PRELIMINARY

Secret Monero Bridge Proof-of-Concept XMR→sXMR Swap

21 March 2021

Preliminary Information:

Secret Monero Bridge Monero wallet address:

Step 1

User sends 1.0 XMR to the Secret Monero Bridge Monero wallet.

```
Starting refresh...
Untagged accounts:
                                            Unlocked balance
        Account
                       4.0000000000000
        0 A1u0oz
                                             2.0000000000000
                                                                  Primary account
         Total
                  4.0000000000000
                                            2.0000000000000
Currently selected account: [0] Primary account
Tag: (No tag assigned)
Balance: 4.0000000000000, unlocked balance: 2.00000000000 (8 block(s) to unlock)
[wallet A1uQoz]: transfer 9yjvUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEgQHVNfVdcdmtbt5gFqCnBAt81QakWg83G
CkibK 1.0
Transaction 1/1:
Spending from address index 0
Sending 1.000000000000. The transaction fee is 0.000033700000
Is this okay? (Y/Yes/N/No): Y
[wallet A1uQoz]:
```

To complete the collection of the Monero proof-of-payment for the transaction, the user obtains the TXKEY for the payment transaction:

```
[wallet A1uQoz]: get_tx_key 3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62
Tx key: a3017c8e43101abc1f6078971fe68ed4da7efd03caa732bdd3364bec9265d307
[wallet A1uQoz]:
```

Now the three pieces of information representing the Monero proof-of-payment have been obtained:

TXID: 3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62 **TXKEY:** a3017c8e43101abc1f6078971fe68ed4da7efd03caa732bdd3364bec9265d307 **Payment Address:**

9yjvUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEqQHVNfVdcdmtbt5qFqCnBAt81QakWq83GCkibK

Now the user can check the Monero proof-of-payment by submitting the **check_tx_key** command in his/her Monero wallet:

```
[wallet A1uQoz (out of sync)]: check_tx_key 3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62 a3017c8
e43101abc1f6078971fe68ed4da7efd03caa732bdd3364bec9265d307 9yjvUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEg
QHVNfVdcdmtbt5gFqCnBAt81QakWg83GCkibK
9yjvUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEgQHVNfVdcdmtbt5gFqCnBAt81QakWg83GCkibK received 1.000000000
000 in txid <3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62>
This transaction has 2 confirmations
[wallet A1uQoz (out of sync)]:
```

We can see that Monero wallet address:
9yjvUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEgQHVNfVdcdmtbt5g
FqCnBAt81QakWg83GCkibK

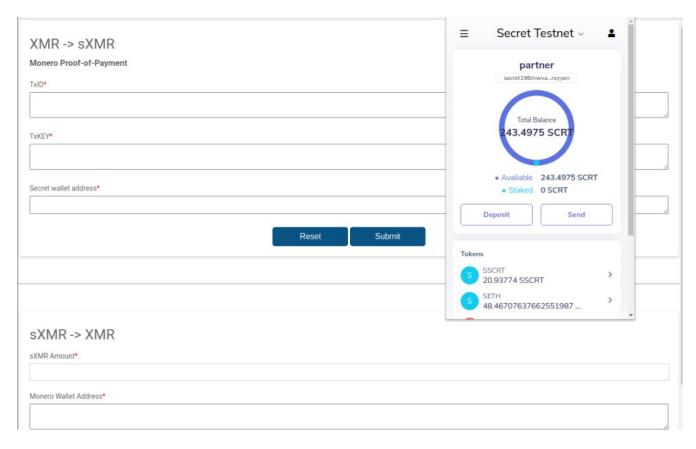
received 1.00000000000 XMR in txid: 3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62

and that the transaction has had 2 confirmations.

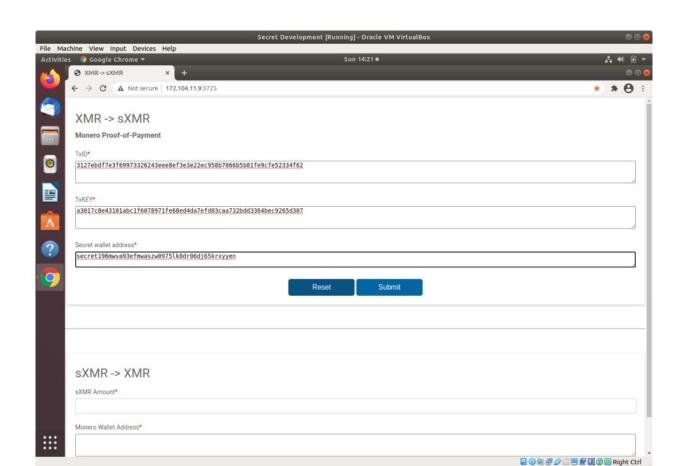
The Secret Monero Bridge web application will then make a call to the locally running monero-wallet-rpc to verify the Monero proof-of-payment (similar to the curl call shown below):

```
waldo1@localhost:~$ curl http://127.0.0.1:18083/json_rpc -d '{"jsonrpc":"2.0","id":"0","method":"check_tx_key","para
ms":{"txid":"3127ebdf7e3f69973326243eee8ef3e3e22ec958b7066b5b81fe9cfe52334f62","tx_key":"a3017c8e43101abc1f6078971fe
68ed4da7efd03caa732bdd3364bec9265d307","address":"9yjvUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEgQHVNfVdc
dmtbt5gFqCnBAt81QakWg83GCkibK"}}' -H 'Content-Type: application/json'
{
    "id": "0",
    "jsonrpc": "2.0",
    "result": {
        "confirmations": 3,
        "in_pool": false,
        "received": 10000000000000
}
}
}waldo1@localhost:~$
```

Proof-of-Concept Web application screen is shown below:



User enters in the Monero proof-of-payment:



Check the Monero proof-of-payment:

Confirmations 2549 in_pool: false

received: 10000000000000

We are now deploying the secret contracts to the holodeck-2 testnet. Next we will have the web application call the secret contract to mint sXMR tokens and send them to the user provided Secret wallet address.

Notes:

The Secret Monero Bridge web application will persist Monero proof-of-payment txids to ensure that no unique txid is processed more than once.

In this Proof-of-Concept we will wait for just 1 confirmation before proceeding.

Next update will connect the web application to the secret contract!