BlockModel NO.202306150001

Tokenomics Security Audit Report

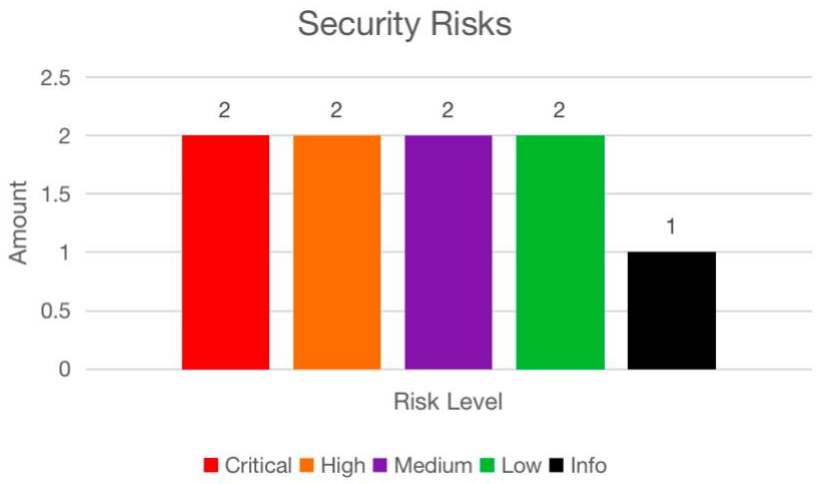
15th, June, 2023

BlockModel

Contents

Summary

After auditing, the project was found to have 2 Critical + 2 High + 2 Medium + 2 Low + 1 Info risks. As of the completion of the audit, all risk items have been fixed or properly handled. Specific audit details will be presented in the later text. Users should pay attention to the following aspects when interacting with this project:



- There is no clear and direct incentive for loan demand, which is the most important source of income of this product. It is recommended to directly give the part of token allocation to loan farming, or the reward of staking is boosted acoording to the loan amount and time.
- The design of TGE is easy for insiders to pump-and-dump, which harms the interests of the project and the community. It's recommended to re-design the TGE schedule.
- There is immediate pressure to sell rewards generated within the economy. It is recommended to set a waiting period for reward

withdrawal.

- No explicit APY design which can fall into the Ponzi trap. It's recommended to design a linear / non-linear APY.
- In the medium and long term, even if token incentive is adopted, the product's loan demand drive is still uncontrollable. It's recommended that incentive should be designed based on loan amount and time.
- In the medium and long term, the demand for the token is insufficient. It's recommended to supplement governance feature, or a design that enjoys a discount when paying interest with the token.
- A fixed x% yield for buybacks may not be enough to suppress selling pressure. It's recommended that this percentage can be adjusted by governance.
- The governance feature is not clearly stated. It's recommended to supplement governance design.
- The introduction of tokens is just icing on the cake, not a necessary part of the product itself.

Overview

Project Overview

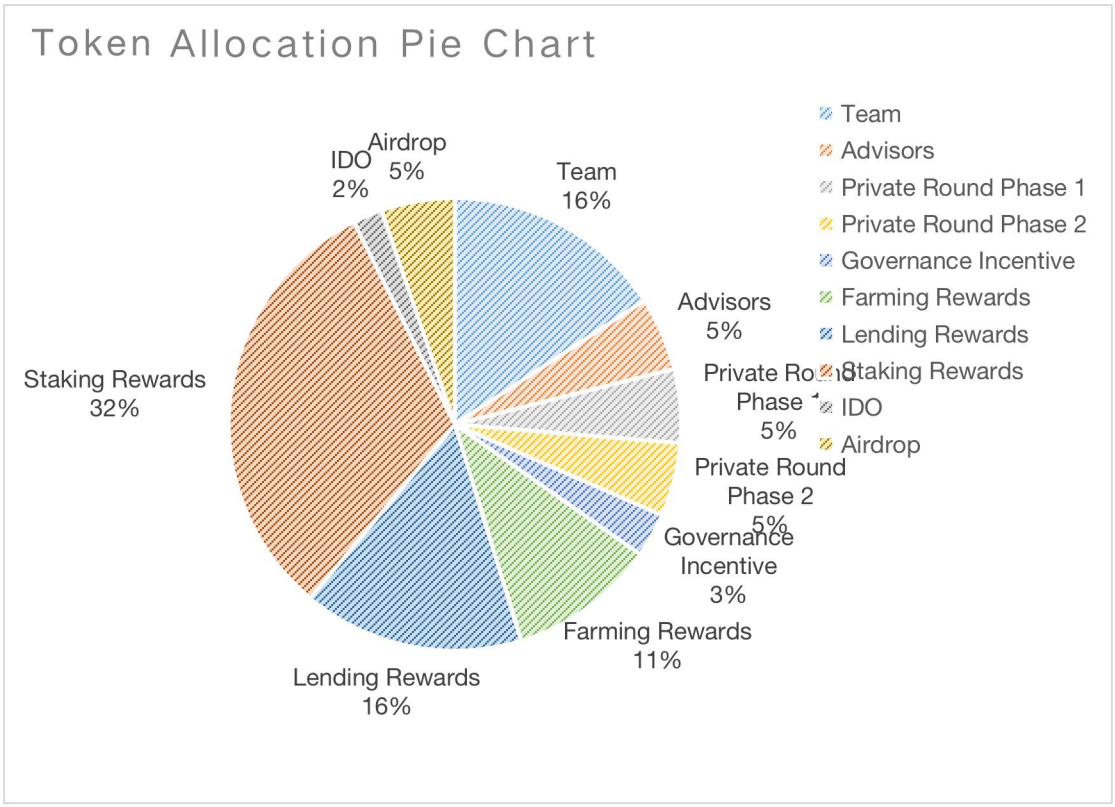
The project is a lending protocol on Ethereum. It provides users with lending, wealth management and asset custody services.

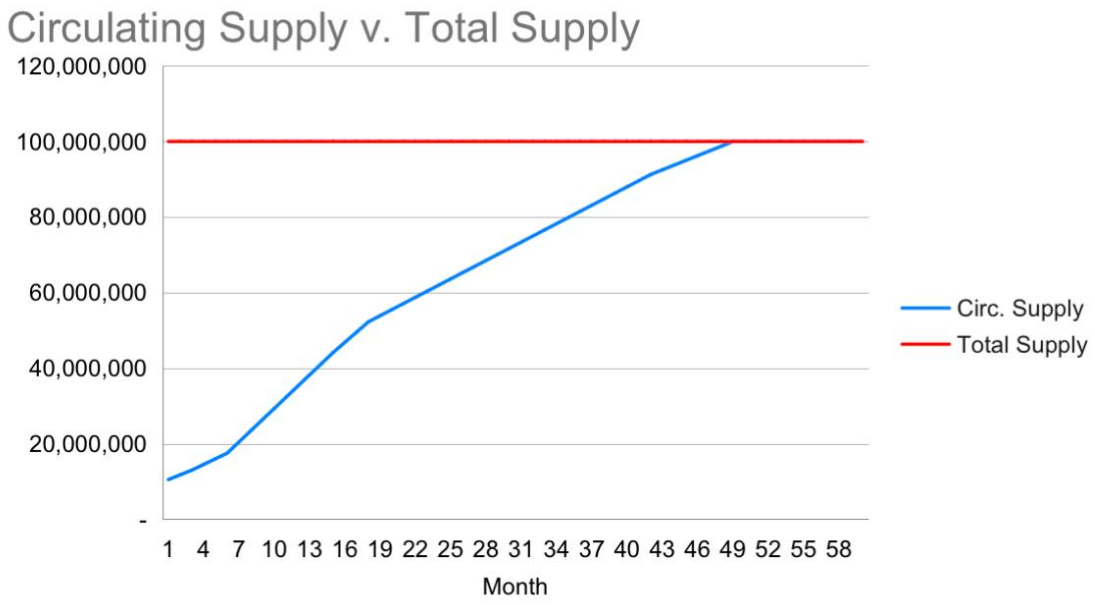
Project website:

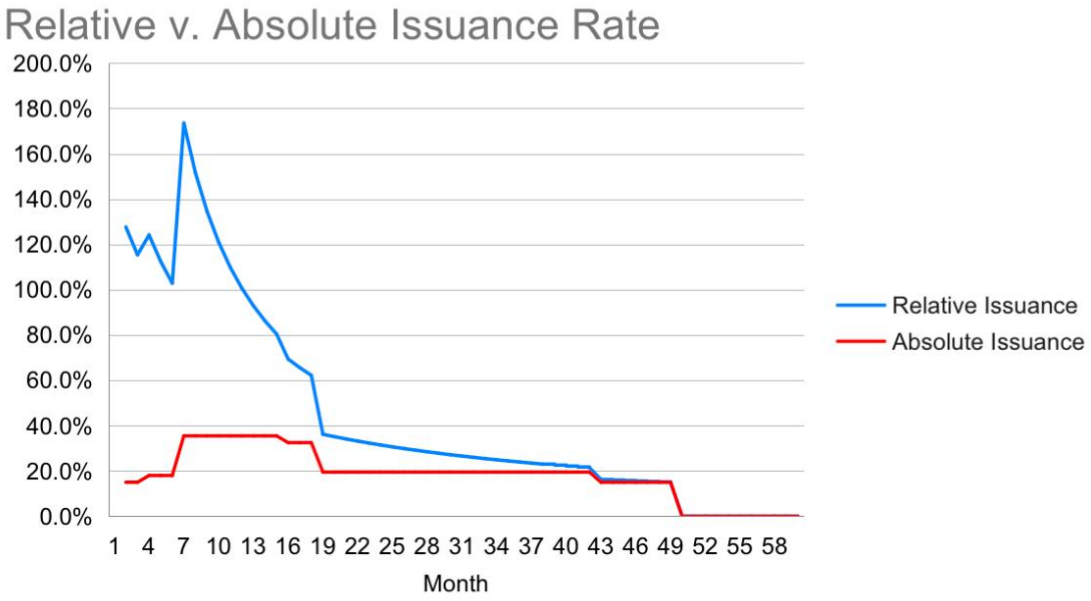
The project has only one token $ABC, with utility function and security function. $ABC allocation and distribution is shown as follow:

$ABC Token Allocation		
Target	**Quota**	**Percentage**
Team	150000000	15.00%
Advisors	50000000	5.00%
Private Round Phase 1	50000000	5.00%
Private Round Phase 2	50000000	5.00%
Governance Incentive	30000000	3.00%
Farming Rewards	150000000	15.00%
Lending Rewards	150000000	15.00%
Staking Rewards	300000000	30.00%
IDO	20000000	2.00%

Airdrop	50000000	5.00%
TOTAL	**1000000000**	**100.00%**




Circulating Supply v. Total Supply
120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
-
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58
Month
Circ. Supply
Total Supply


Relative v. Absolute Issuance Rate
200.0%
180.0%
160.0%
140.0%
120.0%
100.0%
80.0%
60.0%
40.0%
20.0%
0.0%
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58
Month
Relative Issuance
Absolute Issuance

Audit Overview

1. Audit Result:

- **Not Passed**
- Overall Ranking: 25 / 50
- Track Ranking: 5 / 10

2. Audit Methods:

- Structure Analysis
- Simulation Test

Findings

Index	Description	Level	Result
1	Incentive design flaw	Critical	Acknowledged
2	TGE design flaw	Critical	Acknowledged
3	Potential sell pressure	High	Acknowledged
4	Potential Ponzi-trap	High	Acknowledged
5	Uncontrollable demand for product	Medium	Acknowledged
6	Lack of demand for token	Medium	Acknowledged
7	Unproven price support	Low	Acknowledged
8	Unknown governance	Low	Acknowledged
9	Necessity of token	Info	Acknowledged

1. Incentive design flaw

- **Level:** Critical
- **Type:** Mechanism Security
- **Target:** $ABC
- **Description:**

For this project, the profit mainly comes from lending, but the incentive for borrowing demand is not clear. It is only mentioned in the Token Staking mechanism that more favorable borrowing discounts will be given according to the membership level. For users participating in staking, the purpose is likely to be to obtain staking rewards, rather than to carry out actual borrowing operations. Thus, the conversion rate of this process is not clear.

- **Recommendations:**

It is recommended that a certain proportion of Token can be directly allocated to Borrow Farming, similar to Lending Farming that has been considered in the allocation design. Or, another practice can be considered is that Staking Reward can be calculated based on the borrowing behavior (amount & time).

- **Status:** Acknowledged

2. TGE design flaw

- **Level:** Critical
- **Type:** Distribution Security
- **Target:** $ABC
- **Description:**

At TGE, the released amount of tokens is as follows: x% - IDO, ~y% - Investor, z% - Team, v% - Market. IDO, Investor and Team are insiders, while Market is outsider. Therefore, it can be seen that at TGE, insiders have a large control ratio, which is highly-possible to pump-and-dump.

- **Recommendations:**

It is recommended to redesign the distribution of Token TGE. For example, consider reducing the distribution of Investors, or set a cliff for TGE.

- **Status:** Acknowledged

3. Potential sell pressure

- **Level:** High
- **Type:** Sell-pressure
- **Target:** $ABC
- **Description:**

Since the reward release mechanism (Staking Reward / Lending Reward / Farming Reward) is not clear, there may be immediate pressure to sell

rewards in the open market.

- **Recommendations:**

It is recommended to set a cool-down period for the reward withdrawal; or design a non-linear withdrawal.

- **Status:** Acknowledged

4. Potential Ponzi-trap

- **Level:** High
- **Type:** Business Security
- **Target:** $ABC
- **Description:**

Since the project's reward release mechanism is not clear, the early reward APY may be too high, which will attract users to use leverage to engage in speculation, and in the end it will actually damage the interests of later users.

- **Recommendations:**

It is recommended to supplement the design of APY, which can consider about linear / non-linear / fixed / increasing / decreasing.

- **Status:** Acknowledged

5. Uncontrollable demand for product

- **Level:** Medium

- **Type:** Business Security
- **Target:** $ABC
- **Description:**

The project provides lending services and relies heavily on lending for profitability. Both loan demand and token prices are greatly affected by the market environment. In the medium and long term, the survival of products is strongly related to the market environment. Even if token incentive is added, it is still uncontrollable.

- **Recommendations:**

It is recommended to supplement the design of financial management mechanism, trying to fill in the business under the downturn after the deleveraging of the market.

- **Status:** Acknowledged

6. Lack demand for token

- **Level:** Medium
- **Type:** Economy Security
- **Target:** $ABC
- **Description:**

There is not enough usage demand for $ABC token. The current demand for token usage is only to be able to stake to obtain members and enjoy loan discounts.

- **Recommendations:**

It is recommended that the governance ability of the token can be supplemented; or a certain discount can be given when using the token to pay the loan interest.

- **Status:** Acknowledged

7. Unproven price support

- **Level:** Low
- **Type:** Economy Security
- **Target:** $ABC
- **Description:**

The project takes 5% of the revenue every quarter to buyback-and-burn, which can support the token price and give token holders profit expectations to stabilize the selling pressure in the secondary market. However, considering the fluctuations in the market and the unclear profit forecast of the project, it may not be effective to set a fixed 5% of revenue to buyback-and-burn.

- **Recommendations:**

It is recommended to set this parameter by community governance, rather than a fixed number. On the one hand, it can be welcomed by the community, on the other hand, it can flexibly respond to market conditions.

- **Status:** Acknowledged

8. Unknown governance

- **Level:** Low
- **Type:** Governance Security
- **Target:** $ABC
- **Description:**

It is mentioned in the white paper that $ABC token has governance ability. But it did not explain in detail, which may cause bad rumors in the community and have a negative impact on the project and token.

- **Recommendations:**

It is recommended to supplement design of governance, and make it public.

- **Status:** Acknowledged

9. Necessity of token

- **Level:** Info
- **Type:** Business Security
- **Target:** $ABC
- **Description:**

The issuance of token is an act of icing on the cake, not a necessary component for business and product.

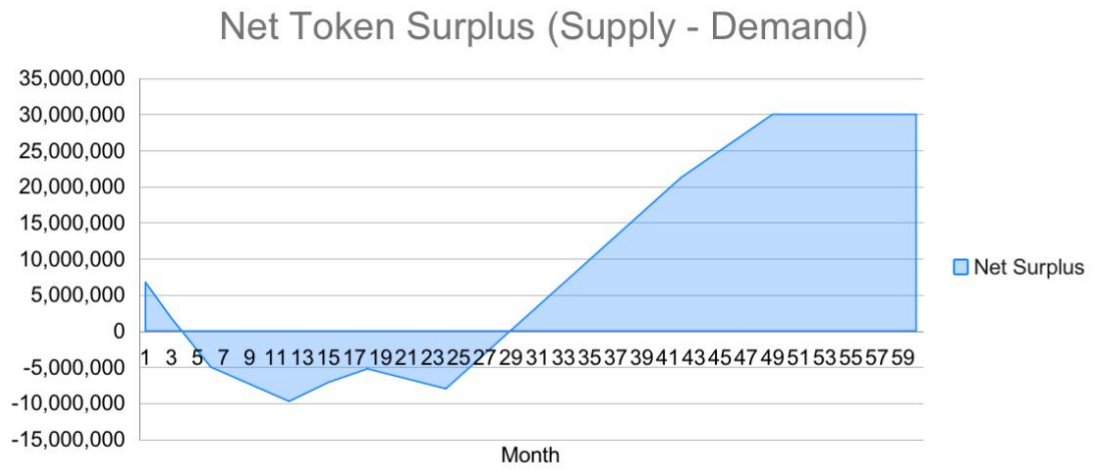
- **Recommendations:**

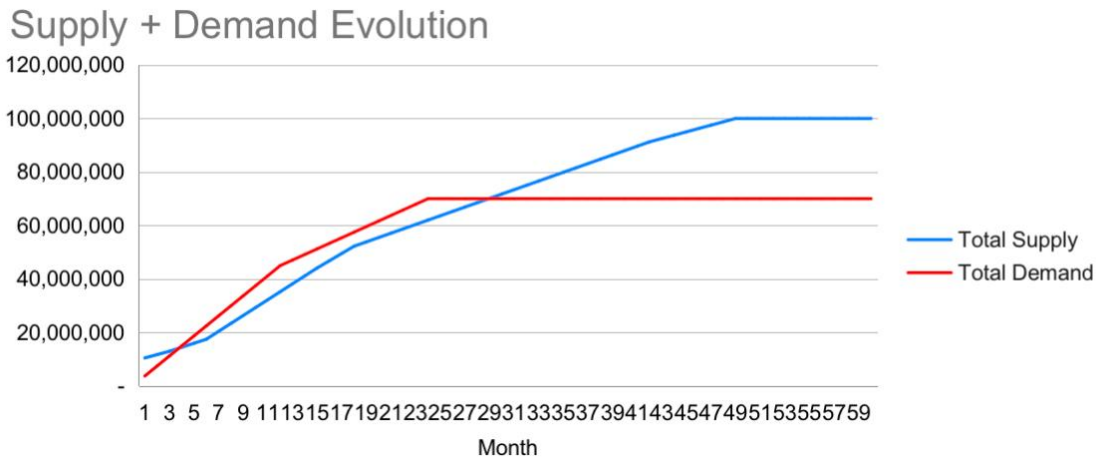
It is recommended that team can consider delaying the schedule of the token listing and verify the product-market-fit first; or design the project token strongly integrated with the lending business. For example: what can be done with the help of native token in decentralized lending service?

- **Status:** Acknowledged

Appendix

Simulation Test





In one of our simulation scenarios, the supply-demand relation of token $ABC is dynamically balanced in the first 30 months. Since then, the demand has been uncertain and supply has remained strong. This could lead to a resonable price drop. It's recommended to keep watching on-chain data to strengthen long-term demand in the future.

Security Assessment Metrics in Tokenomics

Metrics

Term \ Impact	Severe	High	Medium	Low
Short	Critical	High	Medium	Low
Mid	High	Medium	Low	Low
Long	Medium	Low	Low	Info
Very Long	Low	Low	Info	Info

Degree of Term

- **Short-Term**

  0 - 6 months;
- **Mid-Term**

  6 - 24 months;
- **Long-Term**

  24 - 60 months;
- **Very Long Term**

  60 months + ;

Degree of Impact

- **Severe**

Severe impact generally refers to the vulnerability that can have a serious impact on the business & project health, supply-demand stability, token price, commuity interest, as well as other severe harm. Severe impact may cause project to fail.

- **High**

High impact generally refers to the vulnerability that can have a relatively serious impact on the business & project health, supply-demand stability, token price and commuity interest. High impact may cause project to suffer from volatility and

potential death.

- **Medium**

Medium impact generally refers to the vulnerability that can have a relatively minor impact on the business & project health, supply-demand stability, token price and commuity interest. Medium impact may cause project to endure uncertainty and adjustments.

- **Low**

Low impact generally refers to the vulnerability that can have a minor impact on the business & project health, supply-demand stability, token price and commuity interest. Low impact can be defused with low cost.

Audit Categories

No.	Categories	Subitems
1	Business Security	Business & Token relation
		Ponzi-element
2	Economy Security	Value in & out
		Supply & Demand
		Selling pressure
		Token engagement
3	Mechanism Security	Additional value
		Network effect & Scale effect
		Reasonable Incentive & Speculative
		Participation Activity
4	Governance Security	Attack pattern
		User engagement
5	Allocation & Distribution	Pump-and-dump
		Reasonable allocation
		Reasonable distribution schedule
6	Simulation	Stability
		Robustness
		Feedback loop detection

Disclaimer

The Audit Report issued by BlockModel is related to the services agreed in the relevant service agreement. The Project Party or the Served Party (hereinafter referred to as the "Served Party") can only be used within the conditions and scope agreed in the service agreement. Other third parties shall not transmit, disclose, quote, rely on or tamper with the Audit Report issued for any purpose.

The Audit Report issued by BlockModel is made solely for the Tokenomics, and any description, expression or wording contained therein shall not be interpreted as affirmation or confirmation of the project, nor shall any warranty or guarantee be given as to the absolute flawlessness of the tokenomics analyzed, the team, the business model or legal compliance.

The Audit Report issued by BlockModel is only based on the Tokenomics model provided by the Served Party and the technology currently available to BlockModel. However, due to the technical limitations of any organization, and in the event that the model provided by the Served Party is missing information, tampered with, deleted, hidden or subsequently altered, the audit report may still fail to fully enumerate all the risks.

The Audit Report issued by BlockModel in no way provides investment advice on any project, nor should it be utilized as investment suggestions of any type. This report represents an extensive evaluation process designed to help our customers improve tokenomics model quality while mitigating the high risks in business & product.

About BlockModel

BlockModel is an open protocol for Tokenomics design & audit. We provide professional consulting service, and we are the first one focusing on Tokenomics general toolset development in the world. The core team have Profs, Postdocs, PhDs and Masters in Computer Sceince, Economy, and related backgrounds. Our Tokenomics Committee consist of experts focusing on various tracks in Web3, like DAO, GameFi, DeFi and Infra. So far, we have won prizes in global hackathons, such as BeWater Web3 Innovative Campaign and Wanxiang Blockchain Hackathon. Also, we are awarded with grants from Web3 top institutions, for example, Protocol Labs. We are selected into top accelerators / incubators, such as ThreeDAO BuilderCamp and BNB Chain Zero2Hero Incubator.

BlockModel

Official Website: http://block-model.com
Twitter: @Model_Labs