BSC Process

Seraph is a non-custodial blockchain security notary service offered by Halborn that has been added to Beanstalk by the DAO as an extra line of defense against hacks or other destructive actions to Beanstalk.

The **Beanstalk Seraph Committee**, **or BSC**, is an anonymous group of six reputable community members and Beanstalk core contributors whose role is to:

1. Create and manage various Runbooks for each Seraph-protected function; and
2. Remove Seraph if it must be done for the security or censorship resistance of Beanstalk.

BSC Members serve as signers on the BSC Multisig (BSCM), a 4-of-6 Safe multisig that is the sole wallet that has the ability to remove Seraph protection.

By implementing Seraph, the BCM can no longer singlehandedly corrupt Beanstalk. As Beanstalk returns to on-chain governance, the Beanstalk DAO and BSC can continue to work with Seraph as an extra layer of defense.

Seraph

Seraph is a non-custodial blockchain security notary (BSN) service. A BSN is a cybersecurity professional who serves an organization as a third party witness to the signing of important on-chain actions. A BSN's main purpose is to deter fraud and prevent attacks.

Every function protected by the Seraph notary requires a Runbook. Runbooks are the set of rules and procedures for Seraph to process transactions that call protected functions.

Protected Functions

The Seraph code modifier protects 7 of the highest risk owner functions in Beanstalk:

- `diamondCut` — Add, replace and/or remove any function(s) and/or execute an init function with a delegatecall.
- `whitelistToken` — Add a token to the Deposit Whitelist.
- `dewhitelistToken` — Remove a token from the Deposit Whitelist.
- `unpause` — Unpause Beanstalk, which allows the `sunrise` function to be successfully called at the top of the 2nd hour. The TWAP oracle and Season timer will be reset as well.
- `createFundraiser` — Create a Fundraiser.
- `transferOwnership` — Transfer ownership of the Beanstalk contract to a new address.
- `addUnripeToken` — Add an Unripe token to Beanstalk.

Seraph provides 24/7/365 services to review, analyze, and permit or reject any calls to these functions.

Runbooks

Seraph notaries are required to process any function call according to the specific function's Runbook of rules and procedures.

Each of the Seraph-protected functions has a unique Runbook which establishes the rules and procedures for Seraph notaries to process transactions that call the functions and the priority and risk of each function. The Runbooks for each protected function shall remain confidential between Halborn and the BSC.

The details about transactions that call protected functions and whether they have been reviewed, approved or rejected by the Seraph notary are publicly viewable via the Seraph Dashboard.

Multisig Powers

The Seraph contract has a `removeSeraph` function that initiates a 24 hour timelock, after which the `executeRemoval` function removes Seraph protection from Beanstalk.

The BSCM is the only wallet that can call the `removeSeraph` and `executeRemoval` functions to remove Seraph protection from Beanstalk. BSC Members are the only signers on the BSCM. The BSCM is a 4-of-6 multisig deployed using Safe. Parameters m and n are each ultimately defined by Stalkholders and may evolve in the future via Beanstalk Improvement Proposal (BIP).

The BSCM cannot call any of the owner functions of Beanstalk—only the BCM can.

Responsibilities

Seraph notaries have created the Runbooks in collaboration with the BSC to implement and activate the Seraph protections as effectively and safely as possible. The BSC has approved initial Runbooks for all protected functions.

The BSC can work with Halborn to update Runbooks at any time, but must sign a transaction verifying the new Runbooks for the change to be valid.

Seraph may be deactivated at any time via BIP. However, in instances where Halborn is unwilling to commit a passed BIP that removes Seraph, or where Seraph must be removed for the security or censorship resistance of Beanstalk, the BSC is responsible for doing so.

On the Seraph contract, the BSCM can call the `removeSeraph` function that initiates a 24 hour timelock. After the timelock elapses, the BSCM can call the `executeRemoval` function that removes Seraph from Beanstalk.

Signer Best Practices

BSCM Signers shall follow the best practices outlined below. It is of paramount importance that Beanstalk limits key man risk by implementing best practices with respect to multisig key custody. Signers are expected to:

- Regularly check in with the rest of the BSCM and confirm access to their wallet;
- Maintain active communication regarding travel plans and availability in order to ensure that there are always enough Signers on call; and
- Acknowledge their Signer duties and processes.

In addition to the above expectations, Signers shall follow the BCM's wallet security best practices:

- Use a reputable hardware wallet like Trezor or Ledger;
- Use a fresh wallet that doesn't have any pre-existing transactions or balances on it;
- Set up a new passphrase on their hardware wallet device when selecting a new wallet to be the signing wallet; and
- Follow the standard self-custody best practice guide here.

In the event that one or more Signers are compromised, unresponsive or attempting to violate the processes outlined in `# Responsibilities` (or a Signer voluntarily chooses to be removed from the BSCM), the BCSM will rotate them out of the wallet and replace them with another Signer. Emergency changes to the m-of-n configuration of the BSCM that are made to protect Beanstalk do not require a BIP.

Anonymous Multisig Signers

Off-chain governance introduces significant risks related to security and censorship. The BSCM is designed to mitigate as many of those risks as possible by distributing the multisig keys across reputable community members and Beanstalk core contributors, and collectively implementing and adhering to `# Signer Best Practices`.

The most significant risk associated with off-chain governance is the potential corruption of the BSCM from an outside party. In order to minimize the chances of this, the Signers are anonymous. The anonymous Signers are selected by Publius. Signers are anonymous to each other as well, apart from Publius.

Malicious Key Holder Risk

Under this structure, it’s important to acknowledge the risk of anonymous key holders conspiring to attack Beanstalk. Because only Publius knows the identities of the anonymous Signers, Publius would be the main attack vector—if this malicious actor were to compromise Publius before conspiring to attack Beanstalk, they could be reasonably sure that their identity would never be revealed.

In order to mitigate this attack vector, the BSCM institutes the following process whenever the m-of-n configuration of the BSCM is changed:

- Publius will publish a hash of the list of Signers and their corresponding wallets on-chain (see the **Signer Hashes** section of the BSCM Dashboard in the Farmers' Almanac); and
- Publius will share the list of Signers and their wallets with their personal legal counsel, to be released in the event that Publius is compromised such that they cannot publish the list themselves. This makes Publius and their personal legal counsel the only parties with access to the list.

In the event that counsel publishes the list, anyone could verify that it’s the correct list by hashing it and comparing it with the hash on-chain. This creates accountability for the anonymous Signers.