PRELIMINARY
Secret Monero Bridge – Proof-of-Concept
User Experience Improvement Proposal

20 March 2021

Background

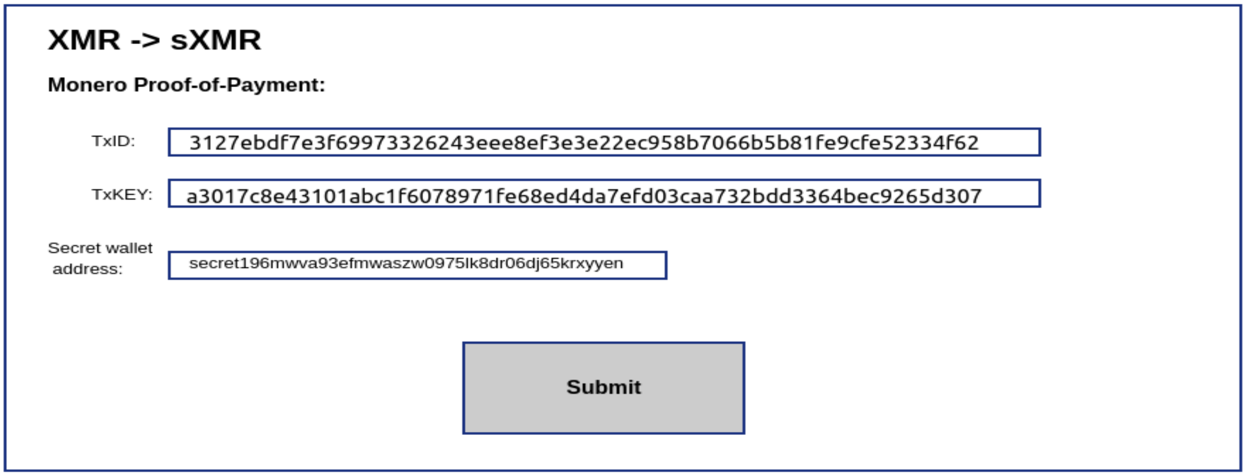
In the XMR→sXMR conversion, a user sends XMR to the Secret Monero Bridge (SMB). The user does this through his/her wallet interface, sending XMR to the SMB Monero wallet address.

Next the user collects the Transaction ID (TXID) of the payment transaction and the Transaction KEY (TXKEY). This completes the data set for the Monero Proof-of-Payment:

- Monero address to which the payment was sent
- TXID of the payment transaction
- TXKEY for the payment transactions

With these 3 data parameters the *check_tx_key* Monero wallet command can be issued to verify a Monero payment.

Once these 3 data parameters are available the user interacts with the SMB web application to perform the XMR→sXMR conversion:



XMR -> sXMR

Monero Proof-of-Payment:

TxID: 3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62

TxKEY: a3017c8e43101abc1f6078971fe68ed4da7efd03caa732bdd3364bec9265d307

Secret wallet address: secret196mwva93efmwaszw0975lk8dr06dj65krxyyen

In the PoC, the user is required to enter the TXID and TXKEY for the Monero Proof-of-Payment as well as the Secret Network wallet address to receive the sXMR.

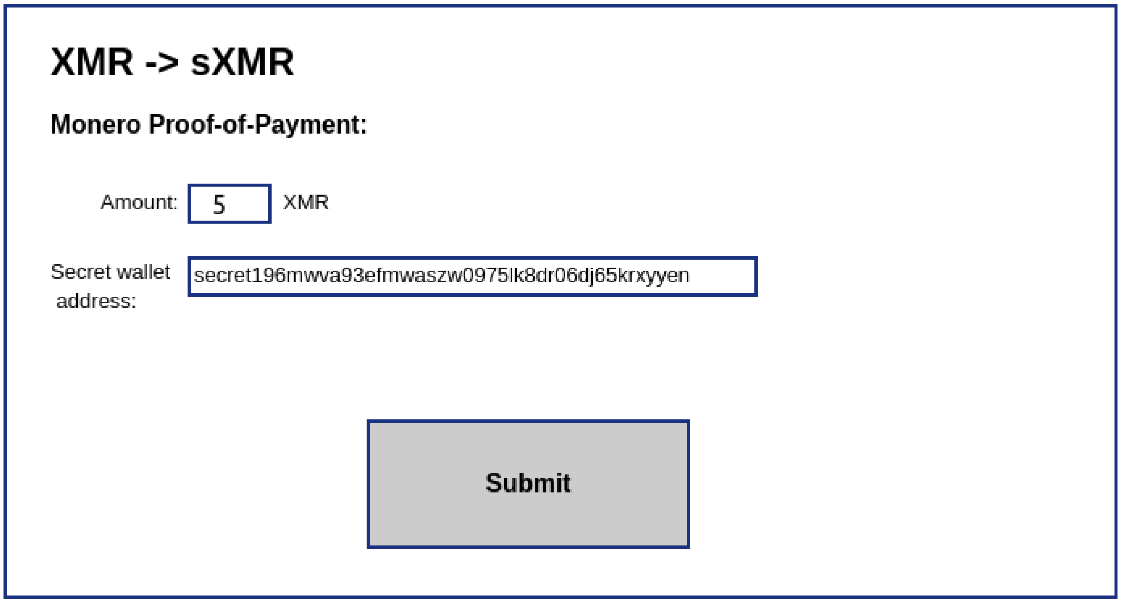
When the user clicks the Submit button, the Monero Proof-of-Payment is verified, the sXMR tokens are minted and then sent to the provided Secret Network wallet address.

Improvement Proposal

To simplify this process and improve the overall user experience, we propose the following:

Provide a Monero wallet interface directly in the SMB UI which will allow the user to make a Monero payment directly from the SMB web application. The SMB web application would then automatically collect the information for the Monero Proof-of-Payment, verify the Monero Proof-of-Payment (in the background). All without requiring manual user interaction.

This would simplify the UI providing a screen similar to:



XMR -> sXMR

Monero Proof-of-Payment:

Amount: 5 XMR

Secret wallet address: secret196mwva93efmwaszw0975lk8dr06dj65krxyyen

 The current XMR→sXMR UX option allowing a user to send XMR to the SMB directly from his/her wallet and later submitting the Monero Proof-of-Payment to mint sXMR tokens will remain an option for users who prefer this approach.

While this approach is less optimal for the user, requiring a higher skill set and more work to accomplish the task. Some users may prefer to use the Monero wallet of their choice rather than the SMB Monero wallet interface.

The improvement proposal objective is to simplify the XMR→sXMR process. It is expected that the majority of users will prefer the improvement proposal approach.