Su: Money Protocol

Interest Protocol Team

Abstract

We propose Su, a money protocol for Sui Network. Su comprises a set of smart contracts that decomposes the Sui coin into two asset classes: Beta Coins and Leveraged Sui. In finance, Beta is the measure of the volatility of an asset. Su can issue two types of Beta coins: Fractional Sui with a beta of 0.1 and Sui Dollar with a beta of 1. Sui Dollar is a stablecoin, and Fractional Sui is a floating stablecoin that tracks 10% of Sui's volatility. The Leveraged Sui coin absorbs the remaining volatility, allowing the Beta coins to keep their peg while providing investors a perpetual contract without liquidations or funding rates. Su is a capital-efficient protocol as it does not depend on over-collateralization to ensure the system's solvency. Instead, it transfers the volatility from risk-averse users to risk-seeking bulls. This design allows users to long Sui while unlocking the market's first scalable and decentralized stablecoins.

1 The Problem: The Stablecoin Trilema

Stablecoins are crucial for DeFi's functioning. Thanks to their fiat peg, users feel comfortable exploring the benefits of DeFi. The stablecoin market is currently valued at 150 billion US dollars[1]. Despite their huge success and adoption, current stablecoin designs sacrifice either scalability, decentralization, or stability. This poses an existential threat to DeFi, as we will explore it later on.

1.1 Type of stablecoins

There are four types of stablecoins, which differ according to their method of pegging[2]:

1. **Cash and equivalents collateralized stablecoins:** they are a form of fiat tokenization.
2. **Asset-back stablecoins:** they employ tangible assets such as precious metals, and commodities.
3. **Crypto over-collateralized stablecoins:** maintain an equal price to the US Dollar ratio through over-collateralized crypto reserves.
4. **Fully algorithmic stablecoins:** they employ clever mechanisms such as minting/burning or rebasing to achieve parity with the US Dollar.

The most popular approach is to sacrifice decentralization by relying on off-chain collateral and a redemption mechanism. USDT and USDC are examples of this design, accounting for over 90% of the stablecoin market. This imposes a high risk on DeFi applications as their censorship resistance relies on external players exposed to uncontrollable events. The recent incident with Silicon Valley Bank showcased this weakness[3]. USDC lost its peg because Circle had 8% of its reserves in SVB, placing several DeFi applications and millions of users at risk. SVB's overexposure to long-term bonds placed the entire crypto market in jeopardy. One entity's bad financial decision should not endanger DeFi.

Collateral Debt Position protocols, or CDPs for short, are the second most popular stablecoin designs. They were designed to address the centralization risks by over-collaterizing their stablecoins with a highly liquid on-chain collateral. While these systems proved resilient, they are capital inefficient for the end users. MakerDAO is the largest CDP in the market, with a minimum collateralization ratio of 150%[4]. Users must have at least $1.5 for every DAI in their account to avoid liquidations.

There have been attempts to create algorithmic stablecoins to address the capital inefficiency of CDPs. However, all designs have proven to be unable to withstand bank runs. The most famous was UST in 2022, when 18 billion US dollars were wiped out[5]. Other algorithmic stable coins chose a hybrid approach of being partially collateralized. However, FRX, the largest one, has decided to fully collateralize its coin to guard its peg[6]. Algorithmic stablecoins remain an unsolved problem.

1.2 Stability

Stability refers to the liquidity and volatility of the collateral asset. Highly liquid and low volatile assets offer strong stability as they are easily redeemable. USDT and USDC are stable because they are backed by the asset they represent. CDP stable coins with conservative collateral ratios and blue chip assets offer strong stability as there is enough liquidity on-chain for liquidations. The more centralized a stablecoin is, the more likely it will have peg stability.

1.3 Scalability

It refers to the capital efficiency design of the stablecoin. Centralized solutions are very efficient and scalable as they are backed 1:1 with their collateral and have no risk of liquidation. CDPs are quite inefficient as users must keep a conservative collateral ratio to avoid liquidation. For example, in order to mint 1 million USDC, Circle must supply 1 million dollars, while MarketDAO would have to supply over 1.5 million USD in Ether. CDPs must constantly monitor the volatility and liquidity of their collateral to ensure they remain solvent. In periods of rapid price declines, more collateral must be added at a higher collateral ratio exacerbating their capital inefficiency. Technically algorithmic stablecoins are the most scalable as they require no collateral at all.

1.4 Centralization

Web3 applications are designed to distribute the ownership, control and decision-making democratically to its stakeholders. The more distributed a network is, the harder it is to make it scalable as you need to align and coordinate with multiple stakeholders instead of one. Stablecoin users have opted to rely on highly trusted centralized solutions, USDT and USDC, over their decentralized counterparts due their scalability constraints.

2 The Solution: Su Protocol

Su Protocol decomposes Sui, a volatility asset, into two asset classes: Leveraged Sui (xSui) and Beta Coins. Unlike previous decentralized designs that rely on over-collateralization and liquidations to maintain the peg against volatility, Su transfers the undesired volatility to a new asset.

- **Leveraged Sui (xSui).** It is a perpetual contract with no funding rate or liquidation. Users can mint by depositing Sui. Its leverage depends on the current amount of stablecoins issued and Sui's US Dollar price.

- **Fractional Sui (fSui).** It is a floating stablecoin with a beta of 0.1. It serves as the currency for the Sui Network, tracking 10% of Sui's volatility.

- **Sui Dollar (SD).** It is a beta coin with a beta of 1, which makes it a stablecoin.

The system is designed around the following invariant:

$$N_{Sui} * NAV_{Sui} = N_{xSui} * NAV_{xSui} + N_{fSui} * NAV_{fSui} + N_{SD} * NAV_{SD}$$

Where N represents the quantity of the asset and NAV the net asset value.

The value of all the collateral, determined by the amount of Sui multiplied by its net asset value, must remain equal to all the coins issued by the protocol. To ensure the system stability, Su protocol limits the supply of the Beta coins based on the amount xSui minted, as the system needs enough xSui to absorb their volatility. It is important to note that the collateral ratio between Su coins does not mandate users to overcollateralize their positions.

A stablecoin is a Beta coin with a beta of 1, as it represents no volatility. Technically, there is no limitation of the type of Beta coins Su can issue. It can mint a coin with a beta of 0.5 just as easily as it mints SD or fSui.

Su protocol maintains the peg of its Beta coins by adjusting the net asset value of xSui according to Sui's US Dollar price. In essence, xSui users take on the wins and losses of the Beta coin users, as they are entitled to the left over collateral after the Beta coin users are paid.

3 Two Way Relationship

fSui tracks a fraction of Sui's price. It moves 10% of Sui's total price movement. For instance, if Sui appreciates 20%, fSui will appreciate 2%. In that sense, fSui can be considered a low-volatility stablecoin or a "floating stablecoin" because 90% of its beta is correlated with the US dollar while the remaining 10% is with Sui. The purpose of having a 0.1 beta is to allow fSui to be more exposed to USD price than to Sui, functioning as a hedge against the devaluation of USD per Sui. If we assume that the price of Sui will appreciate over time, we can think of fSui as a deflationary token.

fSui unites important stablecoin traits: low volatility, decentralized, and liquidity. The low volatility stems from the 0.1 beta. At the same time, decentralization is ensured by storing Sui on-chain instead of with a traditional financial custodian. The only limitation that could affect fSui is its liquidity, which depends on the balance of xSui since its users will get leveraged returns from the fSui and SD deposits. Therefore, a substantial amount of xSui is necessary to support a smaller amount of fSui. The minting of fSui can occur smoothly without affecting the NAV if there is an adequate amount of xSui. SD behaves similarly to fSui. The only difference is that it always has a net asset value of 1.

As mentioned earlier, The xSui coin is the long leverage token whose returns are shared with its minters by absorbing the volatility from fSui and SD. The xSui supply is contingent upon the market's appetite for risk, which historically seems to exist consistently among traders across all market conditions.

4 Liquid Staking

The Sui collateral on Su will be staked on validators to earn around 3 APY[7]. This yield will be available for SD holders who stake their stablecoins. Assuming that Su will have a collateral ratio of 200%, the staked SD stablecoin will have a native APY higher than 6%, which makes it more attractive than U.S. T-Bills's 5.5% APY[8]. This is due to the fact the yield earned from the Sui backing fSui and xSui is rewarded to SD stakers. Su will issue a yield bearing coin to SD stakers to allow them to liquify their positions to be used in DeFi.

5 Invariants

5.1 Collateral

$$\lambda x = \frac{N_{xSui} * NAV_{xSui}}{N_{Sui} * NAV_{Sui}}, \lambda f = \frac{N_{fSui} * NAV_{fSui}}{N_{Sui} * NAV_{Sui}}, \lambda d = \frac{N_{SD} * NAV_{SD}}{N_{Sui} * NAV_{Sui}}$$

$$\lambda x + \lambda f + \lambda d = 1$$

5.2 xSui NAV

$$NAV_{xSui} = N_{Sui} * NAV_{Sui} - \frac{N_{fSui} * NAV_{fSui} + N_{SD} * NAV_{SD}}{N_{xSui}}$$

5.3 fSui NAV

$$r_{fSui} = \beta * (\frac{NAV_{Sui}(t)}{NAV_{Sui}(t-1)} - 1)$$

$$NAV_{fSui} = (1 + r_{fSui}) * NAV_{fSui}(t - 1)$$

5.4 Collateral Ratio

$$CR = \frac{N_{xSui} * NAV_{xSui}}{N_{fSui} * NAV_{fSui} + N_{SD} * NAV_{SD}} * 100\%$$

References

All credits to f(x) by Aladdin DAO https://github.com/AladdinDAO/aladdin-v3-contracts/tree/main/whitepapers

[1] DefiLlama, https://defillama.com/?stables=true&tvl=false

[2] Moodys https://www.moodys.com/web/en/us/about/insights/data-stories/stablecoins-instability.html

[3] CoinDesk, https://www.coindesk.com/business/2023/03/13/usdc-stablecoin-regains-dollar-peg-after-silicon-valley-bank-induced-chaos/

[4] Maker DAO, https://developer.makerdao.com/dai/1/

[5] Coin Desk, https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/

[6] Binance, https://www.binance.com/en-IN/square/post/244376

[7] SuiScan, https://suiscan.xyz/mainnet/validators

[8] Treasury, https://home.treasury.gov/resource-center/data-chart-center/interest-rates/TextView?type=daily_treasury_bill_rates&field_tdr_date_value=2024