21ST CAPITAL

BITCOIN MULTISIGNATURE

Nov. 2024

Balancing Security and Accessibility

Author: Ziya S.
Date: November 8, 2024
Email: contact@21stcapital.com

www.21stcapital.com

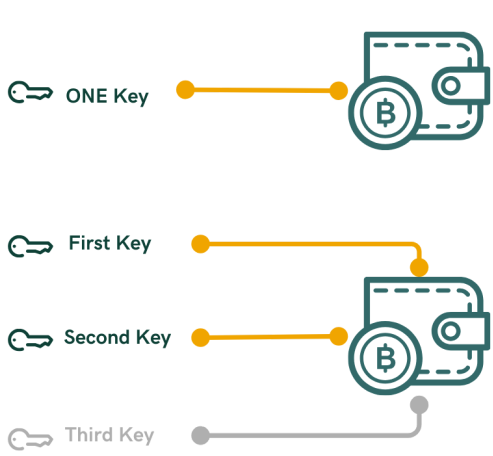
Bitcoin Multisignature: Balancing Security and Accessibility

What Is Bitcoin Multisignature and Which Quorum Is Best Practice for Users? How to Improve on Multisignature and Make It Even Better?

Multisignature is a Bitcoin security technology that's mostly used by high-net-worth individuals or organizations. It simply works in a way that Bitcoin spending would require more than a single step to be spent. Most commonly, it requires two or even more authorizations for a Bitcoin spend to be valid. Before we get into more details about Multisignature, let's first discuss why high-net-worth users are interested in it.

The other common way to use Bitcoin is Single-Signature, or Single-Signature. It's most commonly used by the average user by using their regular wallets that require only one authorization (one key) to spend and send Bitcoin. The security premises here are tied to safeguarding only this single key, which grants authorization. This method is associated with more risks because it's prone to theft, misplacement, or destruction of the key. A permanent loss may occur if this key is compromised or inaccessible.

However, Multisignature mitigates some of these risks to an extent since it overcomes the single point of failure with a Single-Signature wallet for Bitcoin. Multisignature can be tailored more flexibly depending on the needs of its users. It is structured as an M-of-N quorum, where N is the total number of keys involved in the wallet, and M is the number of keys that are needed to produce a valid authorization.



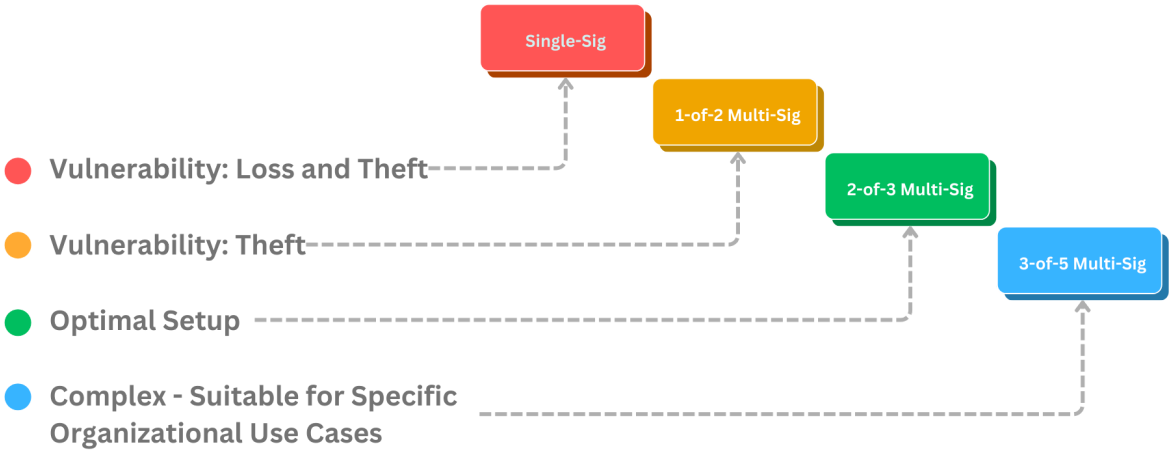
The most common Multisignature scheme is 2-of-3 because it is, first, resilient to key loss since if one key is lost due to mismanagement or disasters, then there are still another two keys that could be used to authorize Bitcoin spending, and the coins will not be lost. Second, it protects against theft because an attacker needs to gain access to more than one key, which makes it very unlikely for an attack on a Multisignature wallet user to go through successfully. This setup is best practiced by a distributed storage scheme where each one of the three keys (or their backups) is kept in separate locations.

Quorum Setups

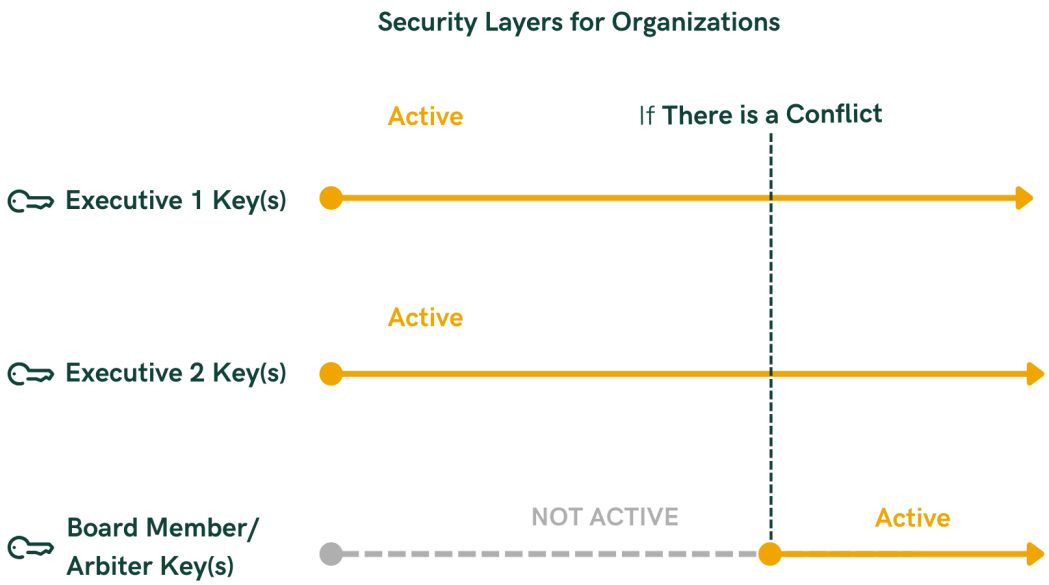
A 1-of-N quorum (1-of-2, 1-of-3) is not resistant to theft and introduces the single point of failure into the equation once again, similar to Single-Signature wallets, because any of the keys here can authorize a Bitcoin spend.

An N-of-N quorum (2-of-2, 3-of-3) introduces a very high risk of loss due to the requirement that all keys must be utilized at all times, and safeguarding multiple keys can be a very challenging process.

An M-of-N quorum (2-of-3, 3-of-5, etc.) is a balanced scheme that mitigates both the risk of theft and the risks associated with loss.



Beyond individual use, M-of-N schemes are also used for organizational use cases. Businesses, governments, or organizations can require approvals from multiple members, or flexible custody structures can distribute the authorization of Bitcoin spending among stakeholders.



Collaborative custody could be practiced by distributing some keys to third parties, where the third party can help secure one or more of your keys on behalf of the owner of the Bitcoin. A third-party company here can enhance security through distributed key management and shared responsibility.

Escrow setups are possible with M-of-N Multisignature schemes where Party A and Party B can each hold one of the keys, and an arbitrator holds the third key to intervene for conflict resolution.

Trade-offs of Multisignature

It is quite complex because, first, it introduces more complexity for key storage because there are simply more keys to maintain. Second, it requires more information for setup and managing. Information like public keys are needed to reconstruct the quorum, which adds one more necessary precaution that users must take into consideration.

Overcoming the Shortcomings of Multisignature

In traditional Multisignature schemes, all keys are active, they all act the same, and there are no policies involved other than how many keys are required to approve a Bitcoin spend. In a layered architecture, a stack of Multisignature schemes can be built on top of each other, enabling policy creation and key hierarchies. These layers are enabled by time delays. In such schemes, more keys can be involved and assigned roles that are kept inactive until they are needed.

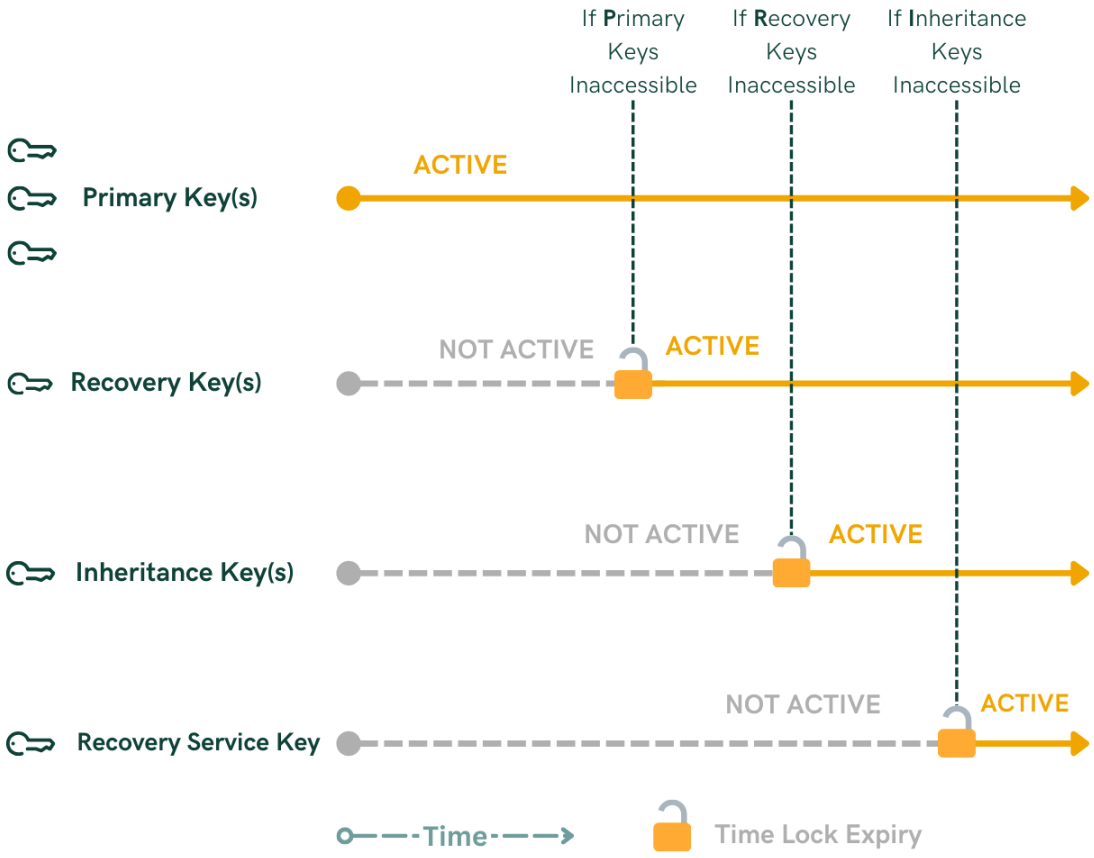
Such a setup could look like this:

Layer 1 (Primary Keys): Acts like a traditional 2-of-3 Multisignature setup.

Layer 2 (Recovery Keys): Only activates when Layer 1 keys are lost, where the 2-of-3 setup becomes 2-of-4, and one extra key activates after a period of time passes.

Layer 3 (Inheritance Keys): External keys that activate when the vault owner is not accessible anymore. These could be completely separate keys (either Single-Signature or a quorum of Multisignature) controlled by some members of a family. These separate keys are included in the wallet setup but kept inactive unless the conditions are met.

Layer 4 (External Recovery Keys): This layer is a failsafe recovery by a third party that only activates after a predetermined amount of time when all other keys are lost. Keys from a third party could be incorporated into the wallet setup but kept inactive unless conditions are met (typically a long time of coin inactivity on the Bitcoin network).



With layered security, users can define multiple recovery methods. If something happens to their primary keys, they can rely on secondary methods, such as backup keys or the help of trusted collaborators. The same user can control keys in all layers or allow other users to own some of the keys in the recovery layers.

> **21st Capital's Smart Vault** is a layered Multisignature wallet with automated recovery structures. It can be set up in a way where users and organizations can incorporate extra keys down in the hierarchy, which are inactive unless needed for recovery, inheritance, or arbitration.
> **Check it out at 21stcapital.com/Demo**

Conclusion

Multisignature substantially enhances the security and resilience of Bitcoin self-custody. It balances the risks of theft and loss more effectively than Single-Signature wallets. However, they are complex, difficult to maintain, and still prone to loss if a specific number of keys are mismanaged. A layered Multisignature mitigates this risk by adding more keys with different roles and keeping them inactive unless they are needed for automated recovery, inheritance, and other use cases.