Beanstalk Community Multisig

BCM Process

The Beanstalk Community Multisig, or BCM, is not intended to have decision making power. Its role is to 1) enact on-chain the decisions Stalkholders make via off-chain voting and 2) review and verify proposals to ensure the suggested changes are truthfully represented.

The BCM is deployed using Gnosis Safe, the most battle-tested multisig contract on Ethereum. Its m-of-n configuration will start as 5-of-9 on Ethereum mainnet. Parameters m and n are each ultimately defined by Stalkholders and may evolve in the future via Snapshot vote.

BCM's Signers are an anonymous and diverse set of:

- Reputable community members; and
- Beanstalk core contributors.

Fertilizer funds will be custodied in the BCM until the Replant.

Multisig Powers

Beanstalk implements the EIP-2535 Diamond Standard, a new standard for fully-upgradeable smart contracts.

The mechanism for upgrading a Diamond is by calling `diamondCut()` which takes arguments of functions to replace and which functions to replace them with. Upon restart, the `diamondCut()` function will only be callable by the owner of Beanstalk, which will be the BCM.

Upgrades should only be executed after a Snapshot has passed and Signers have manually reviewed the code changes. However, in the case of an emergency (like a serious bug or exploit), the BCM may execute transactions to protect the Beanstalk contract. The best practices for emergency response handling are outlined in the `# Emergency Response Procedures` section.

If a community member wants to propose a BIP, they can submit a merge request to the Beanstalk Github repo and begin a formal process with the BCM outlined in the `# Proposing a BIP` section.

In addition to `diamondCut()`, the following functions are also only callable from the owner address:

- `pause()` - when executed, Beanstalk will be Paused and the `sunrise()` function will not be allowed to be called in the contract
- `unpause()` - when executed, Beanstalk will be Unpaused and the `sunrise()` function will again be allowed to be called at the top of the 2nd hour. The TWAP oracle will be reset as well.
- `transferOwnership()` - transfer ownership permissions of the Beanstalk contract to a new address

- `diamondCut()` - add/replace/remove any function(s) and/or execute an init function with a delegatecall
- `createFundraiser()` - creates a Fundraiser
- `whitelistToken()` - add a token to the Silo whitelist
- `dewhitelistToken()` - remove a token from the Silo whitelist

Snapshots

The BCM is an extension of the Beanstalk DAO. As such, BCM's role is to 1) enact on-chain the decisions Stalkholders make via off-chain voting and 2) review and verify proposals to ensure the suggested changes are truthfully represented.

BIPs are voted on at the Beanstalk DAO Snapshot page.

The BCM shall not execute transactions until an associated Snapshot successfully passes in favor of the proposal, except in the case of emergency, cancelling a failed transaction or adding/removing/rotating BCM Signers. Below are the scenarios the BCM will adhere to when transacting:

Transaction	Snapshot?	Voting Period
Proposing BIP	Yes	Up to 7 days as outlined in the **# Voting for BIPs** section
Adding/removing/rotating BCM Signers	No	N/A
Emergency hotfix (needs public notification)	No	N/A
Emergency Pause (needs public notification)	No	N/A
Cancel transaction	No	N/A

Proposing a BIP

Beanstalk's governance is designed to be as censorship resistant as possible. In an effort to promote sufficiently permissionless processes, any community member may submit BIPs after Beanstalk is Replanted. If a community member wishes to propose a BIP, they will need to complete a public proposal process on Discord and submit a Github MR before the BCM will submit a Snapshot on their behalf.

BIP Proposal Process

BIPs consist of two things: a merge request on the public Beanstalk Github repo, and a written explanation

of the changes that would be implemented by the merge request.

The following are the processes in place for community members to submit a BIP and coordinate with the BCM to submit a Snapshot proposal.

1. A proposer must own 0.1% of the total outstanding Stalk supply in order to propose a BIP. The proposer shall verify they meet the Stalk ownership threshold by creating and verifying a signature on etherscan. The steps to create and verify a signature on etherscan can be found here. The proposer will then reach out to the Mods on Discord and from there, the BCM will verify that the address that signed the message has sufficient Stalk.
2. The proposer will submit a merge request on the public Beanstalk Github repo and publish the written proposal in a dedicated channel in the Beanstalk Discord. For assistance creating a channel on Discord, contact the Mods on Discord.
3. The written proposal shall be discussed in the Discord channel for a sufficient amount of time. What constitutes sufficient will be at the sole discretion of the BCM, but the BCM must formally propose the BIP on-chain within 2 weeks of the creation of the dedicated Discord channel, unless the proposer decides to withdraw their proposal.
4. BCM key holders shall verify that they have access to their wallets.
5. The BCM will submit a Snapshot of the written proposal and a corresponding on-chain transaction to formally begin the voting period. In order to ensure that Snapshots are proposed with an associated GitHub MR, the BCM is the only party that can propose BIPs on Snapshot.
6. During the Snapshot voting period (1-7 days), every BCM Signer shall verify the transaction and write an etherscan message confirming their review according to the process outlined in the **# Reviewing and Signing off on Transactions** section. Each Signer is expected to verify every transaction. However, if not all Signers verify the transaction, the BCM may still continue per the process outlined in the **# Rotating Holders In / Out** section.
7. If the Snapshot passes, the Signers will sign m/n signatures and execute the transaction on-chain as soon as possible. If the Snapshot fails, the Signers will submit and execute a cancel transaction with the same nonce as soon as possible.

Voting for BIPs

Voting for BIPs will take place on Snapshot, using Stalk ownership at the time of proposal on Snapshot. Any Stalkholder can vote for or against any Snapshot proposal. In all instances, 1 Stalk equals 1 vote, and voting against a proposal is equivalent to abstaining.

The Snapshot voting period opens when a BIP is submitted to Snapshot and closes after 7 days or once a two-thirds supermajority is reached. In order to be counted, all votes must be signed before the voting period closes.

If at the end of the voting period:

- Less than or equal to half of the total outstanding Stalk at the time of proposal on Snapshot votes in favor of the BIP, the BIP fails; or
-

More than half of the total outstanding Stalk at the time of proposal on Snapshot votes in favor of the BIP, the BIP passes.

If at any time 24 hours or more after the opening and before the closing of the voting period more than two-thirds of the total outstanding Stalk votes in favor of a BIP, the BCM can execute the BIP on-chain.

The BCM shall follow the results of the Snapshot, unless the Stalk distribution is compromised in a flash loan or other governance attack.

BCM Best Practices

BCM 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 custody. Signers are expected to:

1. Regularly check in with the BCM and confirm access to their wallet;
2. Maintain active communication regarding travel plans and availability in order to ensure that there are always enough Signers on call;
3. Regularly rotate Signer wallets every 2-3 months, subject to Snapshot voting; and
4. Acknowledge their Signer duties and processes for signing off on BIPs.

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

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

Signer Duties

Signers are expected to follow best practices and maintain active communication in order to ensure that there are always enough Signers available to execute transactions in case of an emergency. Signer duties are broken down into three stages: 1) confirming access to their wallet, 2) verifying proposed code changes, and 3) executing transactions on the BCM Gnosis wallet.

When a draft BIP is proposed, every Signer shall be notified of the timeline and shall confirm access to their wallet.

Once a Snapshot is proposed, all Signers are expected to promptly review and verify that the proposed code changes are accurately represented. After a Signer has followed the guide laid out in the **# Reviewing and Signing off on Transactions** section, they will submit and sign an etherscan message that publicly confirms their review. This will 1) limit blind signing and 2) encourage each Signer to verify that

a BIP's code changes are accurately represented and distributed to the public. The steps to create and verify a signature on etherscan can be found here. Anyone can verify that the Signer reviewed and signed off on the proposed code changes during the voting period.

Signers will sign the transaction to either execute the proposed transaction or cancel it as soon as possible following the conclusion of the voting period.

Once sufficient signatures have been provided to execute the transaction, is it expected that one of the Signers execute the transaction. Upon Replant, Publius shall initially execute the transaction and pay for gas fees. After Beanstalk Replants and Signers are more comfortable, Publius or Beanstalk Farms shall distribute enough ETH to every Signer to execute a transaction in case of emergency. Signers are not expected to contribute capital to participate in the BCM.

A Signer shall lose their role (by action of the remaining Signers removing them) in case they:

- Act against Stalkholders' off-chain voting;
- Do not follow best practices outlined in the **# BCM Best Practices** section; or
- Get through 2 months or 2 votes (whichever happens first) without performing any of their Signer duties.

Emergency Response Procedures

The BCM's role is to 1) enact on-chain the decisions Stalkholders make via off-chain voting and 2) review and verify proposals to ensure the suggested changes are truthfully represented. However, if a situation arises in the future like the April 17, 2022 exploit, it is of critical importance that the BCM take swift action to protect Beanstalk.

Bugs or security vulnerabilities qualify as emergencies. Emergency action will never be taken for any reason related to the economic health of Beanstalk (like a bank run, for example).

Depending on the severity of a given emergency, BCM members shall swiftly decide the best course of action:

- If an emergency is severe and requires significant code changes to fix, the BCM will Pause Beanstalk and take any necessary extra action to mitigate further damage; or
- If an emergency is minor and does not require significant code changes, an emergency hotfix may be implemented by an emergency vote of the BCM.

After emergency action is taken, the BCM shall swiftly issue a summarized report to the community detailing:

1. the administrative permissions that were used (e.g. Pausing Beanstalk or turning off certain functions);
2. the context and severity of the issue; and
3. the next steps and decisions, if any, that the community must agree on in order for Beanstalk to proceed.

Reviewing and Signing off on Transactions

Everyone on the BCM shall be expected to know how to verify diamond cut data and submit an etherscan transaction confirming they have checked the submitted transaction. Until Beanstalk is Replanted, Signers are not required to verify each transaction, but doing so is strongly encouraged.

As a part of submitting BIPs, the proposer will be responsible for providing thorough documentation or supplementary video to the Beanstalk DAO and BCM for how to review/test all relevant code.

The following should be used as a guide for the minimum review criteria:

- Check function call is as expected
  - If function is diamondCut,
  - confirm Facet Cuts–check Facet address, function selectors and Facet Cut actions are correct
- Check init address and calldata are correct
- Test BIP on mainnet fork or testnet as necessary
- Review conceptual changes involved in BIP
- Review Github MR change log (naming or other small nits)
- Review constants (contract addresses, numbers) in new contracts

Once Signers have verified the transaction, they shall submit and sign a verified etherscan message and distribute the public verification link to the BCM.

Problems During Verification

The BCM will never submit a transaction that was misrepresented on Snapshot.

In the case that any Signer during the verification process determines that a MR does not accurately represent the BIP, that Signer will submit a verified etherscan message indicating as such with context on the issue. At that point, the BCM will not submit the transaction unless it is determined that the Signer is "rogue" and is attempting to censor the BIP. In the case the other Signers determine that one or more Signers is rogue, they will submit a verified etherscan message indicating as such. At that point all present key holders shall submit a new verified etherscan message to cancel the original transaction.

The BCM will notify the community via Discord and work with the proposer to resolve the issue in the MR. Once resolved, a new BIP will be proposed on Snapshot with its associated transaction.

Rotating Holders In / Out

In the event that one or more Signers are compromised or vote against the results of any Snapshot, the BCM will rotate them out of the wallet and replace them with another Signer. In no instance shall more than 4 keys be held by Beanstalk Farms contributors, nor shall more than 1 key be held by Publius.

Once a transaction is submitted on-chain, the BCM will adhere to the results of the Snapshot and each member shall verify the transaction on etherscan during the voting period.

If a situation arises where not all Signers submit a verification, the BCM may continue with execution if the Signer:

1. was not responsive during Snapshot proposal;
2. failed to notify the BCM during the draft phase of the proposal that they would not be able to execute the transaction;
3. missed 2 verifications;
4. was not responsive in 2 months; or
5. votes against the result of any Snapshot vote (AWOL). In this case, the Signer would be subject to removal immediately.

It is important that Signers regularly rotate multisig wallets in order to continuously ensure that all members of the BCM have access to their wallet and that their key is not compromised. Therefore, the multisig wallets will be rotated every other month, independent of whether or not a Signer is staying on the BCM.

Anonymous Multisig Signers

Off-chain governance introduces significant risks related to security and censorship. The BCM 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 BCM best practices.

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

A maximum of 4 Signers will be members of Beanstalk Farms. Publius collectively will hold at most 1 key. The remaining keys will be held by reputable members of the Beanstalk community.

Malicious Key Holder Risk

Under this structure, it's important to acknowledge the risk of anonymous key holders conspiring to attack Beanstalk. Since 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 BCM will institute the following process whenever the m-of-n multisig is changed:

- Publius will publish a hash of the list of Signers and their corresponding wallets on-chain. You can find these on the BCM Dashboard.
- 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.

BIP-20: Migration of Balances

This document outlines the process for voting on and committing BIPs after the ownership has been transferred to the BCM. Beanstalk Farms shall propose transferring ownership of the Beanstalk contract to the BCM in BIP-21.

BIP-20 was approved by the Beanstalk DAO. BIP-20 proposes the series of transactions necessary to perform the migration of balances. This will be the sole instance where multiple BCM transactions are approved in a single BIP.