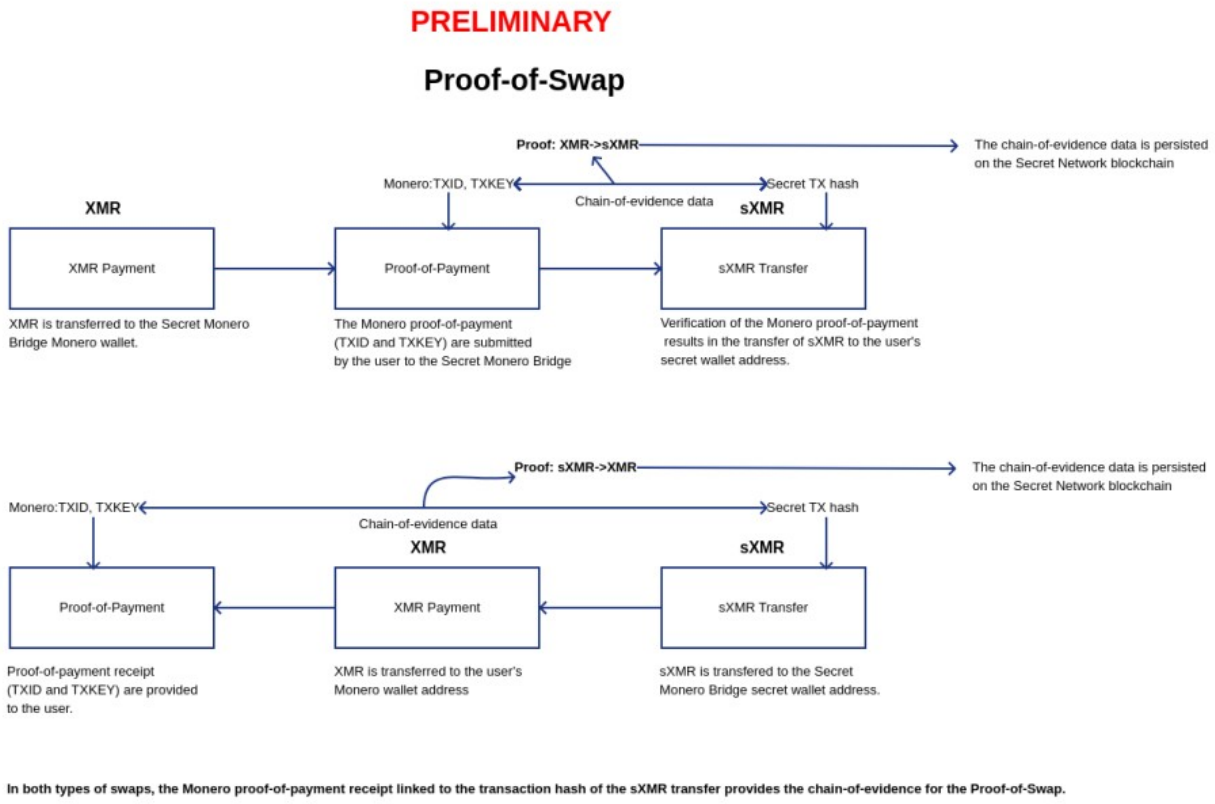
15 March 2021



The Secret Monero Bridge will provide for **Proof-of-Swap.** Proof-of-Swap is a data set of evidence proving that XMR ↔ sXMR swaps were performed.

The preliminary diagram above illustrates the construction of the Proof-of-Swap data set.

The diagram denotes that the Proof-of-Swap chain-of-evidence is persisted on the Secret Network blockchain. This has **not** yet been decided.

This Proof-of-Swap data set should be classified as private data. We wouldn't want entities to be able to access this data as it would violate financial privacy. The Monero proof-of-payment reveals the amount of Monero transferred in a transaction, so revealing this and making it public would circumvent Monero's RingCT as well as the Secret Network's privacy for transaction amounts.

If the Proof-of-Swap data set is decided to be persistent on the Secret Network blockchain, it should be done so with that data encrypted.

The project team will need to decide the details of Proof-of-Swap persistence at a later date.