PRELIMINARY

FAQs

Is the Secret Monero Bridge Wallet a Centralized Wallet?

Yes, as there is only one Secret Monero Bridge wallet. It's address is:

46KTmvCDx862ijymLsCDVaCZ5UNc2A6yNhYEBt4t6AkrLf5CpF7XuB8HjUffdAfcZRTnZD1f3JyeTixqSsdMW7Sd9x1odvN

Since there is a single Monero wallet, there are centralization risks associated with it. To mitigate these centralization risks, we created a multi-signature Monero wallet and we implemented a decentralized network of nodes that we call Multi-Signature Consensus Nodes (MSCNs) that implement our Secret Monero Bridge back-end code. There is an MSCN for each signer in our multi-signature scheme. The MSCNs collaborate in multi-signature operations. We use Monero multi-signature technology to securely manage our Monero wallet as well as Secret Network multi-signature technology to mint and burn sXMR tokens on the Secret Network.

We have developed a governance model for the Secret Monero Bridge to scale our level of decentralization. Our MSCNs are decentralized, peer-to-peer nodes that run identical software and maintain their own copy of deposit/withdrawal transactions. Each MSCN can act as a server or a client. When acting as a server, a MSCN accepts transactions from our decentralized application interface (API), replicates the transaction to the other MSCNs, and that MSCN (acting as a server) is responsible for processing the transaction through its life cycle. The Other MSCNs participate in verifying transaction data and providing digital signatures for multi-signature transactions.

When the number of MSCNs is increased, the complexity of the transaction processing increases and the performance of the overall system decreases in proportion. So the number of MSCNs deployed is one dimension in our overall level of decentralization. Our design team decided that the Secret Monero Bridge decentralization model need additional dimensions to strike an acceptable level of decentralization and created a governance model that includes a governance token. Holders of the governance token help to scale the decentralized nature of the Secret Monero Bridge and provide appropriate governance checks-and-balances. Governance token holders participate in governance decisions and effectively control and manage the Secret Monero Bridge wallet. For example, each of our monero-wallet-rpc nodes operates separately (on a different computer) from the MSCN that interfaces with the monero-wallet-rpc. The MSCN communicates with the monero-wallet-rpc node through an I2P destination utilizing an encrypted lease set. The governance facility has control of the monero-wallet-rpc I2P destination and can turn it on or off. Effectively then governance can connect or disconnect each MSCN from its monero-wallet-rpc node. MSCNs do not have access to the keys or passwords of the Monero wallet. Those are controlled via the governance facility. Each MSCN does hold its key pair for the Secret Network multi-signature operations. However the governance facility can control minting of sXMR tokens. The long-term goal of the Secret Monero Bridge is to evolve an anonymous

Decentralized Autonomous Community (DAC) to govern operations. This DAC will efficiently and effectively scale the level of decentralization for the Secret Monero Bridge.

The governance model is not yet fully implemented and the governance token has not yet been developed. A governance team has been organized to effect various layers of governance until the implementation of DAC governance. Additional information on the governance model will be made available once it is published.

Why Does the Secret Monero Bridge Use the I2P Network?

We use the I2P network to provide anonymity and financial privacy for the on/off ramp between the Monero blockchain and the Secret Network. The I2P network is a private, end-to-end encrypted, peer-to-peer, anonymous network.

The design team decided to strive to make the Secret Monero Bridge an unstoppable and uncensorable service. This means that the Secret Monero Bridge should not present itself as a centralized target that can be easily seized and shutdown by hostile external entities. One primary consideration that led to the Secret Monero Bridge I2P Hidden Services design was the current regulatory environment. The design team is of the opinion that regulators could classify the Secret Monero Bridge multi-signature wallet as a "custodial wallet" and proclaim that the wallet be subject to their regulation. This ultimately could result in the Secret Monero Bridge being a target for seizure and shutdown.

Secret Monero Bridge code is decentralized and resides and executes inside the I2P network which hides the physical location of the machines that execute the code. Secret Monero Bridge Nodes communicate with each other through I2P destinations which are cryptographic constructs, similar to cryptocurrency wallet addresses. Instead of passing value between different addresses, the I2P destinations transfer network communications between I2P destinations. IP addresses (which offer visibility to identities and physical locations) are not exposed, I2P destinations are exposed. Machines behind I2P destinations can be physically moved to a different physical location without disrupting system operation.

As part of our policy to deliver an unstoppable, uncensorable service, Secret Monero Bridge computers will periodically be moved to different physical locations, across different geopolitical jurisdictions because it’s harder to hit a moving target.

What is the Relationship Between the Price of XMR and sXMR?

XMR and sXMR are pegged 1:1. Therefore the price of 1 sXMR will always equal the price of 1 XMR.

Is there a Delay Processing Deposits?

Yes. Secret Monero Bridge deposits require 6 confirmations on the Monero blockchain before the sXMR will be minted.

Users can check the number of confirmations on the blockchain for a deposit payment by using the monero-wallet-cli command:

check_tx_key <txid> <txkey> <payment_address>

Other wallets should provide similar capability, check with your wallet provider.

Is there a Cost to Use the Secret Monero Bridge?

Yes, a bridge fee is charged for every deposit and withdrawal. Bridge fees are paid in sXMR and are set through governance.

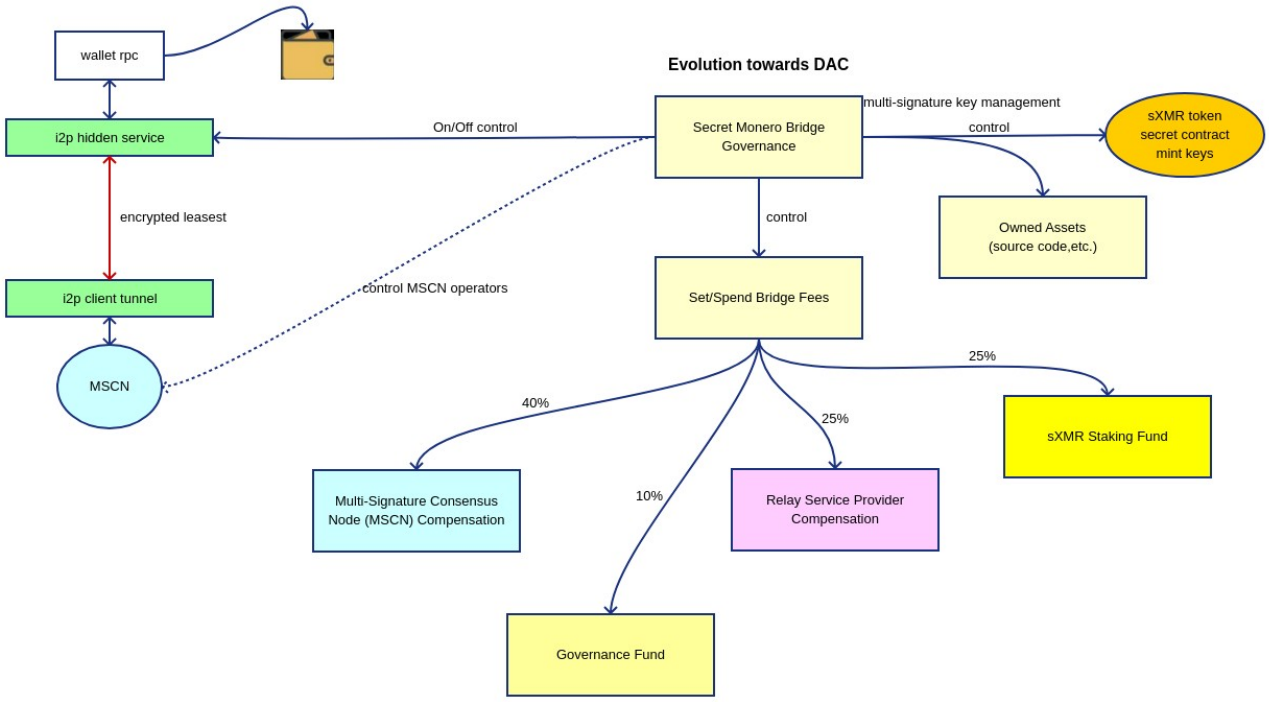
At mainnet launch the bridge fee has been set to 0.0041 sXMR.

Who Gets to Spend Bridge Fees?

Bridge fees are collected to support operations and compensate stakeholders. As shown in the diagram below, Secret Monero Bridge Governance controls the setting and spending of bridge fees. The objective for bridge fees are to fund the operation of the Secret Monero Bridge and this includes the compensation of stakeholders. Bridge fees are collected and spent to:

- compensate MSCN node operation
- compensate Relay Service Providers
- Maintain a governance fund (for governance directed spending)
- Maintain an sXMR Staking fund (providing rewards for staked sXMR)

Secret Monero Bridge Governance Mind Map



What is the Vision for Secret Monero Bridge Governance?

The diagram above shows a portion of the Secret Monero Bridge governance model. The governance model will provide the appropriate controls to ensure the proper operation of the Secret Monero Bridge as required by the community. Examples of what will be covered in governance:

- setting and spending collected bridge fees
- compensating stakeholders such as MSCNs and Relay Service Providers
- Managing a governance fund to fund Secret Monero Bridge governance
- Managing an sXMR staking fund to reward stakers of sXMR from a portion of collected bridge fees
- and more (as defined by the governance DAC community over time)

Is the Secret Monero Bridge Web Application Interface a Decentralized Application (Dapp)?

Yes, the Secret Monero Bridge Dapp is a web application hosted on the Interplanetary File System (IPFS). It does not connect to any centralized servers and runs locally on a user's machine. In version 0.0.1 it uses the Keplr wallet and optionally the user's email client. The Dapp has been designed this way for the user's privacy and anonymity. The Dapp is open source code so that any user has the opportunity to inspect the code.

Why Does the Secret Monero Bridge Require an Email Interface?

One of our primary objectives is to enable privacy and anonymity for our user base and the Secret Monero Bridge itself. The Secret Monero Bridge business model is to enable

deposits and withdrawals for our users. Deposits and withdrawals are implemented through a messaging interface between the user and the Secret Monero Bridge.

Unfortunately most of the technology in use today does not enable sufficient privacy and anonymity. We believe that email is the message transport option that provides us with the least risk to stakeholder privacy and anonymity. The Secret Monero Bridge email account is an i2p mail account which is an anonymous email service residing in the I2P network. User's can also create and use their own i2p email account that would then allow private, and anonymous email messages to flow from the user to the Secret Monero bridge without having to go over the Internet.

Users can use any email service they desire. Our Dapp uses 4096-bit RSA encryption to encrypt the data sent via email messages. However, users should be advised that using services like gmail, yahoo, and others, the email metadata is not encrypted and could be a risk to privacy and anonymity. Metadata such as the user's email (From:) address, Secret Monero Bridge email (To:) address (secretmonero@i2pmail.org), Subject string if provided, are not encrypted and so anyone who has access to the email message can see that the user's email address sent an encrypted message to the Secret Monero Bridge.

If user's choose to use an i2p mail account, this metadata is sent encrypted via I2Ps end-to-end encryption, and is much more private than sending the metadata over the Internet.

Can Users Make Deposits and Withdrawals Without Having to Use the Dapp or the Keplr Wallet?

Yes. We will be providing instructions for how to do this and providing some example scripts to do it. This would be for technically inclined individuals and would require them to use the secretcli and be able to perform RSA encryption using the Secret Monero Bridge public key.

What Support Services are Available?

Because of our privacy/anonymity requirements initial support services are only provided via email (smb@i2pmail.org or smb@mail.i2p).

We will provide a simple private, end-to-end encryption chat communication service for users that have access to I2P in the near-term.

We have been disappointed over and over again with end-to-end encryption messaging packages that have failed to keep communications private and anonymous. We may end up having to build our own as a result.