# Seedless wallet recovery
# Explained using a treasure hunt analogy

## Overview

A prominent skeptic in the cryptocurrency/financial realm recently tweeted, lamenting his tragic experience with Bitcoin when he claimed his wallet seed suddenly stopped working. After an outpouring from the cryptocurrency community, it was later found that this person was attempting to use a pin number, which is presumed to have been associated with his wallet on some type of mobile application. To make matters worse, this person did not save the wallet seed either.

While savvy users of Bitcoin and other cryptocurrencies may see this as a rookie mistake, many also believe it highlights a longstanding issue with wallet seeds in general. They are hard to remember, burdensome to manage—quite frankly that's enough to steer casual users away altogether. Simply put, the barrier to entry with regard to education about wallet seed use is too high. This especially is the case when your ignorance on the finer details can cost you large amounts of money, accompanied by feelings of incompetence. A better approach is long overdue.

To date, memory in the human brain is the only known method of storing a password where it cannot be accessed. Other methods such as biometrics are not effective, as humans leave DNA everywhere they go, display their eyes publicly and leave their fingerprints on everything they touch. All of this can be copied and replayed by an impostor to gain access to secure data, platforms, systems and wallets. Wearable hardware devices can be lost or stolen which either denies you access to your wallet or even worse, potentially gives access to an attacker.

Add this to the fact that every user, at some point in their online life, probably has forgotten their password to something important. This is made worse because online services force users to change their passwords at regular intervals. Every time this change is made, the password is more and more likely to be less relevant to the user's life and thus, more forgettable. Compound this problem with the fact that the user experience is to type a password into an input box and then click some type of button that kicks off the authentication process on a remote server, given the credentials provided. This process has been exploited repeatedly by attackers referred to as *phishers*. They use phishing attacks to gain knowledge of a user's password.

Creative and effective solutions to these problems have been slow to evolve. A case in point is that little has been done to exploit the human brain's ability to remember locations as part of a solution. Locations and their associated imagery can be emotionally intense for humans and thus can be very easy to remember. This points to a methodology that's long overdue to consider.

Center Identity's solution is superior with respect to all of the points mentioned above:

- Passwords are not sent over the wire.
- There's no user experience idiom such as *signing in* or *resetting your password* so these processes can no longer be exploited.
- Passwords are location-based and very memorable for individuals.

**The treasure hunt concept for seedless wallet recovery**

A fitting analogy for this solution is that of searching for a hidden treasure. We use this analogy to gain an easy understanding of the steps involved in our novel solution for seed management. Seedless wallet recovery using the treasure hunt analogy has three components where the wallet seed is referred to as the treasure.

Seeds are generated outside of this process. The process starts after a wallet seed has already been generated.

The following process pertains to seed management:

- Burying the treasure.
- Saving the treasure location.
- Digging up the treasure at a later time.

The wallet seed, given its moniker, implies that there are no other security mechanisms to recover your wallet beyond it. The solution outlined here will show Center Identity can deliver secure wallets and provide an unprecedented level of convenience in wallet management.

**Burying the treasure**

Before one digs for a treasure, a treasure must first be buried. This requires digging a hole to place the treasure into and then filling the hole to conceal the treasure and prevent it from being discovered by anyone other than the one who buried it.

The geographic coordinates of the burial site are intended to reference a special place for the user. This is a place the user will never forget but also a place where neither their friends nor family have any knowledge of the user’s affinity for this location.

To bury the treasure, we need to establish the *header data*. The term header data simply means a concatenation of the latitude, longitude and username values. For example, the geographic coordinates 45.548097, -122.433365 and username of userofyadacoin would render header data equal to 45.548097-122.433365userofyadacoin.

Once the user has decided on those three pieces of data, Center Identity concatenates them to produce the header data. We then use a hashing function to create a one-way cryptographic hash repeatedly until the value of the hash is below a desired value. This process can be compared to a familiar concept in the cryptocurrency realm known as *mining*. Mining, in the physical world, is the process of digging for items of value buried beneath the earth’s surface. In cryptocurrency parlance, this analogy is applied to the process of producing cryptographic hashes until the desired value is found. With this solution, the same process of producing cryptographic hashes until a desired value is found, is also used here.

There are two hashes that need to be discovered and persisted on a database. The first hash below the target, plus one final hash for obfuscation purposes, is the actual encryption key used to encrypt the seed. The second hash below the target, plus one final hash for obfuscation purposes, is the relationship identifier for the encrypted seed and is used as a lookup during recovery. It should be noted that unlike *proof of work* mining, Center Identity does not use a nonce in the header. Instead, Center Identity simply rehashes the resulting hash in a loop and process for finding the values is as follows:

1. Set the target = 0x00000fffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

2. Loop starts.

3. Hash below the target found.
(e.g., 0x000001b979f572871f1c3466e8418bc3a68d4af4dc43490c14e8221babf3c1e7)

4. One more hash for obfuscation,
(e.g., ecryption_key =
0xe1c1f92143dea0b0c93dfe89030a9bea8c138bcd38504dd19acdfd81e14f95bc)

5. Loop continues.

6. Hash below the target found.
(e.g., 0x0000019ed02ef1f65f0349a9515f5dd612210f639f78f728ed7744f6e69db476)

7. One more hash for obfuscation.
(e.g., relationship_id =
0x5ed55bf168817de7729ab94f84de722e0c073eb7bae78d5d056edbd42b7ec96c)

**Digging up the treasure (seed recovery)**

Now that the treasure has been buried, there will be an occasionally need to recover it. This need will arise as the user acquires new devices. Instead of transferring a seed through the various communication platforms available, Center Identity allows the user to *dig up* or recover their seed securely and conveniently.

The process begins by the user providing the coordinates of their secret location. They do this by either a map input or by actually going to that secret location and using the coordinates of their current location. Next, Center Identity asks the user for their username, such as *userofyadacoin,* as used earlier in this example and previous noted in burying section. We Center Identity executes the exact same mining loop to find the two needed values, relationship identifier and encryption key.

The relationship identifier is transmitted to the server or node of a database or blockchain that contains this relationship identifier referencing the encrypted seed. The encrypted seed is returned to the user's device and the encryption key is then used to decrypt the encrypted seed. This seed is then consumed by the wallet application and used to restore the user's wallet.

That's it! This summarizes the entire workflow of encrypting, persisting and restoring the wallet seed.

## Comparison with current password technologies

People can generate a wallet seed from biometric data, retinal scanning, fingerprints or DNA, but these are all completely insecure methods. We either leave these items everywhere we go or display them in full view of the general public.

Passwords are hard to remember and users constantly forget them. This is mainly due to the fact that passwords and wallet seeds have no relevance in people's lives—they're not memorable. When people first started creating usernames and passwords, their passwords were very insecure by today's standards because they were usually relevant words to their lives such as a pet or child's name. So, in forcing non-dictionary words to strengthen passwords, Center Identity has negated the original mechanism that allowed humans to remember them.

The treasure hunt method exploits the relevance mechanism in the human brain using its photographic (image-based) and emotional memory capabilities. This is without distilling the memory down into a short string of characters that can be easily hacked using brute-force techniques.

## Comparing passwords to treasure locations

The average password is eight characters long, so $P$ equals the maximum number of attempts needed to successfully brute-force an eight character password.

**8 x 8 bytes = 64 bits**
$\boldsymbol{P} = \mathbf{2^{64}}$

However, passwords are relegated to an even smaller subset of available characters. Most often, the available characters for a password are upper case, lower case, number and about 10 special characters.

**26 + 26 + 10 + 10 = 72 possible characters**

$\boldsymbol{P} = \mathbf{72^{8} = 7.222041363 \times 10^{14}}$

The most powerful financial and government institutions rely on this probability to protect their sensitive data.

Treasure locations are far more secure than passwords if you consider the components of the header data before mining:

- longitude
- latitude
- username
- digging for the reference
- digging for the decryption key

The decryption key itself is SHA256 which boasts an impressive $2^{256}$ number of possible combinations. Attackers would not likely go this route for brute-forcing the decryption key.

The longitude and latitude decimal numbers are set to a precision of five, which is enough resolution to distinguish an area of about one meter.

Let’s say the username is 12 characters on average. The below equation, we have a sign, longitude decimal number, sign, latitude decimal number, username and then number of possible hashes until a value is found that is less than the target 0x00000fffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

$$\mathbf{2 \text{ x } 18000000 \text{ x } 2 \text{ x } 9000000 \text{ x } 72^{12} \text{ x } 2^{20} = 1.318757299\times10^{43}}$$

Even if you consider that earth is only 29% land.

$$\mathbf{([2 \text{ x } 18000000 \text{ x } 2 \text{ x } 9000000] \text{ x } .29) \text{ x } 72^{12} \text{ x } 2^{20} = 3.824396167\text{x}10^{42}}$$

As you can see, treasure locations are several orders of magnitude more secure than standard passwords.

### Comparing treasure locations to seeds

Treasure locations are even more secure than 12 word seeds if use user chooses a username of 12 characters or more.

With seeds on the other hand, if any longer than 12 words, the average human will likely not remember them which negates the purpose of the seed being human readable. Using 12 words, for that matter, is too long for most humans to remember without significant investment in memorization. The truth is, the vast majority of users will mismanage their wallet because of this.

For this example, let’s use 12 word seeds. There are 2048 words in the BIP39 mnemonic seed word list.

$$\mathbf{2048^{12} = 5.444517871 \text{ x } 10^{39}}$$

This is $10^{43}$ possible combinations for treasure locations versus $10^{39}$ for BIP39 seeds.

To get an idea of just how much effort it would take to crack a treasure location password, let’s take the current Bitcoin hashrate, which is 120,000,000,000,000,000,000 hashes per second. This is arguably the most computing power put towards a single calculation in computing history. However, even with this combined power, it would still take millions of years to brute-force attack this password.

This algorithm can be used to store an existing seed and intended to be compatible with the existing ecosystem of wallet technology. However, the treasure location can also be used to generate the wallet seed itself and thus would not require the secondary relationship identifier and persistence medium.

**Warnings about the Center Identity system**

- Users should NEVER use services in the location where they buried their seed. To do this could give an attacker more clues about possible coordinate values to use for discovering a seed.
- Users should NEVER use the same username as their wallet seed recovery username.

**For more information about Center Identity, visit:**
https://centeridentity.com