Simple summary

Proposing new functions to further improve Aave V3 “New Risk Management Parameters”:

Implement 24 hours & Max collateral usage cap to limit the size of all kind of attacks, and hacks

Abstract

Aave is vulnerable to all kinds of risks(e.g. infinite minting attack, oracle manipulation attack, collateral crash attack, collateral dumping , collatela price manipulation attacks , Aave smart contract hacks, v3 Portal hacks, etc), Aave v3 Risk Management parameters better than any other protocol, and we can make it even better.

Motivation

- We can’t prevent all the risks from occurring, and there is always will be risk attach to the Aave
- We can minimize the risk sizes by setting up some usage limitations
- If Aave gets attacked/hacked in bigger size, then it’ll cause reputation damage, financial damage to SM funds, AAVE token value drop, and might cause protocol bankruptcy.

Concerns & problems:

- Collateral Crash:

if a protocol gets hacked or etc, and the token becomes worthless, then all the token holders instead of selling it(probably can’t sell or selling will effects the price of the token) on open market, they use it to borrow other safe assets on Aave * Most concerning collaterals are: USDC, DAI, TUSD, WBTC, WETH, all other Gov tokens

- e.g. (“Cashio” a stale coin on Solana) etc
- Most concerning collaterals are: USDC, DAI, TUSD, WBTC, WETH, all other Gov tokens
- e.g. (“Cashio” a stale coin on Solana) etc
- Collateral dumping:

if whale holders of a token want to dump a huge mount of token, then they instead of selling it (selling will affects the price of the token) on the market, they will use it as collateral to borrow other token from Aave(more similar tokens on the market will drawn liquidity from Aave until the Aave governance reacts to it) * Most concerning collaterals are: all the Gov tokens, and small cap Gas tokens

- Most concerning collaterals are: all the Gov tokens, and small cap Gas tokens
- Collateral price manipulation:

Few whales(or single big whale) pump the price of a token,and dump all of it at once to drawn other collaterals * Most concerning collaterals are: any cap gov tokens, most concerning are smaller cap collaterals that use DEX as the majority price oracle

- e.g Inverse.Finance recent attack
- Most concerning collaterals are: any cap gov tokens, most concerning are smaller cap collaterals that use DEX as the majority price oracle
- e.g Inverse.Finance recent attack
- Infinite minting:

collaterals like USDC, WBTC, WETH, are relies on multisig signers, so there is always risk of infinit minting, or permissionless mining by attacker(if the wallets are gets attacked, etc); if Makerdao or other protocols gets hacked, and there is infinit minting risks * Most concerning collaterals are: USDC, WBTC, WETH, DAI, etc

- e.g. (“Cashio infiniti minting” a stale coin on Solana)
- Most concerning collaterals are: USDC, WBTC, WETH, DAI, etc
- e.g. (“Cashio infiniti minting” a stale coin on Solana)
- Aave smart contract breach, all kinds of collateral attacks, and all kinds of hacks via flash loan, etc:

I’m pretty sure there are multiple ways to hack Aave smart contract, almost every pool is vulnerable to attacks. * Most

concerning collaterals are: USDC, DAI, ETH, WBTC, like bigger liquidity pools gets hack in bigger size, then it most likely bankrupt Aave protocol;

- I'll post more details about it.
- Most concerning collaterals are: USDC, DAI, ETH, WBTC, like bigger liquidity pools gets hack in bigger size, then it most likely bankrupt Aave protocol;
- I'll post more details about it.
- Aave v3 portal attacks: I'll post more details about it
- etc different kinds of Attacks & hacks

*

Solutions:

24 hours collateral usage cap:

Why is it 24 hours?: because most of the attacks, and hacks will be operated matter of few minutes or free hours(finish the attack before anybody finds out), and all the attacks will be operated in same day, so by setting up a 24 houser cap limit, the lost of any kinds of attack will be limited in size, and give the Aave community enough time to react to the attacks

If we set this limitation, then attackers/hackers will choose other money market protocols instead of Aave(because attacks will be limited in size).

How does it work?:

- By setting 24 hours collateral usage amount limitation, only limited amount of collateral can be used as collateral to borrow other assets in 24 hours period, if the amount hits the max limits, then wait for other borrowers to return the borrowed amount, then new borrowers can borrow
- More well thought out/formulated details will be available in the future

(it's only abstract amount)Cap Amount setting: (e.g. ETH = $200 million, USDC = $10 million, AAVE = $10 millon)

Future thoughts: how do we set the amount? Updating the amount? Etc

Trade offs: (1)limits the single day large amount collateral users (2)if there is above max amount collateral users, then will be limited(we'll set the cap amount based on historical data, so it won't limits as much); (3) etc

Max collateral usage cap:

Why set a Max collateral usage cap?: because protect Aave from all kinds of attacks(e.g. Collateral crash, Collateral dump, and collateral Infinite minting, and all kinds of Smart contract attacks to collateral tokens, etc

Over all it will limits the risk exposure of Aave to collateral attack risk

How does it work?:

- By setting Max collateral usage amount limitation, only limited amount of collateral can be used as collateral to borrow other assets at the same time, if the amount hits the max limits, then wait for other borrowers to reuters the borrowed amount, then new borrowers can borrow
- More well thought out/formulated details will be available in the future

(it's only abstract amount)Amount setting: (e.g. ETH = no limit(because ETH is safe asset), USDC = $500 million, AAVE = $100 millon)

Trade offs: limits the same time collateral usage amount of potential risk bearing collaterals

Potential implementations:

- Testing it out, and setting best efficient cap amounts for different pools will take some work
- (if Aave community deicide to implement it)I don't think it's hard to implement(I suggest implementing it to V2, and V3)

Future improvements:

- Set dynamic cap amount that will change via TVL, fund returning amount

- Set a automated cap changing function based on How many address, and market size of the pool
- Set a credit score based limit illumination function for small amount users
- etc

Additional proposal(extra consideration point only):

Make more stable coins available to use as collateral: with help of Max collateral usage cap, we can set small amount of collateral usage cap for each stable coins; More detailed proposal will be available in the future;

Personal thoughts:

Collateral usage cap will limit Aave at some point, but it'll be way helpful when it comes to protect Aave from All kinds of risk

I don't think setting collateral usage cap should be a long term solution, but currently Aave has to be safe first, and then work on how to make the limitations efficient over time(with more experiments, tests, more data)

I'm thinking on working on address based credit score oracle to eliminate the 24 housers collateral usage cap for frequent small amount Aave users,etc

Thank you for reading all the way though, if you liked it, then drop a like to show you support, thank you!