Farmland Protocol

Whitepaper

v0.3

By Farmland Core

Contents

I. Farmland Introduction

Abstract

Farmland is a decentralized cross-chain platform for DeFi farming and profit 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 present DeFi ecosystem that fundamentally utilizes the ETH network, Farmland is capable of assisting users who hold assets on various public chains in order to participate in DeFi activities like farming, especially for BTC holders who wish to become involved in farming on ETH.
2. 0 Gas fee: Saving users' hundreds of dollars in farming, harvesting, and withdrawing fees, resolving the main point of problem for current farming users.
3. True decentralization: In terms of aggregation, Farmland is different from other centralized aggregators. To attain aggregation, farming, and revenue distribution functions, this protocol is completely decentralized. Moreover, for the cross-chain operations, Farmland does not depend on centralized custodians (Note 1)
4. High security: In addition to complete decentralization and mitigating the risk of capital pool loss, Farmland Protocol also categories farming pool tranches with different risk levels, and attains the most secure farming environment by overlaying insurance protocol layers.
5. Open integration: Besides the cross-chain protocol provided by Farmland itself, users can also incorporate multiple cross-chain protocols through Farmland.

Goals

The existing DeFi projects have displayed excellent potential value for qualified players. Every difficulty resolved by DeFi products, like disintermediation, trustless institutions, etc., resulted in crucial developments in the financial system's effectiveness. We have witnessed the decentralized oracle, lending, payment, transaction, and other DeFi components becoming increasingly complete, and the future blueprint of DeFi is faintly noticeable. Nevertheless, presently, there exists several unresolved issues. Poor user experience, high capital requirements because of high rates, fund safety issues due to code vulnerabilities and backdoors, and other financial security issues have limited the users from using DeFi products. Besides, 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.

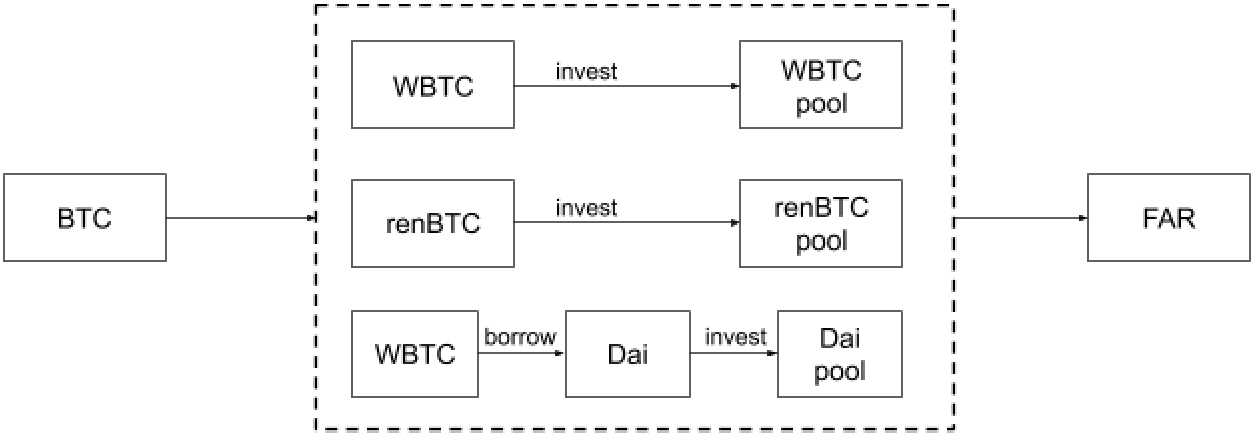
In the context of cross-chain resolutions for DeFi products accessible on the market, we notice that nearly all products are executed on the Ethereum network, whether it is in lending, exchange, or derivatives. These products overlook the enormous Bitcoin community and other public chain communities. The total amount of these communities might surpass the number of Ethereum greatly. 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 to get meaningful profits.

Procedures

The final purpose of Farmland is to combine all of the mainstream public chains and to become the entrance for cross-chain DeFi users. At the first stage, we make the choice of Bitcoin to incorporate with Ethereum DeFi farming, as the market value of Bitcoin surpasses the sum amount of other public chains and the number of token holders is also large. 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

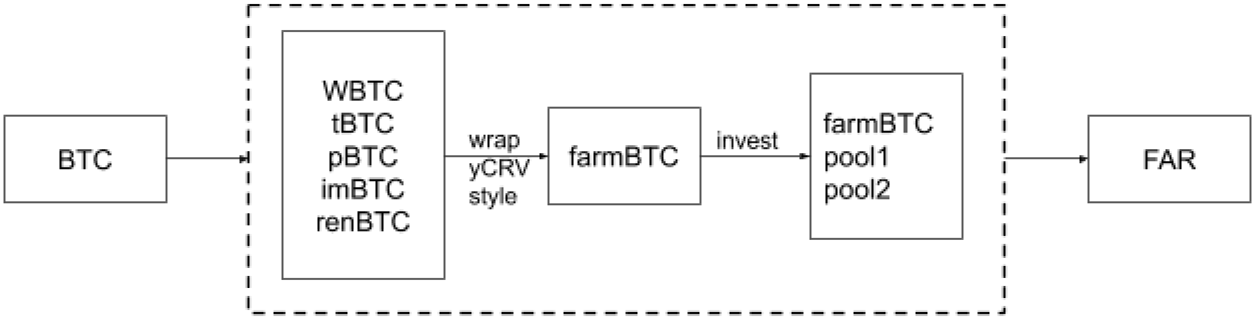
The front-end of Farmland combines the current cross-chain technologies like WBTC and renVM, while the Farmland back-end method intends to obtain aggregate farming and profit distribution functions. The user transfers BTC directly to Farmland and binds the Ethereum address for receiving profit. After the system obtains the token from farming, it will automatically distribute the profit to the user's ETH address. At the level of implementation, Farmland would convert users' BTC into WBTC and renBTC on Ethereum by using WBTC and renVM network, and afterward, transform them into Dai for improved farming by tools like 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.

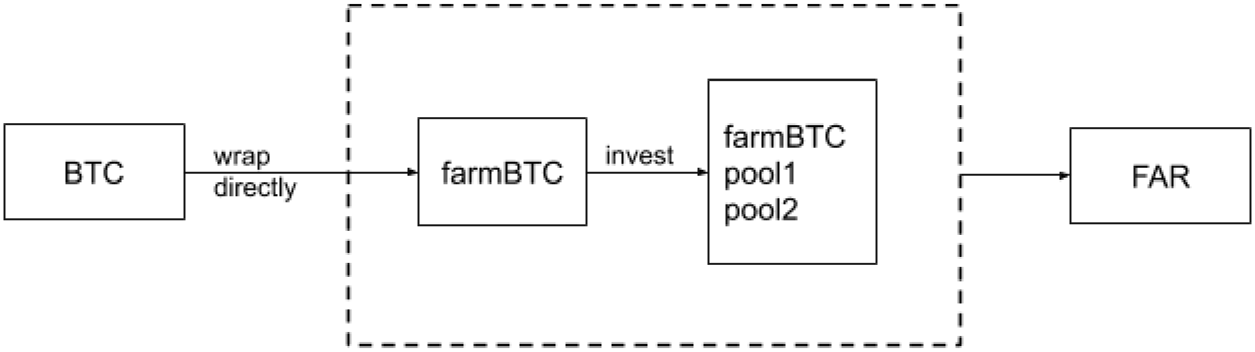


stage II: yCRV-style farmBTC

Stage 3: FarmBTC stage

At this stage, the BTC that the users sent would be directly converted to farmBTC. The conversion mechanism and its benefits will be described detailly in the next part.

The user's FarmBTC would be utilized for aggregate farming. The technical implementation of aggregate farming and how to attain zero handling fees will be explained 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 considered a hotspot for the past many years in the industry. Nevertheless, no projects were proved to be perfect and did not require evolution. Many projects focus on creating ERC-20 Bitcoins, which is a comparatively 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 authorized 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 use it directly.

imBTC

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

tBTC

In present times, tBTC only supports Ethereum and needs the users to deposit Bitcoin of various fixed sizes -- 0.002, 0.01, 0.1, 0.2, 0.5, and 1 BTC, which might be confusing for users. Moreover, extreme market volatility might result in the one-to-one peg.

pBTC

Making use of a secure sandbox as an intermediary, pBTC is currently supporting various different chains including BTC, LTC, and EOS. Nevertheless, this type of execution environment may be vulnerable to attackers.

About farmBTC

During the inauguration time of the liquidity farming platform, instead of all the above, Farmland-wrapped BTCs were to be utilized like the fundamental intermediary trading currency. The following plan would be applicable:

Firstly, 1-2 existing tools will be selected to make our users' BTC switch to ERC20 BTC, for exchange WBTC and renbTC. Then, we will make the addition of another wrap on top of these wrapped BTCs to issue farmBTC. This procedure will be entirely done on the ETH blockchain, which is relatively insightful. These wrapped-twice BTCs would be primarily utilized for our liquidity farming.

Afterward, a yCRV-style mixed way of minting farmBTC will be introduced by us, similar to the figure displayed below. At this stage, farmBTC will be based on a mixed basket of wrapped BTCs and therefore essentially lessens the risk of fatal failure attached with 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 describe participating nodes, making sure the security of farmBTC) will perform an essential part in the governance of farmBTC's. For crows, we intend to design unique mechanisms to deposit several assets as proof and secure integrity methods. This differentiates us from current projects, many of which only contain one kind of asset as deposits.

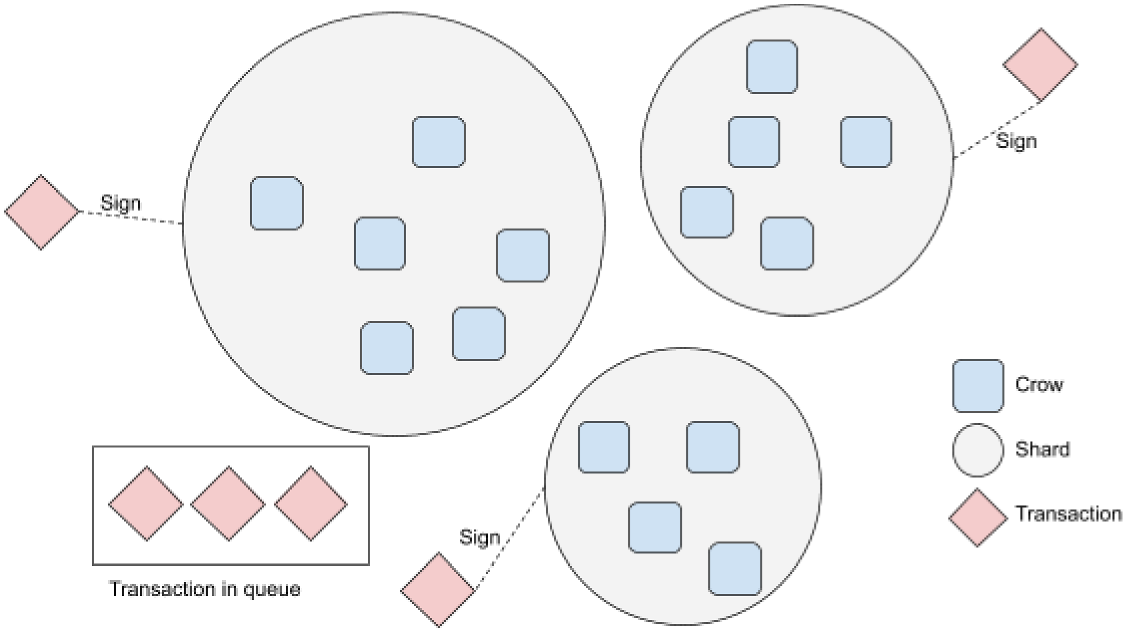
We create a good structure of rewarding for each participating crow and extra rewards for the ones with a long history of integrity. Moreover, we also consider extending the weight of good crows in the whole system of governance. In the ecosystem, the rewards as incentives have a crucial role to play, this is because a worse-than-expected reward will highly enlarge the chances of crows' acting maliciously.

Good behavior must be displayed by each node as well as they must have good incentives to keep so; for dishonesty would not be able to bring them any profits but a big loss for future incomes.

We apply a loose assumption of good crows. Even multiple crows are making efforts maliciously to scam the system, their chance of success will be negligible.

Shards

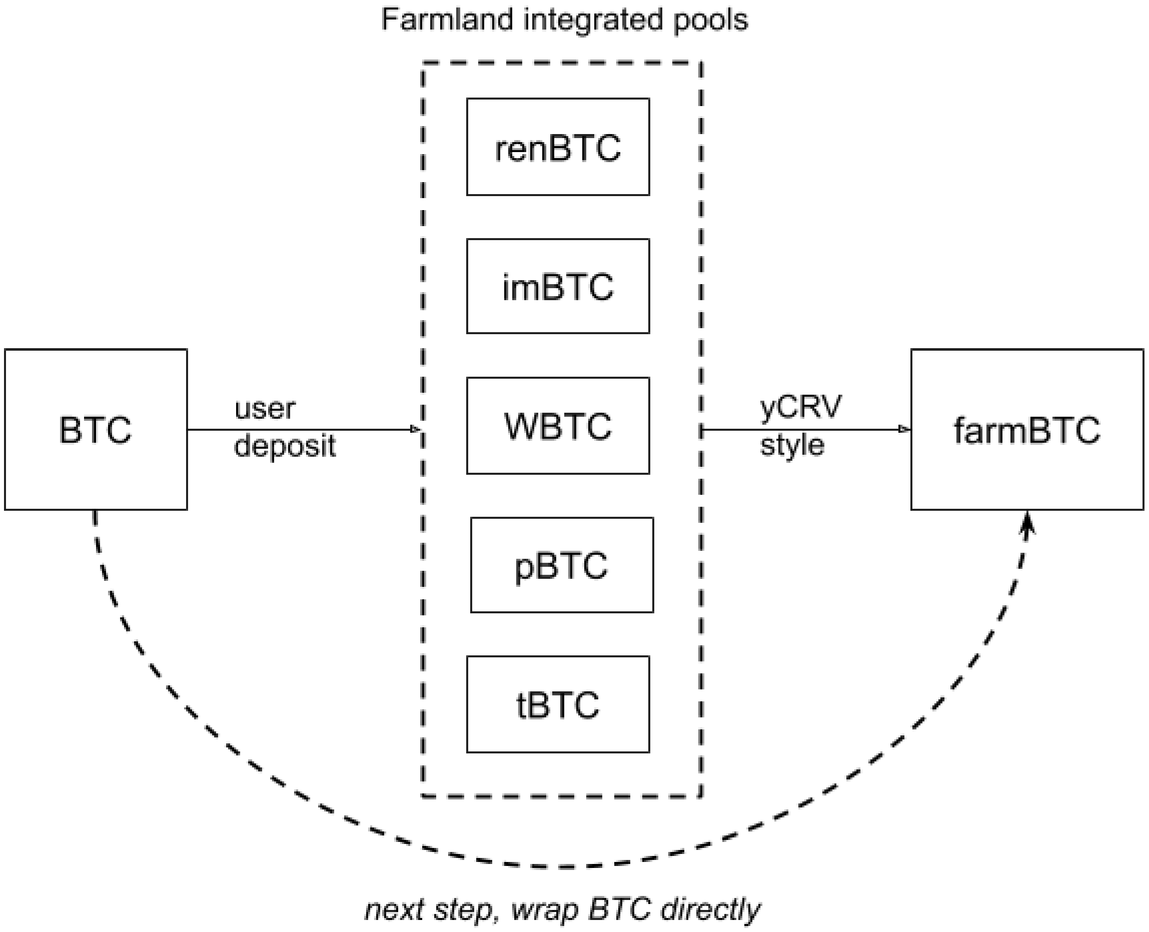
In order to further mitigate the risk attached to crows regarding bad behaviour, Shards are introduced to our system. Crows are grouped randomly various times at some random time every day, as shown below.



These help farmBTC to be able to avoid attacks made by both rational and irrational adversaries. Regardless, every time, farmBTC is able to restore its one-to-one peg in the unforeseen event that an attack succeeds.

Failure Handling

When some grouped crows can’t sign a transaction and maliciously sign a false transaction, it is called “Handling Failure”. This traditionally illustrates a liveness failure from some participants. As such, their bonds are reimbursed to preserve the one-to-one peg, and each remainder is paid to them once the liquidation initiator is rewarded.



Finally, we will move farmBTC to a wrapped mechanism designed by ourselves, learning from all the benefits and drawbacks of existing projects in order to establish the most reliable cross-chain wrapping protocol, while remaining permission less, decentralized, and trustless.

One Hub for All

The Primary Pain Point - Fees

Presently, 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 the Uniswap AMPL-ETH pool, click the Add Liquidity button to raise 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 costs a fee of about 0.04 ETH.

If we assume that one withdrawal is completed after the generation of revenue, this process costs a total of about 0.2 ETH, which makes up to almost 80 USD.

Based on some farming projects and the fees introduced above, it is possible for us to calculate the capital threshold which is needed for profitable farming. In the short-run, the deposit and withdrawal fees hold a crucial impact. Here, we do not consider them, and assume that the farmer applies 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 are required to invest more than $5986USD \times 2 = 11972USD$ in order to generate their income higher than the fees that are paid for processing. No doubt, if we take into account the variability of the actual situation, as the high annual interest rate in the first few days, and also that users might now farm and sell daily, the actual meaningful capital investment is different. However, it should be at least several thousand dollars, or even higher. For users who invest tens of thousands of dollars, even though they are generating profits, the actual rate of return will also be highly lessened due to the handling fee.

At present, some institutions have suggested centralized aggregation methods to assist multiple users sharing high farming fees. However, for users, these products contain three problems:

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

2. The income is not transparent. The return rate provided to users by several products is far lower as compared to the actual return. These institutions use information asymmetry to accommodate a large part of "risk-free returns" belonging to users;

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

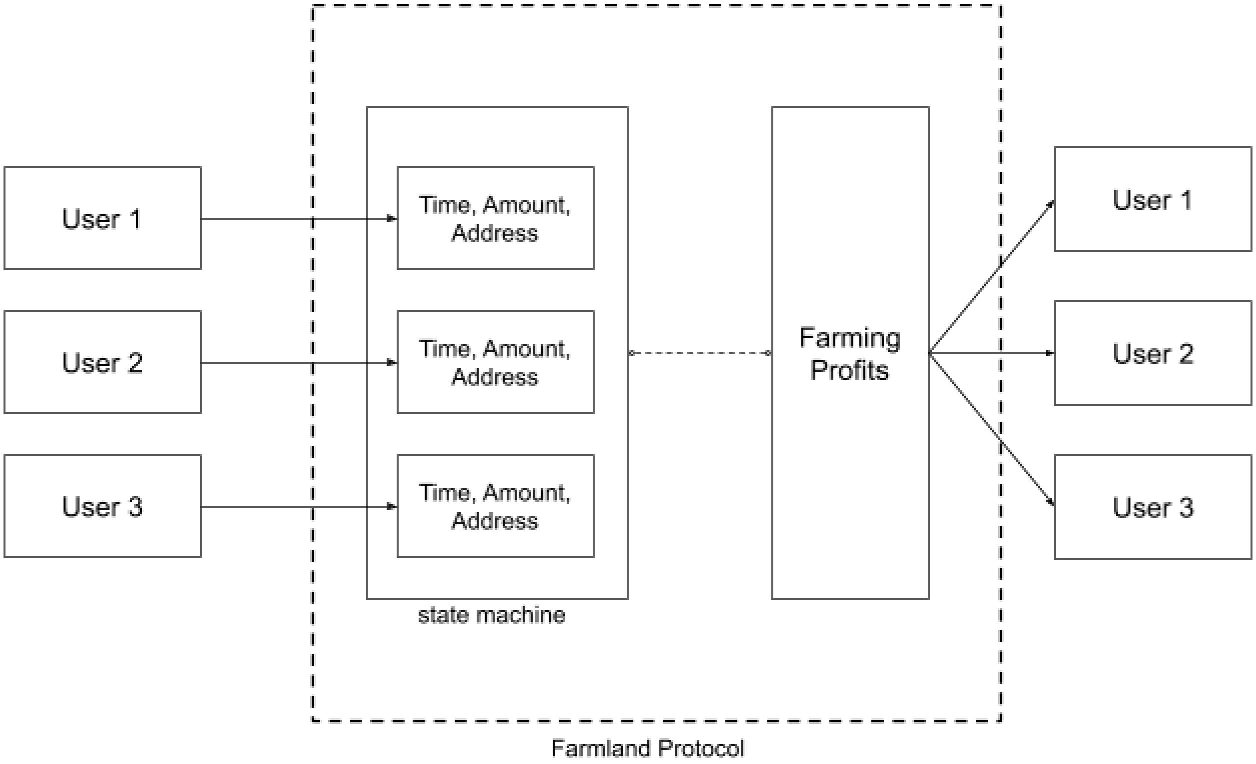
Centralized aggregation solutions are not capable of fully avoiding the above three problems.

Our Approach

Aggregation

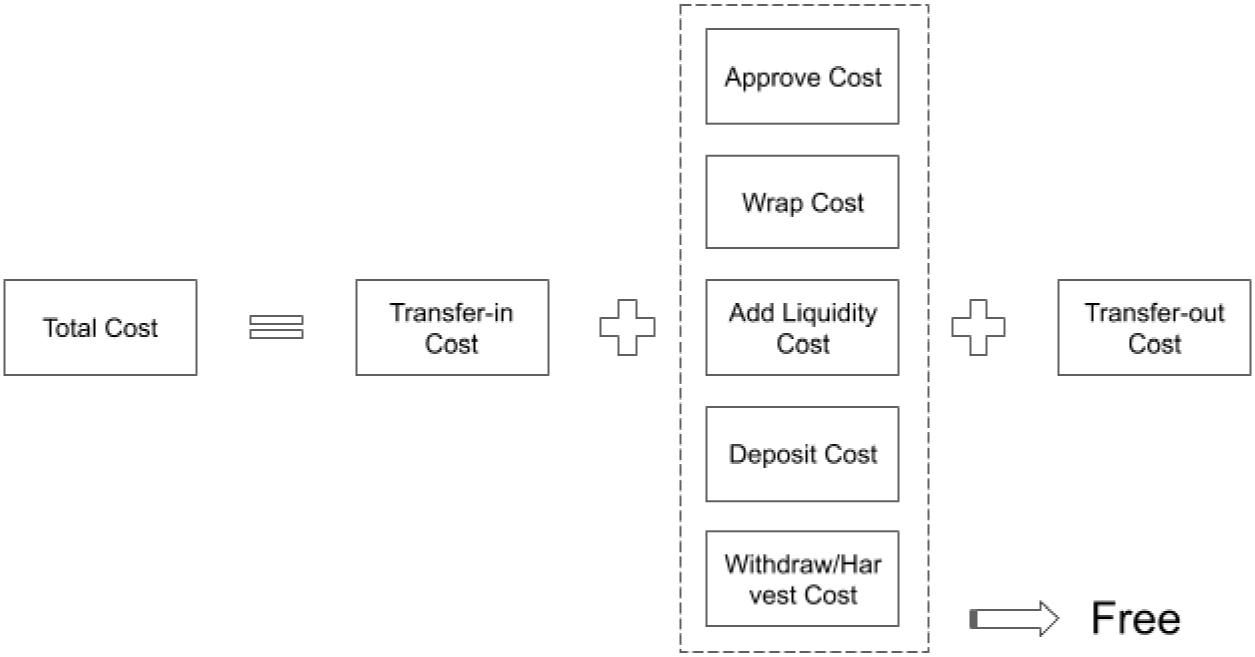
Farmland Protocol employs smart contracts to reach the funds' automatic aggregation, farming, and automatic revenue distribution. The process is completed on the chain, and the flow of funds and revenue distribution are open and transparent.

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.

Following the method mentioned earlier, qualified users are farming at zero cost, which is paid from the revenues generated through farming. The details are mentioned below:



It is provable that as long as the qualified users are higher in contrast to 2 people or equal to them, significant costs can be reduced with the agreement, and zero handling fees can be observed. As illustrated in the above-mentioned figure, users are solely required to pay for the transfer of tokens, which is normal ETH transfer fees, without having to pay high contract fees.

Particularly, the amount of times users interact with wallets is also lessened by us. Taking the Curve Finance's Y pool deposit as an example; If a user holds DAI or USDc and wishes to farm, the user must have adequate ETH in the wallet in order to pay handling fees (at least 0.3 ETH). If the Y pool has never been utilized, they must 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 are required to be aware of the relationship shared by the benefits of farming and the actual costs. Therefore, we must make use of an oracle to fetch the exchange rate of the revenue coin and the lost coin. Specifically, the current market farming revenue might be gained through the oracle machine (for instance, from websites like 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 established in the future.

Duration

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:

$$Duration = Amount \times LockTime$$

In case of duration being lower as compared to a reasonable value, the system will reject service or charge an in-advance fee. Ordinarily speaking, as long as the number of user funds is higher as compared to 1000 USD and the time is exceeding 3 days or even less on specific days when high-yield pools come out, the Duration is capable of reaching 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 like CRV, BAL, YFI, etc. most commonly fluctuate sharply, in several extreme cases, Farmland Protocol would lose money because of handling fee expenditures. This might cause the operating system to fail. Here we offer two techniques to avoid this problem:

Income deduction: Farmland Protocol will gather revenues in advance, applying the data from the oracle. Through utilizing the oracle to attain the expected income of Farmland and make a contrast with the Ethereum network fees:

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

- if income < expenses, users must increase the farming share ratio or expand the farming period. The users hold the right to make this choice when putting funds into the contract at the beginning.

Reserved security pool: Farmland Protocol would collect 1% of the revenue in each revenue pool as a reserved security pool in order to avoid the problem that the contract cannot attain enough start-up fees when following special extreme circumstances.

Addresses Linked

To allow more users to use our protocol conveniently, we have taken notice in 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.

The profit will be distributed in two ways. The primary difference is that when the user sends their principals, it is sent from the personal wallet or other aggregate addresses.

Users would be capable of choosing a mode if there is a difference between the principal sending address and the income receiving address on the Farmland front end. During this mode, the relevance of the two addresses will be confirmed by the farmland and will send the income in advance to the income pool regulated by Farmland. Afterward, it will transfer the income to the user's reserved income receiving address. Insurance

As an entrance to the DeFi world, Farmland will provide more fundamental users along with convenient and easy-to-use services. Since DeFi farming products often include a nested relationship among each other, the risk of code vulnerabilities is cumulative. This suggests a greater risk to primary users. Many primary users are carefree regarding the potential risk of principal loss because of huge returns.

To provide more users with a safer DeFi environment, Farmland Protocol introduces an insurance mechanism, capable of being implemented in subsequent versions of Farmland. Since the first version of the Farmland Protocol focused on decentralized aggregate farming and revenue distribution, we will now solely outline the basic principles and procedures of the insurance mechanism below.

On the basis of various dimensions of integrated farming protocols, Farmland will list these farming protocols with safety standards. These include codes auditing, online time, etc. The safety classification will be divided 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 compensation fund pool: Users will be capable of purchasing a corresponding quantity 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 might be transformed into Farmland governance tokens and demolished. The remaining amount will turn into 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 needs community voting, and the voters are qualified participants in the compensation pool (that is, participants who have invested more as compared to a specific amount of premiums and are not marked as bad credit).

The amount put into the pool of reimbursement by the voter agreeing to pay out, when it exceeds 4 times the amount paid in the project, the reimbursement is permitted. Nevertheless, if the amount put into the compensation pool by the voter who does not approve the compensation exceeds 3 times the compensation amount of the project, the compensation cannot be approved. All voters who participate in voting will receive specific 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 number of premiums will be seized by the system and that address cannot vote for some time. It has been marked as bad credit several times, and voting rights will be terminated.

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

III. Governance

The farmland Protocol will be launched online after initial testing and implements. Moreover, Farmland's governance will completely enter the DAO stage after the initial centralization and selection of appropriate farming pools. The agreement is subject to FAR, and any enhancements will be decided by FAR holders' votes. Some of the powers that can be regulated 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.