Unchained

BITCOIN BASICS

Bitcoin self-custody approaches compared

SINGLESIG OR MULTISIG FOR LONG-TERM SAVINGS?

TOM HONZIK & STEPHEN HALL

26 SEPTEMBER 2023

Unchained

Contact

Follow Tom Honzik on twitter: @tom_honzik

Send Tom Honzik an email: thomas@unchained.com

Follow Unchained on twitter: @unchainedcom

Send Unchained an email: hello@unchained.com

Unchained

Outline

Unchained

Bitcoin self-custody approaches compared

If you want to remove custodial risk from your bitcoin holdings, you must take self-custody. Bitcoin custody is determined by whoever has the keys to control the bitcoin—if you aren't holding the keys to your bitcoin, then someone else is. As the saying goes, "not your keys, not your coins."

Once someone decides that they want to hold their bitcoin in self-custody, the next question becomes how to do it. Most people discover early on that hardware wallets are the most secure way to use bitcoin keys. However, the options don't end with selecting a hardware wallet; you can also choose between singlesig, multisig, and a few other technologies that determine what is required to spend your bitcoin. In this article we will take a look at these options and compare them with one another.

I. Singlesig

Singlesignature describes a wallet structure where only one private key is required to sign off on spending bitcoin. It is the oldest and most basic method of holding bitcoin. For these reasons, over 70% of the total bitcoin supply is currently held in this manner.

Despite being fairly easy to set up and use, many people have found that singlesig does not provide an adequate level of comfort. With only one key, there will always be a single point of failure that can lead to lost funds. For example, if your singlesig key becomes misplaced, then you will no longer have access to your bitcoin. Or, if your key falls into the wrong hands, a thief can sign off on transferring your bitcoin to their own wallet.

It's important to remember that a bitcoin private key is merely randomly-generated secret information. The information can be generated by an offline tool such as a hardware wallet, but it should also be stored physically, as a seed phrase. This will mean keeping a set of 12 or 24 words secure and private.

Even for people who are quite careful and organized, important items can become lost due to mistakes or uncontrollable circumstances. If the lost item happens to be the only key to your bitcoin wealth, that would be catastrophic. Naturally, people are motivated to pursue strategies that will help ensure this never happens. Let's explore some of the popular approaches!

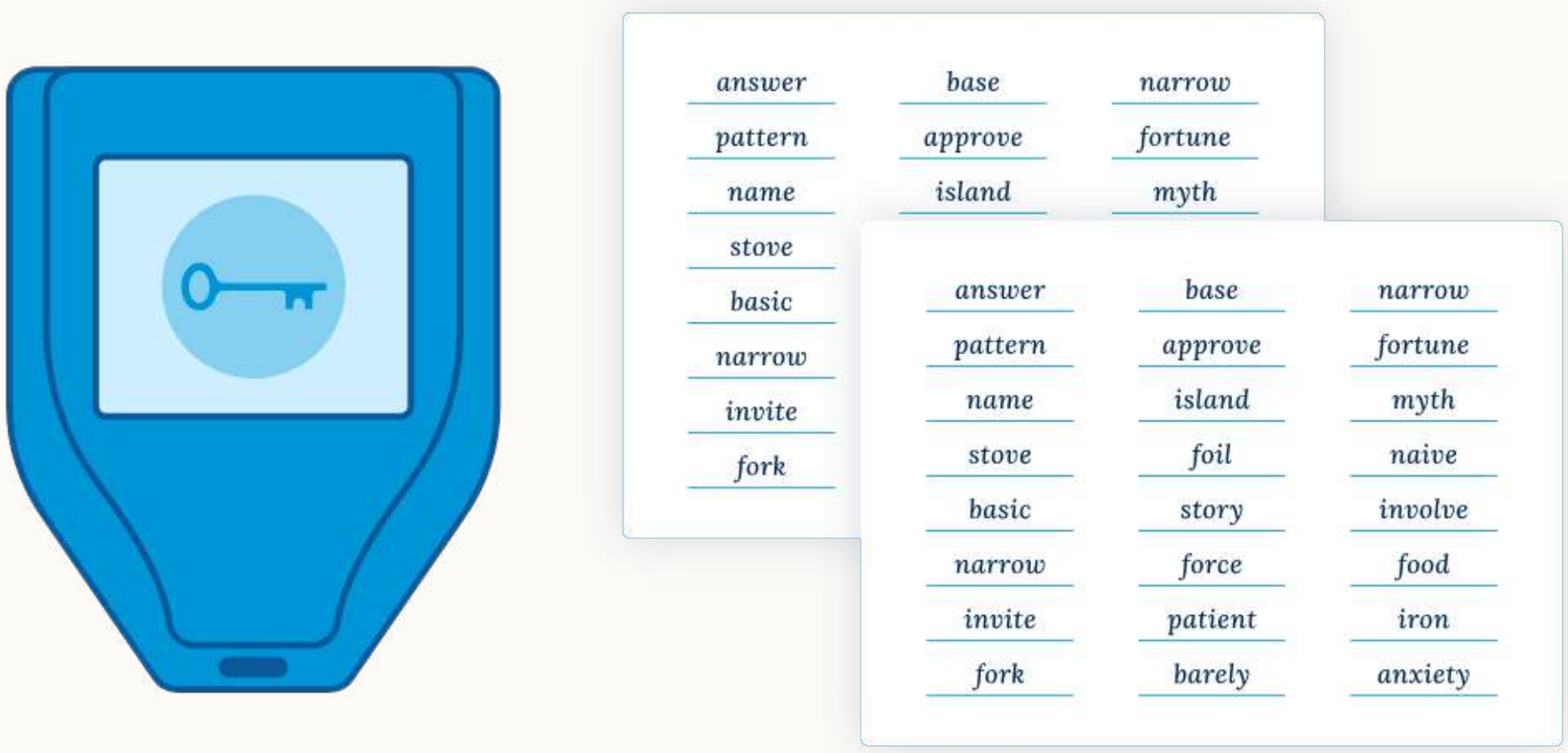
Before we get to multisig, it's worth taking a look at some of the methods people use to modify singlesig arrangements. Some of the ways people try to improve their singlesig security involve improvised strategies, while others involve standardized technological tools.

II. Improvised singlesig modifications

Without learning about additional technologies, someone who holds bitcoin in a singlesig wallet might think of simple techniques that appear to offer protection from losing funds. Examples include making copies of the seed phrase, splitting the seed phrase into separate pieces, encoding the seed phrase, or creating several singlesig wallets to distribute wealth. These techniques all come with trade-offs that users may initially fail to recognize. We'll now briefly cover them in more detail.

Seed phrase copying

Making copies of a seed phrase is one strategy people use to help avoid losing access to their bitcoin in a singlesig wallet. Doing this can provide extra protection against natural disasters or misplacement. By storing multiple copies of a seed phrase in several different locations, one location could suffer unexpected destruction without you losing access to your seed phrase information.

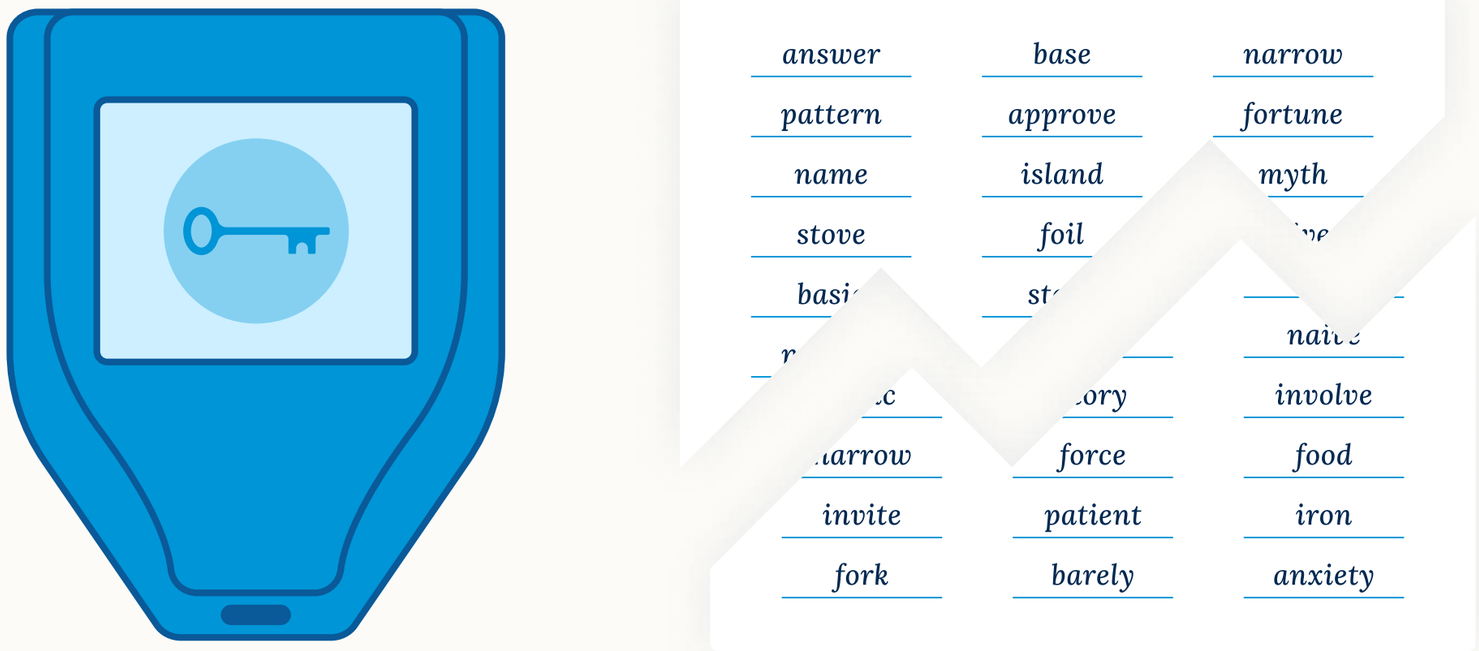


A hardware wallet with two copies of its seed phrase backup.

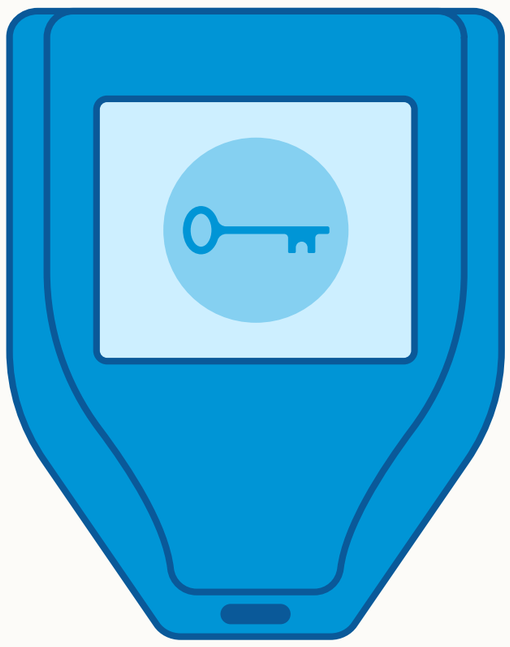
On the other hand, a significant downside to this approach should be considered. With an otherwise basic singlesig arrangement, the seed phrase is the only item someone needs in order to discover your wallet balance and remove bitcoin from your wallet. In other words, if a dishonest person finds any one of your seed phrase copies, they could steal bitcoin from you. Therefore, storing your seed phrase in several locations can increase the chance of this occurring.

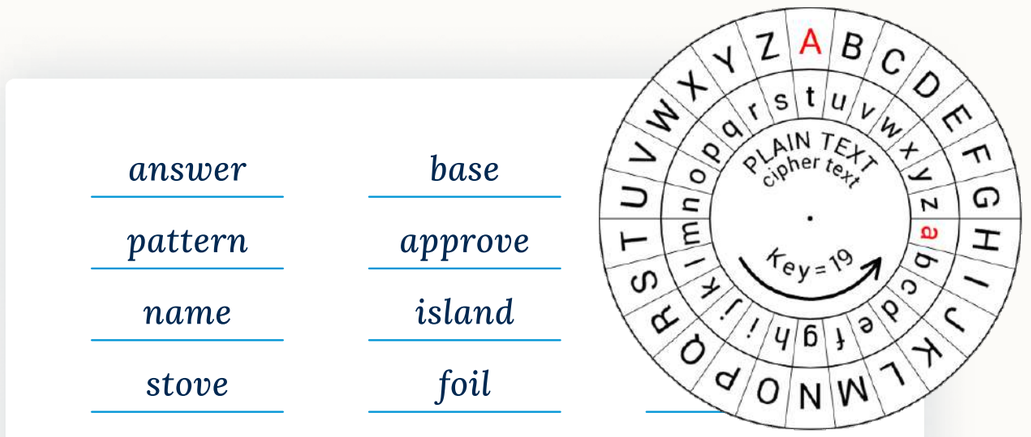
Seed phrase splitting

Because seed phrases typically exist as 12 or 24 words, some users will think to split up the word list into sections and store them separately. This follows the logic that if a thief managed to acquire less than the full word list, they would be unable to steal the bitcoin.



A hardware wallet with its seed phrase backup split into multiple pieces.





A bitcoin hardware wallet with its seed phrase backup and associated custom encoding.

However, out of all the ideas covered in this article, this one is the most problematic. The theft prevention logic is flawed—if a thief managed to find a portion of your seed phrase, they could be substantially closer to being able to guess the remaining words and steal from you. Besides failing to offer the intended level of protection, this approach can also make it more difficult (if not impossible) for you as the user to access your bitcoin if any one of the seed phrase sections becomes lost.

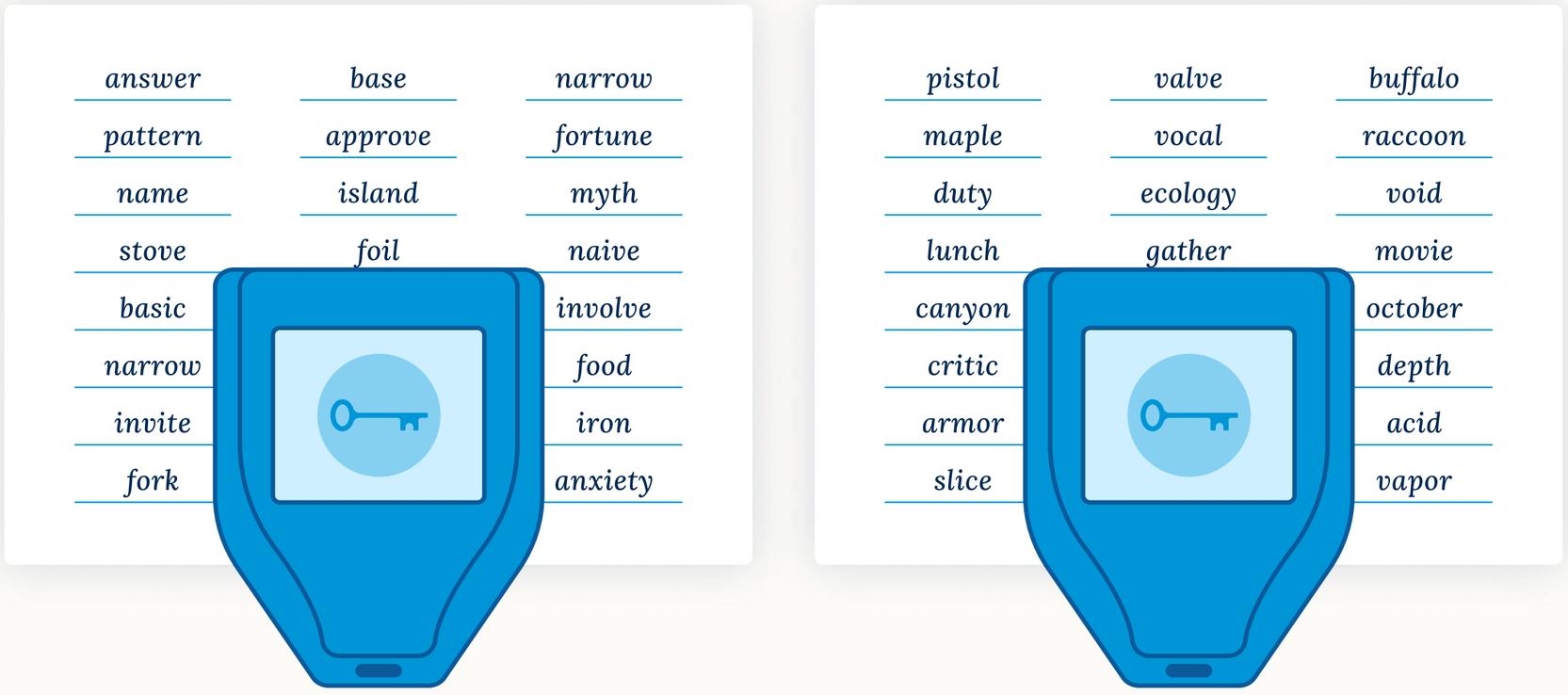
Seed phrase encoding

Some singlesig users will think to encode their seed phrase, with the idea that if a thief finds the resulting information, they will be unable to decode it and obtain the original seed phrase to steal the bitcoin. There are many possible routes to attempt this, including using a secret formula to alter the words, or hiding your seed phrase within a larger set of words.

The more complicated the encoding strategy is, the less chance there will be for a thief to reverse-engineer access to the bitcoin. But this is a double-edged sword, because a complex encoding strategy can also increase the chances of making a mistake, or forgetting how to decode the resulting material yourself. In other words, it adds a new avenue for losing access to your bitcoin.

Multiple singlesig wallets

It is widely recognized wisdom to avoid “putting all your eggs in one basket.” If you hold all of your bitcoin in one singlesig wallet, then the ever-present risk of loss or theft could be a tough pill to swallow. As a result, some people decide to hold portions of their bitcoin among several different singlesig wallets.



Two hardware wallets with their associated seed phrase backups.

The downside to this strategy is that it adds complexity and creates additional sensitive items to keep track of. While splitting your bitcoin across wallets can remove single points of failure for the entire balance, it actually creates more single points of failure for substantial portions of your wealth. For example, if you create four singlesig wallets and spread out 25% of your bitcoin in each one, you may have reduced the chance of losing 100% of your bitcoin, but you will have also increased the chance of losing 25% of your bitcoin, in the event that any one of the four wallets becomes inaccessible or compromised. As we will soon see in the upcoming sections of this article, there are methods to remove single points of failure for your entire bitcoin balance without introducing this issue.

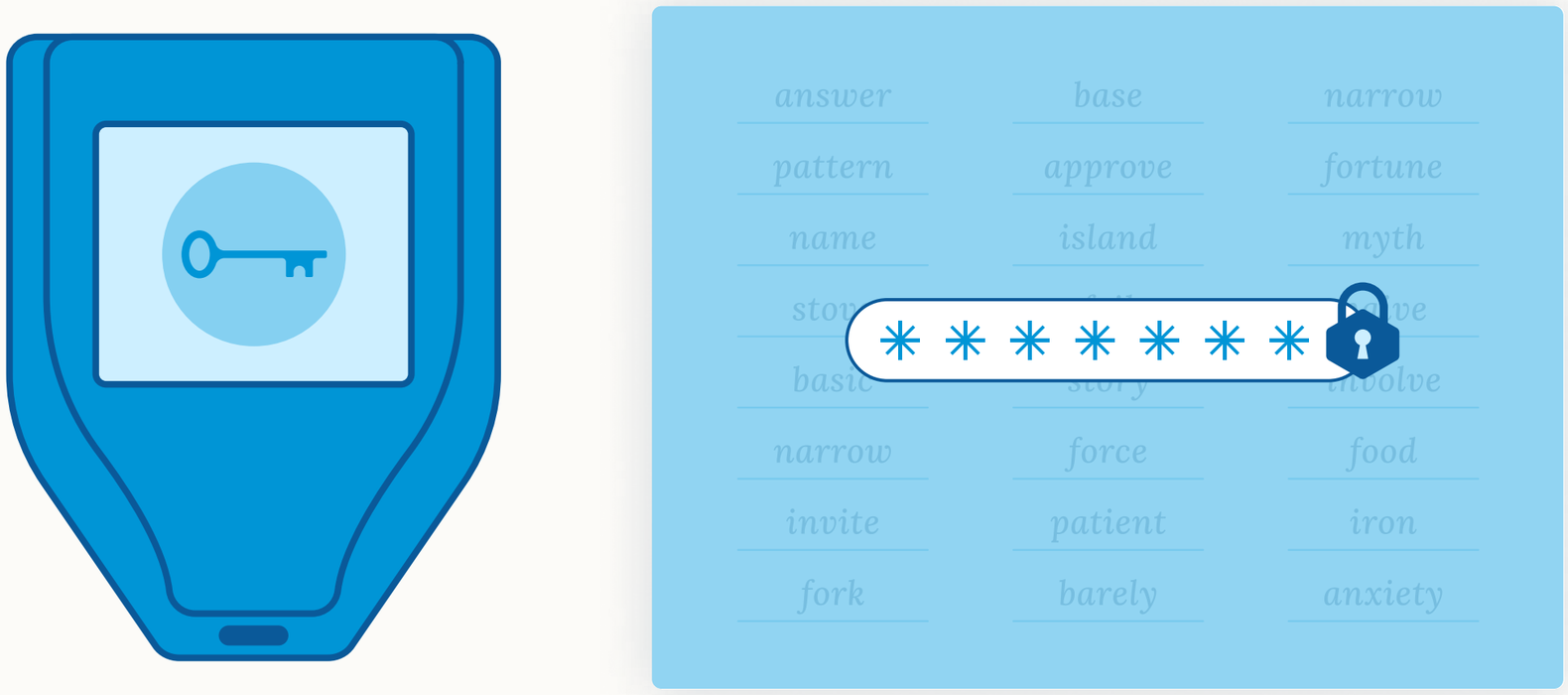
III. Standardized singlesig modifications

Besides some of the makeshift approaches listed above, there are also a few standardized tools available to help address certain risks with singlesig wallets. These include BIP 39 passphrases, Seed XOR, and Shamir's secret sharing. There are trade-offs to consider with each of these options as well.

BIP 39 passphrases

Whenever you generate a bitcoin key, you might be asked if you want to add a passphrase, or you may find the option to do this in the wallet settings. Passphrases are an additional set of characters added to the seed phrase (similar to a 13th or 25th word) that are sensitive to capitalization and can include numbers or special characters. They were introduced as a standard option alongside seed phrases in 2013 as a part of BIP39. If a key is built with a passphrase, then the passphrase will always be required to recreate the key and spend funds.

If a key includes a passphrase that is stored separately from the seed phrase, the result is similar to seed phrase splitting. For someone to access the bitcoin, both components would be required, which adds resistance to theft. A passphrase can actually achieve this without the same security risks as seed phrase splitting, and it also leaves the option open for a decoy wallet (a lesser amount of funds protected by the seed phrase alone, allowing you to plausibly deny that you have additional funds that can be discovered with a passphrase).



A hardware wallet and its associated seed phrase, plus a BIP39 passphrase.

On the other hand, passphrases also create another critical component that could be lost, causing you to permanently lose access to your bitcoin. If you store a passphrase in writing, and then it becomes misplaced or destroyed, your seed phrase will not be enough to regain access to your funds. You would also face a similar situation if you tried to memorize your passphrase and then end up forgetting it. Note that simple, easy-to-remember passphrases are weak and ineffective because they could be guessed by an attacker. It is best to use a strong passphrase instead, but doing this and attempting to remember it is one of the most common ways that people lose bitcoin in self custody.

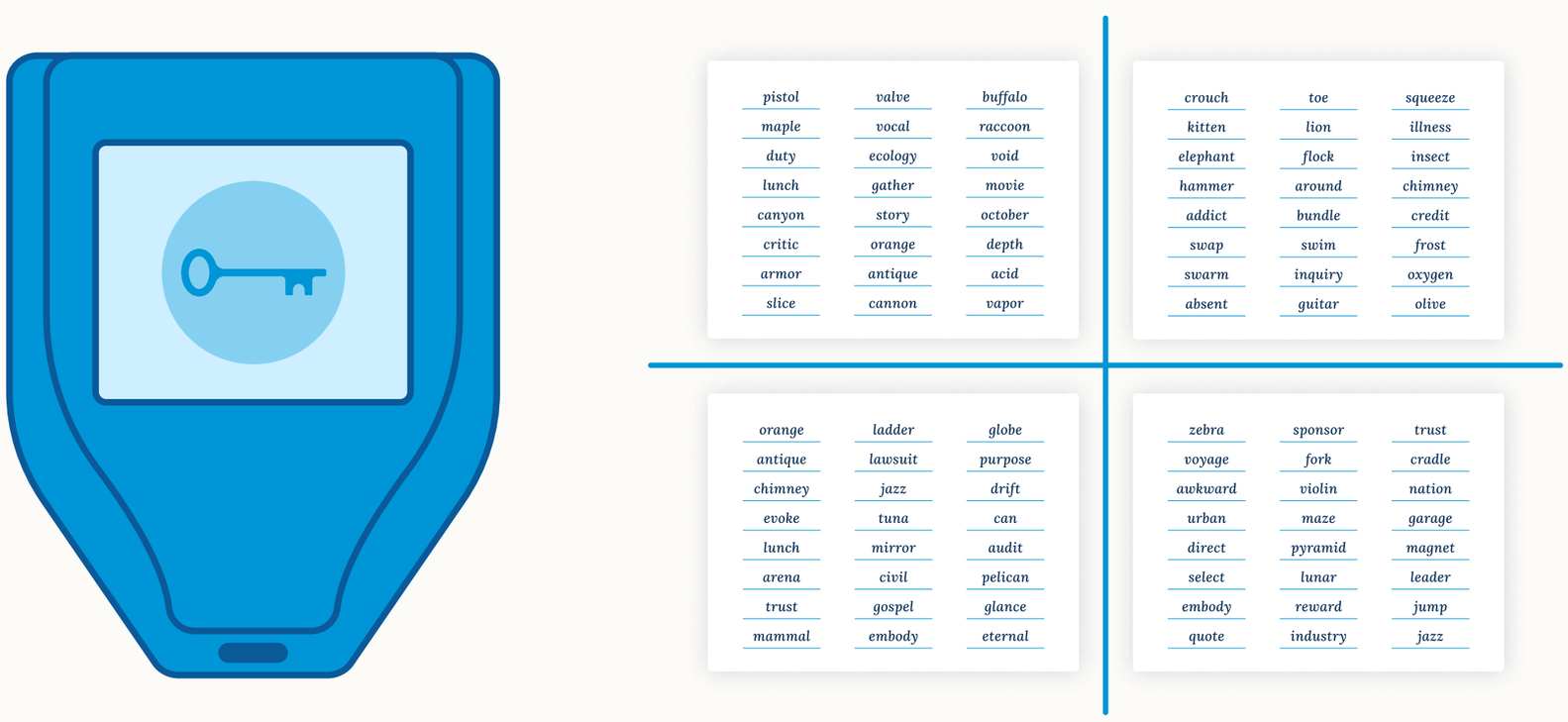
Seed XOR

Coinkite, the manufacturers behind the Coldcard hardware wallet, have introduced another solution called Seed XOR. By using some mathematical magic, Seed XOR allows you to take your seed phrase and split it into multiple unique 12 or 24 word seed phrases that would all need to be recombined in order to reproduce the original seed phrase. By storing the new seed phrases separately, this creates another form of seed phrase splitting without the security risks mentioned in the improvised setup. It also provides the option for decoy wallets, because each resulting seed phrase component could also be used as a key for a new singlesig wallet with a smaller amount of funds.

While Seed XOR functionality is built into Coldcards as an option, the math required to perform the splitting or the recombination can also be done on paper without a Coldcard device. However, keep in mind that Seed XOR contains a similar drawback to what we've covered in previous sections. While offering resistance to theft, it increases the chance of losing access to your bitcoin, because if any one of the newly produced seed phrases becomes lost, you will be unable to recreate your original key and spend out of the original wallet. Next, we will investigate a couple of technologies that can avoid this issue.

Shamir's secret sharing

In 1979, renowned cryptographer Adi Shamir formulated a secret sharing algorithm known as Shamir's secret sharing (SSS). It works by taking secret information (which could be a bitcoin private key) and using it to produce several new pieces of information, sometimes called "shards" or "shares". The shares are useless on their own and must be combined to reproduce the original secret. What makes SSS special, and different from something like Seed XOR, is that it can be structured so that only a portion of the shares are needed to produce the secret, rather than all of them. For example, a user could create a 2-of-3 quorum, where three unique shares exist but any two of them could be brought together to recreate the secret.



A hardware wallet with its seed phrase backup split into multiple parts using Seed XOR.

A hardware wallet with its seed phrase split into multiple parts with Shamir's Secret Share.

The creators of the Trezor hardware wallet, Satoshi Labs, introduced a standard for using SSS while creating a bitcoin key. It's called the "Shamir backup," and the details can be found in SLIP 39. It exists as an option while setting up a Trezor Model T, and if this option is chosen, the device will produce the user's desired quorum of shares, each expressed as 20 words. These sets of 20 words cannot be used as a seed phrase for a decoy wallet (like with Seed XOR), and should not be combined with other words in order to attempt this, because SLIP 39 uses its own special word list.

A notable weakness of SSS is that when the required number of shares are used to reassemble the bitcoin key, perhaps to spend funds out of the singlesig wallet, a temporary single point of failure occurs. The entirety of the key must exist in one place at the time of the signature, which could be an opportune window for exploitation by an attacker. This is an inescapable fact for singlesig, no matter what modifications are used. Multisig, however, can avoid this issue and remove all single points of failure for your bitcoin custody.

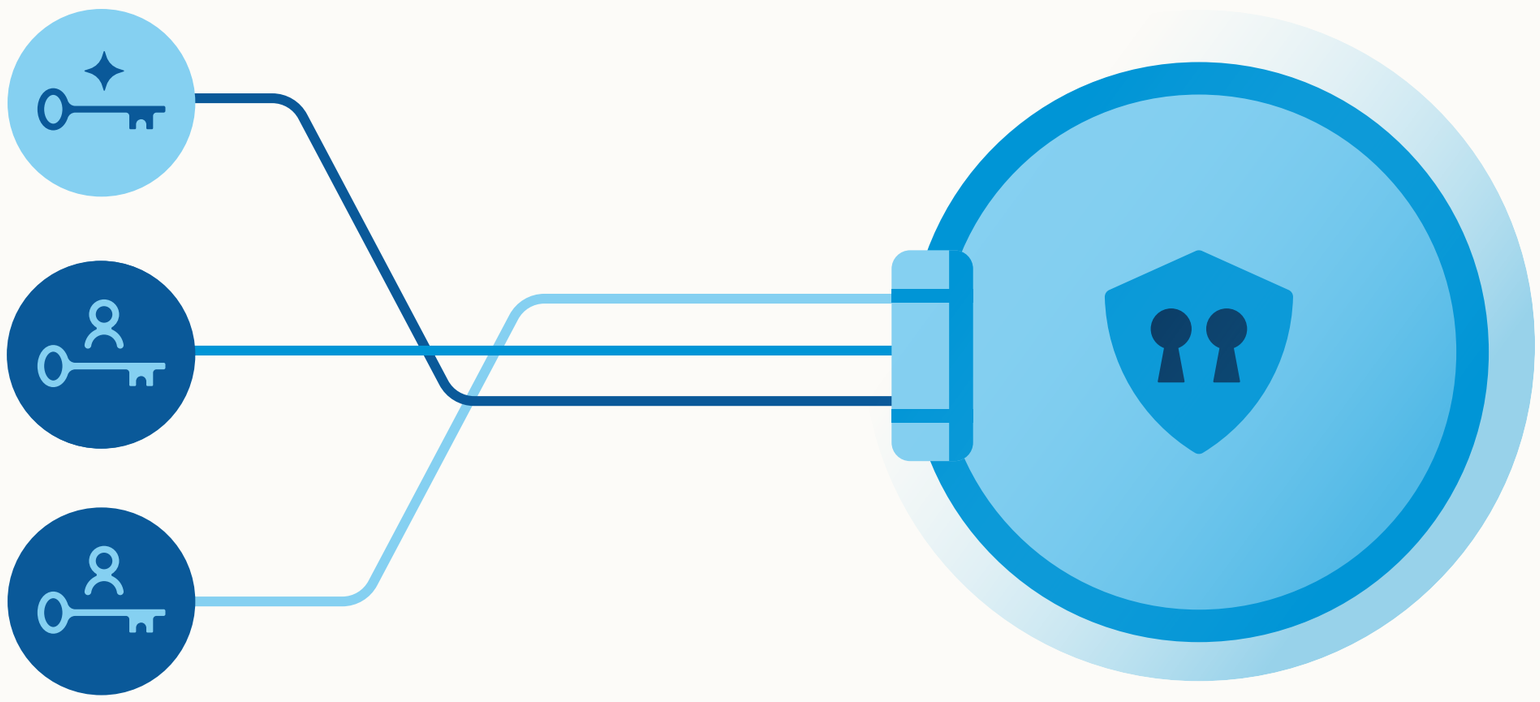
IV. Multisig

Finally we have arrived at multisignature, which is not a singlesig modification like we've covered up to this point, but a fundamentally different structure for holding bitcoin.

As we described in our multisig guide, a multisig wallet is created with multiple unique keys. The number of keys involved is determined by the wallet creator, as well as the amount of those keys that are required to sign off on spending bitcoin out of the wallet. These numbers are expressed as a quorum, such as 2-of-3, which would mean that there are three keys and two of them must provide signatures to spend bitcoin.

Multisig offers much better security than singlesig by eliminating single points of failure—protecting your bitcoin from loss and theft. While not all multisig quorums offer these protections, setups like 2-of-3, which is the only option Unchained offers, sit in a sweet spot for addressing both of these categories adequately for most individuals and businesses.

While multisig quorums might be similar to SSS quorums, there is an important difference. If a transaction is created to spend bitcoin out of a multisig wallet, each key can sign independently, at a different time and place. In other words, although a 2-of-3 multisig wallet requires two keys to sign off on a withdrawal, those keys never



A multisig vault with an individual holding two keys and a collaborative custody partner holding one.

need to be co-located. In fact, the keys don't even need to be brought together when the wallet is first being created, which is not true for SSS. This is great from a security perspective, and is also a much more convenient structure for a group of people who want to manage a bitcoin treasury with different members holding different keys.

Trade-offs: Inconvenience and fees

Multisig provides robust security for your bitcoin, but it comes with the trade-off of lesser convenience. Multisig makes it far more difficult for an attacker to spend your bitcoin, but that comes at the cost of convenience for the end-user as well.

Transactions involving multisig have also historically cost more in mining fees than transactions involving singlesig (on average). However, now that the Taproot soft-fork has been activated, this fact may begin to change. With new technologies utilizing Taproot and increased Taproot adoption, multisig transactions will have the same fee structure as singlesig transactions.

DIY vs. collaborative custody

Because multisig is more complicated than a basic singlesig wallet to set up and use, a significant downside to attempting multisig on your own is the lack of reliable technical support. As we explained in our article covering the basics on this topic, the wallet owner will have more keys to keep track of, and the details about how the wallet was configured is also important to save (in the form of a wallet descriptor or wallet configuration file). If someone is new to bitcoin, managing these extra pieces can feel overwhelming.

Multisig collaborative custody businesses like Unchained can provide the education and support needed for anyone to feel comfortable and confident with multisig. A collaborative custody vault can be accurately called a form of self-custody, because you are the only one who has full power to spend the bitcoin. This approach will typically involve sharing some information with your collaborative partner about your bitcoin, but it comes with the benefit of a simpler setup by reducing the number of items you need to keep track of yourself, help with wallet maintenance, support for passing bitcoin on to beneficiaries, and easy access to financial services like trading and loans.

What about 3-of-5?

One important decision in setting up a multisig vault is choosing the proper quorum, and 2-of-3 and 3-of-5 are by far the most widely used for securing bitcoin in cold storage. While it may be useful in certain circumstances, 3-of-5 introduces more complexity than necessary for most. It can provide extra redundancy, but this point can be repeated to advocate for 4-of-7, and then 5-of-9, and so forth to infinity. We made a graphic to help visualize this.

V. Comparison chart

Now that we have covered all of the well known structures for holding bitcoin, let's place them in a chart to compare their features!

Unchained	SINGLESIG	SINGLESIG WITH PASSPHRASE	SINGLESIG WITH SEED XOR	SINGLESIG WITH 2-OF-3 SHAMIR SECRET SHARE	2-OF-3 DO-IT-YOURSELF MULTISIG	2-OF-3 COLLABORATIVE MULTISIG
SINGLE POINT OF FAILURE IN STORAGE	YES	YES	YES	DEPENDS*	NO	NO
SINGLE POINT OF FAILURE WHILE SIGNING	YES	YES	YES	YES	NO	NO
VULNERABILITY TO LOSS	HIGH	HIGHEST**	HIGHEST	LOW	LOW	LOW
VULNERABILITY TO THEFT	HIGH	LOW**	LOW	LOW	LOWEST	LOWEST
DECOY WALLET CAPABILITY	NO***	YES**	YES	NO***	YES	YES
EASY ACCESS FOR BENEFICIARIES	YES	NO	NO	NO	NO	YES
NONTECHNICAL WALLET SETUP AND OPERATION	YES	YES	NO	NO	NO	EXPERT ASSISTANCE
SPENDING CONVENIENCE	HIGH	HIGH	DEPENDS*	DEPENDS*	LOWEST	LOW
AVERAGE TRANSACTION FEES	LOWER	LOWER	LOWER	LOWER	HIGHER****	HIGHER****
UPFRONT PRIVACY TRADEOFF	NO	NO	NO	NO	NO	YES

* This depends on whether or not you have wiped your hardware wallet in addition to splitting up your physical seed phrase with SSS or Seed XOR.

** Weak passphrases have a chance of being guessed, but strong passphrases are easier to forget yourself.

*** Decoy wallets are technically possible with nonstandard derivation paths or other methods, but are not recommended because it can introduce new risks.

**** With increased Taproot adoption, multisig will have the same fee structure as singlesig.

Unchained

VI. Should I use singlesig or multisig?

As shown in the chart above, there are tradeoffs between all of the different structures for holding bitcoin in self-custody, and this means there is not a universally correct approach. In order to determine whether singlesig or multisig is the better model for you, you must first decide upon your preferences and priorities.

Singlesig and multisig tend to excel in opposite areas, and this important observation begs the question: why not use both? Rather than viewing these models as opponents, they can be perfect compliments to one another! It's reasonable to consider using a multisig wallet for high-security, long-term bitcoin savings and simultaneously using a singlesig wallet to hold smaller amounts for convenient transactions (perhaps a mobile wallet that also supports lightning).

If you're interested in the advantages of collaborative custody multisig, which keeps you in full control over your bitcoin custody while also offering technical support, streamlined inheritance, and easy access to other services, be sure to book a free consultation with the Unchained team! 🤝