Maker Dai Delegate Audit

Justin Bebis, Goober, & BM Apprentices

Design

Dependency on another vault means system failure will cause widespread damage. Consider when allocating debt to this strategy. Otherwise I can see how this strategy would flatten yields and help facilitate broad crypto adoption through Yearn.

Most issues can be averted by calling tend trigger frequently and adjusting as necessary, so ensure automated monitoring is extremely resilient. It would also be interesting to increase collateralization automatically if one of your internal oracles senses volatility so that you can weaken dependence on centralized emergency response units.

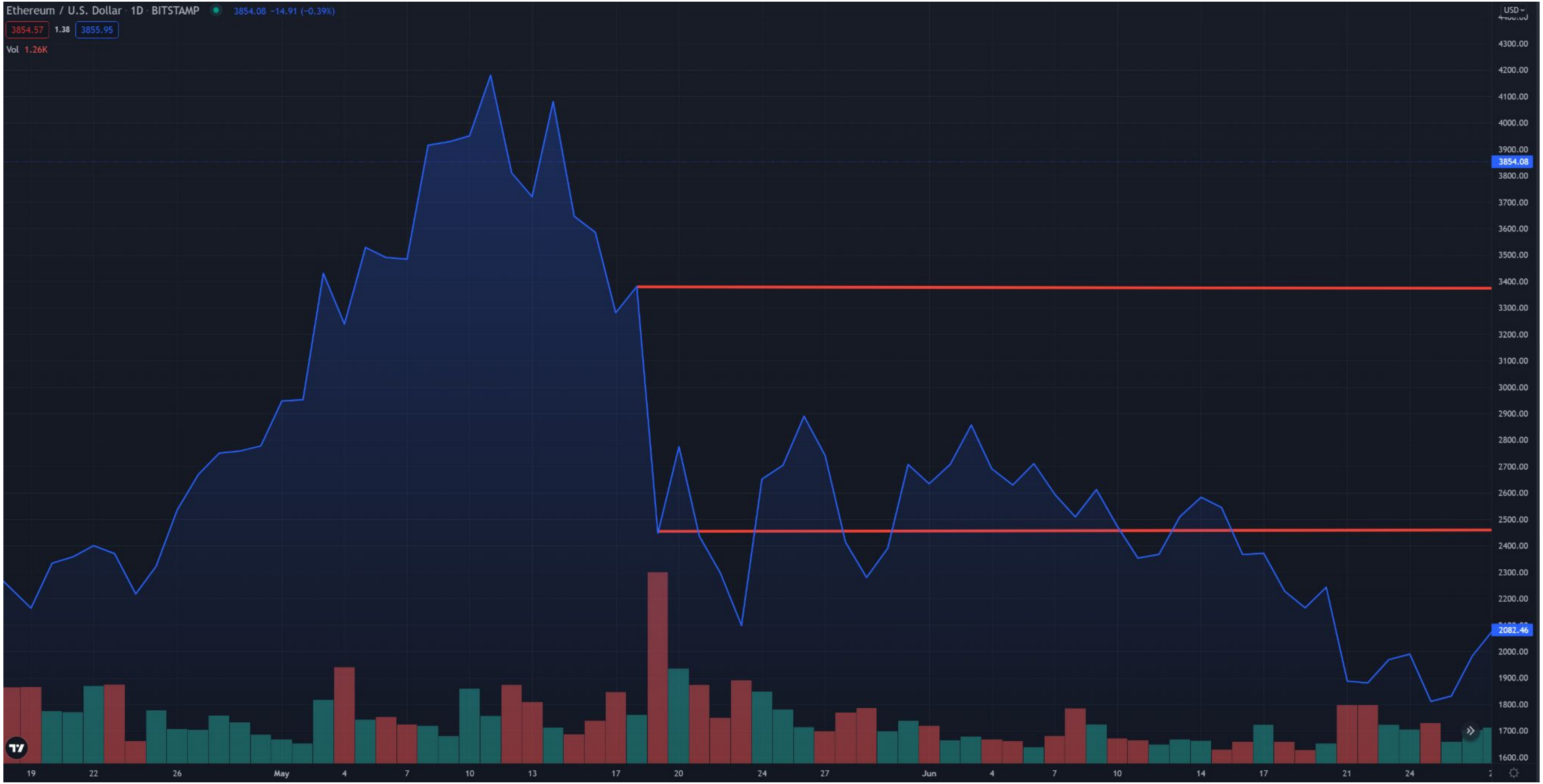
Very lovely strategy with very interesting implications - very excited to see what other auditors think.

Protecting against VAR shocks

Tolerating a 210% c-ratio would mean a 39% drawdown would liquidate an ETH-A pool, 29% an ETH-B pool, and 17% an ETH-C pool. Under extreme conditions, this would potentially liquidate the underlying collateral in under a day if measures aren’t taken to protect the funds, which would result in significant losses. Not quite disaster resistant.

I would consider tightening the tolerance to 10% or less as opposed to lowering the collateral ratio - even lowering the ratio to 220% with a 5% tolerance would be safer and allow more leverage. More frequent adjustments and tighter controls would facilitate more TVL with less risk.

(see chart on the following page for example)


Ethereum / U.S. Dollar · 1D · BITSTAMP
3854.08 −14.91 (−0.39%)
3854.57
1.38
3855.95
Vol 1.26K
USD
4300.00
4200.00
4100.00
4000.00
3900.00
3854.08
3800.00
3700.00
3600.00
3500.00
3400.00
3300.00
3200.00
3100.00
3000.00
2900.00
2800.00
2700.00
2600.00
2500.00
2400.00
2300.00
2200.00
2082.46
2000.00
1900.00
1800.00
1700.00
1600.00
19
22
26
May
4
7
10
13
17
20
24
27
Jun
4
7
10
14
17
21
24

nitpicks

Use of msg.sender - control context better with msgSender() >:)

Natspec on constructor will prevent a lot of confusion - better documentation on names in general will help with understanding for future reviews/audits. More descriptive names that include ‘debt’ and ‘vault’ will also help with this across the board.

_sellCollateralToRepayRemainingDebtIfNeeded

Line 252, safemath will force a revert if the investment has accrued enough value to be worth more than the debt to maker. This shouldn’t ever be true within the parent function’s if-block after the two rounds of repayment and withdrawal, but it should maybe be formally verified / fuzzed heavily if it hasn’t been. Even in the event of a safemath revert this function is relatively low risk so if there was room i’d probably categorize this under nitpicking.

Great Stuff

Inputs and outputs are tightly controlled with the use of min() and security risks inherent to oracles are greatly mitigated. The Maker Security Oracle was especially lovely to see.

The vault also flexes Yearn’s powerful access control, able to use setters that would be considered insecure in the hands of most other protocols.