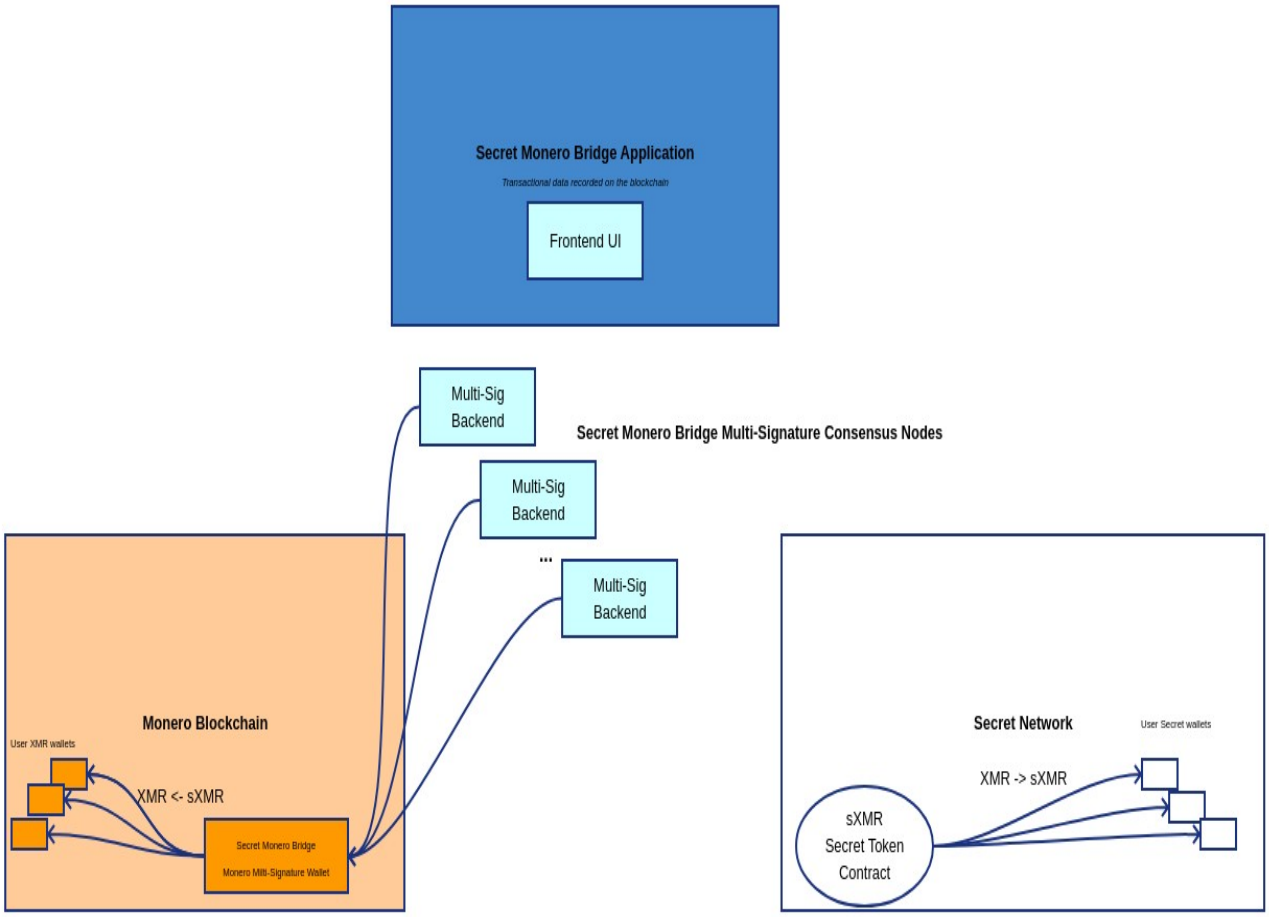
# Secret Monero Bridge – Conceptual High-Level Description

14 March 2021
maxkoda@i2pmail.org




## Conceptual High-Level Description

The **Secret Monero Bridge** would be a system that enables the transfer of value between the Monero blockchain and the Secret Network. Value is represented as **XMR** on the Monero blockchain and as **sXMR** on the Secret Network. The exchange between XMR and sXMR will be pegged 1:1.

The sXMR token will be a SNIP-20 secret token on the Secret Network.

The Secret Monero Bridge will manage a multi-signature Monero wallet where XMR will be locked when swapped for sXMR, with the sXMR tokens then placed into circulation on the Secret Network.

When sXMR is swapped for XMR, the sXMR tokens will be taken out of circulation and the corresponding XMR being transferred from the Secret Monero Bridge's Monero wallet to the provided Monero address.

A decentralized collection of nodes (Multi-Sig Backend boxes in the above diagram) will provide the consensus mechanism to transfer XMR from the Secret Monero Bridge to user wallets within the Monero ecosystem. A **Multi-Signature Consensus Mechanism** is important for the security of the Secret Monero Bridge's Monero wallet management and the transfer of value on the Monero blockchain.

Providing a multi-signature mechanism with a collection of decentralized nodes which are properly incentivized to abide by the rules is critical. *The **Multi-Signature Consensus Mechanism** will be a critical security feature that will need to be developed.* A component feature of the **Multi-Signature Consensus Mechanism** will involve publishing the balance of the Secret Monero Bridge's Monero wallet, to guarantee the balance of XMR in the Secret Monero Bridge's XMR wallet matches the balance of sXMR in circulation on the Secret Network (the Monero protocol provides a mechanism to accomplish this).

Users of the Secret Monero Bridge will be able to perform the following swaps:

**XMR → sXMR**
A user transfers XMR to the Secret Monero Bridge's Monero wallet. The user then interacts with the Secret Monero Bridge web application to submit the proof-of-payment and the secret wallet address for the destination of the sXMR tokens. The Secret Monero Bridge verifies the proof-of-payment and then transfers the corresponding amount of sXMR tokens to the provided secret wallet address. The XMR tokens are locked in the Secret Monero Bridge's Monero wallet.

**sXMR → XMR**
A user interacts with the Secret Monero Bridge application to swap sXMR to XMR. The user designates the amount of sXMR to swap and provides the Monero wallet address to receive the corresponding amount of XMR. Once the sXMR is transferred to the Secret Monero Bridge application's secret wallet address (taken out of circulation), the Secret Monero Bridge application initiates a transaction to send the XMR to the provided user Monero wallet address. The Multi-Sig Backend nodes process the multi-signature transfer transaction that will deliver the XMR to the user's Monero wallet. A proof-of-payment receipt will be recorded and provided to the user.

Secret Monero Bridge transactional log data will be recorded on the Secret Network blockchain with sensitive data being held private and necessary public data readable by the community.

**Monero Proof-of-Payment**
The Monero protocol provides for mathematical proof that a payment was made. The Secret Monero Bridge will rely of this mathematical proof feature and provide value transfer receipts.

*Recording transaction ids of proof-of-payments within the system will be required to ensure that payments are only made once for a given source transaction. This will be an important audit check in the system.*

## Fees

Nominal transaction fees will be collected for value transfers over the Secret Monero Bridge. These fees will be as follows:

XMR → sXMR swap fees will be collected in XMR.
SXMR → XMR swap fees will be collected in sXMR (*or maybe SCRT or sSCRT needs additional consideration in regards to simplifying the reporting of in-circulation balances*)

Swap fees will be used to reward the operators of the Secret Monero Bridge application and the multi-signature back-end nodes to compensate for operations.

## Conclusion

This paper is meant to be a brief high-level conceptual overview of intent for the proposed Secret Monero Bridge. It is meant to facilitate conversation, collaboration, and generate interest. Hopefully enough interest will be generated to kick-off an open source project to deliver a working proof of concept.

**A primary motivation is to inspire the Monero community to join the Secret Network and to benefit in Secret DeFi.**

Please feel free to ask questions or provide feedback to me at the places listed below. If enough interest is collected to start a project, we will provide a better medium for collaboration.

I can be reached at:

maxkoda@i2pmail.org

Discord user: **maxkoda**
Secret Network Forum user: **maxkoda**