

HOW DOES IT APPLY TO LN CHANNELS OPENING?

Open a channel with private coin

Opening a Lightning channel with a coin made private by this technique leaks less information. Constructing a coinjoin is a difficult task, but it's similar to opening a lightning channel. As a result, it's possible to combine both operations to open channels directly inside a coinjoin round, leveraging unfair privacy.

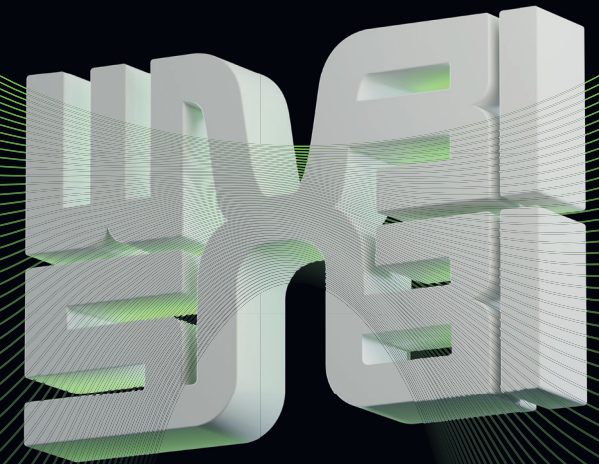
WASABI WALLET SOCIALS



@WASABIWALLET

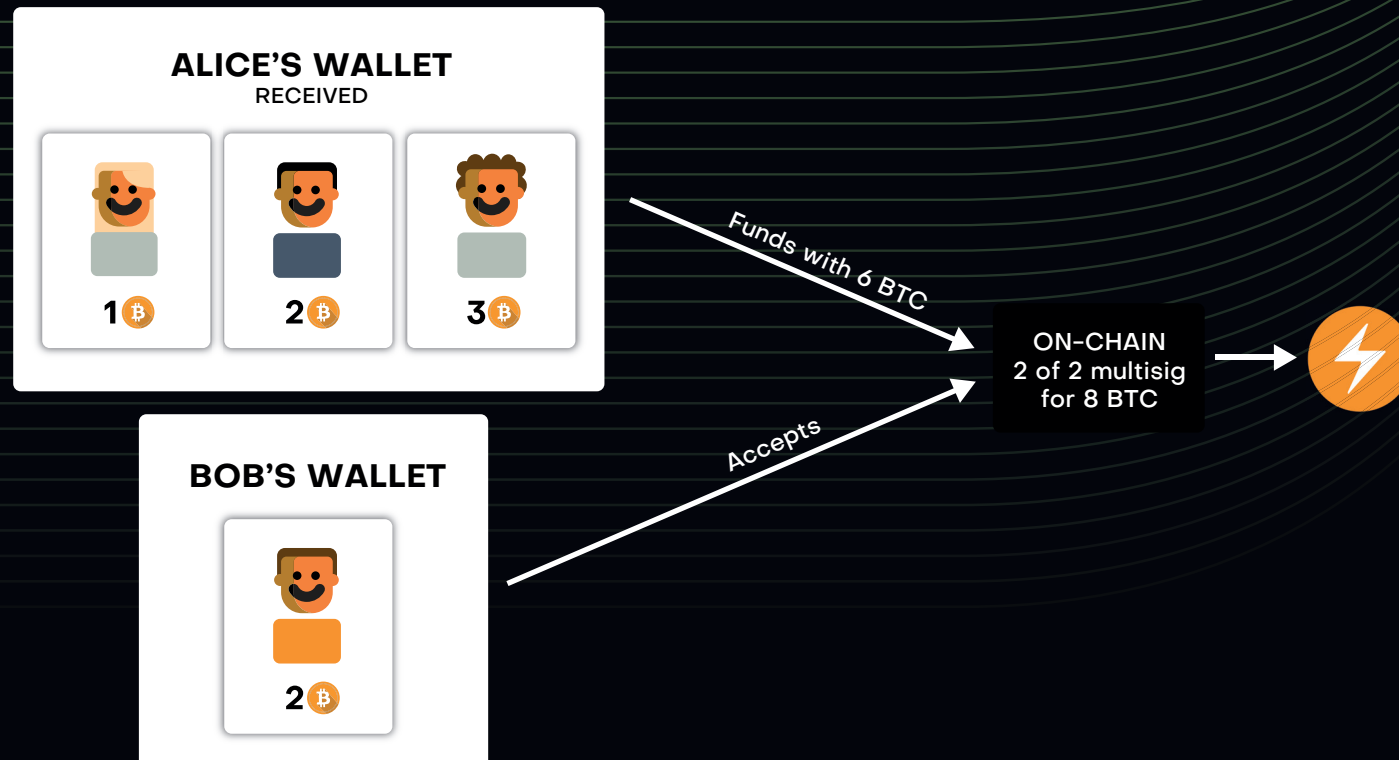


ZKSNACKS/WALLETWASABI



OPENING LIGHTNING CHANNELS PRIVATELY

USING WABISABI COINJOINS FOR HIDING
LIGHTNING'S ONCHAIN DATA



WASABIWALLET.IO

BITCOIN IS NOT PRIVATE AT THE PROTOCOL LEVEL

Bitcoin is not private at the protocol level. Every on-chain transaction reveals information about the sender and receiver to various entities, and in some cases, even to any observer of the blockchain. Similarly, Lightning channels can suffer from the same vulnerabilities since they are settled on-chain. To address these issues, a common technique is to create a multi-party transaction called a coinjoin.

Coinjoin participants register their coins, send them randomly to others and then receive the same value in return; all in

a trustless way. This technique makes it difficult for anyone to track how someone is using their bitcoin. Once someone sends their coins through a coinjoin, it becomes extremely challenging to determine which coins they will receive as outputs. Thus, they can now use their private coins without worrying that they're being spied on. WabiSabi takes the bar even further. This evolution of the standard conjoining protocol (ZeroLink) makes clever use of complex cryptographic concepts such as Keyed-Verifiable Anonymous

Credentials and Peterson Commitments to allow participants to register inputs and outputs of any denomination. WabiSabi enables participants to easily open a multiparty-funded channel with any amount, making it impossible to know which inputs were initially used to fund the round by using a Taproot key instead of a classic P2SH, it would be nearly impossible to know that a lightning channel has been opened in the round.

