

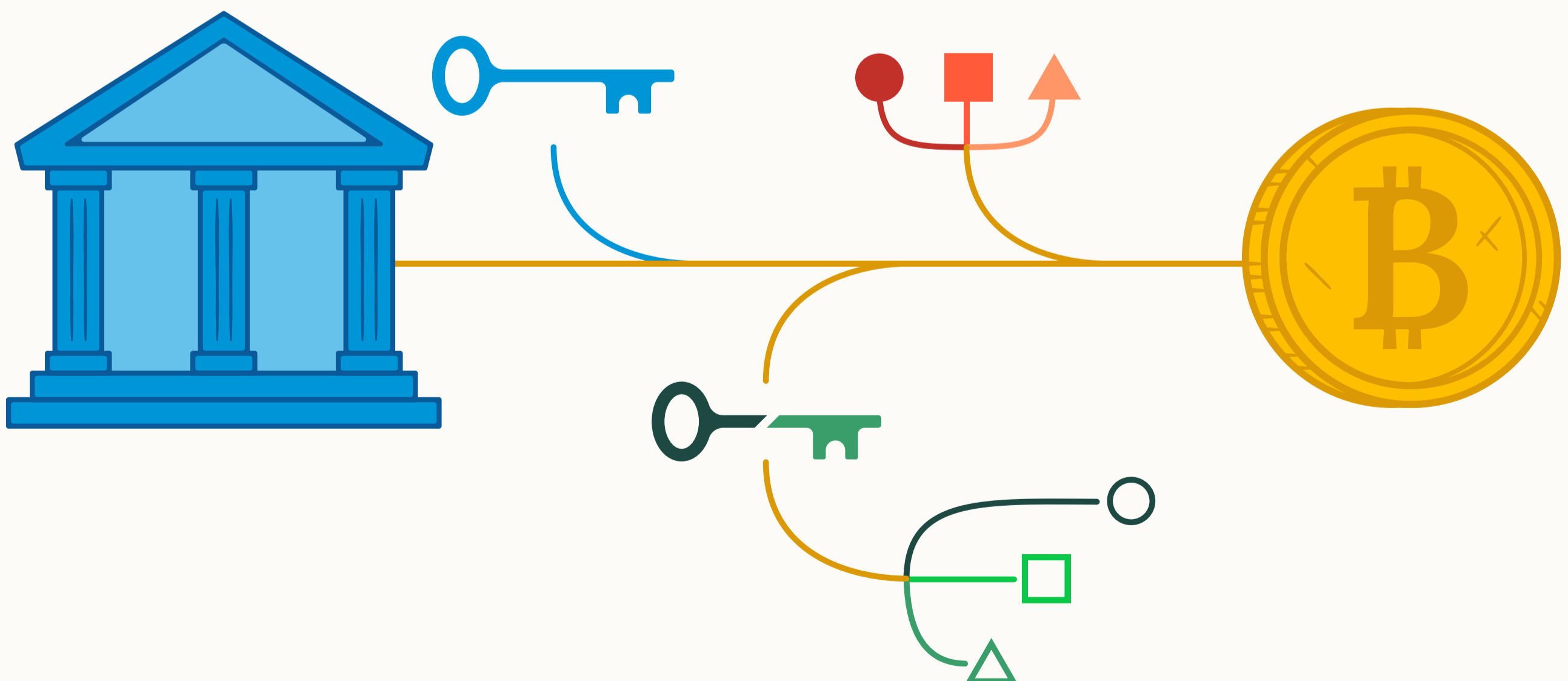
BITCOIN CUSTODY

# Multisig, Shamir's secret sharing, & MPC compared

TAKING A CLOSER LOOK AT  
THRESHOLD SECURITY MODELS  
FOR INSTITUTIONAL-GRADE  
BITCOIN CUSTODY

TOM HONZIK

FEBRUARY 2024



# Contact

Follow Tom Honzik on twitter: [@tom\\_honzik](https://twitter.com/tom_honzik)

Send Tom Honzik an email: [thomas@unchained.com](mailto:thomas@unchained.com)

Follow Unchained on twitter: [@unchainedcom](https://twitter.com/unchainedcom)

Send Unchained an email: [hello@unchained.com](mailto:hello@unchained.com)

This article is provided for educational purposes only, and cannot be relied upon as tax or investment advice. Unchained makes no representations regarding the tax consequences or investment suitability of any structure described herein, and all such questions should be directed to a tax or financial advisor of your choice.

Unchained Capital, Inc. is not a bank. Unchained Capital, Inc. (NMLS ID: 1900773), Unchained Trading, LLC (NMLS ID: 2273761), and Bitcoin Collateral Services LLC (NMLS ID: 2423070) are licensed to provide certain financial services.

# Outline

I. Defining the different approaches

II. What are the trade-offs between threshold models?

III. Which model is best?

IV. Final thoughts

# I. Defining the different approaches

For anyone with substantial bitcoin holdings, a custody structure that includes a single point of failure should be seen as unacceptable. If a wallet has a single component that—when lost or stolen—can lead to a permanent loss of funds, then it's simply too dangerous to consider. Nobody wants to keep significant wealth teetering on the edge of catastrophe.

Individual bitcoin holders have numerous tools available that can help reduce the risk of loss or theft. [In a previous article](#), we covered some of these tools, highlighting modifications commonly applied to singlesig wallets. However, we also explained why these approaches fall short of removing single points of failure entirely.

For a business, government, or other institution that wants to secure a bitcoin treasury, eliminating single points of failure is not just a nice-to-have, but a prerequisite. The only custody models worth considering for these entities are ones that include a threshold requirement in order to access funds. A threshold requirement describes a structure that involves multiple, separately secured components, where a subset of those components are needed to approve any withdrawal. This is the only way of achieving institutional-grade security, with single points of failure eliminated completely.

In this article, we'll cover how to apply threshold security using three different methods: script multisig, Shamir's secret sharing (SSS), and multi-party computation (MPC). We'll also dive into the tradeoffs associated with each approach, and how an institution can choose the best setup to meet their needs.

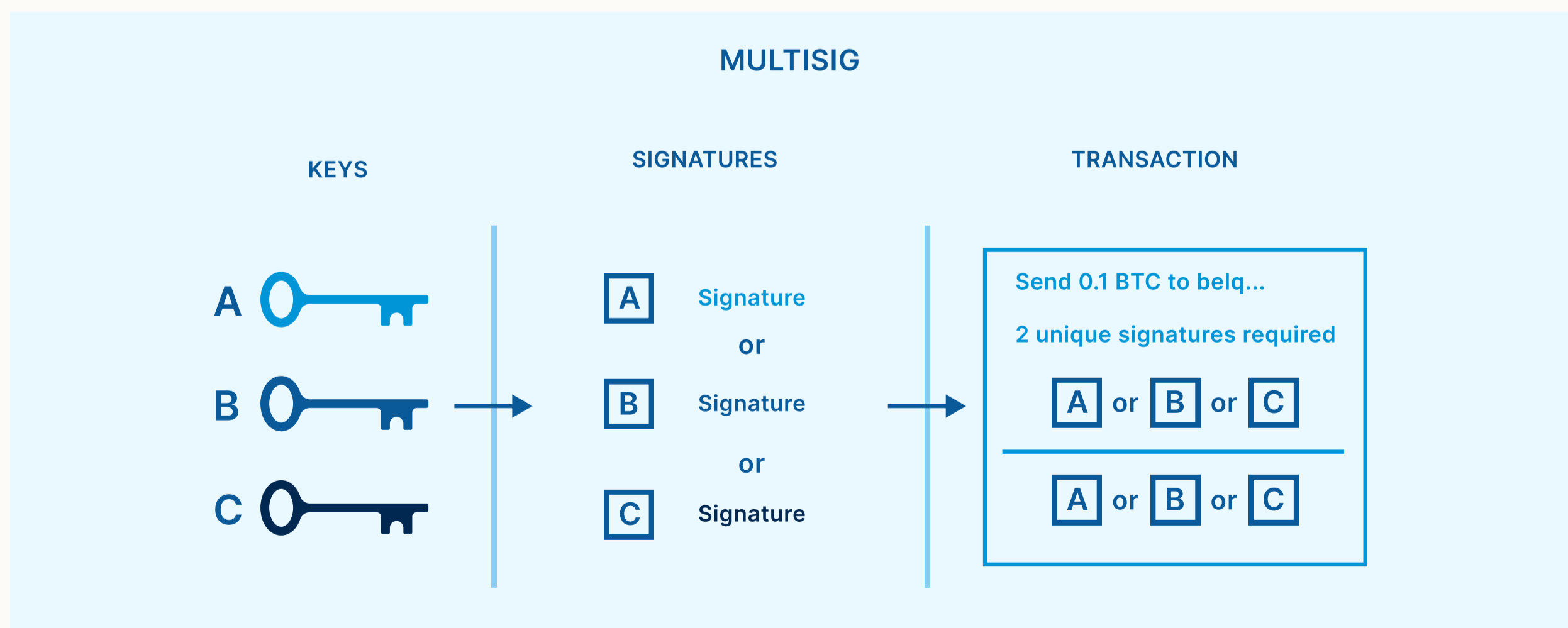
# What is multisig?

If you aren't sure what script multisig is, we recommend checking out our [earlier article](#) dedicated to explaining how multisig wallets work and what they're used for. As a quick review, a multisignature wallet involves multiple [private keys](#), and can be configured so that a specific number (threshold) of those private keys are required to sign any transaction. The signatures can be produced at different times and locations, allowing each key to remain physically separated. Once a threshold number of signatures have been produced, they can be combined into a single bitcoin transaction capable of spending the funds.

This relatively simple way of creating a threshold requirement is highly effective at removing all

single points of failure. As long as the spending threshold is greater than one but less than the total number of keys, then any single key can become lost, stolen or destroyed without bitcoin becoming unrecoverable. The remaining keys could sign a recovery transaction moving funds to a fresh multisig setup.

Satoshi Nakamoto laid the groundwork for multisig when bitcoin was first released, anticipating that it could be a popular mechanism for securing funds. However, it wasn't until the [P2SH softfork in 2012](#) that multisig started to become a widely used tool. Multisig has since proven itself as a battle-tested security model for more than a decade, across several different [address types](#).



A 2-of-3 script multisig quorum, where a threshold of two unique signatures from two keys are required for withdrawals.

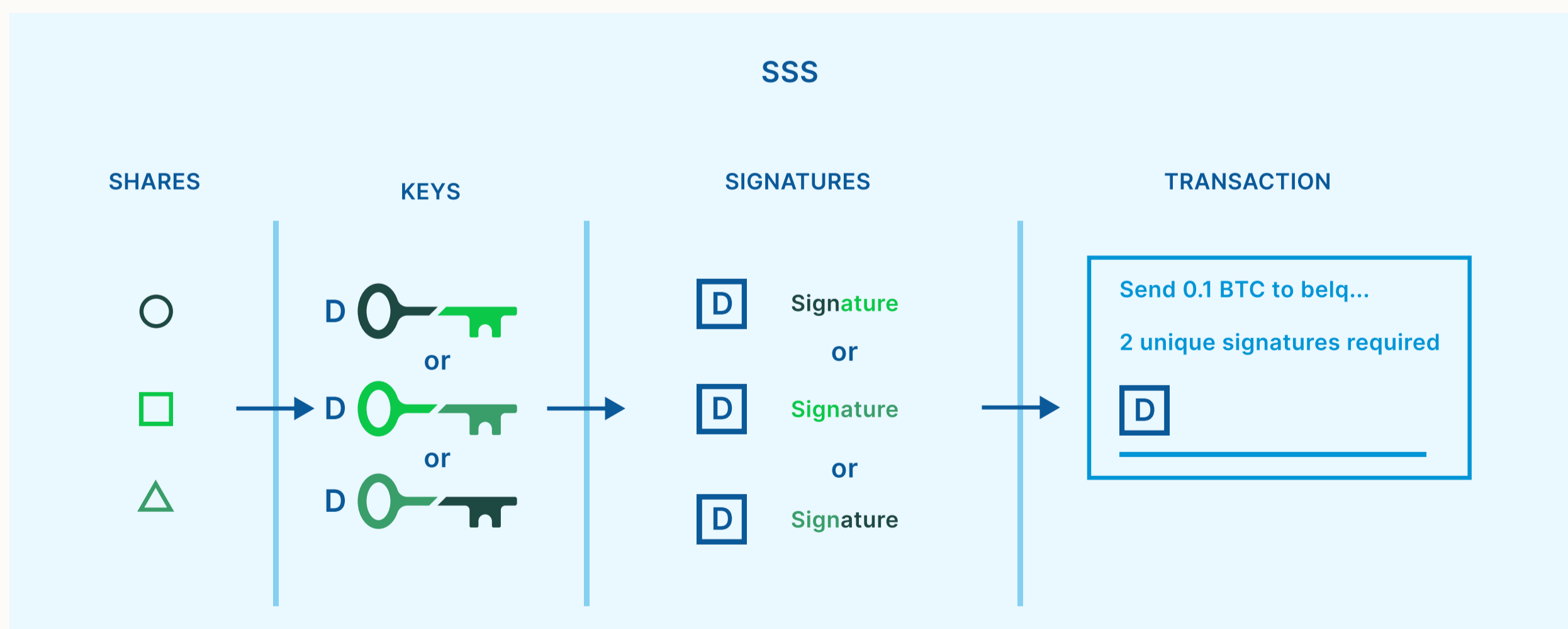
# What is Shamir's secret sharing?

Shamir's secret sharing (SSS) is a secret sharing algorithm that was developed by renowned cryptographer Adi Shamir in 1979. It can be used as another way of introducing a threshold requirement for protecting bitcoin. SSS allows users to split a key into several distributed "shares," with only a certain threshold of the shares needed to reassemble the key. This can be used to design quorums like 2-of-3 or 3-of-5, similar to multisig.

However, this approach still leads to single points of failure at certain instances during its lifecycle. One example is when the key is initially split up into SSS shares.

This operation is usually done on a single device at a single time and place. If an attacker compromises that device, the key generation process or the share creation process, they've compromised the key. Another example is whenever the user needs to reassemble the key to sign a transaction. A threshold number of shares must be brought together, once again on a single device at a single time and place, which an attacker could exploit.

A fairly simple and widely used method of implementing SSS technology for cryptocurrency custody is through the Shamir backup, developed by Satoshi Labs in 2017. It can be found as an option in certain Trezor hardware wallet models.



A 2-of-3 SSS arrangement, where any two shares, represented by the colored shapes, can reassemble the key to a singlesig wallet. The key can produce the single signature needed to withdraw funds.



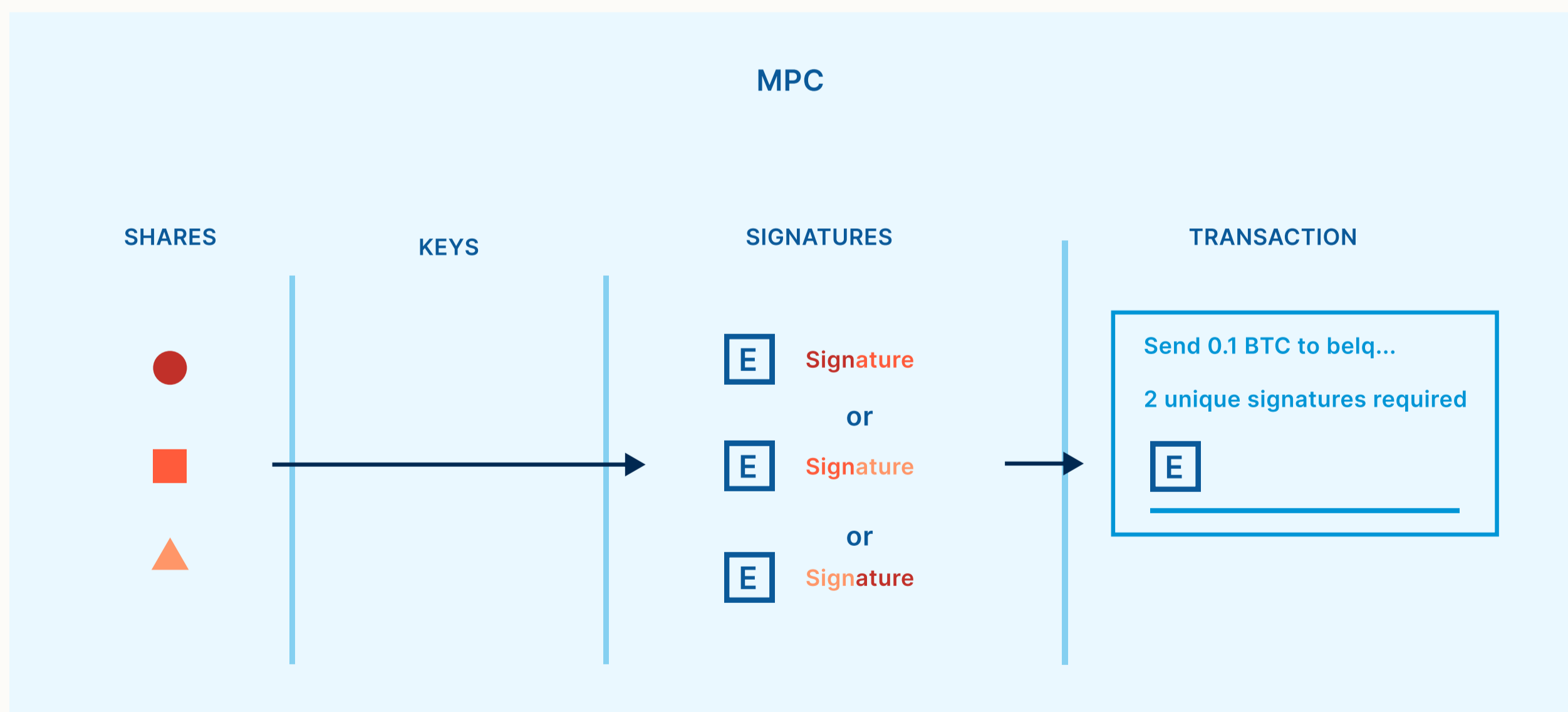
# What is MPC?

MPC, or multi-party computation, is a subfield of cryptography that traces back to the 1970s. The goal of MPC is to allow multiple participants to jointly perform a computation, while each participant's contribution to the computation is not revealed to the rest of the group and therefore can remain private. This allows for multiple parties to collaborate in various contexts without needing to trust each other.

When applied to bitcoin custody, MPC involves distributed "shares," similar to SSS. However, unlike SSS, the shares are not split from a private key nor used to rebuild a private key. Instead, multiple parties compute a single signature directly from a threshold of their shares.

Unlike SSS, MPC does not necessitate a single point of failure. MPC shares can be generated separately from one another, and they never need to be brought together to operate the wallet. Information produced from a share can be communicated to the other participants, without the share itself being revealed.

Since bitcoin and other cryptocurrencies have primarily used a signature system based on ECDSA (Elliptic Curve Digital Signature Algorithm), MPC had to be adapted for this context. The first practical threshold protocols for ECDSA were published in 2018. [\[GG18, LNR18\]](#)



A 2-of-3 MPC arrangement, where any two shares, represented by the colored shapes, can produce a signature directly without assembling a key first.

## II. What are the trade-offs between threshold models?

With three different threshold security models to choose from, the next step is understanding the strengths and weaknesses of each option.

### Tradeoffs with multisig

Script multisig is a standardized way of achieving threshold security, native to the bitcoin protocol. The structure is considered relatively simple and robust. The barrier to entry is also small—if a bitcoin user knows how to operate a singlesig wallet, then it's not a large leap to learn how to set up and use a multisig wallet.

When a multisig wallet is initialized, the addresses produced for receiving bitcoin into the wallet have the threshold requirement built into them. Once a multisig address has been funded, the bitcoin is protected by an immutable contract that has essentially been written into the blockchain itself. The only way to alter the contract (such as changing the access control policy, adjusting which keys are protecting the bitcoin) is to move the bitcoin to a new address that was built with a different contract. For multiple parties who are collaborating to secure bitcoin, this ground-level immutable contract mechanism can provide the highest degree of reassurance that the money is secured according to how all parties have intended. If anything were to be fundamentally

changed, it would become obvious to everyone by the occurrence of a public transaction, and the keys that approved the change would be known. This is why collaborative custody providers such as Unchained rely on script multisig for our products.

However, deploying contracts publicly on the blockchain comes with tradeoffs. As bitcoin is spent out of a multisig address, the access control policy for that address must be permanently published on the blockchain. Observers can then see the details of the multisig quorum that was being used. Although the remaining funds can be easily migrated to a new address going forward, the fact that past security arrangements are exposed isn't ideal. Additionally, needing to move bitcoin from one address to another in order to adjust the access control policy means that transaction fees are always involved with the process (and the larger the quorum, the more expensive it will be).

For entities that value custodial altcoins, such as cryptocurrency exchanges, script multisig can pose more of a challenge than the other two methods of threshold security. This is because a multisig threshold quorum is imposed on the blockchain level, and different cryptocurrencies use different blockchains. Many cryptocurrencies don't even support a native, robust multisig



implementation at all. Meanwhile, SSS and MPC enforce threshold quorums at the key level, and look like singlesig transactions publicly. Since almost all cryptocurrencies support a similar standard for singlesig custody (the same key can be used across most cryptocurrencies), this allows SSS and MPC to be more cross-chain compatible.

## Tradeoffs with Shamir's secret sharing

SSS offers another way of designing a threshold requirement based on relatively simple and battle-tested cryptography. For the purposes of cryptocurrency custody, SSS also has a widely deployed method with a low barrier to entry ([Shamir backup](#)). Once someone has experience using a conventional singlesig wallet, it isn't a huge leap to use a Trezor to set up a wallet with a Shamir backup.

Unlike multisig, SSS operates completely outside of public-facing addresses and transactions on the blockchain. Instead, the threshold requirement is decided by how the private key is split into shares. This means that splitting a key into shares and later reassembling them can be done in private, so that only the people participating in the bitcoin custody arrangement are aware that SSS is being used. In addition to privacy

advantages, keeping the threshold structure outside of the blockchain also means that SSS transactions won't lead to increased fees, and it can be used to secure many different cryptocurrencies. Although most cryptocurrencies have their own unique blockchains, they can all share the same private key as an access point, and that key can in turn be split up using SSS.

The biggest disadvantage to SSS has already been mentioned above—the private key must exist in one place at one time, before it is first split into shares, and also when the shares are recombined for the purposes of approving a withdrawal. These vulnerabilities create temporary single points of failure, meaning that SSS by itself doesn't offer truly institutional-grade security, unlike multisig or MPC.

Additionally, SSS doesn't natively offer a method for adjusting the access control policy. Once a private key is split into a quorum of shares, those shares will always maintain the ability to reproduce that key. If a group is securing a treasury together using SSS and a member of the group leaves, revoking permissions for that individual in a secure manner can pose a challenge. Remaining members of the group could reassemble the key and then split it into new shares, but the old shares would need to be verifiably destroyed. Otherwise, the funds would need to be sent to an entirely new wallet protected by a different key.

implementation at all. Meanwhile, SSS and MPC enforce threshold quorums at the key level, and look like singlesig transactions publicly. Since almost all cryptocurrencies support a similar standard for singlesig custody (the same key can be used across most cryptocurrencies), this allows SSS and MPC to be more cross-chain compatible.

## Tradeoffs with MPC

Much like SSS, MPC enforces the threshold requirement at the key-level instead of the blockchain-level. This unlocks similar advantages, such as granting a higher capacity for privacy, avoiding increased transaction fees, and allowing for one MPC custody structure to be used across many different cryptocurrencies.

Importantly, MPC manages to avoid the temporary single points of failure that come with using SSS. By using a different cryptographic method, the key shares can exist separately from the moment the wallet is first created, and even remain separate while signing withdrawal transactions. Most MPC implementations also include a native method of adjusting the access control policy (creating a new quorum of shares) without having to send funds to a new wallet address.

However, MPC for threshold ECDSA is considered very complex cryptography, and there is not an agreed-upon standard for using it. There are many different protocols, with the first two being developed independently in 2018 by Gennaro and Goldfeder [GG18] and Lindell et al. [LNR18].

Since then, we've also seen protocols from Doerner et al. [DKLs19], Castagnos et al. [CCL+20], Damgård et al. [DJM+20], Canetti et al. [CMP20], Gągol et al. [GKSS20], Gennaro and Goldfeder [GG20], Canetti et al. [CGG+21], Abram et al. [ANO+21], Doerner et al. [DKLs23], and perhaps others. While the newer protocols tend to make certain improvements upon the older ones, they may have had less opportunity for peer-review, audit, and other testing.

The higher level of complexity involved with MPC creates a widened attack surface. With additional components and procedures, there is more room for error and potential security vulnerabilities. Evidence of serious security flaws, including full private key extraction attacks, has already presented itself more than once, affecting some of the threshold ECDSA protocols listed above.

Examples include:

1. [AS20 vulnerabilities](#), September 2020, affecting GG18 implementations
2. [Alpha-Rays vulnerabilities](#), December 2021, affecting GG18 and GG20
3. [TSSHOCK vulnerabilities](#), August 2023, affecting GG18, GG20, and CGG+21
4. [BitForge vulnerabilities](#), August 2023, affecting GG18 and GG20


“Cryptography needs to pass the test of time to attain longevity, and these new protocols clearly didn't pass the test of time[...] this research was not ready for implementation or widespread adoption. From my perspective, implementing and productizing such recent research is quite dangerous.” — Ledger CTO Charles Guillemet, December 2021 [response](#) to Alpha-Rays

“[MPC is] more complicated, more to get wrong. Advanced crypto protocols are fragile in the detail and in the implementation. I'd feel more confident in multisig, which is super simple and rock solid.” — [Post](#) by renowned cryptographer Adam Back, January 2023

MPC is also limited by who can realistically use it in the first place. As previously mentioned, threshold ECDSA is very complicated. For the average individual, there are no tools available to safely or easily set up MPC independently. While some businesses offer collaborative custody MPC wallets that are fairly easy to use, those businesses offer no easy way for users to recover funds if the business disappears (or no way at all, in which case they are a single point of failure). Because script multisig is a simple and open standard, businesses who provide [collaborative custody solutions using multisig](#) can offer [open-source and easy-to-use recovery tools](#). This creates a straightforward avenue for clients to recover their funds even if the collaborative multisig business were no longer available to assist.

# III. Which model is best?

As we just covered, there are numerous tradeoffs between using multisig, SSS, and MPC. They can be arranged in a chart for a visual comparison:



	SCRIPT MULTISIG	SSS	MPC (FOR ECDSA)
SINGLE POINT OF FAILURE AT KEY CREATION	NO	YES	NO
SINGLE POINT OF FAILURE WHILE SIGNING	NO	YES	NO
BATTLE-TESTED SECURITY	YES	YES	NO
SIMPLE TO SETUP AND OPERATE	YES	YES	NO
STANDARDIZED OPEN-SOURCE IMPLEMENTATIONS	YES	YES	NO
CAN ESTABLISH IMMUTABLE CONTRACTS ON-CHAIN	YES	NO	NO
ACCESS CONTROL POLICY MANAGED PRIVATELY OFF-CHAIN	NO	YES	YES
NATIVE WAY TO ADJUST CONTROL POLICY WITHOUT A TRANSACTION	NO	NO	YES
CAN LEAD TO HIGHER TRANSACTION FEES	YES	NO	NO
EASILY USABLE ACROSS MOST CRYPTOCURRENCIES	NO	YES	YES

This chart demonstrates the strengths (blue) and weaknesses (red) for each method of implementing threshold security. Gray could be a strength or weakness depending on one's perspective.

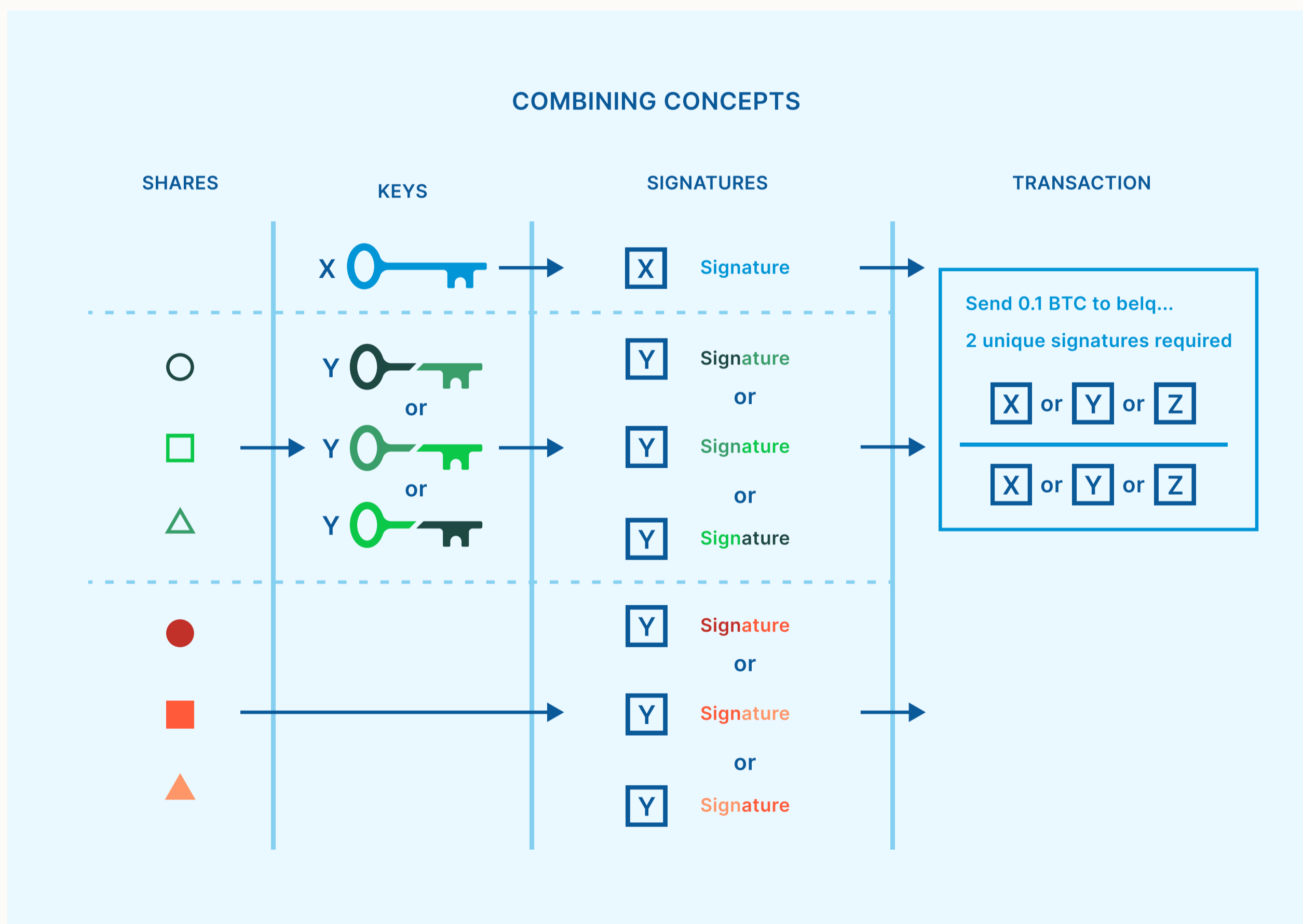
If a business specializes in the custody of many different cryptocurrencies, they might be motivated to hire a team of professionals to carefully set up an MPC custody model. However, if a business or individual were looking for a simple and reliable way to secure bitcoin for the long term, using script multisig and accepting the privacy tradeoffs might be preferable. SSS is rarely used by itself due to its inability to enforce institutional-grade threshold requirements at all times.



# Combining models for collaborative custody

While multisig, SSS, and MPC are often thought of as competing security models, it's possible to incorporate more than one of them into an overall custody structure. As previously described, SSS and MPC allow a threshold of key shares to produce a signature for a transaction.

If the signature was for spending funds out of a singlesig wallet, then nothing else would be required to complete the transaction. However, if instead the signature was for spending funds out of a multisig wallet, additional signatures from other keys could also be needed.



A 2-of-3 multisig structure, where one possible signature could be produced from a normal key, another possible signature could be produced from a key that is reassembled from 2-of-3 SSS shares, and another possible signature could be produced directly from 2-of-3 MPC shares.

While this combination of techniques may sound unnecessary and cumbersome, there are indeed some contexts where it makes practical sense. With the rise in popularity of key agents and multi-institution custody, there is a growing number of specialty businesses that are commissioned by individuals and institutions to secure one of the keys to a multisig wallet. These distributed key agents can help reduce custodial risk. But how should a key agent secure that single key which they are responsible for?

SSS or MPC can be a strategy to minimize or remove single points of failure from this duty. A corporate key agent can design a system where several different officers within the business each hold key shares, and therefore a signature can only be produced upon agreement from a

and therefore a signature can only be produced upon agreement from a threshold of those officers. Additionally, if an attack were to occur during an SSS reassembly, or an MPC implementation ends up suffering from a new key extraction vulnerability like the ones listed earlier, then no customer funds are immediately at risk. The key agent would have time to react and address the issue, while the bitcoin remains protected by the broader multisig wallet.

Using script multisig to create a threshold requirement as a foundational immutable contract, and then commissioning professional key agents to each protect a multisig key using their own SSS or MPC threshold, is far and away the safest method for an institution to keep bitcoin secured for the long-term.

# New capabilities with Taproot

In November of 2021, the Taproot soft-fork occurred, adding new tools into the bitcoin ecosystem. Some of these tools impact the future of institutional-grade bitcoin custody, by allowing for certain improvements and optionalities.

- 1. Schnorr signatures:** The Schnorr signature algorithm is now available in bitcoin as an alternative to ECDSA. Using MPC on top of Schnorr leads to threshold security schemes that are far less complicated, and therefore also provide higher confidence in their security, compared to the ECDSA protocols mentioned earlier. [FROST](#) is the leading Schnorr threshold signature protocol, while [MuSig2](#) is also available specifically for N-of-N quorums. Both of these signature schemes are on the path to becoming standardized tools across the bitcoin industry, and they are expected to make MPC available for regular individuals, with a user experience similar to script multisig.
- 2. Script type privacy:** Pay-to-Taproot (P2TR) addresses are a new [address type](#) that allow script multisig bitcoin addresses to appear identical to the addresses being used for singlesig wallets. This provides a significant privacy improvement, because it means that the bitcoin address itself doesn't provide any clues about its owner's security model, such as whether or not they might be using script multisig.

- 3. Multiple spending paths:** P2TR addresses also have the ability to contain multiple spending paths built into them. This can create new ways of structuring threshold security for institutional-grade custody, as described in [BIP 342](#) (rationale, section 5). For example, a user could create an N-of-N script multisig spending path for every combination of keys that can spend funds. Rather than build a 2-of-3 quorum with keys A, B, and C, a similar outcome can be achieved with three separate 2-of-2 quorums as possible spending paths—one with keys A and B, one with keys A and C, and one with keys B and C. This strategy can increase privacy, because only the spending path that ends up getting used will be revealed. A similar concept can be applied to MPC key share quorums, allowing MuSig2 to be utilized for thresholds.

These Taproot tools are relatively new, and their adoption is still in the early stages. Many bitcoin softwares and services don't yet offer full support for what Taproot has to offer. It's also worth noting that most altcoins don't have these tools natively available.

## IV. Final thoughts

A growing number of institutions are becoming interested in securing a bitcoin treasury, and they require effective solutions. Avoiding single points of failure and minimizing counterparty risk are paramount considerations. The best way to meet these criteria is by leveraging a multisig structure, where keys can be distributed among various enterprise key agents, none of whom will have unilateral control over the bitcoin. Each key agent can use SSS or MPC to add extra threshold protection for their particular key.

Unchained has pioneered an enterprise custody network, built for institutional clients who want to set up an arrangement like this. It's easy to use and customizable, so that each client gets to choose whether they'd like to hold a controlling number of keys themselves, or just a single key, or leave the responsibility of securing keys entirely up to the several, independent enterprise key agents. If you're interested in learning more, [schedule a free consultation with us](#) today!

*Special thanks to Dhruv Bansal for reviewing this article and providing valuable feedback.*