# **What Is A Multi-Signature Wallet, What Are Its Uses?**

When Bitcoin was released upon humanity, it was a marvelous new technology that keeps getting adopted by people all over the globe, where a person can send wealth from themselves to another, without any restriction or major hurdles, so long as they have an internet connection and a Bitcoin wallet.

Over time though, people wanted more secure ways to safeguard their Bitcoin wealth from being stolen or lost, as such, the creation of what's called a multi-signature wallet was created, which also produced a couple of new use-cases and services for the cryptocurrency industry.

## **What is a multisig wallet?**

With a normal Bitcoin wallet, you would have a public address and its corresponding private key that's used to sign outgoing transactions. Basically, if a user with a public Bitcoin address wants to send a few sats to someone, it would need the signature of its private key for the Bitcoin network to accept and confirm the transaction.

With that said, a multi-signature wallet is as the name implies, a wallet that would require multiple signatures from different Bitcoin wallets for outgoing transactions to execute properly.

For example, if you create a 2-of-3 multisig wallet, you would need any of those two wallets out of the three to sign a transaction that's going to send funds to some other Bitcoin user. A single signature would not meet the requirements to execute that transaction.

## **What are multisig wallets used for?**

As mentioned previously, a decent number of Bitcoin users want to practice more safety and security measures, with as little to no single point of failure, where they'd use what's known as cold storage to store most of their funds in and protect their private keys from an online environment, like a hardware wallet, and now with the introduction of the multi-signature process, they would combine their cold storage solution with it to add even more security and safety to their funds.

Let's take a simple example to argue for the use of a multi-signature wallet for safety purposes of preventing the loss of your Bitcoin.

Assume you have a 1-of-2 multi-signature wallet, and one of the wallets is stored somewhere secure why the other is with you most of the time. With this kind of multisig wallet, you would only the one wallet with you to sign transactions. Somehow, you lost the wallet that's always with you, and you don't know where you stored that specific wallet's seed phrase to get it back. In most cases, if you had a normal wallet, you would have lost your Bitcoin funds forever, but since you have a 1-of-2 multi-signature wallet, you would only need to go back and retrieve the other wallet that you've kept secure somewhere, and after you've got it, you realize you still have access to your Bitcoin funds and can transfer them out to a new 1-of-2 multisig wallet, or a 2-of-3 multisig wallet if you'd more security measures to sign transactions going out, where the need for more than one signature is required.

## **What are the best multi-signature wallets out there?**

There are a handful of mobile and/or desktop crypto wallets out there that allow users to create a multi-signature wallet, some with different limitations and better user experience than others.

* [**BlueWallet**](https://bluewallet.io/), an open-source non-custodial Bitcoin-only wallet for mobile and desktop devices, is the best so far from our experience in terms of UX. It supports up to 7 of 7 wallets with the right to authorize outgoing transactions.
* [**Electrum**](https://electrum.org/), an old but gold and reliable non-custodial open-source mobile and desktop Bitcoin wallet application with a lot of advanced features. It supports up to 15 of 15 wallets.
* [**Armory**](https://www.bitcoinarmory.com/), an open-source full node Bitcoin wallet for PC that supports up to 7 of 7 for its multi-signature wallet.

We did mention that there were services that came about because of the creation of this new process, and one of them would be decentralized exchanges like our very own [Whales Heaven](https://www.whalesheaven.com/), where the multi-signature process is used to conduct exchanges between people with other coins, like exchanging BTC with ETH, or other crypto pairs, in a trustless manner. This way, users wouldn't have to give up on their coins while you wait for an exchange to occur.