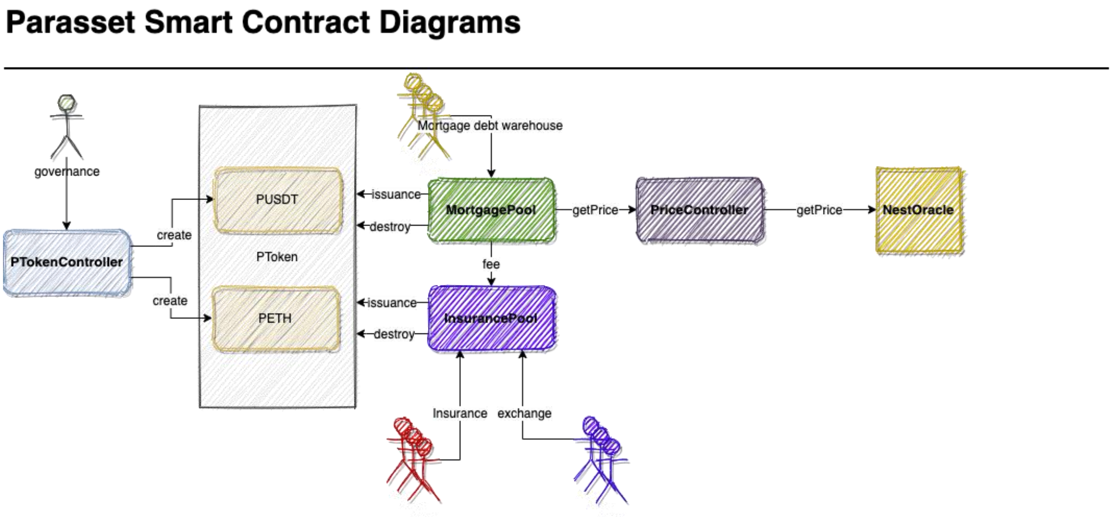
Parasset uses the average Token price-output from the NEST Oracle

Contract Structure



PTokenFactory: create PToken，control the permission of the increment and destruction

MortgagePool: the pool of mortgage assets which supports the operations of minting, adding mortgage assets, reducing mortgage assets, adding minting, reducing minting, and liquidating.

InsurancePool: support the operations of subscribing insurance, redeeming insurance, and exchange.

PriceController: Price control contract, which interfaces with the NEST price contract and outputs the price to the MortgagePool. Separate the administration to avoid the need to update the MortgagePool contract due to the changes in NEST price contract.

PToken: PToken Contract

MortgagePool

Global Parameters

Maximum Collateral Rate: C_{max}, with different volatility (risk) and different K values for each kind of collateralized asset.

Market base rate: r_0

Liquidation line: K. Each kind of mortgage asset has different volatility (risk) and different K values.

Operation of Minting

Input parameters:

1. Token address of Collateral asset: MToken
2. Token address of p asset: PToken
3. Increase the token number of Collateral assets: Δx
4. Customized collateral rate: C_{cus}

Operation restrictions:

1. The protocol allows MToken collateral to mint PToken
2. $C_{cus} > 0$ and $C_{cus} <= C_{max}$
3. $\Delta x > 0$

Realization:

$$P_t = \frac{P_t^P}{P_t^M}$$

$$C_t^1 = \frac{Y_{t-1}}{X_{t-1} * P_t}$$

$$S_t = Y_{t-1} * r_0 * (1 + \frac{3*(C_{t-1} + C_t^1)}{2}) * (h_t - h_{t-1})$$

$$\Delta y = \Delta x * C_{cus} * P_t$$

$$Y_t = Y_{t-1} + \Delta y$$

$$X_t = X_{t-1} + \Delta x$$

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

Notes:

1. P_t^P: The quantity of PToken worth 1 ETH; P_t^M: The quantity of collateral assets worth 1 ETH
2. C_t^1: Position-by-position mortgage rate as the rate before the current operation
3. S_t: The stability fee between the last and the current operation of debt position; r_0: Market base rate; Y_{t-1}: Quantity of debt after the last operation (including liquidation); C_{t-1}: Collateral rate after the last operation of the debt position; h_t: Block ID for current operation of debt position; h_{t-1}: Block ID of the last operation of debt position. The handling fee will be settled first and transferred to the insurance pool and will not
   participate in other calculations
4. Δy: New debt for the current operation
5. Y_t: Quantity of debt after the current operation; X_t: Quantity of collateral assets after the current operation; Δx: Quantity of new collateral assets for the current operation; C_t: Collateral rate after the current operation

Operation of adding collateral assets

Input parameters:

1. Token address of Collateral asset: MToken
2. Token address of p asset: PToken
3. Increase the token number of Collateral assets: Δx

Operation restrictions:

1. The protocol allows MToken collateral to mint PToken

2. Debt position created
3. $\Delta x > 0$

Realization:

$$P_t = \frac{P_t^P}{P_t^M}$$

$$C_t^1 = \frac{Y_{t-1}}{X_{t-1} * P_t}$$

$$S_t = Y_{t-1} * r_0 * (1 + \frac{3*(C_{t-1} + C_t^1)}{2}) * (h_t - h_{t-1})$$

$$Y_t = Y_{t-1}$$

$$X_t = X_{t-1} + \Delta x$$

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

Notes:

1. P_t^P: The quantity of PToken worth 1 ETH; P_t^M: The quantity of collateral assets worth 1 ETH
2. C_t^1: Position-by-position mortgage rate as the rate before the current operation
3. S_t: The stability fee between the last and the current operation of debt position; r_0: Market base rate; Y_{t-1}: Quantity of debt after the last operation (including liquidation); C_{t-1}: Collateral rate after the last operation of the debt position; h_t: Block ID for current operation of debt position; h_{t-1}: Block ID of the last operation of debt position. The handling fee will be settled first and transferred to the insurance pool and will not
participate in other calculations

4. Y_t: Quantity of debt after the current operation; X_t: Quantity of collateral assets after the current operation; Δx: Quantity of new collateral assets for the current

operation; C_t: Collateral rate after the current operation

Operation of reducing collateral assets

Input parameters:

1. Token address of Collateral asset: MToken
2. Token address of p asset: PToken
3. Reduce the token number of Collateral assets: Δx

Operation restrictions:

1. The protocol allows MToken collateral to mint PToken
2. Debt position created
3. $\Delta x > 0$ and $\Delta x \le X_{t-1}$
4. $C_t <= C_{max}$

Realization:

$$P_t = \frac{P_t^P}{P_t^M}$$

$$C_t^1 = \frac{Y_{t-1}}{X_{t-1} * P_t}$$

$$S_t = Y_{t-1} * r_0 * (1 + \frac{3*(C_{t-1} + C_t^1)}{2}) * (h_t - h_{t-1})$$

$$Y_t = Y_{t-1}$$

$$X_t = X_{t-1} - \Delta x$$

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

Notes:

1. P_t^P: The quantity of PToken worth 1 ETH; P_t^M: The quantity of collateral assets worth 1 ETH
2. C_t^1: Position-by-position mortgage rate as the rate before the current operation
3. S_t: The stability fee between the last and the current operation of debt position; r_0: Market base rate; Y_{t-1}: Quantity of debt after the last operation (including liquidation); C_{t-1}: Collateral rate after the last operation of the debt position; h_t: Block ID for current operation of debt position; h_{t-1}: Block ID of the last operation of debt position. The handling fee will be settled first and transferred to the insurance pool and will not
participate in other calculations
4. Y_t: Quantity of debt after the current operation; X_t: Quantity of collateral assets after the current operation; Δx: Quantity of reduced collateral assets for the current operation; C_t: Collateral rate after the current operation

Operation of increasing minting (debt)

Input parameters:

1. Token address of Collateral asset: MToken
2. Token address of p asset: PToken
3. Increase the quantity of debt: Δy

Operation restrictions:

1. The protocol allows MToken collateral to mint PToken
2. Debt position created

3. $\Delta y > 0$

4. $C_t <= C_{max}$

Realization:

$$P_t = \frac{P_t^P}{P_t^M}$$

$$C_t^1 = \frac{Y_{t-1}}{X_{t-1} * P_t}$$

$$S_t = Y_{t-1} * r_0 * (1 + \frac{3 * (C_{t-1} + C_t^1)}{2}) * (h_t - h_{t-1})$$

$$Y_t = Y_{t-1} + \Delta y$$

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

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

Notes:

1. P_t^P: The quantity of PToken worth 1 ETH; P_t^M: The quantity of collateral assets worth 1 ETH
2. C_t^1: Position-by-position mortgage rate as the rate before the current operation
3. S_t: The stability fee between the last and the current operation of debt position; r_0: Market base rate; Y_{t-1}: Quantity of debt after the last operation (including liquidation); C_{t-1}: Collateral rate after the last operation of the debt position; h_t: Block ID for current operation of debt position; h_{t-1}: Block ID of the last operation of debt position. The handling fee will be settled first and transferred to the insurance pool and will not
participate in other calculations

4. Y_t: Quantity of debt after the current operation; X_t: Quantity of collateral assets after the current operation; Δy: Quantity of reduced debt (destroyed PToken) for the

current operation; C_t: Collateral rate after the current operation

Operation of liquidating

Input parameters:

1. Token address of Collateral asset: MToken
2. Token address of p asset: PToken
3. Address with debt position: account
4. Quantity of collateral assets acquired: Δx

Operation restrictions:

1. The protocol allows MToken collateral to mint PToken
2. Debt position created
3. $\Delta x > 0$ and $\Delta x <= X_{t-1}$
4. $C_t^K > K$

Realization:

$$P_t = \frac{P_t^P}{P_t^M}$$

$$C_t^1 = \frac{Y_{t-1}}{X_{t-1} * P_t}$$

$$S_t = Y_{t-1} * r_0 * (1 + \frac{3 * (C_{t-1} + C_t^1)}{2}) * (h_t - h_{t-1})$$

$$C_t^K = \frac{Y_{t-1} + S_t}{X_{t-1} * P_t}$$

$$\Delta y = Y_{t-1} * \frac{\Delta x}{X_{t-1}}$$

$$Y_t = Y_{t-1} - \Delta y$$

$X_t = X_{t-1} - \Delta x$

Notes:

1. P_t^P: The quantity of PToken worth 1 ETH; P_t^M: The quantity of collateral assets worth 1 ETH
2. C_t^1: Position-by-position mortgage rate as the rate before the current operation
3. S_t: The stability fee between the last and the current operation of debt position; r_0: Market base rate; Y_{t-1}: Quantity of debt after the last operation (including liquidation); C_{t-1}: Collateral rate after the last operation of the debt position; h_t: Block ID for current operation of debt position; h_{t-1}: Block ID of the last operation of debt position.
4. C_t^K: Judgment liquidation line
5. Y_t: Quantity of debt after the current operation; X_t: Quantity of collateral assets after the current operation; Δy: Quantity of reduced debt (destroyed PToken) for the current operation; Δx: Quantity of collateral assets reduced by the current operation.

C_t and h_t won't be updated by liquidation operation. If Y_t=0, then C_t=0、h_t=0. Current debt position to be completely liquidated.

Insurance Pool

global parameters

Handling Fee Rate: r_0, two thousandths

Redemption Period: T_0, two weeks

Redemption Duration: T_1, two days

Operation of exchanging PToken for the underlying asset

Input parameters:

1. Token address of P asset: PToken
2. Token number of P asset: Δz

Operation restrictions:

1. The PToken address input is protocol-generated (PToken Verification)
2. The underlying asset to be redeemed must be greater than 0（PToken has 18 bits, there will be a situation that it equals to 0 when exchanging for the underlying asset with less than 18 bits due to the difference in precision）
3. $\Delta z > 0$

Realization:

$$S_t = \Delta z * r_0$$

$$\Delta v = \Delta z - S_t$$

Notes:

1. S_t: Handling fee for the current operation; Δz: Quantity of PToken transferred in; r_0: Handling Fee Rate
2. Δv: Quantity of the underlying asset transferred out

Operation of exchanging the underlying asset for PToken

Input parameters:

1. Token address of the underlying asset: uToken

2. Token number of the underlying asset: Δv

Operation restrictions:

1. The input address of the underlying asset has a corresponding PToken in the protocol

2. PToken to be redeemed must be greater than 0（PToken has 18 bits, there will be a situation that it equals to 0 when the underlying asset has more than 18 bits due to the difference in precision）

3. $\Delta v > 0$

Realization:

$$S_t = \Delta v * r_0$$

$$\Delta z = \Delta v - S_t$$

Notes:

1. S_t: Handling fee for the current operation; Δv: Quantity of the underlying asset transferred in; r_0: Handling Fee Rate

2. Δz: Quantity of PToken transferred out. If there are not enough PToken, directly issue additional PToken.

Operation of insurance subscription

Input parameters:

1. Token address of the underlying asset: uToken
2. Token number of the underlying asset: Δu

Operation restrictions:

1. The input address of the underlying asset has a corresponding PToken in the protocol
2. The net assets in insurance is greater than 0（there is a PToken negative account, the amount of fund available in the insurance must be greater than that in the negative account; $U_{t-1} + V_{t-1} > G_{t-1}$）
3. $\Delta u > 0$

Realization:

$$NP_{t-1} = \frac{U_{t-1}+V_{t-1}-G_{t-1}}{F_{t-1}}$$

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

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

Notes:

1. F_t is the share of insurance fund at time t, the initial share is that $F_0 = 0$
2. NP_{t-1}: Net value before the current operation; U_{t-1}: Balance of underlying assets in insurance; V_{t-1}: Balance of PToken assets in insurance; G_{t-1}: Limit of PToken negative account in insurance; F_{t-1}: Share of insurance fund before the current operation.
3. ΔF_t : The new insurance fund shares added by the current operation; Δu: Quantity of the underlying asset transferred in the current subscription; the additional insurance shares will not be redeemed until the next redemption period

Operation of insurance redemption

Input parameters:

1. Token address of the underlying asset: uToken
2. Number of LP to be redeemed t: Δlp

Operation restrictions:

1. The input address of the underlying asset has a corresponding PToken in the protocol
2. The net assets in insurance is greater than 0（there is a PToken negative account, the amount of fund available in the insurance must be greater than that in the negative account; $U_{t-1} + V_{t-1} > G_{t-1}$）
3. $\Delta lp > 0$
4. The time of this operation is within the duration of the redemption
5. The individual insurance share after the operation is greater than or equal to the frozen insurance share

Realization:

$$\mathrm{NP}_{t-1} = \frac{U_{t-1}+V_{t-1}-G_{t-1}}{F_{t-1}}$$

$$\Delta u = \Delta F_t * \mathrm{NP}_{t-1}$$

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

Notes:

1. F_t is the share of insurance fund at time t, the initial share is that $F_0 = 0$
2. **NP_{t-1}**: Net value before the current operation; U_{t-1}: Balance of underlying assets in

insurance; V_{t-1}: Balance of PToken assets in insurance; G_{t-1}: Limit of PToken negative account in insurance; F_{t-1}: Share of insurance fund before the current operation.

3. ΔF_t : Insurance fund shares redeemed by the current operation Δu: Quantity of the redeemed asset by the current operation; transfer out the underlying assets first, and then transfer out PToken assets if the underlying assets are insufficient.