SECURITY AUDIT SPERAX PROTOCOL

BANKRUPT EXPLOIT IN PROTOCOL DESIGN

CASTVELL
CASTVELL

Content Table

INTRODUCTION

Sperax protocol propose an interesting way of capital optimization, for a fractional reserve similar TRADFI, with this, Sperax protocol could have a vulnerability in a specific case.

As mentioned in USDS Whitepaper, anyone can arbitrage to generate profit, burning and minting according to the case, if the peg is below 1 USD, USDS can be redeemed to obtain:

$$\text{Collateral} + \text{SPA} = 1\ \text{USD}$$

1. SPA is minted when redeeming USDS.

And in the second case, if the peg is below 1 USD, you can minting USDS by giving the protocol:

$$\text{Collateral} + \text{SPA} = 1\ \text{USD}$$

2. SPA is burned when minting USDS.

The protocol has other very interesting mechanics, but in this analysis we are going to use this information for the audit and analysis of a possible bankrupt.

ISSUES

Problem

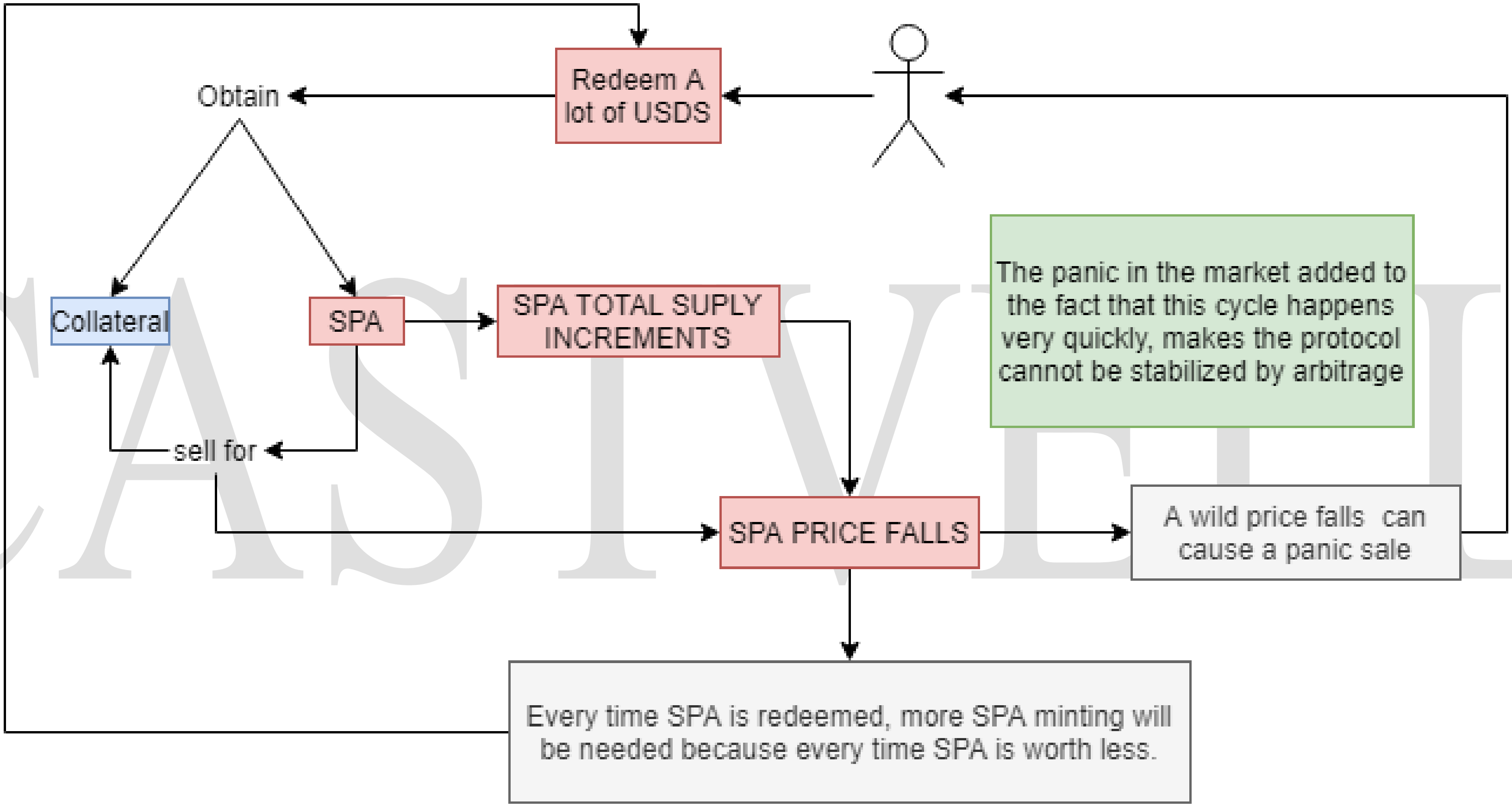
As we know in crypto growing is fast but decrease is exponential, fear is a stronger feeling than greed. Taking this into account, we are going to suppose that there is a whale or a group of people who wish to withdraw from the protocol, either due to false and / or malicious news, due to liquidity taking or panic selling of the market in general.

Assuming this situation, the following events could occur:

A. A large amount of USDS is redeemed in a short period of time.
B. The protocol would adjust the price exponentially through the oracle, upon detecting the sudden price change.
C. Once the USD has been redeemed, the whale proceeds to sell the SPA, which causes a considerable drop in the price of the SPA.
D. If the SPA drops in price, it will take more SPA minting to represent the same amount of USD when redeeming USDS.
E. A sharp drop in the USDS and the SPA protocol token could cause a panic selling of the token holders.
F. In a panic selling, once users claim their collateral, they would proceed to sell the SPA to recover them liquidity.
G. Taking into account (1), more SPA is minting as the price of the SPA continues to fall, therefore, there would be many more SPA tokens in circulation, increasingly devaluing its value.

H. Surely some profit takers try to mine USDS to generate profit, but in this hypothesis, it is assumed that the aforementioned loop passes so fast that they do not have time to arbitrate the situation.

I. Ultimately, this loop would lead to the protocol going bankrupt, as there will not be enough collateral for all users to claim their USDS.


Redeem A lot of USDS
Obtain
Collateral
SPA
SPA TOTAL SUPLY INCREMENTS
sell for
SPA PRICE FALLS
The panic in the market added to the fact that this cycle happens very quickly, makes the protocol cannot be stabilized by arbitrage
A wild price falls can cause a panic sale
Every time SPA is redeemed, more SPA minting will be needed because every time SPA is worth less.

J. This Loop would lead to:

$$SPA\ supply = \infty$$
$$SPA\ price = 0$$

Bug

A problem that would arise as a consequence of the bankruptcy protocol is that if the price of the SPA tends to zero then the amount of SPA that must be printed would tend to infinity, since if the percentage of Collateral is equal to 75% so when redeeming USDS:

Collateral Price * amount of Collateral tokens = 0.75 USD

SPA Price * amount of SPA tokens = 0.25 USD

But if the SPA price tends to 0 due to the loop mentioned above, then:

$$0 \quad * \text{ amount of tokens} \quad = \; 0.25\text{USD}$$

Since no number multiplied by zero gives 0.25, then the number of tokens would tend to infinity, which will surely generate an error in the contract, and finally, prevent users who arrive after the event from being able to redeem their USDS.

$$0 = \frac{0.25\text{USD}}{\text{Amount Of Tokens}}$$

The only way that the condition is met is that the amount of tokens shop at ∞

Analysis

Having a fractional reserve system (in which a currency is not fully collateralized) always carries this problem, in fact, in traditional banking this has happened several times. In TRADFI the usual solution is to make a "Corralito", as happened in Argentina a few years ago, it basically consists in block money withdraws while the market recovers, similar to what Wall Street does, but instead of freezing shares, in a "Corralito", freezes the funds of bank users for a certain amount of time, this happens as long as the bank adding all its assets does not have enough money to return the money.

However, the minting of SPA makes it more difficult to control the situation, in fact this arbitration base system had already been used by another protocol, which suffered the bankruptcy process mentioned above. It is known that for the Sperax protocol to survive this situation, people should only temporarily stop selling the SPA, meanwhile arbiters stabilize the price, but the human being is always irrational, continues to command and always takes actions just for personal interest. Therefore, you always have to expect the worst when designing a protocol.

It must also be taken into account that in crypto what matters most is the first impression, usually a protocol is born, creates hype, many more users get into the project than expected, a stress test is generated due to the massive entry of users, it determines if the protocol is viable and delivers on what was promised to users:

1. If everything works correctly and the expectations given to users are met, the protocol will make a name for itself in the ecosystem and as mentioned in the USDS whitepaper, the protocol will give users more and more confidence as time goes by.
2. If there is a problem with protocol, or the expectations given to the users are not met or change on the way, there is usually a massive exit of users, and although the protocol corrects the failures, it almost always does not have the same traction again.

Possible solutions

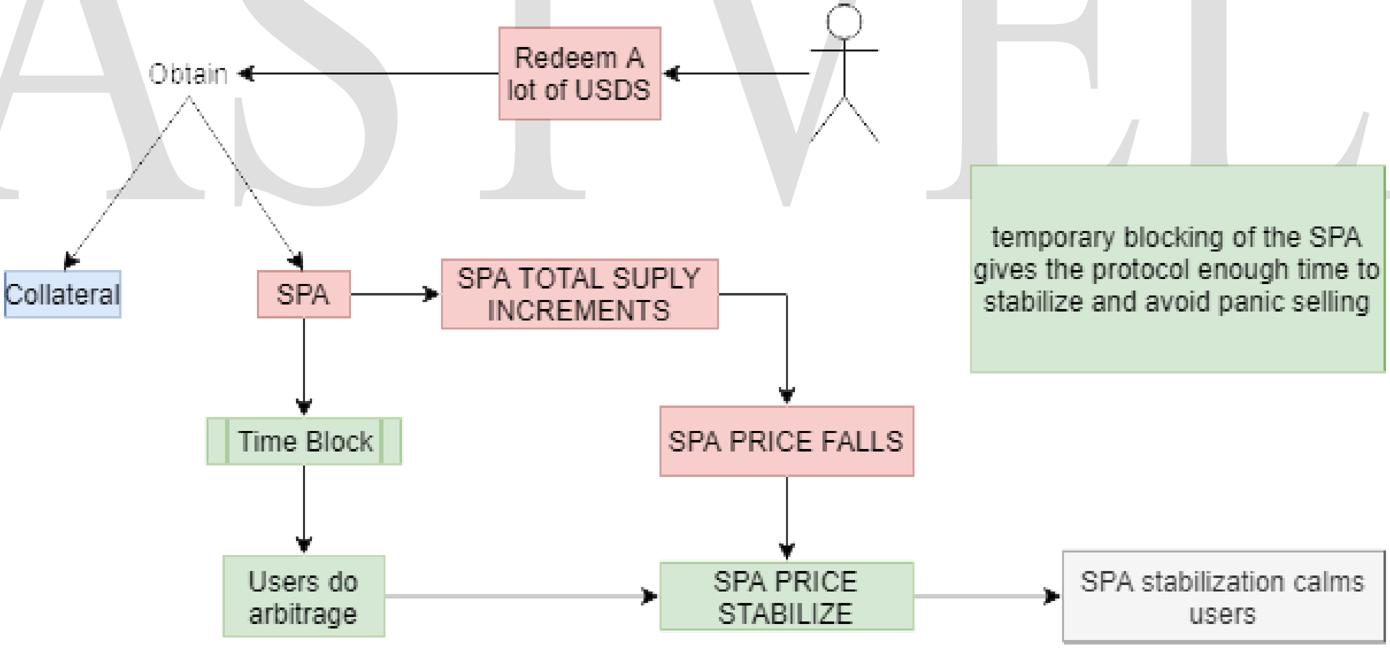
Bug

A. Establish a conditional in the USDS redemption function in which, if the SPA price tends to 0, only the collateral is returned, which would imply that users have real losses.

B. Establish a conditional in the USDS redemption function in which, if the price of the SPA tends to 0, the funds are blocked until the interest generated by the collateral in the DEFI aggregator covers the losses that users would have for the price of the SPA.

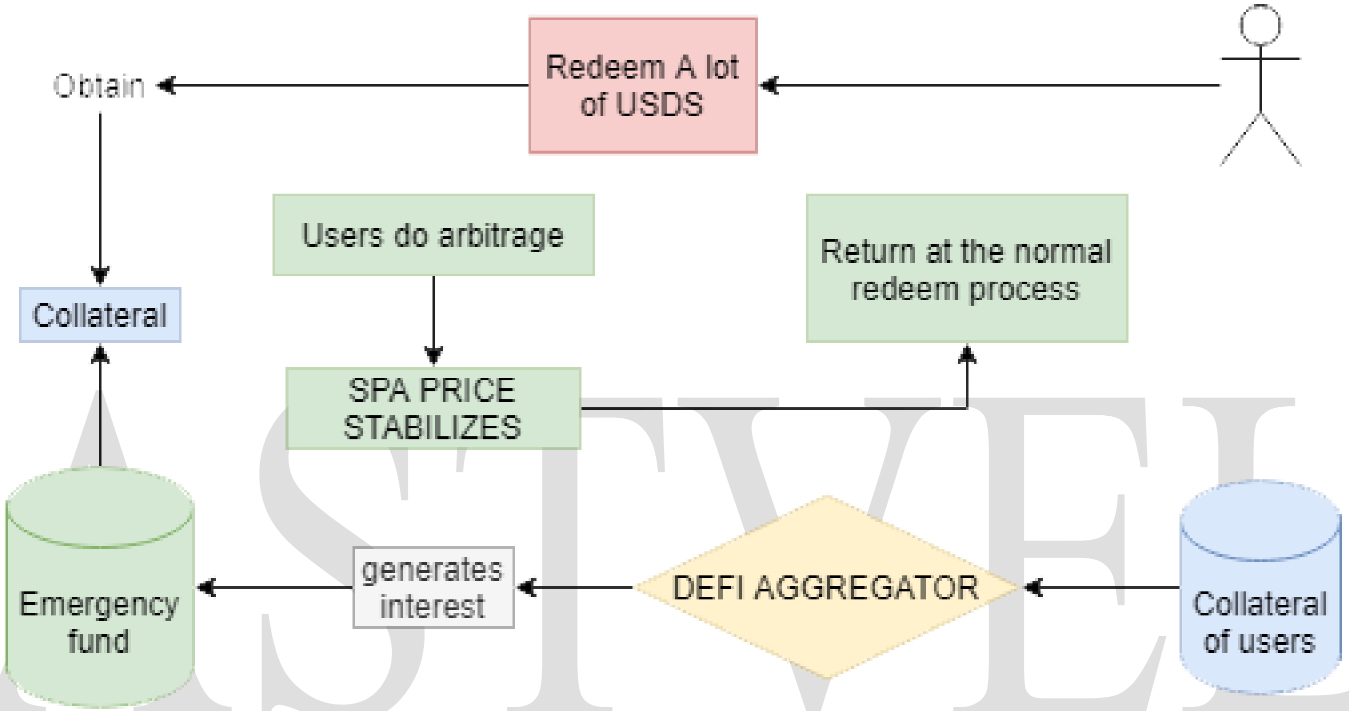
Problem

A. Corralito:


Redeem A lot of USDS
Obtain
Collateral
SPA
SPA TOTAL SUPLY INCREMENTS
temporary blocking of the SPA gives the protocol enough time to stabilize and avoid panic selling
Time Block
SPA PRICE FALLS
Users do arbitrage
SPA PRICE STABILIZE
SPA stabilization calms users

Modify the contract so that all the SPA generated when USDS is redeemed, is blocked for a period of time long enough for the protocol to stabilize.

B. Emergency Fund:



The protocol offers the option of generating interest with the collateral of the users, which opens the door to allocate a percentage of these interests to a multi-sign treasury, which will only be used in the case of a sufficiently abrupt fall, as to bring the price of the SPA to 0, this treasury would allow users not to lose all their funds when redeeming their USDS or at least not to lose so much money.