One With Bitcoin： The Advanced Brain Complete Manual

By: Dage (X, Same as Weibo Account: @BTCDAGE)
https://btcdage2011.github.io/btcdage

nostr：npub17ahz4xa3hvkvvhh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

Introduction

Breaking Cognitive Barriers, Mastering the True Meaning of Wealth - The Birth of the Advanced Brain Wallet

Have you ever been confused by the complexity of Bitcoin private keys, or lost in the multitude of wallet choices? Have you ever worried about the security of your assets, yearning for a management method that is both safe and convenient?

The creation of "One With Bitcoin: The Advanced Brain Complete Manual" is precisely to answer these questions. The Advanced Brain Wallet is a private key management solution that the author, DaGe, has gradually developed since 2020 through continuous exploration, practice, and refinement. In conversations with Bitcoin evangelists, tractor users, and other advanced brain pioneers, it was surprising to discover that early Bitcoin practitioner Li Xiaolai had already adopted similar techniques.

However, there have always been concerns in the industry about the security risks of "one-dimensional brain wallets," which has hindered the promotion of the advanced brain concept. As more and more friends raised related questions, DaGe finally decided to write this "One With Bitcoin: The Advanced Brain Complete Manual" at the beginning of 2025.

This manual will guide you in breaking through the cognitive barriers of traditional wallets, starting from the essence of Bitcoin, and re-examining private key management. It will teach you how to closely integrate memory with private keys, achieving true "One With Bitcoin," making wealth and life intertwined, and truly achieving "where there is a person, there is the coin; where the person goes, the coin follows."

From the basics of Bitcoin to the design, practical application, and security concepts of the Advanced Brain Wallet, this manual will help you fully master this cutting-edge technology. Whether you are a Bitcoin novice or a seasoned player, you will benefit from it immensely. Special thanks to @BitcoinEvangelist for the technical discussions during the compilation of this manual.

Let's explore the mysteries of the Advanced Brain Wallet together and embark on a secure and free Bitcoin future!

Table of Contents

Chapter 1: Understanding Bitcoin - Digital Gold, Key to Freedom

1.1 Introduction: Breaking Free, A New Chapter in Wealth

Have you ever wondered if the money you have in the bank truly belongs to you? You might think it's a given, but in reality, your money is always under the control of banks or other financial institutions. They are like "caretakers" of your assets, and although they are mostly responsible, you still need to rely on them.

The emergence of Bitcoin is like a breath of fresh air, breaking free from the constraints of traditional finance. It's a new form of digital currency, a completely decentralized form of wealth. For the first time, it gives us the opportunity to truly own and control our assets, without relying on any third-party institutions. Just like your phone or your wallet, your Bitcoin should be controlled by you, not by any bank or institution.

So, what is Bitcoin? What makes it so special? In this chapter, we will together unveil the mystery of Bitcoin and introduce you to this digital wonder that is changing the world.

1.2 What is Bitcoin? - A Globally Shared Electronic Ledger

Imagine that you want to transfer money to a friend. In the past, you might have used a bank or a payment service like PayPal, right? These institutions act as intermediaries; they record your transfer information and are responsible for controlling the flow of funds.

Bitcoin, however, is completely different. It's like a globally shared electronic ledger that records every Bitcoin transaction. This ledger is not maintained by any single company or institution, but by thousands of computers around the world. This means that no one can arbitrarily alter or delete Bitcoin transaction records. It's like an open and transparent "grand ledger" that records the ins and outs of every transaction.

More importantly, this ledger is completely decentralized. No single person or institution can control it. This means that we no longer need to rely on banks or payment institutions to conduct transactions freely.

1.3 Characteristics of Bitcoin - Decentralization, Anonymity, Scarcity, Global Circulation

Bitcoin is so special because it has the following four important characteristics:

- **Decentralization:** Bitcoin is not controlled by any single company or government. Instead, it's maintained by thousands of computers worldwide, like a community where public affairs are decided by everyone, not by a single leader. This means that no individual or institution can arbitrarily change the rules of Bitcoin.
- **Anonymity:** A Bitcoin address is like a mysterious code; it doesn't directly correspond to your real identity. Like shopping online, where the merchant only knows your shipping address but not your exact identity, this protects your privacy to a certain extent. Of course, this doesn't mean that Bitcoin is completely anonymous, but it does offer more privacy than traditional financial systems.
- **Scarcity:** The total amount of Bitcoin is limited to 21 million, and it will never increase. Like rare gold, which is expensive because it's limited in quantity, Bitcoin's limited total supply also gives it a certain value-preserving function.
- **Global Circulation:** You can use Bitcoin for transactions anywhere in the world, without being restricted by national borders or exchange rates. Just like shopping online, where you

can buy goods from anywhere in the world without worrying about payment, the circulation of Bitcoin is the same.

1.4 Bitcoin Issuance and Total Supply Limits: "Mining" and the Halving Mechanism

- **Bitcoin Issuance Mechanism:** Bitcoin is not issued by any central institution; it's done through a process called "mining." In essence, nodes in a distributed network compete to record transactions and receive newly issued Bitcoin. This process relies on the "Proof of Work" (PoW) mechanism, where miners need to perform complex calculations with their computers to compete for the right to add new transactions to a new block. The PoW mechanism ensures the security and decentralization of the Bitcoin network, as attackers would need to invest enormous computational resources to tamper with the transaction records.
- **Block Rewards:** To encourage "miners" to maintain the security of the Bitcoin network, the Bitcoin system rewards miners with new Bitcoin when they successfully mine a new block. This is similar to you helping a friend organize their accounts, and they give you payment for it. Initially, every time a miner successfully mines a new block, they would receive a reward of 50 Bitcoin.
- **"Halving" Mechanism:** To control the speed at which Bitcoin is issued, the Bitcoin system has a "halving" mechanism. Every 210,000 blocks produced (approximately every four years), the Bitcoin block reward is halved. This means that the rate at which Bitcoin is issued will gradually slow down over time, eventually approaching zero.
    - Initially, each mined block rewarded 50 Bitcoin.
    - After 210,000 blocks, the reward became 25 Bitcoin.
    - After another 210,000 blocks, the reward became 12.5 Bitcoin.
    - And so on, constantly halving.
- **Total Supply Limit:** Due to the "halving" mechanism, the total supply of Bitcoin is strictly limited to 21 million and will never increase. This is similar to the limited total supply of gold, which gives it scarcity and value-preservation potential.
- **Bitcoin Transaction Confirmation:** When a Bitcoin transaction occurs, it needs to be bundled into a new block by miners. To ensure that the transaction is irreversible, it needs to have several block confirmations on the blockchain. Usually, 6 block confirmations (about 1 hour) are considered a relatively safe

confirmation number. This means that the transaction is recorded on the blockchain and is difficult to tamper with.

1.5 Why Does Bitcoin Have Value? - The Embodiment of Three Values

The value of Bitcoin can be understood in the following three aspects:

- **Store of Value:** Bitcoin's scarcity and immutability allow it to serve as a tool for storing value. Because the Federal Reserve and central banks around the world are continually printing money, inflation devalues your money over time. Bitcoin is a tool to combat the printing presses, giving people a choice that prevents inflation from plundering their wealth.
- **Medium of Exchange:** In some places, you can already use Bitcoin to purchase goods or services, just like you use payment systems like Alipay or WeChat. You can use Bitcoin to buy things in stores. As Bitcoin becomes more widespread, more and more merchants will accept Bitcoin as payment in the future.
- **Investment Asset:** More and more people are beginning to use Bitcoin as an investment asset. Just like you buy stocks or funds, you can also invest in Bitcoin, expecting it to bring you returns. They believe that Bitcoin's value will increase over time, and therefore they hold it for the long term.

1.6 Summary: Bitcoin - A Free and Transparent Future

Bitcoin is a revolutionary digital currency with characteristics like decentralization, anonymity, scarcity, and global circulation. It's not just a payment tool; it's also a store of value, a medium of exchange, and an investment asset. It represents a trend towards future wealth freedom and transparency.

But to truly understand Bitcoin and control your Bitcoin assets, we need to further understand Bitcoin wallets and how to securely manage private keys. In the next chapters, we will explore these issues in depth.

Chapter Quiz:

1. What is the total supply of Bitcoin?
2. What is "mining"?
3. What is the Bitcoin "halving" mechanism?

Chapter 2: Bitcoin Wallets - Your Digital Vault, Guardians of Private Keys

2.1 Bitcoin Wallets: Not Wallets for "Holding Coins"

The "Bitcoin wallets" we often talk about are actually quite different from the wallets we use every day. Your regular wallet is for holding cash, but a Bitcoin wallet isn't really for holding Bitcoin. Bitcoin itself is recorded on the blockchain. You can think of it as digital information existing on the internet, rather than a physical object. It's like it exists in a transparent, large ledger that no one can take away or modify unless they have the private key for that Bitcoin.

So, what exactly is a Bitcoin wallet?

You can think of it as a "toolbox" for managing your Bitcoin. It's mainly used to help you store and use your Bitcoin "keys," which are your private keys. With a private key, you can truly control your Bitcoin. It's like the lock on your door - only you have the key to open it. Likewise, only you can use your Bitcoin if you possess the private key.

2.2 Private Keys: The Keys to the Door of Wealth

- **The Essence of Private Keys:** A private key is a string of random characters, like your bank card password - only you know it, and you should absolutely not disclose it to anyone. It is the only key to opening your Bitcoin account.
- **The Importance of Private Keys:** Whoever holds the private key has control over that Bitcoin. If the private key is lost or stolen, your Bitcoin is in grave danger.
- **The Uniqueness of Private Keys:** Every Bitcoin address corresponds to a unique private key, just like every lock has its unique key.

2.3 Public Keys: "Bank Account Numbers" That Can Be Public

- **The Origin of Public Keys:** Public keys are derived from private keys through complex mathematical operations. You can think of them as your Bitcoin "bank account number" that you can give to others to send funds to your address.
- **The Purpose of Public Keys:** Just as you give your bank account number to others so they can transfer money to your bank card, you give your public key to others so they can send Bitcoin to your Bitcoin address. Because a Bitcoin address is generated from the public key through a public algorithm.
- **The Public Nature of Public Keys:** Public keys can be public, like your bank account number. Without considering quantum supremacy, others knowing your public key will not pose a threat to your assets. However, you must safeguard your private key to ensure your asset security.
- **Public Keys Cannot Be Reversely Engineered into Private Keys:** Without considering quantum supremacy, even if others know your public key, they cannot derive your private key. It's like knowing a bank account number, you still can't figure out the bank card password. Quantum supremacy will be introduced in Chapters 11 and 12.

2.4 Addresses: "Inboxes" for Receiving Bitcoin

- **The Origin of Addresses:** Addresses are also derived from public keys through complex mathematical operations. They are like your Bitcoin "inbox" for receiving Bitcoin transferred by others.
- **The Purpose of Addresses:** Just like your email address, which others use to send you emails, others need your Bitcoin address to send you Bitcoin.
- **The Public Nature of Addresses:** Addresses can be public. You can tell your address to others, allowing them to transfer

funds to your address without worrying about revealing your private key.
- **Multiple Addresses:** You can create multiple Bitcoin addresses, just like having multiple email addresses. You can use different addresses to receive Bitcoin from different sources.

2.5 The Relationship Between Private Keys, Public Keys, and Addresses: A Key, a Lock, and a Mailbox

To better understand their relationships, let's use this analogy:

- **Private Key:** Like the key to your house, only you can open your door.
- **Public Key:** Like the lock on your house, only the corresponding private key can open it.
- **Address:** Like the house number, others can find you through the house number and deliver mail to your mailbox.

Others can send funds to you through your address, just like others know your house number and can deliver mail to your house. Only those who have your private key can unlock the Bitcoin, just as only you have the key to open your house.

2.6 Emphasized Point: Independence of Private Keys, Public Keys, Addresses and the Bitcoin Network

Now, let's emphasize a very important concept: the generation of private keys, public keys, and addresses is not directly related to the Bitcoin network itself!

You can think of the Bitcoin network blockchain as a huge, public, transparent ledger that records every Bitcoin transaction. This ledger is like a public post office where everyone can see the record of each transaction, but only those who hold private keys can manage their own Bitcoin.

Our private keys, public keys, and addresses are like keys, locks, and home addresses. They exist independently and do not depend on any specific "delivery company" or "post office."

- **Analogy of Independence:** Just like your house key, lock, and home address, they do not depend on FedEx or Postal Service. Whether or not there are delivery companies, the function of your key, lock, and address remains unchanged. Similarly, regardless of whether there is a Bitcoin wallet software or

hardware, your private keys, public keys, and addresses are independent. More importantly, the generation of these key pairs is done completely locally, which is a local behavior that does not rely on any network connection or the Bitcoin blockchain. Private keys are generated by random number generation algorithms. Public keys are derived from private keys using specific one-way functions, and Bitcoin addresses are generated through hash operations on public keys. These generation processes are all done locally, and are not related to the Bitcoin network. They are your identity certificates in the Bitcoin world.

- The Role of Wallets: A wallet is just a tool that helps you generate and manage private keys, public keys, and addresses. You can use various different tools to generate these key pairs, such as paper and pen or computer programs. But no matter what tool you use, they are just tools and do not change the nature of your private keys, public keys, and addresses. A wallet's job is to securely store your private keys and facilitate transactions, not to generate key pairs themselves.
- Common Misconceptions: Many beginners mistakenly believe that they must purchase a hardware or software wallet to have a Bitcoin address, which is incorrect. Addresses and key pairs exist independently. You can use various tools to create them, and wallets are just tools used to help you manage these key pairs. The generation of keys is a completely local process, and you can still generate key pairs even if the network connection is disconnected.

In Summary: Our private keys, public keys, and addresses are like an independent key, an independent lock, and an independent home address. They do not depend on any tools, institutions, or the Bitcoin network itself. They exist independently, and their generation process is completely local. If you do not intend to transfer out any funds, and merely intend to generate and store a Bitcoin address and its corresponding private key, you only need to perform some mathematical and character operations locally, without requiring any transactional wallet software or hardware. You only need to import the private key into the wallet software and hardware when you need to transfer out the funds to manage your assets.

2.7 Wallet Functions: Private Key Management Experts

Now we know that the wallet itself does not store Bitcoin. Its main functions are to manage private keys, including:

- **Generating and Storing Private Keys:** Wallets help you generate private keys and securely store them.
- **Generating and Managing Addresses:** Wallets help you generate addresses and manage your Bitcoin addresses, making it easy for you to receive and send Bitcoin.
- **Transaction Signing:** When you want to transfer Bitcoin, the wallet will use your private key to sign the transaction, proving that you initiated the transaction.

2.8 Summary: Private Keys Are the Cornerstone of Bitcoin Security

The core of a Bitcoin wallet is the management of private keys. Private keys are like the key to entering the Bitcoin world. If you have the private key, you own the Bitcoin. Be sure to safeguard your private key and do not disclose it to anyone. Otherwise, your Bitcoin will face great risks.

It should also be clear that: Private keys, public keys, and addresses are independent and do not depend on any tools. Wallets are just tools to help you generate and manage your private keys.

Answers to Previous Chapter Quiz:

1. What is the total supply of Bitcoin?
   Answer: The total supply of Bitcoin is approximately 21 million.
2. What is "mining"?
   Answer: "Mining" is the process of using computers to perform complex calculations to verify and record new transactions and add this transaction information to new blocks.
3. What is the Bitcoin "halving" mechanism?
   Answer: The "halving" mechanism refers to the block reward of Bitcoin being halved approximately every four years (every 210,000 blocks generated on the blockchain).

This Chapter Quiz:

1. What is the function of a private key? Why is it so important?
2. Can public keys and addresses be made public?
3. Do private keys, public keys, and addresses depend on the Bitcoin network blockchain?

Chapter 3: Types of Wallets - A Variety of Options, Each With Strengths

3.1 Classification of Wallets: Connected to the Internet or Not

In the previous chapter, we learned the essence of a Bitcoin wallet, understanding that it is essentially a tool for managing private keys. So, what are the differences between the many types of wallets on the market? We can categorize them into two major types based on whether they are connected to the internet: hot wallets and cold wallets.

- **Hot Wallets:** Like a frequently used wallet, you always carry cash and can take it out at any time. Hot wallets are connected to the internet. Examples include app wallets on your phone, software wallets on your computer, and wallets on exchanges.
    - **Pros:** Easy and convenient to use; you can make transactions anytime.
    - **Cons:** Due to being constantly connected to the internet, they are vulnerable to hacking and carry certain security risks.

- **Cold Wallets:** Like a safe deposit box, once the money is stored, it's locked away and not easily accessed. Cold wallets are not connected to the internet. Examples include hardware wallets, paper wallets, and brain wallets.
    - **Pros:** Due to being disconnected from the internet, they are more secure and less susceptible to hacking.
    - **Cons:** They are relatively cumbersome to use and not as convenient as hot wallets.

Summary: Considering security, we should always choose a cold wallet for storing our Bitcoin.

3.2 Common Types of Wallets: Each with Its Own Focus, Pros, and Cons

Now that we understand the basic concepts of hot wallets and cold wallets, let's take a closer look at some common wallet types and their pros and cons.

- **Software Wallets:** Software wallets are applications installed on your phone or computer, such as imToken, Trust Wallet, and Electrum.
    - **Pros:** Convenient to use; you can use them anytime and anywhere, and they are usually free.
    - **Cons:** Due to relying on the phone or computer environment, they are vulnerable to viruses or malware attacks. They have relatively lower security and privacy.
    - **Suitable For:** Users who store small amounts of Bitcoin and frequently make transactions.
- **Exchange Wallets:** Exchange wallets refer to storing your Bitcoin in an account on a centralized exchange.
    - **Pros:** Convenient for trading; you can buy and sell directly on the exchange.
    - **Cons:** The biggest risk is the exchange itself. If the exchange is hacked, goes bankrupt, or runs away, or if it is frozen by regulators, your Bitcoin will face huge losses.
    - **Suitable For:** Users who trade on exchanges, but not suitable for long-term storage of large amounts of Bitcoin.
- **Hardware Wallets:** Hardware wallets are dedicated hardware devices for storing private keys, such as Ledger and Trezor.
    - **Pros:** Higher security; private keys are stored in the hardware device and are not easily compromised by network attacks.

    - **Cons:** Require the additional purchase of hardware, they are expensive, relatively complex to operate, and dependent on manufacturers, with the risk of manufacturers going bankrupt, backdoors, etc.
    - **Suitable For:** Users who have not yet learned about Advanced Brain Wallets and don't mind the lack of privacy when storing Bitcoin.
- **Paper Wallets:** Paper wallets are a way of printing your private keys and addresses on paper and then storing them offline.
    - **Pros:** High security; private keys do not touch the internet and are less susceptible to hacking.
    - **Cons:** Easily lost, damaged, or copied; using and backing them up is inconvenient; and they are not suitable for frequent transactions.
    - **Suitable For:** Users who have not yet learned about Advanced Brain Wallets and are absolutely confident in their physical storage conditions.
- **Brain Wallets:** Brain wallets store private keys in your brain, using a complex passphrase or a memory to generate the private key.
    - **Pros:** Extremely high privacy; no need to carry any devices; no backup needed; theoretically the most convenient and fastest option.
    - **Cons:** If the passphrase is too complex, you may forget it; if it is too simple, it is easily cracked. Therefore, brain wallets are not suitable for direct use.
    - **Suitable For:** Users with some experience, and who can create a sufficiently complex brain passphrase.

3.3 In-depth Understanding: BIP39 Mnemonic Phrases - Another Way to Express Private Keys

Before understanding Advanced Brain Wallets, we need to understand another commonly used private key generation and management solution: BIP39 mnemonic phrases. BIP39 is an industry standard. It doesn't directly convert a private key into mnemonic words but converts a randomly generated seed into a set of easily memorable words (usually 12, 18, or 24 words) through a series of steps. Then, a private key can be generated from this seed.

- **The Principle of BIP39:**
    1. **Generating Random Numbers (Entropy):** First, BIP39 generates a highly random binary number, known as entropy.

2. **Generating a Seed:** Then, through hash operations, a seed is generated from this entropy. This seed is also a long string of random characters.
3. **Generating Mnemonic Phrases:** The seed is converted into a set of easily memorable words, which are mnemonic phrases.
4. **Generating Private Keys:** Finally, using this seed, multiple private keys and addresses can be generated using specific algorithms.

- **The Essence of BIP39 Mnemonic Phrases:** In essence, each mnemonic word represents a position in a vocabulary list of 2048 words, equivalent to a number from 0 to 2047. Therefore, a minimum of 12 words is needed to ensure sufficient entropy to guarantee the security of the private key.
- **Advantages of BIP39 Mnemonic Phrases:**
  - **Easy Backup:** You can write mnemonic phrases on paper for easy backup and recovery of the wallet.
  - **Strong Compatibility:** Many wallets support the BIP39 protocol.
- **Disadvantages of BIP39 Mnemonic Phrases:**
  - **Difficult to Memorize:** Although mnemonic phrases are words, due to their randomness, they are not easy to memorize. 12, 18, or even 24 unrelated words are not as easy to remember as you might think. This is why we need advanced brain wallets.
  - **Reliance on Third Parties:** You must trust that the tool used to generate mnemonic phrases is secure.
  - **Still Risky:** If the mnemonic phrases are leaked or lost, your Bitcoin will face significant risks.
  - **Not Flexible Enough:** The method of generating private keys using BIP39 mnemonic phrases is fixed, not flexible, and not customizable.
  - **Passphrase Feature:** BIP39 also supports an optional passphrase feature. You can set an additional password, which will be used along with the mnemonic phrases during the private key generation process. This is like adding an extra layer of protection to your mnemonic phrases, increasing security. However, if you forget the passphrase, your Bitcoin will also be lost.
  - **Derivation Feature:** BIP39 supports the concept of a derivation path. This means that you can use the same set of mnemonic phrases to generate countless different private keys and addresses. This is like using one key to open different doors, facilitating asset management and

isolation, but it also has certain management difficulties.

- **Security of BIP39 Mnemonic Phrases:** Many people think that as long as the mnemonic phrases are well kept, they are absolutely safe. However, it is important to note that:
  - **Generation Process of BIP39 Mnemonic Phrases:** The generation of BIP39 mnemonic phrases essentially relies on a random number generator. If the random number generator has vulnerabilities, then the mnemonic phrases also have risks. In addition, BIP39 mnemonic phrases are not the real keys themselves; they are just another representation of keys. It needs to use specific algorithms to convert the mnemonic phrases into a seed, and then derive the private key from the seed. In this process, the generation of the seed and private key both rely on specific algorithms. If the algorithm has vulnerabilities or is not implemented securely, it may cause security risks.
  - **Storage of BIP39 Mnemonic Phrases:** If you store the mnemonic phrases on an electronic device, there is a risk of hacking. If you store them on paper, there is a risk of loss or damage.
  - **Memorization of BIP39 Mnemonic Phrases:** Many people choose to record mnemonic phrases, while others choose to memorize them. However, mnemonic phrases are usually 12, 18, or 24 words. If you misremember them, it can also lead to a risk of losing your assets.

3.4 Comparison Summary: Choose a Wallet That Suits You

Each type of wallet has its pros and cons. There is no absolutely safe or perfect wallet. We need to choose a wallet that suits our needs based on our actual situation.

- **Hot Wallets:** Suitable for storing small amounts of Bitcoin and for users who trade frequently. However, you must pay attention to security and not store large amounts of assets.
- **Cold Wallets:** Suitable for storing large amounts of Bitcoin and for users who prioritize security. However, they are not as convenient to use as hot wallets.
- **Hardware Wallets:** Higher security, suitable for long-term storage, but costly, complex to operate, and with some manufacturer risks. Suitable For: Users who have not yet

learned about Advanced Brain Wallets and don't mind the lack of privacy when storing Bitcoin.

- **Paper Wallets:** Suitable for storing small amounts of Bitcoin and for users who don't trade frequently, but pay attention to paper storage. Suitable For: Users who have not yet learned about Advanced Brain Wallets and are absolutely confident in their physical storage conditions.
- **Brain Wallets:** Extremely private, but also highly risky, suitable for experienced users and those who can create sufficiently complex brain passphrases. Cons: If the passphrase is too complex, you may forget it; if it is too simple, it is easily cracked. Therefore, brain wallets are not suitable for direct use.
- **BIP39:** Convenient and easy to use, but still dependent on third parties and storage risks, and not flexible, and still difficult to memorize.

3.5 Summary: Understand Wallets to Better Protect Your Assets

Understanding different types of wallets will help you better protect your Bitcoin assets. We need to choose the right tools and master safe usage techniques to navigate the Bitcoin world freely.

Answers to Previous Chapter Quiz:

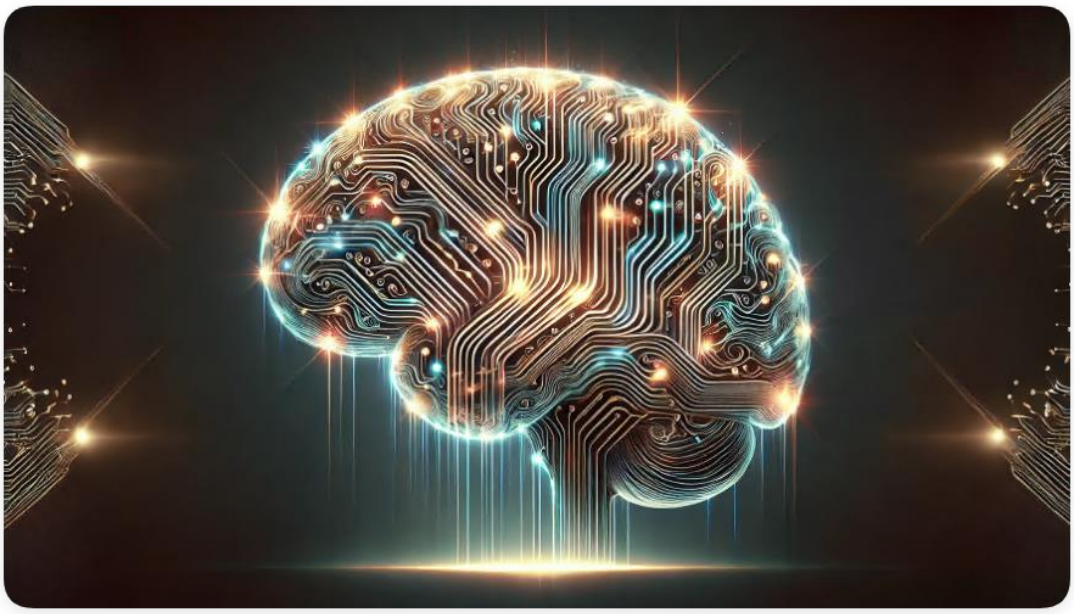
1. What is the function of a private key? Why is it so important?
   Answer: A private key is the unique key to control Bitcoin. Having the private key means you have control over the Bitcoin, making it very important.
2. Can public keys and addresses be made public?
   Answer: Yes, public keys and addresses can be made public and are used to receive Bitcoin.
3. Do private keys, public keys, and addresses depend on the Bitcoin network blockchain?
   Answer: No, private keys, public keys, and addresses do not depend on the Bitcoin network blockchain. They are independent entities.

This Chapter Quiz:

1. What is a hot wallet? What is a cold wallet?

2. What are BIP39 mnemonic phrases? What is the principle behind them?
3. What are the pros and cons of BIP39 mnemonic phrases?

Chapter 4: Introduction to Brain Wallets - Storing Private Keys in Your Brain



4.1 Brain Wallets: The "Ultimate" Storage Method for Private Keys

Through our previous studies, we have learned about various types of wallets and the importance of private keys. We know that a private key is like the key to the door of the Bitcoin world. With the private key, you own the Bitcoin. So, how can we safely and conveniently store and manage our private keys?

The traditional method is to store private keys on hardware devices, paper, or software programs. However, these methods all have certain risks. For example, hardware devices can be damaged, paper can be lost, and software programs can be hacked.

Is there a safer and more convenient storage method? The answer is yes, and that is the brain wallet.

A brain wallet, as the name suggests, stores the private key in your brain. It may sound unbelievable, but in fact, brain wallets are a very ingenious storage method. They generate your private key by having you remember a special passphrase or a profound memory.

4.2 Brain Passphrases: "Spells" to Unlock the Door to Wealth

The core of a brain wallet is the brain passphrase, also called the brain seed. You can think of the brain passphrase as a "spell" to enter the Bitcoin world. This spell can be anything that is easy for you to remember, for example:

- **A sentence:** Your favorite line of poetry, a line from a movie, a phrase that moves you.
- **A passage:** An experience of yours, an insight, or your vision for the future.
- **A story:** A fun childhood experience or an unforgettable moment with your family.
- **A location:** The place where you were born, or where you first dated your loved one.
- **A group of numbers or symbols:** A special sequence of numbers for you, or a unique combination of symbols.
- **Even a melody or lyrics:** Your favorite song, or a memorable melody.

The key is that this brain passphrase must be something only you know and that is easy to remember. It is best if it is meaningful, which will facilitate better memorization and prevent forgetting.

4.3 How Brain Wallets Work: Converting Memory into Private Keys

Once you have determined your brain passphrase, the brain wallet uses a special algorithm to convert it into a complex private key.

- **Hashing:** The brain wallet will calculate your brain passphrase using a special hashing function, generating a fixed-length hash value. This hash value is also a string of random characters.
- **Private Key Generation:** Then, using this hash value, your private key can be generated.

4.4 Advantages of Brain Wallets: No Devices, Private and Secure

Brain wallets are special because they have unparalleled advantages compared to other wallets:

- **No Devices Required:** You don't need to carry any hardware devices or install any software programs. The private key is stored in your brain. As long as you remember your brain passphrase, you can access your Bitcoin anytime, anywhere.

- **High Privacy:** As long as you don't disclose your brain passphrase, no one knows your private key, making your Bitcoin more secure.
- **No Backup Required:** You don't need to back it up like other wallets. As long as your memory is fine, your private key will not be lost.

4.5 Risks of "One-Dimensional Brain Wallets": Passphrases Are Critical, Memory Is Unreliable

To better understand the risks of brain wallets, we will classify the concept of ordinary brain wallets as "one-dimensional brain wallets." The biggest feature of a one-dimensional brain wallet is that it relies on only one simple passphrase to generate the private key, and it is for this reason that there are huge security risks:

- **Weak Passphrases:** If your brain passphrase is too simple, such as "123456" or "password," or even if it is not simple but the same as others use, it is still easily cracked by hackers.
    - **Risk of Duplicate Passphrases:** Even if your passphrase is not a simple combination like "123456," if you use a well-known poem, such as "Quiet Night Thought," as your brain passphrase, there are likely many others who are using the same passphrase. In this case, hackers can collect these common passphrases to crack one-dimensional brain wallets in batches.
    - **Dictionary Attacks:** Hackers will prepare a dictionary containing a large number of commonly used passphrases in advance and then use this dictionary to attempt to crack your brain passphrase. Some popular brain wallet tools (such as bitaddress.org) already have publicly available dictionaries collected by others, making it easy to crack using brute force.
- **Memory Loss:** If your brain passphrase is too complex or if too much time has passed, you may forget it, preventing you from recovering your private key.
- **Leakage Risks:** If you accidentally reveal your brain passphrase to others, your Bitcoin will be at risk of theft.
- **Reliance on Personal Memory:** The security of brain wallets depends entirely on your personal memory ability, which is a huge challenge for many people.
- **Historical Cracking Records:** There have been many cases in history where one-dimensional brain wallets have been cracked.

Some users have had their Bitcoin stolen due to using passphrases that were too simple or too common.

    - **Case Analysis:** In 2015, Ryan Castellucci detailed how to crack one-dimensional brain wallets using the "Brainflayer" high-speed cracking tool. Current computers can make millions, billions, or even trillions of guesses per second, and some common passphrases can be cracked in a day. Ryan Castellucci shared his experience of accidentally stealing 250 bitcoins (which he later returned), which fully illustrates the huge risk of directly using one-dimensional brain wallets.
- **Risks Even With Strong Passphrases:** Even if you use a high-strength passphrase and ensure that it is not repeated, you still cannot completely guarantee security. For example, if your computer is infected with malware that records your keyboard input, your brain passphrase can still be leaked, leading to the theft of your private keys. In addition, some advanced attackers may use social engineering to obtain your brain passphrase through deception. Additionally, if the algorithm used to generate the private key has vulnerabilities, even if your passphrase is very strong, security cannot be guaranteed. Therefore, relying solely on passphrase strength to protect brain wallets is very dangerous.

4.6 Why We Do Not Recommend Direct Use of "One-Dimensional Brain Wallets"?

Because the risks of “one-dimensional brain wallets” are so high, we do not recommend ordinary users to use them directly. Most people cannot guarantee that their passphrases are complex or safe enough, nor can they guarantee that they will never forget them. “One-dimensional brain wallets” are just a concept, not a product. They pose extremely high risks.

4.7 Summary: The Idea of Brain Wallets, The Foundation of Advanced Brain Wallets

Brain wallets provide a very interesting and unique way to store private keys. They also offer new ideas for balancing security and convenience. Although we don’t recommend that ordinary people directly use “one-dimensional brain wallets,” the idea of “one-dimensional brain wallets” provides an important theoretical foundation for our subsequent study of advanced brain wallets.

Answers to Previous Chapter Quiz:

1. What is a hot wallet? What is a cold wallet?
   Answer: A hot wallet is a wallet that is connected to the internet, and a cold wallet is a wallet that is not connected to the internet.
2. What are BIP39 mnemonic phrases? What is the principle behind them?
   Answer: BIP39 mnemonic phrases are an industry standard for converting a seed into a set of easily remembered words.
3. What are the pros and cons of BIP39 mnemonic phrases?
   Answer: The advantage of BIP39 mnemonic phrases is that they are easier to remember and back up than private keys, but the disadvantages are that they rely on third parties for generation, still have the risk of leakage, and are not flexible enough.

This Chapter Quiz:

1. What is a brain wallet? What is its core?
2. What is a brain passphrase? What are its characteristics?
3. What are the advantages of brain wallets?
4. What is a "one-dimensional brain wallet"? What are its risks?
5. Why do we not recommend using "one-dimensional brain wallets" directly?

Chapter 5: Why Do We Need Advanced Brain Wallets?

5.1 Limitations of Ordinary Brain Wallets: Seemingly Secure, but Actually Full of Danger

In the last chapter, we learned about "one-dimensional brain wallets." They store private keys in the brain, which seems very secure and convenient, but in reality, there are many risks. We know that the biggest problem with "one-dimensional brain wallets" is that they rely on only one simple passphrase, and this passphrase is likely too simple and easy to crack; or it may be too common and easily duplicated; or we ourselves may forget it.

It's like a house with only one door. Although it looks very safe, as long as someone can open that door, they can enter your room. A one-dimensional brain wallet is like this house with only one combination lock. Once the lock is cracked, all your assets will be exposed to risk.

So, is there a better way to utilize the convenience of brain wallets while avoiding their inherent security risks? The answer is yes, and that is what we will learn next - advanced brain wallets.

5.2 Advanced Brain Wallets: A Leap from "One-Dimensional" to "Multi-Dimensional"

Advanced brain wallets are not a simple upgrade of ordinary brain wallets but rather a completely new private key management philosophy. The biggest difference between them and ordinary brain wallets (also known as "one-dimensional brain wallets") is:

- **One-Dimensional Brain Wallets:** Rely on only one simple passphrase to generate private keys.
- **Advanced Brain Wallets:** Do not rely on just one simple passphrase but instead design a complex set of algorithmic rules to generate private keys.

You can think of an advanced brain wallet as a complex maze made up of multiple doors and locks. Even if a hacker knows one of your passphrases or a lock, it is difficult to find the real exit and difficult to break through the defense system.

5.3 The Core Idea of Advanced Brain Wallets: Hiding Rules, Not Just Simple Passphrases

The core idea of advanced brain wallets is to hide the rules rather than just increase the initial entropy.

- **Ordinary Brain Wallets:** Try to improve security by increasing the complexity of the passphrase (for example, by increasing the length of the passphrase or using complex character combinations).
- **Advanced Brain Wallets:** Focus more on hiding the rules for generating private keys. Even if a hacker knows your passphrase, they don't know the rules for generating your private key, making it difficult to crack your private key.

You can think of this process as a magic trick. The magician will not tell the audience how they do the magic; they hide the secret behind the trick. Advanced brain wallets are the same; they hide the secret of private key generation, making it difficult for hackers to crack.

5.4 Advantages of Advanced Brain Wallets: Multiple Protections, More Secure

Compared to "one-dimensional brain wallets," advanced brain wallets have the following significant advantages:

- **Complex Rules:** Advanced brain wallets do not directly calculate the private key by hashing the passphrase. Instead, they process the passphrase multiple times through a complex set of

algorithmic rules before generating the private key. This is like adding multiple layers of encryption on top of the original, greatly increasing the difficulty of cracking.

- **Hidden Rules:** Only you know the algorithmic rules you use. Even if others know your passphrase, it will be difficult for them to reconstruct your private key. This is like a map of a maze; only you know how to get out of the maze, and no matter how much others try, they will not succeed.
- **Easy to Remember:** Advanced brain wallets do not just pursue the complexity of the passphrase. They also focus on making the passphrase easy to remember. You don't need to remember a random string of characters; you can remember some meaningful words or stories and use a set of simple rules to generate private keys while ensuring sufficient security.

5.5 The Necessity of Advanced Brain Wallets: Avoiding the Risks of "One-Dimensional Brains"

The reason we need advanced brain wallets is because "one-dimensional brain wallets" have too many risks, and these risks can be avoided through the ingenious design of advanced brain wallets:

- **Avoid Dictionary Attacks:** Hackers can collect common passphrases to try to crack one-dimensional brain wallets. However, advanced brain wallets have hidden rules, so even if hackers have a dictionary, they cannot crack your private key.
- **Avoid Duplicate Passphrases:** Even if the passphrase you use is common, you can still generate a unique private key through a unique set of algorithmic rules.
- **Avoid Memory Burdens:** You don't need to remember an overly complex random string; instead, you can generate a private key by using a meaningful passphrase and simple rules, while achieving a high level of security.
- **More Flexible and Customizable:** You can design your own unique advanced brain wallet scheme according to your preferences and habits, which is something that "one-dimensional brain wallets" and BIP39 cannot achieve.

5.6 Summary: Advanced Brain Wallets - The Perfect Combination of Security and Convenience

Advanced brain wallets are a safer and more flexible private key management solution. They not only inherit the convenience of brain wallets but also overcome the security risks of "one-dimensional

brain wallets." They represent a trend for private key management in the future and are worthy of our in-depth study and mastery.

Answers to Previous Chapter Quiz:

1. What is a brain wallet? What is its core?
   Answer: A brain wallet is a wallet that stores private keys in the brain, and its core is the brain passphrase.
2. What is a brain passphrase? What are its characteristics?
   Answer: A brain passphrase is a passphrase used to generate private keys. It has characteristics such as ease of memorization and uniqueness.
3. What are the advantages of brain wallets?
   Answer: The advantages of brain wallets are no devices required, high privacy, and no backup required.
4. What is a "one-dimensional brain wallet"? What are its risks?
   Answer: A "one-dimensional brain wallet" refers to a brain wallet that relies on only one simple passphrase to generate private keys. Its risks include a weak passphrase, memory loss, leakage risk, and reliance on personal memory.
5. Why do we not recommend direct use of "one-dimensional brain wallets"?
   Answer: We do not recommend direct use of "one-dimensional brain wallets" because there are too many security risks that most people cannot avoid.

This Chapter Quiz:

1. What are the risks of "one-dimensional brain wallets"?
2. What is the biggest difference between advanced brain wallets and ordinary brain wallets ("one-dimensional brain wallets")?
3. What is the core idea of advanced brain wallets?

Chapter 6: The Security Foundation of Advanced Brain Wallets - Building Your Exclusive "Encryption Fortress"

6.1 Why Do We Need to Understand Security Foundations? - Sharpening the Axe Doesn't Delay the Wood Cutting

In the last chapter, we understood the necessity and core idea of advanced brain wallets and learned that they are more secure than ordinary "one-dimensional brain wallets." However, how do we design a truly secure advanced brain wallet? This requires us to understand some basic cryptographic concepts.

Learning these concepts is like learning the basic principles of building a house. Only by understanding the structure of the foundation, load-bearing walls, and roof can you build a strong and durable house. Similarly, only by understanding the security foundations such as hash algorithms, collision resistance, and diffusion can you design a truly secure advanced brain wallet, thereby protecting our Bitcoin assets.

6.2 Hash Algorithms: The Magical "Information Fingerprints"

- **What is a Hash Algorithm?** A hash algorithm is like a magical "blender" that "blends" input information of any length (e.g., text, numbers, pictures, videos, etc.) into a fixed-length

output information, called a hash value. The hash algorithm is like your "takeout order number." No matter how complicated your takeout order is, it will eventually generate a fixed-length order number, and according to this order number, the takeout vendor can quickly find your order information.

- Characteristics of Hash Algorithms:
  - One-Way: Hash algorithms are one-way, meaning you can only get the hash value from the input information but cannot reverse-engineer the input information from the hash value. This is like knowing the takeout order number, but you cannot reverse-engineer which dishes the customer ordered from the order number.
  - Fixed-Length Output: Regardless of how long the input information is, the generated hash value is of a fixed length. For example, the SHA-256 algorithm generates a 256-bit hash value regardless of the length of the input information.
  - Avalanche Effect: Any tiny change in the input information will cause a huge change in the generated hash value. Imagine that if you order an extra meal in your takeout order, the order number will change completely, with no relation to the previous one.
- Applications of Hash Algorithms: Hash algorithms have a wide range of applications in the computer field, such as:
  - File Verification: You can verify whether downloaded files have been tampered with.
  - Password Storage: Websites will store users' passwords after hashing them, rather than storing plain text passwords, to prevent password leaks.
  - Blockchain: The Bitcoin blockchain uses hash algorithms extensively.
- SHA-256 Algorithm: SHA-256 is a very commonly used hash algorithm. Bitcoin uses the SHA-256 algorithm to generate addresses. We can use SHA-256 or other hash algorithms when designing advanced brain wallets.

6.3 Collision Resistance: The Secret to Avoiding "Wearing the Same Clothes"

- What is Collision Resistance? Collision resistance means that it is difficult for a hash algorithm to find two different input information that can generate the same hash value. It's like when you queue to buy something, it's unlikely that two

people will have the same queue number at the same time, because the queue numbers are all unique.

- **Importance of Collision Resistance:** If the collision resistance of a hash algorithm is poor, then the private keys we generate using different passphrases may be the same. If two people have the same private key, their Bitcoin will be exposed to risk.
- **Collision Resistance of SHA-256:** The SHA-256 algorithm has very good collision resistance. It can be considered impossible for a collision to occur in practical applications.

6.4 Diffusion: Making "Information Fingerprints" More Random

- **What is Diffusion?** Diffusion means that even a tiny change in the input information will cause a huge, random change in the generated hash value. This is also known as the avalanche effect of hash algorithms. As with the previous analogy, suppose you take out a chili from your takeout order, and the takeout order number changes from 87613 to 19321, which has nothing to do with the original order number.
- **Importance of Diffusion:** Diffusion ensures that even if you change only one character in your passphrase, the generated hash value will change dramatically, and the generated private key will also be completely different. This further enhances the security of advanced brain wallets.

6.5 The Concept of Entropy: Measuring the "Randomness" of Information

- **What is Entropy?** In information theory, entropy is used to measure the uncertainty or randomness of information. The higher the entropy, the more random and unpredictable the information. You can think of entropy as an indicator of "disorder."
    - **High Entropy:** Like rolling a 100-sided die or randomly selecting a star in a vast sky, there are many possibilities for the outcome, and it is almost impossible to predict the result. Therefore, its "disorder" is high, and its entropy is also high.
    - **Low Entropy:** Like tossing a coin, there are only two possibilities: heads or tails. Or if you randomly pick a ball from a small box with only two colors, the results are relatively easy to predict. Therefore, its "disorder" is low, and its entropy is also low.

    - You can also think of entropy as the toys in your house. If your toys are arranged very neatly and clearly, then their entropy is relatively low. If your toys are piled up in a mess, and it's hard to see everything at a glance, then their entropy is relatively high.
      You roll the dice, and the more unpredictable the result, the higher the entropy. You toss a coin, and there are only two possible outcomes, so the entropy is relatively low.
- **Importance of Entropy:** In cryptography, the higher the entropy, the more secure the password and the harder it is to crack. A secure private key needs sufficient entropy. Just like a high-security safe, there needs to be enough complex password combinations to prevent it from being easily cracked, and entropy is the indicator to measure the complexity of a password.
- **Entropy of the Initial Seed and the Final Private Key:** Here, we must emphasize a counterintuitive but very important concept.
    - **Entropy of Different Inputs:** For example, the entropy of inputting 'a' is much less than the entropy of inputting '5JdVTqvNscmQiYeGGVmuFX6gb8EJVyuZ97yGodo7PrJ8nTfSVex'.
    - **Consistency of Hash Value Entropy:** But due to the diffusion of SHA-256, the entropy of the hash value of sha256('a') and the hash value of sha256('5JdVTqvNscmQiYeGGVmuFX6gb8EJVyuZ97yGodo7PrJ8nTfSVex') are mathematically equal. That is, after one hash algorithm, no matter how low the entropy of the input initial value is, the entropy of the output hash value is high enough and can be regarded as a uniformly distributed random number.
    - **Hash Chaining Does Not Increase the Entropy of the Final Seed:** No matter how many steps of hash chaining are performed, it does not actually increase the entropy of the final passphrase used for generating the private key. As long as it is not a plain text string to make the last passphrase when generating the private key, then since the entropy is large enough, the collision resistance of the calculation process of the last step of private key generation is qualified. That is, after hashing, the entropy of the initial seed is no longer important; what is important is the safety of our final private key.

6.6 Why Do We Need Multiple Hashing and Emphasize the Importance of Rules? - The Key to Preventing Dictionary Attacks

Since one hashing operation can make the seed entropy high enough, why do we need multiple hashing, adding salt, and emphasize the importance of rules? This is because we also need to prevent dictionary attacks.

- **Purpose of Hash Chaining:** Multiple hashing operations (i.e., hash chaining) and adding salt are not to increase the entropy of the final seed (the first hashing has already maximized the entropy). Instead, it is to prevent the risk of dictionary attacks.
- **The Cracking Principle of One-Dimensional Brain Wallets:** The reason why one-dimensional brain wallets can be cracked is because they use public hashing algorithms, and most of the passphrases are relatively simple. Hackers only need to establish a dictionary of commonly used passphrases, then hash the passphrases in the dictionary, and compare the calculation results to crack your private key.
- **The Protection Principle of Advanced Brain Wallets:** The core of advanced brain wallets lies in protecting the rules you use to generate private keys. These rules include:
    - What information you use as the initial seed.
    - What salt value you use.
    - How many hashing operations you perform.
    - What hash algorithm you use.
    - **The Importance of Rule Confidentiality:** As long as the rules you use are complex enough and are not leaked, even if hackers know your passphrase, they will not be able to crack your private key. Because they cannot know your rules, they cannot build a dictionary, and they cannot carry out targeted cracking. This is like your door is invisible; they don't even know where the door is, so how can they pick the lock?

6.7 How to Use This Knowledge to Design Safer, More Inheritable Advanced Brain Wallets? - The "Information Pointer Memory Method"

Now that we understand concepts such as hash algorithms, collision resistance, diffusion, and entropy, we can apply this knowledge to design our advanced brain wallet scheme.

Here, we reiterate the importance of the "Information Pointer Memory Method" and add some suggestions on the selection of brain passphrases, salt values, and "key brain passphrases":

- **What is the Information Pointer Memory Method?** This is a new password generation and memorization strategy. It does not require you to memorize complex strings; instead, it converts complex strings into directional information that is easy for you to remember. It's like a treasure map. You don't need to remember the exact location of the treasure; you just need to remember the locations marked on the treasure map and then follow the map to find the treasure.
- **Selection of Initial Brain Passphrases:**
  - **Avoid Using Overly Common Information:** Try to avoid using common poems, lyrics, movie quotes, etc., as initial passphrases. This information is easily collected by hackers, increasing the risk of cracking.
  - **Add Unique Personal Information:** You can add unique personal information, such as the name of your first love and the location of your first meeting, the nickname of your child and their school enrollment number, or the names and birthdays of your parents, etc. This information is not only easy to remember but also makes your brain passphrase more unique, reducing the risk of cracking.
    - **Use BIP39 Mnemonic Phrases:** You can even use BIP39 to generate a set of mnemonic phrases to become a part of your initial brain passphrase.
    - **Security Analysis:** Since BIP39 itself is highly random, it can be used as one of your initial brain passphrases, greatly increasing the complexity and uniqueness of the passphrase.
    - **Memorization Method:** You do not need to directly remember the mnemonic phrases. Instead, you can memorize the directional information "Mnemonic phrases generated by BIP39." You can back them up in various ways (paper, electronic devices, or even online storage) without worrying about leaking your true private keys because this set of mnemonic phrases is just part of the initial brain passphrase.
    - **Important Tips:** Do not directly use this set of mnemonic phrases as your brain passphrase; you should use it as part of the advanced brain wallet

algorithm and encrypt it through hashing, adding salt, etc.

- **Use Nostr Public/Private Keys:** Similarly, you can use the public or private key of Nostr as part of your initial brain passphrase.
- **Security Analysis:** Nostr public and private keys are also highly random strings, which can effectively increase the entropy of your initial brain passphrase and increase the difficulty of cracking.
- **Memorization Method:** You do not need to directly remember Nostr public/private keys. Instead, you can memorize directional information such as "My Nostr public key" or "My Nostr private key" and back them up.
- **Important Tips:** Do not directly use Nostr public/private keys as your brain passphrase; you should use them as part of the advanced brain wallet algorithm and encrypt them through hashing, adding salt, etc.
- **Use Randomly Generated Bitcoin Key Pairs:** You can even randomly generate a Bitcoin public key, address, and private key and use them as part of your initial brain passphrase.
- **Security Analysis:** Bitcoin key pairs are also highly random strings, which can effectively increase the entropy of your initial brain passphrase and increase the difficulty of cracking.
- **Memorization Method:** You do not need to directly memorize this information. Instead, you can memorize directional information such as "My randomly generated Bitcoin key pair" and back this information up through various methods.
- **Important Tips:** Do not directly use Bitcoin key pairs as your brain passphrase; you should use them as part of the advanced brain wallet algorithm and encrypt them through hashing, adding salt, etc.
- **Flexible Combination:** You can combine multiple "information pointers" to increase the complexity and security of your private keys.

- **Meaning and Function of Salt Values:**
  - **What is a Salt Value?** A salt value is a random string that will be used together with your brain passphrase in a hash operation to generate a more complex hash value.

    - The Role of Salt Values:
        - **Preventing Rainbow Table Attacks:** A rainbow table is a pre-calculated table of corresponding hash values and original values. Traditional rainbow table attacks reverse-engineer passwords by looking up values in this table. However, if a salt value is used, even if two users use the same brain passphrase, their hash values will be completely different because the salt values are different, which invalidates the pre-calculated rainbow table. That is, even if a hacker gets your hash value, if they don't know your salt value, they cannot crack your password through rainbow table attacks.
        - **Increase Complexity:** Even if two users use the same brain passphrase, if they use different salt values, the generated private keys will be completely different, further increasing the difficulty of cracking.
        - **Guarantee the Uniqueness of the Rules:** Salt values can be combined with your rules to increase the uniqueness of your rules, ensuring your private key is more secure.
    - Suggestions for Selecting Salt Values:
        - **Easy to Remember:** Salt values also need to be easy to remember. You can set it to a meaningful date, a favorite word, or some unique numerical symbols.
        - **Maintain Uniqueness:** Salt values should also be unique, avoid using overly common character combinations, and do not record them on any physical media to avoid leakage.
- The Concept of "Key Brain Passphrases":
    - **What is a "Key Brain Passphrase"?** In our advanced brain wallet design, we introduce a unique concept called the **"key brain passphrase."** It can be one of several brain passphrases used in calculations, or it can be one of the salt values.
    - Characteristics of "Key Brain Passphrases":
        - **Very Unique and Memorable:** It is a brain passphrase that is unforgettable and absolutely unique to the user.
        - **Only Memorized in the Brain:** It cannot have any physical backups and is only memorized in the brain to ensure its absolute privacy.

        - **Not Limited by Length:** With the existence of the "Information Pointer Memory Method," its length does not matter; what matters is that it is highly unique and irreplaceable.
    - **The Role of "Key Brain Passphrases":**
        - **Last Line of Defense:** The "key brain passphrase" is our last line of defense in our advanced brain wallet. Even if other brain passphrases and algorithmic rules are leaked, as long as the "key brain passphrase" is not leaked, you can ensure that it will not be cracked in the short term.
        - **Inheritability:** When designing an advanced brain wallet, the algorithmic rules can vary widely, like the Dugu Nine Swords, where the absence of a fixed move is more effective than any fixed move (which can be disclosed to family members). Several brain passphrases and salt values can also be backed up in multiple locations (which do not have to be disclosed to family members but can be locked in a safe). However, the "key brain passphrase" must be remembered by yourself and your family members and must not be recorded in the physical world. This design ensures safety while allowing your family to inherit your Bitcoin assets when necessary by using the backed-up algorithmic rules, other brain passphrases and salt values, and the key brain passphrase that you and your family members remember. This is called the "inheritability" of advanced brain wallets.

- **How to Use the "Information Pointer Memory Method" to Design Advanced Brain Wallets:**

1. **Choose Meaningful Information:** You can choose a piece of poetry you like, a sentence, lyrics, a story, a movie, or a date, etc., as your source of information.
2. **Set Rules:** Set a set of rules that belong to you, for example: take the nth character or nth word from this piece of information and hash these characters or words to generate your private key.
3. **Flexible Combination:** You can combine multiple "information pointers" to increase the complexity and security of your private keys.
4. **Add Salt Values:** On the basis of the information source, you can add some salt values that are unique to you, or combine different information sources for use.

5. **Use Key Brain Passphrases:** In the last step of the hashing operation, use the key brain passphrase as the last variable to participate in the calculation, ensuring that only you can completely control your private keys.

- **Emphasis on the Uniqueness and Hiding of the Rules:** The key to advanced brain wallets is the uniqueness and hiding of the rules. You need to ensure that only you know these rules and that others cannot easily guess them.

6.8 Summary: Use Security Foundations to Build Your Security Fortress

After studying the knowledge in this chapter, we have understood the cryptographic concepts such as hash algorithms and how to use the "information pointer memory method" to design advanced brain wallets. We know that the core of advanced brain wallets is to hide the rules, not to increase the initial entropy. We can combine various information sources, use hash algorithms to generate private keys, and store our private keys in our heads with a high degree of security. At the same time, we need to add personal information, use salt values rationally, use "key brain passphrases", and use BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs to make our brain passphrases more unique and secure while also considering the inheritability of advanced brain wallets.

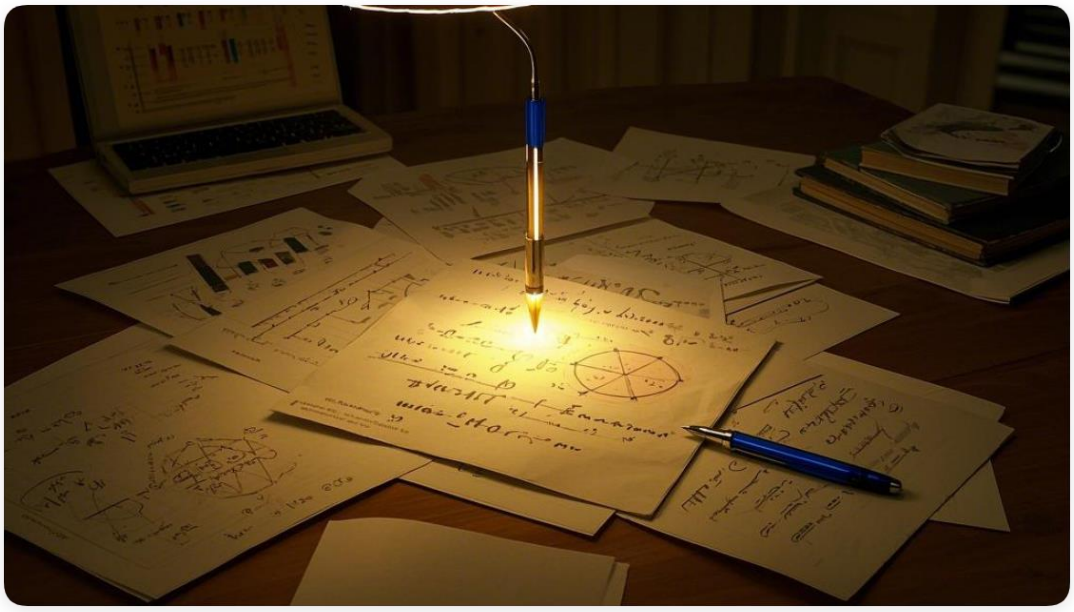
Answers to Previous Chapter Quiz:

1. What are the risks of "one-dimensional brain wallets"?
   Answer: "One-dimensional brain wallets" are at risk of having weak passphrases, memory loss, leakage, and reliance on personal memory. They also risk being subjected to dictionary attacks and are easily repeated with others.
2. What is the biggest difference between advanced brain wallets and ordinary brain wallets ("one-dimensional brain wallets")?
   Answer: Advanced brain wallets do not rely on a simple passphrase; instead, they design a complex set of algorithmic rules to generate private keys.
3. What is the core idea of advanced brain wallets?
   Answer: The core idea of advanced brain wallets is to hide the rules rather than increase the initial entropy.

This Chapter Quiz:

1. What is a hash algorithm? What are its characteristics?
2. What is collision resistance? Why is it important?
3. What is diffusion? What is its purpose?
4. What is entropy? What is its significance in cryptography?
5. Is the entropy of the initial seed the same as that of the hash value? Why?
6. What is the purpose of hash chaining? Is it to increase the entropy of the seed?
7. What issues should we pay attention to when selecting initial brain passphrases and salt values?
8. What is a "key brain passphrase"? What are its characteristics and roles?
9. How can BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs be used as part of the initial brain passphrase?
10. What is the core of advanced brain wallets?
11. How do advanced brain wallets achieve inheritability?

Chapter 7: Designing Your Advanced Brain Wallet Algorithm - Creating Your Unique "Secret Recipe"



7.1 Design Principles: Flexibility, Security, and Memorability

After studying the previous chapters, we have understood the security foundations and design philosophy of advanced brain wallets, and we also realize that the core of advanced brain wallets is hiding the rules. Now, we can finally start designing our own advanced brain wallet algorithm!

When designing the algorithm, we need to follow these three principles:

- **Flexibility:** Your algorithm should have enough flexibility and can be adjusted according to your actual situation and preferences. Just like building with blocks, you can use different information sources, different rules, and different salt values, and you can combine them flexibly to create a unique algorithm.
- **Security:** Your algorithm must be secure enough to effectively prevent attacks from hackers. Just like the lock on your house, it must be strong enough to protect the security of your property.

- **Memorability:** Your algorithm must be easy to remember, convenient for you to use at any time, but not too simple to prevent hackers from cracking it. Just like the key to your house, it must be convenient to carry but not easy to duplicate.

7.2 Design Steps: A Wonderful Journey from Seed to Private Key

Designing an advanced brain wallet algorithm is like taking a wonderful trip, starting with the seed, going through several steps, and finally reaching our destination - the private key.

Below, I will explain in detail the steps for designing an advanced brain wallet:

1. **Select Initial Brain Passphrases:**
    - **Follow the Pointer Memory Method:** We can use the "Information Pointer Memory Method" to convert complex strings into directional information that is easy for you to remember, such as your favorite poems, stories, movie quotes, or combine it with unique personal information such as the name of your first love or your child's birthday.
    - **BIP39, Nostr, and Bitcoin Key Pairs:** You can also use BIP39 to generate a set of mnemonic phrases, use the public/private keys of Nostr, or even randomly generated Bitcoin key pairs, and use them as part of your initial brain passphrase. This information is highly random and can be easily backed up. But please remember that this information is just a part of your initial brain passphrase and not directly used to generate the private key. You still need to process it using your own rules.
2. **Select Salt Values:**
    - **Increase Complexity:** Salt values can increase the complexity of the hash operation and prevent rainbow table attacks.
    - **Ensure Uniqueness:** Salt values can be combined with your rules to increase the uniqueness of your rules.
    - **Easy to Remember and Unique:** Salt values need to be easy to remember and unique. You can set them to a meaningful date, a favorite word, or some unique numerical symbols, but remember not to record them on any physical media to avoid leakage.
3. **Determine the Number of Hashing Operations:**

- **Hash Chaining:** Multiple hash operations can increase the difficulty of cracking.
- **Personalized Settings:** You can set a fixed number of hashing operations, or you can link it to your brain passphrase or birthday, etc.
- **Specific Process of Hash Chaining:** In advanced brain wallets, we recommend using a hash chaining process like this: Each time you hash, use the result of the previous operation as the new passphrase, concatenate it with the salt value, and perform the next hash operation. This method makes each hash operation more complex and has a better avalanche effect.

4. **Determine the Hashing Algorithm:**
   - **Choose Safe Algorithms:** You can choose a safe hash algorithm such as SHA-256.
   - **Flexibility:** You can also choose to mix multiple hash algorithms to increase complexity. However, it is recommended to use SHA-256 for the final step.
5. **Introduce a "Key Brain Passphrase":**
   - **Last Line of Defense:** Add your "key brain passphrase" to a step in the process as an input to a certain hash operation, thereby ensuring that even if other brain passphrases or algorithm steps are leaked, your private key cannot be cracked.
   - **Only Exists in the Brain:** The key brain passphrase only exists in your brain and is not recorded on any physical media.
6. **Set Up Multiple Addresses:**
   - **Use Sequence Numbers:** You can generate different addresses by changing the sequence numbers, which is convenient for managing your Bitcoin assets.
   - **Use Variables:** You can also generate different addresses by changing the number of hashing operations or other variables.
   - **Layered Storage:** You can use different addresses to receive Bitcoin from different sources, thereby protecting your privacy.

7.3 Designing Advanced Brain Wallet Algorithms

Before we start using tools to generate addresses, we need to design our own advanced brain wallet algorithm. Please remember that the core of advanced brain wallets is to hide the rules, not to increase the initial entropy. You need to use the "Information Pointer Memory

Method" flexibly and combine it with your personal situation to design a unique algorithm.

Here are some examples for your reference:

- **Example 1: Based on Poetry and Salt Values**
  1. **Initial Brain Passphrase:** "I first saw the moon on my 5th birthday."
  2. **Salt Value:** "When will the moon be clear? I ask the blue sky while drinking wine."
  3. **Number of Hashing Operations:** Use the last four digits of the current Bitcoin block height.
  4. **Hashing Algorithm:** SHA-256
  5. **Key Brain Passphrase:** The name of your first love.
  6. **Rules:**
     - Concatenate the initial brain passphrase, sequence number, key brain passphrase, and salt value.
     - Hash Chaining: Hash the concatenated string using SHA-256. The result of the first hash will be used as the passphrase for the next hash operation and concatenated with the salt value until the number of hash operations meets the condition.
     - If needed, change the sequence number to generate different addresses.
- **Example 2: Based on Stories and Personal Information**
  1. **Initial Brain Passphrase:** "When I was in the third grade of elementary school, I found a strange rock on the hill behind the school."
  2. **Salt Value:** Your mother's birthday.
  3. **Number of Hashing Operations:** The last two digits of your child's school enrollment number.
  4. **Hashing Algorithm:** SHA-256
  5. **Key Brain Passphrase:** The chorus of your favorite song.
  6. **Rules:**
     - Concatenate the sequence number, the story, and the salt value.
     - Hash Chaining: Hash the concatenated string using SHA-256. The result of the first hash will be used as the passphrase for the next hash operation and concatenated with the salt value until the number of hash operations meets the condition. Then, use the key brain passphrase to perform the last hash.
     - If needed, change the sequence number to generate different addresses.

- Example 3: Based on BIP39, Nostr, and Date
    1. Initial Brain Passphrase: Use BIP39 to generate a set of 12 mnemonic phrases and remember the directional information “I used BIP39 to generate a set of mnemonic phrases.” Use the public key of Nostr and remember the directional information "My Nostr public key."
    2. Salt Value: The date of your wedding anniversary.
    3. Number of Hashing Operations: Add up the single digits from the day, month, and year of your wedding anniversary.
    4. Hashing Algorithm: SHA-256
    5. Key Brain Passphrase: The name of your favorite movie.
    6. Rules:
        - Concatenate the sequence number, the mnemonic phrases, the Nostr public key, and the salt value.
        - Hash Chaining: Hash the concatenated string using SHA-256. The result of the first hash will be used as the passphrase for the next hash operation and concatenated with the salt value until the number of hash operations meets the condition. Then, use the key brain passphrase to perform the last hash.
        - If needed, change the sequence number to generate different addresses.

Please think carefully about the above examples and modify and innovate them based on your own situation to design a unique algorithm.

7.4 Summary: Design Your Exclusive "Encryption Secret Recipe"

Through studying this chapter, we have understood the principles and steps for designing advanced brain wallet algorithms and learned how to use the “Information Pointer Memory Method.” Now, you can use your wisdom to create a unique “encryption secret recipe” to safely manage your Bitcoin assets.

For more detailed examples and practical operations, please refer to the practical section in Chapter 14.

Answers to Previous Chapter Quiz:

1. What is a hash algorithm? What are its characteristics?
   Answer: A hash algorithm is an algorithm that converts input

information of any length into fixed-length output information. Its characteristics are one-way, fixed-length output, and the avalanche effect.

2. What is collision resistance? Why is it important?
   Answer: Collision resistance means that it is difficult for a hash algorithm to find two different input information that can generate the same hash value. It ensures the uniqueness of the private key.
3. What is diffusion? What is its purpose?
   Answer: Diffusion means that any small change in the input information will cause a huge and random change in the generated hash value. It ensures the randomness and collision resistance of the private keys.
4. What is entropy? What is its significance in cryptography?
   Answer: Entropy is a concept that measures the uncertainty or randomness of information. In cryptography, the higher the entropy, the more secure the password.
5. Is the entropy of the initial seed the same as that of the hash value? Why?
   Answer: The entropy of the initial seed is not the same as that of the hash value. The entropy of the initial seed may be low, but after using a hash algorithm, the entropy of its hash value is high enough and can be regarded as a uniformly distributed random number.
6. What is the purpose of hash chaining? Is it to increase the entropy of the seed?
   Answer: The purpose of hash chaining is not to increase the entropy of the seed but to prevent dictionary attacks.
7. What issues should we pay attention to when selecting initial brain passphrases and salt values?
   Answer: Using the "Information Pointer Memory Method" can reduce the difficulty of memorization, increase the width of information sampling, and use various combinations of information sources.
8. What is a “key brain passphrase”? What are its characteristics and functions?
   Answer: A "key brain passphrase" is a brain passphrase that is unforgettable and absolutely unique to the user and is only stored in the brain, not recorded in any physical space. It is the last line of defense for advanced brain wallets and also plays an important role in family inheritance.
9. How can BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs be used as part of the initial brain passphrase?

Answer: BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs can be used as part of the initial brain passphrase and further processed in subsequent hash operations to improve the randomness and uniqueness of the brain passphrase.

10. What is the core of advanced brain wallets?
    Answer: The core of advanced brain wallets is to hide the rules rather than increase the initial entropy.
11. How do advanced brain wallets achieve inheritability?
    Answer: The inheritability of advanced brain wallets means that, while ensuring security, family members can inherit the user's Bitcoin assets when necessary by using the backed-up algorithmic rules, other brain passphrases and salt values, and the key brain passphrase that the user and family members remember together.

This Chapter Quiz:

1. What principles should be followed when designing advanced brain wallet algorithms?
2. What are the main steps for designing an advanced brain wallet algorithm?
3. What is the "Information Pointer Memory Method," and how can it be used to design an advanced brain wallet?
4. What are some suggestions for choosing initial brain passphrases?
5. How can BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs be used when designing an advanced brain wallet?

Chapter 8: Using Tools to Generate Addresses - Safely Verifying Your "Encryption Secret Recipe"

8.1 Why Do We Need Tools? - Leave Professional Tasks to Professional Tools

In the last chapter, we learned how to design advanced brain wallet algorithms. Now, we need to put the algorithms we designed into practice and generate private keys and addresses. Although theoretically we can manually calculate the hash values, this method is inefficient and error-prone. Therefore, we need to use professional tools to complete this task.

Just like when we want to build a house, we need to use a cement mixer instead of mixing cement by hand. Using professional tools can make our tasks easier and more efficient and ensure the accuracy of the results.

8.2 Choosing Suitable Tools: Open Source, Secure, and Offline

When choosing tools, we need to pay attention to the following:

- Open Source: Try to choose open-source tools. Open source means that the code is open and transparent, and anyone can view and verify the code, thus ensuring the security of the tool. When

we choose a restaurant to eat at, we also try to choose restaurants with an open kitchen so that we can see if the ingredients are fresh and whether the cooking process is hygienic.

- **Secure:** When choosing a tool, ensure that the source of the tool is reliable and that there are no backdoors or malicious code. Just like when we choose to shop online, we try to choose merchants with a good reputation to avoid buying fake or inferior products.
- **Offline:** When generating private keys and addresses, be sure to operate in an offline environment to avoid leaking private keys. Just like when we withdraw a bank card password, we try to do so in a safe environment to avoid being spied upon by others.

In the previous chapter, we recommended DaGe's (@btcdage) open-source Python advanced brain wallet tool, which meets the above requirements. It can be found on Github:

- **Open Source Address:** https://github.com/btcdage2000/BrainWalletGenerator/
    - **Executable File Download Address:** https://github.com/btcdage2000/BrainWalletGenerator/releases/tag/v0.1.0

8.3 The Importance of Offline Operations: Protecting the Lifeline of Private Keys

When generating private keys and addresses, be sure to make sure your computer is offline. This is because, once your computer is connected to the internet, your private keys may be exposed to attacks from hackers.

Here are a few things to keep in mind:

- **Disconnect Network Connection:** Turn off WiFi and Bluetooth, and unplug the network cable to make sure your computer is not connected to any network.
- **Use a Dedicated Offline Computer:** If conditions permit, try to use a dedicated computer for generating private keys. Do not install any other software or connect to any network. This is the safest method.
- **USB Bootable Offline System:** If you do not have a dedicated offline computer, you can use a USB flash drive to boot an offline operating system. This is more secure than using a

virtual machine because a virtual machine still relies on the security of the host machine. If conditions allow, unplug the data cable or power cord of the local hard drive to improve security.

- **Virtual Machine:** You can run the tool in a virtual machine, but the virtual machine still relies on the security of the host machine. If the host machine already has a virus, it may take screenshots of the virtual machine, so a virtual machine is a last resort.
- **Do Not Screenshot:** Do not take screenshots of the generated private keys and addresses to avoid information leakage.
- **Clear Browser Cache in Time:** If you use a browser-based JS tool to generate private keys, remember to clear your browser cache in time to avoid residual information.

8.4 Using DaGe's Python Tool to Generate Addresses: Step-by-Step Instructions

Now, let's go into detail about how to use DaGe's Python tool to generate addresses:

1. **Download the Tool:**
    - **Download Source Code:** Download DaGe's open-source Python tool from Github and save it to your computer.
    - **Download Executable File:** You can also download the compiled executable file from the Github Release page, which eliminates the need to install a Python environment.
        - **Download Address:** https://github.com/btcdage2000/BrainWalletGenerator/releases/tag/v0.1.0
2. **Disconnect Network Connection:** Follow the above requirements to disconnect your computer's network connection and ensure that your computer is offline.
3. **Run the Tool:**
    - **Run the Source Code:** If you choose to download the source code, you need to install Python 3.6 or higher first. Then, in the terminal or command prompt, enter the command python brain_wallet_generator.py to run the tool.
    - **Run the Executable File:** If you downloaded the executable file, you can run it directly without installing a Python environment.
4. **Concatenate Initial Information:**
   Important Tip: DaGe's tool is only responsible for the hash

chaining and salting operations. Therefore, you need to concatenate all the information that needs to be spliced, such as the initial brain passphrase, salt value, sequence number, and "key brain passphrase," according to your designed rules. Then, enter the concatenated string into the "Passphrase / 脑口令" input box.

    - **Enter Brain Passphrase:** You need to concatenate all the information you need to splice, such as your initial brain passphrase, salt value, the sequence number you calculated, and even the final "key brain passphrase" according to the rules you designed, and then enter the concatenated string into the "Passphrase / 脑口令" input box.
    - **Enter Salt Value:** If your algorithm uses a salt value, you need to enter the salt value you selected in the "Salt / 加盐" input box.
5. **Set the Number of Hashing Operations:** In the "Hash Times / 哈希次数" drop-down menu, select the number of hashing operations that you set.
6. **Generate Keys:** Click the "Generate Brain Wallet / 开始计算" button, and the tool will perform calculations according to your set hash chaining process to generate information such as private keys, public keys, P2PKH addresses, and Bech32 addresses.
7. **Back Up Addresses:** Back up the generated P2PKH addresses and Bech32 addresses separately. You can write them down on paper or copy them to a USB drive. Please make sure that the addresses you copy match the addresses displayed in the tool.
8. **Clear Information:** Click the "Clear All / 清空所有" button to clear all information to avoid leakage.

8.5 Verify Addresses: Ensure Address Accuracy

To ensure that the generated addresses are correct, we need to verify them.

- **Use Wallets such as Electrum:** You can use wallet software such as Electrum to import your private keys and then verify whether the generated addresses are correct.
    - **Precautions:** Please be sure to perform the import and verification operations offline to avoid private key leaks.

8.6 Summary: Safely Generate Your "Encryption Secret Key"

In this chapter, we learned how to use tools to generate private keys and addresses for advanced brain wallets and emphasized the importance of offline operations. Now that you have your "encryption secret recipe," you can start managing your Bitcoin assets safely.

Answers to Previous Chapter Quiz:

1. What principles should be followed when designing advanced brain wallet algorithms?
   Answer: When designing advanced brain wallet algorithms, the principles of flexibility, security, and memorability should be followed.
2. What are the main steps for designing an advanced brain wallet algorithm?
   Answer: The main steps include selecting the initial brain passphrase, selecting salt values, determining the number of hashing operations, determining the hashing algorithm, introducing a "key brain passphrase," and setting up multiple addresses by changing sequence numbers.
3. What is the "Information Pointer Memory Method," and how can it be used to design an advanced brain wallet?
   Answer: The "Information Pointer Memory Method" is a method of converting complex strings into easy-to-remember directional information. You can use poems, stories, songs, news, etc., as information sources and convert them into brain passphrases by using rules.
4. What are some suggestions for choosing initial brain passphrases?
   Answer: When choosing initial brain passphrases, you should avoid using overly common information and try to add unique personal information or use high-entropy information such as BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs as a part of it.
5. How can BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs be used when designing an advanced brain wallet?
   Answer: You can use BIP39 mnemonic phrases, Nostr keys, and randomly generated Bitcoin key pairs as part of the initial brain passphrase and further process them in subsequent hashing operations to improve the randomness and uniqueness of the brain passphrase.

This Chapter Quiz:

1. Why do we need to use tools to generate addresses for advanced brain wallets?
2. What aspects do we need to pay attention to when choosing a generation tool?
3. Why is offline operation very important when generating private keys?
4. What steps should be taken when using DaGe's Python tool to generate addresses?
5. After generating addresses, how do we verify the correctness of the addresses?
6. What precautions should be taken when verifying addresses using wallets such as Electrum?
7. What is the function of DaGe's Python tool? How should you use it to implement the advanced brain wallet algorithm you designed?

Chapter 9: Secure Storage and Backup - Protecting Your "Encryption Secret Recipe"

9.1 Why Do We Need Secure Storage and Backup? - Prepare for a Rainy Day, Prevent Problems Before They Occur

In the last chapter, we learned how to use tools to generate addresses for advanced brain wallets. Now that we have our private keys and addresses, it is like we have built a house. Next, we need to consider how to protect it.

In advanced brain wallets, the key information we need to protect includes:

- **Algorithmic Rules:** The steps and methods you use to generate your private keys, including the hash algorithms you selected, salt values, and the number of hashing operations.
- **Brain Passphrases:** The initial passphrases you use to generate your private keys, including the poems, stories, and personal information you use, etc.
    - **Key Brain Passphrase:** Your unique key brain passphrase that serves as the last line of defense.
- **Salt Values:** The salt values you use to increase complexity.

This information is like the foundation, load-bearing walls, and door locks of our house. If it is lost or leaked, your house is in danger. Therefore, we need to take the storage and backup of this information seriously to ensure its safety.

9.2 The Special Nature of the "Key Brain Passphrase": Only Remembered in the Brain, Not Written Down

In advanced brain wallets, the "key brain passphrase" plays a very special role:

- **Last Line of Defense:** It is the last line of defense for our advanced brain wallet. Even if other information is leaked, as long as it is not lost, the security of your Bitcoin assets can be guaranteed.
- **Unique:** It only exists in your brain and should not be recorded on any physical media.
- **Unforgettable:** It should be unforgettable and unique information in your memory.

Therefore, the storage strategy of the "key brain passphrase" is different from other information:

- **Storage Method:** It can only exist in your brain and cannot be recorded on any paper, electronic device, or any other form of physical media.
- **Memorization Method:** You can use the "Information Pointer Memory Method" to associate the "key brain passphrase" with a special experience in your life to ensure that it is unforgettable and difficult to forget.
- **Passing Method:** It can be passed verbally to the most trusted family members to ensure that they understand the meaning and importance of the "key brain passphrase."

9.3 Backup Strategies for Algorithmic Rules: Print Multiple Copies and Store Them Separately

Algorithmic rules are the core of your advanced brain wallet. You need to make meticulous backups of them to ensure that they are not lost.

- **Print Multiple Copies:** Print multiple copies of your algorithmic rules. We recommend at least three copies.
    - **Avoid Single Points of Failure:** Multiple copies can prevent the loss or damage of a single copy.

- **Store Separately:** Store the printed algorithmic rules in different safe locations.
    - **Safety Deposit Box:** You can store one copy in a bank safety deposit box to ensure its safety.
    - **Hidden Corner at Home:** You can store another copy in a hidden corner at home, but make sure only you know about it.
    - **Trusted Family Members:** Give one copy to the family member you trust the most.
- **Regular Review:** Check your algorithmic rules regularly to make sure your backups are complete and that there are no omissions or errors.

9.4 Backups for Other Brain Passphrases and Salt Values: Flexible Choices, Multiple Safeguards

For other brain passphrases and salt values other than the "key brain passphrase," you can flexibly choose a suitable backup method:

- **Physical Backups:** You can write them down on paper or print them out, and then store them in different safe locations, such as a safety deposit box or a hidden corner at home.
    - **Avoid Physical Risks:** Pay attention to waterproofing, fireproofing, and insectproofing to avoid paper loss or damage.
- **Digital Backups:** You can also encrypt them and store them on mobile devices such as USB drives, portable hard drives, or in cloud storage such as cloud drives.
    - **Encryption Security:** Use encryption software to encrypt backup files to ensure that your information is not leaked even if your mobile device is lost or your cloud account is stolen.
- **Multiple Backups:** You can combine physical backups and digital backups to implement multiple safeguards.
    - **Double Insurance:** Multiple backup methods can increase the reliability of backups, and if one backup method fails, you can use other backup methods to recover.

9.5 Inheritability: Preparing for the Future

The design of advanced brain wallets should not only consider security but also inheritability, which is how your family can inherit your Bitcoin assets if something happens to you:

- **Inform Your Family:** Inform your family about your advanced brain wallet rules in advance and verbally teach them your "key brain passphrase."
    - **Communicate in Advance:** Communicating in advance can ensure that your family members know how to use advanced brain wallets and how to correctly inherit your Bitcoin assets.
- **Multiple Backups:** Ensure that your family members know the location of your backup information. For example, tell them where the key to your bank safety deposit box is and which USB drive or portable hard drive you backed up other brain passphrases and salt values on.
    - **Multiple Safeguards:** Multiple backups can ensure that even if your family members do not know your "key brain passphrase," they can transfer your Bitcoin assets in a timely manner if they know the other brain passphrases and rules.
- **Legal Documents:** You can also write the inheritance of Bitcoin assets into legal documents such as a will to ensure a smooth transfer of assets.
    - **Legal Protection:** Using legal documents can maximize the safe inheritance of your Bitcoin assets.
    - **Tip:** You should consult with legal professionals to develop appropriate legal documents in accordance with the laws and regulations of your location.

9.6 Summary: Take Care of Your "Encryption Secret Recipe"

The security of advanced brain wallets not only depends on the complexity of the algorithm, but also on whether you can take good care of your algorithmic rules, brain passphrases, and salt values, and whether you are prepared for the future to ensure that your Bitcoin assets can be safely inherited.

Answers to Previous Chapter Quiz:

1. Why do we need to use tools to generate addresses for advanced brain wallets?
   Answer: We need to use tools to generate addresses for advanced brain wallets because manual calculations are inefficient and prone to errors.
2. What aspects do we need to pay attention to when choosing a generation tool?

Answer: When choosing a generation tool, we need to pay attention to open source, security, and offline operation.

3. Why is offline operation very important when generating private keys?
   Answer: Offline operation is very important when generating private keys because it can prevent private keys from being leaked.
4. What steps should be taken when using DaGe's Python tool to generate addresses?
   Answer: When using DaGe's Python tool to generate addresses, you need to first download the tool, disconnect the network, then enter the initial information, generate the keys, back up the addresses, and finally clear the information.
5. After generating addresses, how do we verify the correctness of the addresses?
   Answer: After generating addresses, you can use wallets such as Electrum to verify the correctness of the addresses.
6. What precautions should be taken when verifying addresses using wallets such as Electrum?
   Answer: When verifying addresses using wallets such as Electrum, you need to ensure that the operation is performed offline.
7. What is the function of DaGe's Python tool? How should you use it to implement the advanced brain wallet algorithm you designed?
   Answer: The function of DaGe's Python tool is to perform hash chaining and salting operations. You need to splice the initial brain passphrase and salt values together according to the rules you designed, then enter the result as a parameter, and run the tool to generate private keys.

This Chapter Quiz:

1. What key information do we need to protect in advanced brain wallets?
2. What is the special nature of the "key brain passphrase" in advanced brain wallets? How should it be stored?
3. How do you back up your algorithmic rules?
4. How do you back up your other brain passphrases and salt values?
5. What is the "inheritability" of advanced brain wallets? Why is it important?

6. How will you ensure that your family can inherit your Bitcoin assets when necessary?

Chapter 10: HD Wallets, Derivation Paths, and Multiple Addresses

10.1 HD Wallets: One Seed, Infinite Possibilities

In Bitcoin wallets, in addition to advanced brain wallets, there is another common type of wallet called an HD wallet, which stands for Hierarchical Deterministic Wallet.

- **The Principle of HD Wallets:** The core of an HD wallet is the use of a seed. Just as one seed can grow into countless trees, this seed can be used to generate countless private keys and addresses. You can think of an HD wallet as a "keychain." With just one master key, countless different keys can be generated, and each key can open a different door. This "seed" is usually composed of 12, 18, or 24 mnemonic phrases, which represents the root for generating all private keys and addresses.
- **Master Private Key and Master Public Key:** HD wallets first generate a master private key and a master public key based on the seed. They are the roots of all private keys and addresses. The master private key and master public key are like your "master key" and "master lock." They can generate other keys and locks.

- **BIP32 and BIP44:** To standardize the operation of HD wallets, the Bitcoin community has developed some standards, such as BIP32 and BIP44. They define rules on how to generate private keys and addresses based on the master private key, ensuring that different wallets can be compatible.

10.2 Derivation Paths: A "Roadmap" for Generating Keys

- **What are Derivation Paths?** HD wallets use derivation paths to generate different private keys and addresses. A derivation path is like a "roadmap." It tells the HD wallet how to generate specific private keys and addresses based on the master private key. A derivation path is like your "address book." Every time you need to use an address, the HD wallet will generate the corresponding address according to the roadmap recorded in the "address book."
- **The Structure of Derivation Paths:** Derivation paths are usually composed of a string of numbers and slashes, such as m/44'/0'/0'/0/0. Where m represents the master private key and the numbers represent different path levels.
- **The Role of Derivation Paths:** Through different derivation paths, HD wallets can generate countless different private keys and addresses, which facilitates users to manage and isolate assets.

10.3 Multiple Addresses: A "Separation Technique" for Managing Assets

- **Multiple Addresses of HD Wallets:** HD wallets use derivation paths to generate multiple different addresses, called multiple addresses. This is like having multiple bank accounts where you can store different assets in different accounts, which is convenient for management.
- **Benefits of Multiple Addresses:**
    - **Convenient Management:** You can store Bitcoin for different purposes in different addresses, which is convenient for management and tracking.
    - **Improved Privacy:** Using multiple addresses can increase the anonymity of transactions, avoiding the association of all your Bitcoin with the same address.

10.4 Differences in Thinking Between Advanced Brain Wallets and HD Wallets: Manual Generation vs. Automatic Derivation

Although both HD wallets and advanced brain wallets are tools for managing private keys and addresses, their design philosophies are quite different:

- HD Wallets:
  - Reliance on a Seed: They rely on a seed to generate all private keys and addresses. This seed is the root of all private keys. Having the seed gives you control over all the private keys.
  - Automatic Derivation: They use derivation paths to automatically derive private keys and addresses.
  - Centralized Management: All private keys and addresses are derived from a single master private key. There is a connection between them.
  - Default Recommendation: Almost all wallet software uses HD wallets by default.
- Advanced Brain Wallets:
  - Independent Generation: They do not rely on a single seed. Instead, they use a series of complex rules to generate private keys and addresses. You can think of the rules as the seed, but you have full control over the rules and you can flexibly customize them.
  - Manual Generation: They require manual design of the algorithm to generate different private keys and addresses.
  - Independent Addresses: There is no necessary connection between the addresses you manually generate.
  - Privacy First: The design concept of advanced brain wallets is to pursue extreme security, privacy, independence, and flexibility.

10.5 The Philosophy of Advanced Brain Wallets: Manual Management, Privacy First, Defense Against Quantum Supremacy, Ensuring Secure Coin Receipt

The core philosophy of advanced brain wallets is manual management, privacy first, defense against quantum supremacy, and ensuring secure coin receipt, and they adhere to the following principles:

- Manually Generate Addresses: We prefer to design algorithms manually and then generate different addresses, rather than relying on HD wallets to automatically derive them.
- Use One Address Only Once: We emphasize the principle of "use one address only once." Each time a new Bitcoin is received, a new address is used to avoid linking different transactions.

    - Why "Use One Address Only Once":
        - **Protect Privacy:** On the blockchain, all transaction records are public. If multiple transactions use the same address, then your assets will be exposed to the public view, resulting in low privacy.
        - **Defend Against Quantum Supremacy:** More importantly, in Satoshi Nakamoto's design, your public key is exposed on the blockchain as soon as you initiate a Bitcoin transfer. Once exposed, you will face the threat of future quantum computers. Therefore, for security reasons, a new address is used for each transfer to prevent your Bitcoin from being exposed to the threat of quantum supremacy.
        - **Ensure Secure Coin Receipt:** In addition, "use one address only once" can also ensure the address security when storing Bitcoin because your address is absolutely safe before it is used. You do not need to generate the corresponding private key, nor do you need to import it into any wallet.
- **Change Address:** When we conduct a Bitcoin transfer, we set the change address to another new address generated by advanced brain wallets, rather than the default old address. You can use a new address as the change address for each transaction. This can effectively improve the privacy of the transaction.
- **Avoid Centralized Management:** We do not prefer to use mnemonic phrases generated by tools such as BIP39 and use these mnemonic phrases to derive all addresses. Instead, we recommend that you use advanced brain wallets to manually manage and generate different addresses, so that there is no necessary connection between the addresses and they are safer.
- **Security of the Source Address After Transfer:** Because we adhere to the principle of "use one address only once," when you need to transfer funds, you can temporarily import the private key corresponding to the address into a hot wallet. After the transfer is completed, set the change address to another unexposed public key address generated by the advanced brain wallet. In this way, even if you publicly release the private key corresponding to the source address or if the hot wallet is hacked, it will not pose a threat to your assets because the source address has been discarded and is no longer used.

10.6 Summary: The Uniqueness of Advanced Brain Wallets

In this chapter, we learned about the concepts of HD wallets, derivation paths, and multiple addresses, and we compared their design philosophies with those of advanced brain wallets. We know that an advanced brain wallet is not a simple "keychain" but a more flexible and secure private key management solution. It pays more attention to manual management, privacy first, defense against quantum supremacy, and ensuring secure coin receipt.

Answers to Previous Chapter Quiz:

1. What key information do we need to protect in advanced brain wallets?
   Answer: In advanced brain wallets, the key information we need to protect includes the algorithmic rules, brain passphrases (including the "key brain passphrase"), and salt values.
2. What is the special nature of the "key brain passphrase" in advanced brain wallets? How should it be stored?
   Answer: The "key brain passphrase" in advanced brain wallets is the last line of defense. It is only memorized in the brain, not recorded on any physical media, and it is unforgettable.
3. How do you back up your algorithmic rules?
   Answer: When backing up algorithmic rules, you should print multiple copies and store them separately in different safe locations.
4. How do you back up your other brain passphrases and salt values?
   Answer: When backing up other brain passphrases and salt values, you can use a combination of physical backups and digital backups and encrypt them.
5. What is the "inheritability" of advanced brain wallets? Why is it important?
   Answer: The "inheritability" of advanced brain wallets means that, while ensuring security, family members can inherit the user's Bitcoin assets when necessary by using the backed-up algorithmic rules, other brain passphrases and salt values, and the key brain passphrase that the user and family members remember together.
6. What should you do to ensure that your family can inherit your Bitcoin assets?
   Answer: To ensure that family members can inherit Bitcoin assets, they need to be informed of the rules of the advanced brain wallet in advance, and the “key brain passphrase”

should be verbally taught to them. You also need to ensure that family members know how to find your other backed-up information.

This Chapter Quiz:

1. What is an HD wallet? What is its core?
2. What is a derivation path? What is its function?
3. What are multiple addresses? What are their benefits?
4. What is the difference in the design philosophy between HD wallets and advanced brain wallets?
5. Why do we emphasize "use one address only once"?
6. In advanced brain wallets, how do you handle the change from Bitcoin transfers?
7. In addition to privacy, why can "use one address only once" also defend against the threat of quantum supremacy?
8. How does "use one address only once" ensure the security of the address when you receive Bitcoin and the security of the original address after a transfer?

Chapter 11: Advanced Brain Security Concepts

11.1 Security is Not Absolute: Risks Are Everywhere

After studying the previous chapters, we have mastered the methods for designing and using advanced brain wallets. However, we must always remember that security is not absolute. No security measures can guarantee 100% security.

- **Risks Are Everywhere:** The Bitcoin world is full of various unknown risks, such as hacking attacks, device damage, information leaks, and even cognitive biases. These risks may cause you to lose your Bitcoin assets.
    - **Important Tip:** However, if you have mastered the essence of advanced brain wallets and generate and manage private keys offline in a secure environment according to the requirements of advanced brain wallets, then risks such as hacking attacks can be ignored at the software system level. This is precisely the advantage of advanced brain wallets. It is not afraid of vulnerabilities at the software system level.
- **Nothing is Set in Stone:** Technology is constantly developing, and new attack methods may appear. Therefore, you need to continuously learn and update your knowledge to keep up with the times to meet new challenges.

- **Stay Vigilant:** Never let your guard down. Always be skeptical about everything. Do not easily trust strangers, and do not click on unknown links.

11.2 Security Habits: Improve a Little Bit Every Day

In addition to technical security measures, we also need to develop good security habits to better protect our Bitcoin assets:

- **Continuous Learning:** Always pay attention to the latest Bitcoin security trends, understand the latest attack methods and defense methods, and adjust your security strategies according to your actual situation.
    - **Pay Attention to Security Information:** Pay more attention to articles, blogs, and forums related to Bitcoin security. Follow DaGe's Weibo and Nostr (@btcdage) and learn from the experiences and lessons of other users.
- **Regular Review:** Regularly check all aspects of your advanced brain wallet to ensure that your algorithmic rules are not forgotten, your brain passphrases are correct, and your backups are complete and reliable.
- **Cautious Operation:** When using advanced brain wallets, treat each step carefully to ensure that there are no omissions.
    - **Secure Environment Testing:** Conduct more testing of advanced brain wallets in offline mode to ensure that no problems will occur during actual operations.
- **Risk Awareness:** Always maintain risk awareness. Do not easily believe any unfamiliar information, and do not click on unknown links.

11.3 Security is a Self-Responsibility: No One Can Be Completely Relied Upon

In the world of Bitcoin, security is your own responsibility. No one can help you assume your security responsibilities.

- **Protect Your Own Assets:** You must be responsible for your own Bitcoin assets. Do not rely on others, and do not place your hopes on the security measures of others.
    - **Autonomous Management:** You must manage your private keys autonomously and take sufficient security measures.
- **Autonomous Management:** Manage your advanced brain wallets autonomously. Do not tell anyone your brain passphrases, rules, and salt values to avoid the risk of leaks.

    - **Do Not Rely on Others:** Do not rely on any third-party institutions, including wallet service providers, exchanges, or other individuals.
- **Assume Risks:** You need to understand that using advanced brain wallets requires taking certain risks and be willing to assume corresponding responsibilities.
    - **Risk Assessment:** You need to carefully assess the potential risks of the advanced brain wallet algorithm rules you designed and be mentally prepared.

11.4 Advanced Brain Wallet Tools: Just Tools, Security Depends on You

Advanced brain wallets themselves are just tools. Their security ultimately depends on how you use them:

- **Tools Cannot Solve All Problems:** Advanced brain wallet tools can only help you generate and manage private keys and addresses and cannot guarantee your absolute safety. You need to use it in conjunction with security concepts and complete the corresponding backup work.
    - **Use Tools Correctly:** You need to understand and use the tools correctly to avoid errors that could lead to private key leaks.
- **Security Depends on People:** The security of advanced brain wallets ultimately depends on your own awareness and behavior, your security habits, and your awareness and prevention of risks.
    - **Improve Security Awareness:** You must constantly learn and practice to truly master the essence of security.

11.5 Advanced Brain Wallets vs. Hardware Wallets: Comparison of Advantages

In terms of the secure storage of Bitcoin, in addition to advanced brain wallets, hardware wallets are also a common choice. However, after careful comparison, we can find that advanced brain wallets have greater advantages than hardware wallets in terms of security, independence, flexibility, and privacy.

- **Disadvantages of Hardware Wallets:**
    - **Cannot Verify Open Source:** Hardware wallets rely on hardware manufacturers. Their hardware design and software code often cannot be completely verified to be open-source, which creates a trust risk. You do not know

if the random seed it generates is truly random, and you do not know whether there are backdoors in its firmware. Hardware wallets are like black boxes. You cannot fully understand their internal operation mechanism. Even if they claim to be open-source, you will not use the original design drawings to make the hardware yourself.
    - **Increased Trust Costs:** Hardware wallets were invented and launched only after BIP39 appeared. They are completely unnecessary in the use of Bitcoin. They are just an additional node. More nodes mean more entities that you need to trust, which does not conform to Occam's Razor principle.
    - **Exposing Bitcoin Holding Information:** If you put a hardware wallet at home or carry it with you, you are exposing information about your Bitcoin holdings, which is unacceptable for users who value privacy. The existence of a hardware wallet in itself exposes the fact that you may own Bitcoin, which can easily attract the attention of criminals.
- **Advantages of Advanced Brain Wallets:**
    - **Can Verify Open Source:** You can choose to compile and run the source code of various open-source brain wallet tools. You can also write your own tools or make modifications to the source code of others. You have full control over the private key generation process.
    - **No Additional Trust Required:** When we use advanced brain wallets, we do not directly use BIP39 to manage private keys. Even if you use BIP39 mnemonic phrases as part of the initial brain passphrase, you can generate them with various software wallets, without spending money to buy a hardware wallet. Because it is only one of the initial brain passphrases, it is completely okay to use hot wallets.
    - **Complete Control:** If you master advanced brain wallets, hardware wallets are completely unnecessary. You no longer need to rely on any manufacturer and can completely control your Bitcoin assets.
    - **Hardware Wallets for Other Blockchains:** The only purpose of hardware wallet manufacturers is to serve other encrypted blockchains such as Ethereum, which are Turing complete, require address reuse, and require frequent authorization. However, "Bitcoin does not need hardware wallets."

    - **Higher Privacy:** All information in advanced brain wallets only exists in your brain and does not rely on any hardware devices. This can protect your privacy to the greatest extent and will not reveal that you hold Bitcoin.
- **Response to Hacking Attacks:** As long as you generate and manage private keys offline in a secure environment according to the requirements of advanced brain wallets, then risks such as hacking attacks can be ignored at the software system level. This is precisely the advantage of advanced brain wallets. It is not afraid of vulnerabilities at the software system level.

11.6 Advanced Brain Wallets vs. Multi-Signature Wallets: Streamlining is Greater Than Redundancy

In addition to hardware wallets, multi-signature wallets are also a common security solution. Multi-signature wallets allow multiple private keys to jointly manage the same Bitcoin assets. For example, a 2-of-3 multi-signature wallet requires any two out of three private keys to move assets. Although this method seems to provide better security, we can find some problems after careful analysis:

- **The "False Redundancy" of Multi-Signature:**
    - **Redundancy in Theory:** The starting point of multi-signature wallets is to provide redundancy. Even if part of the private key is lost, assets can still be managed with the remaining private keys.
    - **Actual Insufficiency:** For example, if you use three sets of BIP39 mnemonic phrases to generate three private keys for a multi-signature wallet, even if you lose any set of mnemonic phrases, as long as you keep the other two sets, you can still generate the final private key.
    - **Difficulty in Saving Mnemonic Phrases:** However, please note that even if you use the simplest plan with 12 mnemonic phrases, three sets of mnemonic phrases are already 36 mnemonic phrases. No matter what, as long as you lose any amount greater than 12 mnemonic phrases, for example, if you lose 13 mnemonic phrases, the two sets of mnemonic phrases will not be complete, and the multi-signature wallet will not work. That is, under a multi-signature situation, the number of mnemonic phrases you need to store becomes at least 24 or even more, which greatly increases the difficulty of memorization and storage.

    - **Multi-Signature Is Not a Better Choice:** Multi-signature wallets seem to provide redundancy. However, this redundancy is false. It only increases the difficulty of memorization and storage. It is a superficial form of security instead of a more reliable security solution.
- The "Streamlined Advantage" of Advanced Brain Wallets:
    - **Core is the Rules:** Although advanced brain wallets belong to single-signature management, without a redundancy mechanism, with the help of the Information Pointer Memory Method, we can manage the algorithmic rules and various brain passphrases and salt values with a variety of easy-to-remember methods. This reduces the number of elements that need to be memorized, and they are easier to back up and manage.
    - **From Complex to Simple:** The advantage of advanced brain wallets is that they provide a more streamlined security solution. Compared to multi-signature wallets that require the management of a large number of mnemonic phrases, we only need to protect the unique algorithmic rules and key brain passphrase we designed to achieve a higher level of security.
    - **Streamlined is Greater than Redundancy:** Instead of using seemingly secure and actually management-burden-increasing false redundancy, it is better to choose a more streamlined and safer advanced brain wallet.
- **Real Use Cases for Multi-Signature Wallets:** Multi-signature wallets are not completely useless. They are still very important in specific scenarios.
    - **Joint Management of Assets by Multiple Parties:** When Bitcoin assets need to be jointly controlled by multiple parties, multi-signature wallets are an ideal choice. For example, the Bitcoin assets of a company or team should not be controlled by a single person or a few individuals alone but should be jointly managed by multiple parties.
    - **Avoid Single Points of Failure:** Multi-signature can enable everyone to jointly decide on the right to use assets. This is like a safe with multiple locks, and everyone needs to open each lock at the same time to open the treasure chest. This effectively avoids single points of failure and prevents abuse of authority or accidents caused by one person or a few individuals that could lead to loss of assets.
    - **Not the First Choice for Individuals:** For personal assets, the single-signature solution of advanced brain

wallets is usually more reasonable and reliable. Multi-signature adds complexity but does not bring about actual security improvements. It is only more suitable for scenarios that require joint management and decision-making by multiple parties.

11.7 Summary: The Path to Security is Endless. Bitcoin Does Not Need Hardware Wallets, and Advanced Brain Wallets Are Better Than Multi-Signature.

The path to security is endless. Advanced brain wallets are powerful tools, but their security ultimately depends on you. We must always remain vigilant and constantly learn and improve to truly protect our Bitcoin assets. And remember that Bitcoin does not need hardware wallets. Advanced brain wallets are a more sensible choice. They have stronger privacy and security and are more streamlined and efficient than multi-signature wallets, while ensuring your safety.

Answers to Previous Chapter Quiz:

1. What is an HD wallet? What is its core?
   Answer: An HD wallet is a wallet that uses a seed to generate infinite private keys and addresses. Its core is to use a seed to generate all private keys and addresses.
2. What is a derivation path? What is its function?
   Answer: A derivation path is a "roadmap" used by HD wallets to generate different private keys and addresses. It enables HD wallets to generate countless different private keys and addresses.
3. What are multiple addresses? What are their benefits?
   Answer: Multiple addresses are multiple different addresses generated by HD wallets using derivation paths. They make it easy to manage and improve privacy.
4. What is the difference in the design philosophy between HD wallets and advanced brain wallets?
   Answer: HD wallets rely on a seed for automatic derivation and centralized management, while advanced brain wallets emphasize manual management, privacy first, independent generation, and customized rules.
5. What is the core philosophy of advanced brain wallets?
   Answer: The core philosophy of advanced brain wallets is manual management, privacy first, defense against quantum supremacy, and ensuring secure coin receipt.

6. Why do we emphasize “use one address only once”?
   Answer: In order to protect privacy, avoid linking all your Bitcoin to the same address, and, more importantly, to cope with future threats of quantum supremacy.
7. In advanced brain wallets, how do you handle the change from Bitcoin transfers?
   Answer: In advanced brain wallets, you need to set the change address to another new address generated by the advanced brain wallet, rather than the default old address.
8. In addition to privacy, why can “use one address only once” also defend against the threat of quantum supremacy?
   Answer: Because in Satoshi Nakamoto’s design, as soon as you initiate a Bitcoin transfer, your public key will be exposed on the blockchain. Once exposed, you will face the threat of future quantum computers. Therefore, “use one address only once” can prevent your Bitcoin from being exposed to the threat of quantum supremacy.
9. How does "use one address only once" ensure the security of the address when you receive Bitcoin and the security of the original address after a transfer?
   Answer: "Use one address only once" can ensure the security of your address when storing Bitcoin because your address is absolutely safe before it is used. You do not need to generate the corresponding private key, and you do not need to import it into any wallet. When you need to transfer funds, you can temporarily import the private key corresponding to that address into a hot wallet. After the transfer is complete, set the change address to another unexposed public key address generated by the advanced brain wallet. In this way, even if you publicly release the private key corresponding to the source address or if the hot wallet is hacked, it will not pose a threat to your assets because the source address has been discarded and is no longer used.

This Chapter Quiz:

1. What are some potential risks in the Bitcoin world?
2. What security habits do you need to develop to protect your Bitcoin assets?
3. In the world of Bitcoin, whose responsibility is security?
4. Can advanced brain wallet tools solve all problems?

5. What does the security of advanced brain wallets ultimately depend on?
6. Why should you emphasize testing and reproducing the secure environment in advanced brain wallets?
7. What are the advantages of advanced brain wallets compared to hardware wallets?
8. Why do we say that “Bitcoin does not need hardware wallets”?
9. Why is it easy for hardware wallets to expose information that you own Bitcoin?
10. If you have mastered advanced brain wallets and generate and manage private keys offline in a secure environment according to the requirements of advanced brain wallets, what will happen to risks such as hacking attacks?
11. What are the advantages of advanced brain wallets compared to multi-signature wallets?

Chapter 12: The Future of Bitcoin Security

12.1 The Threat of Quantum Computing: The Invisible Enemy of the Future

In the future development of Bitcoin, we have to pay attention to a potential threat, which is quantum computing.

- **The Power of Quantum Computers:** Quantum computers are a new type of computer that uses the principles of quantum mechanics to perform calculations. They have powerful computing capabilities that far exceed the traditional computers we use today.
- **The Threat of Cracking Passwords:** The emergence of quantum computers may pose a threat to the encryption algorithms we currently use (including the elliptic curve encryption algorithm used by Bitcoin). Once cracked, it will become possible to reverse-engineer private keys from public keys.
- **“Quantum Supremacy”:** The rapid development of quantum computing makes “quantum supremacy” a reality. Once a quantum computer can crack currently used encryption algorithms, we may face the risk of private keys being cracked and assets being stolen.
- **The Risk of Address Reuse:** If you repeatedly use a Bitcoin address, your public key will be exposed on the blockchain when

the transaction is broadcast. Once quantum computing technology breaks through, you may face the risk of being cracked.

12.2 The Impact of Technological Development: Challenges and Opportunities Coexist

Although the emergence of quantum computing has brought us new security challenges, technological development has also brought us new opportunities:

- **Emergence of New Technologies:** As technology develops, new encryption algorithms will continue to emerge. We may find encryption algorithms that can resist attacks from quantum computers.
    - **Continuous Learning:** We need to continuously learn and adapt to new technologies to meet new challenges.
- **Discovery of Security Vulnerabilities:** Any system may have vulnerabilities. We need to discover and fix these vulnerabilities in a timely manner to ensure system security.
    - **Timely Updates:** We need to update our software, tools, and systems in a timely manner to fix known vulnerabilities.
- **Changes in Threat Power:** The attack methods of hackers will also continue to upgrade. We need to continuously improve our security awareness to better respond to various security threats.
    - **Security Concepts:** We need to adhere to the correct security concepts to remain invincible in future competitions. Using advanced brain wallets correctly is one way to minimize the possibility of hacker attacks.

12.3 Precautions for Advanced Brain Wallets: Recognize Limitations and Continuously Improve

Although advanced brain wallets have many advantages, we also need to recognize some of their limitations and always remain vigilant:

- **Reliance on the Human Brain:** The security of advanced brain wallets ultimately depends on your memory. If your memory has errors or you leak key information, your assets are still at risk.
    - **Correct Use:** You need to fully understand the principle of advanced brain wallets and use them correctly according to requirements.

- **Not Applicable to All Scenarios:** Advanced brain wallets are not suitable for scenarios with frequent transactions because each time they require generating new private keys and addresses, which is cumbersome.
    - **Flexible Selection:** You need to choose the appropriate wallet type flexibly according to your actual needs.
- **Continuous Learning and Improvement:** The Bitcoin world is changing rapidly. We need to continuously learn and improve to better cope with future challenges.
    - **Embrace Technology:** We need to embrace new technologies and explore safer and more convenient ways to manage wealth.

12.4 Summary: The Path to Security is Endless, and We Must Jointly Face Future Challenges

The secure future of Bitcoin is full of both challenges and opportunities. We need to always remain vigilant and continuously learn and improve to better cope with future challenges.

Answers to Previous Chapter Quiz:

1. What are some potential risks in the Bitcoin world?
   Answer: In the Bitcoin world, there are multiple potential risks, such as hacking attacks, device damage, information leakage, and even cognitive biases.
2. What security habits do you need to develop to protect your Bitcoin assets?
   Answer: To protect your Bitcoin assets, you need to develop security habits such as continuous learning, regular review, cautious operation, and risk awareness.
3. In the world of Bitcoin, whose responsibility is security?
   Answer: In the world of Bitcoin, security is a self-responsibility. You need to be responsible for your own Bitcoin assets.
4. Can advanced brain wallet tools solve all problems?
   Answer: Advanced brain wallet tools cannot solve all problems. They are just tools. Real security depends on how you use them.
5. What does the security of advanced brain wallets ultimately depend on?
   Answer: The security of advanced brain wallets ultimately depends on your own awareness and behavior, your security habits, and your awareness and prevention of risks.

6. Why should you emphasize testing and reproducing the secure environment in advanced brain wallets?
   Answer: To ensure the effectiveness of your algorithmic rules, you need to conduct offline security environment tests to avoid problems during actual operations.
7. What are the advantages of advanced brain wallets compared to hardware wallets?
   Answer: Compared to hardware wallets, advanced brain wallets have higher security, independence, flexibility, and privacy and do not require trusting any hardware manufacturers.
8. Why do we say that "Bitcoin does not need hardware wallets"?
   Answer: Because if you master advanced brain wallets, you no longer need to rely on any hardware devices to manage your Bitcoin assets.
9. Why is it easy for hardware wallets to expose information that you own Bitcoin?
   Answer: Because if you put a hardware wallet at home or carry it with you, you are exposing information that you own Bitcoin, which is unacceptable to users who value privacy.
10. If you have mastered advanced brain wallets and generate and manage private keys offline in a secure environment according to the requirements of advanced brain wallets, what will happen to risks such as hacking attacks?
    Answer: If you have mastered the essence of advanced brain wallets and generate and manage private keys offline in a secure environment according to the requirements of advanced brain wallets, risks such as hacking attacks can be ignored at the software system level.
11. What are the advantages of advanced brain wallets compared to multi-signature wallets?
    Answer: Although advanced brain wallets belong to single-signature management and do not have a redundancy mechanism, they have the advantages of being streamlined and more flexible. Although multi-signature wallets have redundancy, they increase the difficulty of management because they require storing a large number of mnemonic phrases. This redundancy is false.

This Chapter Quiz:

1. What is quantum computing? What is its threat to current cryptography?

2. What are some opportunities in the process of technological development?
3. What are the limitations of advanced brain wallets?
4. What is the future trend of Bitcoin security?

Chapter 13: Keys to Freedom, Security in Partnership

13.1 Review: The Journey We Have Taken

Congratulations, you've made it all the way here!

In this journey, we have explored the mysteries of Bitcoin together, understood the essence of wallets, compared the advantages and disadvantages of different types of wallets, recognized the uniqueness of advanced brain wallets, learned the security foundations for designing advanced brain wallets, mastered how to use tools to generate addresses, and understood how to securely store and back up private keys and how to inherit your Bitcoin assets.

Now, let's briefly review the key knowledge we have learned:

- **Bitcoin:** A revolutionary digital currency with the characteristics of decentralization, anonymity, scarcity, and global circulation. It is not only a payment tool but also a store of value and an investment vehicle.
- **Private Key:** The only credential for controlling Bitcoin, it must be properly protected.
- **Wallet:** A tool for managing private keys and addresses. It does not store Bitcoin itself.
- **Advanced Brain Wallet:** A special type of wallet that stores private keys in your brain. It uses complex algorithmic rules

and the "Information Pointer Memory Method" to ensure the security and memorability of private keys.

- **Core Ideas:** The core ideas of advanced brain wallets are to hide rules instead of increasing the initial entropy, to manually generate addresses, to prioritize privacy, to defend against quantum supremacy, and to ensure secure coin receipt.
- **Advantages:** Compared to other types of wallets, advanced brain wallets have higher security, flexibility, independence, and privacy. They can effectively defend against hacker attacks, do not require reliance on any third-party institutions, and are convenient to remember and easy to manage.
- **"Use One Address Only Once":** Use a new address each time you receive and send Bitcoin to maximize your privacy and defend against potential threats from future quantum supremacy.
- **Bitcoin Does Not Need Hardware Wallets:** If you have mastered advanced brain wallets, hardware wallets are completely unnecessary.

13.2 The Essence of Advanced Brain Wallets: Mastering the Core and Integrating Knowledge

The essence of advanced brain wallets lies in:

- **Rules First:** The security of advanced brain wallets depends on the rules you design, not on your initial passphrase itself. Therefore, you must carefully design your rules and ensure that they are unique and hidden.
- **Flexible Application:** Advanced brain wallets have a high degree of flexibility. You can customize various different algorithmic rules according to your needs and preferences.
- **Lifelong Learning:** Security is a dynamic process. You need to continuously learn and update your knowledge to adapt to the ever-changing Bitcoin world.
- **Truth Comes From Practice:** Only through continuous practice can you truly master the essence of advanced brain wallets and flexibly use them to protect your Bitcoin assets.

13.3 The True Meaning of "One With Bitcoin": Integrating Wealth Into Life

Advanced brain wallets are not just a technology but also a philosophy. They achieve true "One With Bitcoin."

- **Wealth and Life:** "One" represents your body, your life, and your memory. "Bitcoin" represents your Bitcoin. Advanced brain

wallets closely integrate your memory with Bitcoin, making your wealth truly a part of your life.
    - **Mind Over Matter:** Once you master advanced brain wallets, you truly master your wealth, and you can use your Bitcoin anytime, anywhere.
- **No Hardware Devices Required:** You no longer need to rely on hardware wallets, nor do you need to engrave mnemonic phrases on iron plates, because these physical devices may expose the fact that you own Bitcoin, thereby bringing security risks.
    - **Do Not Expose Your Identity:** Even if you back up your initial brain passphrases everywhere, they are only part of your initial brain passphrases and will not reveal your private key or expose the fact that you own Bitcoin.
    - **Complete Control:** As long as you master advanced brain wallets, you have complete control over your Bitcoin.
- **True Meaning of "Privatization":** You will find that advanced brain wallets allow us to truly realize the privatization of wealth for the first time. Just like your thoughts, as long as your memory is not lost, your wealth will always be with you. You can achieve true "where there is a person, there is the coin; where the person goes, the coin follows."
    - **You Can't Take it With You When You're Born, You Can Take it With You When You Die:** Advanced brain wallets make Bitcoin a truly personal wealth that you "can't take with you when you're born, and you can take with you when you die." You can carry all of your Bitcoin assets in your mind anywhere on the planet.

13.4 Looking Ahead to the Future: Embrace Change and Explore Infinite Possibilities

The world of Bitcoin is full of infinite possibilities and also faces various challenges. But we believe that with the continuous development of technology, Bitcoin will become more and more mature and more secure.

- **Explore Safer Wealth Management Methods:** Let us explore safer and more convenient methods of wealth management together, so that our assets are truly controlled by ourselves and achieve true "One With Bitcoin."
    - **Active Learning:** Continuously learn new knowledge and technologies to improve your security capabilities.
    - **Be Willing to Try:** Be willing to try new tools and methods to explore safer management methods.

- **Embrace Technological Change:** Let us embrace technological change, embrace the future of Bitcoin, and jointly create a more free and secure new era of wealth management.
    - **Maintain Curiosity:** Maintain curiosity about new things and actively explore and practice them.
    - **Continuous Improvement:** Continuously improve your security strategies and adapt to the ever-changing environment.

Answers to Previous Chapter Quiz:

1. What is quantum computing? What is its threat to current cryptography?
   Answer: Quantum computing is a new type of computer that uses the principles of quantum mechanics to perform calculations. It has powerful computing capabilities that may pose a threat to the encryption algorithms we currently use.
2. What are some opportunities in the process of technological development?
   Answer: In the process of technological development, we may find new encryption algorithms that can resist attacks from quantum computers, and we can enhance the security of the Bitcoin system by updating and fixing vulnerabilities in a timely manner.
3. What are the limitations of advanced brain wallets?
   Answer: The limitations of advanced brain wallets are that they rely on human memory and are not suitable for high-frequency transaction scenarios.
4. What is the future trend of Bitcoin security?
   Answer: The future of Bitcoin security will develop towards being more privacy-focused, more flexible and personalized, and more focused on defending against quantum supremacy.

This Chapter Quiz:

1. What is the core idea of advanced brain wallets?
2. What is the most important thing when designing an advanced brain wallet?
3. What else do you need to do after mastering advanced brain wallets?

4. How do you understand the "One With Bitcoin" concept of advanced brain wallets?
5. How do advanced brain wallets achieve "where there is a person, there is the coin; where the person goes, the coin follows"?

Chapter 14: Advanced Brain Wallet Practical Tutorial

14.1 Practice

Welcome to the practical section of advanced brain wallets! In previous chapters, we have explored the theoretical knowledge, design principles, and security foundations of advanced brain wallets in depth. Now, we will translate this knowledge into actual operations and teach you step by step how to use advanced brain wallets to securely manage your Bitcoin assets. This appendix is intended to provide a clear and detailed practical guide to help you move from theory to practice. Please read this appendix carefully and operate in a secure offline environment.

14.2 Preparation

Before starting the practical exercises, be sure to do the following preparations to ensure the safety of the operation:

- **Offline Environment:** This is the most important point! Be sure to disconnect your computer from the network (including Wi-Fi and network cables) to ensure that your computer is completely offline. It is recommended to use a dedicated offline computer for generating private keys. Do not install any other software and do not connect to any network. If conditions do not allow,

you can use a USB flash drive to boot an offline operating system.

- **Open-Source Tools:** We recommend using DaGe's (@btcdage) open-source Python advanced brain wallet tool, which you can find on Github:
  - **Open-Source Address:** https://github.com/btcdage2000/BrainWalletGenerator/
  - **Executable File Download Address:** https://github.com/btcdage2000/BrainWalletGenerator/releases/tag/v0.1.0
  - **Important Tips:** Be sure to download from the official address and verify the integrity of the file.
- **Paper, Pen, and Backup Devices:** Prepare paper, pens, and backup devices such as USB flash drives and portable hard drives to record your algorithmic rules, brain passphrases, salt values, and the addresses you generate.

14.3 Designing an Advanced Brain Wallet Algorithm

The following examples are for demonstration purposes only. Do not copy them exactly in actual operations.

Before using the tool to generate addresses, we need to design our own advanced brain wallet algorithm. Please remember that the core of advanced brain wallets is to hide the rules rather than increase the initial entropy. You need to use the "Information Pointer Memory Method" flexibly and combine it with your personal situation to design a unique algorithm.

For example, we will use the following algorithmic rules for this test (all examples are for reference only):

1. Use any Nostr client to generate 10 Nostr private keys and save them. Here, I will directly generate them using code.

```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()
```

```
Pair 1:
Private key: nsec1wdgf4dp5heua8axfapc1nvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrm
Public key: npub15pgu0u205dkcpe630trvfjr79jywpzd79thze4zmjjqccmqwtucqf3yptc

Pair 2:
Private key: nsec1ct8t37t4kldv1w50xmsulqjszvffr03m44rmrmm08de58jhfu68q0g74mx
Public key: npub1qndjqcqaregvhck82nrx4wpppcm76920cmkat7jcyfl6qhjkmmaq409y69

Pair 3:
Private key: nsec14pj5jvc12vr8k4n4mdex9ngv4nen27pvt9980snhr343fkr5draqrr8vc8
Public key: npub196dq6aktla3g205jqrcwfwgr7psqd4g4fz2f2adgpwc13m9j318qfx7537

Pair 4:
Private key: nsec1csazzt20m00xz8su870gf5uzgtsk4880s8egdestqjvsm9k6zc8s6560pd
Public key: npub1pxzt4qwm6wygnugca7ynpks3ypag1086hqmzsz3p2asnam66fp2sdkr03t

Pair 5:
Private key: nsec1tx83axcdlx2g3de51u2q889ksy4jmgjnh424fsnrpkueg0xkmfes6w8tkz
Public key: npub1v6d6f9hx3xjrfx4p3w7npjqp9gycsjehpa46pk3j16h2mvhqvd0s2yfww4

Pair 6:
Private key: nsec1wur0jntgkygchyre4c5gvmdy414q9hd47rcptjqak8z35jdcness00gjma
Public key: npub120y3s38ay5qywm6gdp9r37syeweq5c57nvjvw0hgphkluvf2v2tqdq4msj

Pair 7:
Private key: nsec1gj4vjg2rlzslfl0lysuk2xu2lhvhng7g24u70ax88s2wggec5cdsmxpyxe
Public key: npub16ednqnz9pd5jc5zwkqfeejvkau5lyssyszlpev3hj8j8hq2zvt3s0k2j4x

Pair 8:
Private key: nsec1g8ee4ueu2m8hgm8u4h567q38x3dkj40k3mcgxa49znv564h8kkhq5xgmtn
Public key: npub1trkegnjg6sfumeg6jgnef2w66c9ke39f0rcxw2qhs45pr57qt59qkqw6z6

Pair 9:
Private key: nsec1fsmjzgyrcrkd79etkxegax36cu87kuc6jq99d9jrxuu0keqkz91q0rpu4g
Public key: npub16ray2vdumuecaqkzykxv3rf5xngjutfzgeygs9kr2ukk34p3vwpstujxzk

Pair 10:
Private key: nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3sa
Public key: npub1znrnyr1nrww1wykvscg9c84ngw5t0qp90zj1u1yuse440gqn7kjqgzm1sc
```

2. Set the key brain passphrase to DaGe’s signature: “I COME, I SEE, I HODL.”
3. Set the number of hashing operations to 673 (BTC->673).
4. Set the initial brain passphrase as the first Nostr private key + key brain passphrase:

   nsec1wdgf4dp5heua8axfapc1nvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrm I COME,I SEE,I HODL.

5. Set the salt value as the last Nostr private key + key brain passphrase:

   nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3sa I COME,I SEE,I HODL.

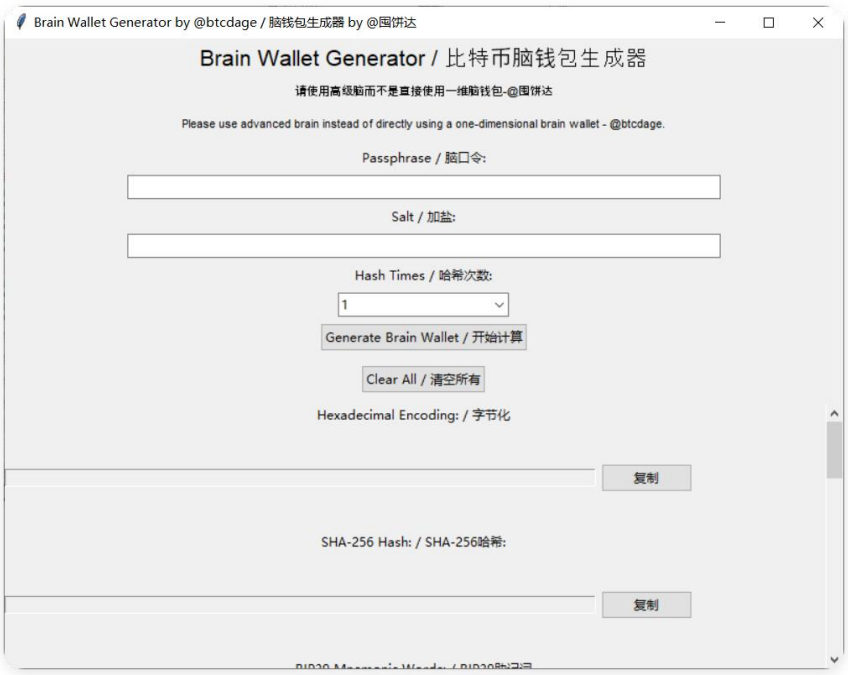
6. Append the sequence number to the right of the salt value. For example, the generation method of the first address is:

   nsec1fwcnhq0zjy0dqnza3tfxzuhf03fp8yneway3m86uspcp3c0zn8qqaep3sa I COME,I SEE,I HODL.1

14.4 Using Tools to Generate Addresses

Now, we can use DaGe’s tool to generate addresses.

1. **Download the Tool:** Download DaGe’s open-source Python tool from Github and save it to your computer. Alternatively, download the compiled executable file.
2. **Disconnect Network Connection:** Following the methods mentioned earlier, disconnect your computer’s network connection to ensure that your computer is offline.
3. **Run the Tool:**
   - If you choose to download the source code, you need to install Python 3.6 or higher first. Then, in the terminal or command prompt, enter the command python brain_wallet_generator.py to run the tool.
   - If you downloaded the executable file, you can run it directly without installing a Python environment.



4. **Concatenate Initial Information:**
   - **Important Tips:** DaGe's tool is only responsible for the hash chaining and salting operations. Therefore, you need to concatenate all the information that needs to be spliced, such as the initial brain passphrase, salt value, sequence number, and “key brain passphrase”, according to your designed rules. Then, enter the concatenated string into the "Passphrase / 脑口令" input box.
   - **Enter Brain Passphrase:** According to your designed rules, concatenate all the information you need to splice, such as your initial brain passphrase, salt value, the sequence number you calculated, and even the final "key brain passphrase." Then enter the concatenated string into the "Passphrase / 脑口令" input box.
   - **Enter Salt Value:** If your algorithm uses a salt value, you need to enter the salt value you selected into the "Salt / 加盐" input box.
5. **Set the Number of Hashing Operations:** In the "Hash Times / 哈希次数" drop-down menu, select the number of hashing operations you set.
6. **Generate Keys:** Click the "Generate Brain Wallet / 开始计算" button, and the tool will perform calculations according to the hash chaining process you set to generate information such as private keys, public keys, P2PKH addresses, and Bech32 addresses.

7. **Back Up Addresses:** Back up the generated P2PKH addresses and Bech32 addresses separately. You can write them down on paper or copy them to a USB drive. Be sure to confirm that the addresses you copy match the addresses displayed in the tool.
8. **Clear Information:** Click the “Clear All / 清空所有” button to clear all information to avoid leakage.

14.5 Verify Address Accuracy

To ensure that the generated address is correct, we need to verify it.

- **Use Wallets such as Electrum:** You can use wallet software such as Electrum to import your private keys and then verify whether the generated address is correct.
    - **Precautions:** Be sure to perform the import and verification operations offline to avoid private key leakage.

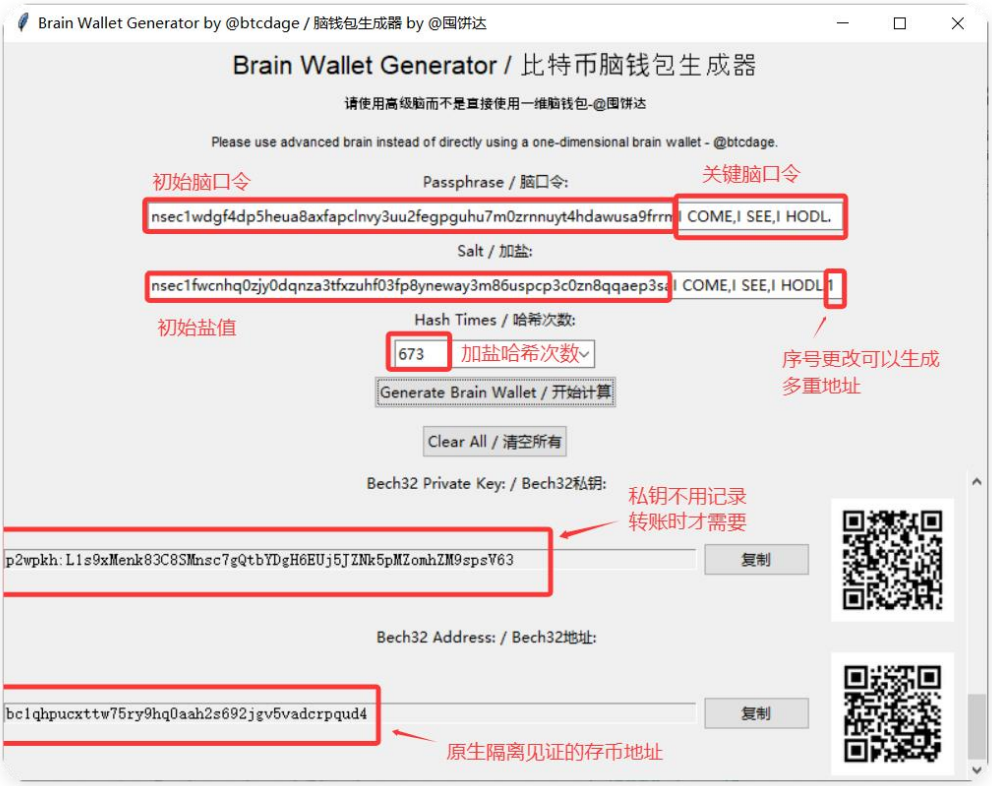
14.6 Secure Storage and Backup

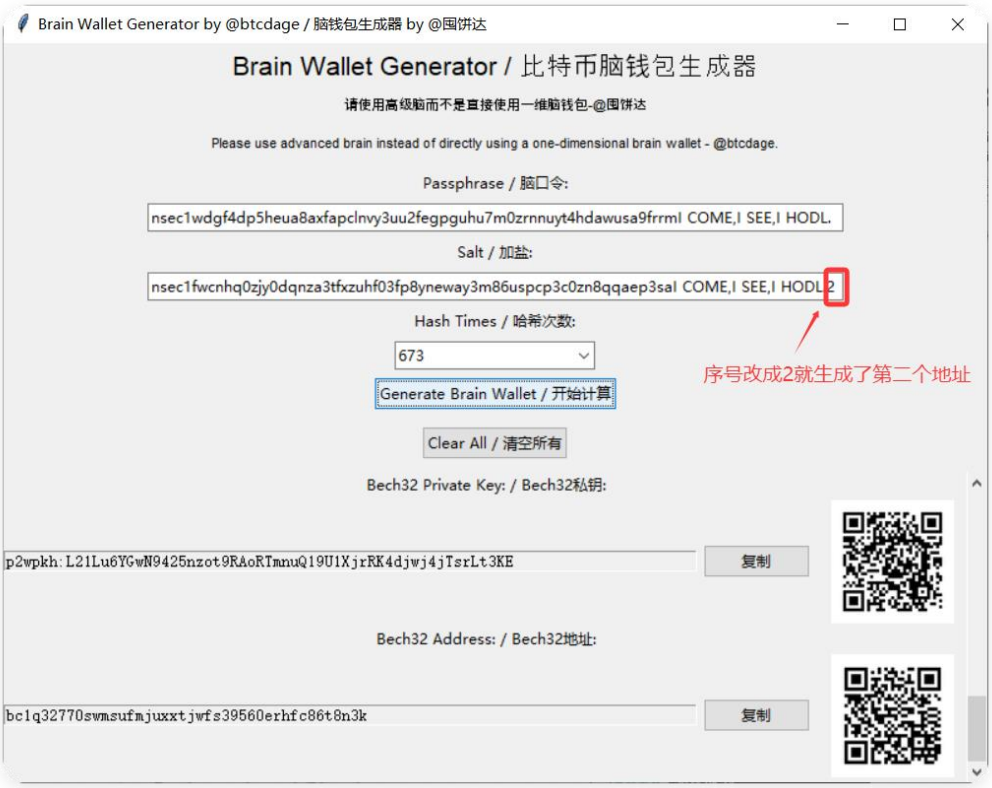
Secure storage and backup are important steps in protecting your Bitcoin assets and must be treated seriously:

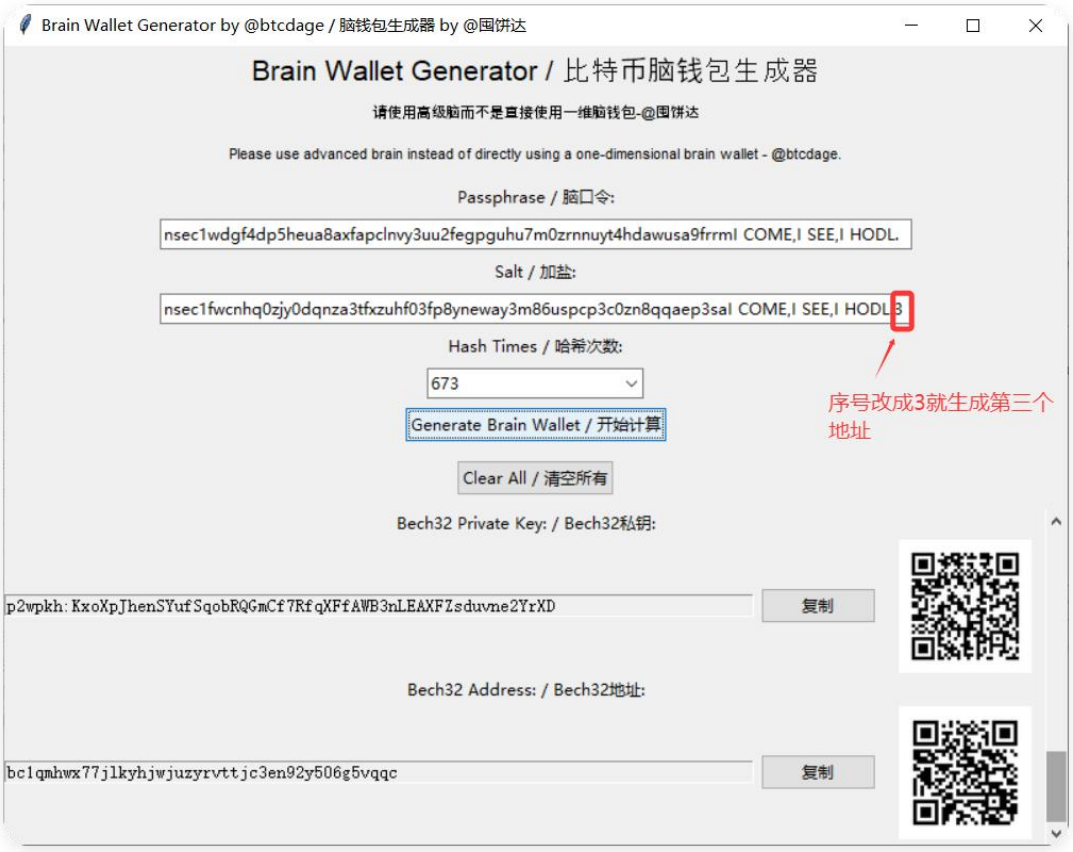
- **Special Storage of the "Key Brain Passphrase":** The “key brain passphrase” can only exist in your brain and cannot be recorded on any paper, electronic device, or any other form of physical media.
- **Backup of Algorithmic Rules:** Print multiple copies of your algorithmic rules and store them separately in different safe locations, such as a safety deposit box, a hidden corner at home, or with a trusted family member.
- **Backup of Other Brain Passphrases and Salt Values:** You can write them down on paper or encrypt them and store them on mobile devices such as USB drives and portable hard drives, or in cloud storage such as cloud drives.
- **Regular Review:** Regularly check your backups to ensure that they are complete and reliable.

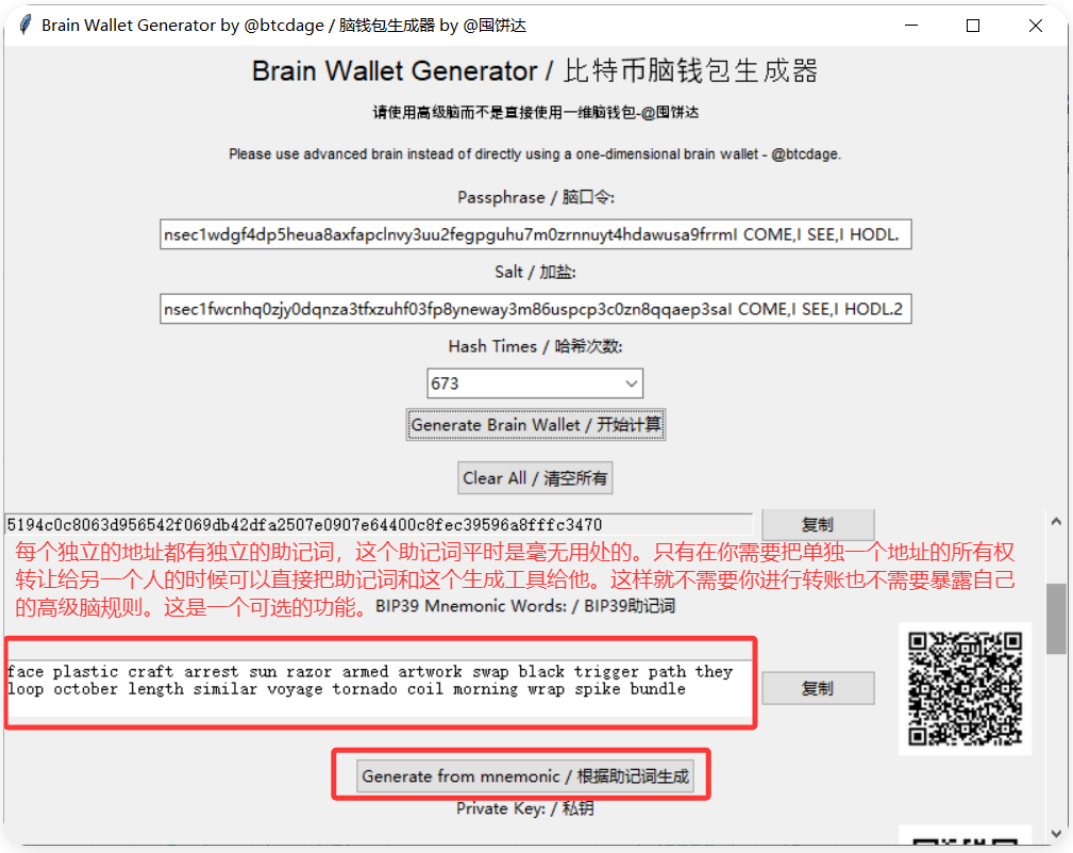
14.7 Demonstration Screenshots

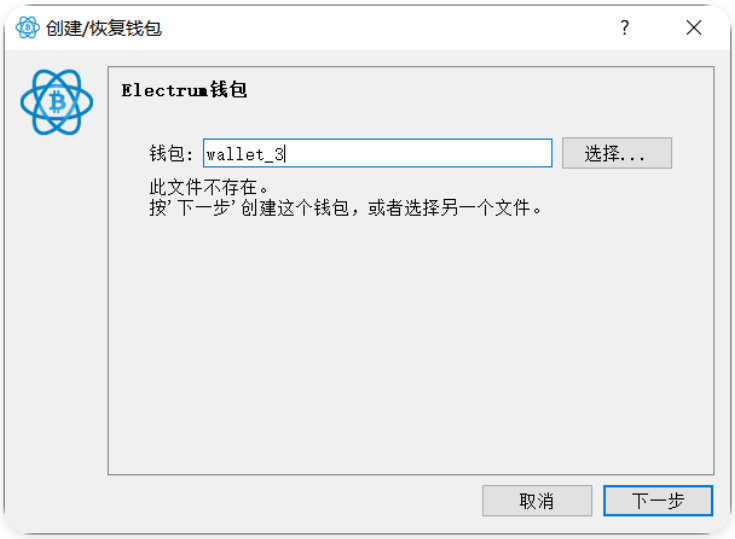
These are demonstration screenshots to mainly show the tool interface and demonstrate the operation steps. Please refer to 14.3 to 14.6 for the complete operation steps.


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

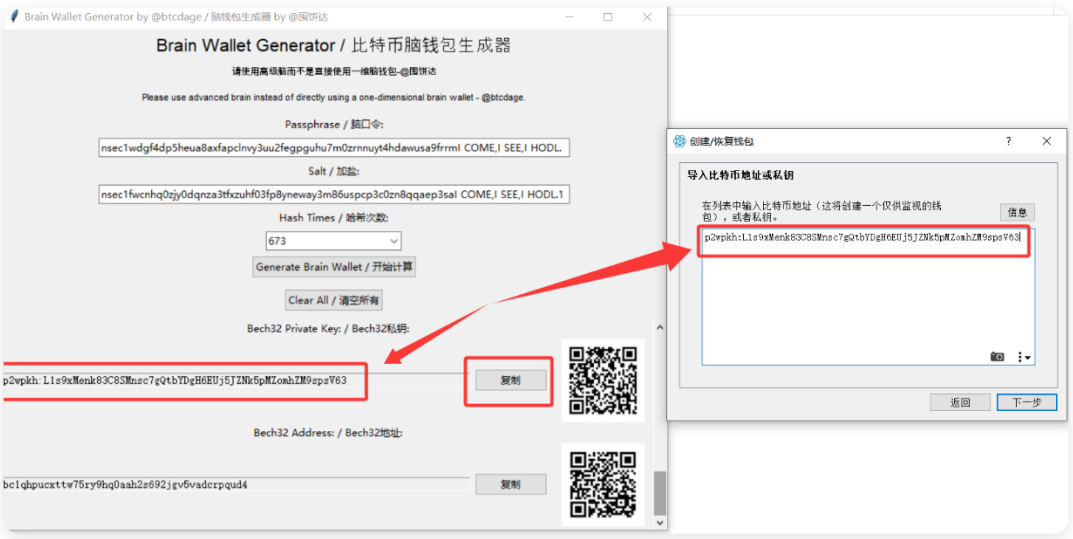

Brain Wallet Generator by @btcdage / 脑钱包生成器 by @国饼达
Brain Wallet Generator / 比特币脑钱包生成器
请使用高级脑而不是直接使用一维脑钱包-@国饼达
Please use advanced brain instead of directly using a one-dimensional brain wallet - @btcdage.
Passphrase / 脑口令:
nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrml COME,I SEE,I 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

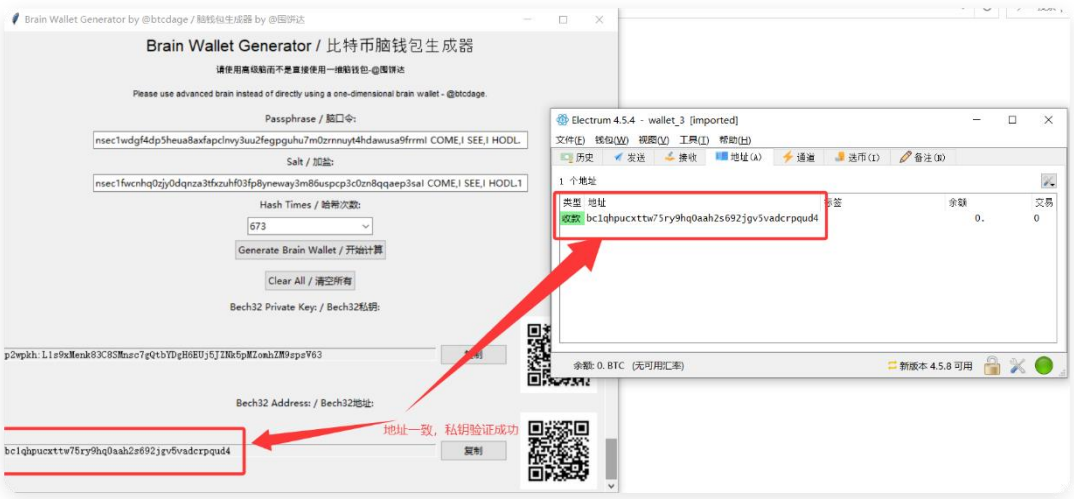

Brain Wallet Generator by @btcdage / 脑钱包生成器 by @国饼达
Brain Wallet Generator / 比特币脑钱包生成器
请使用高级脑而不是直接使用一维脑钱包-@国饼达
Please use advanced brain instead of directly using a one-dimensional brain wallet - @btcdage.
Passphrase / 脑口令:
nsec1wdgf4dp5heua8axfapclnvy3uu2fegpguhu7m0zrnnuyt4hdawusa9frrmI COME,I SEE,I 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 @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:
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
导入比特币地址或私钥
返回
下一步



14.8 Frequently Asked Questions

- Q: What if I forget the “key brain passphrase”?
  - A: Because the "key brain passphrase" only exists in your brain, once you forget it, you will not be able to recover it. Therefore, you must ensure that you can remember it. It is recommended to use the "Information Pointer Memory Method" to associate it with an unforgettable experience and review it frequently to deepen your memory.
- Q: Can I use online tools to generate addresses?
  - A: It is strongly not recommended to use online tools to generate addresses because there is a risk of private key theft. Be sure to use offline tools for operation.
- Q: Can I tell my family members about my algorithmic rules?
  - A: You can back up your algorithmic rules and tell your family members about them, and be sure to tell them your "key brain passphrase" but do not record them in the physical world. If something happens to you, your family members can use your backup information combined with the "key brain passphrase" you told them to recover your Bitcoin assets.
- Q: Can I use paper wallets or hardware wallets?
  - A: The philosophy of advanced brain wallets is that you do not need to rely on any third-party hardware or software. Although paper wallets and hardware wallets also have a certain degree of security, they are not necessary. After learning about advanced brain wallets, you will find that using advanced brain wallets to store Bitcoin is safer.

14.9 Summary

Congratulations, you have completed the practical tutorial for advanced brain wallets! Now that you have mastered the basic operations of advanced brain wallets and how to protect your Bitcoin assets. Be sure to practice more and continuously learn and improve. Remember that the path to security is endless.

Answers to Previous Chapter Quiz:

1. What is the core idea of advanced brain wallets?
   Answer: The core idea of advanced brain wallets is to hide the rules rather than increase the initial entropy, to manually generate addresses, prioritize privacy, defend against quantum supremacy, and ensure secure coin receipt.
2. What is the most important thing when designing an advanced brain wallet?
   Answer: The most important thing when designing an advanced brain wallet is to design algorithmic rules that are unique and hidden.
3. What else do you need to do after mastering advanced brain wallets?
   Answer: After mastering advanced brain wallets, you still need to continuously learn and practice to truly master the essence of security and use it flexibly to protect your Bitcoin assets.
4. How do you understand the "One With Bitcoin" concept of advanced brain wallets?
   Answer: Advanced brain wallets closely integrate your memory with Bitcoin, making your wealth truly a part of your life and allowing you to truly master your Bitcoin assets.
5. How do advanced brain wallets achieve "where there is a person, there is the coin; where the person goes, the coin follows"?
   Answer: Because the private key generation method of advanced brain wallets is stored in your brain, you can carry all your Bitcoin assets in your mind anywhere on the planet, which makes it possible to achieve “where there is a person, there is the coin; where the person goes, the coin follows."

Conclusion: One With Bitcoin, Security in Partnership, The Future is Defined by You

"One With Bitcoin: The Advanced Brain Complete Manual" officially concludes here. Thank you for your companionship along the way as we have explored the mysteries of advanced brain wallets together. From the initial understanding of Bitcoin to the complete mastery of advanced brain wallets, we have embarked on a significant journey together.

Advanced brain wallets are a revolution in traditional private key management concepts. They store private keys in the brain, avoiding third-party risks and achieving a high degree of "decentralized" wealth management. They also allow us to understand that the security of Bitcoin ultimately rests in our own hands.

The concept of advanced brain wallets originated in 2020, took shape through practice, and was systematically presented in the form of this manual in 2025. Special thanks to Bitcoin Evangelist, Tractor, for their in-depth discussions, and to A Jian and other fellow members for the inspiration in the discussions. We also want to thank all the group members and fans for their continuous support. We also realized that early practitioners such as Li Xiaolai had already adopted similar techniques, which further confirmed the advancement and practicality of the advanced brain wallet concept.

Through the study of this manual, you have mastered the knowledge and skills of advanced brain wallets and are able to manage your Bitcoin assets more securely. This is also a power, a power to truly control your own wealth.

The journey of Bitcoin has just begun. Let us work together to usher in a new era of safer and more free wealth management! And this future is ultimately defined by you!

DaGe @btcdage
https://btcdage2011.github.io/btcdage
January 15, 2025