NEW BEE SWARM: a better storage infrastructure at Ethereum

New Bee Swarm Lab*

01.07.2021

Abstract

The Ethereum network is developing rapidly, and the large number of DApps have brought huge storage demands. Therefore, providing a satisfied distributed storage services for Ethereum is undoubtedly a battlefield for the blockchain storage research teams, even including the Ethereum technical team itself. Swarm is a system of peer-to-peer networked nodes that create a decentralised storage and communication service, founded by the original Ethereum founding team members and has received a lot of attention in recent months. However, this star project is extremely rough, no matter from its internal technical framework design, the economic model to the way how the swarm team operate the project, which makes the entire project stagnated and greatly harms the interests of node participants. In order to develop a fairer and more sustainable Ethereum decentralized storage ecosystem, we decided to fork the Swarm project, and therefore we introduce the New Bee Swarm.

I. Background

New Bee Swarm project is created to replace the absolutely defective Swarm project for the Ethereum network. This is the result after seeing the Swarm team running the Swarm project badly and treating it as a pure money-making tool. Ironically contrast that the Swarm team has made tons of money, the poor reward system of the node operators makes the node participants got insufficient income to support their node operation, and this amazing Swarm team did nothing except teach all the node owners to stay patient, with the following problems:

1. **Flawed Economic Model.** Official Swarm team is holding a dominated proportion of the BZZ tokens (c.f. BZZ token allocation), which shows the existing benefit limit of all the other Swarm participants. The Swarm token model does not rule out the possibility of additional issuance, and the total amount of BZZ is unlimited, therefore the price of BZZ is not easy to rise dramatically. Even at this early stage, for the miners there is no need for pre-staking, resulting in insufficient purchase motivation.

2. **Poor Bonding Curve Design.** Swarm adopted a bonding curve mechanism, but mistakenly linked the buying and selling behavior with the issuance and destruction of BZZ. Under this stupid relationship, the price of BZZ is most likely not to skyrocket and plummet, but to stabilize. Clearly, the mainnet launch is absolutely not reflected in the price of BZZ. Previously the OTC price of BZZ related futures was as high as 300 USDT, but the highest exchange price of BZZ after the launch was only 28 USDT, which was obviously not match with the market expectation. The setting of bonding curve itself

*https://github.com/FBZZ

determines that the market price of BZZ cannot increase significantly.

3. **Illogical Incentive Mechanism.** By the incentive mechanism, Swarm is trying to motivate: 1. More node deployment. 2. Much stable bandwidth supply. Theoretically, this two pieces together in the early stage should contribute the main source of income for node participants. The P2P has to integrate the bandwidth of all nodes, the more nodes are deployed, the greater the bandwidth of the entire network and therefore the better revenue of a single node. All sounds good until we start to consider the built-in storage incentive income. Currently the whole ecosystem of Swarm relies on the task posting mechanism: a task provider publishes a task (say, set 100 BZZ as the reward). After the bee node completes the task it can share the allocation of 100 BZZ in proportion to the contribution. The problem is that if there is no task provider to publish tasks, there is no way to dig BZZ, which is exactly the problem we are facing as a BZZ miner.

4. **Peculiar Hardware Requirement.** The Swarm team claims that they hope to provide a decentralised data storage and distribution technology, to power the next generation of censorship resistant, unstoppable serverless apps. However, when we have a deeper understanding of its incentive mechanism and related hardware requirements, we will find that even Raspberry Pi can run the bee client (and the official Swarm team actually uses it themselves). If the swarm network is only run by low-cost machines, no one can guarantee the service quality. "Decentralized data storage" seems more like a slogan.

II. What we do

New Bee Swarm project provides a better version of data storage and distribution services to truly power DApps on the Ethereum network. New Bee Swarm avoids all the defects of Swarm and adds more new features which we believe can really help the entire storage network become more stable and sustainable:

- Forked from Swarm, but independent of Swarm network and better than Swarm.
- More efficient storage experience.
- More complete economic model.
- No bonding curve and no tokens reserved by the team.

III. How we do

.1 Forking

Forking refers to modification of the rules of the existing network. Upcoming New Bee Swarm (FBZZ) fork is a hard fork direction competing with Swarm. What's going to happen is Swarm will be forked, and users who hold the existing BZZ before the fork will have chance to get the upcoming new assets. Parts of the FBZZ token will be used to redeem BZZ.

.2 Connectivity

New Bee Swarm keeps the underlay P2P network, which maintains a network of nodes in such a way that all nodes can send messages between each others. Messages exchange happen via long-lasting between nodes using peer-to-peer network protocol, and the topological basis for node connectivity of New Bee Swarm adopts Kademlia structure.

.3 Storage

- Distributed storage system of New Bee Swarm uses a data integrity certification scheme based on the Merkel tree. After user encrypts the file, the user generates and saves a random challenge, which corresponds to the block data (one-to-one). The block data and the random challenge are hashed together to form a Merkel leaf node, which is constructed into a Merkel tree, and the user saves the node information of the Merkel tree leaves and the height of the Merkel tree.

  In the verification phase, the user randomly selects a challenge from the random challenge and sends it to the New Bee Swarm storage engine. The engine sends the challenge to the storage provider for verification and then returns the user result. The storage system of New Bee Swarm includes the roles of users, storage engines, and storage providers. There are three core stages of the entire process: data storage, data retrieval, and transaction payment. In the data storage stage, users submit data and files to the storage engine, and the engine will distribute the data to the storage provider after the encryption.

Process

1. *Application Stage*
   a. User pledges FBZZ token and sends a storage request, and the user provides information to our storage engine.
   b. The New Bee Swarm storage engine checks the user's qualifications. The audit result is written into the chain and after the network node is confirmed if the New Bee Swarm storage engine issues an access certificate to the user; if the audit fails, the access will not issue a certificate.

2. *Registration Stage*
   a. Send the license to the user for storage request.
   b. After New Bee Swarm confirms the user's identity, the user encrypts the file private key and sends it to the storage engine.

3. *Preparation Stage*
   a. After the user encrypts the data, a series of challenge factors are randomly generated and verified, then the challenge factors are saved. The user hashes the challenge factor with the data and constructs the file Merkel tree. The user saves the file tree locally and sends the block file data to the file intermediary.
   b. The intermediary distributes the file data to the storage provider, and informs the user about the distribution.

4. *Challenge and Retrieval Stagee*
   a. The user randomly selects a challenge factor and sends it to the storage supplier.
   b. The storage provider generates a data integrity certificate and sends evidence of data integrity to the user, and then the user verifies whether the proof of completeness is correct.

5. *Payment Stage*
   A sequence expired revocable contract channel has been established between the user and the storage provider. When the system verifying the data integrity certificate in the challenge stage, the user pays storage fees to the storage provider through the New Bee Swarm network.

Proof of Storage

Storage is proved by providing a segment of the original file and a list of hashes from the file's Merkle tree. This information is sufficient to prove that the segment came from the original file since proofs are submitted onchain, so anyone can verify its validity or invalidity. Each storage proof uses a randomly selected segment. Clearly if the possession of a random segment is able to be demonstrated consistently, then they are very likely storing the whole file. Storing only 50% of the file will be unable to complete approximately 50% of

the proof.

What's worth to point out is, New Bee Swarm integrates the data integrity certification scheme with the SWAP to ensure that (I) peers keep track of each other's bandwidth contribution; (II) node operators collaborate in routing messages, while protecting the network against frivolous use of bandwidth; (III) it is free to use for those who are downloading or uploading a small amount of content or are willing to wait until they have earned credit by providing reciprocal services on each peer connection.

Ecosystem

C.f., Section .5 Algorithmic Economy.

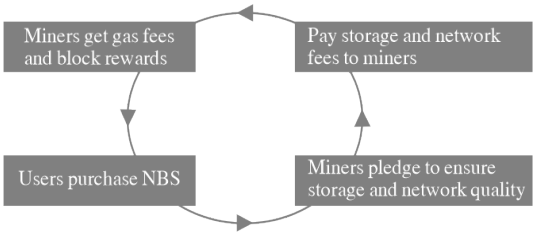

Figure 1: *Sustainable Ecosystem*

.4 Govenance

New Bee Swarm embeds with off-chain governance, because the core of New Bee Swarm is distributed storage computing. The off-chain governance mechanism allows some nodes (super nodes) to perform monitoring and advanced calculations that are different from ordinary nodes. So far, there are super nodes in the New Bee Swarm system, responsible for determining the tightness and activeness of the connection. The mainnet relies on an unforeseen random number algorithm to select 15-30 (to be determined) nodes, so that only a few nodes in the entire network can complete the calculation of simple hash sharding tasks, so that the remaining nodes can handle more basic tasks (such as storage or elastic computing). The process of randomly selecting some nodes can greatly avoid the waste of computing power and allow more micro-computing equipments to participate. At the same time, we can foresee that there will be different types of mining machines produced for different tasks. It creates an opportunity for existing mining machines (produced for other storage projects) on the market to switch to FBZZ mining. Also the unpredictable random number algorithm makes all nodes in the network have the same probability to be selected.

.5 Algorithmic Economy

First, there is no bonding curve in New Bee Swarm so no factor here can affect the market pricing.

Second, FBZZ staking is adopted to provide economic security for New Bee Swarm. A node needs storage resources or workload guarantees to have a stake quota. There is a conversion rate X between its storage resources or workload guarantees and the FBZZ quota. The effective pledge base of storage resources per TB is β, and the effective pledge amount weight coefficient of meaningful storage data per TB is α. The design of X is divided into two stages. The formula for the first stage is:

$$X=Z^*\beta+M^*\beta,$$

where M refers to effective data volume and Z refers to spare storage resources, both take TB as unit. The effective data M refers to the data uploaded to the node after the user places a storage order through the storage market. The spare storage resource Z refers to the remaining storage resources of the node after the effective data is removed.

Taking into account that the number of copies of each file is not the same, so the effective quota of each node is calculated as:

$$X=Z^*\beta+\sum_{i=0}^{n}(\alpha_i{}^*M_i\beta),$$

As the network grows, when the number of effective FBZZ stakes in the entire network

reaches a certain percentage of the total amount of the entire network, it enters the second stage. In the second stage:

$$X=R*V/\sum_{i=0}^{n}(V_i)*Amount_{nb},$$

where R refers to conversion factor, V refers to effective quota of node resources under the stage one, n is the number of all networked nodes and $Amout_{nb}$ is the total number of FBZZ tokens in the entire network.

Follow this design, the coefficient R sets the upper limit of FBZZ for effective staking in the system. When the coefficient is small, the economic characteristics will be closer to the proof of storage resources. At this time, the security of the network is mainly guaranteed by storage resources, and the benefit distribution will flow to the resource nodes; but when R is big enough, the economic characteristics tend to be PoS. The security of the network is mainly guaranteed by staking FBZZ token in the network, and a large proportion of the benefits will be allocated to accounts that hold FBZZ.

.6 Token Allocation

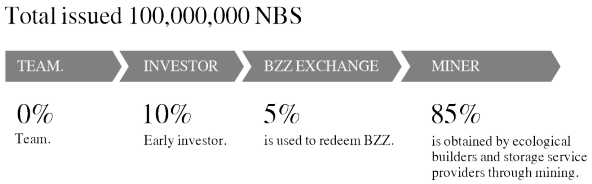

Figure 2: *Token Model for Different Purposes*

IV. Conclusion

Incentive mechanism plays a really important role in blockchain projects. A healthy incentive mechanism can attract miners to join and maintain the network (we can do this by setting an appropriate ratio for miners when allocating tokens). On the other hand, an appropriate proportion of tokens reserved by the team allows the founding team to obtain the return they deserves while maintaining sufficient motivation to continually running the project. However, the official Swarm team performed completely opposite on these two points. So we can only go to self-help, let's join New Bee Swarm right now.

References

[Swarm, 2021] Swarm Team. (2021). Swarm: storage and communication infrastructure for a self-sovereign digital society. *v1.0*, [Online]. Available: https://www.ethswarm.org/swarm-whitepaper.pdf

[Tron, 2020] Viktor Tron. (2020). The Book Of Swarm: storage and communication infrastructure for self-sovereign digital society back-end stack for the decentralised web. *v1.0*, [Online]. Available: https://www.ethswarm.org/The-Book-of-Swarm.pdf