人饼合一：高级脑完全手册

作者：达哥（X、微博同号：@BTCDAGE ）
https://btcdage2011.github.io/btcdage

nostr：npub17ahz4xa3hvkvvhh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

引言:打破认知藩篱，掌握财富真谛

你是否曾困惑于比特币私钥的复杂性，在琳琅满目的钱包选择中迷失方向？你是否曾担忧自己的资产安全，渴望找到一种既安全又便捷的管理方式？

《人饼合一：高级脑完全手册》的诞生，正是为了解答这些困惑。高级脑钱包是作者达哥自 2020 年起，在不断探索、实践和完善中逐渐成型的私钥管理方案。在与比特币布道者、拖拉机等高级脑先驱者的交流中，更是令人惊讶的发现，比特币早期实践者李笑来早已采用了类似技术。

然而，业界对“一维脑钱包”的安全风险一直存在担忧，这导致高级脑概念未能得到推广。随着越来越多朋友的相关疑问，达哥最终决定在 2025 年开年之际，编写这本《人饼合一：高级脑完全手册》。

本手册将带你打破传统钱包的认知藩篱，从比特币的本质出发，重新审视私钥管理。它将教你如何将记忆与私钥紧密结合，实现真正的 “人饼合一”，使财富与生命融为一体，真正做到“人在币在，人走币随”。

从比特币的基础知识入手，到高级脑钱包的设计、实战、安全理念，本手册将助你全面掌握这项前沿技术。 无论你是比特币新手还是资深玩家，都将从中获益匪浅。在此感谢 @比特币布道者 在本手册编纂过程中的技术探讨。

让我们一起探索高级脑钱包的奥秘，开启安全、自由的比特币未来！

目录

第一章：认识比特币——数字黄金，自由之钥

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、匿名性、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。
- **匿名性（Anonymity）：** 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是完全匿名的，但它确实比传统的金融系统更保护用户的隐私。
- **稀缺性（Scarcity）：** 比特币的总量被限制在 2100 万个，永远不会增加。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，比特币的总量被严格限制在 2100 万个，永远不会增加。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

比特币是一种革命性的数字货币，它具有去中心化、匿名性、稀缺性和全球流通等特点。它不仅仅是一种支付工具，更是一种价值储存、交易媒介和投资标的。它代表着未来财富自由和透明的一种趋势。

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？

第二章：比特币钱包——你的数字金库，私钥的守护者

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唯一钥匙。
- **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：** 每一个比特币地址都对应一个独一无二的私钥，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？

第三章：钱包的种类——百花齐放，各有所长

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，安全性更高，不容易被黑客攻击。
    - **缺点：** 使用起来相对麻烦一些，不如热钱包方便。

小结： 综合考虑安全因素，我们存储比特币一定要选择冷钱包。

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，无需备份，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——私钥的另一种表达方式

在了解高级脑钱包之前，我们需要先了解一下另一个常用的私钥生成和管理方案，那就是 BIP39 助记词。BIP39 是一种行业标准，它并非直接将私钥转换为助记词，而是通过一系列步骤，将一个随机生成的 种子（Seed）转换成一组易

于记忆的单词，通常是 12 个、18 个或者 24 个单词。然后，通过这个种子，可以生成对应的私钥。

- **BIP39 的原理：**
  1. **生成随机数（熵）：** 首先，BIP39 会生成一个高随机性的二进制数，也就是 熵（Entropy）。
  2. **生成种子：** 然后，通过哈希运算，由这个熵生成一个种子（Seed），这个种子本身也是一串很长的随机字符。
  3. **生成助记词：** 再将这个种子转换为一组易于记忆的单词，也就是助记词。
  4. **生成私钥：** 最后，使用这个种子，可以通过特定的算法，生成多个私钥和地址。
- **BIP39 助记词的本质：** 实质上，每一个助记词都代表着一个在由 2048 个单词组成的词汇表中的位置，相当于一个 0 到 2047 的数字，因此最少需要 12 个词，才能保证足够的熵，从而确保私钥的安全性。
- **BIP39 助记词的优势：**
  - **方便备份：** 你可以将助记词抄写在纸上，方便备份和恢复钱包。
  - **兼容性强：** 很多钱包都支持 BIP39 协议。
- **BIP39 助记词的不足：**
  - **记忆难度大：** 助记词虽然是单词，但是由于它的随机性，因此记忆方便程度并非那么强。12 个或者 18 个甚至 24 个相互毫无关系的单词，没有想象的那么容易记忆。这也是为什么我们需要高级脑钱包的原因。
  - **依赖第三方：** 你必须相信生成助记词的工具是安全的。
  - **仍然存在风险：** 如果助记词泄露或者丢失，你的比特币将会面临很大的风险。
  - **不够灵活：** BIP39 的助记词生成私钥的方式是固定的，不够灵活，也不可自定义。
  - **密码功能：** BIP39 还支持一个可选的 密码（passphrase） 功能。你可以设置一个额外的密码，这个密码会和助记词一起参与私钥的生成过程。这相当于给你的助记词又加了一层保护，提高了安全性。但是，如果忘记了密码，那么你的比特币也将会丢失。
  - **派生功能：** BIP39 支持 派生路径 (Derivation Path) 的概念。这意味着你可以使用同一组助记词，生成无数个不同的私钥和地址。这就如同用一把钥匙，打开不同的门，方便管理和隔离资产，但是也存在着一定的管理难度。
- **BIP39 助记词的安全性：** 很多人认为，只要保管好助记词，就绝对安全了，但是需要注意的是：
  - **BIP39 助记词的生成过程：** BIP39 的助记词的生成，本质上仍然依赖于随机数生成器，如果随机数生成器存在漏洞，那么助记词也存在风险。**此外，BIP39 助记词本身并不是真正的密钥，它只是密钥的另一种表现形式。它需要通过特定的算法，将助记词转化为种子，再从种子衍生出私钥。在这个过程中，种子和私钥的**

生成都依赖于特定的算法，如果算法存在漏洞，或者实现不安全，都可能导致安全风险。

- **BIP39 助记词的存储：** 如果将助记词存储在电子设备上，存在被黑客攻击的风险，如果将助记词存放在纸质上，则面临着丢失或者损毁的风险。
- **BIP39 助记词的记忆：** 很多人会选择记录助记词，但也有人选择直接记忆助记词，但是助记词通常是 12 个、18 个或者 24 个单词，如果记忆有误，也会导致资产丢失的风险。

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唯一钥匙，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：公钥和地址是可以公开的，用来接收比特币的。

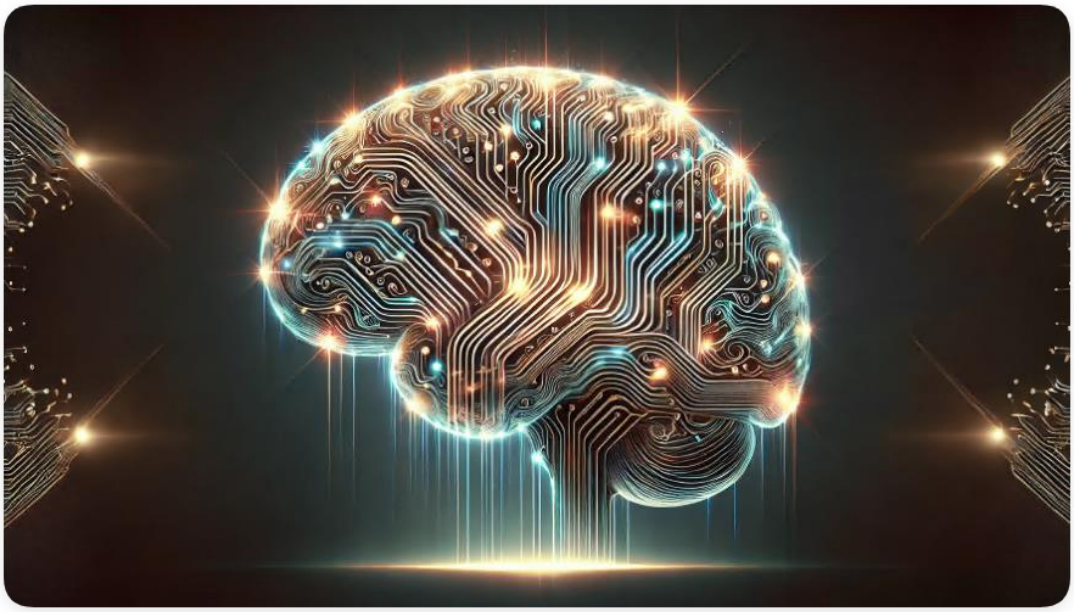
3. 私钥、公钥和地址是否依赖于比特币网络区块链？

   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？

第四章：初识脑钱包——把私钥藏在你的大脑里



4.1 脑钱包：私钥的“终极”存储方式

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。
- **无需备份：** 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”？

第五章：为什么我们需要高级脑钱包？

5.1 普通脑钱包的局限性：看似安全，实则危机四伏

上一章我们了解了“一维脑钱包”，它将私钥存储在大脑中，看似很安全、很便捷，但实际上，却存在着诸多风险。我们知道，“一维脑钱包”最大的问题在于它只依赖于一个简单的口令，而这个口令，很可能过于简单，容易被破解；也可能过于常见，容易与他人重复；或者，这个口令我们自己也可能遗忘。

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：隐藏规则，而非简单口令

高级脑钱包的核心思想在于：**隐藏规则，而不是提高初始熵**。

- **普通脑钱包：** 试图通过增加口令的复杂性（比如增加口令的长度，或者使用复杂的字符组合）来提高安全性。
- **高级脑钱包：** 更加注重隐藏生成私钥的规则，即使黑客知道你的口令，也不知道你生成私钥的规则，也很难破解你的私钥。

你可以把这个过程想象成一个魔术表演，魔术师不会告诉观众他是如何完成魔术的，他隐藏了魔术背后的秘密。高级脑钱包也一样，它隐藏了私钥生成的秘密，让黑客难以破解。

5.4 高级脑钱包的优势：多重保护，更加安全

相比于“一维脑钱包”，高级脑钱包具有以下明显的优势：

- **复杂规则：** 高级脑钱包不是直接将口令进行哈希运算就计算出私钥，而是会通过一套复杂的算法规则，将口令进行多次处理，再生成私钥。这就像在原有的基础上增加了多重加密，大大增加了破解的难度。
- **隐藏规则：** 只有你知道你使用的算法规则，即使别人知道你的口令，也很难还原出你的私钥。这就如同迷宫的地图，只有你知道如何走出迷宫，别人再怎么尝试也无法成功。
- **方便记忆：** 高级脑钱包不仅仅追求口令的复杂性，还注重口令的易记性。你不需要记住一串随机的字符串，而是可以记住一些有意义的词语或者故事，并使用一套简单的规则来生成私钥，并且保证足够的安全性。

5.5 高级脑钱包的必要性：避免“一维脑”的风险

我们之所以需要高级脑钱包，是因为“一维脑钱包” 存在着太多的风险， 而这些风险，通过高级脑钱包巧妙的设计都可以避免：

- **避免字典攻击：** 黑客可以通过收集常见的口令，来尝试破解一维脑钱包，而高级脑钱包因为有隐藏规则，黑客即使有字典库，也无法破解你的私钥。
- **避免口令重复：** 即使你使用的口令比较常见，但是通过一套独特的算法规则，也可以生成独一无二的私钥。
- **避免记忆负担：** 你不需要记住过于复杂的随机字符串，而是可以通过一个有意义的口令，和简单的规则来生成私钥，并达到高级别的安全性。

- **更加灵活和可自定义：** 你可以根据自己的喜好和习惯，设计一套属于自己的独特的高级脑钱包方案，而这是“一维脑钱包”和 BIP39 等方式都无法实现的。

5.6 小结：高级脑钱包——安全与便捷的完美结合

高级脑钱包是一种更加安全、更加灵活的私钥管理方案。它不仅继承了脑钱包的便捷性，还克服了“一维脑钱包”的安全隐患。它代表着未来私钥管理的一种趋势，值得我们深入学习和掌握。

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、无需备份。

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？

第六章：高级脑钱包的安全性基础——构建你的专属“加密堡垒”

6.1 为什么我们要了解安全性基础？——磨刀不误砍柴工

上一章我们了解了高级脑钱包的必要性和核心思想，知道它比普通的“一维脑钱包”更安全。但是，我们该如何设计一个真正安全的高级脑钱包呢？这就需要我们了解一些密码学的基本概念。

学习这些概念，就像学习盖房子的基本原理一样。只有了解了地基、承重墙、屋顶等结构，才能盖出坚固耐用的房子。同样，只有了解了哈希算法、抗碰撞性、散列性等安全性基础，才能设计出真正安全的高级脑钱包，从而保护好我们的比特币资产。

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：**
    - **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：** 无论输入信息多么长，生成的哈希值都是固定长度的。比如 SHA-256 算法，无论输入信息多长，都会生成一个 256 位的哈希值。
    - **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：
    - **文件校验：** 你可以校验下载的文件是否被篡改。
    - **密码存储：** 网站会将用户的密码进行哈希运算后存储，而不是直接存储明文密码，这样可以防止密码泄露。
    - **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 是一种非常常用的哈希算法，比特币就使用了 SHA-256 算法来生成地址。在设计高级脑钱包时，我们可以使用 SHA-256 或者其他的哈希算法。

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 算法具有非常好的抗碰撞性，可以认为在实际应用中，不可能出现碰撞的情况。

6.4 散列性：让“信息指纹”更随机

- **什么是散列性？** 散列性是指，即使输入信息的微小改变，生成的哈希值也会发生巨大的、随机的变化，这也就是哈希算法的雪崩效应。就像之前的比喻，假设外卖订单里少点了一份辣椒，外卖的订单号就从 87613 改变成了 19321，和原有订单号一点关系也没有。
- **散列性的重要性：** 散列性保证了即使你的口令只修改一个字符，生成的哈希值也会发生巨大变化，从而生成的私钥也会完全不同。这进一步提高了高级脑钱包的安全性。

6.5 熵的概念：衡量信息的“随机性”

- **什么是熵？** 在信息论中，熵用来衡量信息的不确定性或者随机性。熵越高，信息就越随机，越难以预测。**你可以把熵想象成一个“混乱程度”的指标。**
    - **高熵：** 就像你掷一个有 100 个面的骰子，或者在巨大的星空中随机选择一个星星，结果的可能性非常多，你几乎不可能预测出结果，因此它的 “混乱程度” 高，熵也高。

    - **低熵：** 就像你掷一枚硬币，只有正面和反面两种可能，或者在一个只有两种颜色的小盒子里随机取出一个球，结果比较容易预测，因此它的“混乱程度”低，熵也低。
    - 你还可以把熵想象成你家里的玩具，如果你的玩具摆放的非常整齐，一目了然，那么它们的熵就比较低，如果你的玩具乱糟糟的堆在一起，你很难一眼就看出都有什么，它们的熵就比较高。你掷骰子，结果越难以预测，熵就越高。你掷硬币，结果只有两种，熵就较低。
- **熵的重要性：** 在密码学中，熵越高，密码就越安全，越难以被破解。一个安全的私钥，需要有足够的熵。**就像一个高安全性的保险箱，需要有足够多的复杂密码组合，才能防止被轻易破解，而熵就是衡量密码复杂度的指标。**
- **初始种子的熵和最终私钥的熵：** 我们在这里要强调一个反常识但是非常重要的概念。
    - **不同输入的熵：** 比如，输入 ’a’ 的熵远小于输入 ’5JdVTqvNscmQiYeGGVmuFX6gb8EJVyuZ97yGodo7PrJ8nTfSVex’ 的熵。
    - **哈希值熵的一致性：** 但是由于 SHA-256 的散列性，sha256(’a’) 的哈希值 和 sha256(’5JdVTqvNscmQiYeGGVmuFX6gb8EJVyuZ97yGodo7PrJ8nTfSVex’) 的哈希值的熵，在计算上是相等的。也就是说，经过一次哈希算法后，无论输入的初始值的熵有多低，输出哈希值的熵都足够高了，可以看作是均匀分布的随机数。
    - **哈希套娃不增加最终种子的熵：** 无论做了多少步哈希套娃，其实没有增加最后一步脑口令的熵。只要不是用一串明文来做最后一次生成私钥时的脑口令，那么由于熵都是足够大的，最后一步的计算生成私钥的过程，防碰撞性是合格的。也就是说，在经过哈希运算后，初始种子的熵已经不再重要了，重要的是我们最终私钥的安全。

6.6 为什么需要多次哈希，以及强调规则的重要性？——防字典攻击的关键

既然一次哈希运算就可以使种子熵足够高，那么我们为什么还要进行多次哈希，或者加盐，以及强调规则的重要性？这是因为我们还需要防范 **字典破解攻击**。

- **哈希套娃的目的：** 多次的哈希运算（也就是哈希套娃），以及加盐，并非是为了增加最后种子的熵（第一次哈希就已经将熵最大化了），而是为了**防止字典破解攻击的风险**。
- **一维脑钱包的破解原理：** 一维脑钱包之所以会被破解，是因为它使用公开的哈希算法，并且口令大多比较简单，黑客只需要建立一个常用的口令字典库，然后对字典库中的口令进行哈希运算，对比计算结果，就可以破解你的私钥。

- **高级脑钱包的保护原理：** 而高级脑钱包的核心在于保护你使用的生成私钥的规则。规则包括：
  - 你使用哪些信息作为初始种子。
  - 你使用什么盐值。
  - 你进行多少次哈希运算。
  - 你使用了什么哈希算法。
  - **规则保密的重要性：** 只要你使用的规则足够复杂，并且规则没有泄露，那么黑客即使知道你的口令，也无法破解你的私钥。因为他们无法知道你的规则，也就无法构建字典库，无法进行有针对性的破解。这就像你的房门是隐形的，他们连门都不知道在哪，也就无从谈起如何撬锁。

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”

现在我们已经了解了哈希算法、抗碰撞性、散列性、熵等概念，我们就可以将这些知识应用于设计我们的高级脑钱包方案。

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：

- **什么是信息的指针记忆法？** 这是一种新的密码生成和记忆策略，它不需要你记住复杂的字符串，而是将复杂的字符串转换为你容易记住的指向性信息。就像一个藏宝图，你不需要记住宝藏的具体位置，只需要记住藏宝图上标记的地点，然后根据地点去寻找宝藏。
- **初始脑口令的选择：**
  - **避免使用过于常见的信息：** 尽量避免使用常见的诗歌、歌词、电影台词等作为初始口令，这些信息容易被黑客收集，从而增加破解风险。
  - **加入个人独特的信息：** 可以适当加入你个人独有的信息，比如初恋女友的名字和初次相遇的地点，孩子的小名和入学的学号，父母的名字和生日等。这些信息不但容易记忆，也让你的脑口令更具有独特性，降低被破解的风险。
    - **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：** 由于 BIP39 本身具有很高的随机性，它可以作为你的初始脑口令之一，从而大大提高口令的复杂度和独特性。
      - **记忆方法：** 你不需要直接记住助记词，而是记住 ″用 BIP39 生成的助记词″ 这个指向信息，就可以利用各种方式（纸质、电子设备、甚至网盘）对其进行备份，而不用担心泄露真正的私钥，因为这组助记词仅仅是初始脑口令的一部分。

        - **重要提示：** 千万不要直接使用这组助记词作为脑口令，而是应该将其作为高级脑钱包算法的一部分，并通过哈希、加盐等方式进行加密处理。
    - **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。
        - **安全性分析：** Nostr 公钥和私钥本身也是高随机性的字符串，可以有效增加你初始脑口令的熵，提高破解难度。
        - **记忆方法：** 你不需要直接记住 Nostr 公钥/私钥，而是记住 ″我的 Nostr 公钥″或者 “我的 Nostr 私钥” 这类指向信息，并进行备份。
        - **重要提示：** 千万不要直接使用 Nostr 公钥/私钥作为脑口令，而是应该将其作为高级脑钱包算法的一部分，并通过哈希、加盐等方式进行加密处理。
  - **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。
    - **安全性分析：** 比特币密钥对本身也是高随机性的字符串，可以有效增加你初始脑口令的熵，提高破解难度。
    - **记忆方法：** 你不需要直接记住这些信息，而是记住 ″我随机生成的比特币密钥对″这类指向信息，并将这些信息通过各种方式进行备份。
    - **重要提示：** 千万不要直接使用比特币密钥对作为脑口令，而是应该将其作为高级脑钱包算法的一部分，并通过哈希、加盐等方式进行加密处理。
  - **灵活组合：** 可以将多个“信息的指针”进行组合，以增加私钥的复杂度和安全性。
- **盐值的意义和功能：**
  - **什么是盐值？** 盐值是一段随机字符串，它会和你的脑口令一起参与哈希运算，从而生成一个更加复杂的哈希值。
  - **盐值的作用：**
    - **防止彩虹表攻击：** 彩虹表是一种预先计算好的哈希值和原始值的对应表。**传统的彩虹表攻击通过查表来逆向推导密码。但是，如果使用了盐值，即使两个用户使用了相同的脑口令，由于盐值不同，他们的哈希值也完全不同，这就使得预先计算好的彩虹表失效。** 也就是说，即使黑客得到了你的哈希值，如果不知道你的盐值，也无法通过彩虹表攻击破解你的密码。
    - **增加复杂度：** 即使两个用户使用了相同的脑口令，如果使用了不同的盐值，生成的私钥也会完全不同，进一步增加破解难度。
    - **保证规则的唯一性：** 盐值可以和你的规则相结合，提高你规则的独特性，保证你的私钥更加安全。
  - **盐值的选择建议：**

        - **易于记忆：** 盐值也需要容易记忆，你可以将其设置为一个对你有意义的日期、一个你喜欢的词语、或者一些你独特的数字符号等。
        - **保持独特性：** 盐值也应该具有独特性，避免使用过于常见的字符组合，并且不要记录在任何的物理介质上，避免泄露。
- **“关键脑口令”的概念：**
    - **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。
    - **“关键脑口令”的特点：**
        - **非常独特好记：** 它是用户刻骨铭心，绝对不可能忘记的一个脑口令。
        - **只记忆在脑子里：** 它不可以有任何物理空间的备份，只记忆在脑子里，保证它的绝对私密性。
        - **不受长度限制：** 因为有了 “信息的指针记忆法” 的存在，它的长短并不重要，重要的是它具有极高的独特性和不可替代性。
    - **“关键脑口令”的作用：**
        - **最后一道防线：** “关键脑口令” 是我们高级脑钱包的最后一道防线。即使其他脑口令和规则算法泄露，只要“关键脑口令”不泄露，就可以确保在短期内不会被破解。
        - **可继承性：** 在设计高级脑钱包时，规则算法可以多种多样，像独孤九剑一样无招胜有招（可以告知家人），几个脑口令和盐值也可以分散多地备份（可以不告诉家人，但锁在保险箱中）。但是“关键脑口令”一定要自己和家人牢牢记住，并且不记录在物理世界中。这种设计，可以在保证安全性的前提下，让你的家人在必要时通过备份的规则算法、其他脑口令和盐值，以及你和家人共同记忆的关键脑口令，来继承你的比特币资产。这被称为高级脑钱包的“可继承性”。
- **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： 可以选择一段你喜欢的诗歌、一句话、一首歌词、一个故事、一部电影、或者一个日期等，作为你的信息源。
2. 设置规则： 设置一套属于你自己的规则，例如：取这段信息的第几个字或者第几个词，并将这些字或者词进行哈希运算，从而生成私钥。
3. 灵活组合： 你可以将多个“信息的指针”进行组合，以增加私钥的复杂度和安全性。
4. 加入盐值： 在信息源的基础上，可以加入一些你自己独有的盐值，或者将不同的信息源组合起来使用。
5. 使用关键脑口令： 在最后一步哈希运算中，将关键脑口令作为最后一个变量参与计算，确保只有你能够完全掌控私钥。

- **强调规则的独特性和隐藏性：** 高级脑钱包的关键在于规则的独特性和隐藏性，你需要确保只有你知道这套规则，并且其他人无法轻易猜测出来。

6.8 小结：利用安全性基础，构建你的安全堡垒

学习了本章的知识，我们了解了哈希算法等密码学概念，以及如何运用“信息的指针记忆法”设计高级脑钱包。我们知道，高级脑钱包的核心在于隐藏规则，而不是提高初始熵。我们可以将各种信息源进行组合，利用哈希算法生成私钥，让我们的私钥存储在我们的头脑中，并且具有极高的安全性。同时，我们还需要加入个人信息，合理使用盐值，使用“关键脑口令”，以及使用 BIP39 助记词、Nostr 密钥和随机生成的比特币密钥对，使得我们的脑口令具有更好的独特性和安全性，并且要兼顾高级脑钱包的可继承性。

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？

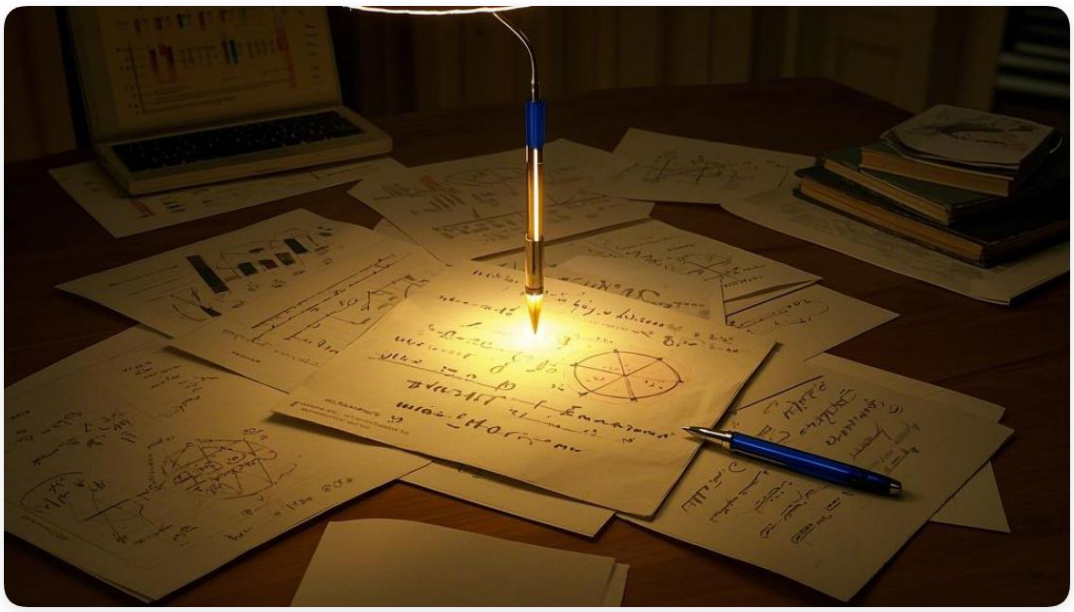
   答：高级脑钱包的核心思想是：隐藏规则，而不是提高初始熵。

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. **初始种子和哈希值的熵一样吗？** 为什么？
6. **哈希套娃的目的是什么？** 是为了增加种子熵吗？
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？

第七章：设计你的高级脑钱包算法——打造独一无二的“秘籍”



7.1 设计原则：灵活、安全、易记

经过前面章节的学习，我们了解了高级脑钱包的安全性基础和设计思想，也认识到高级脑钱包的核心在于隐藏规则。现在，我们终于可以开始设计属于我们自己的高级脑钱包算法了！

在设计算法时，我们需要遵循以下三个原则：

- **灵活：** 你的算法应该具有足够的灵活性，可以根据你的实际情况和喜好进行调整。就像搭积木一样，你可以使用不同的信息源、不同的规则和不同的盐值，灵活组合，创造出独一无二的算法。
- **安全：** 你的算法必须足够安全，能够有效地防止黑客的攻击。就像你家的门锁一样，必须足够坚固，才能保护你的财产安全。
- **易记：** 你的算法必须易于记忆，方便你随时使用，又不能过于简单，以免被黑客破解。就像你家的钥匙一样，必须方便携带，又不能轻易被复制。

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：**
    - **遵循指针记忆法：** 我们可以运用“信息的指针记忆法”，将复杂的字符串转换为你容易记住的指向性信息，比如你最喜欢的诗词、故事、电影台词，或者结合个人独特信息，如初恋的名字，孩子的生日等等。
    - **BIP39、Nostr、比特币密钥对：** 你也可以使用 BIP39 生成一组助记词，或使用 Nostr 的公钥/私钥，甚至是随机生成的比特币密钥对，并将它们作为初始脑口令的一部分。 这些信息具有高随机性，并且可以方便的进行备份。但请务必记住，这些信息只是你初始脑口令的一部分，并非直接用来生成私钥，你还需要使用自己的规则对它们进行处理。
2. **选择盐值：**
    - **增加复杂度：** 盐值可以增加哈希运算的复杂度，防止彩虹表攻击。
    - **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。
    - **易于记忆且独一无二：** 盐值需要易于记忆，也要具有独特性，你可以将其设置为一个对你有意义的日期、一个你喜欢的词语、或者一些你独特的数字符号，但切记不要记录在任何物理介质上，避免泄露。
3. **确定哈希次数：**
    - **哈希套娃：** 多次哈希运算能增加破解难度。
    - **个性化设置：** 哈希次数你可以设置一个固定的数字，也可以将它与你的脑口令或者生日等信息联系起来。
    - **哈希套娃的具体流程：** 在高级脑钱包中，我们推荐使用这样的哈希套娃流程：每次哈希时都将上一次的结果作为新的脑口令，并和盐值拼接，再进行下一次哈希运算。 这种方式能使每次哈希运算都更加复杂，并且具有更好的雪崩效应。
4. **确定哈希算法：**
    - **选择安全的算法：** 你可以选择 SHA-256 等安全的哈希算法。
    - **灵活性：** 你也可以选择多种哈希算法混合使用，增加复杂性。但建议最后一步仍使用 SHA-256。
5. **引入“关键脑口令”：**
    - **最后一道防线：** 在步骤中加入你的 “关键脑口令”，作为某一步哈希运算的输入，从而确保即使其他的脑口令或者算法步骤被泄露，你的私钥也无法被破解。
    - **只存在于大脑：** 关键脑口令只存在于你的大脑中，不记录在任何物理介质上。
6. **设置多重地址：**
    - **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。
    - **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。

- **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

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，高级脑钱包的核心在于隐藏规则，而不是提高初始熵。 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。

以下提供几个案例供您参考：

- **案例一：基于诗词和盐值**
  1. **初始脑口令：** “我第一次看到月亮是在我 5 岁生日那天”
  2. **盐值：** “明月几时有，把酒问青天。”
  3. **哈希次数：** 使用当前比特币区块高度的后四位数字。
  4. **哈希算法：** SHA-256
  5. **关键脑口令：** 你的初恋女友的名字。
  6. **规则：**
     - 将初始脑口令、序号、关键脑口令、盐值拼接在一起。
     - 哈希套娃：将拼接后的字符串，使用 SHA-256 进行哈希运算，第一次哈希结果将作为下一次哈希运算的脑口令，并和盐值拼接，直到哈希次数满足条件。
     - 根据需要，可以修改序号，生成不同的地址。
- **案例二：基于故事和个人信息**
  1. **初始脑口令：** “我小学三年级的时候，在学校后山发现了一块奇怪的石头。”
  2. **盐值：** 你母亲的生日。
  3. **哈希次数：** 你孩子入学学号的最后两位数字。
  4. **哈希算法：** SHA-256
  5. **关键脑口令：** 你最喜欢的一首歌曲的副歌部分。
  6. **规则：**
     - 将序号、故事和盐值拼接在一起。
     - 哈希套娃：将拼接后的字符串，使用 SHA-256 进行哈希运算，第一次哈希结果将作为下一次哈希运算的脑口令，并和盐值拼接，直到哈希次数满足条件，最后再使用关键脑口令进行最后一次哈希。
     - 根据需要，可以修改序号，生成不同的地址。
- **案例三：基于 BIP39、Nostr 和日期**
  1. **初始脑口令：** 使用 BIP39 生成的 12 个助记词，并记住 “我用 BIP39 生成了一组助记词” 这个指向信息。 使用 Nostr 的公钥，并记住 “我的 Nostr 公钥” 这个指向信息。
  2. **盐值：** 你结婚纪念日的日期。
  3. **哈希次数：** 将结婚纪念日的日、月、年分别取出个位数，进行加和。

4. **哈希算法：** SHA-256
5. **关键脑口令：** 你最喜欢的一部电影的名字。
6. **规则：**
    - 将序号、助记词，Nostr 公钥，和盐值，拼接在一起。
    - 哈希套娃：将拼接后的字符串，使用 SHA-256 进行哈希运算，第一次哈希结果将作为下一次哈希运算的脑口令，并和盐值拼接，直到哈希次数满足条件，最后再使用关键脑口令进行最后一次哈希。
    - 根据需要，可以修改序号，生成不同的地址。

请务必认真思考以上案例，并根据自己的情况进行修改和创新，设计出独一无二的算法。

7.4 小结：设计你的专属“加密秘籍”

通过本章的学习，我们了解了设计高级脑钱包算法的原则和步骤，并学习了如何运用“信息的指针记忆法”。 现在，你可以运用你的智慧，创造出独一无二的“加密秘籍”，从而安全地管理你的比特币资产。

更详细的案例和实战操作，请参考第十四章实战部分。

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，它保证了私钥的唯一性。

3. 什么是散列性？它有什么作用？

   答：散列性是指输入信息的微小改变，生成的哈希值也会发生巨大且随机的变化，它保证了私钥的随机性和抗碰撞性。

4. 什么是熵？它在密码学中有什么意义？

   答：熵是衡量信息不确定性或随机性的概念，在密码学中，熵越高，密码就越安全。

5. **初始种子和哈希值的熵一样吗？** 为什么？

答：**初始种子和哈希值的熵并不相同**。初始种子的熵可能很低，但是经过哈希算法后，其哈希值的熵已经足够高，可以看作是均匀分布的随机数。

6. **哈希套娃的目的是什么？** 是为了增加种子熵吗？

   答：哈希套娃的目的不是为了增加种子熵，而是为了防止字典破解攻击。

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”可以降低记忆难度，增加信息采样的宽度，利用各种信息源组合。

8. 什么是“关键脑口令”？它有什么特点和作用？

   答：“关键脑口令”是一个用户刻骨铭心、绝对不可能忘记的脑口令，只记忆在脑子里，不记录在任何物理空间中。它是高级脑钱包的最后一道防线，并且在家族继承的时候也发挥着重要的作用。

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？

   答：可以使用 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，并在后续的哈希运算中进一步处理，提高脑口令的随机性和独特性。

10. 高级脑钱包的核心是什么？

    答：高级脑钱包的核心是隐藏规则，而不是提高初始熵。

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？

第八章：使用工具生成地址——安全验证你的“加密秘籍”

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/v0.1.0

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。
   - **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/v0.1.0
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：**
    - **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。
    - **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：达哥的工具只负责哈希加盐套娃操作。因此，你需要将初始脑口令、盐值、序号、“关键脑口令” 等所有需要拼接的信息，按照你设计的规则进行拼接，然后将拼接后的字符串，填入 “Passphrase / 脑口令” 的输入框中。

- **脑口令输入：** 你需要将你的初始脑口令、盐值，你计算出的序号、甚至最后一步的 “关键脑口令” 等所有需要拼接的信息，按照你设计的规则进行拼接，然后将拼接后的字符串，填入 “Passphrase / 脑口令” 的输入框中。
- * **盐值输入：** 如果你的算法中使用了盐值，你需要将你选择的盐值，填入 “Salt / 加盐” 的输入框中。

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. **备份地址：** 将生成的 P2PKH 地址和 Bech32 地址分别备份下来，你可以把它们抄写在纸上，或者复制到 U 盘里。请务必确认你复制的地址和工具中显示的一致。
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。
    - **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：初始脑口令的选择应该避免使用过于常见的信息，并尽量加入个人独特信息，或者使用 BIP39 助记词，Nostr 密钥和随机生成的比特币密钥对等具有高熵的信息作为一部分。

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，并在后续的哈希运算中进一步处理，提高脑口令的随机性和独特性。

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？**

第九章：安全存储与备份——你的“加密秘籍”的守护之道

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：只记在脑中，不落于纸笔

在高级脑钱包中，“关键脑口令” 扮演着非常特殊的角色：

- **最后一道防线：** 它是我们高级脑钱包的最后一道防线，即使其他信息泄露，只要它不失，就能保证你的比特币资产安全。
- **独一无二：** 它只存在于你的大脑中，不应该记录在任何物理介质上。
- **刻骨铭心：** 它应该是你刻骨铭心，绝对不会忘记的信息。

因此，“关键脑口令”的存储策略和其他信息不同：

- **存储方式：** 它只能存在于你的大脑中，不能记录在任何纸张、电子设备或者其他任何形式的物理介质上。
- **记忆方法：** 你可以运用 “信息的指针记忆法”，将 “关键脑口令” 和你生命中一段特殊的经历联系起来，保证刻骨铭心，难以忘怀。
- **传递方法：** 可以口头传递给最信任的家人，确保他们了解 “关键脑口令” 的含义和重要性。

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？

第十章：HD 钱包、派生路径、多重地址

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：** 使用多重地址可以增加交易的匿名性，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 高级脑钱包的理念：手动管理，隐私至上，防御量子霸权，保障收币安全

高级脑钱包的核心理念是 **手动管理，隐私至上，防御量子霸权，以及保障收币安全**，并坚持以下原则：

- **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。
        - **防御量子霸权：** 更加重要的是，在中本聪的设计中，只要你发起一笔比特币转账，你的公钥就会暴露在区块链上。一旦暴露，你就面临着未来量子计算机的威胁。因此，为了安全起见，**每次转账都只使用新生成的地址**，可以防止你的比特币暴露在量子霸权的威胁之下。
        - **保障收币安全：** 此外，“一个地址只用一次” 还能保证你在 **存储比特币时的地址安全**，因为你的地址在没有被使用之前，是绝对安全的，不需要生成对应的私钥，也不需要导入到任何钱包里。
- **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。
- **避免集中管理：** 我们不倾向于使用 BIP39 等工具生成的助记词，并使用这些助记词派生出所有的地址，而是推荐你使用高级脑钱包，手动管理和生成不同的地址，让地址之间没有必然的关联，并且也更加安全。
- **转账后的源地址安全：** 由于我们遵循了“一个地址只用一次”的原则，因此当你需要转账时，你可以将该地址对应的私钥临时导入到热钱包，在转账完成后，将找零地址设定为高级脑生成的另一个未暴露公钥的地址， 这样，即使你把源地址对应的私钥公开，或者热钱包被黑客攻破，也不会对你的资产造成威胁，因为源地址已经被废弃不再使用。

10.6 小结：高级脑钱包的独特性

本章我们了解了 HD 钱包、派生路径和多重地址的概念，并对比了它们与高级脑钱包在设计理念上的差异。我们知道，高级脑钱包不是一个简单的 “钥匙串”，而是一个更加灵活和安全的私钥管理方案，它更加注重手动管理，隐私至上，防御量子霸权，并保障收币安全。

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，**为什么“一个地址只用一次”还能防御量子霸权的威胁？**
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？**

第十一章：高级脑安全理念

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。
    - **重要提示： 但是，如果你掌握了高级脑钱包的精髓，并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，在软件系统层面是可以忽略不计的。这正是高级脑钱包的优势所在，它不畏惧软件系统层面的漏洞。**
- **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。
    - **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。
    - **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

在比特币的安全存储方面，除了高级脑钱包，硬件钱包也是一个常见的选择。但是，我们认真对比之下，可以发现，高级脑钱包在安全性，独立性，灵活性和隐私性上，相比硬件钱包具有更大的优势。

- **硬件钱包的不足：**
  - **无法验证开源：** 硬件钱包依赖于硬件厂商，它的硬件设计和软件代码往往不能完全验证开源，这就存在着一个信任风险。你不知道它产生的随机种子是不是真随机，你也不知道它的固件是否存在后门。 硬件钱包就像一个黑盒子，你无法完全了解其内部运作机制，即使它宣称开源，你也不会使用源设计图来自己制作硬件。
  - **增加信任成本：** 硬件钱包是 BIP39 出现之后才发明上市的，它在比特币的使用中完全没有必要性，只是一个额外的节点。多一个节点就多一个需要信任的对象，这并不符合奥卡姆剃刀原则。
  - **暴露比特币持有信息：** 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。硬件钱包的存在本身，就暴露了你可能拥有比特币的事实，这容易引起不法分子的注意。
- **高级脑钱包的优势：**
  - **可以验证开源：** 你可以选择各种开源的脑钱包工具的源码进行编译后运行，你也可以自己编写工具，或者在别人的源码上做修改。你可以完全控制私钥的生成流程。
  - **无需额外信任：** 我们使用高级脑钱包，不直接使用 BIP39 来管理私钥。即使使用 BIP39 助记词作为初始脑口令之一，也可以用各种软件钱包来生成，无需花钱购买硬件钱包。由于只是作为初始脑口令之一，所以即使使用热钱包也完全没有问题。
  - **完全掌控：** 掌握了高级脑钱包，硬件钱包完全没有存在的必要。你不再需要依赖任何厂商，可以完全掌控你的比特币资产。
  - **针对其他区块链的硬件钱包：** 硬件钱包厂商存在的意义只能给以太坊等图灵完备的需要地址复用经常授权的其他加密区块链使用。而“比特币不需要硬件钱包”。
  - **更高的隐私性：** 高级脑钱包的所有信息都只存在你的大脑中，不依赖任何的硬件设备，可以最大程度地保护你的隐私，不会暴露你持有比特币的事实。
- **应对黑客攻击： 只要你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，在软件系统层面是可以忽略不计的。这正是高级脑钱包的优势所在，它不畏惧软件系统层面的漏洞。**

11.6 高级脑钱包 vs 多签钱包：精简大于冗余

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“虚假冗余”：**
  - **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。
  - **实际上的不足：** 例如，如果使用三套 BIP39 助记词来生成多签钱包的三个私钥，那么即使你丢失了其中任意一套助记词，只要保留了另外两套，仍然可以生成最终私钥。
  - **助记词保存的难度：** 但是请注意，即使你采用最简单的 12 个助记词的方案，三套助记词也已经是 36 个助记词。无论如何你只要丢失任意大于 12 个助记词，比如丢失了 13 个助记词。则两套助记词就不完整了，多签也就无法工作。也就是说，多签情况下，你需要保存的助记词变成了至少 24 个，甚至更多，这大大提高了记忆和保存的难度。
  - **多签不是更好的选择：** 多签看起来提供了冗余，然而这种冗余是虚假的，它只是以提高了记忆和保存的难度为代价，是一种表面上的安全，而不是更可靠的安全方案。
- **高级脑的“精简优势”：**
  - **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。
  - **化繁为简：** 高级脑钱包的优势在于它提供了一种更为精简的安全方案。相比于多签钱包需要管理大量助记词，我们只需要保护好我们设计的独一无二的算法规则和关键脑口令，就可以达到更高的安全级别。
  - **精简大于冗余：** 与其使用看似安全，实际增加了管理负担的虚假冗余，不如选择更精简，更安全的高级脑钱包。
- **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。**
  - **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。
  - **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。
  - **并非个人首选： 对于个人资产而言，高级脑钱包的单签方案通常更加合理可靠。** 多签增加了复杂性，但并未带来实际的安全提升。它只是更适合需要多方共同管理和决策的场景。

11.7 小结：安全之路，永无止境，比特币不需要硬件钱包，高级脑胜于多签

安全之路，永无止境。高级脑钱包是一个强大的工具，但是它的安全性最终取决于你。我们要始终保持警惕，不断学习和改进，才能真正保护好自己的比特币资产。 并且记住，**比特币不需要硬件钱包**，高级脑才是你更明智的选择，它

拥有更强的隐私性和安全性，而且相比多签更精简高效，同时能保证你的安全。

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：高级脑钱包的核心理念是手动管理，隐私至上，防御量子霸权，以及保障收币安全。
6. **为什么我们要强调“一个地址只用一次”？**
   答：为了保护隐私，避免将你的所有比特币都关联到同一个地址上，更重要的是为了应对未来的量子霸权威胁。
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，为什么“一个地址只用一次”还能防御量子霸权的威胁？**
   答：因为在中本聪的设计中，只要你发起一笔比特币转账，你的公钥就会暴露在区块链上，一旦暴露，你就面临着未来量子计算机的威胁，所以“一个地址只用一次” 可以防止你的比特币暴露在量子霸权的威胁之下。
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：“一个地址只用一次” 能保证你在存储比特币时的地址安全，因为你的地址在没有被使用之前，是绝对安全的，不需要生成对应的私钥，也不需要导入到任何钱包里。当你需要转账时，你可以将该地址对应的私钥临时导入到热钱包，在转账完成后，将找零地址设定为高级脑生成的另一个未暴露公钥的地址， 这样，即使你把源地址对应的私钥公开，或者热钱包被黑客攻破，也不会对你的资产造成威胁，因为源地址已经被废弃不再使用。

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. **为什么说“比特币不需要硬件钱包”？**
9. **为什么说硬件钱包容易暴露你持有比特币的信息？**
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？**

第十二章：比特币安全的未来

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。
- **“量子霸权”：** 量子计算的快速发展，使得“量子霸权”成为现实。一旦量子计算机可以破解目前常用的加密算法，我们就可能面临私钥被破解，资产被盗的风险。
- **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：高级脑钱包相比硬件钱包，具有更高的安全性、独立性、灵活性和隐私性，并且不需要信任任何硬件厂商。
8. **为什么说“比特币不需要硬件钱包”？**
   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. **为什么说硬件钱包容易暴露你持有比特币的信息？**
   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： 如果你掌握了高级脑钱包的精髓，并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，在软件系统层面是可以忽略不计的。
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，并且也更为灵活。 多签钱包虽然有冗余，但是由于需要保存大量的助记词，反而增加了管理难度，这种冗余是虚假的。

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？

第十三章：自由之钥，安全同行

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：** 一种革命性的数字货币，具有去中心化、匿名性、稀缺性和全球流通等特点。它不仅是一种支付工具，更是一种价值储存和投资的标的。
- **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。
- **高级脑钱包：** 一种将私钥存储在大脑中的特殊钱包，它使用复杂的算法规则和 “信息的指针记忆法”，确保私钥的安全性和易记性。
- **核心思想：** 高级脑钱包的核心思想是 **隐藏规则，而不是提高初始熵，并且手动生成地址，隐私至上，防御量子霸权，以及保障收币安全**。
- **优势：** 相比其他类型的钱包，高级脑钱包具有更高的安全性、灵活性、独立性和隐私性。它能有效防御黑客攻击，不需要依赖于任何第三方机构，并且方便记忆，易于管理。

- **“一个地址只用一次”：** 每次接收和发送比特币时都使用一个新的地址，最大程度保护你的隐私，并能防御未来量子霸权可能造成的威胁。
- **比特币不需要硬件钱包：** 掌握了高级脑钱包，硬件钱包完全没有存在的必要。

13.2 高级脑的精髓：掌握核心，融会贯通

高级脑钱包的精髓在于：

- **规则至上：** 高级脑钱包的安全取决于你设计的规则，而不是你的初始口令本身。因此，你要认真设计你的规则，并确保它具有独特性和隐藏性。
- **灵活应用：** 高级脑钱包具有高度的灵活性，你可以根据自己的需求和喜好，定制各种不同的算法规则。
- **终身学习：** 安全是一个动态的过程，你需要不断学习和更新知识，才能适应不断变化的比特币世界。
- **实践出真知：** 只有通过不断的实践，你才能真正掌握高级脑钱包的精髓，并灵活运用，保护自己的比特币资产。

13.3 “人饼合一”的真谛：将财富融入生命

高级脑钱包不仅仅是一种技术，更是一种理念，它实现了真正的“人饼合一”。

- **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。
    - **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。
- **无需硬件设备：** 你不再需要依赖硬件钱包，也不需要使用铁板刻下助记词，因为这些物理设备都有可能泄露你拥有比特币的事实，从而带来安全风险。
    - **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。
    - **完全控制：** 只要你掌握了高级脑钱包， 你就完全掌控了你的比特币。
- **真正意义的“私有化”：** 你会发现，高级脑钱包让我们第一次真正实现了财富的私有化。这就像你的思想一样，只要你的记忆不丢失，你的财富就会一直伴随着你。你可以做到真正的 “人在币在，人走币随”。
    - **生不带来，死能带走：** 高级脑钱包让比特币成为了一种真正“生不带来，死能带走” 的私人财富，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。

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”。
    - **积极学习：** 不断学习新的知识和技术，提升自己的安全能力。
    - **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。
    - **保持好奇心：** 对新事物保持好奇心，积极探索和实践。
    - **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：未来的比特币安全将会朝着更加注重隐私、更加灵活和个性化，并且更注重防御量子霸权的方向发展。

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”？**

第十四章：高级脑钱包实战教程

14.1 实战

欢迎来到高级脑钱包的实战环节！ 在之前的章节中，我们深入探讨了高级脑钱包的理论知识、设计原则以及安全性基础。 现在，我们将把这些知识转化为实际操作，一步步教你如何使用高级脑钱包，安全地管理你的比特币资产。 本附录旨在提供一个清晰、详细的实战指南，帮助你从理论走向实践。 请务必仔细阅读本附录，并在离线安全环境下进行操作。

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/v0.1.0
    - **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：** 准备纸、笔，以及 U 盘、移动硬盘等备份设备，用于记录你的算法规则、脑口令、盐值和生成的地址。

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，高级脑钱包的核心在于隐藏规则，而不是提高初始熵。 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。

比如我们这次测试使用如下算法规则（所有的示例仅供参考）：

1、使用任意 nostr 客户端生成 10 个 nostr 私钥，并保存。这里我直接使用代码生成。

```python
from pynostr.key import PrivateKey

def generate_nostr_key_pairs(num_pairs):
    key_pairs = []
    for _ in range(num_pairs):
        private_key = PrivateKey()
        public_key = private_key.public_key
        key_pairs.append((private_key.bech32(), public_key.bech32()))
    return key_pairs

num_pairs = 10
key_pairs = generate_nostr_key_pairs(num_pairs)
for i, (private_key, public_key) in enumerate(key_pairs):
    print(f"Pair {i+1}:")
    print(f"Private key: {private_key}")
    print(f"Public key: {public_key}")
    print()
```

2、关键脑口令设置为达哥的签名：“I COME,I SEE,I HODL.”
3、哈希次数 673 次（BTC->673）
4、初始脑口令 是第一个 nostr 私钥+关键脑口令：

nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrmI COME,I SEE,I HODL.

5、盐值是最后一个 nostr 私钥+关键脑口令

nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3saI COME,I SEE,I HODL.

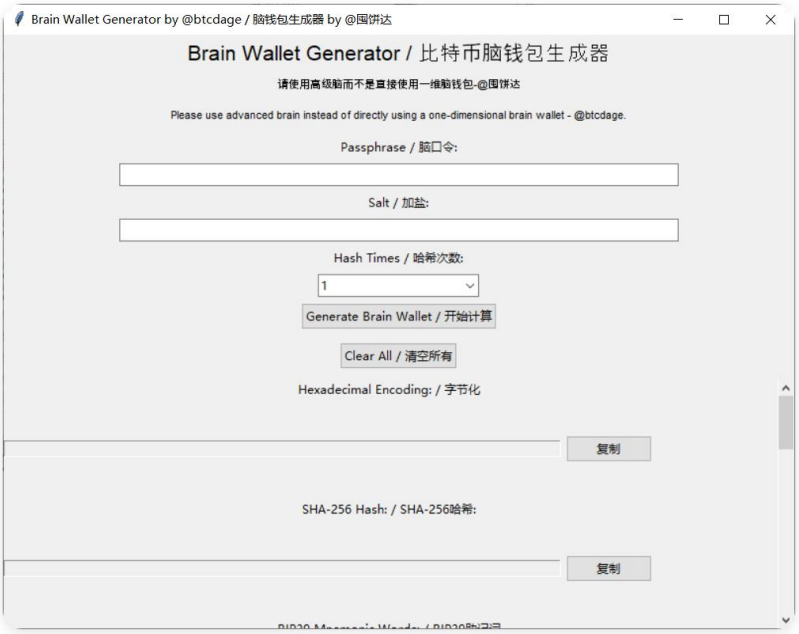
6、序号连接在盐值的右侧，比如第一个地址生成方式：

nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3saI COME,I SEE,I HODL.1

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：**
    - 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。
    - 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：** 达哥的工具只负责哈希加盐套娃操作。因此，你需要将初始脑口令、盐值、序号、“关键脑口令” 等所有需要拼接的信息，按照你设计的规则进行拼接，然后将拼接后的字符串，填入 “Passphrase / 脑口令” 的输入框中。
    - **脑口令输入：** 将你的初始脑口令、盐值，你计算出的序号、甚至最后一步的 “关键脑口令” 等所有需要拼接的信息，按照你设计的规则进行拼接，然后将拼接后的字符串，填入 “Passphrase / 脑口令” 的输入框中。
    - **盐值输入：** 如果你的算法中使用了盐值，你需要将你选择的盐值，填入 “Salt / 加盐” 的输入框中。
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. **备份地址：** 将生成的 P2PKH 地址和 Bech32 地址分别备份下来，你可以把它们抄写在纸上，或者复制到 U 盘里。请务必确认你复制的地址和工具中显示的一致。
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。
    - **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。

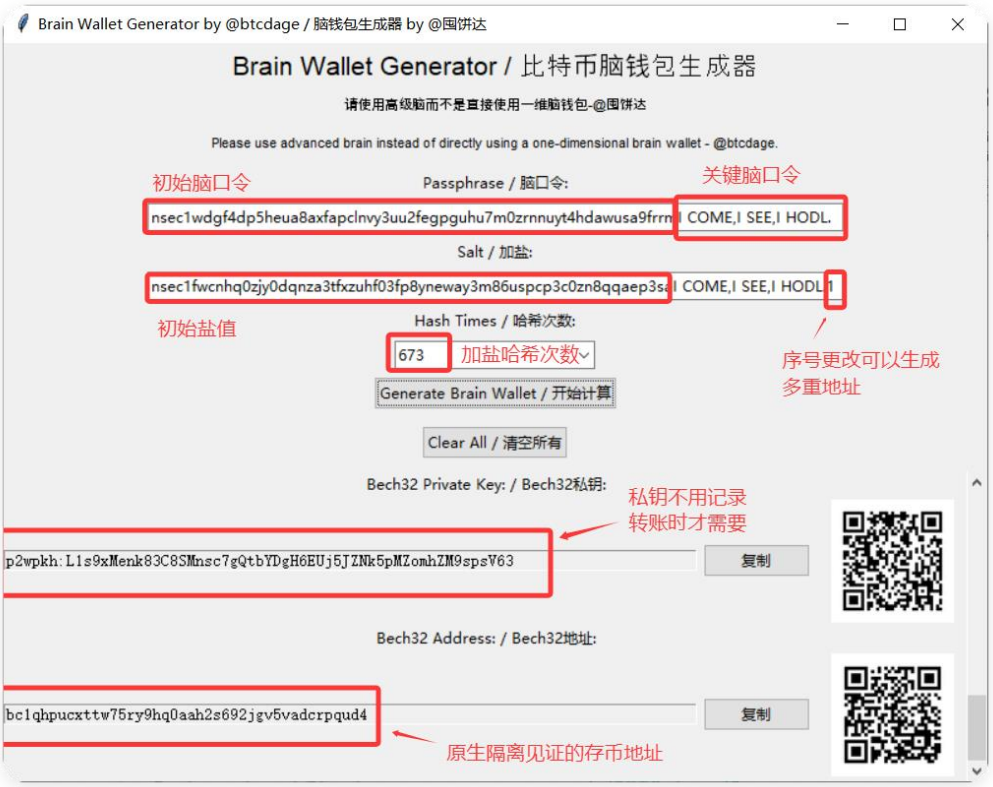
14.6 安全存储和备份

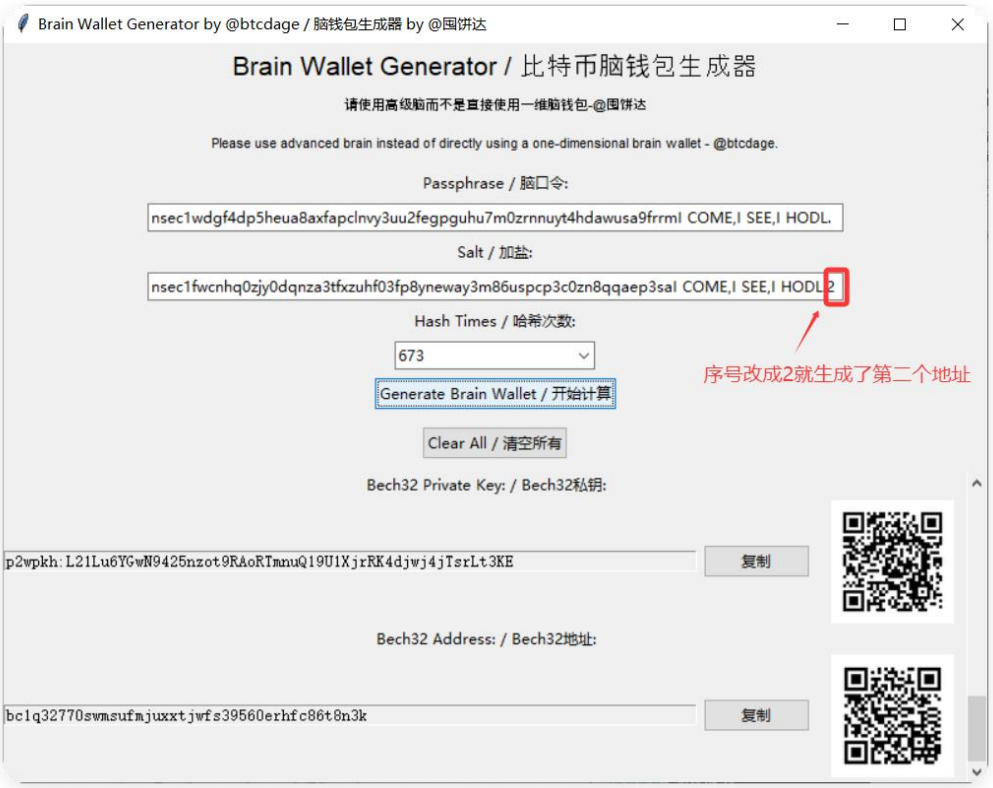
安全存储和备份是保护你比特币资产的重要环节，务必认真对待：

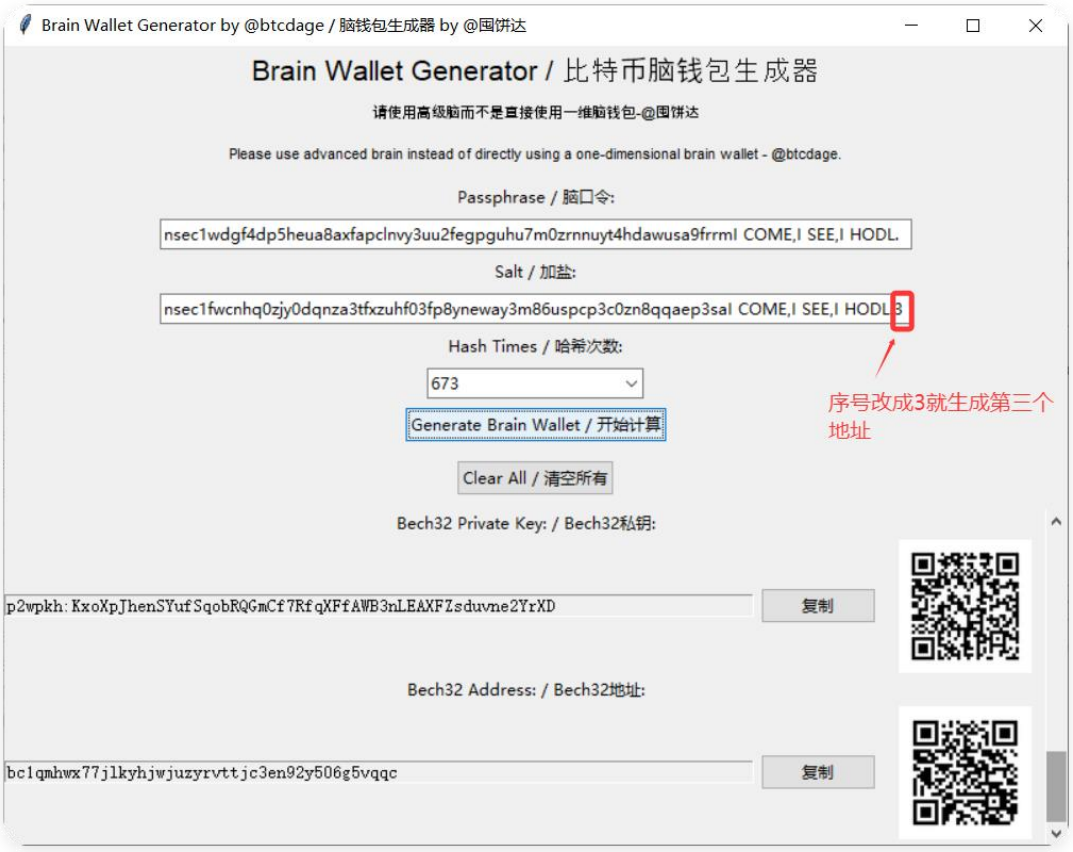
- **“关键脑口令”的特殊存储：** “关键脑口令” 只能存在于你的大脑中，不能记录在任何纸张、电子设备或者其他任何形式的物理介质上。
- **算法规则的备份：** 将你的算法规则打印成多份，分散存储在不同的安全地点，如保险箱、家中隐蔽角落、或者交给信赖的家人。
- **其他脑口令和盐值的备份：** 可以将它们抄写在纸上，或者加密后存储在 U 盘、移动硬盘等移动设备，或者网盘等云端存储中。
- **定期复查：** 定期检查你的备份，确保完整可靠。

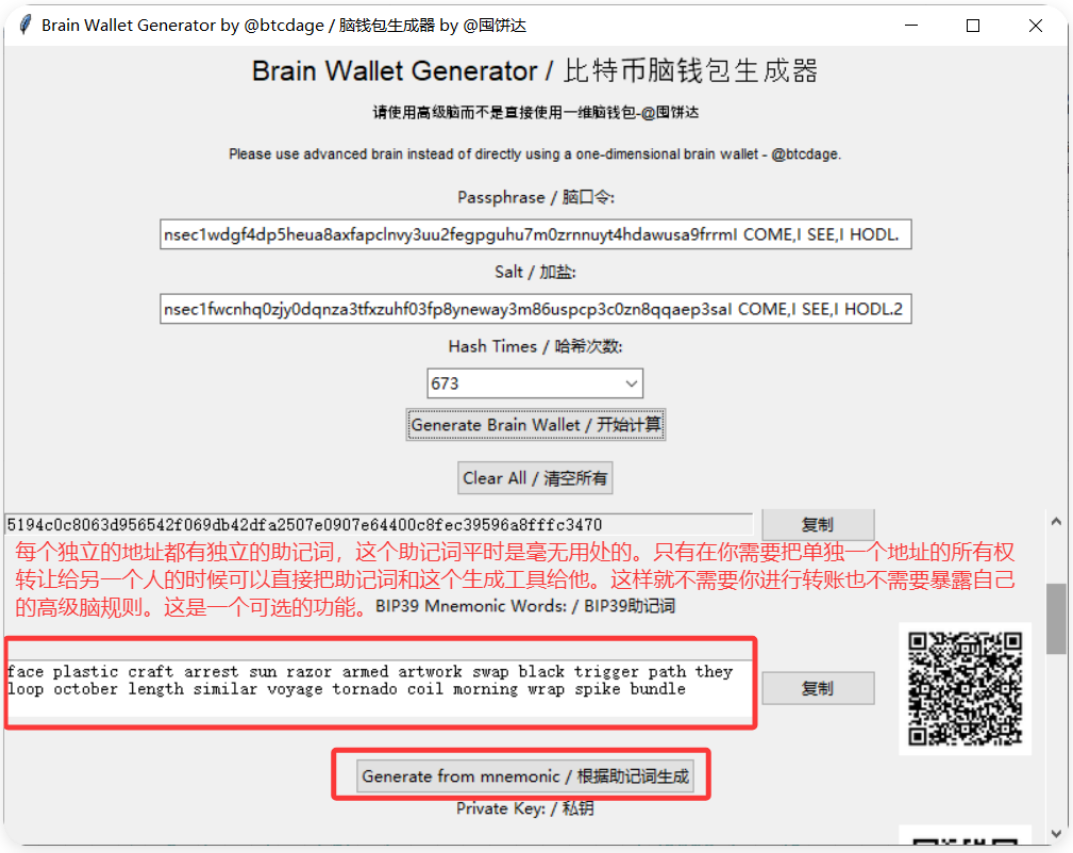
14.7 演示截图

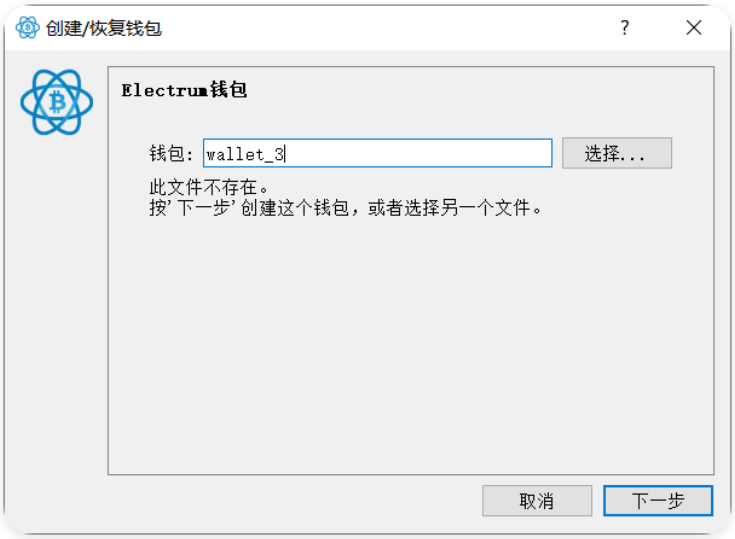
这里为演示截图，主要展示工具界面，以及演示操作步骤。完整的操作步骤请参考 14.3 到 14.6


Brain Wallet Generator by @btcdage / 脑钱包生成器 by @国饼达
Brain Wallet Generator / 比特币脑钱包生成器
请使用高级脑而不是直接使用一维脑钱包-@国饼达
Please use advanced brain instead of directly using a one-dimensional brain wallet - @btcdage.
初始脑口令
Passphrase / 脑口令:
关键脑口令
nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrml COME,I SEE,I HODL.
Salt / 加盐:
nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3sal COME,I SEE,I HODL1
初始盐值
Hash Times / 哈希次数:
673
加盐哈希次数
序号更改可以生成多重地址
Generate Brain Wallet / 开始计算
Clear All / 清空所有
Bech32 Private Key: / Bech32私钥:
私钥不用记录
转账时才需要
p2wpkh:L1s9xMenk83C8SMnsc7gQtbYDgH6EUj5JZNk5pMZomhZM9spsV63
复制
Bech32 Address: / Bech32地址:
bc1qhpucxttw75ry9hq0aah2s692jgv5vadcrpqud4
复制
原生隔离见证的存币地址

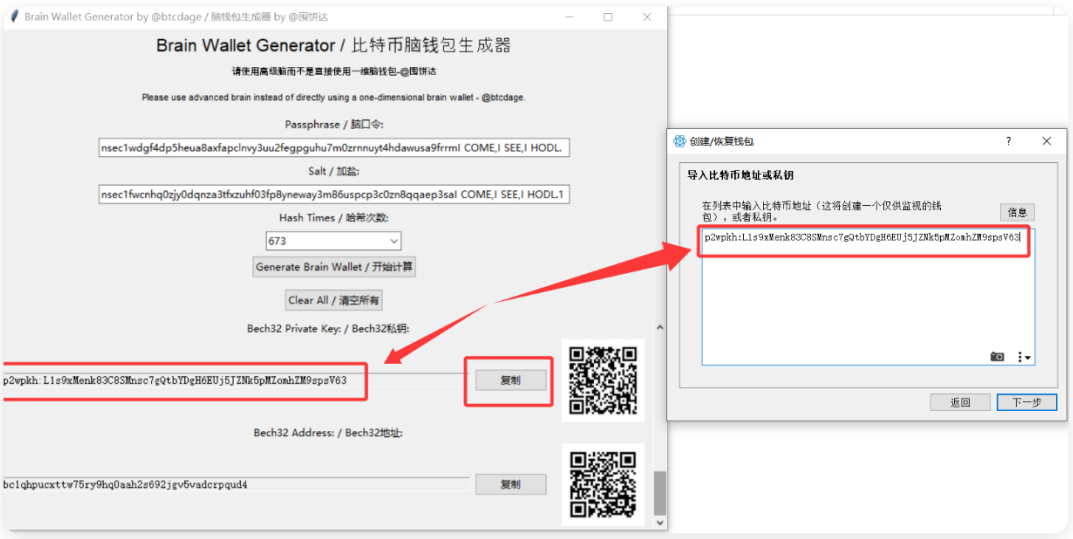

Brain Wallet Generator by @btcdage / 脑钱包生成器 by @国饼达
Brain Wallet Generator / 比特币脑钱包生成器
请使用高级脑而不是直接使用一维脑钱包-@国饼达
Please use advanced brain instead of directly using a one-dimensional brain wallet - @btcdage.
Passphrase / 脑口令:
nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrml COME,I SEE,I HODL.
Salt / 加盐:
nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3sal COME,I SEE,I HODL2
Hash Times / 哈希次数:
673
序号改成2就生成了第二个地址
Generate Brain Wallet / 开始计算
Clear All / 清空所有
Bech32 Private Key: / Bech32私钥:
p2wpkh:L21Lu6YGwN9425nzot9RAoRTmnuQ19U1XjrRK4djwj4jTsrLt3KE
复制
Bech32 Address: / Bech32地址:
bc1q32770swmsufmjuxxtjwfs39560erhfc86t8n3k
复制

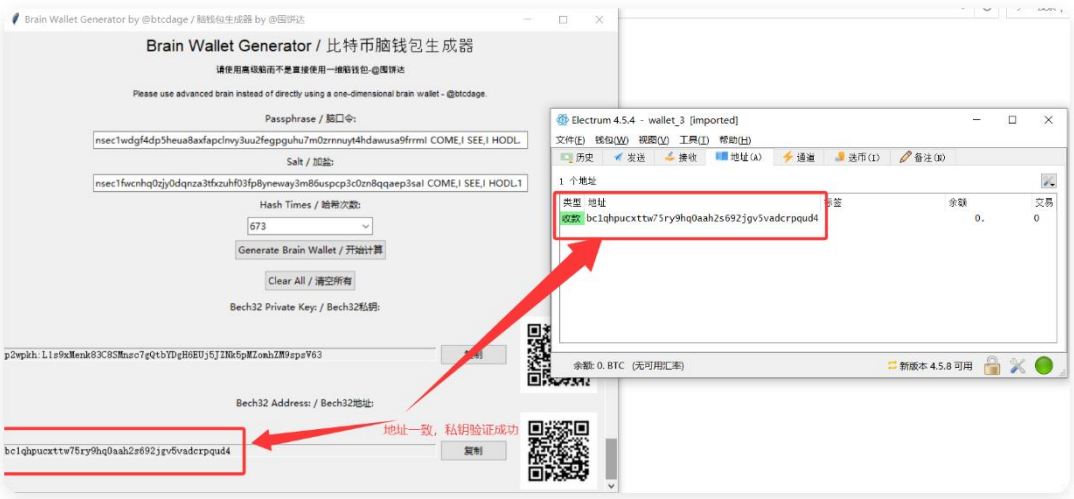

Brain Wallet Generator by @btcdage / 脑钱包生成器 by @囤饼达
Brain Wallet Generator / 比特币脑钱包生成器
请使用高级脑而不是直接使用一维脑钱包-@囤饼达
Please use advanced brain instead of directly using a one-dimensional brain wallet - @btcdage.
Passphrase / 脑口令:
nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrmI COME,I SEE,I HODL.
Salt / 加盐:
nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3saI COME,I SEE,I HODL3
Hash Times / 哈希次数:
673
Generate Brain Wallet / 开始计算
Clear All / 清空所有
Bech32 Private Key: / Bech32私钥:
p2wpkh:KxoXpJhenSYufSqobRQGmCf7RfqXFfAWB3nLEAXFZsduvne2YrXD
复制
Bech32 Address: / Bech32地址:
bc1qmhwx77jlkyhjwjuzyrvttjc3en92y506g5vqqc
复制
序号改成3就生成第三个地址


Brain Wallet Generator by @btcdage / 脑钱包生成器 by @囤饼达
Brain Wallet Generator / 比特币脑钱包生成器
请使用高级脑而不是直接使用一维脑钱包-@囤饼达
Please use advanced brain instead of directly using a one-dimensional brain wallet - @btcdage.
Passphrase / 脑口令:
nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrmI COME,I SEE,I HODL.
Salt / 加盐:
nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3saI COME,I SEE,I HODL.2
Hash Times / 哈希次数:
673
Generate Brain Wallet / 开始计算
Clear All / 清空所有
5194c0c8063d956542f069db42dfa2507e0907e64400c8fec39596a8fffc3470
复制
每个独立的地址都有独立的助记词，这个助记词平时是毫无用处的。只有在你需要把单独一个地址的所有权转让给另一个人的时候可以直接把助记词和这个生成工具给他。这样就不需要你进行转账也不需要暴露自己的高级脑规则。这是一个可选的功能。BIP39 Mnemonic Words: / BIP39助记词
face plastic craft arrest sun razor armed artwork swap black trigger path they loop october length similar voyage tornado coil morning wrap spike bundle
复制
Generate from mnemonic / 根据助记词生成
Private Key: / 私钥


创建/恢复钱包
Electrum钱包
钱包：wallet_3
选择...
此文件不存在。
按'下一步'创建这个钱包，或者选择另一个文件。
取消
下一步


创建/恢复钱包
创建新钱包
你想创建什么样的钱包？
标准钱包
具有双因子认证的钱包
多重签名钱包
导入比特币地址或私钥
返回
下一步


Brain Wallet Generator / 比特币脑钱包生成器
Passphrase / 脑口令:
Salt / 加盐:
Hash Times / 哈希次数:
Generate Brain Wallet / 开始计算
Clear All / 清空所有
Bech32 Private Key: / Bech32私钥:
Bech32 Address: / Bech32地址:
复制
创建/恢复钱包
导入比特币地址或私钥
返回
下一步



14.8 常见问题解答

- **Q：如果我忘记了 “关键脑口令”怎么办？**
  - A：由于“关键脑口令”只存在于你的大脑中，一旦忘记，将无法找回，因此必须确保你能记住它。 建议采用 “信息的指针记忆法”，将它和刻骨铭心的经历联系起来，并经常回顾，加深记忆。
- **Q：我可以使用在线的工具生成地址吗？**
  - 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？**
  - A：你可以将算法规则备份并告诉家人，而且一定要告诉他们你的的“关键脑口令”但千万不要记录在物理世界中。 如果你发生意外，你的家人可以使用你的备份信息，结合你告诉他们的 “关键脑口令”，来恢复你的比特币资产。
- **Q：我可以使用纸钱包或者硬件钱包吗？**
  - 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。 你在学习了高级脑钱包之后，会发现，使用高级脑钱包存储比特币更加安全。

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：高级脑钱包的核心思想是 **隐藏规则，而不是提高初始熵，并且手动生成地址，隐私至上，防御量子霸权，以及保障收币安全**。
2. **设计高级脑钱包时，最重要的是什么？**
   答：设计高级脑钱包时，最重要的是设计具有独特性和隐藏性的算法规则。
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”。

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。

高级脑钱包，是对传统私钥管理理念的一次颠覆。它将私钥存储于大脑，规避了第三方风险，实现了高度的“去中心化”财富管理，也让我们明白，比特币的安全，最终掌握在自己手中。

高级脑的理念，起源于 2020 年，成型于实践，并于 2025 年以本书的形式系统呈现。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，更要感谢各位群友粉丝一直以来的支持。我们也意识到，李笑来等早期实践者，早已采用了类似的技术，这进一步印证了高级脑钱包理念的先进性和实用性。

通过本手册的学习，你已经掌握了高级脑钱包的知识和技能，能够更加安全地管理你的比特币资产。 这也是一种力量，一种真正掌握自己财富的力量。

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

https://btcdage2011.github.io/btcdage

2025 年 1 月 15 日