

# Proof-of-Concept

March 16-26 2021



**Secret Monero Bridge**

A value transfer bridge between the Monero blockchain and the Secret Network.



# Team Members

- segfaultdoctor – secret contracts
- bobcalifornia – web application (UI)
- maxkoda – Monero components and project management



# Motivation

- Connect the Monero community to the Secret Network and Secret DeFi
- Enable value transfer between the Monero blockchain and the Secret Network
- Provide a working reference model for the larger open source Secret Monero Bridge project



# Objectives

- Create a new SNIP-20 secret token for Monero (XMR) on the Secret Network. The new secret token is named sXMR.
- Create a Secret Monero Bridge secret contract responsible for minting new sXMR tokens into circulation as well as for burning sXMR tokens taken out of circulation (converted back into XMR).
- Enable the conversion of XMR to sXMR secret tokens on Secret Network:  $\text{XMR} \rightarrow \text{sXMR}$ .
- Enable the transfer of sXMR secret tokens to XMR on the Monero blockchain:  $\text{sXMR} \rightarrow \text{XMR}$ .



# Secret Contracts

- We deployed 2 secret contracts on the holodeck-2 testnet:
- the sXMR SNIP-20 secret token contract
- The Secret Monero Bridge secret contract



# Secret Contracts

`secret1dxrkvn0pg8js89swp37m8uh72dulu945ye330s`

<b>Code ID:</b>	27890
<b>Creator:</b>	secret1fzatz545pzuvuc3jx8c7kznyu6e64r64xvgzrv
<b>Data Hash:</b>	8BCD5F937B458C3D8D3995751B8EE675262587A41D07E12BFE2197E519CC66D1
<b>Builder:</b>	
<b>Label:</b>	sxmr-v2
<b>Source Code:</b>	N/A
<b>Description:</b>	

`secret1yx6g7j82zp487h95t8wuutzy5uvfhfayl5dqld`

<b>Code ID:</b>	27919
<b>Creator:</b>	secret1fzatz545pzuvuc3jx8c7kznyu6e64r64xvgzrv
<b>Data Hash:</b>	545933EA2A58990CD4633CD02E9DEC7600BDDC387D02742B74B01242151ED699
<b>Builder:</b>	
<b>Label:</b>	sxmr-bridge-3
<b>Source Code:</b>	N/A
<b>Description:</b>	



# Web Application

- We developed a simple web application for this proof-of-concept.
- The web application makes calls to a monero-wallet-rpc service to interact with the Monero blockchain.
- The web application utilizes SecretJS to interact with the Keplr wallet and Secret Network.

# Web Application

## XMR -> sXMR

Monero Proof-of-Payment

TxID\*

TxKEY\*

Secret wallet address\*

## sXMR -> XMR

sXMR Amount\*

Monero Wallet Address\*





# XMR→sXMR conversion

- User sends XMR to the Secret Monero Bridge wallet address [9yjuUbbdcFSXRKAoaCGfQQR9UkbkwVBhqYXihc1EcoPdin8YibndTrCbEgQHVNfVdcdmtbt5gFqCnBA81QakWg83GCkibK](#)
- User submits Monero Proof-of-Payment via the web application
- Web application verifies Monero Proof-of-Payment and then mints sXMR secret tokens and sends them to the user's secret wallet address.
- XMR received by the Secret Monero Bridge remain locked.



# sXMR→XMR Conversion

- User converts sXMR → XMR via use of the web application.
- User indicates the amount of sXMR to convert and provides a Monero wallet address which will receive the XMR.



# What's Next

The Secret Monero Bridge open source project will deliver these future improvements:

- Multi-signature consensus facility to harden Monero wallet security
- Integrated Monero wallet functionality directly in the user interface
- Design the web application as an unstoppable decentralized application (Dapp)
- And more...



# Wrap-up

In this hackathon we learned:

- How to build and deploy secret contracts
- How to use SecretJS in web applications

Additional information and artifacts (demo video) for this proof-of-concept can be found on our github site at:

- <https://github.com/maxkoda-cpu/Secret-Monero-Bridge/tree/main/Proof-of-Concept>