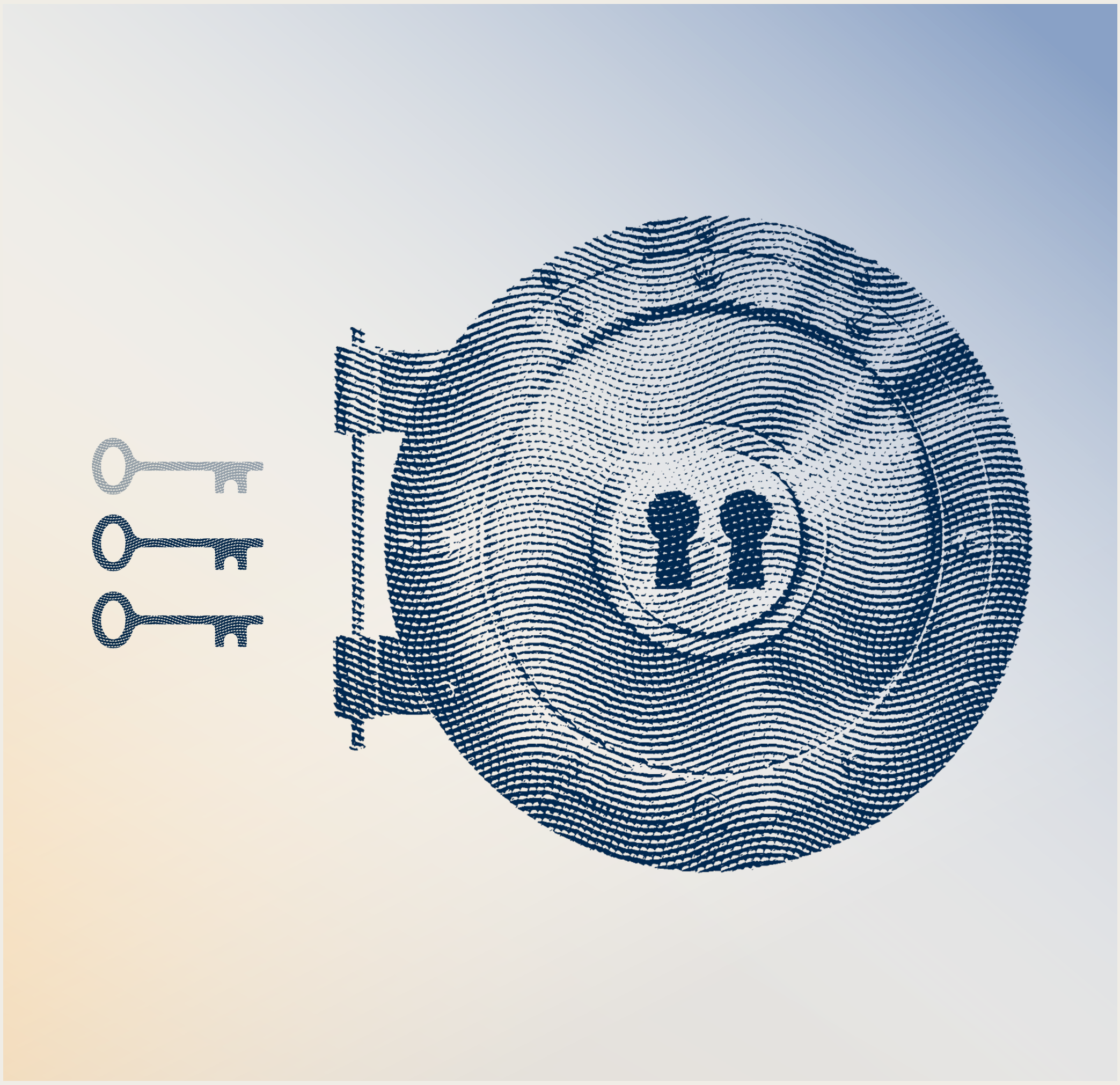
Unchained

What is *Multisig?*

HOW TO SECURE YOUR GENERATIONAL WEALTH



TOM HONZIK & STEPHEN HALL

JANUARY 2026

Unchained

Contact

Follow Unchained on X: @unchained

Send Unchained an email: hello@unchained.com

Unchained

Outline

I. Why should I self-custody?

II. Why use multisig?

III. Additional applications

IV. Trade-offs with multisig

V. How to use multisig

Unchained

What is multisig?

When it comes to storing your bitcoin, multisignature—or multisig for short—is widely recognized as one of the most secure methods. It can eliminate risks associated with exchanges and custodians, and simultaneously addresses the most common issues with self-custody. In this article, we're going to walk through why you should hold your own bitcoin keys, what standard singlesignature self-custody looks like, and how multisig is an improvement for long-term cold storage.

I. Why should I self-custody?

Interest in bitcoin usually begins with recognizing it as an alternative monetary tool that remedies some of the clear dangers of conventional money, such as inflation, censorship, and confiscation. As motivation grows for transferring wealth into bitcoin, people are immediately faced with the decision of how to safely store it.

The first piece of advice you might hear is to avoid custodial solutions. The reason for this is simple: custodians of fiat currencies like the U.S. dollar (banks, brokerages, etc) can offer certain guarantees that custodians of bitcoin cannot. For example, government programs like the FDIC and SIPC provide insurance for when a custodian loses client deposits, and this obligation can always be met. Bitcoin has a strict supply limit—21 million coins—and new units can never be arbitrarily issued to replace coins that are lost by an irresponsible or malicious custodian.

Avoiding a custodian implies taking self-custody. In the world of bitcoin, custody is determined by who controls the private keys, because the private keys are the tools required to spend bitcoin. If you have purchased bitcoin on an exchange and haven't withdrawn it to your own custody controlled by your own keys, then the bitcoin remains controlled by the exchange's keys, and all you have is an IOU, rather than actual bitcoin. As the popular saying goes, "not your keys, not your bitcoin."

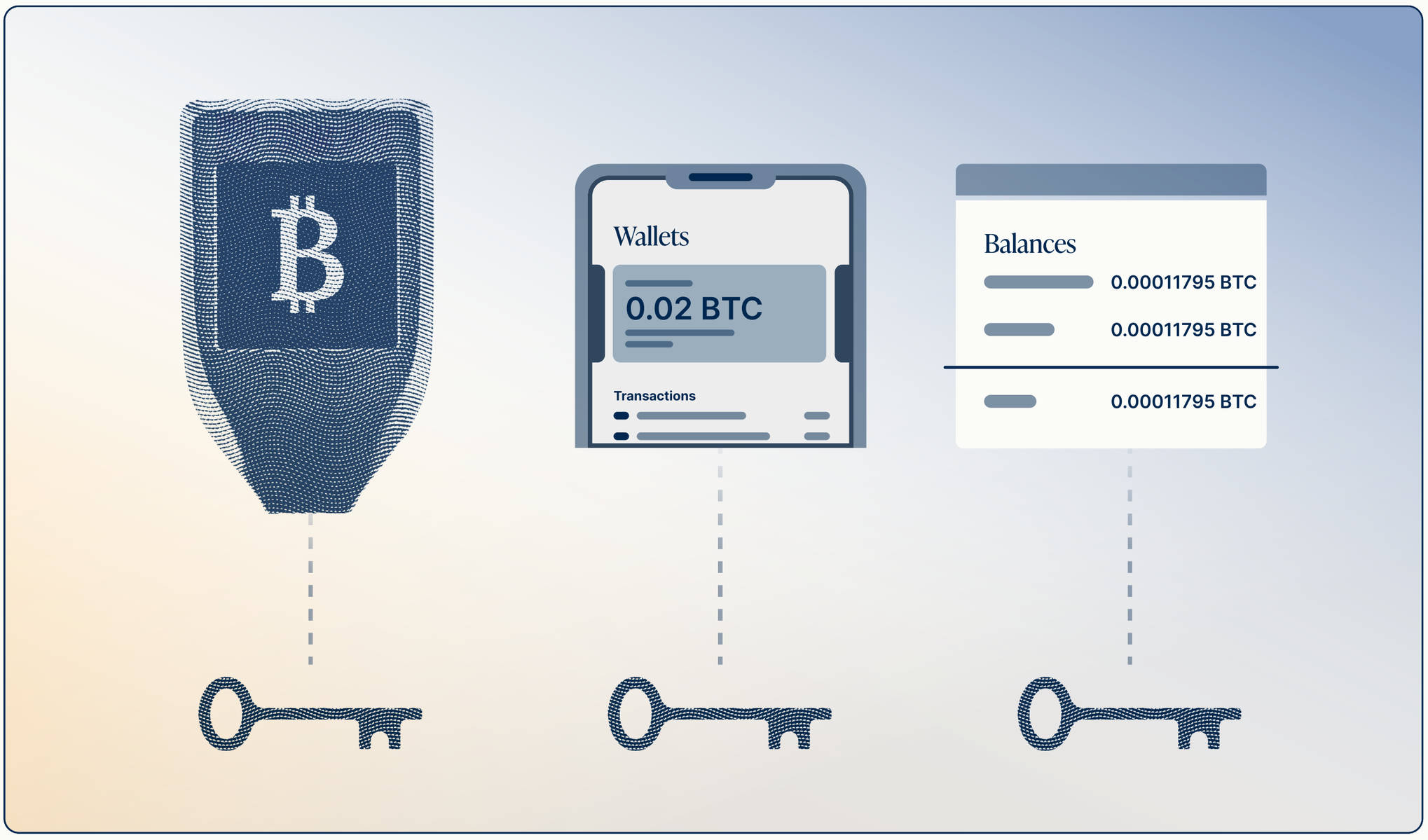
Holding your own keys simply means protecting secretive information, because that's what a private key is: randomly generated data that should be kept private, and cannot realistically be guessed by anyone else. Generating a private key is easy, and can be done on a laptop or a phone app, but it is preferable to use a hardware wallet so that you can have confidence your key was never exposed to the internet. Check out some of our other articles to learn more about the reasons to use hardware wallets, and some of the best device models.

It is completely normal to feel apprehensive about holding your own bitcoin keys. People often lose information such as passwords, or physical items such as sunglasses and car keys. If you are worried that you might lose your bitcoin keys and therefore also lose access to your funds, that is a valid concern! However, multisig can help you rest easy knowing that you have backup plans in the event that you make a mistake and lose some information.

A singlesig wallet is the simplest and most widely used form of self-custody bitcoin wallet. It involves just one master private key, which can generate addresses for receiving bitcoin. If bitcoin is sent to one of those addresses, the amount will be counted towards the wallet balance, and it can only be removed from the wallet after approval from someone who has the private key.

First, what is singlesig?

To understand multisig, it’s important to first understand the predecessor method of bitcoin storage: singlesig.



A few examples of wallets commonly used as “singlesig”

The private key holder can demonstrate approval for a withdrawal by using the private key to cryptographically sign the transaction. You can imagine this like a physical signature being applied to a document that specifies the transaction details, in a verifiably unique way that can't be forged. This is done within your software wallet, or for bitcoin in cold storage, within a hardware wallet. Then the signed transaction can be broadcast to the bitcoin network, where it will only be recognized as valid if the correct signature was applied.

Singlesig wallets have the benefit of being simple to set up, as well as providing fairly quick and easy access to withdrawing funds. Singlesig transaction fees can also cost less than multisig.

However, a major drawback to singlesig is that it always involves a single point of failure. Specifically, there are two glaring issues:

1. **Vulnerability to theft:** If your private key is exposed to someone else, that person may have what they need to steal your bitcoin.
2. **Vulnerability to loss:** If you lose your private key information (due to negligence or a natural disaster), you can lose the ability to spend your bitcoin, meaning you effectively no longer own it.

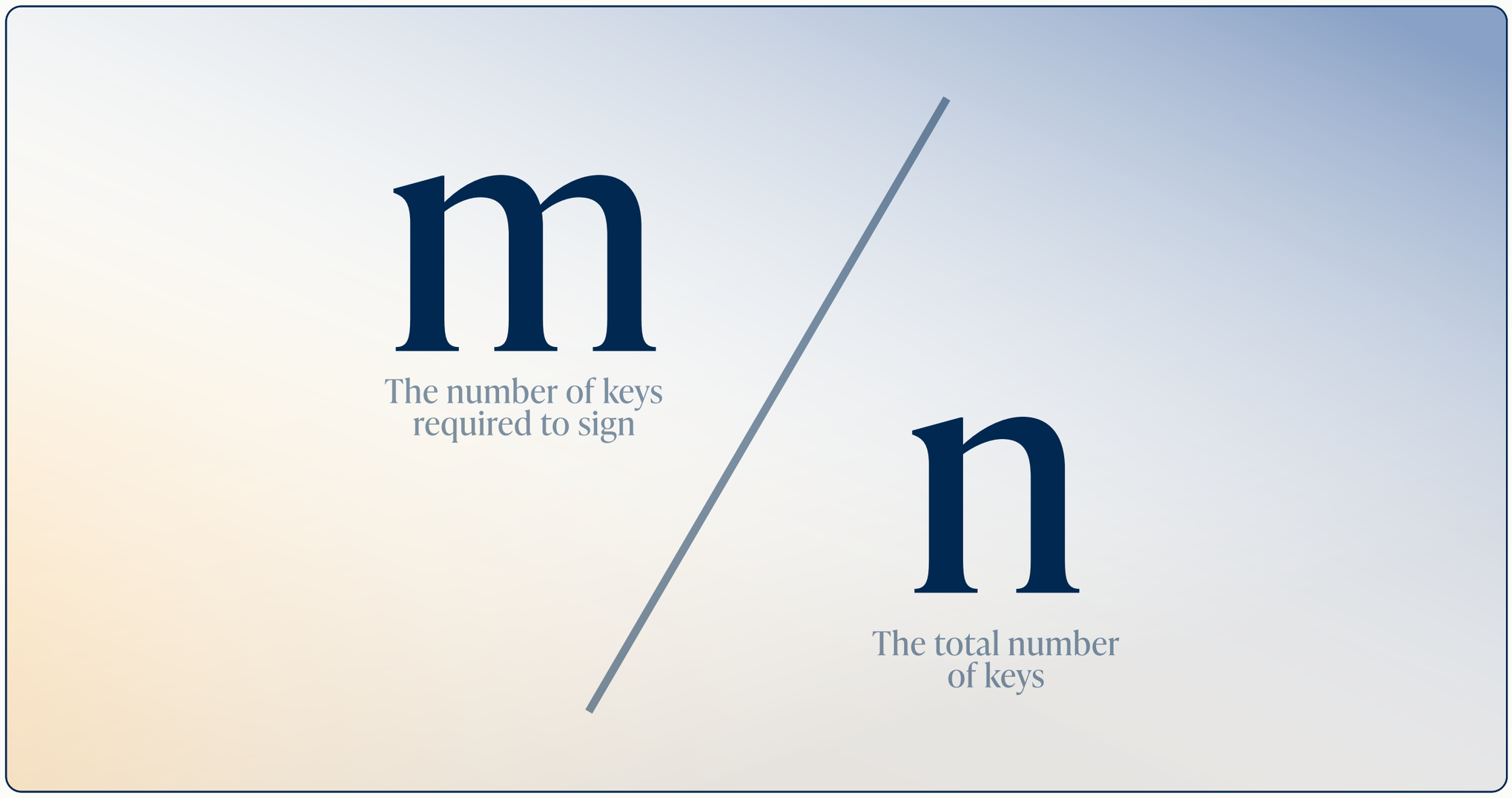
Various mechanisms have been created in an attempt to mitigate these concerns. Introducing tools such as BIP 39 passphrases or Seed XOR into a singlesig setup can help address the first issue, but they come with the trade-off of exacerbating the second issue. Another tool called Shamir's Secret Sharing can create an improvement on both ends, but a single point of failure will still exist when it comes time to sign a transaction.

As a result, many people turn to multisig as the gold standard for removing single points of failure.

How is multisig different?

While bitcoin secured by singlesig requires one signature from one specific private key to spend funds, this is just the beginning of what bitcoin makes possible. A multisignature bitcoin wallet, as the name suggests, is a method of securing bitcoin that can require signatures from multiple private keys in order to spend the bitcoin. A subset of those keys are needed to sign off on spending any bitcoin that has been received into that arrangement.

This structure is popularly described as an m-of-n quorum. The "m" represents the number of private keys that are required to sign for a withdrawal to become valid, while the "n" represents the number of private keys that exist which can produce one of the required signatures.

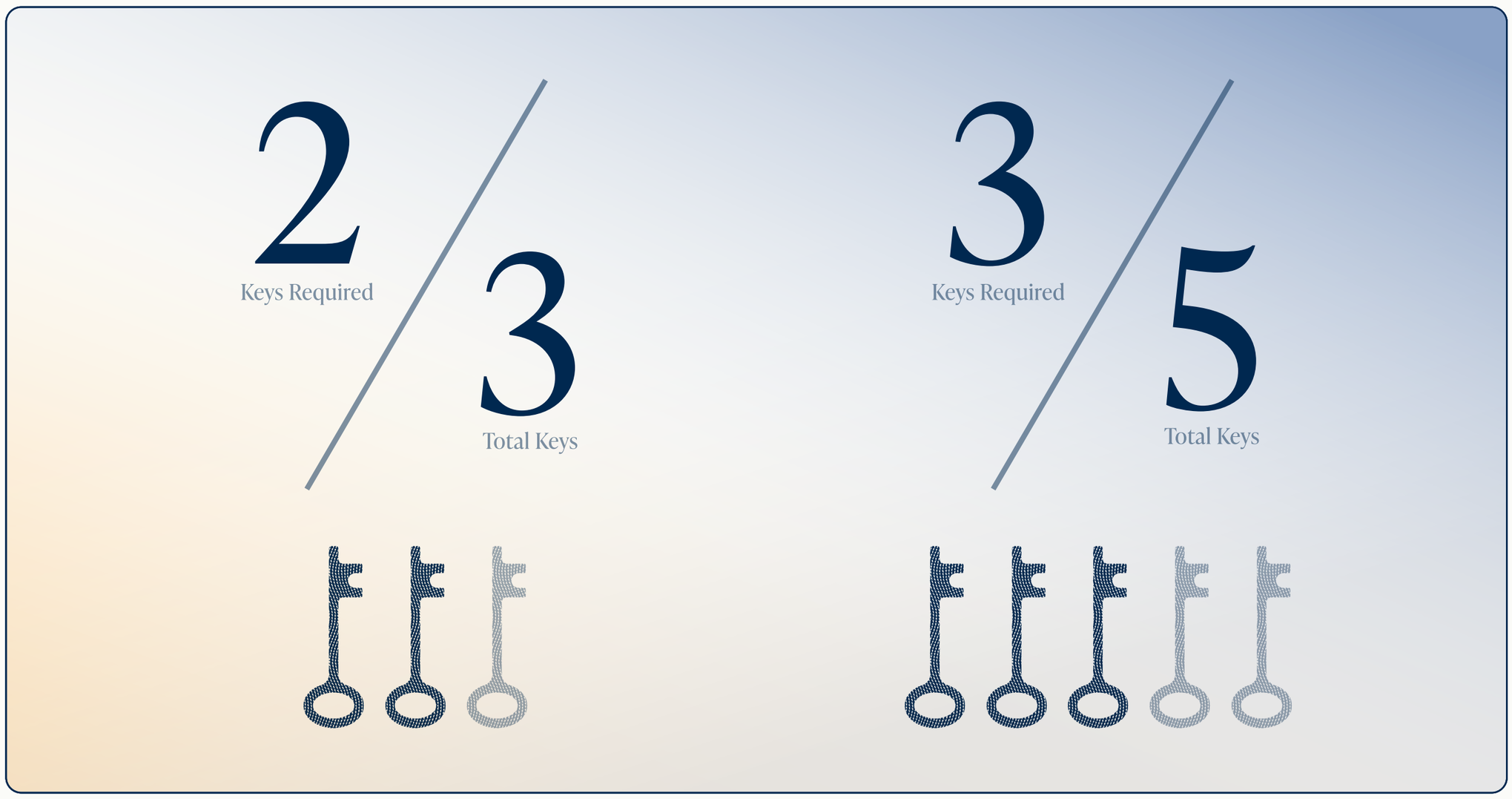


An “m-of-n” quorum representing the keys required to sign and the total number of keys in the multisig setup.

For example, a 2-of-2 quorum indicates that there are two different private keys involved, and signatures from both keys are required to withdraw bitcoin that was received into that arrangement. This idea might be familiar to you if you have ever used a safety deposit box at a bank. Typically, these boxes require two keys to be opened, one of which is held by you, and the other is held by the bank. There are also ancient examples of similar approaches.

Alternatively, you could create a 1-of-2 quorum, where only one out of the two keys involved is needed to approve a spend. Or you could create a quorum that involves more than two keys, such as a 2-of-3. This would mean that three keys exist in the setup and any combination of two of them can sign off on spending bitcoin.

Multisig quorums are customizable to meet the needs of the user, so it can be extended to almost any quorum you could imagine—5-of-6, 2-of-9 or other complex setups. However, some quorums are dramatically more popular than others. 2-of-3 and 3-of-5 are by far the most widely used arrangements for securing bitcoin in cold storage, for reasons that we’ll cover below.



The most common bitcoin quorums: 2-of-3 and 3-of-5. Both strike a balance between complexity and security.

II. Why use multisig?

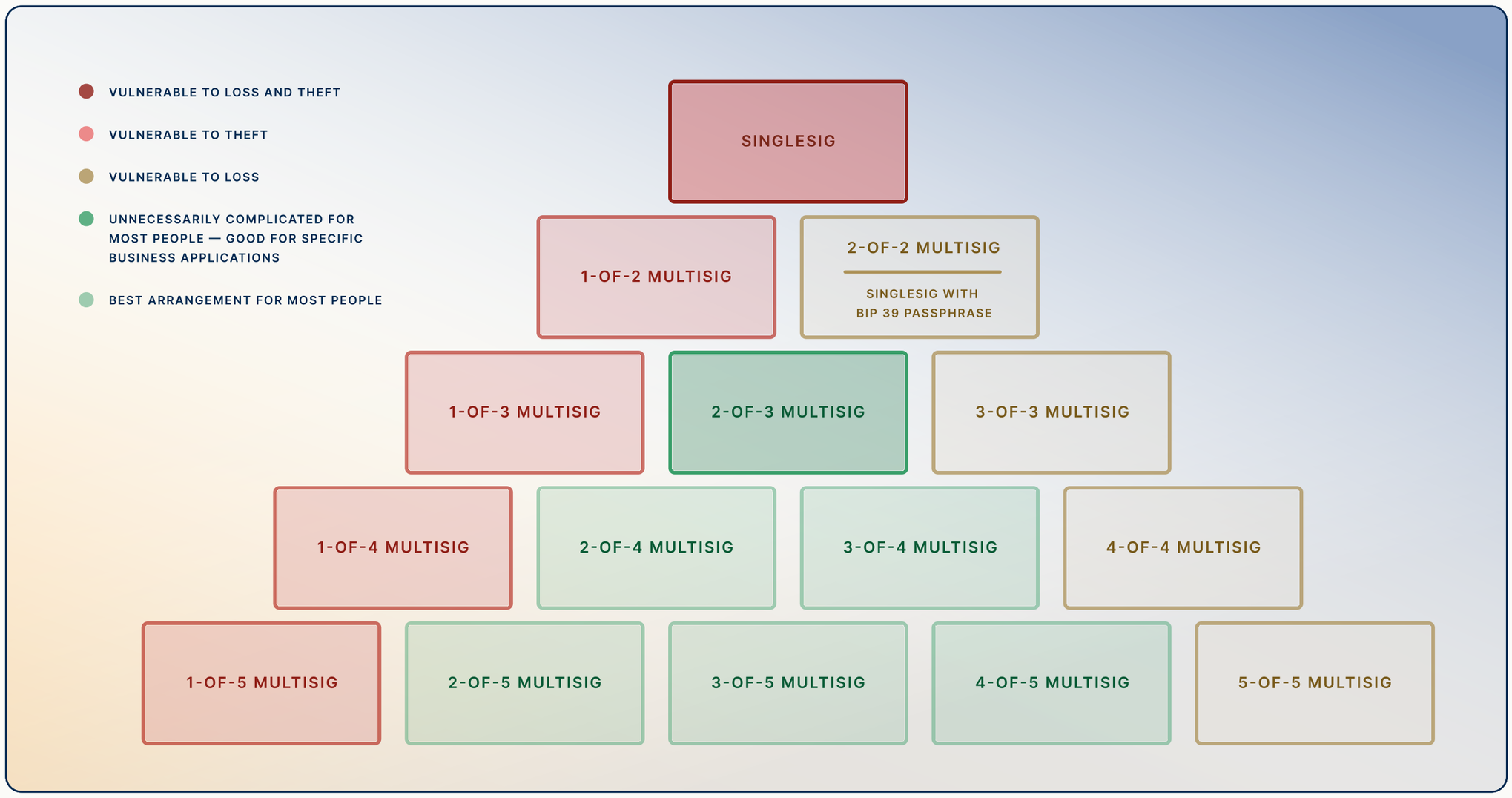
Switching from singlesig to multisig means introducing more keys, and therefore additional complexity. Is it worth it? Let’s take a look at some of the advantages and disadvantages.

Upgraded security

Earlier we discussed some of the biggest concerns that come with using singlesig. These included single points of failure, such as your private key being exposed, lost, or destroyed. How can multisig help?

With certain multisig quorums, redundancy is added to ensure that there's no one thing that, if it breaks or stops working, will cause you to lose your money. You can rest easy knowing that if one of your private keys is exposed to someone, they will not have all the pieces needed to steal your bitcoin. Additionally, if one of your keys is lost or destroyed, you can still recover your bitcoin by using the remaining keys in your possession to transfer funds into a new wallet where you once again have all the pieces.

However, not all multisig quorums offer these protections. A “1-of-n” quorum (such as 1-of-2 or 1-of-5) does not provide adequate resistance to theft, because if any one of the keys is exposed to someone, that person may have what they need to steal bitcoin from you (they still need the associated multisig file). On the other hand, an “n-of-n'' quorum (such as 2-of-2 or 5-of-5) would imply that if any one of the several keys are lost or



Some arrangements disproportionately expose you to risk of theft, while others expose you to risk of loss. 2-of-3 multisig protects you from both with the least amount of added complexity.

destroyed, you will no longer be able to spend your bitcoin.

Setups that fit in between these two extremes are the sweet spot for addressing both categories of single points of failure: loss and theft. The least complex arrangement that satisfies both goals is 2-of-3, which is also the most popular multisig quorum for securing bitcoin in cold storage, and the only one we use at Unchained. A 3-of-5 quorum is a fairly popular arrangement as well, but it introduces more complexity than necessary for most situations. While 3-of-5 can provide extra redundancy, this point can be repeated to advocate for 4-of-7, and then 5-of-9, and so forth to infinity.

If you want to get the most out of the protections offered by a multisig arrangement, you should store all of your different keys in geographically separated locations, so that no two keys can be lost or exposed at the same time. The less complicated your multisig setup is, the easier it will be to create an effective system for keeping your keys secure and separated. You can read more about the trade-offs between 2-of-3 and 3-of-5 in our deeper dive on the topic.

III. Additional applications

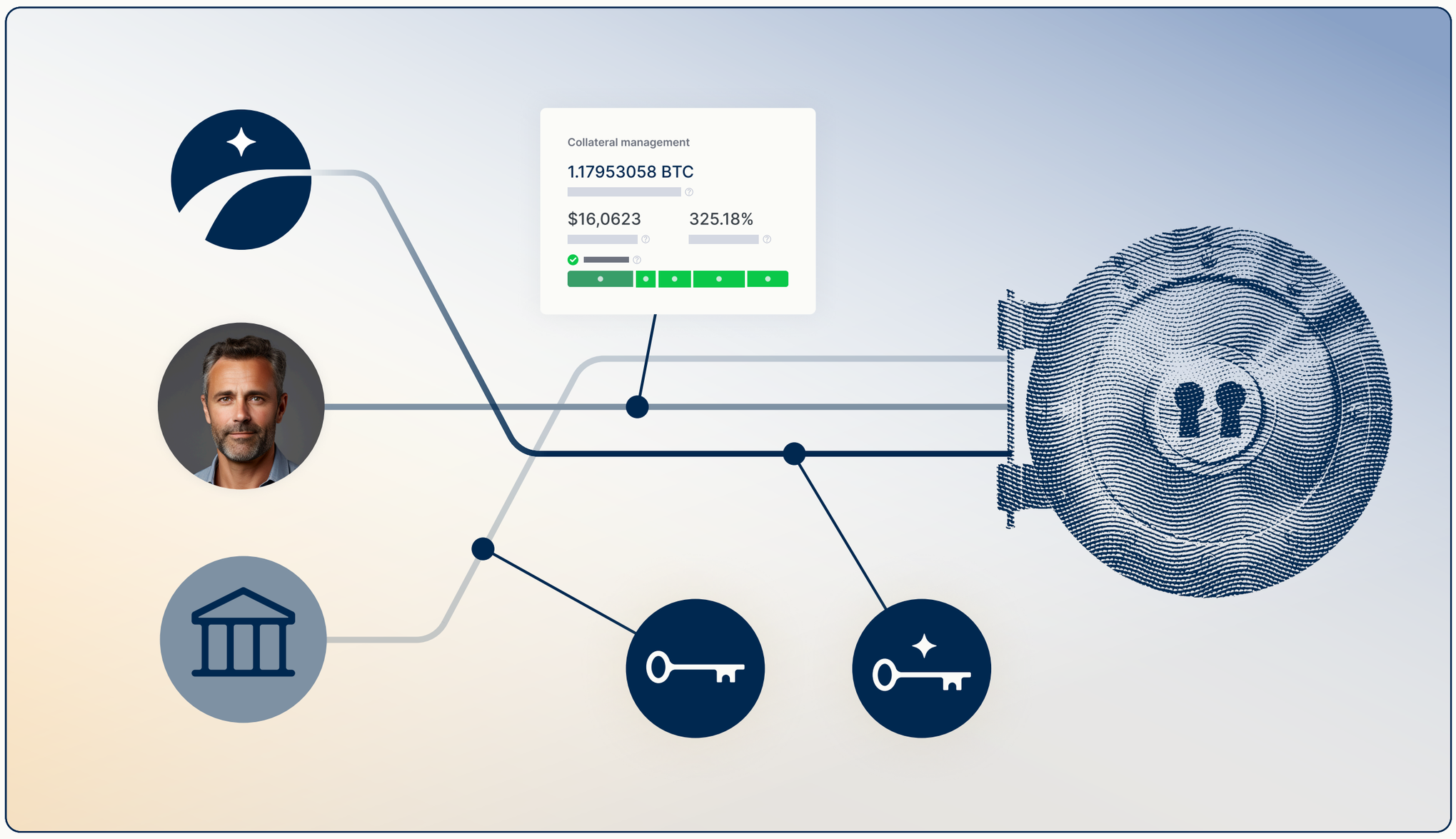
Besides offering new custody options for individuals, multisig can open the door for serving the needs of groups of people. By creating a structure where different people hold different keys within the multisig quorum, some attractive possibilities become available. Let's briefly cover a couple examples.

Treasury management

If a business, government or other organization wishes to hold bitcoin intelligently, multisig is all but required. Not only because of the increased security, but also to ensure that the people within the organization have the appropriate level of power to spend funds on behalf of the group.

Suppose a committee or legislative council consists of 9 people, and this group will be responsible for managing a bitcoin treasury. If each member of the group secures a private key, they can customize their structure so that a particular threshold of members must sign off on a treasury withdrawal. Spending funds could require a small portion of the group (3-of-9), or a majority (5-of-9), or even a supermajority (6-of-9).

Special members of a group like this could also possess additional power to spend funds, if they hold additional keys within the chosen quorum.



Some multisig arrangements allow three parties to share custody to enable things like secure collateralized loans.

Trust-minimized collateral

Many bitcoin holders want to exercise the purchasing power of their bitcoin without selling it, which could result in capital gains taxes as well as missing out on future increases in value.

A popular solution to this dilemma is a bitcoin-backed loan, usually built with a 2-of-3 multisig quorum. A bitcoin holder can borrow cash from a lender after depositing their bitcoin into the multisig wallet, where the borrower keeps one key, the lender holds one key, a third party arbitrator holds one key, and two keys are required to withdraw bitcoin from the wallet.

Once the loan is repaid, the borrower and lender can use their keys to sign off on returning the bitcoin to the borrower's full control. If the loan is not repaid, the bitcoin can be transferred to the lender's full control. If there is a dispute, or either participant is noncooperative, the arbitrator can review the situation and assist the justified party.

With this model, stealing funds would have to involve collusion between two key holders, destroying the reputations of both entities. This structure is referred to as "trust-minimized," a substantial improvement over putting complete trust in a single custodian. It also ensures that the bitcoin is not being rehypothecated and remains available to be moved into the full custody of the rightful owner at any time.

Bitcoin-backed loans are a service offered by Unchained, and you can learn about specifics here.

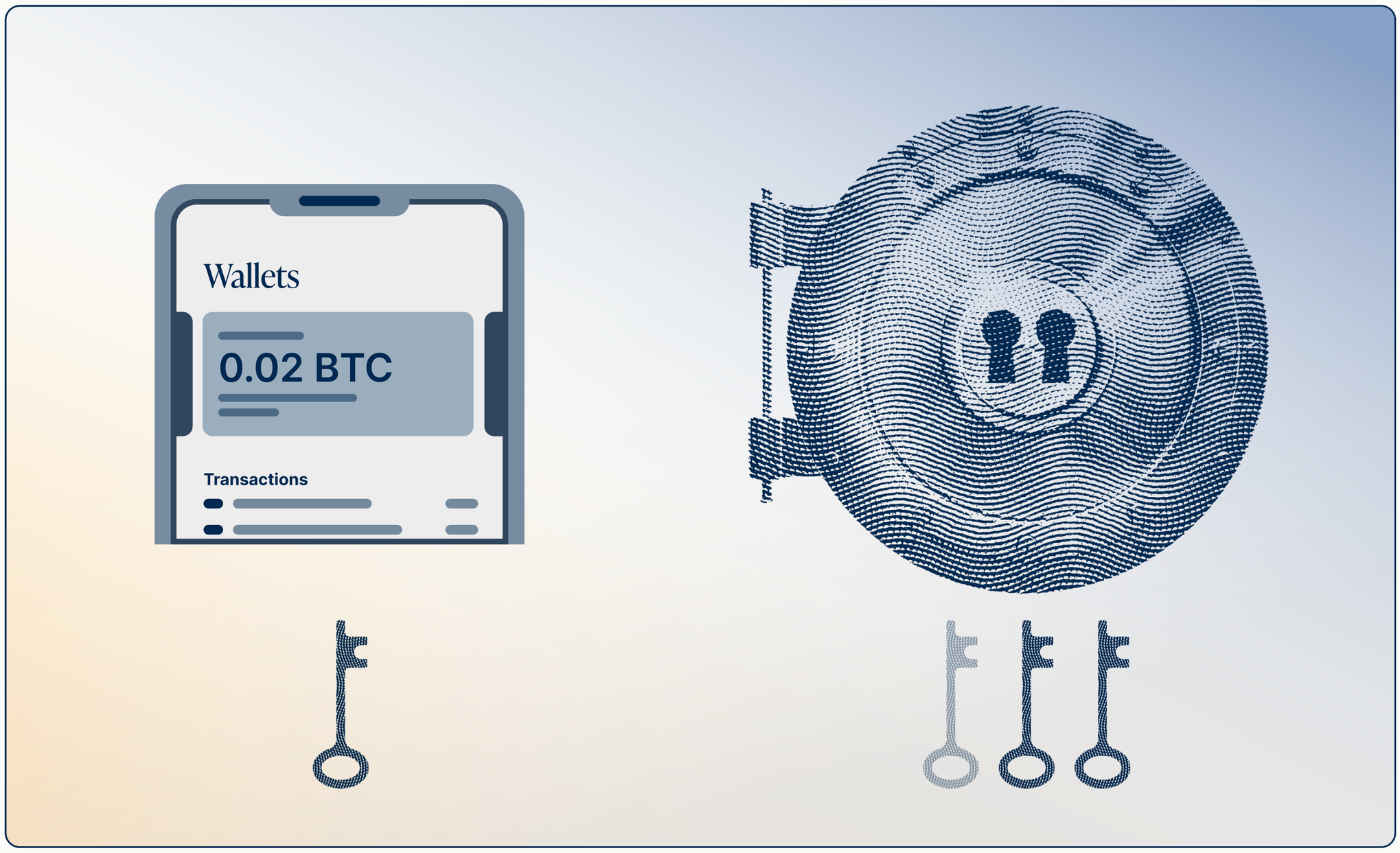
IV. Trade-offs with multisig

As noted earlier, there are a couple of trade-offs when using multisig compared to singlesig.

First is the obvious increase in complexity that comes with incorporating more keys into the custody arrangement. With more keys, there are more items to keep track of, and each item will ideally be kept in separate locations. This will make it more cumbersome to withdraw bitcoin out of the wallet, which is good for preventing unauthorized access, but can cause annoyance when you yourself need to move funds.

Another downside is increased transaction fees. If you receive bitcoin into a multisig wallet, when you later go to spend that bitcoin, it will typically cost you more than if it were in a singlesig wallet. This specifics depend on several other factors, but on average you will be paying more in fees the more complex your quorum is. In other words, singlesig will be cheaper than 2-of-3, and 2-of-3 will be cheaper than 3-of-5.

On the bright side, bitcoin's taproot upgrade in 2021 made it possible for multisig transactions to be indistinguishable from singlesig on the blockchain. This implies that they would cost the same, and there would be no extra fee burden for multisig quorums! However, at the time of writing, this technology has yet to be widely adopted.



At Unchained, we often recommend clients use a singlesig hot wallet for daily use and a multisig cold storage vault for long-term savings.

A popular strategy to utilize the protection benefits of multisig while reducing its drawbacks is to hold some bitcoin within both custody arrangements. For example, you could keep the vast majority of your bitcoin in a cold storage multisig wallet for the purpose of long-term savings, and simultaneously keep a much smaller amount of bitcoin in a singlesig hot wallet on your phone. That way, you could rest comfortably knowing the bulk of your bitcoin wealth has maximum protection, while at the same time you can easily send and receive smaller amounts in a more convenient manner.

V. How to use multisig

Most people who set up multisig for the first time are surprised at how easy and simple the process is, especially if they are already familiar with using singlesig. That said, there are still a couple of methods worth comparing before you dive in.

DIY (do it yourself)

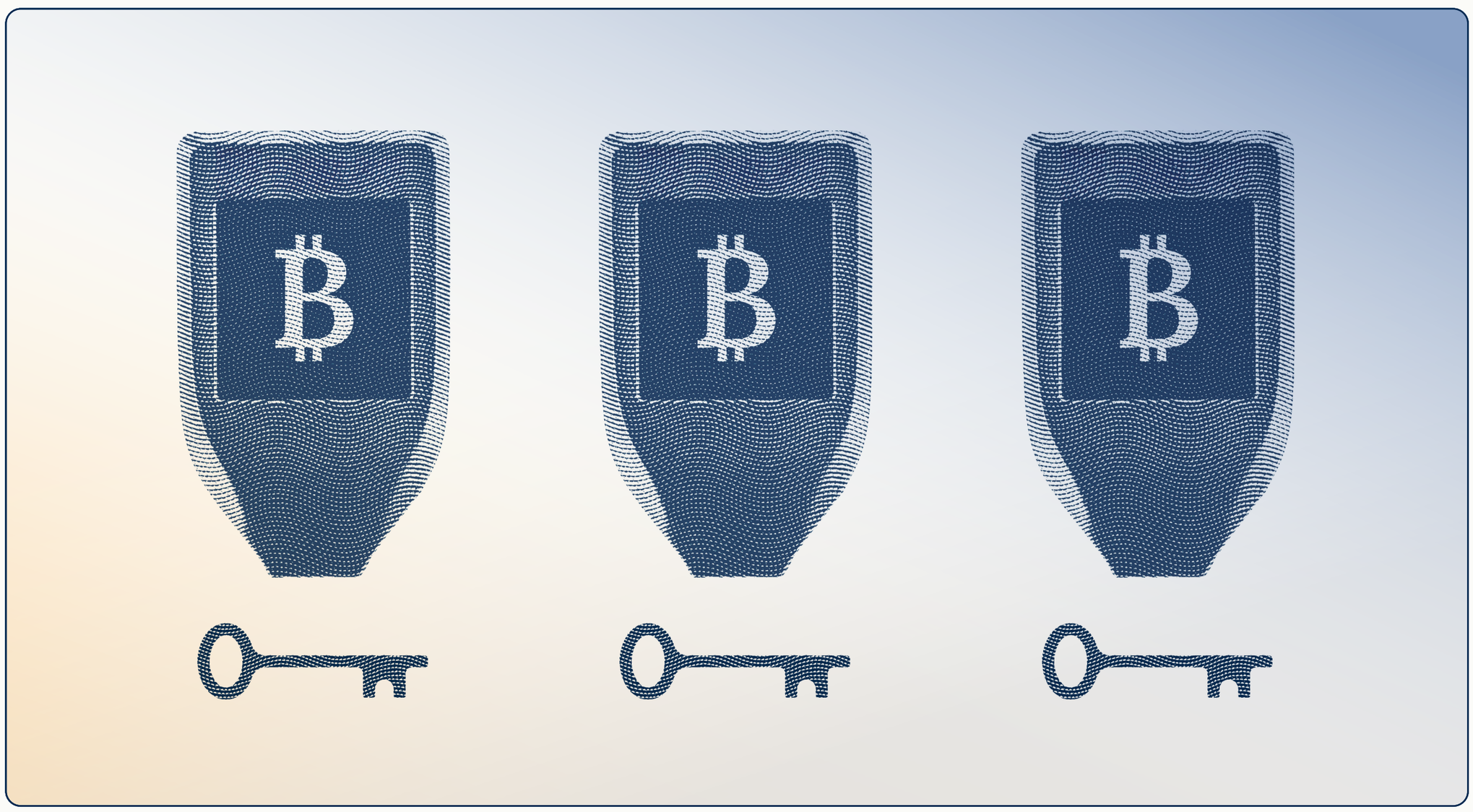
Free and open source programs exist to help you set up a multisig wallet all on your own. Examples of such programs include Caravan, Sparrow Wallet, Electrum, and Specter. There are video tutorials on YouTube if you would like some assistance learning how to use these programs.

Since most bitcoin wallet technology is built to be interoperable, if you use one of these programs to set up your multisig wallet, you should also be able to load that same wallet into one of the other programs (as long as you have your wallet configuration file saved). This provides some peace of mind that if something goes wrong with software you're using, your bitcoin is still safe and accessible.

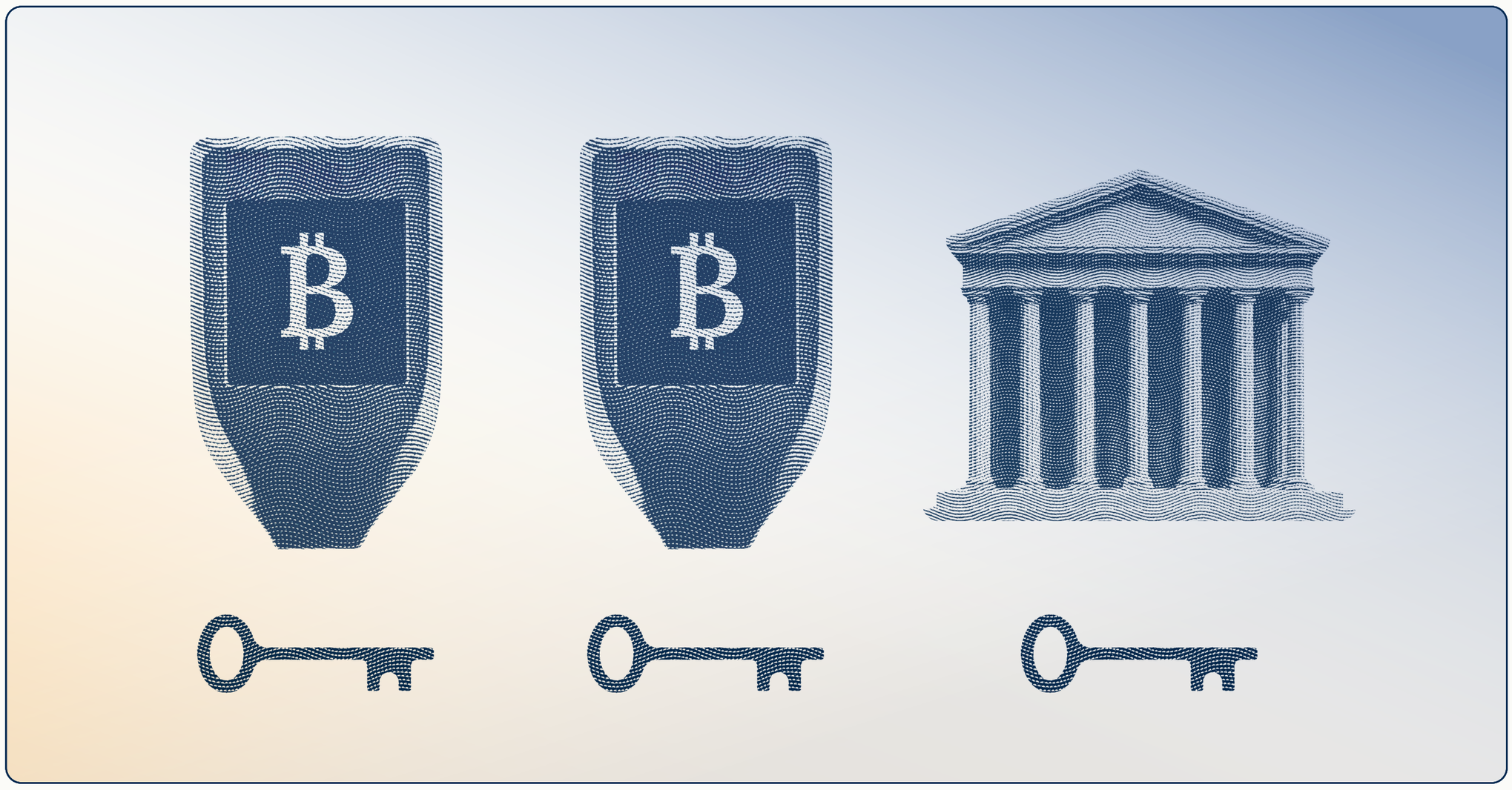
Creating a DIY multisig wallet can be a rewarding educational experience, and it can also be a particularly private method of getting set up. However, if you run into any technical difficulties down the road, it may be a headache to find someone trustworthy who can help you out. Similarly, if something tragic happens to you, your loved ones could be tasked with figuring out the complexities of your multisig arrangement in order to inherit your bitcoin, which they might find quite challenging.

Collaborative custody

While trusting a single custodian with your bitcoin has been shown to be dangerous, collaborative custody multisig is different. When done properly, you can maintain control over the keys to your bitcoin while having the added benefit of experts who can assist you with technical questions or inheritance.



You can set up multisig entirely on your own with several hardware wallets.



You can also set up multisig with fewer hardware wallets and a partner who controls a minority of keys.

For example, with an Unchained vault, a 2-of-3 multisig wallet is constructed where you hold two of the keys and Unchained holds only one key. This means that Unchained can never move your funds out of the vault without your permission, because we can only provide one signature while two signatures are required for any and all withdrawals.

On the other hand, since you hold two of the keys, you can provide the two signatures needed for a withdrawal without ever relying on Unchained's key! What's more, signing and broadcasting a transaction is a permissionless activity, so as long as you are keeping your keys safe and accessible, nobody can ever prevent you from moving your bitcoin elsewhere. Similar to a DIY multisig wallet, you could always load an Unchained vault into another software (using the wallet configuration file) so you aren't forced to rely on our website or business.

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 in your vault. At the same time, Unchained's key can come to the rescue if you lose one of your keys, or it can be used to help streamline the process of passing down your bitcoin in accordance with our Inheritance Protocol.

Using collaborative custody is not perfectly private, because your collaborative partner will have team members with clearance to see your wallet balance while they are assisting you with technical questions. However, it is important to remember that Unchained takes client privacy extremely seriously, and it is impossible for Unchained to spend your funds or restrict your access to your funds.

If you are interested in setting up an Unchained vault, we invite you to learn about our **Concierge Onboarding** package. You will have as much time as you need with one of our experts personally guiding you through every step, and making sure all of your questions are answered.