Farmland Protocol

Whitepaper

v0.2

By Farmland Core

Contents

I. Farmland Introduction

Abstract

Farmland is a decentralized cross-chain platform for DeFi farming and profits distribution.

Applying innovative blockchain interoperability, smart aggregation, distribution technology and DAO governance, Farmland has the following core advantages:

1. Cross-chain assets utilization: Unlike the current DeFi ecosystem that mainly uses the ETH network, Farmland can help users who hold assets on different public chains to participate in DeFi activities such as farming, especially for BTC holders who want to get involved in farming on ETH.
2. 0 Gas fee: Saving users' hundreds of dollars in farming, harvesting and withdrawing fees, which solves the primary pain point of current farming users.
3. True decentralization: In terms of aggregation, Farmland is different from other centralized aggregators. This protocol is completely decentralized to achieve aggregation, farming and revenue distribution functions. And for the cross-chain operations, Farmland does not rely on centralized custodians (Note 1)
4. High security: In addition to fully decentralization and mitigating the risk of capital pool loss, Farmland Protocol also categories farming pool tranches with different risk levels, and achieves the most secure farming environment by overlaying insurance protocol layers.
5. Open integration: In addition to the cross-chain protocol provided by Farmland itself, users can also integrate different cross-chain protocols through Farmland.

Goals

The current DeFi products have shown great potential value to experienced players. Each problem solved by DeFi products, such as disintermediation, trustless institutions, etc., has made significant improvement in the efficiency of the financial system. We have seen the

decentralized oracle, lending, payment, transaction and other DeFi components become increasingly complete, and the future blueprint of DeFi is faintly visible.

However, currently there are still many unresolved problems. Poor user experience, high capital requirements due to high rates, fund safety issues due to code vulnerabilities and backdoors, and other financial security issues have restricted users from using DeFi products. In addition, each public chain is like an isolated island of information. It is difficult for assets on different chains to flow across "boundaries", and it is therefore difficult for the communities of various public chains to unite. These are the problems that DeFi must solve while on the way to replace part of or even the entire traditional finance sector.

In terms of cross-chain solutions for DeFi products available on the market, we see that almost all products are implemented on the Ethereum network, whether it is in lending, exchange or derivatives. These products ignore the huge Bitcoin community and other public chain communities. The total number of these communities may greatly exceed the number of Ethereum.

In order to solve these existing problems, Farmland first integrates with existing cross-chain solutions, and then develops more advanced cross-chain solutions. Meanwhile, as Farmland focuses on DeFi farming, through innovative aggregation and distribution methods, users can enjoy a very low or even zero handling fee, which reduces the threshold of DeFi farming. Users do not need to prepare thousands of USD stable coins in order to get meaningful profits.

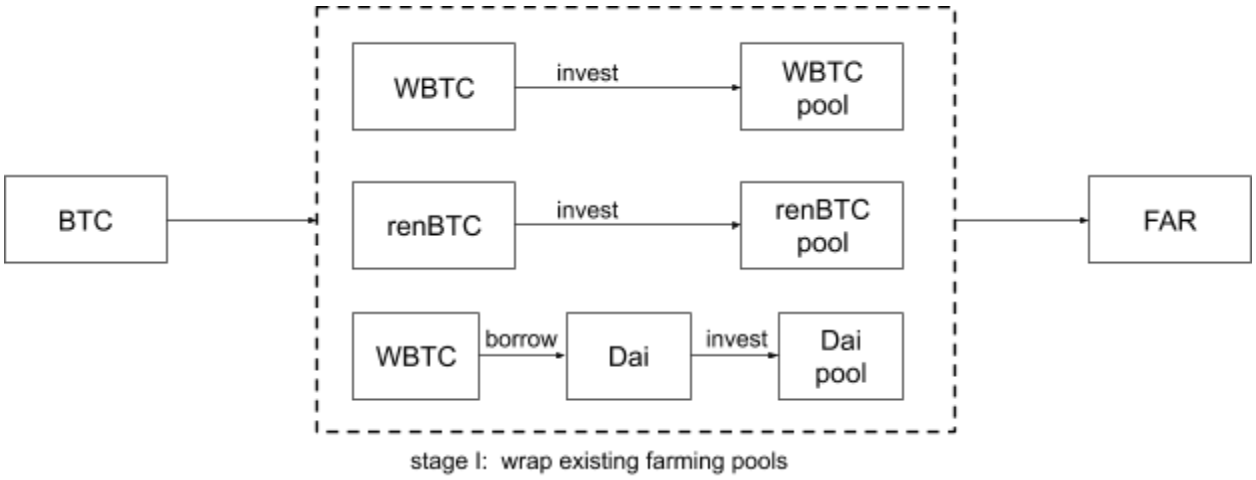
Procedures

The ultimate goal of Farmland is to integrate all of mainstream public chains and to become the entrance for cross-chain DeFi users. At the first stage, wel choose Bitcoin to integrate with Ethereum DeFi farming, as the market value of Bitcoin exceeds the total amount of other public chains and the number of token holders is also huge.

We implement the Bitcoin-Ethereum cross-chain aggregated farming tools, which will be achieved in three stages, without obvious changes in perception at the user level:

Stage 1: Realize the cross-chain aggregation farming stage

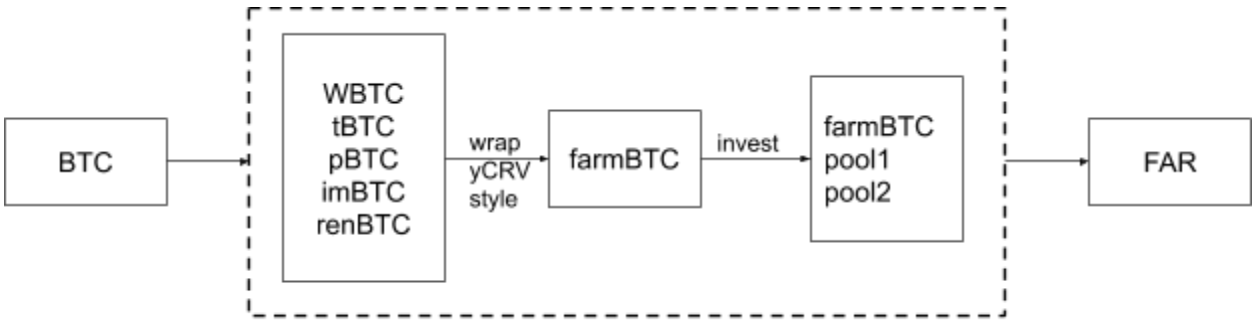
The front-end of Farmland integrates existing cross-chain technologies such as WBTC and renVM, while the Farmland back-end system aims to achieve aggregate farming and profit distribution functions. The user transfers BTC directly to Farmland and binds the Ethereum address for receiving profit. After the system obtains the token from farming, it will automatically distribute the profit to the user's ETH address. At the implementation level, Farmland will convert users' BTC into WBTC and renBTC on Ethereum through WBTC and renVM network, and then convert them into Dai for enhanced farming through tools such as makerDAO.



stage I: wrap existing farming pools

Stage 2: Transitional stage

We will introduce the concept of farmBTC, the purpose of this phase is to pave the way for the third phase. farmBTC is a synthetic asset, mainly consisting of WBTC, imBTC, renBTC, etc. which is similar to yCRV, consisting of USDC, Dai, USDT, etc.

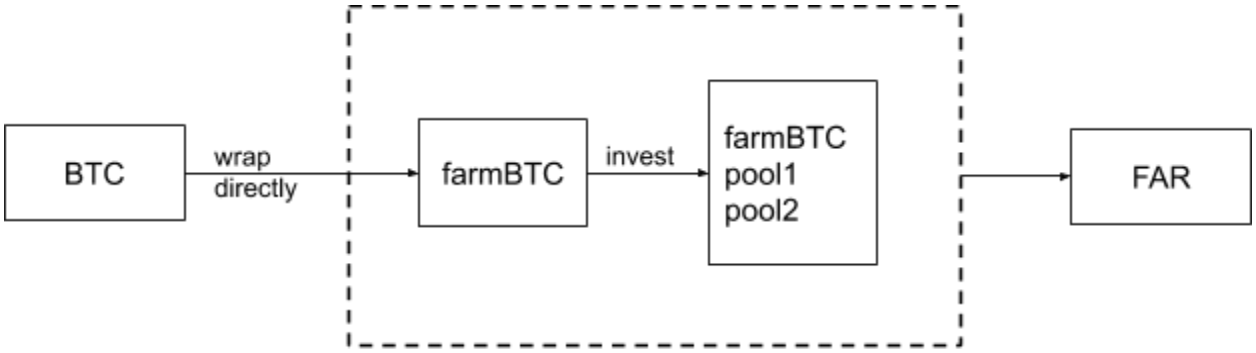


stage II: yCRV-style farmBTC

Stage 3: FarmBTC stage

At this stage, the BTC sent by the user will be directly converted to farmBTC. The conversion mechanism and its advantages will be explained in detail in the next part.

The user's FarmBTC will be used for aggregate farming. The technical implementation of aggregate farming and how to achieve zero handling fee will be discussed in the following.



stage III: farmBTC with new cross-chain mechanism

II. System Architecture

Wrapped BTC

The way of wrapping or mapping BTC on other chains (e.g. ETH), or in general, blockchain interoperability, has been a hotspot for the past several in the industry. However, no projects have been proven to be perfect and do not need to evolve. Many projects focus on creating ERC-20 Bitcoins, which is a relatively less complicated sector for cross-chain operations.

Existing Projects

WBTC

WBTC cooperates with centralized custodian agencies like BitGo to issue 100% backed wrapped ERC20 Bitcoin tokens. Only authorised merchants are allowed to receive Bitcoin, and mint or burn WBTC. Sometimes merchants also require the KYC process. WBTC is widely used, though it is impossible for normal users to directly use it.

imBTC

Issued by Tokenlon and powered by imToken, imBTC is also backed by Bitcoins that are locked in a centralized cold wallet. Users could swap BTC for imBTC on imToken app.

tBTC

Currently tBTC only supports Ethereum, and requires users to deposit Bitcoin of several fixed sizes -- 0.002, 0.01, 0.1, 0.2, 0.5 and 1 BTC, which may be confusing for users. Also extreme market volatility could lead to a failure of the one-to-one peg.

pBTC

Using a secure sandbox as an intermediary, pBTC now supports several different chains including BTC, LTC and EOS. However this kind of execution environment might be vulnerable to attackers.

About farmBTC

At the time our liquidity farming platform is launched, farmBTC instead of all the above wrapped BTCs will be used as the main intermediary trading currency. The following plan will be applied:

At first, we will select 1-2 existing tools to swap our users' BTC to ERC20 BTC, for exchange WBTC and renbTC. We will add another wrap on these wrapped BTCs to issue farmBTC. This procedure will be entirely done on ETH blockchain, which is relatively intuitive. These wrapped-twice BTCs will be used primarily for our liquidity farming.

Later on, we will introduce a yCRV-style mixed way of minting farmBTC, like the figure shown below. At this stage, farmBTC will be based on a mixed basket of wrapped BTCs and therefore significantly reduce the risk of fatal failure of one underlying asset.

Goals

- FarmBTC will be fully decentralized.
- FarmBTC will be 100% backed, without creating new Bitcoin supplies.
- FarmBTC will be minted and redeemed instantly and seamlessly. Users will be able to swap whatever amount at whatever time.

Crows

Crows (from scarecrows, a special term to call participating nodes that ensure the safety of farmBTC) will play a vital role in farmBTC's governance. We design a special mechanism for crows to deposit various assets as a proof and secure method of integrity. This differentiate us from current projects as most of them have only one kind of assets as deposits.

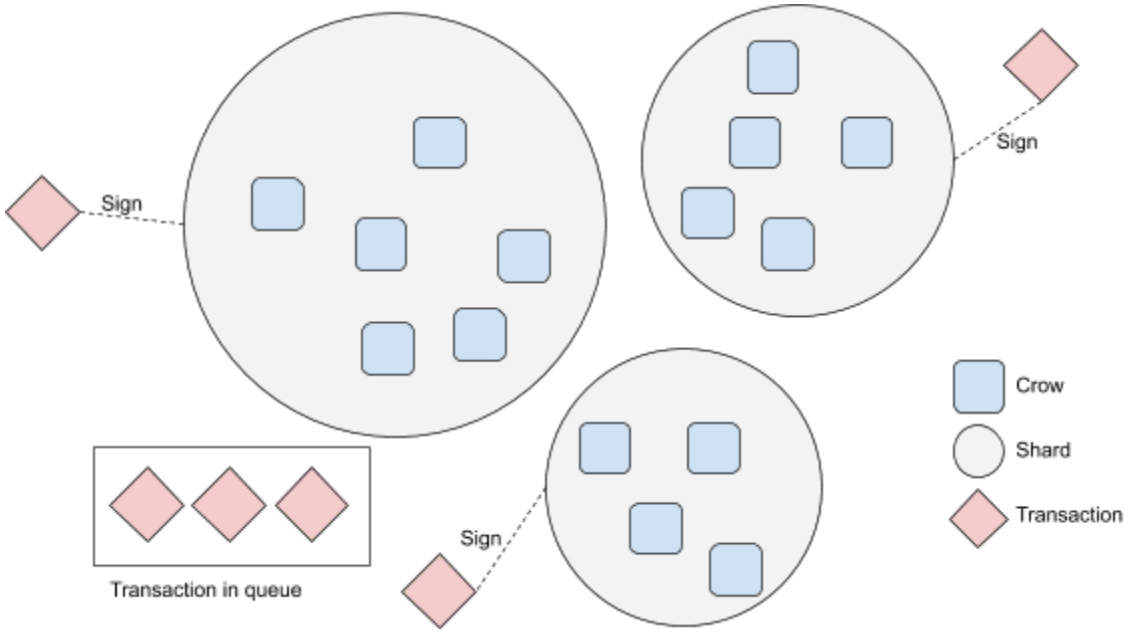
We design a good rewarding structure for all the participating crows and extra rewards for those with a longer history of integrity. We also consider increasing the weight of good crows in the entire governance system. The rewards as incentives play a significant role in the ecosystem, as a worse-than-expected reward will largely increase the chance of crows acting maliciously.

Each node should commit good behavior and they have good incentives to keep so, for dishonesty will not bring them any profits but big loss for future incomes.

We apply a loose assumption of good crows. Even multiple crows are trying maliciously to fraud the system, their chance of winning will be negligible.

Shards

Shards are introduced to our system to further mitigate the risk of crows with bad behavior. crows are randomly grouped several times at some random time every day, as shown below.

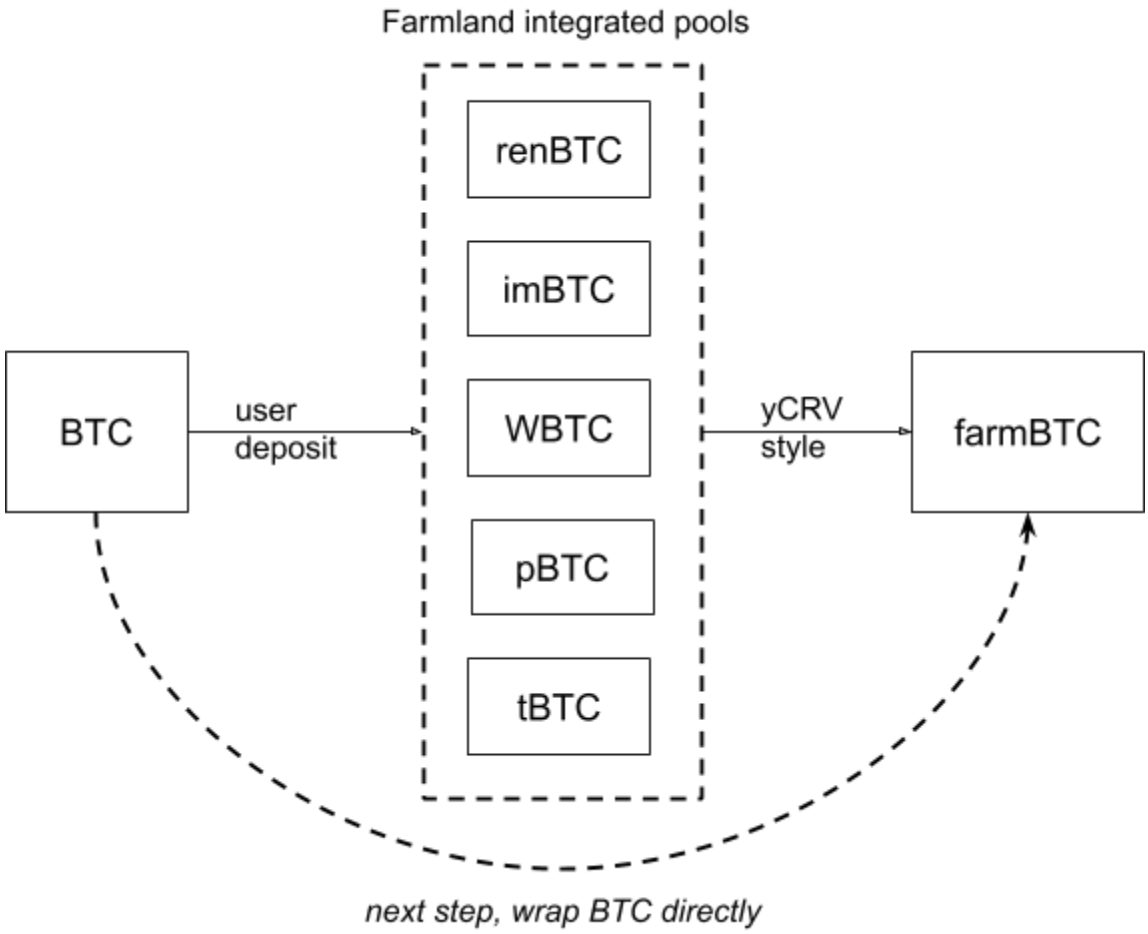


These help farmBTC to resist attacks made by both rational and irrational adversaries. B Regardless, farmBTC is always able to restore its one-to-one peg in the unlikely event that an attack succeeds.

Failure Handling

When some grouped crows fail to sign a transaction and maliciously sign a false transaction, we call it a “Handling Failure”. This typically represents a liveness failure from some

participant. As such, their bonds are liquidated to protect the one-to-one peg, and any remainder is returned to them once the liquidation initiator is rewarded.



Finally we will move farmBTC to a wrapped mechanism designed by ourselves, learning from all the pros and cons of existing projects, to create the most reliable cross-chain wrapping protocol, while remaining permissionless, decentralized and trustless.

One Hub for All

The Primary Pain Point - Fees

Currently, DeFi farming users face extremely high fees. The process of depositing, harvesting and withdrawing can cost hundreds of dollars. Let's analyze the cost structure, starting with ETH and AMPL in the wallet to participating in AMPL_ETH_UNI_LP pool farming in YAM as an example:

1. If you have never used Uniswap, you need to authorize both ETH and AMPL assets separately, and the handling fee each is about 0.01ETH;

2. You need to wrap ETH to get WETH on uniswap, of which this procedure costs about 0.08ETH;

3. On Uniswap's AMPL-ETH pool, click Add Liquidity button to increase liquidity, of which this procedure costs about 0.04ETH;

4. After obtaining LP tokens of the AMPL-ETH trading pair, you can deposit them in the AMPL_ETH_UNI_LP farming pool of YAM. This step costs about 0.03 ETH;

5. If you want to withdraw profits after some time of farming, each withdrawal cost a fee of about 0.04 ETH.

Assuming that one withdrawal is completed after revenue is generated, this process costs a total of about 0.2 ETH, which is equivalent to 80 USD.

We can calculate the capital threshold required for profitable farming, based on the rate of return of some farming projects and the fees introduced above. In the short term, the deposit and withdrawal fees have a significant impact. Here we do not consider them, and assume that the farmer adopts a long-term farming strategy and withdraws the income daily (that is, farming, harvesting and selling), then the one-year fee is:

$$0.04ETH \times 365 \times 410USD/ETH = 5986USD$$

means that in the case of pools with 100% annualized income, users need to invest more than $5986USD \times 2 = 11972USD$ to make their own income greater than the processing fees paid. Of course, considering the variability of the actual situation, such as the high annual interest rate in the first few days, and also that users may not farm and sell every day, the actual meaningful capital investment is different, but it should be at least several thousand dollars, or even higher. For users who invest tens of thousands of dollars, though they are making profits, the actual rate of return will also be greatly reduced because of the handling fee.

At present, some institutions have proposed centralized aggregation tools to help multiple users share the high farming fees. However, for users, these products have three problems:

1. There are always risks of human integrity for centralized fund pools;

2. The income is not transparent. The return rate provided by many products to users is far lower than the actual return. These institutions use information asymmetry to occupy a large part of "risk-free returns" which belongs to users;

3. There are hidden terms that if loopholes occur and farmers' funds are lost, the organization will not compensate users.

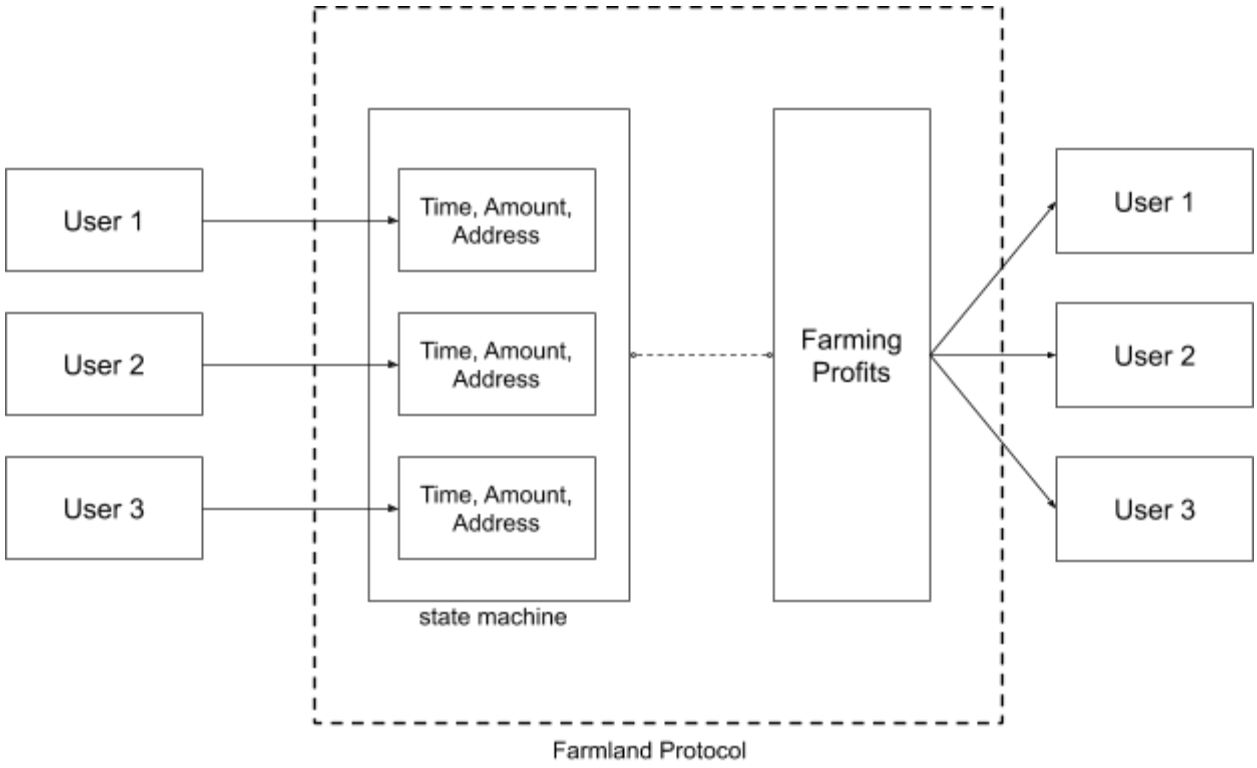
Centralized aggregation solutions cannot fully avoid the above three problems.

Our Approach

Aggregation

Farmland Protocol uses smart contracts to achieve the automatic aggregation of funds, farming and automatic revenue distribution. The process is completely on the chain, and the flow of funds and revenue distribution are open and transparent.

The specific implementation is as follows:

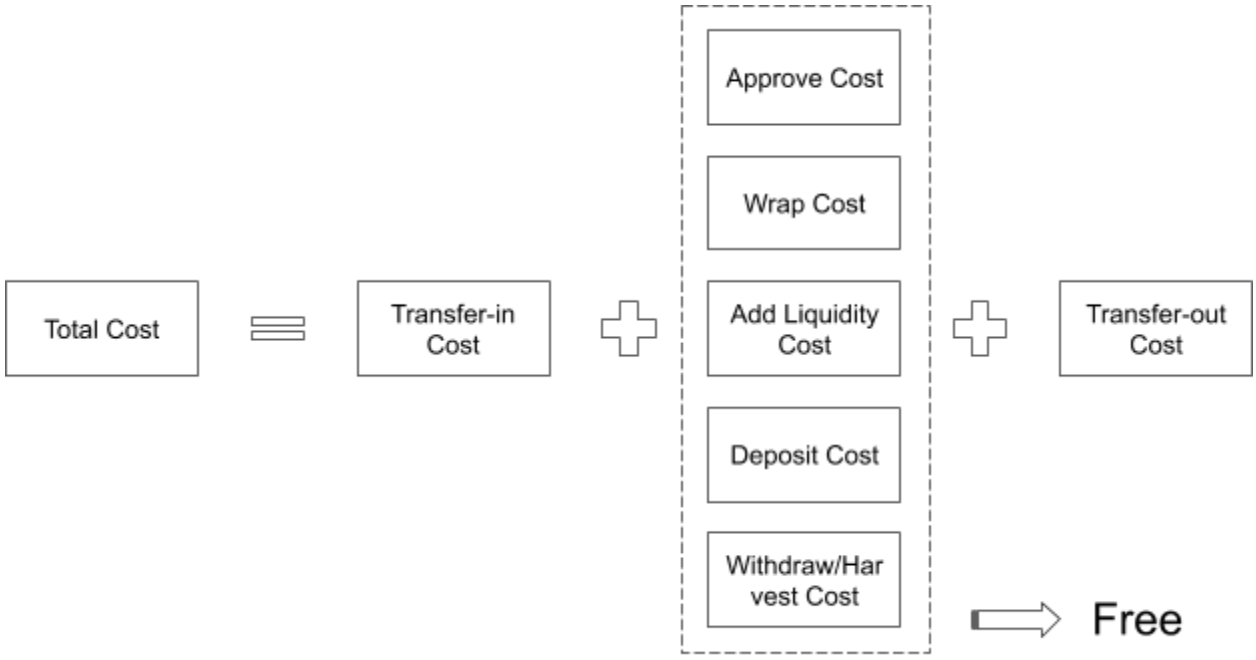


Aggregate users' funds and store the address, time, and amount of the funds sent.

Send funds periodically to farm designated pools.

Harvest and withdraw funds periodically and distribute profits to users according to their pre-settings.

With the above approach, qualified users are farming at zero cost, which is paid from the farming revenues. The details are as follows:



It can be proven that with the agreement, as long as the qualified users are greater than or equal to 2 people, significant costs can be reduced, and zero handling fees can be realized. As shown in the figure above, users only need to pay for the transfer of tokens, which is normal ETH transfer fees, without having to pay high contract fees.

Specifically, we have also reduced the number of times users interact with wallets. Let's take Curve Finance's Y pool deposit as an example. If a user holds DAI or USDc and wants to farm, the user needs to have sufficient ETH in the wallet to pay handling fees (at least 0.3 ETH). If the Y pool has never been used, they need to call the wallet about 3 times. With Farmland, we can complete the same transaction only by having about 0.05 ETH in the wallet and calling the wallet at least once.

Since we should calculate the percentage we withhold for fees, we need to know the relationship between the benefits of farming and the actual costs. Therefore we need to use an oracle to fetch the exchange rate of the revenue coin and the cost coin. Specifically, the current market farming revenue can be obtained through the oracle machine (for example, from websites such as https://yieldfarming.info), and the current farming profit can be

automatically calculated. After this, forms such as profit repurchase, transfer in and transfer out fee subsidies can be set up in the future.

Duration

In order to prevent malicious users from Sybil attacking the Farmland Protocol, we will set the user's basic funding and time requirements for farming. This value can be measured by Duration:

$$Duration = Amount \times LockTime$$

When the Duration is lower than a reasonable value, the system will refuse service or charge a fee in advance. Generally speaking, as long as the amount of user funds is greater than 1000 USD and the time exceeds 3 days, or even less on certain days when high-yield pools come out, the Duration can reach the standard.

Take a fund pool with an average annualized rate of return of 50% as an example, the expected return of $1000\ USD$ is:

$$1000USD \times 3 \times 50\% \div 365 = 4.1USD$$

If the number of users is 20, the total return in 3 days is about 80USD, which is enough to cover the fees. When there are more users, we can provide a lower Duration threshold.

Since the prices of the rewarding tokens such as CRV, BAL, YFI, etc. often fluctuate sharply, in some extreme cases, Farmland Protocol will lose money due to handling fee expenditures, causing the system to fail to operate. Here we propose two methods to avoid this problem:

- Income deduction: Farmland Protocol will collect revenues in advance, applying the data from the oracle. By using the oracle to obtain the expected income of Farmland and compare it with the Ethereum network fees:

- if If income > expenses, no additional operations are required;

- if income < expenses, users need to increase the farming share ratio or extend the farming period. This choice can be made by the user when putting funds into the contract at the beginning.

- Reserved security pool: Farmland Protocol will collect 1% of the revenue in each revenue pool as a reserved security pool to prevent the problem that the contract cannot obtain enough start-up fees under special extreme circumstances.

Addresses Linked

In order to allow more users to use our protocol conveniently, we have considered the situation where many users send their principal from centralized exchanges and wallets. In such cases, the sending address and income receiving address of these users are not the same.

We will distribute the profits in two ways. The main difference is that when the user sends their principals, it is sent from the personal wallet or from other aggregate addresses.

Users will be able to choose a mode if the principal sending address and the income receiving address are different on the Farmland front end. In this mode, Farmland will confirm the relevance of the two addresses, and send the income in advance to the income pool controlled by Farmland, and then transfer the incomes to the user's reserved income receiving address.

Insurance

As an entrance to the DeFi world, Farmland will provide more primary users with convenient and easy-to-use services. Since DeFi farming products often have a nested relationship among each other, the risk of code vulnerabilities is cumulative, this means greater risk for primary users. Many primary users do not care about the potential risk of principal loss because of huge returns.

In order to provide more users with a safer DeFi environment, Farmland Protocol introduces an insurance mechanism, which will be implemented in subsequent versions of Farmland. Since the first version of Farmland Protocol focused on decentralized aggregate farming and

revenue distribution, we will only outline the basic principles and procedures of the insurance mechanism below.

Based on several dimensions of integrated farming protocols, Farmland will classify these farming protocols with safety standards. These include: codes auditing, online time period, etc. The safety classification will be into 4 parts: very safe, relatively safe, relatively dangerous and very dangerous. For relatively dangerous and very dangerous level pools, Farmland will request users to purchase insurances.

Premium and reimbursement fund pool: Users will be able to purchase a corresponding amount of insurance based on their principal amount, and premiums will be paid in stablecoins, ETH or Farmland governance tokens. A small amount (not more than 10%) of this part of the premium may be converted into Farmland governance tokens and destroyed. The remaining amount will become the repayment fund pool.

Reimbursement and process: The upper limit of the reimbursement amount for a single contract is 15% of the total reimbursement pool, and the lower limit is the minimum of the loss of the principal amount and 5 times the premium. The determination of compensation requires community voting, and the voters are qualified participants in the compensation pool (that is, participants who have invested more than a certain amount of premiums and are not marked as bad credit).

When the amount put into the reimbursement pool by the voter who agrees to pay out exceeds 4 times the amount paid in the project, the reimbursement is approved. However, if the amount put into the compensation pool by the voter who disagrees with the compensation exceeds 3 times the compensation amount of the project, the compensation cannot be passed. All voters who participate in voting will receive certain rewards.

If the voter or the participant applying for compensation has maliciously defrauded insurance or maliciously failed to pay after later social determination, the voter’s address will be marked as bad credit, and once marked as bad credit, a small amount of premiums will be seized by the system and that address cannot vote for a period of time. It has been marked as bad credit many times, and voting rights will be terminated.

The above community autonomy process will be fully achieved on the chain.

III. Governance

After initial testing and implements, the Farmland Protocol will be launched online. After the initial centralization and selection of appropriate farming pools, Farmland's governance will completely enter the DAO stage. The agreement is subject to FAR, and any improvements will be decided by FAR holders' votes. Some of the powers that can be controlled by the governance system are listed as follows:

- Set up a new farming pool and select the appropriate farming protocol.
- Update the oracle address.
- Change the income back-end proportionally.
- Set up a new DAO community.
- Change the liquidation threshold, LTV, liquidation bonus, etc.