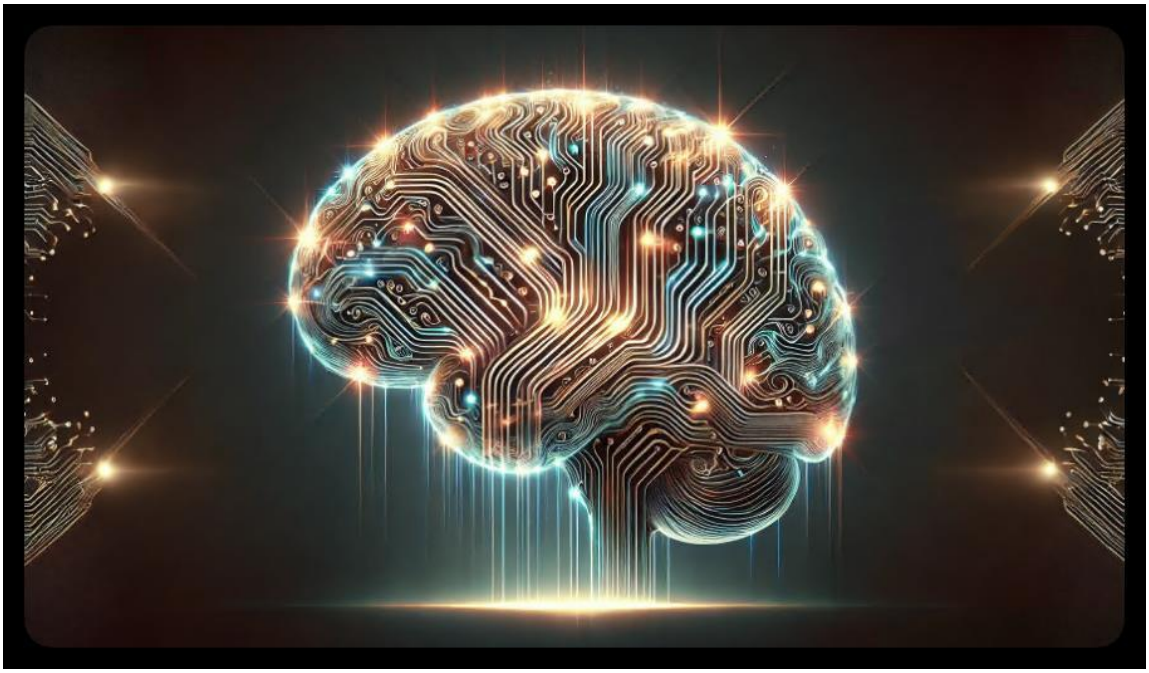
本章小测验：

1. 什么是热钱包？什么是冷钱包？
2. 什么是 BIP39 助记词？它的原理是什么？
3. BIP39 助记词的优势和不足有哪些？

延伸阅读丨随机源风险是故障模式，不是所有随机方案的定论

高级脑希望避免生成时依赖随机数发生器，这是一个可研究的工程目标。BIP39 合格实现的初始熵质量、设备隔离以及恢复工具兼容性则构成另外一套风险管理。两者均须验证软件可信度、材料备份以及长期恢复的可靠性。选择方案时应比较故障模式，而不是只比较口号。

第四章：初识脑钱包——把私钥藏在你的大脑里



生活中的例子 | 背下一个电话号码，与背下“先去通讯录找到某个人，再按一个固定规则读取数字”，是两种不同的记忆方式。脑钱包试图利用记忆保存找回秘密的方法，但只记住一条常见短句，就像把家门钥匙放在门垫下——别人也会首先想到那里。

4.1 脑钱包：把私钥生成规则交给自己掌握

经过前面的学习，我们了解了各种类型的钱包，也知道了私钥的重要性。我们知道，私钥就像你进入比特币世界的大门钥匙，拥有私钥，你就拥有了比特币。那么，我们如何才能安全、便捷地存储和管理私钥呢？

传统的做法，是将私钥存储在硬件设备、纸张或者软件程序中。但是，这些方法都存在一定的风险。比如，硬件设备可能会损坏、纸张可能会丢失、软件程序可能会被黑客攻击。

有没有一种更安全、更便捷的存储方式呢？答案是肯定的，那就是脑钱包。

脑钱包，顾名思义，就是把私钥存储在你的大脑里。这听起来有点不可思议，但实际上，脑钱包是一种非常巧妙的存储方式。它通过让你记住一段特殊的口令，或者一段深刻的记忆，来生成你的私钥。

4.2 脑口令：开启财富之门的“咒语”

脑钱包的核心在于脑口令，也叫做脑种子。你可以把脑口令想象成你进入比特币世界的“咒语”。这个咒语可以是任何你容易记住的东西，例如：

- 一句话： 你最喜欢的一句诗，一句电影台词，一句让你感动的话。
- 一段文字： 你的一段经历，一个感悟，或者你对未来的展望。
- 一个故事： 你小时候的有趣经历，你和家人难忘的瞬间。
- 一个地点： 你出生的地方，你第一次和爱人约会的地方。
- 一组数字或符号： 一串对你特殊的数字，或者一个你独有的符号组合。
- 甚至是一段旋律或者歌词： 一首你最喜欢的歌，一段让你难忘的旋律。

关键在于，这个脑口令必须是只有你知道，并且容易记住的，而且最好是有意义的，这样能够方便你更好的记忆，并且不容易忘记。

4.3 脑钱包的工作原理：将记忆转化为私钥

当你确定你的脑口令之后，脑钱包会通过一种特殊的算法，将你的脑口令转化为一串复杂的私钥。

- 哈希运算： 脑钱包会将你的脑口令通过一种特殊的哈希函数进行计算，生成一个固定长度的哈希值，这个哈希值也是一串随机字符。
- 私钥生成： 然后，使用这个哈希值，就可以生成你的私钥。

4.4 脑钱包的优点：无需设备，私密安全

脑钱包之所以特别，是因为它具有其他钱包无法比拟的优点：

- 无需设备： 你不需要携带任何硬件设备，也不需要安装任何软件程序，私钥就存储在你的大脑中，只要记住你的脑口令，就可以随时随地访问你的比特币。
- 私密性高： 只要你不泄露你的脑口令，没有人知道你的私钥，你的比特币也就更加安全。
- 不依赖单一实体载体（仍应制定恢复方案）： 不需要像其他钱包一样进行备份，只要你的记忆没有问题，你的私钥就不会丢失。

4.5 “一维脑钱包”的风险：口令至关重要，记忆不可靠

为了更好地理解脑钱包的风险，我们将普通脑钱包的概念归类总结为“一维脑钱包”。 一维脑钱包最大的特点就是它只依赖一个简单的口令，来生成私钥，也正是因此，它存在着巨大的安全隐患：

- 口令太弱： 如果你的脑口令过于简单，比如 "123456"、"password" 这种常见的口令，或者虽然不简单，但是却和别人用的一样，仍然很容易被黑客破解。

- 口令重复风险： 即使你的口令不是 “123456” 这种简单的组合，但如果你使用一首大家耳熟能详的诗，比如“静夜思”作为脑口令，很有可能也有很多人和你使用同样的口令。那么，黑客就可以通过收集这些常见口令，来批量破解一维脑钱包。
- 字典攻击： 黑客会事先准备好一个包含大量常用口令的 字典库，然后使用这个字典库尝试破解你的脑口令。一些流行的脑钱包工具（如 bitaddress.org）生成的钱包，已经存在被人收集的公开字典库，很容易就被暴力破解。

- 记忆遗忘： 如果你的脑口令过于复杂，或者时间太久，你可能会忘记，导致无法找回你的私钥。
- 泄露风险： 如果你不小心把脑口令泄露给别人，那么你的比特币就会面临被盗的风险。
- 依赖个人记忆： 脑钱包的安全性完全依赖于你个人的记忆能力，这对于很多人来说，都是一个巨大的挑战。
- 历史破解记录： 历史上已经出现过大量一维脑钱包被破解的案例。一些用户由于使用了过于简单的或者过于常见的脑口令，导致他们的比特币被盗。
  - 案例分析： 2015 年，Ryan Castellucci 详细介绍了如何使用“Brainflayer” 高速破解工具对一维脑钱包进行破解。现在的计算机每秒可以进行数百万、数十亿甚至数万亿次的猜测，一些常见的口令可以在一天之内就被破解。Ryan Castellucci 分享了自己意外窃取 250 枚比特币（后归还）的经历，这充分说明了直接使用一维脑钱包的巨大风险。
- 即使口令强度足够仍然存在风险： 即使你使用了高强度的口令，并且确保不重复，仍然不能完全保证安全性。例如，你的计算机如果感染了恶意软件，记录了你的键盘输入，那么你的脑口令仍然会泄露，导致密钥被盗。此外，一些高级攻击者可能会利用社会工程学手段，通过欺骗等方式来获取你的脑口令。另外，如果生成私钥的算法本身存在漏洞，即使你的口令强度再高，也无法保证安全。 因此，仅仅依赖口令强度来保护脑钱包是非常危险的。

4.6 为什么我们不建议直接使用“一维脑钱包”？

正因为“一维脑钱包”的风险如此之高，所以我们不建议普通用户直接使用 “一维脑钱包”。因为大部分人，都无法保证自己的口令足够复杂，足够安全，也无法保证自己永远不会忘记。“一维脑钱包”只是一个概念，不是一个产品，它是存在着极高风险的一种方式。

4.7 小结：脑钱包的理念，高级脑钱包的基础

脑钱包提供了一种非常有趣和独特的私钥存储方式，它也给我们在安全性和便捷性之间提供了一种新的思路。虽然我们不建议普通人直接使用“一维脑钱包”，但是，“一维脑钱包”的思想，为我们后面学习高级脑钱包提供了重要的理论基础。

上一章小测验答案：

1. 什么是热钱包？什么是冷钱包？

答：热钱包是连接互联网的钱包，冷钱包是不连接互联网的钱包。

2. 什么是 BIP39 助记词？它的原理是什么？

答：BIP39 助记词是一种将种子转换成一组易于记忆的单词的行业标准。

3. BIP39 助记词的优势和不足有哪些？

答：BIP39 助记词的优点是相对私钥更易于记忆和备份，缺点是生成时依赖第三方，仍然存在泄露风险，并且不够灵活。

本章小测验：

1. 什么是脑钱包？它的核心是什么？
2. 脑口令是什么？它有什么特点？
3. 脑钱包的优点有哪些？
4. 什么是“一维脑钱包”？它的风险有哪些？
5. 为什么我们不建议直接使用“一维脑钱包”？

延伸阅读丨记忆不是万能保险箱

“藏在脑中”能够降低某些实体泄露面，也会带来记忆偏差、疾病、意外、胁迫与继承障碍。指针记忆法的价值在于减轻记忆负担，但如果指向的网页、账户、书籍版本或个人信息发生变化，重建结果也可能变化。研究时应固定资料版本，并对恢复条件进行演练。

第五章：为什么我们需要高级脑钱包？



生活中的例子 | 同一段往事，对一个人可能刻骨铭心，对另一个人却毫无意义。高级脑正是从这种差异出发：每个人都有自己的记忆、经历和理解，也可以用这些个人材料设计只有自己掌握的规则。

先把本书的立场说清楚。普通人谈比特币安全，往往只想到加密算法、随机数和密钥长度，仿佛只要选对算法，安全就自然有了。可现实不是这样。算法要由人设计、由工具执行、由人保存和恢复。设备可能被篡改，供应链可能出问题，随机数路径可能实现错误，备份也可能遗失。只研究加密学，不研究整个系统怎样运行，就看不见许多真正的风险。高级脑强调工程学，就是要把这些环节放在一起考虑。

高级脑首先相信一个朴素的事实：每个人的生命经验都不一样。你忘不了的事，别人可能从未听说；别人珍藏的记忆，对你也可能毫无意义。信息指针正是从这里来。它不是统一发给所有人的标准口令，而是每个人从自己的经历中找到的线索。

5.1 普通脑钱包的局限性：看似安全，实则危机四伏

上一章介绍了只依赖单一脑口令的做法。它的问题在于，人的常用词语、纪念日和个人资料往往并不像想象中那样难以猜测；而过度复杂的口令又容易遗忘。高级脑从这里出发，尝试把个人掌握的材料、规则和记忆方式组合起来。

就像一栋只有一扇门的房子，虽然看起来很安全，但只要别人能打开这扇门，就能进入你的房间。而一维脑钱包就如同这栋只有一个密码锁的房子，一旦锁被破解，你所有的资产都将暴露在风险之中。

那么，有没有更好的方法，可以既能利用脑钱包的便捷性，又能避免它存在的安全隐患呢？答案是肯定的，那就是我们接下来要学习的——高级脑钱包。

5.2 高级脑钱包：从“一维”到“多维”的飞跃

高级脑钱包，并不是对普通脑钱包的简单升级，而是一种全新的私钥管理理念。它和普通脑钱包（也就是“一维脑钱包”）最大的区别在于：

- 一维脑钱包： 只依赖于一个简单的口令，来生成私钥。
- 高级脑钱包： 不仅仅依赖于一个简单的口令，而是设计一套复杂的 算法规则，来生成私钥。

你可以把高级脑钱包想象成一个由多个门、多个锁组成的复杂迷宫。即使黑客知道你的某个口令或者某把锁，也很难找到真正的出口，很难攻破这个防御系统。

5.3 高级脑钱包的核心思想：确定性不等于可预测性

设使用者选择个人信息材料 x，并自主设计一套秘密规则 F，最终结果写作 K=F(x)，再按约定进入 SHA-256 散列处理。只要 x 和 F 不变，结果就不变；使用者掌握它们，就能在不同设备上重新生成。外部的人即使知道 SHA-256，也不等于知道 x 和 F。确定性属于计算过程，能否预测则取决于外部掌握的信息。

SHA-256 是公开、成熟的基础散列算法。高级脑的个人化部分在于 F：它可以规定材料从哪里来、怎样取用、怎样编码、按什么顺序拼接、如何迭代，以及怎样处理序号。F 由使用者自主设计、长期掌握，也可以像更换密码口令一样，在完成迁移和验证后更换。公开 SHA-256，与保守自己的 F 并不矛盾。

F 也可以这样设计。使用者不必背诵一套外人看起来复杂、自己却难以记住的程序。可以把个人熟悉的记忆、线索和固定步骤组织成规则：自己知道怎样执行，别人却不知道这些线索之间的联系。对自己好记，对别人复杂，是设计 F 时值得追求的方向。

F 不必是一套难以记忆的复杂程序。它也可以使用信息指针的方式来建立：对本人而言容易记住、容易复现；对不了解本人经历的人而言，却很难从外部资料中还原。F 可以包含个人熟悉的线索、取用方式、字符变换、位置规则和组合步骤。设计时既要考虑别人难以推断，也要保证自己多年以后仍能准确执行。

高级脑的关键，是把个人信息和个人规则结合起来。攻击者即使知道公开的 SHA-256，也不能因此直接得到真实输入；但这不意味着攻击者必须先完整知道 F，才有可能发起攻击。他可以利用公开资料、熟人信息和常见习惯，构造候选信息指针与候选规则，再尝试验证结果。未知 F 的价值，在于增加攻击者识别、组合和验证正确生成过程的难度，而不是让规则猜测在逻辑上变得不可能。

F 的候选空间不能简单把几个参数相乘，就当成可证明的搜索规模。规则之间可能重复、依赖，也可能被个人公开资料大幅缩小。真正需要考察的是：攻击者能获得哪些线索，能构造多少有意义的候选规则，是否存在可靠的结果验证方式，以及完成针对性搜索需要多少时间和资源。规则设计得当，可以提高攻击者还原完整生成过程的成本；但“规则复杂”或“本人觉得独特”，本身都不是安全证明。

5.4 高级脑的特点：自主设计与整体安排

与只依赖单一口令的做法相比，高级脑提供了更多可以由使用者主动安排的环节：

- 规则设计：使用者自主设计 F，把个人信息指针、材料、编码、顺序和处理步骤组织起来。F 要让本人容易记住和复现，同时避免让外人从公开资料中轻易拼出。规则不是越绕越好，重要的是个人掌握、长期稳定，并且不容易被外部还原。
- 个人规则：F 是使用者自己的秘密算法，可以根据个人经历和理解来设计，也可以在一段时间后更换。更换时必须先用新规则完成生成、地址核对和恢复演练，再迁移资产；不能只改了记忆中的规则，却没有确认新旧结果。
- 记忆与组织：高级脑鼓励用信息指针组织信息指针——个人经历既可以帮助记住初始材料，也可以帮助记住 F 的设计。对本人有意义的线索，未必对别人有意义。指针要能稳定指向具体材料，不能依赖模糊记忆或已经消失的网页。

5.5 高级脑钱包的必要性：避免“一维脑”的风险

普通脑钱包把一个口令直接交给公开算法处理，常见口令容易被字典和公开资料覆盖。高级脑把个人信息指针与秘密规则 F 一起纳入生成过程。即使攻击者知道某些个人信息，也不等于知道怎样按照 F 组织它们。高级脑的设计重点，是让本人掌握完整过程，同时让外部人员难以还原这套过程。

- 面对预计算攻击：彩虹表依赖可重复使用的输入与转换规则。F 作为个人秘密规则，会改变攻击者开展通用预计算的条件；但它不能保证针对性攻击无从进行。攻击者仍可能结合个人数字足迹构造候选 F 和信息指针，再尝试验证。因此，设计时要减少公开线索、避免常见模板，并明确哪些材料和规则真正保密。
- 个人化组合：不同的人可以选择不同的信息指针，也可以设计不同的 F。这样形成的不是一套人人通用的口令模板，而是每个人自己掌握的生成体系。
- 记忆与恢复：信息指针让材料与个人经历建立联系，F 也可以通过类似方式记忆。但记忆不能代替恢复安排。使用者必须考虑遗忘、意外和继承，确保多年以后仍能准确重建材料和规则。
- 自主定制：高级脑允许使用者根据自身情况安排材料和步骤。与标准化钱包相比，自定义空间更大，同时也意味着兼容性、审查和恢复责任更多。

5.6 小结：高级脑钱包——安全与便捷的完美结合

高级脑把个人主观价值、信息指针、秘密规则 F 和 SHA-256 组织成一套确定性的私钥生成方法。它主张由使用者掌握自己的材料和规则，减少对外部黑盒设备及厂商的依赖。我们要改变的，是只看算法名称和密钥长度的习惯：真正的安全还要看规则怎样产生、怎样执行、怎样保存，以及能否在多年以后独立恢复。

上一章小测验答案：

1. 什么是脑钱包？它的核心是什么？

答：脑钱包是将私钥存储在大脑中的钱包，它的核心是脑口令。

2. 脑口令是什么？它有什么特点？

答：脑口令是用来生成私钥的口令，它具有方便记忆、独一无二等特点。

3. 脑钱包的优点有哪些？

答：脑钱包的优点是无需设备、私密性高、不依赖单一实体载体（仍应制定恢复方案）。

4. 什么是“一维脑钱包”？它的风险有哪些？

答：“一维脑钱包”是指只依赖一个简单口令来生成私钥的脑钱包，它的风险包括口令太弱、记忆遗忘、泄露风险和依赖个人记忆。

5. 为什么我们不建议直接使用“一维脑钱包”？

答：我们不建议直接使用“一维脑钱包”，因为它存在着太多的安全风险，而大部分人都无法避免。

本章小测验：

1. “一维脑钱包” 存在什么风险？
2. 高级脑钱包和普通脑钱包（“一维脑钱包”）最大的区别是什么？
3. 高级脑钱包的核心思想是什么？

延伸阅读｜规则设计要落到现实生活

设 SHA-256 为公开的散列算法，F 为使用者自主设计并保密的规则。攻击者知道 SHA-256，并不等于知道 F；知道某些个人经历，也不等于知道这些信息在 F 中如何取用、编码和组合。若要建立针对某个人的预计算表，必须先掌握或猜中其 F。F 的秘密性使这类预计算面临时间和存储上的现实障碍；F 的设计质量、个人信息是否泄露、规则是否容易推断，则决定这道障碍有多高。

第六章：高级脑的工程安全基础——从算法走向完整系统



生活中的例子 | 你知道一台机器怎样工作，不代表你知道每个人怎样使用它。SHA-256 是一台公开的散列机器，任何人都能按相同规则计算。高级脑在这台公开机器之外，加入了使用者自己设计并掌握的 F，以及来自个人经历的信息指针。

本章会讲必要的密码学知识，但全书的视角是工程学。我们要看算法怎样进入人的生活：秘密从哪里来，规则由谁掌握，设备是否可信，结果能否复现，发生意外后能否恢复。只知道加密学，却不理解工程过程，就容易把某个算法或设备当成全部安全。

6.1 为什么我们要了解安全性基础？——磨刀不误砍柴工

上一章介绍了高级脑的出发点。本章会补充必要的密码学知识，但请不要把它们当成安全的全部。理解算法，是为了知道工具能做什么、不能做什么；真正的设计还要考虑材料、设备、操作、记忆、备份和恢复。

学习这些概念，就像认识建房时用到的材料和结构。知道水泥的强度，并不代表房子就一定安全；施工、地基、排水、维护和使用习惯同样重要。理解 SHA-256 的抗碰撞性、扩散特性和随机源概念，是为了把它们放在各自正确的位置上。

6.2 哈希算法：神奇的“信息指纹”

- 什么是哈希算法？ 哈希算法就像一个神奇的“搅拌机”，它能把任意长度的输入信息（例如文字、数字、图片、视频等）“搅拌”成一个固定长度的输出信息，这个输出信息叫做 哈希值。哈希算法就像你的“外卖订单号”。无论你点的外卖多么复杂，最终都会生成一个固定长度的订单号，而且根据这个订单号，外卖商家可以快速找到你的订单信息。

- 哈希算法的特点：

o 单向性： 哈希算法是单向的，也就是说，你只能从输入信息得到哈希值，但是无法从哈希值反推出输入信息。这就像我们知道外卖订单号，但是你无法从订单号中反推出顾客点的哪几样菜。

• 固定长度输出：无论输入多长，SHA-256 都会输出 256 位摘要。这个长度说明散列结果的格式，并不意味着它能替代前面的个人信息选择与秘密规则设计。高级脑的生成过程要把 X、F 和散列步骤作为一个整体来理解。

o 雪崩效应： 输入信息的任何微小改变，都会导致生成的哈希值发生巨大变化。想象一下假设你外卖订单多点了一份餐，订单号就会完全改变，和之前的毫无关系。

- 哈希算法的应用： 哈希算法在计算机领域有着广泛的应用，比如：

o 文件校验： 你可以校验下载的文件是否被篡改。

• SHA-256 算法：SHA-256 是比特币体系使用的重要散列算法。比特币地址的生成还涉及公钥处理、SHA-256 与 RIPEMD-160 等步骤，不能简单说地址只由 SHA-256 生成。高级脑以 SHA-256 作为最终散列的基础标准。

o 区块链： 比特币区块链就大量使用了哈希算法。

• SHA-256 算法：SHA-256 是比特币体系使用的重要散列算法，也是高级脑最终散列处理的基础标准。中间步骤可以继续使用 SHA-256，也可以使用 SHA-512 或多个散列结果的组合；本书不建议在中间改用低于 SHA-256 强度的散列算法。

6.3 抗碰撞性：避免“撞衫”的秘密

- 什么是抗碰撞性？ 抗碰撞性是指，哈希算法很难找到两个不同的输入信息，却能生成相同的哈希值。就像你排队买东西，很难出现两个人同时拥有同一张排队号码的情况，因为排队号码都是唯一的。

- 抗碰撞性的重要性： 如果哈希算法的抗碰撞性很差，那么我们使用不同的口令生成的私钥，就可能会相同。如果两个人的私钥相同，那么他们的比特币就会暴露在风险之中。

• SHA-256 的抗碰撞性：SHA-256 具有极强的抗碰撞能力。工程上，寻找一对不同输入却得到相同摘要的结果，需要面对极高的计算门槛。比特币的安全设计正是建立在相关密码学难题在现实计算条件

下不可行的基础上。讨论安全时，应关注现实攻击能力和工程可行性，而不是把任何有限输出空间都说成数学上绝无碰撞。

6.4 散列性：让输入经过充分扩散

• 什么是雪崩效应？输入发生细微变化时，输出通常会有大量比特随之改变。它让不同输入的摘要呈现出明显差异，是散列算法的重要性质。

• 雪崩效应的意义：输入发生微小变化时，输出通常会有大量比特改变。它使输出与输入之间不呈现简单直观的对应关系，是 SHA-256 的重要性质。高级脑使用这一公开散列工具，同时把个人化的秘密规则 F 放在生成过程的核心。

6.5 从一个字母到 64 个十六进制字符：先问清楚“复杂”是什么

例如，输入字符“a”经过 SHA-256 后，会得到 64 个十六进制字符。输出格式能够表示 2 的 256 次方种摘要。这个例子说明散列结果具有固定长度和充分扩散的外观；高级脑的安全设计则还包括个人信息指针、秘密规则 F，以及这些材料如何被本人掌握。

但这里不能只拿一个字母的例子，便断定所有高级脑输入都可以被直接枚举。若输入和规则都公开，当然一次计算就能得到结果；高级脑讨论的完整情形，是攻击者知道公开的 SHA-256，却不知道个人掌握的 F，也未必知道真实的信息指针及其组织方式。两种情形的攻击条件完全不同。

6.5.1 表示空间容量 RSC——一个教学指标

为了描述不同输出格式能够容纳多少种表示，可以使用“表示空间容量”（RSC）这一概念。256 位 SHA-256 摘要的表示空间容量为 256 位。它描述的是输出格式的规模，不是高级脑要求使用者追求的随机性指标。

高级脑不把“输入必须具有多少香农熵”作为设计目标，也不靠输出看起来杂乱来证明安全。我们关心的是完整生成过程：个人信息指针如何选择，F 如何设计并保密，材料怎样编码和组合，攻击者能否识别并还原这套规则。SHA-256 负责既定的散列处理，不能替代 F，也不应脱离 F 单独评价整个体系。

6.5.2 信息论概念与高级脑的设计目标

香农熵用于描述给定概率分布下的不确定性，在分析随机源和 BIP39 初始材料时有明确用途。高级脑的设计目标不同：它不要求生成过程临时抽取随机数，也不以追求某个香农熵数值为目标。高级脑从个人主观价值出发，使用信息指针组织材料，由本人设计并掌握秘密规则 F，再通过确定性步骤生成结果。

6.5.3 从数学性质回到现实使用

讨论高级脑的安全，必须把 F 放回完整生成过程。攻击者是否知道公开的 SHA-256，并不能回答他是否知道个人的信息指针、材料取用方式、编码顺序和秘密规则。若要针对某个使用者建立专门的预计算体系，首先必须识别或还原其 F；这会把攻击带入规则识别、候选组合、计算和存储共同作用的工程问题。

6.6 SHA-256 与个人秘密规则 F

本书以 SHA-256 作为最终散列的基础标准。前面使用不足 32 字节的输入，是为了说明短文本经过散列后会得到固定长度摘要；它不是安全及格线。高级脑的完整生成体系还包括个人信息指针、初始脑口令、秘密规则 F 及其确定性处理步骤。

F 由使用者事先设计并掌握。它可以规定多个信息来源怎样组合、字符如何编码、按什么次序拼接、怎样迭代，以及是否在中间增加散列处理。中间可以使用 SHA-256、SHA-512，也可以把两个 SHA-256 结果按明确的字节或文本格式连接后再处理；不建议使用低于 SHA-256 强度的散列算法。无论中间怎样增强，最终 SHA-256 输出仍为 256 位。多层处理不会把最终输出空间变成 512 位，也不能把多次散列的强度简单相加。

6.6.1 三个一眼就懂的实验

实验一：公开输入“a”，也公开 SHA-256。任何人都能按同一规则得到相同结果。这说明公开散列算法本身不是秘密。

实验二：公开一部分个人材料，但不公开 F。外部人员仍可能根据已知资料猜测材料的取用方式和规则，因此不能把“F 未公开”理解为攻击者无法尝试。它的作用是让攻击者缺少直接、确定的生成路径，并迫使其面对候选规则与验证问题。

实验三：攻击者既不知道完整的信息指针，也不知道 F。他可以利用公开线索提出猜测，但猜测某个生日或姓名，并不等于完成了私钥生成。安全性取决于真实材料、规则设计、可用线索、候选验证条件以及攻击成本的整体情况。

6.6.2 把私钥管理看成一项完整工程

评价高级脑，要从头走到尾：初始脑口令是否符合设计要求，信息指针是否来自个人真实经历，F 是否由本人掌握，工具是否可信，生成结果能否独立核对，备份能否长期保存，换设备后能否重新生成，家人能否按预案恢复。这些环节共同构成高级脑的工程安全。

6.7 如何利用这些知识，设计更安全、更易继承的高级脑钱包？—— “信息的指针记忆法”

现在我们已经了解 SHA-256 的固定输出、扩散和抗碰撞等性质。接下来要把这些知识放进高级脑的规则设计中：先确定个人材料，再规定 F 如何取用、编码和组合，最后固定散列步骤、工具验证和恢复方式。

“汝之鲍鱼，吾之砒霜。”同一件东西，在不同的人眼中价值不同。高级脑所说的信息指针，也是如此。某段经历未必有客观上的特殊之处，却可能在一个人的生命里留下无法替代的印记。我们重视的是这种个人主观价值，以及它与 F 结合后形成的个人化规则。

我们在这里再次强调 “信息的指针记忆法” 的重要性，并补充一些关于脑口令、盐值和“关键脑口令”的选择建议：

- 什么是“信息指针”？它是把个人材料与自己熟悉的经历、场景或记忆联系起来的线索。每个人都有一些刻骨铭心、对别人却未必有意义的事情。对你来说，一段往事可能价值非凡；对别人来说，却只是陌生的细节。这种主观价值，是高级脑选择信息指针的思想根基。指针必须能稳定地指向具体材料，必要时还要固定来源、版本和取用方法。

- 初始脑口令的选择：

o 避免直接照搬公开材料：诗词、歌词、电影台词可以作为个人信息来源，但不要把人人都能查到的一整句公开文本直接当成秘密。真正重要的是个人如何选择信息指针，以及 F 如何组织和处理这些材料。

o 个人信息指针：可以从自己真正记得、理解并赋予意义的经历中选择线索。不要把“别人不知道”简单等同于安全；要结合 F 设计取用和组合方式。个人信息的主观价值，首先在于它属于自己的生命经验，而不是它在外人看来有多复杂。

使用 BIP39 助记词： 甚至可以使用 BIP39 生成一组助记词，成为你初始脑口令的一部分。

安全性分析： BIP39 把一段熵编码为助记词。助记词所包含的信息量，取决于生成它时使用的熵及随机源质量；BIP39 标准本身并不会替代随机源，也不会让弱随机输入自动变强。

记忆方法： 可以记住“这组助记词存放在哪里、属于哪次生成、如何按规则取用”等指向信息。但如果助记词本身是随机生成的，单凭“我曾经生成过一组助记词”无法重新算出原来的词组；必须确保材料有可靠且安全的保存方式。

重要提示： 不要把 BIP39 助记词误认为经过哈希就自动变得更安全。若将它作为高级脑输入的一部分，应明确它是否公开、是否保密、怎样备份，以及它与最终私钥之间的确定性关系。

使用 Nostr 公钥/私钥： 同样，你也可以使用 Nostr 的公钥或者私钥作为初始脑口令的一部分。

若将独立生成且妥善保密的 Nostr 秘密材料纳入完整输入，攻击者还必须面对这份材料本身的保密性和恢复问题。使用前要确认材料确实来自可靠来源，没有公开或复用，并由 F 明确规定取用方式。

记忆方法： 可以用信息指针记录密钥材料的来源和保存位置，但公钥通常是公开信息，私钥则必须按秘密材料保护。不能把二者混为一谈。

重要提示： Nostr 公钥与私钥的性质不同。公开公钥不能提供秘密输入；若使用私钥材料，必须确认其来源、保密状态和用途，并避免复用会影响其他账户安全的密钥。

o 使用随机生成的比特币密钥对： 你甚至可以随机生成一个比特币的公钥、地址和私钥，并将它们作为初始脑口令的一部分。

若将独立生成且妥善保密的比特币秘密材料纳入完整输入，必须确认其生成来源、保密情况和恢复方式；随后如何编码、组合和处理，由 F 事先规定。不要把公开公钥与秘密私钥材料混为一谈。

记忆方法： 如果使用随机生成的比特币密钥材料，必须保存足以恢复原始材料的内容。记住“我生成过一把密钥”并不能重建那把密钥。

重要提示： 不要把已经控制真实资产的私钥随意拿来作为另一个密钥体系的输入，以免因复用、暴露或错误操作造成连带风险。演示和测试应使用没有资产价值的材料。

o 多来源组合：推荐并鼓励组合多个信息来源。不同经历、记忆和知识可以共同构成个人的信息体系，再由 F 规定如何取用和组合。不要把全部生成过程押在一个容易遗忘或容易被外界获知的单一线索上。

- 盐值的意义和功能：

o 什么是盐值？ 盐值是一段与输入一起参与哈希运算的数据。它可以是公开的，也可以由使用者保密；两种设计的作用不同。公开盐值主要用于区分相同输入，秘密盐值则属于整体秘密材料的一部分。

o 盐值的作用：

区分盐值和秘密规则：盐值可以公开，也可以作为秘密材料；它主要参与输入区分。高级脑的 F 则是使用者自主设计并掌握的秘密算法，二者作用不同。

盐值与 F 的区别：盐值可以让相同材料在不同设置下得到不同结果；它本身不一定保密，也不等同于秘密算法。高级脑的核心秘密规则是 F。若盐值也作为秘密材料使用，应明确它在规则中的位置和保护方式。

区分输入： 盐值可以让相同口令在不同场景下得到不同的哈希结果。它可以是公开的，也可以作为秘密材料的一部分；是否保密必须在方案中说清楚。

o 盐值的选择建议：

易于复现：盐值可以来自个人有意义的信息，但不能只凭“对我有意义”就认定别人猜不到。应明确取值、格式和编码，并在测试中验证多年后仍能准确恢复。

妥善保护：盐值是否需要保密，取决于它在完整规则中的作用。不要把所有秘密材料和完整规则未经区分地集中记录，也不要因为某个材料容易记忆就忽视备份和继承。

- “关键脑口令”的概念：

o 什么是“关键脑口令”？ 在我们的高级脑钱包设计中，引入一个独特的概念，叫做**“关键脑口令”**。 它可以是参与运算的多个脑口令中的一个，也可以是盐值中的一个。

o “关键脑口令”的特点：

个人化：关键脑口令可以借助个人信息指针来记忆。选择时要考虑它是否容易被熟人、公开资料或社交媒体推断。

保密与备份：关键脑口令可以作为秘密材料，但“只存在于大脑”并不自动等于安全。要考虑遗忘、疾病、意外和继承；是否采用分离备份或受控恢复，应由完整方案决定。

长度要求：初始脑口令不少于 20 个字符。建议由多个个人信息来源组合，并结合 F 设计；长度不是唯一标准，材料是否属于个人、F 是否保密、规则能否长期复现同样重要。

o “关键脑口令”的作用：

重要秘密材料：关键脑口令可以成为 F 中的一项独立秘密。它与其他材料如何组合、由哪一步使用、是否参与中间散列，都必须在规则中明确。

可继承性： 设计时要同时考虑本人失能、意外和身故后的情况。规则可以留有说明，其他材料可以分开封存，关键秘密也可以设计受控的继承方式。只靠本人和家人“都记得”并不稳妥，具体安排还要兼顾泄露风险与恢复可行性。

- 如何利用“信息的指针记忆法”设计高级脑钱包：

1. 选择有意义的信息：从自己的经历、记忆、知识和生活细节中选择多个信息指针。你的刻骨铭心，对别人可能毫无意义；这正是主观价值在高级脑中的体现。

2. 设计 F：由使用者规定怎样从信息源中取出材料，怎样编码、变换和组合。规则可以包含个人熟悉的字符位置、次序、映射和固定步骤；要让自己容易记住，却不让外人轻易还原。

3. 多来源组合：建议把多个个人信息指针纳入体系，由 F 规定它们的顺序和组合方式。

4. 加入秘密材料：可以加入关键脑口令或其他个人掌握的秘密。公开盐值和秘密材料承担的作用不同，应分别说明。

5. 设计 F 的记忆方式：F 本身也可以使用信息指针来建立，让本人容易记住、准确复现，而别人难以从外部线索中拼出。

- 强调规则的清楚与稳定： 规则可以保密，但更重要的是写得准确、没有歧义、能重复执行。使用者必须知道哪些内容需要记忆，哪些内容必须备份，哪些信息绝不能与其他材料放在一起。

6.8 小结：利用安全性基础，构建你的安全堡垒

本章要读者记住高级脑的两个思想根基。第一，未知 F：每个人自己设计并掌握秘密规则，攻击者不能把公开算法直接套在猜测材料上；通用预计算表因此失去适用基础，针对个人建立专门表则必须先识

别或还原 F。第二，主观价值：每个人都有自己的刻骨铭心，而别人的刻骨铭心对你可能毫无意义。信息指针来自个人生命经验，多个来源可以组合，再由 F 组织起来。SHA-256 提供公开、成熟的散列基础；工具、备份、恢复和长期维护则属于同一项工程。

上一章小测验答案：

1. “一维脑钱包”存在什么风险？

答：“一维脑钱包”存在口令太弱、记忆遗忘、泄露风险和依赖个人记忆的风险，还存在被字典攻击的风险，并且容易和他人重复。

2. 高级脑钱包和普通脑钱包（“一维脑钱包”）最大的区别是什么？

答：高级脑钱包不依赖于一个简单口令，而是设计一套复杂的算法规则来生成私钥。

3. 高级脑钱包的核心思想是什么？

答：高级脑强调由使用者主动设计并掌握一套确定、可复现的规则，把材料选择、信息指针、计算步骤、记忆方式、备份和恢复组织成完整的私钥管理过程。

本章小测验：

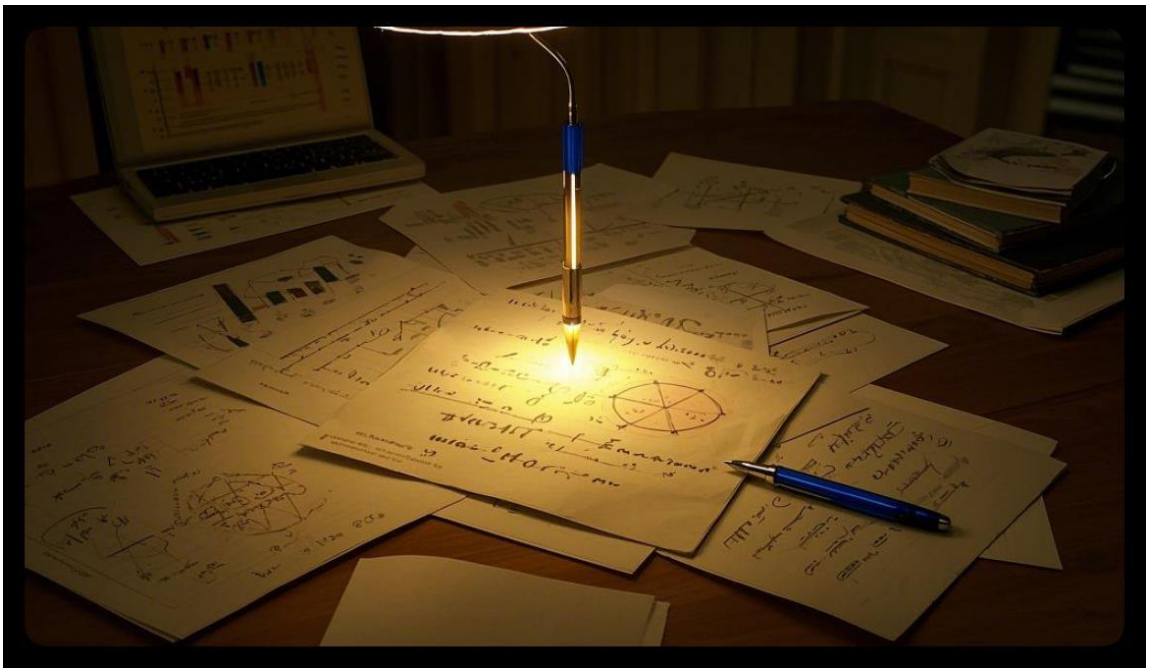
1. 什么是哈希算法？它有什么特点？
2. 什么是抗碰撞性？为什么它很重要？
3. 什么是散列性？它有什么作用？
4. 什么是熵？它在密码学中有什么意义？
5. 高级脑为什么不以随机性或香农熵作为设计目标？
6. 在高级脑中，重复散列和多层散列组合分别起什么作用？
7. 在选择初始脑口令和盐值时，我们应该注意哪些问题？
8. 什么是“关键脑口令”？它有什么特点和作用？
9. 如何使用 BIP39 助记词、Nostr 密钥和随机生成的比特币密钥对作为初始脑口令的一部分？
10. 高级脑钱包的核心是什么？
11. 高级脑钱包如何实现可继承性？

延伸阅读｜研究公约与三个容易混淆的数字

（1）生成过程的随机性：初始材料和完整规则固定后，运行时不再临时抽取随机数；（2）表示空间容量：SHA-256 输出格式为 256 位；（3）攻击者面对的条件：取决于其是否掌握个人信息指针、秘密规则 F 及完整处理步骤。三者描述不同问题，不应混为一谈。

本书先讨论 UTF-8 编码不足 32 字节的 x；但若 F 包含额外秘密输入，则这些输入也应进入完整威胁模型。即使 x 很短，也不能因此先判定系统安全或不安全。

第七章：设计你的高级脑钱包算法——打造独一无二的“秘籍”



生活中的例子 | 给十年后的自己留一份说明书。你今天记得某段经历，也知道怎样从中取出几个字；十年后，若连取字顺序、编码方式和 F 的步骤都说不清，结果就可能变掉。高级脑的规则要让本人记得住，也要让本人多年后做得出来。

7.1 设计原则：灵活、安全、易记

设计高级脑，不是从网上找一套现成模板，而是从自己的信息和记忆出发，设计一套自己掌握的 F。先选择信息指针，再决定怎样组合，最后固定散列步骤、编码和恢复方式。

在设计算法时，我们需要遵循以下三个原则：

- 灵活：信息指针可以来自不同经历，F 也可以按个人习惯设计。每个人的生命经验不同，规则不必千篇一律。
- 秘密：F 由使用者自己掌握。对本人要容易记忆和复现，对外人则不应能从公开资料中轻易推断。规则空间、个人差异和保密方式都要认真考虑。
- 易记：规则必须适合长期使用。太复杂而本人也无法稳定复现的规则，不是好规则。可以用信息指针帮助记忆 F，但必须把编码、顺序和细节固定下来。

7.2 设计步骤：从种子到私钥的奇妙旅程

设计高级脑钱包算法，就像进行一次奇妙的旅行，从种子开始，历经多个步骤，最终到达我们的目的地——私钥。

下面，我将详细讲解设计高级脑钱包的步骤：

1. 选择初始脑口令：

o 信息指针：优先选择自己真正经历、理解并赋予意义的材料。你的刻骨铭心，对别人可能毫无意义；别人熟悉的公开信息，也未必对你有同样价值。

o 初始脑口令：建议不少于 20 个字符。可以由多个个人信息来源组合，也可以纳入独立生成且妥善保密的材料。BIP39 助记词、Nostr 密钥或比特币密钥材料是否适用，取决于它们的真实来源、保密状态和备份安排；公开公钥不能当作秘密。

2. 选择盐值：

o 盐值：盐值可以区分相同输入；若它被设计为秘密材料，也可以纳入 F 的整体秘密体系。不要把公开盐值本身说成秘密算法。

o 保证独特性： 盐值可以和你的规则相结合，提高你规则的独特性。

o 记忆和保存：有意义的个人线索可以帮助记忆，但必须明确它究竟指向什么、怎样取得、如何编码。不要把唯一恢复途径留在模糊的记忆里。

3. 确定哈希次数：

o 哈希套娃：重复散列可以作为 F 规定的确定性处理步骤，也可以增加每次执行所需的计算工作。它不能替代个人信息指针和秘密规则 F；设计时应明确每一步的输入格式、算法和次数，确保本人多年以后仍能准确复现。

o 个性化设置：哈希次数应采用事先确定的固定参数，并准确记录。不要把次数与会变化、难以恢复的外部信息随意绑定。

o 具体流程：可以把上一次 SHA-256 结果按明确格式与盐值或其他材料组合，再进行下一次 SHA-256。若把两个 SHA-256 结果连接起来作为下一步输入，必须明确连接的是原始 32 字节还是 64 位十六进制文本，二者不是同一输入。

4. 确定哈希算法：

o 中间散列：建议不使用低于 SHA-256 强度的散列算法。中间可以采用 SHA-256，也可以采用 SHA-512，或组合多个 SHA-256 结果。

o 最终散列：无论中间步骤怎样增强，最终仍按 SHA-256 生成 256 位结果。中间出现 512 位输入，不代表最终输出空间变成 512 位，也不能把多次散列强度简单相加。

5. 引入“关键脑口令”：

o 关键脑口令：可以作为 F 中的一项秘密材料，参与指定步骤。它能否发挥作用，取决于它是否真正保密、是否容易被猜中，以及规则是否明确。

o 记忆与恢复：关键脑口令可以借助个人信息指针记忆，但不能把“只记在脑中”当作唯一保障。要预先考虑失能、意外和继承。

6. 设置多重地址：

o 使用序号： 你可以通过改变序号来生成不同的地址，方便管理你的比特币资产。

o 使用变量： 你也可以通过改变哈希次数，或者其他的变量来生成不同的地址。

o 分层存储： 你可以用不同的地址来接收来自不同来源的比特币，从而保护你的隐私。

7.3 设计高级脑钱包算法

设计完成后，必须把 F 写成可执行、无歧义的规则：输入材料、信息指针、编码方式、拼接边界、每一步散列算法、迭代次数、序号格式和最终密钥处理都要固定。F 可以保密，但使用者必须能够准确掌握它。

以下提供几个案例供您参考：

• 案例一：多个个人信息指针与秘密 F（结构示例）

1. 初始脑口令：由使用者选择的多个个人经历线索组成，最终文本不少于 20 个字符。这里不展示可直接使用的真实材料。

2. F：由本人设计，规定各信息指针的取用、编码、顺序和组合方式；F 本身也可以借助个人信息指针记忆。

3. 盐值及参数：使用事先固定的材料与常量，明确其是否属于秘密。

4. 中间处理：可以使用 SHA-256 或 SHA-512；也可以把两个 SHA-256 结果按固定格式连接，作为下一步输入。

5. 最终处理：按既定规则执行 SHA-256，得到 256 位最终散列结果。

6. 地址序号：如需生成多个地址，序号的编码和加入位置必须固定，并用测试材料验证。

• 案例二：用个人记忆构建 F（结构示例）

1. 信息来源：选择几段对本人有意义、对外人未必有意义的经历。不要直接使用公开资料中能查到的完整内容。

2. 信息指针：为每段经历设定稳定的指向方式，明确如何取用材料。

3. 秘密规则：由本人设计取用次序、字符处理、拼接边界和固定参数。

4. 初始脑口令：将材料按规则组织成不少于 20 个字符的输入。

5. 散列处理：中间不使用低于 SHA-256 强度的散列算法，最终按 SHA-256 输出。

6. 验证：使用公开测试材料记录每一步的预期结果，确认换设备后仍能复现。

• 案例三：多种来源组合（结构示例）

1. 信息来源：可以组合个人经历、长期记忆和独立生成且妥善保密的材料。公开公钥不能作为秘密材料。

2. F：明确每种材料的取用方式、编码、组合顺序和中间处理步骤。

3. 初始脑口令：不少于 20 个字符，并确保真实材料有可靠的恢复安排。

不少于 20 个字符是本书提出的最低设计要求，不是安全保证。长度不能替代对材料来源、F 的保密性、公开线索和候选验证条件的分析。

4. 散列处理：允许 SHA-256、SHA-512 及多个散列结果组合；最终仍输出 256 位 SHA-256 结果。

5. 复现测试：使用公开测试材料交叉验证，隔一段时间重新执行，确认规则没有歧义。

6. 真实资产：以上示例不可直接照搬。先完成独立审查、备份、恢复和签名演练。

高级脑不提供一套所有人照抄的模板。每个人都应从自己的生命经验中选择信息指针，再设计自己掌握的 F。

F 可以像密码口令一样定期更换，但更换前必须先完成新规则的测试、地址核对和资产迁移。

设计时要把规则写清楚：哪些内容来自记忆，哪些内容必须备份，哪些材料属于秘密，哪些参数不能改变。

不要把“我记得住”当作唯一的恢复方案。十年后的自己也需要一份准确、可执行的说明。

也不要把“别人不知道”当作唯一的安全理由。F 应当有足够的个人化规则空间，并避免从公开生活信息中被轻易推断。

多来源组合是推荐做法，但每个来源都要明确取用方式和边界，避免不同材料拼接时产生歧义。

本章案例用于说明设计思路，不是可以直接用于真实资产的现成算法。

7.4 小结：设计自己的信息指针与秘密规则

设计完成后，先用公开测试材料走完整个流程。隔一段时间，再不看临时提示独立执行一次；换一台可信设备，再核对一次结果。确认规则没有歧义、工具输出一致、备份可以恢复，再考虑真实资产。

SHA-256 输出是一个 256 位数值，但并非每个 256 位数值都能直接作为 secp256k1 私钥。有效私钥必须满足 $1 \le d < n$，其中 n 为 secp256k1 曲线的阶：FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141。若候选值不在此范围内，方案必须事先规定统一、确定性的处理方式，例如按固定编码和计数器生成下一候选值并重

新检查；不得临时修改输入或由使用者自行挑选。不同工具必须实现完全相同的规则，并用公开测试向量交叉验证。本书推荐工具的具体版本是否已按此规则处理，必须通过源码审查和实测确认，不能仅凭界面推断。地址类型、编码和脚本也要固定。

上一章小测验答案：

1. 什么是哈希算法？它有什么特点？

答：哈希算法是一种将任意长度的输入信息转换为固定长度输出信息的算法，其特点是单向性、固定长度输出和雪崩效应。

2. 什么是抗碰撞性？为什么它很重要？

答：抗碰撞性是指很难找到两个不同输入却产生相同摘要。SHA-256 在工程上提供极高的碰撞搜索门槛；私钥是否有效，还要按比特币椭圆曲线的有效范围进行检查。

3. 什么是散列性？它有什么作用？

答：这里指的是哈希函数的雪崩效应：输入发生微小变化时，输出通常会有大量比特改变。它让不同输入的摘要差异明显，但不保证私钥具有随机来源，也不能代替输入材料的质量。

4. 什么是香农熵？它在哪些技术场景中有用？

答：香农熵描述给定概率分布下的平均不确定性。在 BIP39 初始随机材料、随机数发生器等场景中，它是分析材料来源和随机质量的工具。高级脑不以追求香农熵为设计目标，其重点是个人信息指针、秘密规则 F 和确定性生成过程。

5. 高级脑为什么不以随机性或香农熵作为设计目标？

答：高级脑的出发点就是让使用者事先确定个人信息指针和秘密规则 F，在生成时按固定步骤得到可复现的结果。我们不要求生成过程临时抽取随机数，也不把香农熵数值当作高级脑的目标。个人信息指针来自主观价值，F 由本人设计并掌握；攻击者若不知道 F，就不能把猜测的个人材料直接代入真实流程。

6. 在高级脑中，重复散列和多层散列组合分别起什么作用？

答：重复散列和多层散列组合可以成为 F 的一部分，用来安排确定性的处理步骤，也可以增加每次执行所需的计算工作。它们不能代替 F 的秘密性，也不能改变最终 SHA-256 只有 256 位输出这一事实。关键是把输入格式、连接方式、算法和迭代次数写清楚，保证结果能够准确复现。

7. 在选择初始脑口令和盐值时，我们应该注意哪些问题？

答：利用“信息的指针记忆法”，把复杂材料对应到自己熟悉、能够长期回忆的信息上，再按照事先固定的规则组合。信息来源可以多样，但必须考虑公开程度、稳定性和多年后的可恢复性。

8. 什么是“关键脑口令”？它有什么特点和作用？

答："关键脑口令"是高级脑规则中由使用者特别保护的一项秘密材料。把它只记在脑中，是一种减少实体留存的个人选择，但人会遗忘，也会遭遇疾病和意外，因此必须同时认真考虑本人失能、继承和恢复安排，不能把"绝对不会忘记"当成设计前提。

9. 如何使用 BIP39 助记词、Nostr 密钥和随机生成的比特币密钥对作为初始脑口令的一部分？

答：BIP39 助记词、Nostr 密钥或比特币密钥材料可以按设计纳入高级脑的输入体系。使用前要确认材料的来源、保密状态和恢复方式，并由 F 规定如何取用和组合。高级脑不要求把这些材料转化为随机数指标；重点是它们是否属于本人掌握的秘密材料，以及能否在未来准确恢复。

10. 高级脑钱包的核心是什么？

答：高级脑的核心是使用者主动设计并掌握一套确定、可复现的规则，把个人信息、秘密材料、计算步骤、记忆方法和恢复安排组织成完整的私钥管理过程。

11. 高级脑钱包如何实现可继承性？

答：高级脑钱包的可继承性指的是，在保证安全性的前提下，让家人在必要时通过备份的规则算法、其他脑口令和盐值，以及用户和家人共同记忆的关键脑口令，来继承用户的比特币资产。

本章小测验：

1. 设计高级脑钱包算法时，需要遵循哪些原则？
2. 设计高级脑钱包算法的主要步骤有哪些？
3. 什么是"信息的指针记忆法"，如何使用它来设计高级脑钱包？
4. 初始脑口令的选择有哪些建议？
5. 在设计高级脑钱包时，如何利用 BIP39 助记词、Nostr 密钥、和随机生成的比特币密钥对？

延伸阅读｜一份可复现的算法说明至少包含什么

对同一个输入得到同一个结果，需要逐项固定：字符编码（如 UTF-8）、Unicode 规范化方式、大小写及空格保留、材料顺序、分隔符、SHA-256 每次处理的是原始字节还是十六进制文本、迭代起止、序号格式、输出字节序、密钥合法区间以及地址脚本类型。任何一项遗漏，都可能使多年后的恢复失败。

教学演示建议使用毫无资产价值的公开测试向量。书中出现的示例密钥与口令一律视为已公开、不可用于真实持币。

第八章：使用工具生成地址——验证你的规则与生成结果



生活中的例子 | 把生成地址想成给一间尚未入住的房子写门牌号：门牌号可以公开给朋友，但开门的钥匙必须安全保管。第一次生成后，至少要用另一条可靠途径验证门牌号确实对应你的钥匙；练习只能使用公开演示数据，不能把真实口令输入来历不明的网站。

8.1 为什么需要工具？——专业的事情交给专业的工具

上一章我们学习了如何设计高级脑钱包算法，现在，我们需要把我们设计的算法付诸实践，生成私钥和地址。虽然理论上我们可以手动计算哈希值，但这种方式效率低下，且容易出错。因此，我们需要借助专业的工具来完成这项工作。

就像我们要盖房子，需要借助水泥搅拌机，而不是用手搅拌水泥，使用专业的工具，可以事半功倍，并且确保结果的准确性。

8.2 选择合适的工具：开源、安全、离线

在选择工具时，我们需要注意以下几点：

- 开源：尽量选择开源的工具。开源意味着代码是公开透明的，任何人都可以查看和验证代码，从而确保工具的安全性。我们选择餐厅吃饭，也会尽量选择后厨开放的餐厅，这样可以看到食材是否新鲜，制作过程是否卫生。

- 安全：选择工具的时候，确保工具的来源可靠，并且没有后门和恶意代码。就像我们选择网购商品，会尽量选择信誉良好的商家，避免买到假冒伪劣的商品。
- 离线：在生成私钥和地址时，一定要在离线环境下操作，避免私钥被泄露。就像我们取银行卡密码，会尽量选择在安全的环境下进行，避免被他人偷窥。

在上一章，我们推荐了达哥（@btcdage）的 Python 开源高级脑钱包工具，它符合我们上述要求，可以在 Github 上找到：

- 开源地址：https://github.com/btcdage2000/BrainWalletGenerator/
  - 可执行文件下载地址：https://github.com/btcdage2000/BrainWalletGenerator/releases/tag/0.2.1

8.3 离线操作的重要性：保护私钥的生命线

在生成私钥和地址时，一定要确保你的计算机处于离线状态。这是因为，一旦你的计算机连接到互联网，你的私钥就可能会暴露在黑客的攻击之下。

以下是几个需要注意的事项：

- 断开网络连接：关闭 WiFi 和蓝牙，拔掉网线，确保你的电脑没有连接任何网络。
- 使用专门的离线电脑：如果条件允许，尽量使用一台专门用于生成私钥的电脑，不要安装任何其他软件，也不要连接任何网络。这是最安全的方法。
- U 盘启动的离线系统：如果你没有专门的离线电脑，你可以使用 U 盘启动一个离线操作系统，这比使用虚拟机更加安全，因为虚拟机仍然依赖于宿主机的安全性。条件允许的话拔掉本机硬盘的数据线或电源线，可提高安全性。
- 虚拟机：可以在虚拟机中运行工具，但虚拟机仍然依赖于宿主机的安全性，如果宿主机已经存在病毒，可能会对虚拟机进行截屏，因此虚拟机是最后不得已的选择。
- 不要截屏：不要对生成的私钥和地址进行截屏，避免信息泄露。
- 及时清除浏览器缓存：如果你使用了基于浏览器的 JS 工具生成私钥，记得及时清除浏览器缓存，避免信息被残留。

8.4 使用达哥的 Python 工具生成地址：按步骤操作

现在，我们来详细介绍如何使用达哥的 Python 工具生成地址：

1. 下载工具：
   - 下载源码：从 Github 上下载达哥的 Python 开源工具，并将其保存到你的电脑上。

o 下载可执行文件： 你也可以从 Github Release 页面下载编译后的可执行文件，这样就无需安装 Python 环境。

下载地址： https://github.com/btcdage2000/BrainWalletGenerator/releases/tag/0.2.1

2. 断开网络连接： 按照上述要求，断开你的电脑的网络连接，确保电脑处于离线状态。

3. 运行工具：

o 运行源码： 如果你选择下载源码，你需要先安装 Python 3.6 或更高的版本。 然后在终端或者命令提示符中，输入 python brain_wallet_generator.py 命令来运行工具。

o 运行可执行文件： 如果你下载的是可执行文件，则可以直接运行它，无需安装 Python 环境。

4. 拼接初始信息：

重要提示：达哥的开源工具负责执行哈希加盐等确定性处理。初始脑口令建议不少于 20 个字符；使用者先按照自己的 F 完成信息指针取用、编码和组合，再把规则规定的输入交给工具。工具不替你设计或保存 F。高级脑不以随机性或香农熵作为目标，核心在于本人掌握完整材料与规则，并能独立复现。

脑口令输入：按 F 规定的编码和组合方式，准备好完整输入后再填入“Passphrase / 脑口令”输入框。务必固定字符编码、分隔符和拼接顺序。

盐值输入：如果 F 规定使用独立盐值，按既定格式填入“Salt / 加盐”输入框，并记录它是否属于秘密材料。

1. 设置哈希次数： 在 “Hash Times / 哈希次数” 的下拉菜单中，选择你设定的哈希次数。

2. 生成密钥： 点击 “Generate Brain Wallet / 开始计算” 按钮，工具就会按照你设置的哈希套娃流程进行运算，生成私钥、公钥、P2PKH 地址，以及 Bech32 地址等信息。

3. 记录地址：将生成的 P2PKH 地址和 Bech32 地址记录下来，作为公开的核对信息。地址不是私钥，也不能用于恢复资产；不要把“备份地址”当成完成钱包备份。真正需要妥善保存的是能够按既定规则恢复私钥的完整材料、规则说明和必要参数。

4. 清空信息： 点击 “Clear All / 清空所有” 按钮来清空所有信息，避免泄露。

8.5 验证地址：确保地址的正确性

为了确保生成的地址是正确的，我们需要进行验证。

- 使用 Electrum 等钱包： 你可以使用 Electrum 等钱包软件，导入你的私钥，然后验证生成的地址是否正确。

o 注意事项： 请务必在离线状态下进行导入和验证操作，以避免私钥泄露。

8.6 小结：安全生成你的“加密秘钥”

本章我们学习了如何使用工具生成高级脑钱包的私钥和地址，并且强调了离线操作的重要性。现在，你已经拥有了你的“加密秘籍”，你就可以开始安全地管理你的比特币资产了。

上一章小测验答案：

1. 设计高级脑钱包算法时，需要遵循哪些原则？

答：设计高级脑钱包算法时，需要遵循灵活、安全、易记的原则。

2. 设计高级脑钱包算法的主要步骤有哪些？

答：主要步骤包括选择初始脑口令、选择盐值、确定哈希次数、确定哈希算法、引入“关键脑口令”和改变序号设置多重地址。

3. 什么是“信息的指针记忆法”，如何使用它来设计高级脑钱包？

答：“信息的指针记忆法”是一种将复杂字符串转换为容易记忆的指向性信息的方法，可以利用诗词、故事、歌曲、新闻等作为信息源，并通过规则转换为脑口令。

4. 初始脑口令的选择有哪些建议？

答：初始脑口令应符合高级脑的设计要求，建议不少于 20 个字符。可以由多个个人信息来源组合，也可以纳入本人掌握的其他秘密材料；重点是由 F 规定如何取用、编码和组合，并确保多年以后能够准确恢复。

5. 在设计高级脑钱包时，如何利用 BIP39 助记词、Nostr 密钥、和随机生成的比特币密钥对？

答：可以按 F 的规定，将 BIP39 助记词、Nostr 秘密材料或比特币秘密密钥材料纳入输入体系。必须区分公开公钥与秘密材料，并确认来源、保密状态及恢复安排。高级脑关注的是材料与个人规则如何共同构成完整生成过程。

本章小测验：

1. 为什么我们需要使用工具来生成高级脑钱包的地址？
2. 在选择生成工具时，我们需要注意哪些方面？
3. 为什么离线操作在生成私钥时非常重要？
4. 在使用达哥的 Python 工具生成地址时，应该注意哪些步骤？
5. 生成地址后，我们如何验证地址的正确性？
6. 使用 Electrum 等钱包验证地址时，有哪些注意事项？
7. 达哥的 Python 工具的功能是什么？ 你应该如何利用它来实现你设计的高级脑钱包算法？

延伸阅读丨离线不等于可信

离线环境主要降低远程泄露面；被篡改的软件、恶意安装包、剪贴板监视器、离线设备故障以及错误的地址算法依然可能造成损失。建议在独立实现之间对照同一测试向量，验证源代码与发布校验值，并先执行从生成到恢复再到签名的完整测试。

第九章：安全存储与备份——你的“加密秘籍”的守护之道



生活中的例子 | 一份秘密全部放在脑海里，最大的优点是不用随身携带纸张，最大的挑战是记忆也会受到时间、疾病和意外影响。所谓备份，不只是把信息藏好，而是确保真正需要时能够找回来——包括多年后的自己和得到合法授权的家人。

9.1 为什么需要安全存储和备份？——未雨绸缪，防患未然

上一章我们学习了如何使用工具生成高级脑钱包的地址，现在，我们已经拥有了我们的私钥和地址，就如同我们盖好了一栋房子，接下来我们就要考虑如何保护它了。

在高级脑钱包中，我们需要保护的关键信息包括：

- 算法规则： 你用来生成私钥的步骤和方法，包括你选择的哈希算法，盐值以及哈希的次数等。
- 脑口令： 你用来生成私钥的初始口令，包括你使用的诗词、故事、个人信息等等。
- 关键脑口令： 你独有的，作为最后一道防线的关键脑口令。
- 盐值： 你用来增加复杂性的盐值。

这些信息就如同我们房子的地基、承重墙，和门锁，如果丢失或泄露，你的房子就岌岌可危。因此，我们需要认真对待这些信息的存储和备份，确保它们安全无虞。

9.2 “关键脑口令”的特殊性：记忆、保密与恢复

在高级脑钱包中，“关键脑口令” 扮演着非常特殊的角色：

- 重要秘密材料：它可以作为规则中的一项独立秘密。即使其他材料泄露，它也可能继续发挥作用；但其保护效果取决于实际内容、保密情况和整个生成规则，不能视为无条件的安全保证。
- 个人化：可以借助个人经历和信息指针来记忆，但个人熟悉不等于外人无法推测，仍需结合公开资料和熟人可能掌握的信息评估。
- 保密与可恢复：它应当作为秘密材料保护，同时必须考虑遗忘、疾病、意外和继承。记忆有价值，但记忆本身不是可靠的唯一备份。

因此，“关键脑口令”的存储策略和其他信息不同：

- 保存方式：是否只靠记忆、是否采用加密备份或受控封存，应根据个人风险选择。若采用物理或数字备份，必须评估被盗、复制和集中泄露的风险；若只靠记忆，则必须接受遗忘或失能可能导致永久丢失的风险。
- 记忆方法：可以运用“信息的指针记忆法”，将关键脑口令与一段特殊经历联系起来，并定期复核。但不要把“刻骨铭心”当作永不遗忘的保证。
- 传递方法：如需继承，应事先设计受控的交接或恢复安排，明确谁在什么条件下可以取得必要材料。仅靠口头告知，可能造成遗忘、误传或无法执行。

9.3 算法规则的备份策略：打印多份，分散存储

算法规则是你高级脑钱包的核心，你需要对其进行周密的备份，确保不会丢失。

- 打印多份： 将你的算法规则打印成多份，建议至少三份。
  - 避免单点故障： 多份打印可以避免单一副本丢失或损坏。
- 分散存储： 将打印好的算法规则，分别存放在不同的安全地点。
  - 保险箱： 你可以将一份存放在银行保险箱中，确保其安全。
  - 隐蔽的家中角落： 你可以将另一份存放在家中隐蔽的角落，但要保证只有你自己知道。
  - 信赖的家人： 将一份交给最信任的家人。
- 定期复查： 定期检查你的算法规则，确保你的备份是完整的，没有遗漏或错误。

9.4 其他脑口令和盐值的备份：灵活选择，多重保障

对于除了 “关键脑口令” 以外的其他脑口令和盐值，你可以灵活选择合适的备份方式：

- 物理备份：你可以将它们抄写在纸上，或者打印出来，然后将其存放在不同的安全地点，比如保险箱或者隐蔽的家中角落。
  - 避免物理风险：注意防水、防火、防虫，避免纸张丢失或损坏。
- 数字备份：你也可以将它们加密后，存储在 U 盘，移动硬盘等移动设备，或者网盘等云端存储中。
  - 加密安全：使用加密软件对备份文件进行加密，确保即使移动设备丢失或云端账户被盗，你的信息也不会泄露。
- 多重备份：你可以将物理备份和数字备份结合起来使用，实现多重保障。
  - 双重保险：多种备份方式可以增加备份的可靠性，即使某一种备份方式失效，也可以用其他备份方式恢复。

9.5 可继承性：为未来做好准备

高级脑钱包的设计不仅仅要考虑安全性，也要考虑可继承性，也就是在你发生意外时，你的家人如何继承你的比特币资产：

- 告知家人：提前告知家人你的高级脑钱包的规则，并将“关键脑口令”口头传授给他们。
  - 提前沟通：提前沟通可以确保家人了解如何使用高级脑钱包，以及如何正确继承你的比特币资产。
- 多重备份：确保家人知道你的备份信息的位置，例如，告诉他们银行保险箱的钥匙在哪里，你将其他脑口令和盐值备份在哪个 U 盘或者移动硬盘中。
  - 多重保险：多重备份可以确保即使家人没有你的“关键脑口令”，也能在知道其他脑口令和规则的情况下，及时转移你的比特币资产。
- 法律文件：你还可以将比特币资产的继承写入遗嘱等法律文件中，确保资产的顺利继承。
- 法律保障：使用法律文件可以最大程度保障你比特币资产的安全继承。

* 提示：你应该咨询专业的法律人士，根据你所在地的法律法规制定相应的法律文件。

9.6 小结：妥善保管你的“加密秘籍”

高级脑钱包的安全性不仅仅取决于算法的复杂性，更取决于你是否能妥善保管好你的算法规则、脑口令和盐值，以及你是否为未来做好准备，确保你的比特币资产能够安全继承。

上一章小测验答案：

1. 为什么我们需要使用工具来生成高级脑钱包的地址？

答：我们需要使用工具来生成高级脑钱包的地址，因为手动计算效率低下，且容易出错。

2. 在选择生成工具时，我们需要注意哪些方面？

答：在选择生成工具时，我们需要注意开源、安全和离线。

3. 为什么离线操作在生成私钥时非常重要？

答：离线操作在生成私钥时非常重要，因为可以避免私钥被泄露。

4. 在使用达哥的 Python 工具生成地址时，应该注意哪些步骤？

答：在使用达哥的 Python 工具生成地址时，需要注意先下载工具，断开网络连接，然后输入初始信息，生成密钥，备份地址，最后清空信息。

5. 生成地址后，我们如何验证地址的正确性？

答：生成地址后，可以使用 Electrum 等钱包验证地址的正确性。

6. 使用 Electrum 等钱包验证地址时，有哪些注意事项？

答：使用 Electrum 等钱包验证地址时，需要确保在离线状态下进行操作。

7. 达哥的 Python 工具的功能是什么？ 你应该如何利用它来实现你设计的高级脑钱包算法？

答：达哥的 Python 工具的功能是进行哈希加盐套娃操作，你需要将初始脑口令，盐值等按照自己设计的规则拼接在一起，然后作为参数输入，然后运行工具生成私钥。

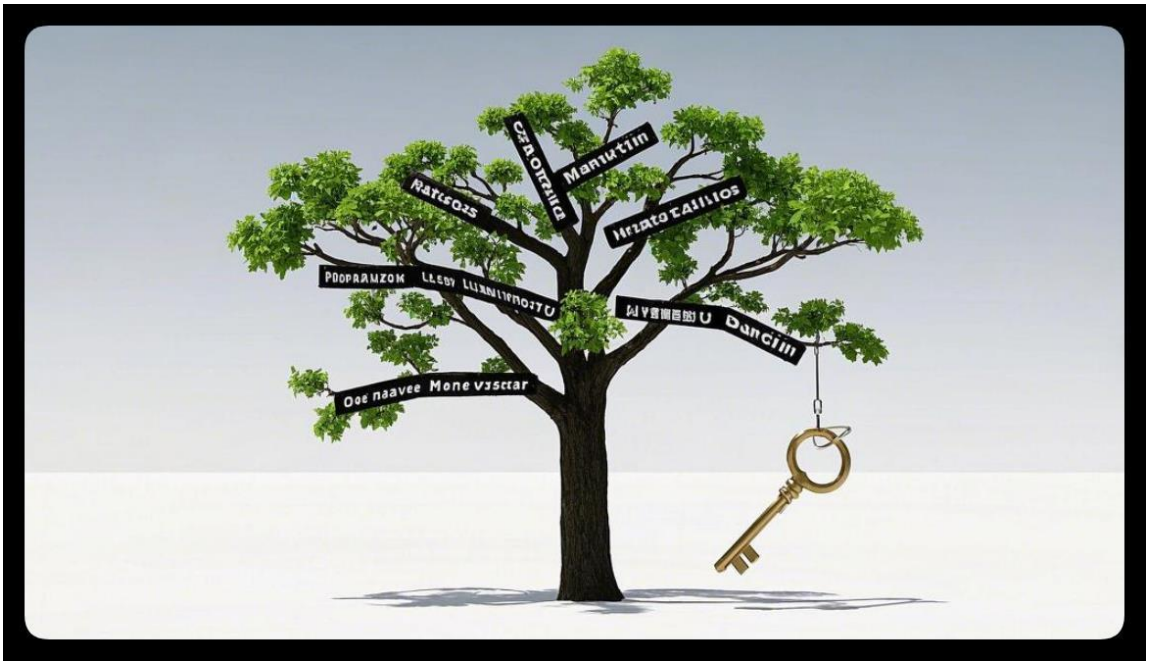
本章小测验：

1. 在高级脑钱包中，我们需要保护哪些关键信息？
2. “关键脑口令” 在高级脑钱包中有什么特殊性？应该如何存储？
3. 如何备份你的算法规则？
4. 如何备份你的其他脑口令和盐值？
5. 什么是高级脑钱包的“可继承性”？为什么它很重要？
6. 你将如何保证你的家人在必要的时候能够继承你的比特币资产？

延伸阅读｜备份方案与继承演练是两套测试

第一套是“本人丢失设备后还能恢复吗”；第二套是“合法继承人在本人无法协助时能完成恢复吗”。不要只测试知道全部答案的自己。秘密材料分散保存可以降低单点泄露风险，也可能增加资料丢失和协作失败的概率。可以采用受控封存、恢复说明、定期复核及专业法律安排。关键脑口令只靠记忆保存，是一种个人取舍，不应作为对所有读者的绝对要求。

第十章：HD 钱包、派生路径、多重地址



生活中的例子 | 同一棵树可以长出许多树枝。HD 钱包也能从根部材料按照约定路径派生许多密钥和地址。树枝编号一旦写错，就可能找到另一根枝条。理解“根、路径、索引”的关系，比死记复杂的路径字符更有用。

10.1 HD 钱包：一颗种子，无限可能

在比特币钱包中，除了高级脑钱包，还有一种常见的钱包类型，叫做 HD 钱包，全称 Hierarchical Deterministic Wallet，也就是 “分层确定性钱包”。

- HD 钱包的原理： HD 钱包的核心在于使用一个种子（Seed），就像一颗种子可以生长出无数颗树一样，通过这个种子，可以生成无数个私钥和地址。你可以把 HD 钱包想象成一个“钥匙串”，只需要一把主钥匙，就可以生成无数把不同的钥匙，每一把钥匙都可以打开不同的门。这个“种子”通常是由 12、18 或 24 个助记词组成，它代表了生成所有私钥和地址的根源。
- 主私钥和主公钥： HD 钱包首先会根据种子生成一个主私钥和一个主公钥，它们是所有私钥和地址的根源。主私钥和主公钥就像是你的“主钥匙”和“主锁”，它们可以生成其他的钥匙和锁。
- BIP32 和 BIP44： 为了规范 HD 钱包的运作，比特币社区制定了一些标准，比如 BIP32 和 BIP44。它们定义了如何根据主私钥生成私钥和地址的规则，确保不同的钱包之间可以兼容。

10.2 派生路径：生成密钥的“路线图”

- 什么是派生路径？ HD 钱包通过 派生路径 (Derivation Path) 来生成不同的私钥和地址。派生路径就像是一张“路线图”，它告诉 HD 钱包应该如何根据主私钥生成特定的私钥和地址。派生路径就像你的“地址簿”，每当你需要使用某个地址时，HD 钱包就会按照 “地址簿” 中记录的路线图来生成相应的地址。
- 派生路径的结构： 派生路径通常由一串数字和斜杠组成，比如 m/44'/0'/0'/0/0。其中， m 代表主私钥， 数字则代表不同的路径层级。
- 派生路径的作用： 通过不同的派生路径，HD 钱包可以生成无数个不同的私钥和地址，从而方便用户管理和隔离资产。

10.3 多重地址：管理资产的“分身术”

- HD 钱包的多重地址： HD 钱包利用派生路径生成多个不同的地址，称为多重地址。这就像你拥有多个银行账户，可以将不同的资产存放在不同的账户里，从而方便管理。
- 多重地址的好处：
  - 方便管理： 你可以将不同用途的比特币分别存储在不同的地址中，方便管理和追踪。
  - 提高隐私： 使用多重地址可以减少不同收款用途之间的直接关联，避免将你的所有比特币都关联到同一个地址上。

10.4 高级脑钱包与 HD 钱包的思路差异：手动生成 vs 自动派生

虽然 HD 钱包和高级脑钱包都是用来管理私钥和地址的工具，但是它们的设计思路却截然不同：

- HD 钱包：
  - 依赖于种子： 它依赖于种子来生成所有私钥和地址。这个种子是所有私钥的根源，拥有了种子就拥有了所有私钥的控制权。
  - 自动派生： 它使用派生路径自动派生私钥和地址。
  - 集中管理： 所有私钥和地址都由一个主私钥派生出来，它们之间存在着关联。
  - 默认推荐： 几乎所有的钱包软件都默认使用 HD 钱包。
- 高级脑钱包：
  - 独立生成： 它不依赖于一个单一的种子，而是通过一系列复杂的规则来生成私钥和地址，你可以把规则看做种子，但是规则完全有你控制，并且可以灵活自定义。
  - 手动生成： 它需要手动设计算法，生成不同的私钥和地址。

- 独立地址： 你手动生成的地址之间，没有必然的关联。
- 隐私至上： 高级脑钱包的设计理念是极度追求安全性，隐私性，独立性，灵活性。

10.5 高级脑的地址管理理念：自主、隐私与可恢复

高级脑强调由使用者掌握生成规则、按需生成地址、减少不必要的地址复用，并让每个地址的来历都能被自己解释和复现。这些做法有助于隐私管理和信息控制。它们并不能替代比特币签名算法本身的安全，也不能单独解决未来量子计算带来的风险。

- 手动生成地址： 我们倾向于手动设计算法，然后生成不同的地址，而不是依赖于 HD 钱包自动派生。
- 一个地址只用一次： 我们强调 “一个地址只用一次” 的原则，每次接收新的比特币都使用一个新的地址，避免将不同交易关联起来。
- 为什么 “一个地址只用一次”：

  保护隐私： 在区块链上，所有的交易记录都是公开的，如果你的多个交易都使用同一个地址，那么你的资产就会暴露在别人的视线之下，隐私性较低。

  - 公钥暴露与量子风险：在相应脚本中，花费交易广播时会公开公钥或可恢复公钥的数据。使用新地址可以减少未花费阶段的长期暴露和地址关联，但不能消除交易进入内存池后至确认前的暴露窗口。因此它是风险降低措施，而不是量子防护保证。

  接收地址管理： 新地址可以减少地址复用和部分关联，但接收前必须确保对应私钥与规则已经正确保存并经过恢复验证。地址未使用不等于“绝对安全”，也不代表可以忽略私钥管理。

- 找零地址： 当我们进行比特币转账时，将找零地址设置为高级脑生成的另一个新的地址，而不是默认的旧地址。你可以在每次交易时都使用一个新的地址作为找零地址，这样就可以有效提高交易的隐私性。
- 选择管理方式： 高级脑允许使用者按自己的规则独立生成地址；HD 钱包则通过标准化派生路径管理一组地址。两者各有取舍。手动生成减少某些自动关联，也增加了地址发现、序号记录和找零管理的工作。
- 转账后的源地址管理： 转账后应核对交易、UTXO 和找零去向。将私钥导入热钱包会扩大秘密暴露面；即使源地址不再接收新款，也不能据此断言其他资产或秘密不受影响。

10.6 小结：高级脑钱包的独特性

本章介绍了 HD 钱包、派生路径和多重地址，也说明了高级脑与自动派生钱包在管理方式上的差异。高级脑更强调使用者亲自掌握材料和规则，按自己的安排生成、记录和验证地址。手动管理带来自主性，也带来更多需要自己负责的步骤；隐私收益和安全效果都要结合实际使用方式判断。

上一章小测验答案：

1. 在高级脑钱包中，我们需要保护哪些关键信息？

答：在高级脑钱包中，我们需要保护的关键信息包括算法规则、脑口令（包括“关键脑口令”）和盐值。

2. “关键脑口令” 在高级脑钱包中有什么特殊性？应该如何存储？

答：“关键脑口令”在高级脑钱包中是最后一道防线，只记忆在脑中，不记录在任何物理介质中，并且刻骨铭心，绝对不可能忘记。

3. 如何备份你的算法规则？

答：备份算法规则时，应该打印多份，并分散存储在不同的安全地点。

4. 如何备份你的其他脑口令和盐值？

答：备份其他脑口令和盐值时，可以使用物理备份和数字备份结合的方式，并进行加密处理。

5. 什么是高级脑钱包的“可继承性”？为什么它很重要？

答：高级脑钱包的“可继承性”指的是，在保证安全性的前提下，让家人在必要时通过备份的规则算法、其他脑口令和盐值，以及用户和家人共同记忆的关键脑口令，来继承用户的比特币资产。

6. 为了保证家人可以继承比特币资产，应该如何做？

答：为了保证家人可以继承比特币资产，需要提前告知家人高级脑钱包的规则，并口头传授 “关键脑口令”， 并确保家人知道如何找到你备份的其他信息。

本章小测验：

1. 什么是 HD 钱包？它的核心是什么？
2. 什么是派生路径？它有什么作用？
3. 什么是多重地址？它有什么好处？
4. HD 钱包和高级脑钱包在设计思路上有什么不同？
5. 为什么我们要强调“一个地址只用一次”？
6. 在高级脑钱包中，你如何处理比特币转账中的找零？
7. 除了隐私性，“一个地址只用一次”能降低哪些风险，又不能解决哪些问题？
8. “一个地址只用一次” 如何保证你接收比特币时的地址安全？以及转账后原地址的安全性？

延伸阅读 | 多地址不等于天然的隐私

换地址可以降低某些直接复用，但找零、UTXO 合并、交易图谱与钱包指纹仍可能关联地址。HD 钱包的派生路径及脚本类型应记录清楚。高级脑手动序号派生需要额外注意序号重叠、恢复范围、地址发现与找零管理。关于量子计算，应区别公钥暴露时间、交易场景与尚未确定的未来迁移方案。

第十一章：高级脑的工程安全观



生活中的例子 | 安全不是一把锁的厚度，而是一套房子的整体防护。锁很结实，窗户却敞开，仍然危险。对于高级脑，口令、规则、计算设备、交易签名、备份、继承都属于这套房子的不同部分：只看某一部分，很难得出完整的安全判断。

前面谈过私钥、哈希、规则和地址。本章把视角再拉远一些：安全不是某个算法或某台设备单独提供的属性，而是整套安排共同产生的结果。算法可以正确，设备也可以可靠，但只要使用者记错一个步骤，或者多年后无人知道怎样恢复，资产仍可能失去控制。工程学关心的，就是这些环节如何衔接。

11.1 安全不是绝对的：风险无处不在

经过前面章节的学习，我们已经掌握了设计和使用高级脑钱包的方法。但是，我们必须时刻牢记，安全不是绝对的。没有任何一种安全措施能够保证 100% 的安全。

- 风险无处不在：比特币世界充满了各种未知的风险，比如黑客攻击、设备损坏、信息泄露、甚至是认知偏差等，这些风险可能会让你失去你的比特币资产。
- 没有一劳永逸：技术在不断发展，新的攻击手段也可能出现，所以你需要不断学习和更新你的知识，与时俱进，才能应对新的挑战。

- 保持警惕： 永远不要放松警惕，对任何事情都要保持怀疑态度，不要轻易相信陌生人，也不要点击不明链接。

11.2 安全习惯：每天进步一点点

除了技术上的安全措施，我们还需要养成良好的安全习惯，才能更好地保护自己的比特币资产：

- 持续学习： 随时关注最新的比特币安全动态，了解最新的攻击手段和防御方法，并根据实际情况，调整你的安全策略。
  - 关注安全资讯： 多关注比特币安全相关的文章、博客和论坛，关注达哥的微博和 nostr（@btcdage），并学习其他用户的经验教训。
- 定期复查： 定期检查你的高级脑钱包的各个环节，确保你的算法规则没有遗忘，脑口令没有错误，备份是完整可靠的。
- 谨慎操作： 在使用高级脑钱包时，要谨慎对待每一步操作，确保没有疏漏。
  - 安全环境测试： 多在离线状态下，进行高级脑钱包的使用测试，确保在实际操作时，不会出现问题。
- 风险意识： 时刻保持风险意识，不要轻易相信任何陌生信息，也不要点击不明链接。

11.3 安全是自我责任：没有人可以完全依赖

在比特币的世界里，安全是自己的责任，没有人可以帮你承担你的安全责任。

- 保护自己的资产： 你必须对自己的比特币资产负责，不要依赖于别人，或者寄希望于别人的安全措施。
  - 自主管理： 你必须自主管理你的私钥，并采取足够的安全措施。
- 自主管理： 自主管理你的高级脑钱包，不要将你的脑口令、规则和盐值告诉任何人，避免泄露风险。
  - 不依赖他人： 不要依赖于任何第三方机构，包括钱包服务商、交易所或者其他个人。
- 承担风险： 你需要明白，使用高级脑钱包需要承担一定的风险，并且愿意为此承担相应的责任。
  - 风险评估： 你需要认真评估自己设计的高级脑钱包算法规则的潜在风险，并做好相应的心理准备。

11.4 高级脑钱包工具：只是工具，安全取决于你

高级脑钱包本身只是一个工具，它的安全最终取决于你如何使用它：

- 工具不能解决所有问题： 高级脑钱包工具只能帮助你生成和管理私钥和地址，并不能保证你绝对安全，你需要结合安全理念来使用它，并做好相应的备份工作。

o 正确使用工具： 你需要正确理解和使用工具，避免错误操作导致私钥泄露。

- 安全依赖于人： 高级脑钱包的安全最终取决于你自己的意识和行为，你的安全习惯，以及你对风险的认知和预防。

我们对硬件钱包的批判不是抽象地说“设备不安全”，而是追问：使用者是否真正知道设备内部怎样生成秘密？随机数是否按设计调用？固件和供应链是否可信？秘密在运输、初始化、输入和显示时经过了哪些环节？只要这些环节需要依赖外部承诺，就存在使用者无法完全掌握的信任边界。高级脑希望把最关键的生成规则掌握在本人手中。

o 提高安全意识： 你要不断学习和实践，才能真正掌握安全的精髓。

11.5 高级脑钱包 vs 硬件钱包：优势对比

本书明确主张：高级脑是更值得信赖的个人私钥自主安全工程体系。它把秘密规则和信息材料交还给使用者掌握，减少对专用黑盒设备、厂商和供应链的依赖。硬件钱包的风险不只在算法，也可能来自随机数实现、固件、芯片、生产、运输和使用过程。高级脑并非没有自己的要求：F 必须真正保密，信息指针必须经过认真选择，工具和计算环境也必须可信。

- 硬件钱包的不足：

o 审查边界： 不同硬件钱包在硬件设计、固件、构建流程和审计透明度方面差异很大。有些项目开放了较多代码和设计资料，有些部分仍需要信任厂商。开源能帮助审查，但不能自动证明硬件、固件和供应链都没有问题。

o 额外依赖：硬件钱包需要使用者信任设备设计、固件、随机数路径、供应链和更新机制。厂商承诺不能代替独立检查。对重视自主掌握的人来说，这些外部依赖本身就是需要认真面对的工程风险。

o 实体暴露： 专用设备可能让旁人推测使用者持有数字资产，但这取决于设备外观、存放方式和使用环境。纸质备份、电脑和手机也可能暴露相关信息，隐私风险并非硬件钱包独有。

- 高级脑的特点：

o 工具可审查： 使用者可以选择开源工具、检查源代码，或使用独立实现交叉验证。但自己编译不等于自动安全，仍要核对依赖、构建环境、发布文件和最终输出。

o 自主掌握：高级脑让使用者自己设计并掌握 F，能够在不同的可信设备上重新生成私钥，不依赖原始设备、原厂服务器或第三方在线服务。达哥开源的高级脑工具是实践中的一种选择；工具是执行规则的帮手，不应成为唯一保存秘密或唯一能够生成结果的地方。

o 自主掌握： 高级脑让使用者能够自行设计密钥生成规则，但自主设计同时意味着使用者要承担规则正确性、长期维护和恢复责任。

- 适用场景： 硬件钱包并非只适用于某一种区块链。是否需要专用设备，应根据签名频率、资产规模、使用环境和个人操作能力判断。
- 隐私安排： 不携带专用硬件可以减少一种实体暴露，但高级脑的纸质说明、备份介质、计算设备和操作过程也需要保护。隐私来自整体安排，而不是某一种载体天然隐形。

- 面对软件攻击： 离线生成能够减少网络远程攻击的机会，但不能忽略恶意程序、被篡改的安装包、固件问题、剪贴板、屏幕、存储介质和人为操作风险。

11.6 现实案例：随机数失效与硬件植入——当保险箱在别处出了问题

想象你去锁匠那里配一把号称拥有天文数字种组合的钥匙。锁的数学原理很可靠，可机器却因为接线错误，反复使用少数几种齿形。你买到的锁看着复杂，却可能被人从有限的钥匙样本中试开。另一个故事更加离奇：锁本身十分坚固，但有人在你拿到锁之前，偷偷在查看备用钥匙的窗口装了一台小摄像机。锁没有被撬开，钥匙的秘密却已经泄露。2026 年发生的两类硬件钱包安全事件，与这两种故事颇为相似。

案例一：COLDCARD 随机数路径错误（2026 年 7 月披露）

Coinkite 于 2026 年 7 月 30 日发布 COLDCARD 安全公告，确认部分固件在生成种子时，原本预期使用的硬件真随机数路径未被正确调用。其后续技术说明指出，问题来自 2021 年引入的构建与链接集成错误，实际调用了 MicroPython 内的通用伪随机数实现 Yasmarang，并非硬件随机数生成器在运行时坏掉后才主动切换。部分受影响型号的种子安全强度可能仅约 40 位，另一些约 72 位，低于原定至少 128 位的目标。制造商确认攻击者曾离线重建弱种子对应的私钥并窃取资金；独立链上分析机构对损失规模提出了估算，但金额和归因应以各自披露日期为准。

这个案例的教训是：即便设计图纸上写着“高质量随机数发生器”，也必须验证交付到用户手中的固件，究竟有没有真正使用它。类似厨房里装了最好的净水器，却误把水管接到了另一条水路。

更值得注意的是，更新固件只能修复今后的生成过程，无法自动改变过去已经生成的弱种子。对于受影响用户，制造商建议核查种子生成来源和固件版本，并依照官方迁移指南创建新的安全种子、转移资金。制造商同时列出了独立骰子熵与强 BIP39 附加口令等具体例外或缓解条件，因此不能把所有 COLDCARD 设备一概认定为不安全。

案例二：Ledger 经销渠道的恶意硬件植入（2026 年 10 月披露）

2026 年 10 月，Ledger 披露部分通过东南亚经销渠道流转的真品设备曾被犯罪团伙拆开、增加隐藏电子组件并重新投放市场。调查显示，植入组件位于屏幕附近，能够在设备初始化、显示 24 词恢复短语时读取这些文字，并借助带有 eSIM 的蜂窝通信模块把内容发给攻击者。Ledger 表示其安全芯片、操作系统和公司服务器并未因此被攻破，将事件界定为离开厂商控制后的局部经销渠道攻击。

这里的关键不是“24 个单词的数学强度不够”，而是原本只应当由所有者看到的秘密，被额外硬件从显示环节复制了出去。好比银行金库的大门仍然牢固，运送保险柜的途中却有人在密码纸旁偷偷装了一个镜头。

从这两起事件理解高级脑的系统安全哲学

第一类事件说明，设备标称具备高质量随机数，不代表实际固件一定正确调用了随机数路径。高级脑采用事先确定的材料和 F，可以避免私钥生成阶段临时调用随机数发生器这一特定失效模式。第二类事件说明，秘密一旦进入被篡改的设备，就可能从输入、显示或计算环节泄露。高级脑要减少对专用设备的依赖，也必须认真保护运行工具的计算环境。

高级脑的主张很明确：个人私钥的生成规则应由本人掌握，能够脱离原始设备和第三方服务重新生成；不把安全完全寄托在厂商的黑盒承诺上。硬件钱包的随机数、固件和供应链案例，正说明工程环节可能成为攻击入口。高级脑要做的是用个人信息指针、秘密 F、SHA-256 和可复现的工具流程，建立一套自主的安全体系。

给读者的三个问题：① 钱包的秘密是如何产生的？② 从产生到备份，秘密会经过哪些硬件和软件环节？③ 一旦某个环节失效，怎样发现并重新建立安全的保管体系？把这些问题问清楚，比只看到“军工级”“256 位”等宣传词更有意义。

资料与事件时间线（截至 2026 年 11 月 1 日）

• Coinkite，《Coldcard Security Advisory》，2026-07-30（后续更新）：https://blog.coinkite.com/coldcard-mk3-seed-generation-warning/

• Coinkite，《Adding to the Public Record on Our Ongoing Investigation》，2026-08-04：https://blog.coinkite.com/adding-to-public-record/

• Coinkite，《COLDCARD Security Update》，2026-08-20：https://blog.coinkite.com/coldcard-security-update-5.6.1-1.5.1q/

• Ledger，《Ledger’s Response to the Hardware Implant Attack》，2026-10-15：https://support.ledger.com/de/article/Ledger-s-Response-to-the-Hardware-Implant-Attack

• CoinDesk，Ledger 硬件植入事件机制报道，2026-10-13：https://www.coindesk.com/tech/2026/10/13/ledger-says-spy-chip-inside-cryptobilis-ledger-devices-transmitted-wallet-keys-over-mobile-network

11.7 高级脑与多签钱包：精简、自主与冗余的取舍

除了硬件钱包，多签钱包也是一种常见的安全方案。多签钱包允许多个私钥共同管理同一笔比特币资产，例如三签二，即需要三把私钥中的任意两把才能动用资产， 这种方式看起来能提供更好的安全性，但是，我们仔细分析，可以发现它也存在着一些问题：

• 多签的冗余与管理成本：

o 理论上的冗余： 多签钱包的出发点是为了提供冗余，即使丢失一部分私钥，仍然可以通过其余私钥来管理资产。

o 实际恢复： 以 2-of-3 多签为例，三把独立密钥中任意两把都可以满足签名门槛。丢失其中一把，剩下两把仍可支配资金；但恢复时还需要掌握钱包描述符、派生路径、脚本类型等必要信息。多签并不是把两套助记词“合并成一把最终私钥”。

o 备份工作： 多签需要妥善保存多份密钥材料和恢复配置。它增加了记录与协调工作，但也提供了单一密钥丢失或单点被盗时的容错空间。管理是否困难，取决于备份设计和参与者能力。

o 适用边界： 多签不一定适合所有个人用户，但也不能称为虚假冗余。它的价值在于把控制权分散到多个密钥或参与方；代价是设置、备份、恢复和日常操作更复杂。

• 高级脑的“精简优势”：

o 核心在于规则： 高级脑钱包虽然属于单签管理，没有冗余机制，但是，我们在信息指针记忆法的帮助下，可以把算法规则，以及各种脑口令和盐值 都通过各种方便记忆的方式进行管理，使得需要记忆的元素量要少得多，并且也更加容易备份和管理。

o 精简的代价： 高级脑可以把多个材料和步骤组织成一套个人规则，减少需要直接记忆的字符串；但如果规则和关键材料没有可靠的备份与继承安排，精简也可能变成单点故障。

o 按需取舍： 高级脑适合重视自主规则和确定性复现、并愿意承担维护责任的使用者；多签适合需要分散控制权或多人共同管理的场景。两者不是简单的优劣关系。

• 多签钱包的真正使用场景： 多签钱包并非完全无用，它在特定场景下仍然非常重要。

o 多方共管资产： 当比特币资产需要由多方共同掌握时，多签钱包是理想的选择。例如，一个公司或团队的比特币资产，不应由某个人或少数人单独控制，而应由多方共同管理。

o 避免单点故障： 多签可以使得大家一起决定资产的使用权，就像一个保险箱上锁了多个锁，大家都需要同时打开每个锁才能打开宝箱。这有效避免了单点故障，防止了某个人或少数人滥用职权或者发生意外而导致资产丢失。

o 个人场景： 个人是否采用多签，应看资产规模、恢复能力、是否需要分散保管以及能否长期维护配置。高级脑单签更精简，但没有多签的多方门槛和密钥冗余。

11.8 小结：安全之路，永无止境，不同托管方式的安全取舍

高级脑主张把个人私钥安全建立在自己掌握的规则和完整工程上。它不是把私钥交给某台设备保管，而是让使用者掌握信息指针、F 和生成步骤，并能在可信设备上独立重新生成。我们认为，这种自主性比依赖不可见的设备内部过程更值得信赖。要让主张落地，仍须完成规则审查、工具核验、离线测试、备份和恢复演练。

上一章小测验答案：

1. 什么是 HD 钱包？它的核心是什么？

答：HD 钱包是一种使用种子生成无限私钥和地址的钱包，它的核心是使用一个种子（Seed）来生成所有私钥和地址。

2. 什么是派生路径？它有什么作用？

答：派生路径是 HD 钱包用来生成不同的私钥和地址的“路线图”，它可以让 HD 钱包生成无数个不同的私钥和地址。

3. 什么是多重地址？它有什么好处？

答：多重地址是 HD 钱包利用派生路径生成的多个不同地址。它可以方便管理、提高隐私。

4. HD 钱包和高级脑钱包在设计思路上有什么不同？

答：HD 钱包依赖种子自动派生，集中管理，而高级脑钱包则强调手动管理，隐私至上，独立生成，自定义规则。

5. 高级脑钱包的核心理念是什么？

答：高级脑强调使用者自主设计和掌握规则，按需管理地址，减少不必要的信息暴露，并对备份、恢复和继承负责。它不能单独解决量子计算对现有签名体系带来的风险。

6. 为什么我们要强调“一个地址只用一次”？

答：主要是减少地址复用、降低交易关联，并减少公钥在未花费阶段的长期暴露；但它不能消除花费交易广播后的公钥暴露窗口，也不能单独解决未来量子风险。

7. 在高级脑钱包中，你如何处理比特币转账中的找零？

答：在高级脑钱包中，你需要将找零地址设置为高级脑生成的另一个新的地址，而不是默认的旧地址。

8. 除了隐私性，“一个地址只用一次”能降低哪些风险，又不能解决哪些问题？

答：新地址可以减少地址复用，并在首次花费前降低公钥长期公开的机会，但不能彻底防御量子攻击。花费交易广播到内存池时，公钥会在相应交易数据中暴露；未来若出现足够快速且实用的量子攻击，广播至确认之间可能形成攻击窗口。因此，“一个地址只用一次”是隐私与风险管理措施，不是量子安全保证。

9. “一个地址只用一次” 如何保证你接收比特币时的地址安全？以及转账后原地址的安全性？

答：新地址可以减少地址复用和部分链上关联，但“未使用”不等于绝对安全，接收前仍需确保对应私钥与规则能够正确恢复。转账时，私钥进入热钱包会增加暴露风险；转账后应确认找零进入自己控制的新地址，并核实原 UTXO 已按预期花费。源地址不再使用可以减少后续风险，却不能撤销此前已经发生的泄露，也不能保证热钱包失陷时其他信息绝对安全。

本章小测验：

1. 在比特币世界中，有哪些潜在的风险？
2. 为了保护你的比特币资产，你需要养成哪些安全习惯？
3. 在比特币的世界里，安全是谁的责任？
4. 高级脑钱包工具能解决所有问题吗？
5. 高级脑钱包的安全最终依赖于什么？
6. 为什么在高级脑钱包中要强调安全环境的测试复现？
7. 高级脑钱包相比硬件钱包有哪些优势？
8. 高级脑与硬件钱包各自解决什么问题？
9. 使用专用设备时，应该怎样考虑实体隐私风险？
10. 如果你掌握了高级脑钱包，按照高级脑钱包的要求在安全环境下离线生成和管理私钥，那么黑客攻击等风险会如何？
11. 高级脑钱包相比多签钱包有哪些优势？

延伸阅读 | 高级脑的自主安全主张

硬件钱包把一部分安全责任交给专用设备、固件、随机数发生器和供应链；高级脑则把生成规则交还给使用者。我们主张高级脑是个人私钥安全更值得信赖的方向，因为使用者能够理解并掌握规则，也能在不同可信设备上重新生成。它的前提是 F 设计得当、信息指针保密、工具可验证、备份可恢复。自主不是一句口号，而是整套工程都能由本人掌握。

第十二章：比特币安全的未来



生活中的例子 | 未来的威胁未必按照今天的想象出现。就像修建一座桥，既要考虑今天的车辆，也要预留检查和维护的办法。长期保存比特币，同样需要关注技术变化、软件升级和迁移能力，而不是把某种方法当成永远无需检验的答案。

12.1 量子计算的威胁：未来的隐形敌人

在比特币的未来发展中，我们不得不关注一个潜在的威胁，那就是 量子计算。

- 量子计算机的强大： 量子计算机是一种使用量子力学原理进行计算的新型计算机，它拥有强大的计算能力，远超我们现在使用的传统计算机。
- 破解密码的威胁： 量子计算机的出现，可能会对我们目前使用的加密算法（包括比特币所使用的椭圆曲线加密算法）造成威胁，一旦被破解，公钥倒推私钥就成为可能。
- “量子计算风险”：未来若出现足以对椭圆曲线离散对数问题实施实用攻击的容错量子计算机，比特币现有签名体系可能面临风险。目前不能把研究进展等同于已经具备现实破解能力；风险评估还需考虑公钥暴露时长、交易确认窗口、协议迁移及资产恢复安排。
- 地址复用的风险： 如果你重复使用比特币地址，在交易发出的时候，你的公钥会被暴露在区块链上，一旦量子计算技术突破，你就有可能会面临被破解的风险。

12.2 技术发展带来的影响：挑战与机遇并存

虽然量子计算的出现给我们带来了新的安全挑战，但是技术的发展同样也为我们带来了新的机遇：

- 新技术的出现： 随着技术的发展，新的加密算法也会不断涌现，我们可能会找到能够抵抗量子计算机攻击的加密算法。
  - 持续学习： 我们需要不断学习和适应新的技术，才能应对新的挑战。
- 安全漏洞的发现： 任何系统都可能存在漏洞，我们需要及时发现并修复这些漏洞，才能确保系统的安全。
  - 及时更新： 我们需要及时更新我们的软件、工具和系统，以修复已知漏洞。
- 威胁力量的变化： 黑客的攻击手段也会不断升级，我们需要不断提高安全意识，才能更好地应对各种安全威胁。
  - 安全理念： 我们需要坚持正确的安全理念，才能在未来的竞争中立于不败之地。而正确使用高级脑就是一种将黑客攻击的可能性降到最低的一种方式。

12.3 高级脑钱包的注意事项：认识局限，不断进步

虽然高级脑钱包具有很多优势，但是我们也需要认识到它的一些局限性，并时刻保持警惕：

- 依赖人脑： 高级脑钱包的安全性，最终依赖于你的记忆力，如果你的记忆出现错误，或者你泄露了关键信息，那么你的资产仍然存在风险。
  - 正确使用： 你需要充分了解高级脑钱包的原理，并按照要求正确使用它。
- 不适用于所有场景： 高级脑钱包并不适合频繁交易的场景，因为它每次都需要重新生成私钥和地址，较为繁琐。
  - 灵活选择： 你需要根据自己的实际需求，灵活选择合适的钱包类型。
- 持续学习和改进： 比特币世界变化迅速，我们需要不断学习和改进，才能更好地应对未来的挑战。
  - 拥抱技术： 我们需要拥抱新技术，探索更安全、更便捷的财富管理方式。

12.4 小结：安全之路，永无止境，共同应对未来挑战

比特币的安全未来既充满挑战，也充满机遇。我们需要时刻保持警惕，不断学习和改进，才能更好地应对未来的挑战。

上一章小测验答案：

1. 在比特币世界中，有哪些潜在的风险？

答：在比特币世界中，存在着黑客攻击、设备损坏、信息泄露、甚至是认知偏差等多种潜在的风险。

2. 为了保护你的比特币资产，你需要养成哪些安全习惯？

答：为了保护你的比特币资产，你需要养成持续学习、定期复查、谨慎操作和保持风险意识等安全习惯。

3. 在比特币的世界里，安全是谁的责任？

答：在比特币的世界里，安全是自我责任，你需要对自己的比特币资产负责。

4. 高级脑钱包工具能解决所有问题吗？

答：高级脑钱包工具不能解决所有问题，它只是一个工具，真正的安全取决于你如何使用它。

5. 高级脑钱包的安全最终依赖于什么？

答：高级脑钱包的安全最终依赖于你自己的意识和行为，你的安全习惯，以及你对风险的认知和预防。

6. 为什么在高级脑钱包中要强调安全环境的测试复现？

答：为了确保你的算法规则的有效性，需要进行离线的安全环境测试，避免实际操作时出现问题。

7. 高级脑钱包相比硬件钱包有哪些优势？

答：高级脑的优势在于使用者自主设计并掌握 F，能够结合个人信息指针确定性地重新生成私钥，减少对专用硬件设备、厂商和供应链的依赖。

8. 高级脑与硬件钱包各自解决什么问题？

答：因为掌握了高级脑钱包，你就不再需要依赖任何硬件设备来管理你的比特币资产。

9. 使用专用设备时，应该怎样考虑实体隐私风险？

答：因为如果你把硬件钱包放在家里或者随身携带，一旦被其他人发现，就会暴露你持有比特币的信息，对于注重隐私的用户来说，这是不可接受的。

10. 如果你掌握了高级脑钱包，按照高级脑钱包的要求在安全环境下离线生成和管理私钥，那么黑客攻击等风险会如何？

答：离线生成可以大幅减少网络远程攻击机会，但不能把所有软件风险都视为零。还要核验工具来源、设备环境、输入输出、备份和恢复过程。高级脑的优势在于规则由本人掌握，能够独立复现。

11. 高级脑钱包相比多签钱包有哪些优势？

答：高级脑钱包虽然属于单签管理，没有冗余机制，但是具有精简的优势，并且在规则设计上更灵活。多签可以降低某些单点风险，但也增加备份、协调和恢复的复杂度；是否合适，要看资产管理场景。

本章小测验：

1. 什么是量子计算？它对当前密码学有什么威胁？
2. 在技术发展的过程中，有哪些机遇？
3. 高级脑钱包有哪些局限性？

4. 未来比特币安全的发展趋势是什么？

延伸阅读丨量子风险不能用“地址未花费”一概化解

不同脚本的公钥可见性存在差异，但未来量子威胁涉及签名体系、迁移窗口及协议演化，尚无法用一种现有地址习惯彻底解决。本书因此以动态风险管理为原则：关注公开安全研究、保持恢复能力、避免不必要的信息暴露，并保留未来迁移的灵活性。

第十三章：自由之钥，安全同行



生活中的例子 | 拥有一把钥匙令人自由，也带来责任。真正的自主控制不是“任何时候都不求助他人”，而是清楚自己依赖什么、保留哪些选择，以及在自己无法操作时有没有可靠的安排。这正是“人在币在，人走币随”值得继续讨论的地方。

13.1 回顾：我们走过的旅程

恭喜你，一路走到这里！

在这段旅程中，我们一起探索了比特币的奥秘，了解了钱包的本质，对比了不同钱包类型的优缺点，认识了高级脑钱包的独特之处，学习了设计高级脑钱包的安全基础，掌握了如何使用工具生成地址，并且明白了如何安全存储和备份私钥，以及如何继承你的比特币资产。

现在，我们来简单回顾一下我们学到的关键知识：

- 比特币：一种去中心化的数字货币，具有假名性、稀缺性和全球流通等特点。它不仅是一种支付工具，也可以作为价值储存和交易媒介。
- 私钥：控制比特币的唯一凭证，必须妥善保管。
- 钱包：管理私钥和地址的工具，本身不存储比特币。
- 高级脑：一种以个人主观价值为信息基础、以个人秘密规则 F 为核心、以 SHA-256 为最终散列基础，并强调独立重新生成的比特币个人私钥安全工程体系。

• 核心思想：每个人都有自己的刻骨铭心，也有别人未必理解的经历。高级脑把这些个人信息组织成信息指针，再由本人设计和掌握 F，完成确定性的私钥生成。

• 自主性：使用者不依赖原始设备、原厂服务器或第三方在线服务，也应能够在可信设备上重新生成私钥。达哥开源的哈希加盐工具可以帮助执行规则，但规则和秘密仍由使用者掌握。

• “一个地址只用一次”：为不同收款用途使用新地址，通常有助于减少链上关联，并可在未花费前避免公开该地址对应的公钥。但它不能彻底消除量子风险：当花费交易进入内存池时，相关脚本或见证数据会暴露公钥，直至交易确认期间仍存在潜在攻击窗口。

• 自主掌握：高级脑主张由使用者掌握私钥生成规则，减少对专用硬件和厂商的依赖；核心要求是能够独立生成、验证、备份和恢复。

13.2 高级脑的精髓：掌握核心，融会贯通

高级脑有两个不能分开的思想根基：未知 F 与主观价值。F 由本人设计、掌握，也可以通过信息指针来记忆；信息指针来自个人生命经验，多个来源可以组合。

• 规则由人设计：F 要适合本人，容易记忆、准确复现，同时不让外人轻易还原。它可以随时间更换，但更换前必须完成新规则的验证和迁移。

• 信息来自个人：每个人都有自己的故事和记忆。你的刻骨铭心，对别人可能毫无意义；别人的鲍鱼，对你也可能是砒霜。高级脑把这种主观价值落实为个人信息指针。

• 整体安排：初始脑口令、多个信息指针、F、散列步骤、工具、地址、备份和恢复都属于同一套工程。初始脑口令建议不少于 20 个字符，中间散列不建议降到低于 SHA-256 的强度，最终按 SHA-256 生成 256 位结果。

• 独立复现：规则必须能在不同可信设备上重新执行。工具可以更换，原始设备可以损坏，服务可以停止，但使用者仍应掌握重新生成的方法。

13.3 “人饼合一”的真谛：将财富融入生命

高级脑不只是一段生成私钥的程序。它把人的记忆、个人规则、信息组织和比特币控制权联系起来，这正是“人饼合一”这个名字想表达的思想。

• 财富与生命：“人”代表你的身体，你的生命，你的记忆，“饼”代表你的比特币。高级脑钱包将你的记忆和比特币紧密结合起来，让你的财富真正成为你生命的一部分。

o 心随意动： 一旦你掌握了高级脑钱包，你就真正掌握了你的财富，你可以在任何时候，任何地点，使用你的比特币。

• 减少专用设备依赖： 高级脑可以不依赖专用硬件钱包，但仍需使用可信的计算设备完成计算与签名，也需要妥善安排备份。

- o 不暴露身份： 即使你到处备份你的初始脑口令，因为它们仅仅是你的初始脑口令的一部分，不会泄露你的私钥，也不会暴露你拥有比特币的事实。
- o 掌握控制过程： 掌握规则和材料，能够独立复现私钥，是自主控制的一部分；实际控制还要求能够安全签名、管理 UTXO 并在必要时完成恢复。
- 个人主权与传承： 私钥由个人掌握，可以减少对托管机构的依赖；但如果只有本人知道恢复方法，身故或失能后也可能造成资产无法继承。个人主权与可传承性必须一并设计。
- o 人在时掌握，身后可传承：高级脑强调个人能够掌握并复现私钥生成过程。但比特币资产不会因为持有人记得私钥就自动完成继承；若希望家人在本人失能或身故后取得资产，必须预先安排必要材料、恢复步骤和合法交接方式。

13.4 展望未来：拥抱变化，探索无限可能

比特币的世界充满了无限的可能，也面临着各种挑战。但我们相信，随着技术的不断发展，比特币将会越来越成熟，越来越安全。

- 探索更安全的财富管理方式： 让我们一起探索更安全、更便捷的财富管理方式，让我们的资产真正由自己掌控，实现真正的“人饼合一”。
- o 积极学习： 不断学习新的知识和技术，提升自己的安全能力。
- o 勇于尝试： 勇于尝试新的工具和方法，探索更安全的管理方式。
- 拥抱技术变革： 让我们一起拥抱技术变革，拥抱比特币的未来，共同创造一个更加自由、更加安全的财富管理新时代。
- o 保持好奇心： 对新事物保持好奇心，积极探索和实践。
- o 不断改进： 不断改进自己的安全策略，适应不断变化的环境。

上一章小测验答案：

1. 什么是量子计算？它对当前密码学有什么威胁？

答：量子计算是一种使用量子力学原理进行计算的新型计算机，它拥有强大的计算能力，可能会对我们目前使用的加密算法造成威胁。

2. 在技术发展的过程中，有哪些机遇？

答：在技术发展的过程中，我们可能会找到能够抵抗量子计算机攻击的新型加密算法，并且可以通过及时更新和修复漏洞来增强比特币系统的安全性。

3. 高级脑钱包有哪些局限性？

答：高级脑钱包的局限性在于它依赖于人脑记忆，不适用于高频交易场景。

4. 未来比特币安全的发展趋势是什么？

答：未来的比特币安全既需要密码学和协议层面的进步，也需要更好的工程实践，包括密钥生成、设备审查、备份恢复、隐私管理和继承安排。

本章小测验：

1. 高级脑钱包的核心思想是什么？
2. 设计高级脑钱包时，最重要的是什么？
3. 在掌握高级脑钱包之后，还需要做什么？
4. 你如何理解高级脑钱包的“人饼合一”理念？
5. 高级脑钱包如何实现“人在币在，人走币随”？

延伸阅读丨自由与责任并行

“人在币在”强调个人独立控制，“人走币随”强调合理传承。前者涉及信息最小暴露与密钥主权，后者涉及可靠记录和继承执行。只追求完全不可见的秘密，可能反而伤害继承；只追求无条件方便，又可能扩大泄露面。高级脑的成熟，应该体现在对这种权衡的清醒认识。

第十四章：高级脑钱包实战教程



生活中的例子 | 把实战当成消防演习，而不是第一次就拿真正的房子试火。先用公开测试数据完整走一遍：生成、记录、验证、恢复，再在隔离环境里检查每一步是否可复现。只有演练成功，才能谈得上评估真实资产使用的风险。

14.1 实战

本章把前面的理念落实为操作流程。请先使用没有资产价值的公开测试材料，依次完成规则记录、工具运行、结果核对、备份和恢复。只有每一步都能独立复现，才算完成一次有效演练。以下步骤不构成对当前工具版本的安全认证。

14.2 准备工作

在开始实战之前，请务必做好以下准备工作，确保操作过程的安全：

- 离线环境： 这是最重要的一点！ 请务必断开你的电脑的网络连接（包括 Wi-Fi 和网线），确保你的电脑处于完全离线的状态。 建议使用一台专门用于生成私钥的离线电脑，不要安装任何其他软件，也不要连接任何网络。 如果条件不允许，可以使用 U 盘启动一个离线操作系统。
- 开源工具： 我们推荐使用达哥（@btcdage）的 Python 开源高级脑钱包工具，你可以在 Github 上找到：
  - 开源地址： https://github.com/btcdage2000/BrainWalletGenerator/

- 可执行文件下载地址：
  https://github.com/btcdage2000/BrainWalletGenerator/releases/tag/0.2.1
- 重要提示： 请务必从官方地址下载，并验证文件的完整性。

- 纸笔和备份设备： 准备记录规则版本、非秘密操作说明、测试向量和必要备份的介质。不要把所有秘密材料、关键口令和完整规则未经区分地放在同一处；应先设计泄露与丢失时的应对方式。

14.3 设计高级脑钱包算法

以下案例仅用于演示，实际操作中请勿完全照搬。

在开始使用工具生成地址之前，我们需要先设计好我们自己的高级脑钱包算法。 请务必记住，高级脑强调使用者亲自设计并掌握确定性规则，把材料、记忆、工具、备份和恢复安排成完整过程。 你需要灵活运用 “信息的指针记忆法”，并结合你的个人情况，设计出独一无二的算法。

下面给出一个不含真实秘密的结构示例。它只用于说明如何把确定性输入与确定性规则写清楚，不提供可直接用于资产的口令或参数：

1、输入材料 x：由使用者事先确定的短文本材料。此处不填写真实口令，也不调用随机数生成器。

2、关键材料 k：由使用者事先确定并独立保管的秘密文本（此处以 [关键材料] 代替）。

3、处理规则：明确规定字符编码、拼接顺序、分隔符和 SHA-256 迭代次数；示例中以 [固定参数] 代替具体值。

4、输入组合示意：x || [关键材料]。实际方案必须明确每个字段的边界与编码，避免拼接歧义。

[为避免复用公开示例秘密，此处不展示任何真实格式的口令、盐值或密钥材料。]

5、盐值（如方案使用）：以 [预先确定的盐值] 表示。盐值是否保密、是否固定及其用途，必须在规则说明中明确。

[为避免复用公开示例秘密，此处不展示任何真实格式的口令、盐值或密钥材料。]

6、地址序号：以明确的整数编码规则加入输入，例如固定宽度十进制或二进制编码；不能只写“连接在右侧”而不规定边界。

[为避免复用公开示例秘密，此处不展示任何真实格式的口令、盐值或密钥材料。]

14.4 使用工具生成地址

现在，我们可以使用达哥的工具来生成地址了。

1. 下载工具： 从 Github 下载达哥的 Python 开源工具，并将其保存到你的电脑上。或者，下载编译好的可执行文件。

2. 断开网络连接： 按照之前提到的方法，断开你的电脑的网络连接，确保电脑处于离线状态。

3. 运行工具：

o 如果你选择下载源码，你需要先安装 Python 3.6 或更高的版本。 然后在终端或者命令提示符中，输入 python brain_wallet_generator.py 命令来运行工具。

o 如果你下载的是可执行文件，则可以直接运行它，无需安装 Python 环境。

4. 拼接初始信息：

重要提示：达哥的开源工具负责执行哈希加盐等确定性处理。初始脑口令应不少于 20 个字符；使用者先按照自己的 F 完成信息指针取用、编码和组合，再把规则规定的输入交给工具。工具不替你设计或保存 F。

脑口令输入：按 F 规定的编码和组合方式，准备好完整输入后再填入“Passphrase / 脑口令”输入框。务必固定字符编码、分隔符和拼接顺序。

盐值输入：如果 F 规定使用独立盐值，按既定格式填入“Salt / 加盐”输入框，并记录它是否属于秘密材料。

5. 设置哈希次数： 在 “Hash Times / 哈希次数” 的下拉菜单中，选择你设定的哈希次数。

6. 生成密钥： 点击 “Generate Brain Wallet / 开始计算” 按钮，工具就会按照你设置的哈希套娃流程进行运算，生成私钥、公钥、P2PKH 地址，以及 Bech32 地址等信息。

7. 记录地址并保存恢复材料：将生成的 P2PKH 地址和 Bech32 地址记录下来，作为公开核对信息。地址不是私钥，不能用于恢复资产。请按第九章的方案保存完整生成规则、必要秘密材料和恢复说明，并确保备份经过实际恢复测试。

8. 清空信息： 点击 “Clear All / 清空所有” 按钮来清空所有信息，避免泄露。

14.5 验证地址的正确性

为了确保生成的地址是正确的，我们需要进行验证。

- 使用 Electrum 等钱包： 你可以使用 Electrum 等钱包软件，导入你的私钥，然后验证生成的地址是否正确。

o 注意事项： 请务必在离线状态下进行导入和验证操作，以避免私钥泄露。

• 独立恢复演练：使用另一台可信设备，按照已备份的规则和材料重新生成私钥，再核对地址是否与原记录完全一致。建议使用无真实资产的测试材料先完成演练。只有地址一致、签名测试通过且恢复过程可重复，才算完成验证。

14.6 安全存储和备份

安全存储和备份是保护你比特币资产的重要环节，务必认真对待：

- 关键脑口令： 如果选择只靠记忆保存，必须充分考虑遗忘、疾病、意外和继承风险。不要把“我绝不会忘记”当成唯一保障；是否设置受控的继承安排，应在设计阶段明确。
- 算法规则的备份： 保存准确、版本化的规则说明，明确哪些字段是秘密、哪些可以公开、哪些必须分开保存。规则说明本身应足以让未来的自己理解每一步，但不能无意中把所有秘密集中暴露。
- 其他材料和盐值的备份： 根据它们是否属于秘密，选择分开封存、加密保存或由可信来源重新取得。公开盐值与秘密输入的处理方式不同，不应一概而论。
- 定期复查： 定期检查你的备份，确保完整可靠。

14.7 演示截图

以下图片恢复自第一版纸本/PDF 中的历史操作界面，用于帮助读者认识当时工具的界面布局。它们不是对当前软件版本的实时截屏，按钮、字段和操作流程可能已经变化。

图 14-1 | 高级脑钱包生成工具的历史界面（示例输入、盐值、私钥、地址及二维码均已遮蔽）



图 14-2 | 通过改变序号生成不同地址的历史界面示意（所有可识别秘密材料均已遮蔽）

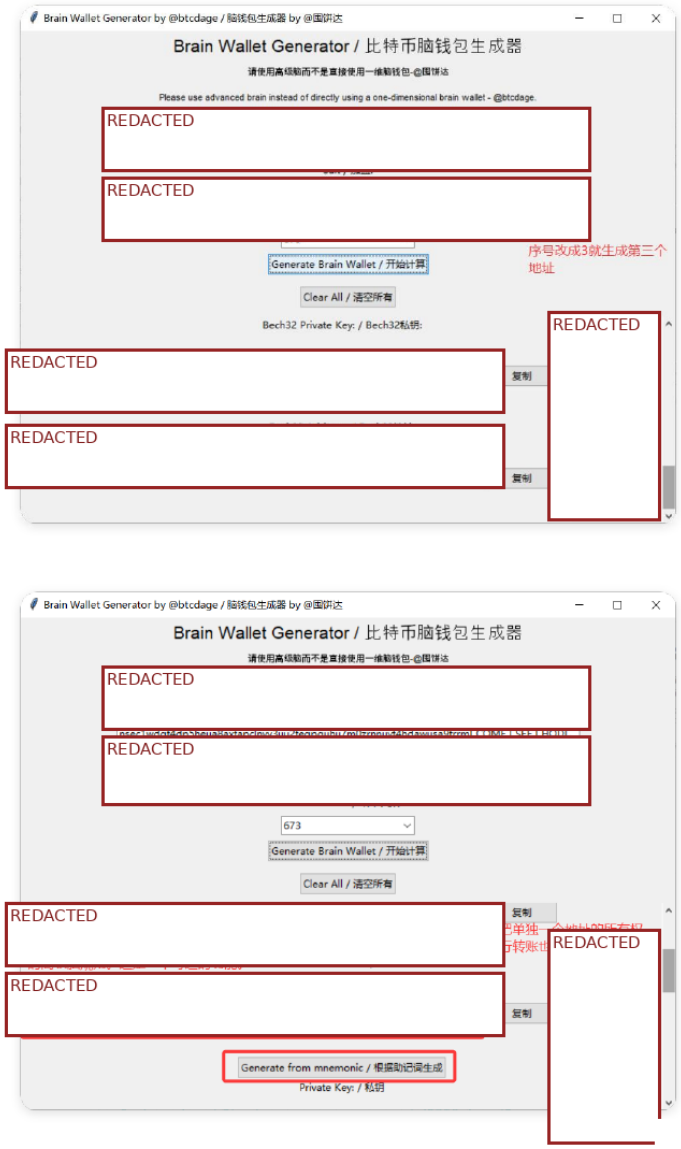


图 14-3 | Electrum 历史导入流程示意。界面版本可能不同；真实私钥只能在可信离线环境中处理。



安全提醒：第一版截图中出现过的脑口令、盐值、私钥、地址和二维码均属于公开示例材料，已在本版遮蔽。绝不可复制、扫描或复用这些旧示例。图示仅作历史界面说明，不构成对旧工具当前安全性、下载来源或生成结果的认证。

14.8 常见问题解答

- Q：如果我忘记了“关键脑口令”怎么办？

o A：如果关键脑口令没有任何备份，且本人确实无法回忆，通常就无法按原规则恢复。因此，设计时应提前决定采用记忆、受控备份或两者结合的方式，并定期进行恢复演练。不要把“我一定记得住”当作唯一保障。

- Q：我可以使用在线的工具生成地址吗？

o A：强烈不建议使用在线工具生成地址，因为存在被窃取私钥的风险。 请务必使用离线的工具进行操作。

- Q：我可以将我的算法规则告诉我的家人吗？

o A：可以向家人说明恢复流程，并根据继承安排提供必要材料。关键脑口令是否交给家人、何时交付、以何种方式保存，应在本人清醒且有能力安排时预先决定。不要一边要求家人恢复，一边又让所有必要秘密永远只存在于本人记忆中。

- Q：我可以使用纸钱包或者硬件钱包吗？

o A：高级脑的理念是无需依赖任何第三方硬件，软件。虽然纸钱包和硬件钱包也有一定的安全性，但是它们并不是必须的。 高级脑提供了一种不同的自托管思路；实际资产使用前仍需完成独立验证、恢复测试与风险比较。

14.9 小结

恭喜你，完成了高级脑钱包的实战教程！ 现在，你已经掌握了高级脑钱包的基本操作，以及如何保护你的比特币资产。 请务必多加练习，并不断学习和改进。 记住，安全之路，永无止境。

上一章小测验答案：

1. 高级脑钱包的核心思想是什么？

答：高级脑强调由使用者设计并掌握确定性生成规则，把材料、记忆、工具、备份、隐私和恢复安排成一套能够长期执行的个人工程。

2. 设计高级脑钱包时，最重要的是什么？

答：最重要的是把规则设计清楚：材料从哪里来、每一步如何执行、哪些内容需要保密、怎样验证结果，以及多年以后怎样恢复。独特性和保密性是其中的考虑因素。

3. 在掌握高级脑钱包之后，还需要做什么？

答：在掌握高级脑钱包之后，还需要不断学习和实践，才能真正掌握安全的精髓，并灵活运用，保护自己的比特币资产。

4. 你如何理解高级脑钱包的“人饼合一”理念？

答：高级脑钱包将你的记忆和比特币紧密结合起来，让你的财富真正成为你生命的一部分，并使你真正掌握自己的比特币资产。

5. 高级脑钱包如何实现“人在币在，人走币随”？

答：由于高级脑钱包的私钥的生成方法是存储在你的大脑中，你可以在地球的任何一个角落，都随脑携带你的所有比特币资产，这做到了“人在币在，人走币随”。

延伸阅读丨实战发布安全闸门（务必先读）

真实资产使用前的最低检查：使用隔离的测试环境；审查或独立验证工具；使用公开测试向量比对不同实现；固定编码和完整规则；核对地址类型、脚本与签名；在不接触真实资产的前提下完成完整恢复演练；再开展个人风险评估。没有通过上述测试的自定义方案，应保持在研究与教学范围。

结语：人饼合一，安全同行，未来由你定义

《人饼合一：高级脑完全手册》至此正式结束，感谢您一路相伴，共同探索了高级脑钱包的奥秘。 从对比特币的初步认识，到高级脑钱包的全面掌握，我们一起走过了一段意义非凡的旅程。

很多人谈到比特币安全，首先想到加密算法、随机数和密钥长度。这些知识重要，却不是全部。真正决定个人能否长期掌握比特币的，还有秘密从哪里来、规则由谁掌握、设备是否可信、工具是否可检查、备份能否恢复、家人能否在意外发生后接手。只知道加密学而不懂工程学，就容易把安全寄托在某个设备或厂商身上。高级脑要改变的，正是这种习惯。

高级脑的思想起源于 2020 年，成型于实践，并于 2025 年以本书的形式系统呈现。它从个人主观价值出发，鼓励每个人选择自己的信息指针，设计并掌握秘密规则 F，再以 SHA-256 完成确定性散列。特别感谢比特币布道者、拖拉机的深入交流，以及阿剑等小伙伴在讨论中的启发，也感谢各位群友和读者一路以来的支持。

读完本手册，希望你带走的不只是一个生成私钥的办法，更是一种安全观：自己的秘密，自己设计；自己的规则，自己掌握；自己的资产，自己负责。先用公开测试材料完成验证、备份和恢复演练，再决定是否用于真实资产。

比特币的旅程，才刚刚开始。 让我们携手同行，开启一个更加安全、更加自由的财富管理新时代！ 而这个未来，最终由你来定义！

——达哥（@BTCDAGE）

2026 年 11 月

https://btcdage2011.github.io

https://btcdage.rf.gd

Nostr：npub17ahz4xa3hvkvvhh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

附录 A｜安全术语速查

确定性：相同的完整输入和计算规则重复产生相同输出。它描述计算过程，不等于任何攻击者都能预测结果。

随机源依赖：在创建初始秘密的过程调用随机数生成器的需求；高级脑在本书研究模型下尝试避免这一依赖。

表示空间容量（RSC）：固定输出格式能够表示的理论状态数量的以 2 为底对数；用于描述输出格式，不代表高级脑追求的随机性或秘密程度。

香农熵：在明确概率分布下，随机变量的平均不确定性。它可用于分析随机源和 BIP39 初始材料；高级脑不以香农熵作为设计目标。

工程安全：把算法、秘密材料、个人规则、设备、工具、操作、备份、恢复和继承放在一起设计。高级脑强调未知 F、个人信息指针和独立重新生成；攻击者是否能够识别和还原完整规则，是评估现实攻击的重要问题。

秘密规则 F：由使用者自主设计、长期掌握的个人算法。F 可以利用信息指针构建，规定材料来源、编码、组合、迭代和其他确定性步骤；可以在完成验证与迁移后更换。

测试向量：使用完全公开、无资产价值的输入与预期输出，供不同实现比较、排错与长期复现。

附录 B｜真实资产使用前的十二项核验

1. 完整规则有版本号；2. UTF-8 和 Unicode 规范化已锁定；3. 每一步输入与输出格式已锁定；4. 迭代次数与边界已记录；5. 密钥有效性检查完成；6. 地址脚本类型明确；7. 独立实现交叉验证；8. 离线设备与工具来源核查；9. 全流程签名测试；10. 断开原设备后的恢复测试；11. 继承及失能情境评估；12. 文档和备份定期复审。

附录 C｜参考标准与阅读索引

Bitcoin 白皮书：Bitcoin: A Peer-to-Peer Electronic Cash System。

BIP32：Hierarchical Deterministic Wallets；BIP39：Mnemonic code for generating deterministic keys；BIP44：Multi-Account Hierarchy for Deterministic Wallets；BIP84：Derivation scheme for P2WPKH based accounts；BIP86：Key Derivation for Single Key P2TR Outputs。

SHA-256：NIST FIPS 180-4（Secure Hash Standard）。

本书未对工具版本、在线资源和未来共识变更提供实时认证；读者应以标准原文和独立验证结果为准。