Parasset: Value Reconstruction Based on Oracle

Background

With the version upgrade of NEST Protocol, NEST Token and quotation certificates with a circulation of more than 5 million have been updated to a dual-track quotation mechanism, that is, each mining requires a total of 120 ETH quotation assets and 200,000 NEST (no more than 5 million) The quotation certificate also requires at least 60ETH and 100,000 NEST) to obtain quotation qualification. Miners holding asset quotes also bear the risk of asset fluctuations. Parallel assets start from internal requirements and try to establish a closed loop of applications. Mortgage asset quotes, only need to pay interest expenses, can reduce the loss caused by the fluctuation of various assets. Stability is a relative concept. An asset with a volatility of 0 relative to ETH is a stable currency of ETH, but we generally set anchor assets as legal currency. Due to decentralization and high liquidity, the two processes of mortgage and liquidation are involved, which constitute the two core risks of mortgage: downtime risk and liquidation risk. Downtime risk refers to the length of time from the beginning of the mortgage to the triggering of liquidation. Liquidation risk refers to the ability to normally liquidate assets that are not lower than the mortgage rate. The price trend is generally effective in the long-term (there may be fluctuations in the short-term, causing the liquidation may not be completed), and the triggering of the shutdown is the price reaching the liquidation line. Assuming that the risk-free return of funds is 0, a person mortgages a loan, and once the machine stops, he gets the interest income from the beginning of the loan to the stop time. In the case of a given interest rate, different mortgage rates at different time points will allow the lender to get different returns. The essence of liquidation risk is whether the collateral can be quickly traded within the prescribed liquidation time. This will be affected by the three factors of volatility, asset liquidity and liquidation scale. There is a fixed ratio between the mortgage rate and the liquidation line, within a range of 10% to 20%. Liquidation may also fail. For example, poor liquidity leads to so-called short positions, or the entire liquidation scale is too large to make liquidation impossible.

Insurance Fund

Risk control plays a vital role in financial development. In order to eliminate and manage liquidation risks as much as possible, insurance funds are born from time to time to escort liquidity providers. After the introduction of insurance funds, liquidity providers only need to pay a certain guarantee fee to enjoy security. The income of the underlying asset stabilization fee, although it also constitutes a liability to the system, has its own value. The jump risk caused by the incomplete market cannot be hedged. The stability fee is partly determined by the mortgage rate (downtime risk), and partly by the total mortgage ratio, such as the ratio of the total amount of ETH mortgage to the total circulation. It can also refer to the volatility rate, taking into account the consideration of liquidity and liquidation scale. In this way, insurance funds can obtain extremely high interest rates according to their scale, and balance them naturally. Insurance funds cannot hedge and assume incomplete market risks and may lose money. The blockchain is a game system, and any behavior that occurs on the chain will have an absolute impact on the next participant. Insurance funds help to form self-reinforcing. If people who mortgage loans bear each other's liquidation risks without sufficient income compensation, the whole process will be messy. The introduction of insurance funds generates a ledger for everyone, which is a stable currency that can be used for settlement.

Concept Explanation

Collateral Assets: Decentralized on-chain native assets, such as ETH and NToken, are used to generate parallel assets.

Underlying Assets: The digital asset of the target in the parallel universe.

Parallel Assets: The intrinsic value of the underlying asset is anchored year-on-year, and it is mortgaged by agreement.

Collateral Rate: When the initial coin is minted, users enter mortgage assets to generate parallel assets. The mortgage rate is the ratio of unit mortgage assets to the price of mortgage assets, and the mortgage rate is less than 1.

Liquidation Line: When the price of mortgaged assets drops, the liquidation line and the mortgage rate conform to a certain relationship, and the liquidation line is generally 10%-20% higher than the mortgage rate.

Debt Position: After the mint user enters the mortgage assets into the contract, a debt warehouse for keeping the mortgage assets is generated. When the user redeems the mortgage assets in the debt warehouse, the debt warehouse ends. If the mortgage assets are increased or mortgaged again, the same debt warehouse is shared.

Insurance Capital Pool: used to ensure that the exchange relationship always maintains a 1:1 ratio when liquidation occurs, and the insurance fund pool needs to be entered into USDT. Anyone can use a digital asset to enter the insurance fund pool to generate a parallel asset, or return a parallel asset to the pool in exchange for a digital asset.

Oracle: Call NEST Protocol to provide on-chain price information for mortgage assets.

Stability Fee: Based on the stability fee designed by the mortgage rate, each debt warehouse must pay the stability fee according to the difference between the settlement line and the current price and the time period when adding mortgage, minting new coins, redeeming and liquidating.

Minter: A user who mortgages for parallel assets.

Insurer: The liquidity provider of the insurance fund.

Insurance Net Value: See core algorithm four for details.

Operation Process

The minter pledges the digital assets that meet the requirements to the contract, and generates parallel assets such as PBTC, PETH, and PUSD according to the selected mortgage rate. At the same time, the system generates the corresponding debt warehouse and liquidation line (Minting). Before the debt warehouse is liquidated, at

any time, the mint can retrieve the mortgaged assets by returning the corresponding amount of stable coins (Redemption). Once the mortgage asset price is below the liquidation line, anyone can trigger the liquidation, and the liquidation is in accordance with the following rules: Anyone can use the parallel assets of $(X_t \times 0.9)$ to liquidate, take away the mortgaged assets, the 0.9 of the liquidation goes into the insurance fund, and the parallel assets are destroyed (Clearing). The user can replenish the mortgage at any time, enter the same debt warehouse with the supplementary mortgage, and modify the liquidation line at the same time. The rule is Algorithm 1 (Supplementary Collateral). Anyone can inject insurance funds into the insurance fund pool. The requirement is the corresponding underlying asset. After the injection, the share is calculated according to the net value (Inject Insurance). The insurance funds specify the redemption date and the period is 3 months. Each share needs to be held for at least one period and redeemed according to the net value: the underlying assets will be redeemed first, and the parallel assets will be redeemed if they are insufficient (Withdraw Insurance). Users can re-mint coins in the original debt warehouse, and at the same time correct the liquidation line, according to the core algorithm (Second Minting). Users can inject 1USDT into the insurance fund pool to get 1PUSD, or inject 1PUSD in exchange for 1USDT. 2‰ handling fee is paid according to the scale, and the handling fee is measured by assets (Fast Minting and Exchange). Stability fees are calculated in blocks. Stability fees are charged for each operation of coin minting, redemption, replenishment, and liquidation. Stability fees are calculated in parallel with assets. See Core Algorithm 2 for details (Stability Fee).

Core Algorithm

Mortgage Rate

For a certain debt position, the total amount of collateral assets at time t is recorded as x_t, the change in collateral assets is recorded as x_t,, then:

$$X_t = X_{t-1} + x_t$$

The process of collateralizing assets will generate debts, which are generating parallel assets. The calculation formula is as follows:

$$B_t = B_{t-1} + b_t$$

Formula notes:

1.1 The total debt pledged at time t

1.2 The amount of change in debt caused by this pledge or redemption

1.3 C_t is the mortgage rate at time t, and its formula:

$$C_t = \frac{B_t}{P_t * X_t}$$

Among them P_t is the price of the underlying asset X_t, which comes from the NEST oracle

1.4 Initial collateral, then:

$$\begin{cases} X_t = X_0 \\ B_0 = X_0 * C_0^0 * P_0 \end{cases}$$

Among them, C_0^0 is the initial collateral rate selected by the investor during the initial collateral.

1.5 Full redemption, then:

$$\begin{cases} X_N = 0 \\ B_N = 0 \end{cases}$$

1.6 Partial redemptionb_t

$$\begin{cases} X_t = X_{t-1} - \frac{X_{t-1} * b_t}{B_t} \\ B_t = B_{t-1} - b_t \end{cases}$$

1.7 Second Minting x_t

$$\begin{cases} X_t = X_{t-1} + x_t \\ B_t = B_{t-1} + x_t * C_t^0 * P_t \end{cases}$$

$C_t^0$is the initial collateral rate selected by the investor during second minting

1.8 Liquidation line:

$$P_t < \frac{B_{t-1} + S_t}{X_{t-1}} * k$$

Where k is a constant, $k = 1.2 \text{ or } 1.33$; Total debt(B_t)includes the stability fee for the last paragraph (S_t); When the liquidation line is reached, anyone can use $(X_t \times 0.9)$'s parallel assets to liquidate, take away X_t mortgage assets, $0.9X_t$ of the liquidation goes into the insurance fund, and destroy the parallel assets B_{t-1}: that is, the parallel asset account of the insurance fund increased by $0.9X_t - B_{t-1}$

Stability Fee

$$S_t = B_{t-1} * r_0 * (1 + 2 * (C_{t-1} + \frac{B_{t-1}}{X_{t-1} * P_t})) * (h_t - h_{t-1})$$

Formula notes:

2.1 $S_t$is the stability fee at h_t

2.2 $h_t$represents block height

2.3 $B_t$is the total amount of debt pledged at h_t

2.4 $C_{t-1}$is the mortgage rate at time t-1, its formula:

$$C_{t-1} = \frac{B_{t-1}}{P_{t-1} * X_{t-1}}$$

Among them, $X_{t-1}$is the collateralized assets, $P_{t-1}$is the price of the underlying asset, which comes from the NEST oracle

2.5 r_0 is the market base interest rate

Insurance Fund

The two accounts of the insurance fund are recorded as: the underlying assetsU_t and parallel assetsV_t, the sum of the two is the net assets of the insurance fund.

Net Value

$$NP_t = \frac{N_t}{F_t}$$

Formula notes:

4.1 Net assets $N_t = U_t + V_t$

4.2 $F_t$is the insurance fund share at time t, the initial share is F0, then:

$$F_t = F_{t-1} + \Delta F_t$$

ΔF_t's formula is

$$\Delta F_t = \frac{u_t}{NP_{t-1}}$$

Among them, $u_t$is the new LP asset

Risk Disclosure

You need to understand the following risks and ensure that you participate in the parasset protocol in the right way when you enter the parasset contract and become a user/contract of the insurance fund LP (those who do not understand or cannot accept the risks are not recommended to participate):

1) Insurance funds may be at a loss in extreme situations, for example, asset prices fluctuate and lead to wear wearhouse storm, and insurance funds are

responsible for compensation. Therefore, insurance funds are not a risk-free investment

2) The rate of return of the insurance fund is uncertain: given a stable fee return, the more people participate in insurance, the lower the rate of return of the insurance fund; and the insurance premium depends on the asset size and the rate, which is also uncertain , So you can't treat insurance funds as a fixed-income investment

3) The insurance fund invests in the underlying assets, but at the time of redemption, if the underlying assets in the insurance pool are insufficient, the underlying assets will be replaced by parallel assets. Therefore, there are situations in which only parallel assets can be obtained in the end when the underlying assets are invested. The insurance fund LP needs to be very clear about this risk

4) Redemption time limit: The insurance fund cannot be redeemed immediately after the investment. It needs to be redeemed according to the agreed redemption time. The insurance fund LP needs to specifically clarify this restriction

You need to understand the following risks and ensure that you participate in the parasset protocol in the right way when you enter the parasset protocol to become a minter (those who do not understand or cannot accept the risks are not recommended to participate)

1) Liquidation risk: When the asset price reaches the liquidation line, anyone can liquidate the debt position, causing the minter to lose a certain amount of residual value of the asset (the excess of the underlying asset generated)

2) Stability fee fluctuation risk: The stability fee is calculated based on the collateral rate and the system basic rate. Therefore, changes in the collateral rate or the system basic rate will bring fluctuations in the stability fee

3) Parasset price fluctuation risk: The internal mechanism ensures that the value of the parallel asset and the underlying asset is 1:1, but if the liquidation fails, the insurance fund goes bankrupt or the supply and demand in the secondary market cannot be effectively balanced, the price of the parallel asset will fluctuate.

4) The risk of dynamic data display: there is a certain delay risk between reading the data and the actual execution of the data, which will affect the decision of the minter. It is necessary to carefully understand the Ethereum, NEST and parasset mechanisms to ensure that the risk is understood

5) Redemption requires to use parallel assets, so lack of parallel assets may lead to failure to redeem the collateral

Users/contracts holding parallel assets need to understand the following risks and ensure that they participate in the parasset procol in the right way (those who do not understand or cannot accept the risks are not recommended to participate)

1) Parallel asset price fluctuation risk: The internal mechanism ensures that the value of the parallel asset and the underlying asset is 1:1, but if the liquidation fails, the insurance fund goes bankrupt or the supply and demand in the secondary market cannot be effectively balanced, the price of the parallel asset will fluctuate.

All participants need to understand that there are the following risks and ensure that they participate in the parasset protocol in the right way (those who do not understand or cannot accept the risks are not recommended to participate)

1) Oracle risks: NEST oracles are decentralized, and there may be risks such as code vulnerabilities, being attacked, and large price deviations, which will bring losses to PARASSET

2) Code risk: parasset is a decentralized protocol, due to the risk brought by the

code, all participants may lose part or all of the funds; code upgrades may also bring the risk of incompatibility between the old and new protocols, resulting in the loss of part of the time value

3) ETH underlying risk: Vulnerabilities in ETH underlying code may cause the entire contract to become invalid or cause large losses

4) Due to the calculation of the accuracy of the token, there will be a loss of accuracy in the redemption of insurance funds

5) Regulatory risk: At present, DEFI has no clear regulatory policy, so any changes in regulatory policy may bring the risk of user losses

6) Risk of incorrect operation: the user cannot operate the contract correctly, resulting in losses

7) The user failed to identify the correct contract address and entered the contract that was maliciously copied, causing the risk of loss

8) The mismatch of user risk preferences makes it impossible to achieve expectations, so it is recommended to fully understand the parasset mechanism and the risk structure of DEFI