What Is A Bitcoin Multi-Signature Setup, And Should You Have One?

Your Bitcoin wallet is like a simple safe, where there's money inside said safe, and the one who can open it and be able to take the money out of it to spend it is the one with the key that's used to unlock it. If we look at your Bitcoin wallet, you can consider your public address as the safe, and its corresponding private address is the key to have access to what's inside the safe.

But what do banks do when they want to increase security for their big safe that has a lot of money in it? They increase the number of keys needed to open that safe, like requiring two keys, out of three, to open it. That's what some people would like to have for a Bitcoin wallet.

What's a Bitcoin multisig wallet?

It's the process of connecting multiple addresses with a main address to require some or all of those addresses to sign on a transaction sent by the main address to successfully send out its money.

For example, we have created a new multisig Bitcoin wallet connected to two other wallets, with a rule that there need to be at least two out of the three addresses involved to sign an outgoing transaction, for it to be successful. That's what's called a two-of-three multisig wallet.

What are its use cases?

For one, if someone steals your multisig Bitcoin wallet, where you've set it up to have 2-of-3 signatures, the thief can't spend your money without at least another one of those addresses signing off on it.

Because of this technology, we can now take benefit of decentralized exchanges (DEX) like Whales Heaven, where we don't have to give up control of our funds to a centralized exchange and trust them as a third party, risking our funds and privacy because of the KYC process, to be able to trade with others.

Should you have a multi-signature setup?

It depends. While the difficulty has decreased and the user experience has improved quite a bit over the years, it might prove as harmful as it is beneficial to those who don't know what they're doing.

For example, you've set up a 2-of-2 multisig Bitcoin wallet, and you've lost one of the two keys that are needed to sign an outgoing transaction, which results in never having the ability to spend the coins within that wallet, even if you have access to the main address.

As mentioned above, security is increased and it can act as a backup plan, but a side effect is that you may lose access to your funds if you lose the ability to fulfill the requirements you've set up, like in the example above.

How to create a multisig Bitcoin wallet?

A handful of wallets have support to set up a multisig Bitcoin wallet. One such wallet is Bluewallet, where you tap on "Add a wallet" and then selecting the "Vault" option. This will start the process of creating a 2-of-3 multisig Bitcoin wallet, where for all of the three addresses that are needed, you can

either create them all within the app, which is highly not advisable, or you can create the first one there then import the other two from other wallets using their xPUB addresses, where you'd then transfer the coordination setup of your multisig Bitcoin wallet to those other wallets.

That's pretty much it, but make sure to research this more and look at multiple tutorials to gain more solid knowledge about it, and use small amounts of money experimenting, to avoid any sizable amount of funds if something were to go wrong.