Standardized Yield Stripping - efficient yield stripping mechanism on DeFi's yield generating assets

Vu Nguyen
vu@pendle.finance

October 14, 2022

Abstract

Yield generating assets are the bedrock of any financial system, both in traditional finance (TradFi) and decentralised finance (DeFi). Yield stripping loosely refers to the process of splitting a yield generating asset into two components: its principal and yield components. These components take on different forms with wide-ranging applications. In DeFi, a number of protocols have proposed different ways to do yield stripping. In this paper, we will propose Standardized Yield Stripping - an efficient, composable and permissionless mechanism for yield stripping on most yield generating assets in DeFi

1 Standardized Yield Stripping (SYS)

In this section, we introduce SYS, a yield stripping mechanism on most yield generating assets in DeFi. SYS works on all SY tokens, as defined in the Standardized Yield paper [1] where the compound interest is always positive ($SYIndex(t)$ is a non-decreasing function).

1.1 Overview

Yield stripping in SYS must always be in the context of a **SY token**, and an expiry. With a chosen **expiry**, a **SY token** is split into a Yield Token (YT) and a Principal Token (PT).

YT represents the right to claim the real-time yields until the expiry, and PT represents the right to redeem the principal after the expiry.

SYS白皮书的SYIndex就相当于SY白皮书的exchangeRate

1.2 Basic definitions

yield stripping pool is a pool of **SY tokens** that were deposited in total for yield stripping up to an **expiry**. At time t, there are $S(t)$ SY tokens in the yield stripping pool, which is worth $A(t) = S(t) \times SYIndex(t)$ of **asset**.

SY token is a Standardized Yield token as defined in the SY paper [1]. Most yield generating mechanisms in DeFi can be converted into SY token.

expiry the end of the period where yield can be traded until. Short form: t_{expiry}

asset is the unit to measure value of SY tokens, as defined in the SY standard and GYGP model

users are entities who interact with the yield stripping pool in one way or another.

Yield Token (YT) is a unit that could be created (minted), destroyed (burned) or transferred between users. Loosely speaking, it is the yield component that is stripped from the SY token. At time t, a user u has a YT balance of $ytBalance_u(t)$. The total YT in existence at time t is $ytSupply(t)$

$$\sum_u ytBalance_u(t) = ytSupply(t) \tag{1}$$

Principal Token (PT) is a unit that could be created (minted), destroyed (burned) or transferred between users. Loosely speaking, it is the principal component of the SY token. At time t, a user u has a PT balance of $ptBalance_u(t)$. The total PT in existence at time t is $ptSupply(t)$

$$\sum_u ptBalance_u(t) = ptSupply(t) \tag{2}$$

reward tokens are tokens generated from holding SY tokens over time, as defined in (insert reference). There are $n_{rewards}$ different reward tokens for the **SY token**. At time t, $R_i(t)$ is the total amount of **reward token** i that has been accrued for the **yield stripping pool** since $t = 0$. These reward tokens would be distributed among the users. At time t, a user u is entitled to receive a total of r_{u_i} **reward token** i

user total accrued interest From t_{start} until time t, a user u is entitled to receive a total of $i_u(t)$ of **SY token** as interests for holding YT over time.

user claimed interest From t_{start} until time t, a user u has claimed $c_u(t)$ of **SY token** as interests from the **yield stripping pool**. This means that at time t, user u has an unclaimed amount of interest $i_u(t) - c_u(t)$ in **SY token** that is sitting in the **yield stripping pool**

1.3 State changes

At any point in time, let's define $t*$ to be the timestamp of the latest global state change. There are 4 types of state changes:

1.3.1 Initialisation

At the start at t_{start}:

$$S(t_{start}) = A(t_{start}) = R_i(t_{start}) = ytSupply(t_{start}) = ptSupply(t_{start}) = 0$$

1.3.2 Minting/Redeeming YT and PT before the expiry

At time $t < t_{expiry}$, a user u can send in d_{SY} **SY token**, which is worth d_a **asset** into the **yield stripping pool**, to mint d_a YT and d_a PT out. If $d_{SY} < 0$, this becomes a redemption where the user redeems $-d_{SY}$ **SY token** from the **yield stripping pool** after burning $-d_a$ YT and $-d_a$ PT. It is required that $-d_a \leq min(ytBalance_u(t*), ptBalance_u(t*))$ to ensure that the user has enough

PT and YT for redemption.

$$
\begin{aligned}
d_a &= d_{SY} \times SYIndex(t) \\
ytBalance_u(t) &= ytBalance_u(t*) + d_a \\
ptBalance_u(t) &= ptBalance_u(t*) + d_a \\
S(t) &= S(t*) + d_{SY} \\
A(t) &= A(t*) + d_a \\
ytSupply(t) &= ytSupply(t*) + d_a \\
ptSupply(t) &= ptSupply(t*) + d_a
\end{aligned}
$$

1.3.3 Redeeming after expiry

At time $t \geq t_{expiry}$, a user u can burn d_a PT, to redeem d_{SY} **SY token** which is worth d_a **asset** ($d_a \leq ptBalance_u(t*)$).

$$
\begin{aligned}
d_{SY} &= \frac{d_a}{SYIndex(t)} \\
ptBalance_u(t) &= ptBalance_u(t*) - d_a \\
S(t) &= S(t*) - d_{SY} \\
A(t) &= A(t*) - d_a \\
ptSupply(t) &= ptSupply(t*) - d_a
\end{aligned}
$$

直接用于生产

1.3.4 Earning of compound interests for SY token

At time $t < t_{expiry}$, there could be some interest earned for the **SY token**, such that $SYIndex(t) > SYIndex(t*)$. Each user u's total accrued interest will increase by an amount $dInterest_u$ as follows:

$$
\begin{aligned}
dInterest_u &= ytBalance_u(t*) \times \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right) \\
i_u(t) &= i_u(t*) + dInterest_u
\end{aligned}
$$

生产环境中，如果是simple SY，直接用lemma 6即可

1.3.5 Earning of rewards for SY token

At time $t < t_{expiry}$, there could be d_{r_i} of **reward token** i earned by the **yield stripping pool**. We will distribute these rewards to each user, proportionally to each user's **SY balance to receive rewards.**

Reward generating SY balance of a user at time t is the amount of **SY tokens** that each user is entitled to get reward tokens for, $rewardGeneratingSY_u(t)$. It is the sum of the unclaimed interest and the SY equivalent amount of the YT balance:

$$
rewardGeneratingSY_u(t) = i_u(t) - c_u(t) + \frac{ytBalance_u(t)}{SYIndex(t)} \tag{3}
$$

用户未领取的利息（以SY代币计算）

用户持有的所有YT代币能够兑换成SY代币的数量

奖励生成SY余额是用户有资格赚取奖励代币的SY代币数量，而不是说生成的奖励有多少SY代币

With the definition of $rewardGeneratingSY_u(t)$, we can define the formula for distributing d_{r_i} of **reward token** i among the users: each user u will receive $d_{r_{i_u}}$ of **reward token** i:

$$d_{r_{i_u}} = rewardGeneratingSY_u(t*) \times \frac{d_{r_i}}{S(t*)} \tag{4}$$

1.3.6 User claiming interests

At time t, a user u can claim all of their claimable interests of $i_u(t*) - c_u(t*)$, such that:

$$\begin{aligned} c_u(t) &= i_u(t*) \\ S(t) &= S(t*) - (i_u(t*) - c_u(t*)) \end{aligned}$$

1.4 Proofs

With the mechanism defined, we can prove a number of results:

1.4.1 Lemma 1

Before the expiry, there will always be the same amount of YT and PT.

$$ytSupply(t) = ptSupply(t)$$

This is a trivial result because the only state change prior to expiry that changes YT and PT supply (3.3.2) can only change their supplies by the same amount.

1.4.2 Lemma 2

The total amount of **SY token** in the **yield stripping pool** at any time $t < t_{expiry}$ is exactly the amount of **SY token** that could be redeemed by all the YT and PT, plus the sum of all unclaimed interests by users.

$$S(t) = \frac{ytSupply(t)}{SYIndex(t)} + \sum_u i_u(t) - c_u(t) \tag{5}$$

This can be proved by induction. Right after initialisation, it's trivial that (5) is correct since both sides are 0. Assume that (5) holds for $t*$, which means:

$$S(t*) = \frac{ytSupply(t*)}{SYIndex(t*)} + \sum_u i_u(t*) - c_u(t*) \tag{6}$$

we could prove that (5) will still hold at t for all the possible state changes:

Minting/redeeming YT and PT before expiry All the $i_u(t)$ and $c_u(t)$ values do not change, and both $S(t)$ and $\frac{ytSupply(t)}{SYIndex(t)}$ increases by d_{SY}. Hence, (5) still holds for t

Earning of compound interests for SY token

$$
\begin{aligned}
&\sum_u i_u(t) - c_u(t) \\
&= \sum_u i_u(t*) + dInterest_u - c_u(t*) \\
&= \sum_u i_u(t*) - c_u(t*) + ytBalance_u(t*) \times \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right) \\
&= \left(\sum_u i_u(t*) - c_u(t*) \right) + \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right) \times \sum_u ytBalance_u(t*) \\
&= \left(\sum_u i_u(t*) - c_u(t*) \right) + \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right) \times ytSupply(t*) \\
&= S(t*) - \frac{ytSupply(t*)}{SYIndex(t*)} + \frac{ytSupply(t*)}{SYIndex(t*)} - \frac{ytSupply(t*)}{SYIndex(t)} \\
&= S(t) - \frac{ytSupply(t)}{SYIndex(t)}
\end{aligned}
$$

Hence, (5) is satisfied as well.

Earning of rewards for SY token It is trivial that (5) still holds for t as the values don't change,

User claiming interests Both $S(t)$ and $\sum_u i_u(t) - c_u(t)$ decrease by the same amount $i_u(t*) - c_u(t*)$. Hence, (5) still holds true for t,

Since (5) is true for t_{start}, and is always true for t given that it's true for $t*$, (5) is always true by induction.

1.4.3 Lemma 3

The interest accrued by user X holding an amount of a YT token from $t1$ to $t2$ is equivalent to the interest accrued by user Y holding a **asset** worth of **SY token** from $t1$ to $t2$
The interests for Y in units of SY:

$$
\begin{aligned}
interest_Y &= \frac{\frac{a}{SYIndex(t1)} \times SYIndex(t2) - a}{SYIndex(t2)} \\
&= a \times \left(\frac{1}{SYIndex(t1)} - \frac{1}{SYIndex(t2)} \right)
\end{aligned}
$$

The interests for X in units of SY: (where $t1'$ is the time stamp of the state change right after $t1$)

$$
\begin{aligned}
interest_X &= \sum_{t1'}^{t2} dInterest_X \\
&= \sum_{t1'}^{t2} ytBalance_X(t*) \times \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right) \\
&= a \times \left(\frac{1}{SYIndex(t1)} - \frac{1}{SYIndex(t2)} \right)
\end{aligned}
$$

Hence, Lemma 3 is proven.

1.4.4 Lemma 4

The total amount of **reward token** i accrued by the **yield stripping pool** until time t is the same as the sum of all users' total entitled rewards.

$$\sum_u r_{u_i}(t) = R_i(t) \tag{7}$$

At the start, (7) is trivially true with both values being 0. The only state change that changes the rewards is 1.3.5 (Earning of rewards for SY token). Hence, we just need to prove that the sum of new rewards to all the users is the same as the total new rewards:

$$\sum_u d_{r_{i_u}} = d_{r_i}$$

To prove it:

$$\begin{aligned}
L.H.S = \sum_u d_{r_{i_u}} &= \sum_u rewardGeneratingSY_u(t*) \times \frac{d_{r_i}}{S(t*)} \\
&= \frac{d_{r_i}}{S(t*)} \times \sum_u \left(i_u(t) - c_u(t) + \frac{ytBalance_u(t)}{SYIndex(t)} \right) \\
&= \frac{d_{r_i}}{S(t)} \times \left(\sum_u (i_u(t) - c_u(t)) + \sum_u \frac{ytBalance_u(t)}{SYIndex(t)} \right) \\
&= \frac{d_{r_i}}{S(t)} \times \left(\sum_u (i_u(t) - c_u(t)) + \frac{ytSupply(t)}{SYIndex(t)} \right) \\
&= \frac{d_{r_i}}{S(t)} \times S(t) \qquad \text{(From Lemma 2)} \\
&= d_{r_i} \\
&= R.H.S
\end{aligned}$$

Hence, (7) is proven.

1.5 Lemma 5

If a user u does not claim their interest, mint or redeem from $t1$ to $t2$, their $rewardGeneratingSY_u(t)$ stays the same.

如果claim了

We just need to prove the lemma for state change 1.3.5 (Earning of compound interests for SY token), which is the only state change left that changes $rewardGeneratingSY_u(t)$. Let's say the state change happen at t, and $t*$ was the timestamp of the previous state change.

$$\begin{aligned}
rewardGeneratingSY_u(t) &= i_u(t) - c_u(t) + \frac{ytBalance_u(t)}{SYIndex(t)} \\
&= i_u(t*) + dInterest_u - c_u(t*) + \frac{ytBalance_u(t)}{SYIndex(t)} \\
&= i_u(t*) + ytBalance_u(t*) \times \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right) - c_u(t*) + \frac{ytBalance_u(t)}{SYIndex(t)} \\
&= i_u(t*) - c_u(t*) + \frac{ytBalance_u(t*)}{SYIndex(t*)} \\
&= rewardGeneratingSY_u(t*)
\end{aligned}$$

$$c_u(t) = i_u(t*)$$

$$S(t) = S(t*) - (i_u(t*) - c_u(t*))$$

如果claim了，这两个相减为0

$$dInterest_u = ytBalance_u(t*) \times \left(\frac{1}{SYIndex(t*)} - \frac{1}{SYIndex(t)} \right)$$

$$i_u(t) = i_u(t*) + dInterest_u$$

As such, we have proven that $rewardGeneratingSY_u$ remains unchanged.

这些SY代币刚好可以转化为a单位个基础资产

1.5.1 Lemma 6

If the **SY token** is a Simple SY token (as defined in the SY paper [1]), the amount of **reward token** i gotten by user X holding an amount of a YT token from $t1$ to $t2$ is exactly the same as the amount of **reward token** i gotten by user Y holding a **asset** worth of **SY token** from $t1$ to $t2$

First, we will define:

- $r_{u_i}^{SY}(t)$ as the equivalent of $r_{u_i}(t)$ in the SY paper [1] (the total rewards for rewards token i accrued for user u until time t)
- $S^{SY}(t)$ as the equivalent of $S(t)$ in the SY paper [1] (total number of shares)
- $s_u^{SY}(t)$ as the equivalent of $s_u(t)$ in the SY paper [1] (amount of shares of user u)

At $t1$, a **asset** is equivalent to $s_u = \frac{a}{SYIndex(t1)}$ **SY tokens**

a个基础资产等价于a/SYIndex个SY代币，而且这里还表示该用户的份额，具体需要见SY白皮书

The amount of **reward token** i for X (from section 4.1 in the SY paper [1])

$$rewards_X = s_u \times (rewardIndex_i(t2) - rewardIndex_i(t1))$$

Denote $t*$ as the timestamp of the state change right before a state change at t. For the whole yield stripping pool, the amount of reward token i received from $t*$ to t is:

$$d_{r_i}(t) = S(t*) \times (rewardIndex_i(t) - rewardIndex_i(t*)) \tag{8}$$

As such, the amount of reward token i received by Y from $t*$ to t is:

$$\begin{aligned}
d_{r_{i_u}}(t) &= rewardGeneratingSY_u(t*) \times \frac{d_{r_i}(t)}{S(t*)} && \text{From (4)} \\
&= rewardGeneratingSY_u(t1) \times (rewardIndex_i(t) - rewardIndex_i(t*)) \\
& && \text{From (8) and lemma 5} \\
&= \left(i_u(t1) - c_u(t1) + \frac{ytBalance_u(t1)}{SYIndex(t1)}\right) \times (rewardIndex_i(t) - rewardIndex_i(t*)) && \text{From (3)} \\
&= \frac{a}{SYIndex(t1)} \times (rewardIndex_i(t) - rewardIndex_i(t*)) && \text{Since } i_u(t1) = c_u(t1) = 0
\end{aligned}$$

Hence, the total amount of **reward token** i for Y from t_1 to t_2 is:

$$\begin{aligned}
rewards_Y &= \sum_{t_1'}^{t_2} \frac{a}{SYIndex(t1)} \times (rewardIndex_i(t) - rewardIndex_i(t*)) \\
&= \frac{a}{SYIndex(t1)} \times (rewardIndex_i(t2) - rewardIndex_i(t1)) \\
&= s_u \times (rewardIndex_i(t2) - rewardIndex_i(t1))
\end{aligned}$$

Therefore, $rewards_X = rewards_Y$ and lemma 6 is proven.

$$rewardGeneratingSY_u(t) = i_u(t) - c_u(t) + \frac{ytBalance_u(t)}{SYIndex(t)} \tag{3}$$

References

[1] Vu Nguyen and Long Vuong. *Standardized Yield*. URL: `https://pendle.finance/SY.pdf`.