Attack on algorithmic stable coins

Payam NAGHDI

payamnaghdy2@gmail.com

Abstract –

1 Motivation

Stability for a currency is a must to be used by businesses such that they won't be exposed to volatility and risks of the currency; options in the crypto-currency space are mostly central (using fiat currency or gold as collateral), but some attempts were made to create a decentralized stable coin with a two token system one stable and other one unstable named governance token to absorb the volatility. But there is a fundamental issue with the design of these coins that can cause the stable coin to depeg from the fiat currency, and the governance token will evaporate.

2 Background

The algorithmic (two token systems) coin maintains the peg by incentivizing arbitragers:

Let S be the stable coin, and G be the governance one. The protocol reads the price of governance coin in the fiat currency from an oracle and assumes the stable coin price is always 1 unit of the fiat money.

For example price of G is $100, there will be two scenarios: If the price of S falls below $1, there is a chance for arbitragers to buy S from the market and burn it. Then the protocol gives them an equivalent value of G (for example, 100 S is one G in this example) then they sell G for a profit. This increases the demand for S (buying S) and decreases the supply (burning to get G), so the price of S will increase to $1 again

So if the price of S falls to 90 cents, arbitragers can buy 100S for $90, then burn them to get one G and sell that for $100 and collect 10 dollars of profit.

If the price of the S goes above $1, there is an arbitrage possibility to buy G, then burn them for S (For instance, arbitrager burns 1G and gets 100S), then sells S in the market to accumulate the gain.

3 Attack by selling S

Although an attack by selling a considerable amount of S, the protocol burns S and creates large amounts of G to maintain the peg. Then, because there are more Gs in the market price of B falls; for the next round of arbitrage, more Gs need to be created to sure up the price of S. The protocol falls into the death spiral. It can be done on paper, but the attacker is at risk of losing significant amounts of money during the attack, and it's doubtful to happen in the real world.

4 Possible attack

The two token systems can work for some time, but it allows an attacker to bring the system down and make money from it.

4.1 First step

The attacker needs to buy G and burn them to get S. This causes a rise in the price of G and a fall in the price of S, so the attacker needs to do this in batches and wait for the protocol to recover the peg, so the amount of S that he/she owns does not depreciate.

4.2 Second step

The attacker will open a short position on G on the market. This step increases G supply on the market so that the price will fall (the attacker might need to open the position gradually to remain unknown in this step).

4.3 Third step

The Ss in the first step act as a margin of safety and control on risk for the attacker. He/She sells the Ss. This step also needs to be done gradually to make sure the Ss owned by the attacker will be sold at the right price, and this will trigger the algorithm to step in and maintain the price, so it creates G in the process cost of G will fall. So the short position goes into profit. The protocol will fall into the death spiral with the right amount of S and the right selling pace.

5 The Luna's case

5.1 Introduction

Luna and TerraUSD were the two token system coins Luna acted as G and TerraUSD(UST) as S.

Figure 1: Circulating Supply of luna

5.2 Circulating Supply

A glance at the circulating supply of Luna suggests that the meltdown was caused by an attack similar to section 4. As we can see in Figure 1 in section A of the chart protocol works normally, and the supply of Luna changes randomly(to maintain the peg in the normal situation), but in section B, there is a pattern in the supply change and decreases linearly then attacker waits for the UST to recover (the rise in the supply after the decrease) then does it again till it falls into the death spiral.

6 Proposed Work

- In depth analysis of the attack
- Propose a new system for a non-volatile coin with no peg (one token system that incentivizes the miners, or stakeholders, to burn assets in times of inflation, with a promise of more significant returns when the price recovers with the bigger returns in the times of rapid growth.