Beanstalk DAO Disclosures

Interacting with Beanstalk involves many risks. Before interacting with Beanstalk, you should review the relevant documentation to make sure you understand how Beanstalk works, as well as information about the current state of Beanstalk. Beanstalk Farms has created this set of disclosures to assist in the educational process. These disclosures are not exhaustive. The Beanstalk Whitepaper, the Farmers' Almanac, and other Beanstalk resources, as well as participating in the Beanstalk community, can help to understand the protocol. Before participating in the protocol, everyone should do their own research, investigation and analysis.

Transparency is the cornerstone of DeFi. The Beanstalk decentralized autonomous organization (DAO) endeavors to be as transparent as possible, particularly as it pertains to communicating the risks of interacting with Beanstalk.

1. BEANSTALK WAS ATTACKED ON APRIL 17, 2022 VIA ON-CHAIN GOVERNANCE. ALL ~$77M IN NON-BEAN ASSETS WERE STOLEN. PROTOCOL GOVERNANCE HAS BEEN CHANGED TO A 5-OF-9 COMMUNITY MULTISIG.

On April 17, 2022, Beanstalk was attacked via on-chain governance resulting in a theft of all ~$77M in non-Beanstalk user assets. The attacker used a flash loan to compromise the governance mechanism and steal the assets deposited in the DAO.

Shortly after the attack, Beanstalk was Paused and on-chain governance was removed. Since the attack, governance votes have taken place on Snapshot. Beanstalk is now owned by a community-run multisig wallet (the Beanstalk Community Multisig, or BCM) responsible for executing the will of the DAO as indicated via Snapshot vote. The keys to the BCM are custodied by an anonymous group of nine Beanstalk community members and contributors. This serves as a temporary security measure until a secure and fully-decentralized governance mechanism has been developed and sufficiently audited. All contract changes under the BCM structure require the signature of 5-of-9 BCM members.

The old Bean token was replaced with a new one. The obsolete token has no value according to Beanstalk.

More information:

- Past BIPs
- Beanstalk Governance Exploit
- BCM Process

2. THERE IS NO MAXIMUM BEAN SUPPLY. THE BEAN SUPPLY CAN GROW INFINITELY THROUGH DEMAND-BASED MINTING AND GOVERNANCE.

Beanstalk increases the Bean supply every Season where the liquidity and time weighted average price of 1 Bean is greater than $1 over the previous Season. Enough Beans are minted such that if all the newly minted Beans were sold, the Bean price would return to $1. Those Beans are distributed to Stalkholders, Pod holders and Active Fertilizer holders.

The Bean supply is uncapped and grows as demand for Beans increases. Beans can also be minted arbitrarily through governance (see #7).

More information:

- Beanstalk Analytics Links
- Whitepaper, Section 8.10, Bean Supply
- Bean Supply Documentation

3. BEANSTALK DID NOT HAVE A PRE-MINE, PRE-SALE, OR TEAM ALLOCATION. ALL BEANS HAVE BEEN MINTED IN ACCORDANCE WITH EITHER THE MINTING SCHEDULE OR GOVERNANCE.

Beanstalk did not have a pre-mine, pre-sale or team allocation of any kind. The first 100 Beans were minted when the `init` function was called to deploy Beanstalk.

Beanstalk launched without the need to raise capital. However, after an on-chain governance attack on April 17, 2022 (see #1), a fundraiser known as the Barn Raise is being used to recapitalize the non-Bean funds stolen in the exploit. The terms offered in the fundraiser are available to any Ethereum address.

More information:

- BFP-72: The Path Forward, No Haircuts
- Whitepaper, Section 7, Barn
- Barn Raise Documentation

4. BEANSTALK RELIES ON THIRD PARTIES TO PROVIDE CREDIT TO RETURN THE BEAN PRICE TO ITS PEG. THERE IS NO LENDER OF LAST RESORT.

Beanstalk uses a credit based model, allowing anyone to lend Beans to the protocol to participate in peg maintenance. Beanstalk burns any Beans it borrows. As a consequence, the ability of the protocol to return the price of a Bean to the peg relies on the availability of willing creditors, which is not guaranteed. The economic design of Beanstalk fails if it can no longer attract creditors.

More information:

- Whitepaper, Section 6, Field
- Field Documentation

5. BEANSTALK DOES NOT GUARANTEE THE BEAN PRICE. INSTEAD BEANSTALK INCENTIVIZES THE REGULAR OSCILLATION OF THE BEAN PRICE ABOVE AND BELOW ITS PEG THROUGH PROTOCOL-NATIVE INCENTIVES.

Bean is not a collateralized stablecoin and Beanstalk offers no guarantee of the value of Bean. Beanstalk was deployed on August 6, 2021. Since then, the Bean price has crossed its dollar peg thousands of times. Even so, Beanstalk is still in an early stage and various parts of its economic design continue to be improved through governance.

Beanstalk tries to incentivize the regular oscillation of the Bean price above and below its peg. While the protocol's incentives are designed to return the price of a Bean to its peg, the timing of oscillations is indeterminate. The price will almost never be exactly equal to its peg. Crossing the peg in the past is no guarantee of it happening again in the future.

More information:

- Whitepaper, Section 8.1, Ideal Equilibrium
- Peg Maintenance Documentation

6. BEANSTALK-NATIVE DEBT DOES NOT HAVE A MATURITY DATE AND THEREFORE MAY NEVER BECOME REDEEMABLE FOR BEANS.

Beanstalk borrows Beans from lenders in exchange for Pods and Sprouts. Bean loans have fixed interest rates but do not have fixed maturity dates.

Pods and Sprouts are repaid when the liquidity and time weighted average price of 1 Bean is greater than $1 over the previous Season, but there is no guarantee this will continue until all Pods and Sprouts become redeemable (see #4). Governance may also arbitrarily modify the redeemability of Beanstalk debt (see #7).

More information:

- Whitepaper, Section 11.2, Strong Credit
- Economics Documentation

7. STALKHOLDERS CAN MAKE ARBITRARY CHANGES TO BEANSTALK THROUGH GOVERNANCE, IF ENACTED BY THE BEANSTALK COMMUNITY MULTISIG. THERE IS NO GUARANTEE THE CHANGES WILL BE BENEFICIAL TO BEANSTALK.

Beanstalk is governed by the Beanstalk DAO—the Silo, which is comprised of Stalkholders. Stalkholders vote on Beanstalk Improvement Proposals (BIPs), which can arbitrarily change Beanstalk. Voting rights come from Stalk ownership (see #8 for details on Stalk).

Any community member that meets a certain Stalk ownership threshold may propose a BIP. If the BIP passes, the Beanstalk Community Multisig (see #9 for details on the BCM) executed the will of the DAO based on the results of the vote, unless the Stalk distribution is compromised in a flash loan or other governance attack. Through this governance process, Stalkholders may make arbitrary changes to Beanstalk.

More information:

- Beanstalk DAO Snapshot
- Past BIPs

8. ANYONE CAN RECEIVE STALK BY DEPOSITING WHITELISTED ASSETS IN THE SILO. EARLIER DEPOSITORS IN THE SILO HAVE PROPORTIONALLY GREATER GOVERNANCE POWER RELATIVE TO THE BEAN DENOMINATED VALUE ORIGINALLY DEPOSITED.

Depositors earn Stalk and Seeds. Seeds yield 1/10000 new Stalk every Season. Stalkholders participate in governance and earn Bean seigniorage. Stalk ownership, and thus governance power, decentralizes over time.

As earlier Depositors in the Silo have been accruing Stalk from Seeds for more Seasons compared to later Depositors, these Depositors have greater governance power in proportion to the Bean Denominated Value (BDV) of their original Deposits.

More information:

- Whitepaper, Section 5.1, The Stalk System
- The Stalk System Documentation

9. THE BEANSTALK CONTRACT IS OWNED BY THE BEANSTALK COMMUNITY MULTISIG. THE MULTISIG CAN MAKE ARBITRARY CHANGES TO BEANSTALK WITH 5-OF-9 SIGNATURES FROM THE ANONYMOUS SIGNERS. THERE IS NO GUARANTEE THE MULTISIG ENACTS THE GOVERNANCE DECISIONS OF THE DAO.

Ownership of the Beanstalk contracts is held by a 5-of-9 multisig known as the Beanstalk Community Multisig (BCM). The BCM is an extension of the Beanstalk DAO. The BCM's role is to enact on-chain the decisions Stalkholders make via off-chain voting on Snapshot. Besides Publius (one of the members), all members of the BCM are anonymous. Publius selected the other members, who Publius believes will act in the best interest of Beanstalk. This process was approved via governance.

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 a set of best practices. There is no guarantee the BCM enacts the governance decisions the DAO voted on via Snapshot.

More information:

- BFP-73: Beanstalk Community Multisig
- BCM Multisig Powers Documentation
- Anonymous Multisig Signers Documentation
- BCM Dashboard

10. AS GOVERNANCE POWER IS DETERMINED THROUGH STALK OWNERSHIP, SUFFICIENT CAPITAL COULD PURCHASE SIGNIFICANT GOVERNANCE POWER AND TAKE OVER BEANSTALK.

Beanstalk is governed by Stalkholders, as described in #7. Stalk ownership, and thus governance power, decentralizes over time given the inflationary nature of Stalk. However, there is no maximum Stalk supply. Stalk is minted for Deposits based on the Bean Denominated Value (BDV) of the Deposit, up to any arbitrary BDV.

Stalk ownership was previously compromised via flash loan, which enabled the on-chain governance attack on April 17, 2022 (see #1). The Beanstalk Community Multisig serves as a temporary security measure until a secure and fully-decentralized governance mechanism has been developed and sufficiently audited.

More information:

- Whitepaper, Section 5.1, The Stalk System
- BCM Process

11. MOST OWNER FUNCTIONS OF THE BEANSTALK CONTRACT ARE PROTECTED BY SERAPH, A BLOCKCHAIN SECURITY NOTARY SERVICE, IMPLEMENTED BY HALBORN, INC. THERE IS NO GUARANTEE THE RUNBOOKS FOR SERAPH PROTECTED FUNCTIONS ARE FOLLOWED OR THAT THE RUNBOOKS HELP PROTECT BEANSTALK. THERE IS NO GUARANTEE THAT SERAPH PROTECTIONS ARE ONLY REMOVED WHEN APPROPRIATE.

The Beanstalk DAO implemented Seraph into Beanstalk, a blockchain security notary service offered by Halborn, Inc. Every function protected by Seraph requires a Runbook. Runbooks are the set of rules and procedures for Seraph to process transactions that call protected functions.

Seraph notaries created and maintain the Runbooks in collaboration with the Beanstalk Seraph Committee (BSC) to activate and implement the Seraph protections as effectively and safely as possible. The BSC's other responsibility is serving as signers on the multisig that is the only wallet that can remove Seraph protection from Beanstalk. The BSC members are anonymous and were selected by Publius. This process was approved via governance.

Seraph introduces significant risks related to security and censorship. There is no guarantee that:

- The Runbooks approved by the BSC are followed by Seraph notaries;
- Any of the Runbooks that are followed protect Beanstalk;
- The BSC will remove Seraph protections when necessary for the security or censorship resistance of Beanstalk; or that
- The BSC does not remove Seraph protections when it is not beneficial to Beanstalk.

More information:

- BIP-34: Seraph
- BSC Process
- BSCM Dashboard

12. A VULNERABILITY IN ETHEREUM COULD RESULT IN A LOSS OF FUNDS. BEANSTALK ASSUMES THE SECURITY OF ETHEREUM.

Ethereum is the largest smart contract blockchain by market capitalization, total value deposited, and dollar denominated transaction value. In general, open source networks with large amounts of value on them and long track records indicate security, but there is no guarantee. Beanstalk assumes the security of the Ethereum network.

13. A VULNERABILITY IN CURVE COULD RESULT IN A LOSS OF FUNDS. BEANSTALK ASSUMES THE SECURITY OF CURVE AMMs.

Bean's sole liquidity pool (at Replant) is a BEAN:3CRV pool on the Curve AMM. Curve is among the largest Ethereum-native decentralized exchange protocols by volume. In general, open source protocols with large amounts of value on them and long track records indicate security, but there is no guarantee. Beanstalk assumes the security of Curve.

More information:

- BFP-76: Choose Replant Liquidity Pool

14. THE BEAN PRICE IS DERIVED FROM THE VALUE OF ASSETS IT TRADES AGAINST IN DECENTRALIZED AMMS. THERE IS NO GUARANTEE ANY OF THESE ASSETS RETAIN VALUE.

The value of Beans is derived from the non-Bean assets trading against it in decentralized liquidity pools. Each of these assets have their own set of associated risks, unique to the asset. Beanstalk implicitly assumes risk associated with these assets.

15. BECAUSE BEANS DERIVE THEIR VALUE FROM THE ASSETS THEY TRADE AGAINST, AND NOT COLLATERAL, IT IS NOT POSSIBLE FOR ALL BEAN HOLDERS TO EXIT AT A DOLLAR OF VALUE FOR EVERY BEAN.

Beans are not redeemable for any other asset; they can only be traded for another asset that Beans are trading against. As Bean holders sell their Beans, there is less and less value trading against Beans. Thus, unlike collateralized stablecoins, it is not possible for the Bean supply to scale down to zero with every Bean holder getting a dollar of value for every Bean sold.

16. BEANSTALK REQUIRES TRUSTLESS AND RELIABLE ACCESS TO A MANIPULATION-RESISTANT PRICE ORACLE FOR A DOLLAR. BEANSTALK USES THE ON-CHAIN PRICES OF OTHER STABLECOINS TO DETERMINE THE PRICE OF A DOLLAR. THERE IS RISK ASSOCIATED WITH EACH OF THESE STABLECOINS THAT CAN COMPROMISE THEIR INTEGRITY AS ACCURATE PRICE ORACLES.

Beanstalk's core objective is to oscillate the price of a Bean above and below its dollar peg. To do this, Beanstalk must be able to reliably measure the price of a dollar on-chain without trusting a centralized third-party to provide it. A robust, decentralized stablecoin requires a tamper-proof, manipulation resistant and decentralized price oracle.

At Replant, Beans are traded in the BEAN:3CRV pool on Curve. 3CRV consists of USDC, USDT and DAI. Beanstalk assumes the average value of each USDC, USDT and DAI in the pool is equal to $1. A disruption in the reliability or accuracy of 3CRV as an accurate measure of $1 could impact Bean minting, resulting in adverse consequences for Beanstalk.

More information:

- Whitepaper, Section 8.2, Decentralized Price Oracle
- Decentralized Price Oracle Documentation

17. BEANSTALK REQUIRES THAT THE SUNRISE FUNCTION IS CALLED AT THE TOP OF EACH HOUR ON ETHEREUM. FAILURE TO SUCCESSFULLY INCENTIVIZE THE CALLING OF THE SUNRISE FUNCTION COULD HAVE AN ADVERSE AFFECT ON BEANSTALK'S ABILITY TO OSCILLATE THE BEAN PRICE ABOVE AND BELOW ITS PEG.

Beans and/or Soil are minted upon a successful call of the `sunrise` function. Beanstalk covers the cost of `sunrise` by awarding the sender of an accepted `sunrise` function call with newly minted Beans. The failure of Beanstalk to successfully incentivize the calling of `sunrise` would effectively result in the failure of Beanstalk to influence the size of the Bean supply, and thereby the Bean price.

More information:

- Whitepaper, Section 4, Sun
- Sun Documentation

18. THE BEANSTALK CONTRACTS ARE OPEN SOURCE. ANYONE CAN VIEW THE SOURCE CODE AND ATTEMPT TO FIND VULNERABILITIES.

The Beanstalk contracts are open source and deployed on the Ethereum blockchain. There may be bugs, flaws, or other unintended consequences from using open source code to govern irreversible financial transactions on a decentralized network. These issues may lead to a loss of funds if present and discovered by malicious actors, and has in the past (see #1).

More information:

- Beanstalk on GitHub

19. BEANSTALK IS AUDITED BUT AUDITS CANNOT GUARANTEE SECURITY. IT IS ANTICIPATED THAT FUTURE CODE WILL NOT BE AUDITED BEFORE IMPLEMENTED.

Security is paramount to Beanstalk's success. Prior to Replant, the majority of Beanstalk's code was audited by Halborn and Trail of Bits. While both are reputable audit firms, there is no guarantee Beanstalk is secure. Beanstalk was audited by Omniscia prior to the attack.

In the future, it is anticipated that the DAO will vote to implement unaudited code. There is always additional risk associated with implementing unaudited code.

Halborn has performed a pentest of the Beanstalk UI hosted at app.bean.money, but there is no guarantee that interacting with Beanstalk through the Beanstalk UI is secure. Any issues could lead to a loss of funds.

The Beanstalk SDK is unaudited. There is no guarantee that interacting with Beanstalk through the Beanstalk SDK is secure. Any issues could lead to a loss of funds.

More information:

- Beanstalk Audit Reports
- Beanstalk UI Halborn Report
- Beanstalk SDK on GitHub

20. THE APP.BEAN.MONEY FRONTEND CAN BE CENSORED AS IT IS HOSTED ON A CLOUD PROVIDER.

The Beanstalk UI hosted at app.bean.money is hosted on Netlify, a privately held, United States based cloud provider. Netlify could censor the frontend at will, or a technical disruption could prevent access. In either scenario, Beanstalk would not be accessible from a web browser until (1) Beanstalk Farms, the decentralized development organization that manages the site, could deploy the frontend elsewhere, or (2) other parties could use the open source code to deploy their own frontends to interact with the Beanstalk contracts.

There have been multiple instances of Netlify getting compromised, resulting in phishing attacks. There is no guarantee that the Beanstalk UI will not be subjected to similar attacks.

More information:

- Beanstalk UI on GitHub

21. THE APP.BEAN.MONEY FRONTEND DEPENDS ON THE BEANSTALK SUBGRAPH FOR DISPLAYING VARIOUS ON-CHAIN DATA. THERE IS NO GUARANTEE THAT SUBGRAPH DATA IS ACCURATE.

The Beanstalk UI hosted at app.bean.money depends on the Beanstalk Subgraph for displaying data, particularly on the Market and Analytics pages. The Beanstalk Subgraph is primarily developed and deployed by Beanstalk Farms.

By default the Beanstalk UI uses a version of the subgraph hosted by Beanstalk Farms, which can be censored. The subgraph that the Beanstalk UI uses can be adjusted in the settings.

More information:

- Beanstalk Subgraph on GitHub
- BFSM Dashboard

22. REGULATORY INTEREST IN STABLECOINS AND DECENTRALIZED FINANCE WILL RESULT IN NEW INDUSTRY REGULATIONS. THE IMPACT OF FUTURE REGULATIONS ON BEANSTALK IS UNCERTAIN.

In alignment with the ethos of DeFi, Beanstalk has been designed to be permissionless and censorship resistant, without the requirement for any trust-providing intermediary.

It is unclear what regulations, if any, governments will attempt to impose on DeFi. Therefore, it is impossible to predict how any new government regulations of DeFi will affect Beanstalk, or any of the protocols or networks Beanstalk relies on as part of its ecosystem.

23. BEANSTALK IS PRIMARILY DEVELOPED BY PAID AND UNPAID CONTRIBUTORS AT BEANSTALK FARMS AND BEAN SPROUT.

Beanstalk is not a finished protocol and requires ongoing technical, ecosystem and community development. The Beanstalk DAO is responsible for the formation and governance of two independent, symbiotic organizations with distinct mandates: Beanstalk Farms (BF) and Bean Sprout (BS). Beanstalk Farms focuses on protocol and community development and Bean Sprout is a Beanstalk accelerator program. Budgets for BF and BS have been minted via governance and have been approved quarterly by the Beanstalk DAO.

Publius, the pseudonym for the three co-founders of Beanstalk, continues to be influential within BF, BS, and the Beanstalk DAO. The identities of Publius are public. The identities of most of the remaining contributors of BF and BS are anonymous.

More information:

- Beanstalk Farms Documentation
- Bean Sprout Documentation